Orientações

EBA/GL/2019/04

28 de novembro de 2019

Orientações da EBA relativas à gestão dos riscos associados às TIC e à segurança

Obrigações de cumprimento e de comunicação de informação

Natureza das presentes orientações

1. O presente documento contém orientações emitidas ao abrigo do artigo 16.º do Regulamento (UE) n.º 1093/2010 [1] . Nos termos do artigo 16.º, n.º 3, do Regulamento (UE) n.º 1093/2010, as autoridades competentes e as instituições financeiras devem desenvolver todos os esforços para dar cumprimento às orientações.

2. As orientações refletem a posição da EBA sobre o que constituem práticas de supervisão adequadas no âmbito do Sistema Europeu de Supervisão Financeira ou sobre o modo como a legislação da União Europeia 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 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 comunicação de informações

3. Nos termos do disposto no artigo 16.º, n.º 3, do Regulamento (UE) n.º 1093/2010, as autoridades competentes confirmam à EBA se dão ou tencionam dar cumprimento às presentes orientações ou, caso contrário, indicam as razões para o não cumprimento até ([dd.mm.aaaa]). Na ausência de qualquer notificação até à referida data, a EBA considera que as autoridades competentes em causa não cumprem as orientações. As notificações efetuam-se mediante o envio do formulário disponível no sítio Web da EBA para o endereço compliance@eba.europa.eu com a referência «EBA/GL/2019/04». 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 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).

Objeto, âmbito de aplicação e definições

Objeto

5. As presentes orientações baseiam-se no disposto no artigo 74º da Diretiva 2013/36/UE (Diretiva Requisitos de Fundos Próprios) relativa ao governo interno e derivam do mandato para emitir orientações previsto no artigo 95.º, n.º 3, da Diretiva (UE) 2015/2366 (segunda Diretiva de Serviços de Pagamento, DSP2).

6. As presentes orientações especificam as medidas de gestão dos riscos que as instituições financeiras (na aceção do n.º 9 abaixo) devem tomar, em conformidade com o artigo 74.º da Diretiva Requisitos de Fundos Próprios, para gerir os seus riscos associados às TIC e à segurança para todas as atividades, e que os prestadores de serviços de pagamento (PSP, na aceção do n.º 9 abaixo) devem tomar, em conformidade com o artigo 95.º, n.º 1, da DSP2, para gerir os riscos operacionais e de segurança (considerados como os «riscos associados às TIC e à segurança») relacionados com os serviços de pagamento por si prestados. As orientações incluem requisitos para a segurança da informação, incluindo a cibersegurança, na medida em que a informação é mantida em sistemas de TIC.

Âmbito de aplicação

7. As presentes orientações aplicam-se em relação à gestão dos riscos associados às TIC e à segurança nas instituições financeiras (na aceção do n.º 9). Para efeitos das presentes orientações, a expressão «riscos associados às TIC e à segurança» aborda os riscos operacionais e de segurança previstos no artigo 95.º da DSP2 no que diz respeito à prestação de serviços de pagamento.

8. No que se refere aos prestadores de serviços de pagamento (na aceção do n.º 9), as presentes orientações aplicam-se à sua prestação de serviços de pagamento, em consonância com o âmbito e o mandato previstos no artigo 95.º da DSP2. No que se refere às instituições (tal como definidas no n.º 9), as presentes orientações aplicam-se a todas as atividades por si exercidas.

Destinatários

9. As presentes orientações destinam-se às instituições financeiras que, para efeitos das presentes orientações, se referem a (1) prestadores de serviços de pagamento, na aceção do artigo 4.º, n.º 11, da DSP2, e a (2) instituições, ou seja, instituições de crédito e empresas de investimento, na aceção do artigo 4.º, n.º 1, ponto 3, do Regulamento (UE) n.º 575/2013. As presentes orientações aplicam-se igualmente às autoridades competentes, na aceção do artigo 4.º, n.º 1, ponto 40, do Regulamento (UE) n.º 575/2013, incluindo o Banco Central Europeu no âmbito das matérias relacionadas com as atribuições que lhe foram conferidas pelo Regulamento (UE) n.º 1024/2013, e às autoridades competentes nos termos da DSP2, na aceção do artigo 4.º, n.º 2, alínea i), do Regulamento (UE) n.º 1093/2010.

Definições

10. Salvo especificação em contrário, os termos utilizados e definidos na Diretiva 2013/36/UE (Diretiva Requisitos de Fundos Próprios), no Regulamento (UE) n.º 575/2013 (Regulamento de Requisitos de Capital) e na Diretiva (UE) 2015/2366 (DSP2) têm o mesmo significado nas presentes orientações. Adicionalmente, para efeitos das presentes orientações, aplicam-se as seguintes definições:

Riscos associados às TIC e à segurança	O risco de perdas por violação da confidencialidade, falta de integridade de sistemas e dados, inadequação ou indisponibilidade de sistemas e dados ou incapacidade para alterar as tecnologias da informação (TI) num período de tempo e custos razoáveis quando o ambiente ou os requisitos empresariais se alteram (isto é, agilidade)[2]. Tal inclui riscos de segurança resultantes de eventos externos ou processos internos inadequados ou deficientes, incluindo ciberataques ou uma segurança física inadequada.
Órgão de administração	(a) Para as instituições de crédito e empresas de investimento, este termo tem o mesmo significado que a definição constante do artigo 3.º, n.º 1, ponto 7, da Diretiva 2013/36/UE. (b) Para as instituições de pagamento ou instituições de moeda eletrónica, este termo aplica-se aos diretores ou pessoas responsáveis pela gestão das instituições de pagamento e instituições de moeda eletrónica e, quando relevante, às pessoas responsáveis pela gestão das atividades de serviços de pagamento das instituições de pagamento e instituições de moeda eletrónica. (c) Para os prestadores de serviços de pagamento referidos no artigo 1.º, n.º 1, alíneas c), e) e f), da Diretiva (UE) 2015/2366, este termo tem o significado que lhe é conferido pelo direito nacional ou comunitário aplicável.
Incidente operacional ou de segurança	Um único evento ou uma série de eventos conexos e imprevistos pela instituição financeira que tem, ou poderá vir a ter, um impacto negativo na integridade, disponibilidade, confidencialidade e/ou autenticidade dos serviços.
Direção de topo	(a) Para as instituições de crédito e empresas de investimento, este termo tem o mesmo significado que a definição constante do artigo 3.º, n.º 1, ponto 9, da Diretiva 2013/36/UE. (b) Para as instituições de pagamento e instituições de moeda eletrónica, este termo aplica-se às pessoas singulares que exercem funções executivas dentro de uma instituição e que

[2] Definição constante das Orientações relativas aos procedimentos e metodologias comuns a seguir no âmbito do processo de revisão e avaliação pelo supervisor, de 19 de dezembro de 2014 (EBA/GL/2014/13), com a redação que lhe foi dada pelo documento EBA/GL/2018/03.

