



EBA/GL/2022/15

22/11/2022

Orientações

relativas à utilização de Soluções de Integração de Clientes (*Onboarding*) à Distância nos termos do artigo 13.º, n.º 1, da Diretiva (UE) 2015/849



1. Obrigações em matéria de cumprimento e de notificação

Natureza jurídica das presentes orientações

1. O presente documento contém orientações emitidas ao abrigo do artigo 16.º do Regulamento (UE) n.º 1093/2010¹. Nos termos do artigo 16.º, n.º 3, do Regulamento (UE) n.º 1093/2010, as autoridades competentes e as instituições financeiras devem envidar todos os esforços para dar cumprimento a estas orientações.
2. As Orientações definem a posição da Autoridade Bancária Europeia (EBA) sobre práticas de supervisão adequadas no âmbito do Sistema Europeu de Supervisão Financeira ou sobre o modo como a legislação da União deve ser aplicada num domínio específico. As autoridades competentes, na aceção do artigo 4.º, n.º 2, do Regulamento (UE) n.º 1093/2010, às quais as presentes orientações se aplicam, devem dar cumprimento às mesmas, incorporando-as nas suas práticas de supervisão, conforme for mais adequado (por exemplo, alterando o seu enquadramento jurídico ou os seus processos de supervisão), incluindo nos casos em que as orientações são aplicáveis, em primeira instância, a instituições.

Requisitos de notificação

3. Nos termos do disposto no artigo 16.º, n.º 3, do Regulamento (UE) n.º 1093/2010, as autoridades competentes devem notificar a EBA se dão ou tencionam dar cumprimento às presentes orientações, ou, caso contrário, indicar as razões para o não cumprimento até 30.05.2023. Na ausência de qualquer notificação até à referida data, a EBA considerará que as autoridades competentes em causa não cumprem as orientações. As notificações efetuam-se mediante o envio do modelo disponível no sítio Web da EBA com a referência «EBA/GL/2022/15». As notificações devem ser efetuadas por pessoas devidamente autorizadas a notificar a situação de cumprimento em nome das respetivas autoridades competentes. Qualquer alteração no que respeita à situação de cumprimento deve igualmente ser comunicada à EBA.
4. As notificações serão publicadas no sítio Web da EBA, em conformidade com o disposto no artigo 16.º, n.º 3.

¹ Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Bancária Europeia), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/78/CE da Comissão (JO L 331 de 15.12.2010, p. 12).



2. Objeto, âmbito de aplicação e definições

Objeto e âmbito de aplicação

5. As presentes orientações estabelecem as medidas que as instituições de crédito e financeiras devem tomar aquando da adoção ou revisão de soluções que visem cumprir as obrigações previstas no artigo 13.º, n.º 1, alíneas a), b) e c), da Diretiva (UE) 2015/849² no âmbito da integração de novos clientes à distância. Estabelece igualmente as medidas que as instituições de crédito e financeiras devem adotar quando recorrem a terceiros, em conformidade com o capítulo I, secção 4, da Diretiva (UE) 2015/849, e as políticas de controlo e procedimentos que devem estabelecer em relação às medidas de diligência quanto à clientela (CDD) a que se referem o artigo 8.º, n.º 3, e (4) alínea a), da Diretiva (UE) 2015/849, caso estas medidas de CDD sejam executadas à distância.
6. As autoridades competentes devem ter em conta as presentes orientações ao avaliarem a adequação e eficácia de as medidas adotadas pelas instituições de crédito e financeiras no cumprimento das obrigações da Diretiva (UE) 2015/849, no contexto da integração de clientes à distância.

Destinatários

7. As presentes orientações destinam-se às autoridades competentes, na aceção do artigo 4.º, n.º 2, do Regulamento (UE) n.º 1093/2010. As presentes orientações destinam-se igualmente aos operadores do setor financeiro, na aceção do artigo 4.º, n.º 1-A, do referido regulamento, que são instituições de crédito e financeiras na aceção do artigo 3.º, n.º 1, e do artigo 3.º n.º 2, da Diretiva (UE) 2015/849.

² Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo



Definições

8. Salvo especificação em contrário, os termos utilizados e definidos na Diretiva (UE) 2015/849 têm o mesmo significado nas presentes orientações. Adicionalmente, para efeitos das presentes orientações, entende-se por:

Dados biométricos

Dados pessoais relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, tais como imagens faciais ou dados dactiloscópicos, obtidos e tratados por meios técnicos.

