EBA/GL/2017/17

12/01/2018

Orientações

sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE) 2015/2366 (PSD2)

1. 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 referido Regulamento, 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 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 confirmam à EBA se dão ou tencionam dar cumprimento às presentes Orientações, ou, caso contrário, indicam as razões para o não cumprimento até 12.03.2018. 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 para o endereço compliance@eba.europa.eu com a referência «EBA/GL/2017/11». As notificações devem ser apresentadas por pessoas devidamente autorizadas para o efeito pelas 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, 15.12.2010, p.12).

2. Objeto, âmbito de aplicação e definições

Objeto e âmbito de aplicação

5. As presentes Orientações derivam do mandato conferido à EBA, no âmbito do n.º 3 do artigo 95.º da Diretiva (UE) 2015/2366[2] (DSP2).

6. As presentes Orientações especificam os requisitos para o estabelecimento, a implementação e a monitorização das medidas de segurança que os prestadores de serviços de pagamento devem aplicar, em conformidade com o n.º 1 do artigo 95.º da DSP2, para gerir os riscos operacionais e de segurança relacionados com os serviços de pagamento por si prestados.

Destinatários

7. Estas Orientações são dirigidas aos prestadores de serviços de pagamento conforme definido no n.º 11 do artigo 4.º da DSP2, e conforme referido na definição de «instituições financeiras» do n.º 1 do artigo 4.º do Regulamento (UE) n.º 1093/2010, e às autoridades competentes, de acordo com a alínea i) do n.º 2 do artigo 4.º do referido Regulamento com referência à Diretiva 2007/64/CE[3] revogada (atualmente Diretiva (UE) 2015/2366[4]).

Definições

8. Salvo especificação em contrário, os termos utilizados e definidos na DSP2 têm o mesmo significado nas presentes Orientações. Adicionalmente, para efeitos das presentes Orientações, aplicam-se as seguintes definições:

Órgão de administração	(a) Para os prestadores de serviços de pagamento que são instituições de crédito, este termo tem o mesmo significado

[2] Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE, 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE (JO L 337, de 23.12.2015, p. 35).

[3] Diretiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro de 2007, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE e revoga a Diretiva 97/5/CE (JO L 319, de 5.12.2007, p. 1).

[4] Nos termos do segundo parágrafo do artigo 114.º da Diretiva (UE) 2015/2366, qualquer referência à Diretiva 2007/64/CE revogada deve ser interpretada como uma referência à Diretiva (UE) 2015/2366 e deve ser lida de acordo com o quadro de correspondência constante do anexo II da Diretiva (UE) 2015/2366.

	que a definição constante no ponto 7 do n.º 1 do artigo 3.º da Diretiva 2013/36/UE[5]; (b) Para os prestadores de serviços de pagamento que são instituições de pagamento ou instituições de moeda eletrónica, este termo aplica-se aos diretores ou pessoas responsáveis pela gestão do prestador de serviços de pagamento e, quando relevante, às pessoas responsáveis pela gestão das atividades de serviços de pagamento do prestador de serviços de pagamento; (c) Para os prestadores de serviços de pagamento referidos nas alíneas c), e) e f) do n.º 1 do artigo 1.º 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 evento único ou uma série de eventos conexos e não previstos pelo prestador de serviços de pagamento, que tem, ou poderá vir a ter, um impacto negativo na integridade, disponibilidade, confidencialidade, autenticidade e/ou continuidade dos serviços relacionados com pagamentos.
Direção de topo	(a) Para os prestadores de serviços de pagamento que são instituições de crédito, este termo tem o mesmo significado que a definição constante no ponto 9 do n.º 1 do artigo 3.º da Diretiva 2013/36/UE; (b) Para os prestadores de serviços de pagamento que são 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 são responsáveis perante o Órgão de administração pela gestão diária do prestador de serviços de pagamento; (c) Para os prestadores de serviços de pagamento referidos nas alíneas c), e) e f) do n.º 1 do artigo 1.º da Diretiva (UE) 2015/2366, este termo tem o significado que lhe é conferido pelo direito nacional ou comunitário aplicável.
Risco de segurança	O risco resultante de uma inadequação ou deficiência de procedimentos internos ou de eventos externos que tenham ou possam vir a ter um impacto adverso na disponibilidade, integridade, confidencialidade dos sistemas de tecnologias de informação e de comunicação e/ou informação utilizada para a prestação de serviços de pagamento. Inclui o risco proveniente de ciberataques ou de segurança física inadequada.
Apetência pelo risco	O nível agregado e os tipos de risco que uma instituição está disposta a assumir no contexto da sua capacidade e de acordo