	são responsáveis e respondem perante o órgão de administração pela gestão diária da instituição. (c) Para os prestadores de serviços de pagamento referidos no artigo 1.º, n.º 1, alíneas c), e) e f), da Diretiva (UE) 2015/2366, este termo tem o significado que lhe é conferido pelo direito nacional ou comunitário aplicável.
Apetência pelo risco	Os tipos de risco e o seu nível agregado que os prestadores de serviços de pagamento e as instituições estão dispostos a assumir no contexto da sua capacidade de risco, de acordo com o seu modelo de negócio, para alcançar os seus objetivos estratégicos.
Função de auditoria	(a) Para as instituições de crédito e empresas de investimento, a função de auditoria é a referida na secção 22 das Orientações da EBA sobre governo interno (EBA/GL/2017/11). (b) Para os prestadores de serviços de pagamento que não sejam instituições de crédito, a função de auditoria deve ser independente do prestador de serviços de pagamento, podendo ser uma função de auditoria interna e/ou externa.
Projetos de TIC	Qualquer projeto, ou parte dele, em que os serviços e sistemas de TIC sejam alterados, substituídos, rejeitados ou aplicados. Os projetos de TIC podem fazer parte de planos mais vastos de TIC ou de transformação de negócio.
Terceiros	Uma organização que tenha estabelecido relações comerciais ou celebrado contratos com uma entidade para fornecer um produto ou prestar um serviço[3].
Ativo de informação	Um conjunto de informações, tangíveis ou intangíveis, que vale a pena proteger.
Ativo de TIC	Um ativo de *software* ou de *hardware* que se encontra no ambiente empresarial.
Sistemas de TIC[4]	TIC implementadas no quadro de um mecanismo ou de uma rede de interligação que suporta as operações de uma instituição financeira.
Serviços de TIC[5]	Serviços fornecidos pelos sistemas de TIC a um ou mais utilizadores internos ou externos. Exemplificando, incluem-se os serviços de introdução, armazenamento, tratamento e comunicação de dados, mas também os serviços de monitorização e de apoio às operações e à tomada de decisão.

[3] Definição dos elementos fundamentais do G7 para a gestão do risco cibernético de terceiros no setor financeiro.
[4] Definição constante das Orientações relativas à avaliação do risco das TIC no âmbito do processo de revisão e avaliação pelo supervisor (SREP) (EBA/GL/2017/05).
[5] Ver nota de rodapé 4.

Implementação

Data de aplicação

11. As presentes orientações são aplicáveis a partir de 30 de junho de 2020.

Revogação

12. As Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança (EBA/GL/2017/17) emitidas em 2017 serão revogadas pelas presentes orientações na data em que estas se tornarem aplicáveis.

Orientações relativas à gestão dos riscos associados às TIC e à segurança

1.1. Proporcionalidade

1. Todas as instituições financeiras devem cumprir as disposições estabelecidas nas presentes orientações de forma proporcional e tendo em conta a dimensão das instituições financeiras, bem como a sua organização interna e a natureza, o âmbito, a complexidade e o grau de risco dos serviços e produtos que as instituições financeiras fornecem ou tencionam fornecer.

1.2. Governo e estratégia

1.2.1. Governo

2. O órgão de administração deve assegurar que as instituições financeiras disponham de um quadro adequado de controlo interno e de governo interna para gerir os seus riscos associados às TIC e à segurança. O órgão de administração deve definir funções e responsabilidades claras para as funções de TIC, a gestão dos riscos de segurança da informação e continuidade de negócio, incluindo as do órgão de administração e dos respetivos comités.
3. O órgão de administração deve assegurar que a quantidade e as competências do pessoal das instituições financeiras são adequadas para apoiar as suas necessidades operacionais de TIC e os seus processos de gestão dos riscos associados às TIC e à segurança, numa base contínua, e para garantir a aplicação da sua estratégia em matéria de TIC. O órgão de administração deve assegurar que o orçamento atribuído é adequado para cumprir o acima exposto. Além disso, as instituições financeiras devem assegurar que todos os membros do pessoal, incluindo os colaboradores que desempenham funções essenciais, recebam formação adequada sobre os riscos associados às TIC e à segurança, nomeadamente sobre a segurança da informação, anualmente, ou com maior frequência, se necessário (ver também a secção 1.4.7).

4. O órgão de administração assume a responsabilidade global pela definição, aprovação e supervisão da aplicação da estratégia em matéria de TIC das instituições financeiras como parte da sua estratégia de negócio global, bem como pelo estabelecimento de um quadro eficaz de gestão dos riscos associados às TIC e à segurança.

1.2.2. Estratégia

5. A estratégia em matéria de TIC deve ser harmonizada com a estratégia de negócio global das instituições financeiras, devendo definir:

    a) A forma como as TIC das instituições financeiras devem evoluir para apoiar e participar eficazmente na sua estratégia de negócio, incluindo a evolução da estrutura organizacional, as alterações do sistema de TIC e as principais dependências em relação a terceiros;
    b) A estratégia planeada e a evolução da arquitetura das TIC, incluindo as dependências em relação a terceiros;
    c) Objetivos claros em matéria de segurança da informação, centrados nos sistemas e serviços de TIC, no pessoal e nos processos.

6. As instituições financeiras devem elaborar conjuntos de planos de ação que contenham medidas a tomar para alcançar o objetivo da estratégia em matéria de TIC. Estes devem ser comunicados a todo o pessoal pertinente (incluindo contratantes e prestadores de serviços terceiros, quando aplicável e pertinente). Os planos de ação devem ser revistos periodicamente para garantir a sua pertinência e adequação. As instituições financeiras devem igualmente criar processos para monitorizar e medir a eficácia da aplicação da sua estratégia em matéria de TIC.

1.2.3. Recurso a prestadores de serviços terceiros

7. Sem prejuízo das Orientações da EBA relativas à subcontratação (EBA/GL/2019/02) e do artigo 19.º da DSP2, as instituições financeiras devem assegurar a eficácia das medidas de redução dos riscos definidas pelo seu quadro de gestão dos riscos, incluindo as medidas estabelecidas nas presentes orientações, quando as funções operacionais dos serviços de pagamento e/ou dos serviços de TIC, e dos sistemas de TIC de qualquer atividade, forem subcontratadas, incluindo a entidades pertencentes ao mesmo grupo, ou quando se recorra a terceiros.

8. Para assegurar a continuidade dos serviços de TIC e dos sistemas de TIC, as instituições financeiras devem assegurar que os contratos e acordos de nível de serviço (tanto em circunstâncias normais como em caso de interrupção dos serviços — ver igualmente a secção 1.7.2) celebrados com prestadores de serviços (prestadores de serviços subcontratados, entidades pertencentes ao mesmo grupo ou prestadores de serviços terceiros) incluam o seguinte:

    a) Objetivos e medidas adequados e proporcionais relacionados com a segurança da informação, incluindo requisitos como requisitos mínimos de cibersegurança; especificações do ciclo de vida dos dados da instituição financeira; quaisquer requisitos

relativos à cifragem de dados, à segurança da rede e aos processos de monitorização da segurança, bem como à localização dos centros de dados;

b) Procedimentos de tratamento de incidentes operacionais e de segurança, incluindo de escalonamento e de comunicação de informações.

9. As instituições financeiras devem monitorizar e assegurar o nível de conformidade de tais prestadores com os objetivos de segurança, medidas e metas de desempenho da instituição financeira.

1.3. Quadro de gestão dos riscos associados às TIC e à segurança

1.3.1. Organização e objetivos

10. As instituições financeiras devem identificar e gerir os seus riscos associados às TIC e à segurança. A(s) função(ões) de TIC encarregada(s) dos sistemas, processos e operações de segurança de TIC deve(m) dispor de processos e controlos adequados para garantir que todos os riscos são identificados, analisados, medidos, monitorizados, geridos, comunicados e mantidos dentro dos limites da apetência pelo risco da instituição financeira e que os projetos e sistemas que fornecem e as atividades que desenvolvem estão em conformidade com os requisitos externos e internos.