3. Implementação

Data de aplicação

As presentes orientações são aplicáveis a partir de 02.10.2023.



4. Orientações relativas à utilização de Soluções de Integração de Clientes (*Onboarding*) à Distância nos termos do artigo 13.º, n.º 1, da Diretiva (UE) 2015/849

4.1 Políticas e procedimentos internos

4.1.1 Políticas e procedimentos relativos à integração de clientes à distância

9. As instituições de crédito e as instituições financeiras devem implementar e manter políticas e procedimentos que visem cumprir as suas obrigações nos termos do artigo 13.º, n.º 1, alínea a) e c) da Diretiva (UE) 2015/849 nas situações em que o cliente é integrado (*onboarded*) à distância. Estas políticas e procedimentos devem ser baseados no risco e incluir/definir, pelo menos:
- a) uma descrição geral da solução adotada pelas instituições de crédito e financeiras para recolher, verificar e registar informações ao longo de todo o processo de integração de clientes à distância. Tal deve incluir uma explicação das características e do funcionamento da solução;
 - b) as situações em que a solução de integração de clientes à distância pode ser utilizada, tendo em conta os fatores de risco identificados e avaliados em conformidade com o artigo 8.º, n.º 1, da Diretiva (UE) 2015/849 e a avaliação do risco ao nível do negócio, incluindo uma descrição da categoria de clientes, produtos e serviços elegíveis para a integração à distância;
 - c) que etapas são totalmente autónomas e que etapas exigem intervenção humana;
 - d) os controlos em vigor para assegurar que a primeira transação com um novo cliente é executada apenas depois de aplicadas todas as medidas iniciais de diligência quanto à clientela (CDD);
 - e) uma descrição dos programas de formação inicial e regular que visem assegurar a sensibilização dos colaboradores e o seu conhecimento atualizado do funcionamento da solução de integração de clientes à distância, dos riscos que lhe estão associados e das políticas e procedimentos de integração de clientes à distância destinados a atenuar esses riscos.



10. As políticas e os procedimentos, uma vez implementados, devem permitir que as instituições de crédito e as instituições financeiras assegurem o cumprimento do disposto nas secções 4.2 a 4.7 das presentes orientações.

4.1.2 Governo interno

11. Além das disposições estabelecidas na secção 4.2.4 das Orientações da EBA relativas ao responsável pela conformidade³, o Responsável pela Conformidade ABC/CFT⁴ deve, no âmbito do seu dever geral de elaborar políticas e procedimentos aplicáveis ao cumprimento das obrigações de CDD, assegurar que as políticas e os procedimentos de integração de clientes à distância são aplicados de forma eficaz, revistos regularmente e alterados sempre que necessário.
12. O órgão de administração da instituição de crédito e financeira deve aprovar políticas e procedimentos de integração de clientes à distância e supervisionar a sua correta aplicação.

4.1.3 A avaliação prévia à implementação da solução de integração de clientes à distância

13. Ao ponderarem a adoção de uma nova solução de integração de clientes à distância, as instituições de crédito e financeiras devem realizar uma avaliação prévia à implementação dessa solução de integração de clientes à distância.
14. As instituições de crédito e as instituições financeiras devem definir nas suas políticas e procedimentos o âmbito, as etapas e os requisitos de manutenção de registos da avaliação prévia à implementação, que deve incluir, pelo menos:
 - a) uma avaliação da adequação da solução no que respeita à exaustividade e exatidão dos dados e documentos a recolher, bem como da fiabilidade e da independência das fontes de informação que utiliza;
 - b) uma avaliação do impacto da utilização da solução de integração de clientes à distância nos seus riscos ao nível do negócio, incluindo BC/FT, riscos operacionais, reputacionais e jurídicos;
 - c) a identificação de possíveis medidas de mitigação e de medidas corretivas para cada risco identificado na avaliação prevista na alínea b);
 - d) a realização de testes para avaliar os riscos de fraude, incluindo os riscos de fraude de usurpação de identidade e outros riscos de tecnologias da informação e de comunicação («TIC») e os riscos de segurança, em conformidade com a disposição