[5] Diretiva 2013/36/UE do Parlamento Europeu e do Conselho relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176, de 27.6.2013, p. 338).

	com o seu modelo de negócio, para atingir os seus objetivos estratégicos.

3. Execução

Data de aplicação

9. As presentes Orientações são aplicáveis a partir de 13 de janeiro de 2018.

4. Orientações

Orientação 1: Princípio geral

1.1 Todos os prestadores de serviços de pagamento devem cumprir com todas as disposições estabelecidas nas presentes Orientações. O nível de detalhe deve ser proporcional à dimensão do prestador de serviços de pagamento, bem como à natureza, ao âmbito de aplicação, à complexidade e aos riscos dos serviços específicos que o prestador de serviços de pagamento presta ou pretende prestar.

Orientação 2: Governação

Quadro de gestão dos riscos operacionais e de segurança

2.1 Os prestadores de serviços de pagamento devem estabelecer um quadro de gestão dos riscos operacionais e de segurança (doravante «quadro de gestão de riscos»), que deve ser aprovado e revisto, pelo menos uma vez por ano, pelo Órgão de administração e, quando relevante, pela Direção de topo. Este quadro deve focar-se em medidas de segurança para mitigar os riscos operacionais e de segurança e deve estar totalmente integrado nos processos de gestão de risco globais do prestador de serviços de pagamento.

2.2 O quadro de gestão de riscos deve:

a) incluir um documento de política de segurança abrangente conforme referido na alínea j) do n.º 1 do artigo 5.º da Diretiva (UE) 2015/2366;

b) ser consistente com a apetência pelo risco do prestador de serviços de pagamento;

c) definir e atribuir as funções essenciais e responsabilidades, bem como as respetivas linhas de reporte, necessários para fazer cumprir as medidas de segurança e gerir os riscos de operacionais e de segurança;

d) estabelecer os procedimentos e sistemas necessários para identificar, medir, monitorizar e gerir o conjunto de riscos decorrentes das atividades relacionadas com pagamentos do prestador de serviços de pagamento e aos quais está exposto, incluindo os planos de continuidade de negócio.

2.3 Os prestadores de serviços de pagamento devem assegurar que o quadro de gestão de riscos se encontra devidamente documentado e atualizado com as «lições aprendidas» durante a sua implementação e monitorização.

2.4 Os prestadores de serviços de pagamento devem assegurar que, antes de uma alteração importante ao nível de infraestruturas, processos ou procedimentos e após cada incidente operacional ou de segurança de carácter severo que afete a segurança dos serviços de pagamento

que prestam, é efetuada uma revisão, sem demora indevida, para identificar as alterações ou melhorias necessárias ao quadro de gestão de riscos.

Gestão de risco e modelos de controlo

2.5 Os prestadores de serviços de pagamento devem estabelecer três linhas de defesa efetivas, ou um modelo de controlo e gestão de riscos interno equivalente, para identificar e gerir riscos operacionais e de segurança. Os prestadores de serviços de pagamento devem assegurar que o modelo de controlo interno acima mencionado possui suficiente autoridade, independência, recursos e linhas de reporte direto para o Órgão de administração e, quando relevante, para a Direção de topo.