11. As instituições financeiras devem atribuir a responsabilidade pela gestão e supervisão dos riscos associados às TIC e à segurança, a uma função de controlo, cumprindo os requisitos da secção 19 das Orientações da EBA sobre governo interno (EBA/GL/2017/11). As instituições financeiras devem assegurar a independência e a objetividade desta função de controlo, separando-a devidamente dos processos operacionais de TIC. Esta função de controlo deve ser diretamente responsável perante o órgão de administração, e responsável pelo acompanhamento e controlo da observância do quadro de gestão dos riscos associados às TIC e à segurança. Deve assegurar que os riscos associados às TIC e à segurança sejam identificados, medidos, avaliados, geridos, monitorizados e comunicados. As instituições financeiras devem assegurar que esta função de controlo não seja responsável por qualquer auditoria interna.

    A função de auditoria interna deve, seguindo uma abordagem baseada no risco, ter a capacidade de rever de forma independente e garantir de forma objetiva a conformidade de todas as unidades e atividades relacionadas com as TIC e a segurança de uma instituição financeira com as políticas e procedimentos da instituição financeira e com os requisitos externos, cumprindo os requisitos da secção 22 das Orientações da EBA sobre governo interno (EBA/GL/2017/11).

12. As instituições financeiras devem definir e atribuir funções e responsabilidades fundamentais, bem como linhas de comunicação de informações pertinentes, para que o quadro de gestão dos riscos associados às TIC e à segurança seja eficaz. Este quadro deve ser totalmente integrado nos processos globais de gestão dos riscos das instituições financeiras e estar alinhado com os mesmos.

13. O quadro de gestão dos riscos associados às TIC e à segurança deve incluir processos para:

    a) Determinar a apetência pelo risco no que se refere aos riscos associados às TIC e à segurança, de acordo com a apetência pelo risco da instituição financeira;
    b) Identificar e avaliar os riscos associados às TIC e à segurança a que uma instituição financeira está exposta;
    c) Definir medidas de redução dos riscos, incluindo controlos, para reduzir os riscos associados às TIC e à segurança;
    d) Controlar a eficácia destas medidas, bem como o número de incidentes comunicados, incluindo, para os prestadores de serviços de pagamento, os incidentes comunicados em conformidade com o artigo 96.º da DSP2, que afetam as atividades relacionadas com as TIC, e agir no sentido de corrigir as medidas, se necessário;
    e) Informar o órgão de administração sobre os controlos e riscos associados às TIC e à segurança;
    f) Identificar e avaliar se existem riscos associados às TIC e à segurança resultantes de qualquer alteração significativa do sistema de TIC ou dos serviços, processos ou procedimentos de TIC, e/ou após qualquer incidente operacional ou de segurança significativo.

14. As instituições financeiras devem assegurar que o quadro de gestão dos riscos associados às TIC e à segurança seja documentado, e continuamente melhorado, com base nos «lições aprendidas» durante a sua aplicação e monitorização. O quadro de gestão dos riscos associados às TIC e à segurança deve ser aprovado e revisto, pelo menos uma vez por ano, pelo órgão de administração.

1.3.2. Identificação de áreas, processos e ativos

15. As instituições financeiras devem identificar, criar e manter atualizado o inventário das suas áreas de negócio, funções e processos de apoio para identificar a importância de cada um destes e as suas interdependências relativamente aos riscos associados às TIC e à segurança.

16. Além disso, as instituições financeiras devem identificar, criar e manter atualizado o inventário dos ativos de informação que apoiam as suas áreas de negócio e processos críticos, como os sistemas de TIC, pessoal, contratantes, terceiros e dependências de outros sistemas e processos internos e externos, para poderem, pelo menos, gerir os ativos de informação que apoiam as suas áreas de negócio e processos críticos.

1.3.3. Classificação e avaliação dos riscos

17. As instituições financeiras devem classificar as áreas de negócio, processos de apoio e ativos de informação identificados referidos nos n.^{os} 15 e 16 em termos de criticidade.

18. Para definir a criticidade das áreas de negócio, dos processos de apoio e dos ativos de informação identificados, as instituições financeiras devem, no mínimo, considerar os requisitos de confidencialidade, integridade e disponibilidade. Deve haver uma clara atribuição de responsabilização e responsabilidade pelos ativos de informação.

19. As instituições financeiras devem rever a adequação da classificação dos ativos de informação e da documentação pertinente aquando da realização da avaliação dos riscos.

20. As instituições financeiras devem identificar os riscos associados às TIC e à segurança que têm impacto nas áreas de negócio, nos processos de apoio e nos ativos de informação identificados e classificados, de acordo com a sua criticidade. Esta avaliação dos riscos deve ser realizada e documentada anualmente ou, se necessário, a intervalos mais curtos. Tal avaliação dos riscos deve igualmente ser realizada sobre quaisquer alterações significativas das infraestruturas, dos processos ou dos procedimentos que afetem as áreas de negócio, os processos de apoio ou os ativos de informação, devendo, consequentemente, ser atualizada a atual avaliação dos riscos das instituições financeiras.

21. As instituições financeiras devem assegurar que monitorizam continuamente as ameaças e vulnerabilidades pertinentes para os seus processos empresariais, funções de apoio e ativos de informação, devendo rever regularmente os cenários de risco que os afetam.

1.3.4. Redução dos riscos

22. Com base nas avaliações dos riscos, as instituições financeiras devem determinar que medidas são necessárias para reduzir os riscos identificados, associados às TIC e à segurança, para níveis aceitáveis e se é necessário introduzir alterações nos processos empresariais, nas medidas de controlo, nos sistemas de TIC e nos serviços de TIC existentes. Uma instituição financeira deve ter em consideração o tempo necessário para implementar estas alterações e o tempo para tomar medidas provisórias adequadas de redução dos riscos para reduzir os riscos associados às TIC e à segurança, a fim de se manter dentro dos limites da apetência pelo risco da instituição financeira, no que se refere aos riscos associados às TIC e à segurança.

23. As instituições financeiras devem definir e aplicar medidas para reduzir os riscos identificados, associados às TIC e à segurança, e para proteger os ativos de informação de acordo com a sua classificação.

1.3.5. Comunicação de informações

24. As instituições financeiras devem comunicar os resultados da avaliação dos riscos ao órgão de administração de forma clara e atempada. Essa comunicação não prejudica a obrigação dos prestadores de serviços de pagamento de fornecerem às autoridades competentes uma avaliação exaustiva e atualizada dos riscos, tal como previsto no artigo 95.º, n.º 2, da Diretiva (UE) 2015/2366.

1.3.6. Auditoria

25. O governo, os sistemas e os processos de uma instituição financeira para os seus riscos associados às TIC e à segurança devem ser auditados periodicamente por auditores com conhecimentos, competências e experiência suficientes em matéria de riscos associados às TIC, à segurança e pagamentos (no que se refere aos PSP), que lhes permitam fornecer uma garantia independente da sua eficácia, ao órgão de administração. Os auditores devem ser

independentes da instituição financeira. A frequência e o objetivo de tais auditorias devem ser proporcionais aos riscos relevantes associados às TIC e à segurança.