³ Projeto de orientações relativas às políticas e procedimentos em matéria de gestão da conformidade e ao papel e responsabilidades do responsável pela conformidade em matéria de ABC/CFT nos termos do artigo 8.º e do capítulo VI da Diretiva (UE) 2015/849

⁴ Em conformidade com os critérios de proporcionalidade estabelecidos na secção 4.2.2 das orientações para o responsável pela conformidade



- 43 das Orientações da EBA relativas à gestão dos riscos associados às TIC e à segurança⁵;
- e) testes *end-to-end* ao funcionamento da solução, que visem o(s) cliente(s), o(s) produto(s) e o(s) serviço(s) identificado(s) nas políticas e procedimentos de integração de clientes à distância.
15. As instituições de crédito e as instituições financeiras devem considerar cumpridos os critérios do parágrafo 14, alíneas a), d) e e), quando a solução implementada recorra a um dos seguintes meios:
- a) sistemas de identificação eletrónica notificados em conformidade com o artigo 9.º do Regulamento (UE) n.º 910/2014 e que cumpram os requisitos dos níveis de garantia «substancial» ou «elevado», em conformidade com o artigo 8.º do mesmo regulamento;
- b) serviços de confiança qualificados relevantes que cumpram os requisitos do Regulamento (UE) n.º 910/2014, em particular o capítulo III, secção 3, e o artigo 24.º, n.º 1, parágrafo 2, alínea b), desse regulamento.
16. As instituições de crédito e financeiras devem conseguir demonstrar à respetiva autoridade competente quais as avaliações que realizaram antes da implementação da solução de integração de clientes à distância, o resultado da sua avaliação e de que forma a utilização desta solução é adequada à luz dos riscos de BC/FT identificados para o(s) tipo(s) de cliente(s), serviço(s), geografias e produtos abrangidos pelo seu respetivo âmbito de aplicação.
17. As instituições de crédito e financeiras só devem começar a utilizar uma solução de integração de clientes à distância depois de comprovarem que a mesma pode ser integrada no sistema de controlo interno mais vasto da instituição, permitindo-lhe assim gerir adequadamente os riscos de BC/FT que possam decorrer da utilização dessa solução de integração de clientes à distância.

4.1.4 Monitorização contínua da solução de integração de clientes à distância

18. As instituições de crédito e financeiras devem monitorizar continuamente a solução de integração de clientes à distância, a fim de assegurar que esta funciona em conformidade com as suas expectativas. Devem complementar as suas políticas e procedimentos descritos no parágrafo 9 com uma descrição de, pelo menos:
- a) as medidas que tomarão para se certificarem da qualidade, exaustividade, exatidão e adequação, ao longo do tempo, dos dados recolhidos durante o processo de

⁵ EBA/GL/2019/04



integração de clientes à distância, que devem ser proporcionais aos riscos de BC/FT a que a instituição de crédito ou financeira está exposta;

- b) o âmbito e a frequência dessas revisões periódicas e
- c) as circunstâncias que desencadearão revisões ad hoc, que devem incluir, pelo menos:
 - a. alterações da exposição ao risco de BC/FT da instituição de crédito ou financeira;
 - b. deficiências no funcionamento da solução detetadas no decurso das atividades de monitorização, auditoria ou supervisão;
 - c. Perceção de um aumento das tentativas de fraude;
 - d. alterações do quadro legal ou regulamentar.

19. As instituições de crédito e financeiras devem estabelecer medidas corretivas nos seus procedimentos e processos, caso se tenha concretizado um risco ou sempre que tenham sido identificados erros que tenham impacto na eficiência e eficácia da solução geral de integração de clientes à distância. Estas medidas devem incluir, no mínimo:

- a) uma revisão de todas as relações de negócio afetadas, a fim de avaliar se as instituições de crédito e as instituições financeiras realizaram uma CDD inicial em termos suficientes para cumprir com o disposto no artigo 13.º, n.º 1, alíneas a), b) e c), da AMLD. As instituições de crédito e as instituições financeiras devem dar prioridade às relações de negócio que comportam o maior risco de BC/FT;
- b) com base nas informações obtidas na análise acima referida, a realização de uma avaliação para determinar se uma relação de negócio afetada deve ser:
 - a. sujeita a medidas de diligência adicionais;
 - b. sujeita a limitações, tais como limites ao volume de transações, quando tal seja permitido pela legislação nacional, até que seja sujeita a revisão;
 - c. terminada;
 - d. comunicada à UIF;
 - e. reclassificada numa categoria de risco diferente.

