BANCO DE PORTUGAL
EUROSISTEMA

BOAS PRÁTICAS RELATIVAS À VIDEOCONFERÊNCIA COMO PROCEDIMENTO ALTERNATIVO DE COMPROVAÇÃO DE ELEMENTOS IDENTIFICATIVOS

I. INTRODUÇÃO

A Instrução no Banco de Portugal n.º 9/2017, de 3 de julho, estabeleceu pela primeira vez a possibilidade de recurso à videoconferência como procedimento alternativo de comprovação dos elementos identificativos, pelas entidades sujeitas à supervisão do Banco de Portugal em matéria de prevenção do branqueamento de capitais e do financiamento do terrorismo (doravante, apenas "entidades obrigadas"). Este procedimento foi definido pelo normativo acima citado – definição que se mantém atualmente – como um *"(…) meio de comunicação não presencial de identificação do cliente que consiste numa forma de comunicação interativa que permite a transmissão e captação de som, imagem e dados em tempo real."*

Após a entrada em vigor desta Instrução, foi emitida a Carta Circular n.º CC/2018/00000038, de 14 de junho ("Carta Circular n.º CC/2018/00000038"), que listou um conjunto de clarificações relativas ao quadro normativo vigente, assim como um conjunto de orientações tendentes ao seu efetivo cumprimento, e incluiu ainda a indicação de que a respetiva observância seria posteriormente objeto de ações de verificação *on-site* por parte do Banco de Portugal, tal como veio a suceder.

A 26 de setembro de 2018 foi publicado o Aviso do Banco de Portugal n.º 2/2018, ("Aviso n.º 2/2018"), que, entre outros aspetos, incorporou no seu Anexo I os requisitos de admissibilidade do recurso à videoconferência[1] enquanto meio ou procedimento alternativo de comprovação dos elementos identificativos que ofereçam graus de segurança idênticos aos exemplificados nas subalíneas i) e ii) da alínea c) do n.º 4 do artigo 25.º da Lei n.º 83/2017, de 18 de agosto ("Lei n.º 83/2017"), revogando a Instrução no Banco de Portugal n.º 9/2017, de 3 de julho. Este instrumento incorporou ainda algumas das orientações constantes da Carta Circular n.º CC/2018/00000038.

O Banco de Portugal decidiu, com base na avaliação que fez do grau de cumprimento do quadro normativo vigente tendo em conta os resultados das ações de supervisão efetuadas, assim como nas dificuldades identificadas na compreensão do mesmo pelo setor, elaborar o presente documento, por via do qual se esclarecem vários aspetos relacionados com os requisitos e obrigações aplicáveis, e se define um conjunto de boas práticas que devem nortear a atuação das entidades obrigadas na implementação e gestão da videoconferência como procedimento

[1] Assim como o recurso à identificação por prestadores qualificados de confiança.

alternativo de comprovação de elementos identificativos. Neste âmbito, foi ainda considerado oportuno definir algumas orientações relativas à relação da entidade financeira com o cliente.

As presentes orientações visam contribuir para o robustecimento dos meios, mecanismos e procedimentos adotados pelas entidades obrigadas neste contexto e, nessa medida, para o efetivo cumprimento do quadro normativo aplicável. Para o efeito, o Banco de Portugal, na elaboração destas boas práticas, socorreu-se não apenas do seu conhecimento enquanto supervisor, mas também das orientações e posições expressas por organismos internacionalmente reconhecidos nesta matéria, em particular pelas Autoridades Europeias de Supervisão[2], o Grupo de Ação Financeira[3] e a Comissão Europeia[4].

Esclarece-se ainda que é admissível o recurso ao procedimento de videoconferência para comprovar os elementos de identificação do representante de uma pessoa coletiva, pelo que, para efeitos das presentes boas práticas e sempre que aplicável, deverá entender-se a expressão "cliente" como referente também aos representantes do cliente.

Por fim, salienta-se a natureza não exaustiva e dinâmica das presentes boas práticas, que se pretendem adaptáveis ao surgimento de eventuais novas diretrizes nesta matéria, incluindo de natureza regulamentar ou tecnológica. Neste contexto, reitera-se que o recurso à videoconferência como procedimento alternativo de comprovação de elementos identificativos não desonera as entidades obrigadas do estrito cumprimento do dever de identificação e diligência que lhes é aplicável, nomeadamente através da realização das diligências complementares que se revelem necessárias (*vide*, para o efeito, o artigo 2.º do Anexo I do Aviso n.º 2/2018). Nessa medida, as entidades obrigadas devem garantir, no âmbito deste procedimento como de qualquer outro enquadrável no dever de identificação e diligência, não apenas o cumprimento do quadro normativo expressamente previsto para o mesmo (nomeadamente, o disposto no Anexo I do Aviso n.º 2/2018), como também a adoção de uma abordagem baseada no risco, garantindo a aplicação de medidas de identificação e diligência proporcionais ao perfil de risco do cliente e às características da relação de negócio.

[2] Cf. JC 2017 81 OPINION ON THE USE OF INNOVATIVE SOLUTIONS BY CREDIT AND FINANCIAL INSTITUTIONS IN THE CUSTOMER DUE DILIGENCE PROCESS:
https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf
[3] Cf. FATF Guidance on Digital ID:
https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html
[4] Cf. Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions:
https://ec.europa.eu/info/files/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-December2019_en

II. BOAS PRÁTICAS NO ÂMBITO DOS REQUISITOS PRÉVIOS À ADOÇÃO DA VIDEOCONFERÊNCIA

BP 1: Adequação e suficiência da análise de risco

Conforme resulta expressamente do quadro normativo vigente, previamente à adoção da videoconferência como procedimento alternativo de comprovação de elementos identificativos, a entidade obrigada deve efetuar uma análise de risco que identifique de forma unívoca os riscos de BC/FT que lhes estão especificamente associados, assim como os meios, procedimentos e mecanismos de controlo que se mostrem adequados à respetiva mitigação.