2.6 As medidas de segurança estabelecidas nas presentes Orientações devem ser auditadas por auditores especializados em tecnologias de informação de segurança e pagamentos e operacionalmente independentes, a nível interno ou externo, do prestador de serviços de pagamento. A periodicidade e o foco destas auditorias deve ter em conta os respetivos riscos de segurança.

Externalização

2.7 Os prestadores de serviços de pagamento devem assegurar a eficácia das medidas de segurança estabelecidas nas presentes Orientações quando as funções operacionais dos serviços de pagamento, inclusive os sistemas de tecnologias de informação, forem externalizados.

2.8 Os prestadores de serviços de pagamento devem assegurar que os objetivos de segurança, medidas e metas de desempenho são definidos, de forma adequada e proporcional, nos contratos e acordos de nível de serviço celebrados com os prestadores a quem externalizaram essas funções. Os prestadores de serviços de pagamento devem monitorizar e assegurar o nível de conformidade de tais prestadores com os objetivos de segurança, medidas e metas de desempenho definidos.

Orientação 3: Avaliação de risco

Identificação de áreas, processos e ativos

3.1 Os prestadores de serviços de pagamento devem identificar, estabelecer e atualizar regularmente um inventário das suas áreas de negócio, funções essenciais e processos de suporte no sentido de mapear a importância de cada área, função e processo de suporte e as suas interdependências relativamente aos riscos operacionais e de segurança.

3.2 Os prestadores de serviços de pagamento devem identificar, estabelecer e atualizar regularmente um inventário dos ativos de informação, como os sistemas de tecnologias de informação e comunicação, as suas configurações, outras infraestruturas, bem como as interligações com outros sistemas internos e externos de forma a ser capaz de gerir os ativos que suportam as suas áreas de negócio e processos críticos.

Classificação de áreas, processos e ativos

3.3 Os prestadores de serviços de pagamento devem classificar as referidas áreas de negócio, processos de suporte e ativos de informação em termos de criticidade.

Avaliações de risco de áreas, processos e ativos

3.4 Os prestadores de serviços de pagamento devem assegurar que monitorizam, de forma contínua, as ameaças e vulnerabilidades e que reveem periodicamente os cenários de risco que afetam as suas áreas de negócio, processos críticos e ativos de informação. Como parte da obrigação de realizar e disponibilizar às autoridades competentes uma avaliação de risco completa e atualizada sobre os riscos operacionais e de segurança relacionados com os serviços de pagamento que prestam e sobre a adequação das medidas de mitigação e mecanismos de controlo implementados para responder a esses riscos, conforme estabelecido no n.º 2 do artigo 95.º da Diretiva (UE) 2015/2366, os prestadores de serviços de pagamento devem efetuar e documentar avaliações de risco, pelo menos anualmente ou em intervalos mais curtos quando determinado pela autoridade competente, às áreas, processos e ativos de informação que identificaram e classificaram de forma a identificar e avaliar os principais riscos operacionais e de segurança. Estas avaliações de risco devem também ser realizadas antes de efetuada qualquer alteração importante ao nível de infraestruturas, processos ou procedimentos que afetem a segurança dos serviços de pagamento.

3.5 Com base nas avaliações de risco, os prestadores de serviços de pagamento devem averiguar se, e em que medida, são necessárias alterações às medidas de segurança existentes, tecnologias utilizadas e procedimentos ou serviços de pagamento oferecidos. Os prestadores de serviços de pagamento devem ter em consideração o tempo necessário para implementar estas alterações e para aplicar medidas de segurança provisórias adequadas de forma a minimizar incidentes operacionais ou de segurança, fraudes e potenciais efeitos disruptivos na prestação de serviços de pagamento.

Orientação 4: Proteção

4.1 Os prestadores de serviços de pagamento devem estabelecer e implementar medidas de segurança preventivas contra riscos operacionais e de segurança identificados. Estas medidas devem assegurar um nível adequado de segurança de acordo com os riscos identificados.