20. As instituições de crédito e financeiras devem considerar a forma mais eficaz de controlar a adequação e a fiabilidade, ao longo do tempo, das soluções de integração de clientes à distância. Devem considerar um ou mais dos seguintes meios, mas não exclusivamente:



- i. testes de garantia da qualidade;
 - ii. alertas críticos e notificações automatizados;
 - iii. relatórios de qualidade automatizados regulares;
 - iv. testes por amostragem;
 - v. análises manuais.
21. A presente secção também se aplica quando são utilizadas soluções de integração de clientes à distância totalmente automatizadas, que dependem fortemente de algoritmos automatizados, sem ou com pouca intervenção humana.
22. As instituições de crédito e as instituições financeiras devem conseguir demonstrar à respetiva autoridade competente as análises que efetuaram e as medidas corretivas que tomaram para corrigir eventuais deficiências identificadas ao longo da vida da solução de integração de clientes à distância.

4.2 Obtenção de informações

4.2.1 Identificação do cliente

23. Além dos pontos referidos no parágrafo 9, as instituições de crédito e financeiras devem indicar nas suas políticas e procedimentos as informações necessárias para identificar o cliente, os tipos de documentos, dados ou informações que a instituição utilizará para verificar a identidade do cliente e a forma como essas informações serão verificadas.
24. As instituições de crédito e as instituições financeiras devem assegurar que:
- a) as informações obtidas através da solução de integração de clientes à distância estão atualizadas e são adequadas para cumprir as normas legais e regulamentares aplicáveis em matéria de diligência inicial quanto à clientela;
 - b) quaisquer imagens, vídeos, som e dados são captados num formato legível e com qualidade suficiente para que o cliente seja inequivocamente reconhecível;
 - c) o processo de identificação não prossegue se forem detetadas deficiências técnicas ou interrupções inesperadas da ligação.
25. As instituições de crédito e as instituições financeiras devem considerar cumpridos os critérios do parágrafo 24 quando a solução implementada recorra a um dos seguintes meios:
- a) sistemas de identificação eletrónica notificados em conformidade com o artigo 9.º do Regulamento (UE) n.º 910/2014 e que cumpram os requisitos dos níveis de



garantia «substancial» ou «elevado», em conformidade com o artigo 8.º do mesmo regulamento;

- b) serviços de confiança qualificados relevantes que cumpram os requisitos do Regulamento (UE) n.º 910/2014, em particular o capítulo III, secção 3, e o artigo 24.º, n.º 1, parágrafo 2, alínea b), desse regulamento.

26. Os documentos e informações recolhidos durante o processo de identificação à distância, que devem ser conservados em conformidade com o artigo 40.º, n.º 1, alínea a), da Diretiva (UE) 2015/849, devem ser carimbados com data e hora (*time-stamped*) e armazenados de forma segura pela instituição de crédito e pela instituição financeira. O conteúdo dos registos armazenados, incluindo imagens, vídeos, som e dados, deve estar disponível num formato legível e permitir verificações ex post.

4.2.2 Identificação de pessoas singulares

27. As instituições de crédito e as instituições financeiras devem determinar nas suas políticas, tal como estabelecido no parágrafo 9 da Secção 4.1.1, as informações de que necessitam para identificar os clientes à distância, em conformidade com o artigo 13.º, n.º 1, alínea a), e alínea c), da Diretiva (UE) 2015/849. Além disso, as instituições de crédito e as instituições financeiras devem definir que informações:

- a) são introduzidas manualmente pelo cliente;
- b) são automaticamente captadas a partir da documentação fornecida pelo cliente;
- c) são recolhidas através de outras fontes internas ou externas.

28. As instituições de crédito e as instituições financeiras devem implementar e manter mecanismos adequados para garantir que as informações que recolhem automaticamente, em conformidade com o parágrafo 27, são fiáveis. Devem aplicar controlos para fazer face aos riscos associados, incluindo os riscos associados à recolha automática de dados, como a ofuscação da localização dos endereços IP (IP) do dispositivo do cliente ou serviços como redes privadas virtuais (VPN).