26. O órgão de administração de uma instituição financeira deve aprovar o plano de auditoria, incluindo todas as auditorias das TIC e todas as alterações significativas das mesmas. O plano de auditoria e a sua execução, incluindo a frequência de auditoria, devem refletir e ser proporcionais aos riscos inerentes associados às TIC e à segurança na instituição financeira, devendo ser atualizados regularmente.

27. Deve ser estabelecido um processo formal de acompanhamento que inclua disposições para a verificação e a correção atempadas dos resultados cruciais de auditorias das TIC.

1.4. Segurança da informação

1.4.1. Política de segurança da informação

28. As instituições financeiras devem desenvolver e documentar uma política de segurança da informação que deve definir os princípios e regras de alto nível para proteger a confidencialidade, integridade e disponibilidade dos dados e das informações das instituições financeiras e dos seus clientes. Para os prestadores de serviços de pagamento, esta política é identificada no documento relativo à política de segurança, a adotar em conformidade com o artigo 5.º, n.º 1, alínea j), da Diretiva (UE) 2015/2366. A política de segurança da informação deve estar em consonância com os objetivos de segurança da informação das instituições financeiras e basear-se nos resultados pertinentes do processo de avaliação dos riscos. A política deve ser aprovada pelo órgão de administração.

29. A política deve incluir uma descrição das principais funções e responsabilidades da gestão da segurança da informação, devendo estabelecer os requisitos aplicáveis ao pessoal e aos contratantes, aos processos e à tecnologia em relação à segurança da informação, reconhecendo que o pessoal e os contratantes a todos os níveis têm a responsabilidade de garantir a segurança da informação das instituições financeiras. A política deve assegurar a confidencialidade, integridade e disponibilidade dos ativos e recursos críticos, quer sejam físicos ou lógicos, e dos dados sensíveis de uma instituição financeira, independentemente de estarem armazenados, em trânsito ou em utilização. A política de segurança da informação deve ser comunicada a todo o pessoal e a todos os contratantes da instituição financeira.

30. Com base na política de segurança da informação, as instituições financeiras devem estabelecer e aplicar medidas de segurança para reduzir os riscos associados às TIC e à segurança a que estão expostas. Estas medidas devem incluir:

    a) A organização e a governação em conformidade com os n.^{os} 10 e 11;
    b) A segurança lógica (secção 1.4.2);
    c) A segurança física (secção 1.4.3);
    d) A segurança das operações de TIC (secção 1.4.4);
    e) A monitorização da segurança (secção 1.4.5);
    f) Revisões, avaliação e testes da segurança da informação (secção 1.4.6);
    g) Formação e sensibilização em matéria de segurança da informação (secção 1.4.7).

1.4.2. Segurança lógica

31. As instituições financeiras devem definir, documentar e aplicar procedimentos de controlo de acesso lógico (identidade e gestão de acesso). Estes procedimentos devem ser aplicados, executados, monitorizados e revistos periodicamente. Os procedimentos devem igualmente incluir controlos para monitorizar anomalias. Estes procedimentos devem, no mínimo, aplicar os seguintes elementos, nos quais o termo «utilizador» inclui igualmente os utilizadores técnicos:

    (a) **Necessidade de tomar conhecimento, privilégios mínimos e segregação de funções:** as instituições financeiras devem gerir os direitos de acesso aos ativos de informação e aos seus sistemas de apoio com base na «necessidade de tomar conhecimento» incluindo no que se refere ao acesso remoto. Devem ser concedidos aos utilizadores direitos mínimos de acesso, estritamente necessários para a execução das suas funções (princípio dos «privilégios mínimos»), isto é, para evitar o acesso injustificado a um grande conjunto de dados ou para impedir a atribuição de combinações de direitos de acesso que possam ser utilizadas para contornar os controlos (princípio da «segregação de funções»).

    (b) **Responsabilização do utilizador:** as instituições financeiras devem limitar, tanto quanto possível, a utilização de contas de utilizador genéricas e partilhadas, e garantir que os utilizadores possam ser identificados pelas ações realizadas nos sistemas de TIC.

    (c) **Direitos de acesso privilegiados:** as instituições financeiras devem aplicar controlos rigorosos sobre o acesso privilegiado ao sistema, limitando estritamente e supervisionando de perto as contas com elevados direitos de acesso ao sistema (por exemplo, as contas de administrador). Para assegurar uma comunicação segura e reduzir o risco, deve ser apenas concedido o acesso remoto administrativo aos sistemas críticos de TIC com base na necessidade de tomar conhecimento e quando são utilizadas soluções de autenticação forte.

    (d) **Registo das atividades dos utilizadores:** no mínimo, todas as atividades de utilizadores privilegiados devem ser registadas e monitorizadas. Os registos de acesso devem ser protegidos para evitar alterações ou eliminações não autorizadas, e mantidos durante um período proporcional à criticidade das áreas de negócio, processos de apoio e ativos de informação identificados, em conformidade com a secção 1.3.3, sem prejuízo dos requisitos de retenção estabelecidos no direito nacional ou comunitário. Uma instituição financeira deve utilizar esta informação para facilitar a identificação e investigação de atividades anómalas que tenham sido detetadas durante a prestação de serviços.

    (e) **Gestão de acesso:** os direitos de acesso devem ser concedidos, retirados ou alterados de forma atempada, de acordo com fluxos de trabalho de aprovação pré-definidos, que envolvam o proprietário das informações consultadas (proprietário do ativo de informação). Em caso de cessação do contrato de trabalho, os direitos de acesso devem ser imediatamente revogados.

(f) **Recertificação de acesso:** os direitos de acesso devem ser revistos periodicamente para assegurar que os utilizadores não possuam privilégios excessivos e que os direitos de acesso sejam revogados quando já não são necessários.

(g) **Métodos de autenticação:** as instituições financeiras devem aplicar métodos de autenticação suficientemente sólidos para garantir o cumprimento adequado e eficaz das políticas e procedimentos de controlo de acesso. Os métodos de autenticação devem ser proporcionais à criticidade dos sistemas de TIC, da informação ou do processo a que se acede. Estes métodos devem, no mínimo, incluir palavras-passe complexas ou métodos de autenticação mais fortes (como a autenticação de dois fatores), com base no risco relevante.

32. O acesso eletrónico através de aplicações a dados e sistemas de TIC deve ser limitado ao mínimo necessário para prestar o serviço em causa.

1.4.3. Segurança física

33. As medidas de segurança física das instituições financeiras devem ser definidas, documentadas e aplicadas para proteger as suas instalações, centros de dados e zonas sensíveis, do acesso não autorizado e dos perigos ambientais.

34. O acesso físico aos sistemas de TIC deve apenas ser permitido a pessoas autorizadas. A autorização deve ser atribuída de acordo com as tarefas e responsabilidades da pessoa em causa, bem como limitada a pessoas que sejam devidamente formadas e monitorizadas. O acesso físico deve ser revisto regularmente, para assegurar que os direitos de acesso desnecessários sejam imediatamente revogados quando não forem necessários.

35. As medidas adequadas de proteção contra perigos ambientais devem ser proporcionais à importância dos edifícios e à criticidade das operações, ou dos sistemas de TIC localizados nestes edifícios.