É considerada boa prática que, em momento prévio à elaboração da análise de risco, as entidades obrigadas incluam o responsável pelo cumprimento normativo (RCN) nos trabalhos de desenvolvimento ou alteração do procedimento de videoconferência. A inclusão do RCN durante os trabalhos de desenvolvimento permite, desde logo, eliminar ou mitigar determinados riscos de BC/FT, contribui para que a análise de risco seja suficientemente detalhada, e garante que o RCN dispõe da informação e conhecimento específicos essenciais para a elaboração do seu parecer prévio sobre esta análise.

A análise de risco deve conter um mapeamento dos riscos de BC/FT inerentes ao procedimento – e respetivos mitigadores –, incidindo, nomeadamente, sobre:

- A **tipologia de clientes** elegíveis;
- O tipo de **documentos de identificação** aceites;
- A tipologia de **produtos, serviços e operações** acessíveis através deste procedimento;
- Os **riscos de BC/FT associados ao procedimento** (nomeadamente, os resultantes da tipologia de clientes elegíveis, tipos de documentos de identificação aceites e tipologia de produtos, serviços e operações acessíveis).

Finalmente, recorda-se que as práticas de gestão de risco adotadas deverão ser revistas e atualizadas de modo a acautelarem adequadamente, a todo o tempo, a realidade operativa específica da entidade obrigada. Nessa medida, a introdução de quaisquer alterações ao procedimento implica, naturalmente, a revisão dos requisitos prévios, nomeadamente da análise de risco inicialmente efetuada.

BP 2: Riscos associados à tipologia de clientes

- **Identificação**

A robustez e a segurança do procedimento de videoconferência devem influenciar, desde logo, a determinação das tipologias de clientes que o podem utilizar. Assim, o incremento da fiabilidade do procedimento permitirá às entidades obrigadas, em princípio, incorrerem num risco intrínseco mais elevado na escolha das tipologias de relações de negócio elegíveis.

A entidade obrigada deve considerar os fatores de risco inerentes à tipologia de clientes elegíveis, incluindo:

- A qualidade de "pessoa politicamente exposta", "membro próximo da família", "pessoa reconhecida como estritamente associada", ou "titular de outros cargos políticos ou públicos";
- O risco associado (i) à respetiva situação profissional; (ii) à atividade desenvolvida; (iii) a clientes residentes ou que desenvolvam atividade em zonas de risco geográfico mais elevado, ou (iv) a clientes que apresentem uma morada fiscal diferente da morada de residência;
- O risco associado à pessoa coletiva ou ao centro de interesses coletivos sem personalidade jurídica, quando a pessoa singular a identificar seja um representante deste tipo de clientes.

A entidade obrigada deve ainda ponderar o impacto que o recurso à videoconferência tem no perfil de risco dos clientes que recorrem à mesma. Quando relevante, tal deve ser tido em conta no desenvolvimento da ferramenta destinada à definição e atribuição do perfil de risco de clientes.

- **Mitigação**

Se a entidade obrigada optar por incluir clientes de risco mais elevado na tipologia de clientes elegíveis, deverá assegurar-se de que a sua análise de risco inclui procedimentos de controlo aptos a mitigar esse mesmo risco (e.g.: previsão de recolha de informação adicional, nomeadamente através da inclusão no *script* de conversação de perguntas específicas direcionadas para tipologias de clientes de risco mais elevado).

Em particular, esclarece-se que a implementação de procedimentos de videoconferência de natureza simplificada ou particularmente expedita, que prevejam procedimentos de identificação e diligência idênticos para todos os clientes - independentemente do seu concreto perfil de risco -, não é compatível com a possibilidade de um universo muito amplo ou diversificado de clientes recorrer a este meio alternativo de identificação.

Em linha com o quadro normativo vigente, a entidade obrigada deve garantir que a aferição da qualidade de "pessoa politicamente exposta", "membro próximo de família", "pessoa reconhecida como estritamente associada", e "titular de outro cargo político ou público", assim como a deteção de pessoa identificada em medidas restritivas adotadas pelo Conselho de Segurança das Nações Unidas ou pela União Europeia, tem por base informação previamente comprovada pela mesma (e.g.: nome completo do cliente). Adicionalmente, é boa prática que a análise de alertas constantes de relatórios de filtragem seja efetuada por colaboradores afetos ao RCN, ainda que após a realização da videoconferência (em todo o caso, relembramos, que tal análise deverá ocorrer em momento prévio ao estabelecimento da relação de negócio).

BP 3: Riscos associados aos documentos de identificação

- **Identificação**

As entidades obrigadas devem listar os documentos de identificação admissíveis no âmbito da videoconferência, e mapearem o risco de os mesmos serem contrafeitos, terem sido alterados ou reciclados[5], ou não estarem atualizados.