4.2.3 Identificação de entidades jurídicas

29. Sempre que as instituições de crédito e as instituições financeiras integrem à distância clientes que sejam entidades jurídicas, devem definir, nas suas políticas e procedimentos, tal como estabelecido na secção 4.1.1, parágrafo 9, que categorias de entidades jurídicas irão integrar à distância, tendo em conta o nível de risco de BC/FT associado a cada categoria, e o nível de intervenção humana necessário para validar os elementos de identificação.

30. As instituições de crédito e as instituições financeiras devem assegurar que a solução de integração de clientes à distância tem funcionalidades para recolher:



- a) toda a informação e documentação relevantes para identificar e verificar a pessoa coletiva
- b) toda a informação e documentação relevantes para confirmar que a pessoa singular que age em nome da pessoa coletiva está legalmente habilitada a agir como tal;
- c) as informações relativas aos beneficiários efetivos, em conformidade com a disposição 4.12 das Orientações da EBA relativas aos fatores de risco⁶.

31. Relativamente à pessoa singular que age em nome de uma pessoa coletiva, as instituições de crédito e as instituições financeiras devem aplicar o processo de identificação descrito na secção 4.2.2.

4.2.4 Determinação da natureza e da finalidade da relação de negócio

32. Quando as instituições de crédito e financeiras avaliam e, conforme aplicável, obtêm informações sobre a finalidade e a natureza pretendida da relação de negócio, em conformidade com o artigo 13.º, n.º 1, alínea c), da Diretiva (UE) 2015/849, conforme especificado na secção 4.38 das Orientações da EBA relativas aos fatores de risco, devem, para efeitos das presentes orientações, ter concluído as ações relevantes antes do final do processo de integração de clientes à distância.

4.3 Autenticidade e integridade do documento

33. Sempre que as instituições de crédito e as instituições financeiras aceitem reproduções de um documento original e não examinem o documento original, devem tomar medidas para garantir a fiabilidade dessa reprodução. As instituições de crédito e as instituições financeiras devem estabelecer, pelo menos, o seguinte:

- a) se a reprodução inclui os elementos de segurança incorporados no documento original e se as especificações do documento original que estão a ser reproduzidas são válidas e aceitáveis, nomeadamente o tipo, o tamanho dos caracteres e a estrutura do documento, comparando-os com bases de dados oficiais, como o PRADO⁷;
- b) se os dados pessoais foram alterados ou manipulados de outra forma ou, se aplicável, se a fotografia do cliente incorporada no documento foi substituída;
- c) se a integridade do algoritmo utilizado para gerar o número de identificação único do documento original, no caso de o documento oficial ter sido emitido com uma zona de leitura ótica (MRZ);

⁶ EBA/GL/2021/02

⁷ <https://www.consilium.europa.eu/prado/en/prado-start-page.html>



- d) se a reprodução fornecida é de qualidade e definição suficientes, de modo a garantir que as informações relevantes são inequívocas;
 - e) que a reprodução fornecida não foi exibida num ecrã baseado numa fotografia ou digitalização do documento de identidade original.
34. Sempre que as instituições de crédito e financeiras utilizem funcionalidades para ler automaticamente informações de documentos, tais como algoritmos de reconhecimento ótico de caracteres (OCR) ou verificações da zona de leitura ótica (MRZ), devem tomar as medidas necessárias para assegurar que esses instrumentos captam as informações de forma exata e coerente.
35. Nas situações em que o dispositivo utilizado pelos clientes para provar a sua identidade permita a recolha de dados relevantes, por exemplo, porque os dados estão contidos no chip de um bilhete de identidade nacional, e for tecnicamente viável para as instituições de crédito e financeiras acederem a esses dados, as instituições de crédito e financeiras devem considerar a possibilidade de utilizar essas informações para verificar a sua consistência com as informações obtidas através de outras fontes, como os dados fornecidos ou outros documentos apresentados pelo cliente.
36. Se existentes, as instituições de crédito e financeiras devem verificar os elementos de segurança incorporados no documento oficial durante o processo de verificação, tais como hologramas, como prova da sua autenticidade.
37. As instituições de crédito e financeiras devem definir, nas suas políticas e procedimentos, a forma como irão ajustar os seus pedidos de documentação para efeitos de inclusão financeira. Caso sejam aceites formas de documentação menos robustas ou não tradicionais, as instituições de crédito e financeiras devem, para além das medidas previstas no ponto 4.10 das Orientações da EBA relativas aos fatores de risco, controlar ou reforçar a intervenção humana para se certificarem de que compreendem o risco de BC/FT associado à relação de negócio.