1.4.4. Segurança das operações de TIC

36. As instituições financeiras devem aplicar procedimentos para evitar a ocorrência de problemas de segurança nos sistemas e serviços de TIC, e devem minimizar o seu impacto na prestação de serviços de TIC. Estes procedimentos devem incluir as seguintes medidas:

a) Identificação de potenciais vulnerabilidades, que devem ser avaliadas e corrigidas, assegurando que o *software* e o *firmware* estão atualizados, incluindo os programas informáticos fornecidos pelas instituições financeiras aos seus utilizadores internos e externos, através da implementação de correções críticas de segurança ou da aplicação de controlos compensatórios;

b) Aplicação de linhas de base de configuração seguras de todos os componentes da rede;

c) Aplicação de segmentação de rede, sistemas de prevenção de perda de dados e cifragem do tráfego de rede (de acordo com a classificação dos dados);

d) Aplicação da proteção de terminais, incluindo servidores, estações de trabalho e dispositivos móveis; as instituições financeiras devem avaliar se os terminais cumprem

as normas de segurança por si definidas antes de lhes ser concedido acesso à rede empresarial;

e) Garantia da existência de mecanismos para verificar a integridade do *software*, do *firmware* e dos dados;

f) Cifragem dos dados armazenados e em trânsito (de acordo com a classificação dos dados).

37. Além disso, as instituições financeiras devem averiguar, numa base contínua, se as alterações ao ambiente operacional existente influenciam as medidas de segurança em vigor, ou exigem a adoção de medidas adicionais para reduzir os riscos conexos de forma adequada. Estas alterações devem fazer parte do processo de gestão de alterações formal da instituição financeira, o qual deve assegurar que as alterações são devidamente planeadas, testadas, documentadas, autorizadas e implementadas.

1.4.5. Monitorização da segurança

38. As instituições financeiras devem estabelecer e implementar políticas e procedimentos para detetar atividades anómalas que possam ter impacto na segurança da informação das instituições financeiras e para responder devidamente a esses eventos. Como parte desta monitorização contínua, as instituições financeiras devem implementar recursos adequados e eficazes para detetar e comunicar intrusões físicas ou lógicas, bem como violações de confidencialidade, integridade e disponibilidade dos ativos de informação. Os processos de monitorização e deteção contínuos devem abranger:

a) Fatores internos e externos pertinentes, incluindo as áreas administrativas de negócio e de TIC;

b) Operações, para detetar a utilização abusiva do acesso por terceiros ou outras entidades e a utilização abusiva interna do acesso;

c) Potenciais ameaças internas e externas.

39. As instituições financeiras devem estabelecer e implementar processos e estruturas organizacionais para identificar e monitorizar constantemente as ameaças à segurança que possam afetar materialmente a sua capacidade de prestar serviços. As instituições financeiras devem monitorizar ativamente os desenvolvimentos tecnológicos para assegurar que têm conhecimento dos riscos de segurança. As instituições financeiras devem implementar medidas de deteção, por exemplo para identificar possíveis fugas de informação, códigos maliciosos e outras ameaças à segurança, bem como vulnerabilidades em termos de *software* e *hardware* publicamente conhecidas, e verificar a existência de novas atualizações de segurança correspondentes.

40. O processo de monitorização da segurança deve igualmente ajudar uma instituição financeira a entender a natureza dos incidentes operacionais ou de segurança, a identificar tendências e a apoiar as investigações da organização.

1.4.6. Revisões, avaliação e testes da segurança da informação

41. As instituições financeiras devem realizar uma série de revisões, avaliações e testes da segurança da informação para garantir a identificação eficaz de vulnerabilidades nos seus sistemas e serviços de TIC. Por exemplo, as instituições financeiras podem realizar análises de lacunas em relação às normas de segurança da informação, revisões de conformidade, auditorias internas e externas dos sistemas de informação ou revisões de segurança física. Além disso, a instituição deve ter em consideração boas práticas, como revisões do código fonte, avaliações da vulnerabilidade, testes de penetração e exercícios realizados por uma equipa de segurança ofensiva externa (*Red Team*).

42. As instituições financeiras devem estabelecer e implementar uma estrutura de teste da segurança da informação que valide a robustez e a eficácia das suas medidas de segurança da informação e assegurar que esta estrutura tenha em consideração as ameaças e vulnerabilidades, identificadas através da monitorização das ameaças e do processo de avaliação dos riscos associados às TIC e à segurança.

43. A estrutura de teste deve assegurar que os testes:

    a) São efetuados por pessoal independente com conhecimentos, competências e experiência suficientes para testar medidas de segurança da informação e que não está envolvido no desenvolvimento das medidas de segurança da informação;
    b) Incluem análises de vulnerabilidade e testes de penetração (incluindo testes de penetração orientados por ameaças, quando necessário e adequado) proporcionais ao nível de risco identificado com os sistemas e processos empresariais.

44. As instituições financeiras devem realizar testes, de forma contínua e repetida, às medidas de segurança. Para todos os sistemas de TIC críticos (n.º 17), estes testes devem ser realizados pelo menos anualmente e, no caso dos prestadores de serviços de pagamento, farão parte da avaliação global dos riscos de segurança relacionados com os serviços de pagamento por si prestados, em conformidade com o artigo 95.º, n.º 2, da DSP2. Os sistemas não críticos devem ser testados regularmente recorrendo a uma abordagem baseada no risco, mas no mínimo a cada três anos.

45. As instituições financeiras devem assegurar que os testes às medidas de segurança sejam realizados no caso de alterações da infraestrutura, dos processos ou dos procedimentos, e se forem feitas alterações devido a incidentes operacionais ou de segurança de caráter severo, ou devido ao lançamento de aplicações críticas com ligação direta à Internet, novas ou significativamente alteradas.

46. As instituições financeiras devem monitorizar e avaliar os resultados dos testes de segurança e atualizar as suas medidas de segurança em conformidade, sem demora no caso dos sistemas de TIC críticos.

47. Para os prestadores de serviços de pagamento, a estrutura de teste deve abranger igualmente as medidas de segurança pertinentes para (1) terminais de pagamento e dispositivos utilizados para a prestação de serviços de pagamento, (2) terminais de pagamento e dispositivos utilizados para autenticar os utilizadores de serviços de pagamento (PSU) e (3) dispositivos e

programas informáticos fornecidos pelo prestador de serviços de pagamento ao utilizador de serviços de pagamento para gerar/receber um código de autenticação.

48. Com base nas ameaças de segurança verificadas e nas alterações efetuadas, devem ser realizados testes para incorporar cenários de potenciais ataques pertinentes e conhecidos.

1.4.7. Formação e sensibilização em matéria de segurança da informação

49. As instituições financeiras devem estabelecer um programa de formação, incluindo programas periódicos de sensibilização para a segurança, para todos os funcionários e contratantes, a fim de assegurar que estes possuam formação para desempenhar as suas funções e responsabilidades de forma coerente com as políticas e procedimentos de segurança pertinentes para reduzir o erro humano, o roubo, a fraude, a utilização indevida ou a perda e de forma a abordar os riscos relacionados com a segurança da informação. As instituições financeiras devem assegurar que o programa de formação proporcione formação a todos os membros do pessoal e contratantes pelo menos uma vez por ano.