- **Mitigação**

A entidade obrigada deve avaliar se os controlos implementados mitigam de forma adequada o risco associado aos **documentos de identificação** definidos como admissíveis no âmbito da videoconferência. Neste contexto, é boa prática restringir a aceitação a documentos de identificação com elevadas características de segurança. Caso optem por não estabelecer essa restrição, as entidades obrigadas devem implementar medidas adicionais de mitigação de risco.

Neste âmbito, considera-se boa prática a previsão de **controlos adicionais durante a própria videoconferência** (e.g. comprovações automáticas tais como sistemas de reconhecimento

[5] Em linha com a *OPINION ON THE USE OF INNOVATIVE SOLUTIONS BY CREDIT AND FINANCIAL INSTITUTIONS IN THE CUSTOMER DUE DILIGENCE PROCESS*, entende-se que são: i) **alterados** - documentos genuínos cuja informação tenha sido alterada, ii), **documentos contrafeitos** - reproduções de documentos de identidade, e iii) **documentos reciclados** - identidades fraudulentas criadas com base em materiais de documentos genuínos.

facial, obrigatoriedade de apresentação de documentos de identificação adicionais, como por exemplo a carta de condução, ou previsão de recolha de informação adicional, nomeadamente através da inclusão no *script* de conversação de perguntas adicionais sobre a identidade do cliente), ou **após a conclusão da videoconferência** (procedimentos de monitorização adicionais, e.g. estabelecimento de critérios mais exigentes ou periodicidades mais curtas para a geração ou análise de alertas).

Nesta matéria, é também boa prática conjugar as verificações dos elementos de segurança do documento de identificação realizadas por colaboradores devidamente treinados para o efeito, com verificações realizadas por sistemas informáticos capazes de automaticamente identificar diferentes documentos de identificação e verificar as suas características de segurança.

Reforça-se que as entidades obrigadas devem assegurar que os seus colaboradores têm conhecimentos suficientes (cf. **BP 15**) e que os seus sistemas estão adequadamente parametrizados para realizar não só a recolha, a análise e a verificação da informação constante dos documentos de identificação aceites, mas também a verificação das características, em particular das de segurança, de tais documentos.

BP 4: Riscos associados aos produtos, serviços e operações disponibilizados

- **Identificação**

Cumpre recordar que os riscos de BC/FT associados aos produtos, serviços ou operações passíveis de serem disponibilizados às relações de negócio em que seja admissível o recurso a videoconferência concorrem para a determinação do risco de BC/FT associado ao próprio procedimento.

Nessa medida, a análise dos riscos de BC/FT relacionados com novos produtos ou serviços pelas entidades obrigadas, conforme impõe o artigo 15.º da Lei n.º 83/2017, deve considerar a suscetibilidade de os mesmos virem a ser disponibilizados no âmbito de relações de negócio em que seja admissível o recurso a videoconferência.

Por seu turno, a análise dos riscos de BC/FT, a efetuar previamente à implementação do procedimento de videoconferência, deve incluir um mapeamento dos produtos, serviços ou operações disponibilizados através deste canal e descrever em que medida a utilização do mesmo potencia os riscos desses produtos, serviços ou operações.

- **Mitigação**

Se a entidade obrigada optar por permitir o acesso a **produtos, serviços ou operações** de risco mais elevado, deverá incluir na sua análise de risco a descrição dos procedimentos de controlo que irá implementar de modo a garantir a mitigação dos riscos BC/FT concretamente identificados.

Para este efeito, após o estabelecimento da relação de negócio, é boa prática prever a intervenção de níveis hierárquicos mais elevados para a autorização ao acesso (destes clientes) a produtos, serviços ou operações de risco mais elevado, bem como a obtenção de informação adicional em momento anterior a tal acesso.

BP 5: Riscos associados ao próprio procedimento

- **Identificação**

Em acréscimo aos riscos já mencionados, importa clarificar que devem ser igualmente considerados os riscos de BC/FT inerentes ao próprio procedimento de videoconferência, nomeadamente os decorrentes da ausência de presença física do cliente no momento da sua identificação.

A entidade obrigada deve ainda considerar o fluxo do processo, os intervenientes no mesmo (e.g. recurso a terceiros prestadores de serviços), bem como as soluções tecnológicas e ferramentas informáticas utilizadas (cf. **BP 6**).

- **Mitigação**

A entidade obrigada deve detalhar os procedimentos de controlo implementados para fazer face aos riscos inerentes ao próprio procedimento, incluindo os mecanismos de redundância previstos (com vista a garantir a completa e correta execução do procedimento estabelecido, bem como a mitigar eventuais falhas no mesmo). Deve também ser assegurado que a gravação da videochamada contém informação referente ao controlo de integridade do respetivo ficheiro (e.g. *hash*).

Neste âmbito, recorda-se a necessidade de implementar mecanismos de controlo da atuação dos colaboradores que realizam o procedimento de videoconferência, por forma a garantir, nomeadamente: i) que sempre que não se verifiquem as condições técnicas necessárias à boa condução do processo de comprovação de elementos identificativos, a videoconferência é interrompida e dada sem efeito, e ii) a efetiva conservação da gravação das videoconferências realizadas (incluindo as dadas sem efeito). Devem ser privilegiados procedimentos estruturados,

faseados, que incluam controlos sistemáticos, e que prevejam a intervenção de diferentes colaboradores, departamentos, áreas, ou unidades de estrutura no processo (devendo ser indicado o tipo de validação ou controlo adicional efetuado por cada um dos intervenientes). Nomeadamente, é boa prática que o processo de videoconferência executado seja revisto, uma vez completo, por outro colaborador, para validação ou correção (se necessário, através de novo contacto com cliente com vista à repetição do processo), assim como para a confirmação da informação e documentação recolhida.