4.2 Os prestadores de serviços de pagamento devem estabelecer e implementar uma abordagem de «defesa em profundidade» através da implementação de controlos com vários níveis que abranjam pessoas, processos e tecnologia, em que cada nível constitui uma rede de segurança para os níveis precedentes. A defesa em profundidade deve basear-se na definição de mais do que um controlo para a cobertura do mesmo risco, tal como o princípio dos «quatro olhos», a autenticação de dois fatores, a segmentação de rede e as múltiplas barreiras de proteção (*firewalls)*.

4.3 Os prestadores de serviços de pagamento devem assegurar a confidencialidade, integridade e disponibilidade dos seus ativos e recursos críticos, quer sejam físicos ou lógicos, e dos dados de pagamento sensíveis dos seus utilizadores de serviços de pagamento, independentemente de estarem armazenados, em trânsito ou em utilização. Se estes dados incluírem dados pessoais, as medidas devem ser implementadas em conformidade com o Regulamento (UE) 2016/679[6] ou com o Regulamento (CE) 45/2001[7], se aplicável.

4.4 Os prestadores de serviços de pagamento devem averiguar, numa base contínua, se as alterações ao ambiente operacional existente influenciam as medidas de segurança existentes ou exigem a adoção de novas medidas para mitigar o risco envolvido. Estas alterações devem fazer parte do processo de gestão de alterações formal do prestador de serviços de pagamento, o qual deve assegurar que as alterações são devidamente planeadas, testadas, documentadas e autorizadas. Com base nas ameaças de segurança verificadas e nas alterações efetuadas, devem ser realizados testes para incorporar cenários de potenciais ataques relevantes e conhecidos.

4.5 Na conceção, desenvolvimento e prestação de serviços de pagamento, os prestadores de serviços de pagamento devem assegurar que são aplicados os princípios de segregação de funções e de «privilégios mínimos». Os prestadores de serviços de pagamento devem prestar especial atenção à segregação dos ambientes de tecnologias de informação, em particular aos ambientes de desenvolvimento, teste e produção.

Integridade e confidencialidade dos dados e sistemas

4.6 Na conceção, desenvolvimento e prestação de serviços de pagamento, os prestadores de serviços de pagamento devem assegurar que a recolha, encaminhamento, processamento, armazenamento e/ou arquivo e visualização de dados de pagamento sensíveis do utilizador de serviços de pagamento são adequados, relevantes e limitados ao estritamente necessário para a prestação dos respetivos serviços de pagamento.

4.7 Os prestadores de serviços de pagamento devem verificar regularmente se o *software* utilizado para a prestação de serviços de pagamento, incluindo o *software* relacionado com o pagamento dos utilizadores, está atualizado e se foram implementadas as correções críticas de segurança. Os prestadores de serviços de pagamento devem assegurar que os mecanismos de verificação de integridade estão implementados de forma a verificar a integridade de *software*, *firmware* e da informação relativamente aos seus serviços de pagamento.

[6] Regulamento (UE) do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119, de 4.5.2016, p. 1).

[7] Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8, de 12.1.2001, p. 1).

Segurança física

4.8 Os prestadores de serviços de pagamento devem ter implementadas adequadas medidas de segurança física, em particular para proteger os dados de pagamento sensíveis dos utilizadores de serviços de pagamento, bem como os sistemas de tecnologias de informação e de comunicação utilizados para prestar serviços de pagamento.

Controlo de acesso

4.9 O acesso físico e lógico aos sistemas de tecnologias de informação e de comunicação deve apenas ser permitido a pessoas autorizadas. A autorização deve ser atribuída de acordo com as tarefas e responsabilidades do pessoal, limitada a pessoas que são adequadamente formadas e controladas. Os prestadores de serviços de pagamento devem instituir controlos que restrinjam de forma fiável o acesso a estes sistemas a quem cumpra os respetivos requisitos de negócio. O acesso eletrónico através de aplicações a dados e sistemas deve ser limitado ao mínimo necessário para prestar o respetivo serviço.