1.5. Gestão de operações de TIC

50. As instituições financeiras devem gerir as suas operações de TIC com base em processos e procedimentos documentados e implementados (que, no caso dos prestadores de serviços de pagamento, incluem o documento relativo à política de segurança em conformidade com o artigo 5.º, n.º 1, alínea j), da DSP2) que são aprovados pelo órgão de administração. Este conjunto de documentos deve definir a forma como as instituições financeiras operam, monitorizar e controlar os seus sistemas e serviços de TIC, incluindo a documentação de operações de TIC críticas, devendo permitir às instituições financeiras manter um inventário atualizado dos ativos de TIC.

51. As instituições financeiras devem assegurar que o desempenho das suas operações de TIC esteja alinhado com os seus requisitos empresariais. As instituições financeiras devem manter e melhorar, quando possível, a eficiência das suas operações de TIC, incluindo, mas não exclusivamente, a necessidade de ter em consideração a forma de minimizar potenciais erros decorrentes da execução de tarefas manuais.

52. As instituições financeiras devem implementar procedimentos de registo e de monitorização de operações de TIC críticas para permitir a deteção, análise e correção de erros.

53. As instituições financeiras devem manter um inventário atualizado dos seus ativos de TIC (incluindo sistemas de TIC, dispositivos de rede, bases de dados, etc.). O inventário de ativos de TIC deve armazenar a configuração dos ativos de TIC e as ligações e interdependências entre os diferentes ativos de TIC, para permitir um processo adequado de configuração e gestão de alterações.

54. O inventário de ativos de TIC deve ser suficientemente pormenorizado para permitir a rápida identificação de um ativo de TIC, bem como da sua localização, classificação de segurança e propriedade. As interdependências entre ativos devem ser documentadas para ajudar na resposta a incidentes operacionais e de segurança, incluindo ciberataques.

55. As instituições financeiras devem monitorizar e gerir os ciclos de vida dos ativos de TIC, para garantir que estes continuem a cumprir e a apoiar os requisitos empresariais e de gestão dos riscos. As instituições financeiras devem monitorizar se os seus ativos de TIC são apoiados pelos seus fornecedores e promotores externos ou internos, e se todas as correções e atualizações pertinentes são aplicadas com base em processos documentados. Os riscos decorrentes de ativos de TIC desatualizados ou não apoiados devem ser avaliados e mitigados.

56. As instituições financeiras devem implementar processos de monitorização e de planeamento da capacidade e do desempenho para prevenir, detetar e responder atempadamente a importantes questões de desempenho dos sistemas de TIC e de escassez de capacidade em matéria de TIC.

57. As instituições financeiras devem definir e implementar procedimentos de segurança e de recuperação de dados e de sistemas de TIC, para garantir que possam ser recuperados conforme necessário. O âmbito e a frequência das cópias de segurança devem ser definidos em consonância com os requisitos de recuperação de negócio e a criticidade dos dados e dos sistemas de TIC, e avaliados de acordo com a avaliação dos riscos realizada. Os testes aos procedimentos de segurança e de recuperação devem ser realizados periodicamente.

58. As instituições financeiras devem garantir que as cópias de segurança dos sistemas de TIC e dos dados sejam armazenadas de forma segura e estejam suficientemente afastadas da localização primária, para que não estejam expostas aos mesmos riscos.

3.5.1 Gestão de problemas e incidentes em matéria de TIC

59. As instituições financeiras devem estabelecer e implementar um processo de gestão de problemas e incidentes, para monitorizar e registar incidentes operacionais e de segurança em matéria de TIC, e para permitir que as instituições financeiras continuem ou retomem, em tempo útil, áreas de negócio e processos críticos quando ocorrerem perturbações. As instituições financeiras devem determinar critérios e limiares adequados para classificar os eventos como incidentes operacionais ou de segurança, conforme estabelecido na secção «Definições» das presentes orientações, bem como indicadores de alerta precoce que devem servir de alerta para permitir a deteção precoce destes incidentes. Tais critérios e limiares, para os prestadores de serviços de pagamento, não prejudicam a classificação de incidentes de caráter severo em conformidade com o artigo 96.º da DSP2 e as Orientações sobre a comunicação de incidentes de caráter severo, ao abrigo da Diretiva (UE) 2015/2366 (EBA/GL/2017/10).

60. Para minimizar o impacto de eventos adversos e permitir uma recuperação atempada, as instituições financeiras devem estabelecer processos e estruturas organizacionais adequados, para assegurar uma monitorização, um tratamento e um acompanhamento coerentes e integrados dos incidentes operacionais e de segurança e para garantir que as principais causas sejam identificadas e eliminadas, a fim de evitar a repetição de incidentes. O processo de gestão de problemas e incidentes deve estabelecer:

    a) Os procedimentos para identificar, detetar, registar, categorizar e classificar os incidentes de acordo com uma prioridade, com base na criticidade para o negócio;

b) As funções e responsabilidades para diferentes cenários de incidentes (por exemplo, erros, mau funcionamento, ciberataques);
c) Os procedimentos de gestão de problemas para identificar, analisar e resolver a principal causa subjacente a um ou mais incidentes — uma instituição financeira deve analisar os incidentes operacionais ou de segurança suscetíveis de a afetar e que tenham sido identificados ou que tenham ocorrido dentro e/ou fora da organização, e deve ter em consideração as principais lições aprendidas destas análises e atualizar as medidas de segurança em conformidade;
d) Planos de comunicação interna eficazes, incluindo procedimentos por etapas em caso de incidentes e de notificação de incidentes — abrangendo igualmente as reclamações de clientes relacionadas com a segurança — para garantir que:
    i) os incidentes com um impacto adverso potencialmente elevado nos sistemas e serviços de TIC críticos sejam comunicados à gestão de topo pertinente e à gestão de topo em matéria de TIC;
    ii) o órgão de administração seja informado numa base *ad hoc* em caso de incidentes significativos e, pelo menos, informado do impacto, da resposta e dos controlos adicionais a definir em resultado dos incidentes.
e) Procedimentos de resposta a incidentes para atenuar os impactos relacionados com estes e para assegurar que o serviço se torne operacional e seguro em tempo útil;
f) Planos de comunicação externa específicos para áreas de negócio e processos críticos, a fim de:
    i) colaborar com as partes interessadas pertinentes para responder eficazmente ao incidente e recuperar do mesmo;
    ii) fornecer informações oportunas a partes externas (por exemplo, clientes, outros participantes no mercado, a autoridade de supervisão), conforme adequado e em consonância com um regulamento aplicável.

1.6. Gestão de alterações e de projetos de TIC

1.6.1. Gestão de projetos de TIC

61. Uma instituição financeira deve implementar um programa e/ou um processo de governação de projetos que defina funções, responsabilidades e obrigações de prestação de contas, para apoiar eficazmente a implementação da estratégia em matéria de TIC.

62. Uma instituição financeira deve monitorizar e mitigar adequadamente os riscos decorrentes da sua carteira de projetos de TIC (gestão de programas), tendo igualmente em consideração os riscos que podem resultar de interdependências entre diferentes projetos e de dependências de múltiplos projetos em relação aos mesmos recursos e/ou conhecimentos especializados.

63. Uma instituição financeira deve estabelecer e implementar uma política de gestão de projetos de TIC que inclua, no mínimo:

    a) Os objetivos dos projetos;
    b) As funções e responsabilidades;

c) Uma avaliação dos riscos dos projetos;
d) Um plano, um calendário e as etapas dos projetos;
e) Os principais marcos;
f) Os requisitos de gestão de alterações.