Mormente, deve estar expressamente prevista a intervenção do RCN ou de colaboradores da sua equipa, devendo, para o efeito, ser indicado:

- O momento, no fluxo do processo, em que se dá a intervenção dos mesmos (e.g. revisão dos processos de identificação de clientes de risco mais elevado); ou
- As situações específicas que despoletam a intervenção dos mesmos (e.g. sempre que o procedimento de identificação não seja aceite por existirem dúvidas quanto ao teor, idoneidade, autenticidade, atualidade, exatidão ou suficiência dos documentos de identificação apresentados).

BP 6: Soluções tecnológicas e ferramentas informáticas

As soluções tecnológicas e as ferramentas informáticas em que se baseie ou que sejam aplicadas ao procedimento de videoconferência devem ser robustas, e estar devidamente atualizadas e calibradas ao tipo de tarefas que visam desempenhar (nomeadamente, no que concerne o tipo de documentos de identificação aceites e respetivas características físicas e tecnológicas).

Uma boa prática neste âmbito é o recurso a comprovações automáticas (análise de caracteres, biometria e outras), pois considera-se que estas imprimem um grau de segurança acrescido ao processo de videoconferência, nomeadamente coartando o erro humano, e permitindo a realização de verificações de elevada complexidade. No entanto, o recurso a este tipo de ferramenta tecnológica não deve substituir as confirmações manuais a realizar pelo colaborador que assegura a videoconferência, mas antes auxiliar, informar e complementar essas mesmas tarefas.

Também se considera uma boa prática nesta matéria a utilização consentida de sistemas que permitam identificar a localização do cliente durante a videoconferência, na medida em que constituem ferramentas de identificação e gestão de risco relevantes, nomeadamente, permitindo aferir o risco geográfico associado à localização em questão, a racionalidade dessa

localização face aos restantes elementos identificativos e caracterizadores do cliente, assim como despistar eventuais situações potencialmente suspeitas (e.g. coincidência na localização de vários clientes que pretendam aceder a este procedimento, sem justificação para a mesma).

BP 7: Testes de efetividade e de segurança

Conforme resulta expressamente do quadro normativo vigente, em momento prévio à respetiva implementação, a entidade obrigada deve realizar testes de efetividade e de segurança ao procedimento de videoconferência, que devem constar de documento ou registo escrito, e ser repetidos periodicamente. O suporte documental destes testes deve incluir a descrição das diligências efetuadas e o suporte informático comprovativo das mesmas.

Os testes realizados devem permitir aferir cabalmente a adequação, a qualidade e a eficácia do procedimento implementado, incluindo a sua adequação em matéria de prevenção do BC/FT. Nessa medida, devem versar sobre todo o procedimento, mesmo que este seja assegurado, no todo ou em parte, por terceiros prestadores de serviços (*outsourcing*), e permitir a deteção de quaisquer deficiências que afetem a qualidade, fiabilidade, eficácia ou segurança do mesmo.

As entidades obrigadas devem assegurar que os testes de efetividade e segurança são realizados de forma independente pela própria entidade ou por uma entidade terceira devidamente qualificada para o efeito. Nos casos em que a entidade obrigada tenha optado por externalizar o procedimento de videoconferência (em todo ou em parte), os testes devem ser assegurados pela própria entidade obrigada ou por uma entidade independente da que irá assegurar (ou da que assegura) o procedimento de videoconferência.

Na realização destes testes, as entidades obrigadas devem garantir que serão consideradas as tendências mais recentes em matéria de contratação à distância e videoconferência, de modo a acautelar, nomeadamente, as mais recentes práticas de fraude e falhas de segurança, incluindo possíveis formas de intrusão no sistema.

As entidades obrigadas devem ainda assegurar que as soluções tecnológicas e as ferramentas informáticas em que se baseie ou que sejam aplicadas ao procedimento de videoconferência são suficientemente testadas (em particular, as de cariz inovador), e deve ser conhecedora do respetivo grau de fiabilidade e eventuais fragilidades, ainda que estas soluções tecnológicas ou ferramentas informáticas tenham sido implementadas ou sejam geridas por terceiros prestadores de serviços.

As entidades obrigadas devem definir um calendário para a realização de testes periódicos, com uma periodicidade adequada ao risco de BC/FT identificado na análise de risco. Por norma, as entidades obrigadas adotam para estes testes uma periodicidade pelo menos idêntica à tida em conta para a realização dos testes de avaliação de eficácia previstos no artigo 8.º do Aviso n.º 2/2018.

É considerada boa prática que os testes periódicos incluam amostras de videoconferências:

- Definidas aleatoriamente;
- Definidas com base na existência de fatores de risco de BC/FT potencialmente mais elevado;
- Que não deram origem ao estabelecimento de relações de negócio (nomeadamente, por terem sido consideradas sem efeito).

Os testes de efetividade realizados em momento posterior à implementação do procedimento de videoconferência devem detalhar o universo de clientes incluídos na respetiva amostra, assim como a representatividade e quantidade dos casos objeto de análise no universo de relações de negócio estabelecidas através de videoconferência. É também considerada boa prática que a representatividade e quantidade dos casos objeto de análise seja revista a cada teste a realizar, de modo a adequadamente refletir a dimensão e o impacto da videoconferência no âmbito dos procedimentos de identificação e diligência utilizados pela entidade obrigada.