4.4 Correspondência com a identidade do cliente como parte do processo de verificação

38. As soluções de integração de clientes à distância implementadas por instituições de crédito e financeiras devem, no mínimo, permitir confirmar, como parte do seu processo de verificação, o seguinte:
- a) que existe uma correspondência entre a informação visível da pessoa singular e a documentação fornecida;



- b) se o cliente for uma entidade jurídica, que esta consta de registo público, quando aplicável;
 - c) se o cliente for uma entidade jurídica, que a pessoa singular que o representa tem legitimidade para agir em seu nome.
39. Caso a solução de integração de clientes à distância envolva a utilização de dados biométricos para certificação da identidade dos clientes, as instituições de crédito e financeiras devem certificar-se de que os dados biométricos são suficientemente únicos para estarem inequivocamente associados a uma única pessoa singular. As instituições de crédito e financeiras devem utilizar algoritmos sólidos e fiáveis para verificar a correspondência entre os dados biométricos fornecidos no documento de identidade apresentado e o cliente a ser integrado. Nas situações em que a solução não proporcione o nível de confiança exigido, devem ser aplicados controlos adicionais.
40. Nos casos em que os comprovativos apresentados sejam de qualidade insuficiente, resultando em ambiguidade ou incerteza que afete a realização de controlos à distância, o processo individual de integração de cliente à distância deve ser interrompido e reiniciado ou redirecionado para uma verificação presencial.
41. Quando as instituições de crédito e financeiras utilizam soluções de integração à distância não acompanhadas, nas quais o cliente não interage com um colaborador para que este realize o processo de verificação, devem:
- a) assegurar que todas as fotografias ou vídeos são captados em condições de iluminação adequadas e que as propriedades exigidas são captadas com a clareza necessária para permitir a correta verificação da identidade do cliente;
 - b) assegurar que qualquer fotografia ou vídeo é captado no momento em que o cliente realiza o processo de verificação;
 - c) realizar verificações de *liveness detection*, que podem incluir procedimentos nos quais é solicitada uma ação específica ao cliente para verificar a sua presença ou que podem basear-se na análise dos dados recebidos e não exigem uma ação específica por parte do cliente;
 - d) utilizar algoritmos sólidos e fiáveis para verificar se a(s) fotografia(s) ou vídeo(s) captado(s) corresponde(m) à(s) fotografia(s) extraída(s) do(s) documento(s) oficial(ais) pertencente(s) ao cliente.
42. Sempre que as instituições de crédito e financeiras utilizem soluções de integração de clientes à distância nas quais o cliente interaja com um colaborador para realizar o processo de verificação, devem:



- a) assegurar que a qualidade da imagem e do áudio é suficiente para permitir a verificação adequada da identidade do cliente e que são utilizados sistemas tecnológicos fiáveis;
 - b) prever a participação de um colaborador que tenha conhecimentos suficientes acerca da regulamentação ABC/CFT aplicável e dos aspetos de segurança da verificação à distância, assim como formação suficiente para antecipar e impedir a utilização intencional ou deliberada de técnicas de manipulação relacionadas com a verificação à distância, bem como para detetar e reagir em caso de ocorrência de tais técnicas;
 - c) elaborar um guia de entrevista que defina as várias etapas do processo de verificação à distância, bem como as ações exigidas ao colaborador. O guia de entrevista deve incluir orientações sobre a vigilância e a identificação de fatores psicológicos ou outras características que possam caracterizar comportamentos suspeitos durante a verificação à distância.
43. Sempre que possível, as instituições de crédito e financeiras devem utilizar soluções de integração de clientes à distância que incluam aleatorização na sequência de ações a realizar pelo cliente para efeitos de verificação, a fim de prevenir riscos como a utilização de identidades sintéticas ou de coação. Sempre que possível, as instituições de crédito e financeiras devem também prever atribuições aleatórias para o colaborador responsável pelo processo de verificação à distância, a fim de evitar a colusão entre o cliente e o colaborador responsável.
44. Além do que precede, e sempre que tal seja proporcional ao risco de BC/FT associado à relação de negócio, as instituições de crédito e financeiras devem utilizar um ou mais dos controlos seguintes ou uma medida semelhante para aumentar a fiabilidade do processo de verificação. Entre estes controlos ou medidas podem incluir-se, entre outros, os seguintes:
- a) que o primeiro pagamento seja efetuado através de uma conta titulada, individual ou conjuntamente, pelo cliente, numa instituição de crédito ou financeira regulamentada no EEE ou num país terceiro com requisitos de ABC/CFT que não sejam menos rigorosos do que os requisitos exigidos pela Diretiva (UE) 2015/849;
 - b) enviar ao cliente um código de acesso gerado aleatoriamente para confirmar a sua presença durante o processo de verificação à distância. O código de acesso deve ser um código de utilização única e com limite de tempo;
 - c) recolher dados biométricos para os comparar com os dados recolhidos através de outras fontes independentes e fiáveis;
 - d) contactos telefónicos com o cliente;
 - e) envio direto (eletrónico e postal) ao cliente.