64. A política de gestão de projetos de TIC deve assegurar que os requisitos de segurança da informação sejam analisados e aprovados por uma função que seja independente da função de desenvolvimento.

65. Uma instituição financeira deve assegurar que todas as áreas afetadas por um projeto de TIC estejam representadas na equipa do projeto e que a equipa do projeto possua os conhecimentos necessários para garantir uma implementação segura e bem-sucedida do projeto.

66. O estabelecimento e o progresso dos projetos de TIC e os riscos que lhe estão associados devem ser comunicados ao órgão de administração, individualmente ou de forma agregada, dependendo da importância e dimensão dos projetos de TIC, regularmente e numa base *ad hoc*, conforme adequado. As instituições financeiras devem incluir os riscos associados ao projeto no seu quadro de gestão dos riscos.

1.6.2. Aquisição e desenvolvimento de sistemas de TIC

67. As instituições financeiras devem desenvolver e implementar um processo que regule a aquisição, o desenvolvimento e a manutenção de sistemas de TIC. Este processo deve ser concebido utilizando uma abordagem baseada no risco.

68. Uma instituição financeira deve assegurar que, antes de qualquer aquisição ou desenvolvimento de sistemas de TIC, os requisitos funcionais e não funcionais (incluindo os requisitos de segurança da informação) sejam claramente definidos e aprovados pelas áreas de gestão de negócio pertinentes.

69. Uma instituição financeira deve assegurar que sejam implementadas medidas para reduzir o risco de alteração não intencional ou de manipulação intencional dos sistemas de TIC, durante o desenvolvimento e a implementação no ambiente de produção.

70. As instituições financeiras devem dispor de uma metodologia para testar e aprovar os sistemas de TIC antes da sua primeira utilização. Esta metodologia deve ter em consideração a criticidade dos ativos e processos empresariais. Os testes devem assegurar que os novos sistemas de TIC têm o desempenho pretendido. Devem igualmente utilizar ambientes de teste que reflitam adequadamente o ambiente de produção.

71. As instituições financeiras devem testar os sistemas de TIC, serviços de TIC e medidas de segurança da informação para identificar potenciais fragilidades, violações e incidentes em matéria de segurança.

72. Uma instituição financeira deve implementar ambientes de TIC distintos, para assegurar a segregação adequada de funções e para atenuar o impacto de alterações não verificadas nos sistemas de produção. Especificamente, uma instituição financeira deve assegurar a segregação dos ambientes de produção em relação aos ambientes de desenvolvimento, de

teste e de outros ambientes de não produção. Uma instituição financeira deve assegurar a integridade e a confidencialidade dos dados de produção em ambientes de não produção. O acesso aos dados de produção é limitado a utilizadores autorizados.

73. As instituições financeiras devem implementar medidas para proteger a integridade dos códigos fonte dos sistemas de TIC, que são desenvolvidos internamente. Devem igualmente documentar exaustivamente o desenvolvimento, a implementação, o funcionamento e/ou a configuração dos sistemas de TIC para reduzir qualquer dependência desnecessária de peritos na matéria. A documentação do sistema de TIC deve conter, quando aplicável, pelo menos a documentação do utilizador, a documentação técnica do sistema e os procedimentos operacionais.

74. Os processos de aquisição e desenvolvimento de sistemas de TIC de uma instituição financeira devem igualmente aplicar-se a sistemas de TIC desenvolvidos ou geridos pelos utilizadores finais da área de negócio, fora da organização de TIC (por exemplo, aplicações informáticas para utilizadores finais), utilizando uma abordagem baseada no risco. A instituição financeira deve manter um registo destas aplicações que apoiam áreas de negócio ou processos críticos.

1.6.3. Gestão de alterações em matéria de TIC

75. As instituições financeiras devem estabelecer e implementar um processo de gestão de alterações em matéria de TIC, para assegurar que todas as alterações introduzidas nos sistemas de TIC sejam registadas, testadas, avaliadas, aprovadas, implementadas e verificadas de forma controlada. As instituições financeiras devem lidar com as alterações durante situações de emergência (isto é, alterações que devem ser introduzidas o mais rapidamente possível) seguindo procedimentos que proporcionem salvaguardas adequadas.

76. As instituições financeiras devem averiguar se as alterações do ambiente operacional existente, influenciam as medidas de segurança em vigor ou exigem a adoção de medidas adicionais para reduzir os riscos envolvidos. Estas alterações devem estar em conformidade com o processo de gestão de alterações formal das instituições financeiras.

1.7. Gestão da continuidade da atividade

77. As instituições financeiras devem estabelecer um processo sólido de gestão da continuidade de negócio para maximizar as suas capacidades de prestação de serviços numa base contínua e para limitar as perdas na eventualidade de uma perturbação grave da sua atividade, em consonância com o artigo 85.º, n.º 2, da Diretiva 2013/36/UE e com o título VI das Orientações da EBA sobre governo interno (EBA/GL/2017/11).

1.7.1. Análise de impacto na atividade

78. Como parte de uma gestão sólida da continuidade de negócio, as instituições financeiras devem realizar análises de impacto no negócio (BIA), analisando a sua exposição a perturbações graves no negócio e avaliando os seus potenciais impactos (nomeadamente na confidencialidade, integridade e disponibilidade), quantitativa e qualitativamente, recorrendo a dados internos

e/ou externos (por exemplo, dados de prestadores terceiros pertinentes para um processo de negócio ou dados publicamente disponíveis que possam ser pertinentes para a análise de impacto no negócio) e à análise de cenários. A análise de impacto no negócio deve igualmente ter em consideração a criticidade das áreas de negócio, dos processos de apoio e dos ativos de informação e de terceiros identificados e classificados, bem como as suas interdependências, em conformidade com a secção 1.3.3.

79. As instituições financeiras devem assegurar que os seus sistemas e serviços de TIC sejam concebidos e alinhados com as suas análises de impacto no negócio, por exemplo, através da redundância de determinados componentes críticos, para evitar perturbações causadas por eventos que tenham impacto nesses componentes.

1.7.2. Planeamento da continuidade de negócio

80. Com base nas suas análises de impacto no negócio, as instituições financeiras devem elaborar planos para assegurar a continuidade de negócio (planos de continuidade de negócio, PCNs), os quais devem ser documentados e aprovados pelos seus órgãos de administração. Os planos devem ter especificamente em consideração os riscos que possam ter um impacto negativo nos sistemas e serviços de TIC. Os planos devem apoiar objetivos para proteger e, se necessário, restabelecer a confidencialidade, integridade e disponibilidade das suas áreas de negócio, apoiando processos e ativos de informação. As instituições financeiras devem coordenar-se com as partes interessadas internas e externas pertinentes, se for caso disso, durante a elaboração destes planos.

81. As instituições financeiras devem criar PCNs para garantir que conseguem reagir adequadamente a potenciais cenários de falha e que são capazes de recuperar as operações das suas atividades comerciais críticas, após perturbações, dentro de um objetivo de tempo de recuperação (o intervalo de tempo máximo dentro do qual um sistema ou processo deve ser restaurado após um incidente) e de um objetivo de ponto de recuperação (o intervalo de tempo máximo durante o qual é aceitável que os dados se percam em caso de incidente). Em casos de perturbações graves da atividade que desencadeiem planos específicos de continuidade de negócio, as instituições financeiras devem atribuir prioridade a ações de continuidade de negócio recorrendo a uma abordagem baseada no risco, que pode basear-se nas avaliações dos riscos realizadas ao abrigo da secção 1.3.3. Para os prestadores de serviços de pagamento, tal pode incluir, por exemplo, a facilitação do tratamento de operações críticas, enquanto prosseguem os esforços de correção.