Se, em resultado da realização dos testes periódicos, forem identificados erros ou fragilidades relativamente à solução implementada, devem ser tomadas medidas tendentes a:

- Analisar as relações de negócio afetadas, com vista a determinar se os respetivos procedimentos de identificação e diligência devem ser complementados ou repetidos;
- Aferir se, após a correção dos erros ou das fragilidades identificados, e da realização da análise supra referida, as relações de negócio afetadas podem ser mantidas ou devem ser terminadas, se a execução de transações relacionadas com essas mesmas relações de negócio deve ser suspensa, e se a realização de comunicações nos termos do artigo 43.º da Lei n.º 83/2017 deve ser realizada.
- Caso os erros ou fragilidades identificados sejam relevantes, a entidade obrigada deve avaliar (i) se o nível de fiabilidade da solução implementada é compatível com o risco BC/FT que lhe é aplicável, (ii) a eventual necessidade de implementar melhorias à solução implementada ou (iii) a própria viabilidade da solução implementada.

BP 8: Parecer do RCN

Conforme resulta expressamente do quadro normativo vigente, a entidade obrigada deve obter um parecer prévio do RCN sobre o procedimento de videoconferência a implementar, em particular, com vista a avaliar a adequação dos mecanismos, políticas e controlos destinados a mitigar os riscos de BC/FT especificamente identificados na análise de risco.

O parecer emitido deve configurar uma avaliação cabal da adequação dos mecanismos, políticas e controlos destinados a mitigar os riscos identificados, e incluir, nomeadamente: (i) uma análise efetiva relativa aos concretos riscos de BC/FT associados à implementação do procedimento de videoconferência, (ii) uma demonstração relativa à forma como se encontram assegurados os requisitos consagrados no Anexo I do Aviso n.º 2/2018; e (iii) a identificação do seu autor, a respetiva assinatura, e a data da sua elaboração.

Ademais, cumpre esclarecer que o RCN deve acompanhar de forma ativa tanto a implementação como a execução continuada do procedimento de videoconferência, revendo o seu parecer sempre que necessário e, pelo menos, na sequência dos testes periódicos a que se refere a **BP 7**.

BP 9: Normativos internos

A definição dos meios e mecanismos de mitigação mencionados nas boas práticas anteriores compreende a elaboração de normativos internos suficientemente abrangentes e detalhados, que incidam especificamente sobre o cumprimento dos deveres de prevenção do BC/FT aplicáveis no âmbito do procedimento de comprovação de elementos identificativos através de videoconferência.

Assim, os procedimentos a definir e implementar pelas entidades obrigadas devem atender e ser adequados aos riscos de BC/FT concretamente identificados. Nessa medida, entre outros elementos relevantes, os normativos internos a elaborar devem conter, pelo menos:

- Uma definição clara da repartição de tarefas e responsabilidades entre as diferentes equipas, áreas ou departamentos que intervenham no procedimento, incluindo as responsabilidades a cargo do RCN;
- A tipologia de clientes elegíveis e riscos associados;
- O tipo de documentos de identificação aceites e riscos associados;

- A tipologia de produtos, serviços e operações acessíveis através deste procedimento e riscos associados;
- Os requisitos aplicáveis à videoconferência e riscos associados ao próprio processo;
- A identificação de situações que devem conduzir à não-aceitação da videoconferência como meio de comprovação de elementos identificativos, e procedimentos a adotar;
- A identificação das situações em que a videoconferência é considerada sem efeito e procedimentos a adotar;
- A não-aceitação da comprovação de elementos de identificação tidos como incorretos, imprecisos ou desatualizados (incluindo no que concerne à informação sobre a residência ou a situação profissional);
- A identificação de situações-tipo que exigem a execução de procedimentos/controlos adicionais.
- A calendarização dos testes periódicos a que se refere a **BP 7**.
- A identificação, quando aplicável, dos terceiros prestadores de serviços contratados e dos respetivos processos, serviços ou atividades por estes prestados - cf. **BP 10** e **BP 11**.

É considerada boa prática a preparação e disponibilização aos colaboradores responsáveis pela condução da videoconferência de um guião ("*script* de conversação"), que contenha todos os passos a seguir no âmbito da realização do procedimento em apreço. Este guião deverá compreender não só as perguntas a efetuar e os requisitos a observar durante a videoconferência, mas também exemplos práticos retirados de situações reais que ofereçam dúvidas e quais os procedimentos a seguir nesses casos (incluindo "perguntas mais frequentes" colocadas por colaboradores relevantes).

As entidades obrigadas devem ainda garantir que os colaboradores cujas funções sejam relevantes para efeitos de cumprimento dos deveres em matéria de prevenção do BC/FT, em particular os colaboradores afetos à realização do procedimento de comprovação de elementos identificativos através de videoconferência, conhecem e compreendem adequadamente os procedimentos definidos e implementados nesta sede **– cf. BP 15.**

Ademais, é considerada boa prática neste contexto sistematizar os normativos internos relevantes num único manual ("manual do procedimento de videoconferência"), preferencialmente em formato digital, que deverá ser facilmente atualizável e acessível a todos os colaboradores relevantes.

Aproveita-se, por fim, para reforçar que as entidades obrigadas devem assegurar-se que estes normativos internos permanecem atualizados, e que refletem a todo o tempo os procedimentos efetivamente implementados.