45. As instituições de crédito e as instituições financeiras devem considerar cumpridos os critérios dos parágrafos 38 a 43 quando a solução implementada recorra a um dos seguintes meios:
- a) sistemas de identificação eletrónica notificados em conformidade com o artigo 9.º do Regulamento (UE) n.º 910/2014 e que cumpram os requisitos dos níveis de garantia «substancial» ou «elevado», em conformidade com o artigo 8.º do mesmo regulamento;
 - b) serviços de confiança qualificados relevantes que cumpram os requisitos do Regulamento (UE) n.º 910/2014, em particular o capítulo III, secção 3, e o artigo 24.º, n.º 1, parágrafo 2, alínea b), desse regulamento.

4.5 Recurso a terceiros e externalização

46. Além dos pontos referidos no parágrafo 9, as instituições de crédito e as instituições financeiras devem incluir nas suas políticas e procedimentos especificações que definam quais as funções e atividades de integração de clientes à distância que serão exercidas ou realizadas pela instituição de crédito e financeira, por terceiros ou por outro prestador de serviços externalizado.

4.5.1 Recurso a terceiros em conformidade com o capítulo II, secção 4, da Diretiva (UE) 2015/849

47. Além das Orientações da EBA relativas aos fatores de risco⁸, em especial as orientações 2.20 a 2.21 e 4.32 a 4.37 dessas Orientações, devem aplicar os seguintes critérios:
- a) adotar as medidas necessárias para se certificar de que os processos e procedimentos de CDD dos sistemas de integração de clientes à distância dos terceiros, bem como as informações e os dados que estes recolhem nesse contexto, são suficientes e coerentes com os requisitos estabelecidos nas presentes orientações;
 - b) assegurar a continuidade das relações de negócios estabelecidas entre o cliente e a instituição de crédito ou financeira, a fim de prevenir acontecimentos que possam revelar deficiências no processo de integração de clientes à distância realizado pelo terceiro.

4.5.2 Externalização da CDD

48. Caso as instituições de crédito e as instituições financeiras externalizem a totalidade ou parte do processo de integração de clientes à distância a um prestador de serviços externalizado, nos termos do artigo 29.º da Diretiva (UE) 2015/849, devem aplicar, para além das orientações 2.20 a 2.21 e 4.32 a 4.37 das Orientações da EBA relativas aos fatores de risco e,

⁸ EBA/GL/2021/02



quando aplicável, das Orientações da EBA relativas à externalização,⁹ antes e durante a relação de negócio com o prestador de serviços externalizado, as seguintes medidas, cuja extensão deve ser ajustada em função do risco:

- a) assegurar que o prestador de serviços externalizado efetivamente aplica e cumpre as políticas e os procedimentos de integração de clientes à distância da instituição de crédito e financeira, em conformidade com o acordo de subcontratação. Este objetivo deve ser alcançado através de relatórios periódicos, de um acompanhamento contínuo, de visitas ao local ou de testes por amostragem;
- b) realizar avaliações para assegurar que o prestador de serviços externalizado dispõe de meios suficientes e capacidade para realizar o processo de integração de clientes à distância. As avaliações podem incluir, nomeadamente, a avaliação da formação do pessoal, da adequação dos meios tecnológicos e da gestão dos dados do prestador de serviços externalizado;
- c) assegurar que o prestador de serviços externalizado informa as instituições de crédito e as instituições financeiras de qualquer proposta de alteração do processo de integração de clientes à distância ou de qualquer alteração à solução fornecida pelo prestador de serviços externalizado.