82. Uma instituição financeira deve considerar um conjunto de diferentes cenários no seu PCN, incluindo os mais extremos mas plausíveis, aos quais pode estar exposta, incluindo um cenário de ciberataque, e deve avaliar o potencial impacto que tais cenários podem ter. Com base nestes cenários, uma instituição financeira deve descrever a forma como a continuidade dos sistemas e serviços de TIC, bem como a segurança da informação da instituição financeira, são asseguradas.

1.7.3. Planos de recuperação e resposta

83. Com base nas suas análises de impacto na atividade (n.º 78) e nos cenários plausíveis (n.º 82), as instituições financeiras devem elaborar planos de recuperação e resposta. Estes planos devem especificar as condições que podem conduzir à rápida ativação dos planos, e as ações que devem ser tomadas para assegurar a disponibilidade, continuidade e recuperação, pelo menos, dos sistemas e serviços de TIC críticos das instituições financeiras. Os planos de recuperação e resposta devem visar o cumprimento dos objetivos de recuperação das operações das instituições financeiras.

84. Os planos de recuperação e resposta devem ter em consideração as opções de recuperação a curto e a longo prazo. Os planos devem:

    a) Centrar-se na recuperação das operações das áreas de negócio críticas, processos de apoio, ativos de informação e respetivas interdependências para evitar efeitos adversos no funcionamento das instituições financeiras e no sistema financeiro, incluindo nos sistemas de pagamento e nos utilizadores de serviços de pagamento, bem como para assegurar a execução de operações de pagamento pendentes;
    b) Ser documentados e disponibilizados às unidades de negócio e de apoio e facilmente acessíveis em caso de emergência;
    c) Ser atualizados em consonância com as lições aprendidas dos incidentes, testes, novos riscos identificados e ameaças, bem como das alterações introduzidas nos objetivos de recuperação e prioridades.

85. Os planos devem igualmente ter em consideração opções alternativas em que a recuperação possa não ser viável a curto prazo devido a custos, riscos, logística ou circunstâncias imprevistas.

86. Além disso, como parte dos planos de recuperação e resposta, uma instituição financeira deve ter em consideração e implementar medidas de continuidade para atenuar as falhas de prestadores terceiros, que são de importância fundamental para a continuidade dos serviços de TIC de uma instituição financeira (em consonância com as disposições das Orientações da EBA relativas à subcontratação (EBA/GL/2019/02) relativas aos PCNs).

1.7.4. Teste dos planos

87. As instituições financeiras devem testar periodicamente os seus PCNs. Em particular, devem assegurar que os PCNs das suas áreas de negócio críticas, processos de suporte, ativos de informação e respetivas interdependências (incluindo os fornecidos por terceiros, quando aplicável) sejam testados pelo menos uma vez por ano, em conformidade com o n.º 89.

88. Os PCNs devem ser atualizados pelo menos uma vez por ano, com base nos resultados dos testes, nas informações sobre ameaças atuais e nas lições aprendidas de eventos anteriores. Eventuais alterações dos objetivos de recuperação (incluindo objetivos de tempo de recuperação e objetivos de ponto de recuperação) e/ou alterações das áreas de negócio, processos de suporte e ativos de informação devem igualmente ser tidas em consideração, quando pertinente, como base para a atualização dos PCNs.

89. Os testes das instituições financeiras aos seus PCNs devem demonstrar que estas instituições são capazes de manter a viabilidade das suas atividades até ao restabelecimento das operações críticas. Em particular, devem:

    a) Incluir testes de um conjunto adequado de cenários graves, mas plausíveis, incluindo os tidos em consideração para o desenvolvimento dos PCNs (bem como testes dos serviços prestados por terceiros, quando aplicável); tal deve incluir a mudança de áreas de negócio críticas, processos de apoio e ativos de informação para o ambiente de recuperação, na sequência de catástrofes, e a demonstração de que os mesmos podem ser geridos desta forma durante um período suficientemente representativo e de que o funcionamento normal pode ser restaurado posteriormente;
    b) Ser concebidos para desafiar os pressupostos sobre os quais se baseiam os PCNs, incluindo acordos de governo e planos de comunicação de crises; e
    c) Incluir procedimentos para verificar a capacidade do seu pessoal e contratantes, sistemas de TIC e serviços de TIC para responder adequadamente aos cenários definidos no n.º 89, alínea a).

90. Os resultados dos testes devem ser documentados e quaisquer deficiências identificadas resultantes dos testes devem ser analisadas, abordadas e comunicadas ao órgão de administração.

1.7.5. Comunicação de crises

91. No caso de uma interrupção ou emergência, e durante a implementação dos PCNs, as instituições financeiras devem assegurar-se de que dispõem de medidas eficazes de comunicação de crises para que todas as partes interessadas pertinentes, internas e externas, incluindo as autoridades competentes quando tal for exigido por regulamentos nacionais, e também os prestadores de serviços pertinentes (prestadores de serviços subcontratados, entidades pertencentes ao mesmo grupo ou prestadores de serviços terceiros), sejam informados de forma atempada e adequada.

1.8. Gestão da relação com os utilizadores de serviços de pagamento

92. Os prestadores de serviços de pagamento devem estabelecer e implementar processos para sensibilizar os utilizadores de serviços de pagamento para os riscos de segurança associados aos serviços de pagamento através da prestação de assistência e orientação aos utilizadores de serviços de pagamento.

93. A assistência e a orientação oferecidas aos utilizadores de serviços de pagamento devem ser atualizadas, em função de novas ameaças e vulnerabilidades, e as alterações devem ser comunicadas aos utilizadores de serviços de pagamento.

94. Quando a funcionalidade do produto o permitir, os prestadores de serviços de pagamento devem permitir que os utilizadores de serviços de pagamento desativem funcionalidades de pagamento específicas, relacionadas com os serviços de pagamento prestados.

95. Quando, em conformidade com o artigo 68.º, n.º 1, da Diretiva (UE) 2015/2366, um prestador de serviços de pagamento tiver acordado com o ordenante limites de despesa para as operações de pagamento executadas, através de instrumentos de pagamento específicos, o prestador de serviços de pagamento deve dar ao ordenante a opção de ajustar tais limites até ao limite máximo acordado.

96. Os prestadores de serviços de pagamento devem dar aos utilizadores de serviços de pagamento a opção de receber alertas sobre tentativas iniciadas e/ou falhadas para iniciar operações de pagamento, permitindo assim detetar a utilização fraudulenta ou maliciosa das suas contas.

97. Os prestadores de serviços de pagamento devem manter os utilizadores de serviços de pagamento informados quanto a atualizações nos procedimentos de segurança, que afetam os utilizadores de serviços de pagamento em matéria de prestação de serviços de pagamento.

98. Os prestadores de serviços de pagamento devem prestar assistência aos utilizadores de serviços de pagamento em todas as questões, pedidos de apoio e notificações de anomalias ou de problemas relacionados com a segurança dos serviços de pagamento. Os prestadores de serviços de pagamento devem ser devidamente informados sobre a forma como podem obter esta assistência.