III. BOAS PRÁTICAS NO ÂMBITO DA EXTERNALIZAÇÃO (*OUTSOURCING*)

BP 10: Recurso a terceiro prestador de serviços

Recorda-se que o recurso a terceiros prestadores de serviços para executar, de forma contínua, processos, serviços ou atividades que normalmente seriam realizados pelas próprias entidades obrigadas, observa o disposto no artigo 38.º do Aviso n.º 2/2018.

Em particular, cumpre reiterar que as entidades obrigadas:

- Permanecem exclusivamente responsáveis pelo exato cumprimento dos deveres de prevenção BC/FT previstos no quadro normativo aplicável, estando, nomeadamente, obrigadas a manter o poder de decisão final relativamente a quaisquer tarefas incluídas nos processos, serviços ou atividades externalizados;
- Estão impedidas de recorrer a terceiros prestadores de serviços estabelecidos em países com regimes legais que prevejam proibições ou restrições que impeçam ou limitem o cumprimento das normas legais e regulamentares em matéria de prevenção do BC/FT, incluindo ao nível da prestação e circulação de informação.

Face ao exposto, é considerada boa prática o recurso a terceiros prestadores de serviços que sejam publicamente reconhecidos como idóneos, credíveis e especialistas no desenvolvimento de soluções de identificação remota.

Frisa-se ainda que serviços prestados por plataformas globais, com termos de utilização de simples adesão, podem não assegurar o poder de decisão final por parte da entidade obrigada, nomeadamente pela dificuldade em introduzir alterações "*tailor-made*" que respondam à sua realidade operativa e às necessidades de correção que por esta forem identificadas. Assim, a impossibilidade de a entidade obrigada impor os necessários ajustamentos aos fornecedores de

serviços tecnológicos denota a ausência de poder de decisão final e, como tal, acarreta a consequente cessação do serviço.

BP 11: Escolha e avaliação do terceiro prestador de serviços

Quando recorra a um terceiro prestador de serviços para execução da comprovação dos elementos identificativos com recurso à videoconferência, a entidade obrigada deve:

- Garantir que dispõe de um conhecimento exato e atualizado quanto aos termos concretos em que o procedimento em referência deve ser assegurado pelo prestador de serviços;
- Garantir que dispõe de um conhecimento exato e atualizado quanto aos termos concretos em que o procedimento em referência se encontra efetivamente a ser assegurado pelo prestador de serviços;
- Implementar mecanismos que assegurem uma estreita e permanente articulação com aquele prestador de serviços;
- Definir e implementar procedimentos e mecanismos de controlo relativamente aos processos, serviços ou atividades prestadas pelo prestador de serviços.

Devem ser tidos em conta, nomeadamente, no âmbito da coordenação e monitorização acima referidas, os seguintes temas:

- A tipologia de clientes elegíveis a aceder ao procedimento (previamente definida pela entidade obrigada);
- O tipo de documentação admissível;
- A natureza (exclusiva ou não) da afetação dos colaboradores do prestador de serviços à realização de videoconferências para a entidade obrigada;
- O conteúdo da formação e dos documentos de trabalho (e.g. *script* de conversação) dos colaboradores que irão assegurar as videoconferências;
- As condições de salvaguarda estabelecidas relativamente às gravações das videoconferências realizadas. Neste contexto, é considerada boa prática o recurso a soluções que reconhecidamente garantam a conservação dos ficheiros durante longos períodos de tempo, com elevada fiabilidade e integridade;

- As condições de acesso estabelecidas relativamente às gravações das videoconferências realizadas. É considerada boa prática que, entre outros, sejam detalhados os seguintes aspetos: (i) as pessoas, afetas a ambas as entidades, com permissões para efetuar o pedido de acesso e disponibilizar as gravações; (ii) os canais de comunicação a utilizar para efeitos da formulação do pedido; (iii) os meios e prazos para efeitos de disponibilização das gravações; (iv) o local de arquivo das gravações e respetivas condições de acesso;
- Os termos em que é assegurado o acesso e a integridade da informação detida pelo prestador de serviços, em caso de falha no respetivo sistema ou cessação do contrato de prestação de serviços com a entidade obrigada.

Caso o terceiro prestador de serviços apresente um processo que configure ou utilize soluções ou tecnologias novas ou em fase de desenvolvimento, é boa prática que a entidade obrigada, além de garantir uma adequada avaliação do risco e a execução de testes de eficácia e segurança adequados aos riscos de BC/FT associados ao procedimento de videoconferência, implemente o procedimento por fases. Assim, por exemplo, numa primeira fase, tal procedimento só estaria disponível para clientes de risco baixo e permitiria apenas aceder a serviços, produtos e operações igualmente de risco baixo. Numa segunda fase, e apenas após a execução dos testes periódicos mencionados na **BP 7** – dos quais resultasse uma avaliação positiva do procedimento –, a entidade obrigada alargaria o universo de clientes elegíveis e/ou dos serviços, produtos e operações acessíveis através do mesmo.

Nos casos em que as videoconferências são asseguradas em espaços físicos não pertencentes ou geridos pela entidade obrigada, é considerada boa prática que a entidade os conheça e promova visitas periódicas aos mesmos, de modo a garantir que são adequados e cumprem os requisitos que lhe são aplicáveis.