49. Caso o prestador de serviços externalizado armazene dados dos clientes, incluindo, mas não exclusivamente, fotografia, vídeos e documentos, durante o processo de integração à distância, as instituições de crédito e financeiras devem assegurar que:

- a) apenas os dados necessários do cliente são recolhidos e armazenados, em conformidade com um período de conservação claramente definido;
- b) o acesso aos dados é estritamente limitado e registado;
- c) são aplicadas medidas de segurança adequadas para garantir a proteção dos dados armazenados.

4.6 Gestão dos riscos associados às TIC e à segurança

50. As instituições de crédito e financeiras devem identificar e gerir os seus riscos em matéria de TIC e de segurança relacionados com a utilização do processo de integração de clientes à distância, nomeadamente nos casos em que as instituições de crédito e financeiras dependem de terceiros ou quando o serviço é externalizado, incluindo a entidades do grupo.

51. Além do cumprimento dos requisitos estabelecidos nas Orientações da EBA relativas à gestão dos riscos associados às TIC e à segurança¹⁰ quando aplicável, as instituições de crédito e financeiras devem utilizar canais de comunicação seguros para interagir com o cliente durante

⁹ Orientações da EBA relativas à subcontratação.docx (europa.eu)

¹⁰ EBA/GL/2019/04



o processo de integração de clientes à distância. A solução de integração de clientes à distância deve utilizar protocolos e algoritmos criptográficos seguros de acordo com as melhores práticas do setor, a fim de salvaguardar a confidencialidade, a autenticidade e a integridade dos dados trocados, quando aplicável.

52. As instituições financeiras e de crédito devem proporcionar um ponto de acesso seguro para iniciar o processo de integração de clientes à distância com base em certificados qualificados de selos eletrônicos, tal como referido no artigo 3.º, n.º 30, do Regulamento (UE) n.º 910/2014, ou de autenticação de sítios Web, tal como referido no artigo 3.º, n.º 39, do mesmo regulamento. O cliente deve ainda ser informado das medidas de segurança aplicáveis que devem ser tomadas para garantir uma utilização segura do sistema.
53. Sempre que seja utilizado um dispositivo polivalente para executar o processo de integração de clientes à distância, deve ser utilizado um ambiente seguro para a execução do código de software do lado do cliente, quando aplicável. Devem ser aplicadas medidas de segurança adicionais para garantir a segurança e a confiança do código de software e dos dados recolhidos, de acordo com a avaliação dos riscos de segurança estabelecida nas Orientações da EBA relativas à gestão dos riscos associados às TIC e à segurança.

4.7 Conformidade com as presentes orientações nos casos em que as instituições de crédito e as instituições financeiras utilizam serviços de confiança e processos de identificação nacionais, tal como referido no artigo 13.º, n.º 1, alínea a), da Diretiva (UE) 2015/849

54. As instituições de crédito e as instituições financeiras podem utilizar os serviços de confiança e os processos de identificação eletrónica relevantes regulamentados, reconhecidos, aprovados ou aceites pelas autoridades nacionais relevantes a que se refere o artigo 13.º, n.º 1, alínea a), da Diretiva (UE) 2015/849 para dar cumprimento às presentes orientações. Ao utilizarem essas soluções, as instituições de crédito e financeiras devem avaliar em que medida a solução está em conformidade com as disposições das presentes orientações e aplicar as medidas necessárias para atenuar quaisquer riscos relevantes decorrentes da utilização dessas soluções. Devem ter especialmente em conta se são tidos em conta os seguintes riscos:
 - a) os riscos envolvidos na autenticação, e definir nas suas políticas e procedimentos medidas de atenuação específicas, especialmente no que diz respeito aos riscos de fraude de usurpação de identidade;
 - b) o risco de que a identidade do cliente não seja a identidade alegada;



- c) o risco de provas de identidade perdidas, roubadas, suspensas, revogadas ou caducadas, implementando, conforme apropriado, ferramentas para detetar e impedir a utilização de fraudes de usurpação de identidade.