IV. BOAS PRÁTICAS NO ÂMBITO DA REALIZAÇÃO DA VIDEOCONFERÊNCIA

BP 12: Requisitos técnicos e condução da videoconferência

A entidade obrigada deve proceder à validação da qualidade da gravação após a geração do ficheiro de vídeo, dando a videoconferência sem efeito sempre que se não se verifiquem as condições técnicas necessárias à boa condução do processo, incluindo nas situações previstas no n.º 5 do artigo 8.º Anexo I do Aviso n.º 2/2018 e quando ocorra dessincronização entre o som e a imagem da gravação. Para o efeito, os colaboradores relevantes devem estar munidos de documentação de apoio para a condução da videoconferência, como seja o *script* de conversação referido na **BP 9**, o qual deve determinar a obrigatoriedade de repetir o processo na sua totalidade, sempre que ocorram falhas ou interrupções de natureza técnica.

Na aferição da **qualidade e fidedignidade da imagem**, as entidades obrigadas devem adotar critérios técnicos de caráter objetivo (por exemplo, com base em padrões internacionais, tais como as normas ISO) e assegurar que os colaboradores relevantes são, em cada caso, capazes de proceder à verificação dos documentos de identificação apresentados e de despistar eventuais situações de contrafação, alteração ou reciclagem dos mesmos. Para tanto, os colaboradores em causa devem assegurar que as feições do cliente e os detalhes dos documentos de identificação são perfeitamente reconhecíveis e estar preparados para deslindar situações nas quais exista o risco de: (i) a imagem do cliente estar a ser comprometida/alterada, ou (ii) a imagem do documento de identificação pertencer a uma pessoa distinta, mas com características físicas semelhantes às do cliente.

Para assegurar a **rastreabilidade do procedimento** e a sua realização em tempo real e **sem pausas**, a entidade obrigada deve implementar mecanismos de confirmação automática do código único descartável (OTP – *one time password*), definindo claramente o tempo limite para a respetiva inserção pelo cliente e não admitindo alterações ao contacto telefónico previamente disponibilizado para este efeito, no decurso da videoconferência.

A indicação da **data/hora** da realização da videoconferência deve seguir o fuso horário português. Neste âmbito, é boa prática a utilização de sistemas que permitam que a informação da data/hora esteja visível na imagem do vídeo durante toda a videoconferência. Quando a entidade obrigada opte por um sistema que não permita a inclusão dessa informação, os metadados do ficheiro de gravação da videoconferência devem permitir obter informação fiável

e rigorosa sobre a duração efetiva do vídeo, não sendo considerado suficiente que o operador de videoconferência faça referência verbal à data e hora relativas ao início e à conclusão do procedimento. A entidade obrigada deve igualmente assegurar que as imagens de frente e verso dos documentos de identificação dos clientes, captadas durante a realização da videoconferência, contêm indicação, aposta na respetiva imagem, da data e hora da respetiva captação.

Ademais, a entidade obrigada deve ainda assegurar que os meios técnicos utilizados permitem que os colaboradores relevantes que procedam à comprovação de elementos identificativos através de videoconferência possam apor nos registos internos de suporte menção que claramente os identifique e a data em que tal comprovação foi realizada. Muito embora a gravação da imagem do colaborador que realiza a videoconferência, ou a sua apresentação no início da videoconferência possam ser elementos relevantes, não substituem a aposição destes registos.

Por último, é boa prática que a entidade obrigada defina procedimentos de condução da videoconferência dinâmicos, que prevejam:

- A identificação de comportamentos suspeitos e a adaptação da atuação dos colaboradores relevantes, especialmente quando estes suspeitem que o cliente possa estar a prestar falsas declarações ou a ser coagido;
- A adequação da atuação dos colaboradores relevantes ao caso concreto (e.g. identificando situações em que devem ser aplicados procedimentos complementares de diligência, nomeadamente, quando obter informação adicional sobre a finalidade e natureza pretendida da relação de negócio).

V. BOAS PRÁTICAS NO ÂMBITO DA ENTREGA DE FUNDOS INICIAL

BP 13: Meios e jurisdições aceites

Nos termos do quadro normativo aplicável, as entidades estão obrigadas a assegurar que a entrega de fundos inicial é efetuada através de meio rastreável que permita a identificação do ordenante, com origem em conta aberta junto de entidade obrigada ou outra legalmente habilitada que, não se situando em país terceiro de risco elevado, comprovadamente aplique medidas de identificação e diligência compatíveis com as previstas na Lei n.º 83/2017 e no Aviso n.º 2/2018 (cf. alínea a) do n.º 4 do artigo 2.º do Anexo I do Aviso n.º 2/2018).

Para este efeito, a entidade deve expressamente prever uma lista com (i) os tipos de operações através das quais pode ser efetuada a entrega de fundos inicial e (ii) os países/jurisdições (de origem da entrega de fundos inicial) admissíveis. Neste âmbito, esclarece-se que não é considerada suficiente a existência de uma norma interna que apenas remeta para as regras gerais relativas à monitorização das operações em função do país/jurisdição de origem.

Ademais, reitera-se que o meio através do qual é efetuada a entrega de fundos inicial deve permitir a identificação do ordenante efetivo e não somente da entidade intermediária na transferência. Considera-se particularmente eficaz a implementação de um mecanismo que possibilite a conferência automática entre a titularidade da conta e o primeiro e último nome associado ao IBAN (de onde se origina a transferência).

Cumpre esclarecer que depósitos em numerário não constituem meios rastreáveis, ainda que realizados de forma presencial, ao balcão da entidade obrigada, pelo titular da conta, pelo que não podem ser utilizados para a entrega de fundos inicial. Por outro lado, esclarece-se ainda que, quando a entrega de fundos inicial é realizada através de depósito de cheque, deverá ser identificada a identidade do depositante e do emitente do mesmo.

É igualmente considerada boa prática que a entrega de fundos inicial só possa ter origem em conta titulada pelo cliente. Caso a entidade obrigada opte por permitir que a entrega de fundos inicial tenha origem em conta titulada por pessoa diversa do cliente, esse facto deve estar especificamente previsto nos normativos que regem o procedimento de videoconferência.

BP 14: Mecanismos de controlo específicos

A entidade obrigada deve privilegiar a adoção de mecanismos de controlo automáticos relativos ao primeiro movimento efetuado em contas abertas com recurso ao procedimento de videoconferência, como sejam bloqueios automáticos de receção de fundos. Nos casos em que estes controlos tenham carácter manual, a entidade deve implementar rotinas que permitam a deteção de situações em que a entrega de fundos inicial não ocorreu nos moldes definidos (mecanismos de controlo ou de verificação *ex post*), e a aplicação de medidas adequadas a tais situações, tais como o bloqueio da conta em questão e a análise das razões que permitiram o incumprimento de tais requisitos.

VI. BOAS PRÁTICAS NO ÂMBITO DA FORMAÇÃO E ATUAÇÃO DOS COLABORADORES

BP 15: Ações de formação específica

A entidade obrigada deve assegurar que todos os colaboradores que realizam o procedimento de videoconferência participam em:

- Ações de formação em matéria de prevenção do BC/FT;
- Ações de formação específicas em matéria de comprovação de elementos identificativos através do procedimento de videoconferência (que deverão abranger os requisitos regulamentares específicos para este procedimento, bem como os normativos internos elaborados sobre o mesmo); e
- Ações de formação em matéria de fraude e falsificação de documentos de identificação.

Em particular, os colaborares afetos à realização da videoconferência, de modo a adequar a sua atuação ao caso concreto, devem estar familiarizados com:

- Os documentos de identificação admissíveis para efeitos de comprovação de elementos de identificação (incluindo as suas características de segurança), devendo receber formação atualizada sempre que este rol for alterado, e ser sensibilizados para a necessidade de recolha de informação precisa e atualizada.
- As tipologias de comportamentos suspeitos.
- Os diferentes perfis de risco BC/FT previstos pela entidade obrigada.

Paralelamente, todos os colaboradores da entidade obrigada com funções relevantes em matéria de prevenção BC/FT (em particular, os colaboradores afetos ao RCN) devem possuir um conhecimento adequado quanto ao procedimento de videoconferência implementado, nomeadamente, respetivas condições, requisitos e especificidades, assim como quanto aos riscos que lhe são inerentes, mesmo que este seja assegurado, em todo ou em parte, por terceiros prestadores de serviços.

VII. BOAS PRÁTICAS NO ÂMBITO DA RELAÇÃO COM O CLIENTE

BP 16: Prestação de informação

A entidade obrigada, quando disponibiliza o procedimento de videoconferência, deve informar previamente o cliente sobre o seguinte:

- O horário em que é possível efetuar este procedimento e / ou a possibilidade do seu agendamento (se aplicável);
- Quais os documentos que lhe vão ser exigidos (e.g. cartão de cidadão) e os dispositivos ou meios necessários (e.g., o telemóvel ou acesso ao correio eletrónico fornecidos para onde será enviada a OTP) no decurso da videoconferência;
- Que, não estando preenchidas as condições legal e regulamentarmente exigidas, o procedimento será interrompido e/ou não será considerado válido para efeitos da comprovação dos elementos identificativos, podendo ser necessário o recurso a outro meio ou procedimento para este efeito.

Caso a entidade obrigada opte por apresentar uma estimativa de tempo para a realização do procedimento de videoconferência, deve ser indicado um período de tempo médio adequado, e que o procedimento poderá ultrapassar o tempo referido.

É considerada boa prática a adoção de mecanismos de assistência e esclarecimento do cliente sobre o procedimento de videoconferência (e.g., incluir conteúdos nas perguntas frequentes ou apresentar um vídeo explicativo sobre o procedimento de videoconferência).

BP 17: Melhorias ao procedimento

A entidade obrigada deve ponderar as observações apresentadas pelos clientes, nomeadamente no contexto de reclamações ou da resposta a questionários de satisfação realizados após a videoconferência, no âmbito da eventual necessidade de implementar melhorias a este procedimento.

VIII. ESTATUTO DAS PRESENTES BOAS PRÁTICAS E *FOLLOW-UP*

As presentes boas práticas são emitidas ao abrigo do n.º 1 do artigo 98.º da Lei n.º 83/2017.

Todos os procedimentos a adotar em cumprimento destas boas práticas, bem como a documentação comprovativa da respetiva execução, devem ser reduzidos a escrito e conservados nos moldes previstos no artigo 51.º da Lei n.º 83/2017, em termos que permitam o imediato acesso aos mesmos pelo Banco de Portugal.

As entidades obrigadas, nos termos e para os efeitos do n.º 3 do artigo 98.º da Lei n.º 83/2017, devem justificar a decisão de não acatar, no todo ou em parte, as presentes boas práticas. Essa decisão deve ser reduzida a escrito, identificando claramente os aspetos não acatados e apresentando justificação fundamentada que sustente o não acatamento. Os suportes documentais elaborados neste âmbito devem ser arquivados pelas entidades obrigadas igualmente nos moldes previstos no artigo 51.º da Lei n.º 83/2017, em termos que permitam a imediata disponibilização dos mesmos ao Banco de Portugal, a solicitação deste.