4.10 Os prestadores de serviços de pagamento devem instituir controlos reforçados sobre o acesso privilegiado ao sistema, através de limitação restrita e supervisão atenta ao pessoal com elevados direitos de acesso ao sistema. Devem ser implementados controlos como o acesso baseado em funções, o registo e revisão das atividades efetuadas nos sistemas pelos utilizadores privilegiados, a autenticação forte e a monitorização de anomalias. Os prestadores de serviços de pagamento devem gerir os direitos de acesso aos ativos de informação e aos seus sistemas de suporte com base na "necessidade de conhecer". Os direitos de acesso devem ser revistos periodicamente.

4.11 Os registos de acesso devem ser mantidos durante um período proporcional à criticidade das áreas de negócio, processos de suporte e ativos de informação identificados, em conformidade com as Orientações 3.1 e 3.2, sem prejuízo dos requisitos de retenção estabelecidos no direito nacional ou comunitário. Os prestadores de serviços de pagamento devem utilizar esta informação para facilitar a identificação e investigação de atividades anómalas que tenham sido detetadas durante a prestação de serviços de pagamento.

4.12 Para assegurar uma comunicação segura e reduzir o risco, deve ser apenas concedido o acesso remoto administrativo aos componentes críticos de tecnologias de informação e de comunicação com base na "necessidade de conhecer" e quando são utilizadas soluções de autenticação forte.

4.13 O funcionamento dos produtos, ferramentas e procedimentos relacionados com os processos de controlo de acesso devem proteger estes processos de serem comprometidos ou contornados. Tal inclui o registo, entrega, revogação e cancelamento dos respetivos produtos, ferramentas e procedimentos.

Orientação 5: Deteção

Contínua monitorização e deteção

5.1 Os prestadores de serviços de pagamento devem estabelecer e implementar processos e recursos para monitorizar, de forma contínua, as áreas de negócio, os processos de suporte e os ativos de informação, de forma a detetar atividades anómalas na prestação de serviços de pagamento. Como parte desta monitorização contínua, os prestadores de serviços de pagamento devem ter implementados adequados e eficazes recursos para detetar intrusão física ou lógica, bem como violações de confidencialidade, integridade e disponibilidade dos ativos de informação utilizados na prestação de serviços de pagamento.

5.2 Os processos de monitorização e deteção contínuos devem abranger:

a) fatores internos e externos relevantes, incluindo as áreas administrativas de negócio e de tecnologias de informação e de comunicação;

b) transações para detetar o uso indevido de acesso por parte de prestadores de serviços ou outras entidades; e

c) potenciais ameaças internas e externas.

5.3 Os prestadores de serviços de pagamento devem implementar medidas de deteção para identificar possíveis fugas de informação, programação maliciosa e outras ameaças de segurança, e vulnerabilidades de *software* e *hardware* publicamente conhecidas, e verificar a existência de novas atualizações de segurança relevantes.

Monitorização e comunicação de incidentes operacionais ou de segurança

5.4 Os prestadores de serviços de pagamento devem determinar adequados critérios e limites para classificar um evento como um incidente operacional ou de segurança, conforme estabelecido na secção «Definições» das presentes Orientações, bem como indicadores de alerta prévio que permitam ao prestador de serviços de pagamento ser capaz de detetar atempadamente incidentes operacionais ou de segurança.

5.5 Os prestadores de serviços de pagamento devem estabelecer adequados processos e estruturas organizacionais para assegurar consistência e integração na forma de monitorização, tratamento e acompanhamento dos incidentes operacionais ou de segurança.

5.6 Os prestadores de serviços de pagamento devem estabelecer um procedimento de comunicação dos incidentes operacionais ou de segurança, bem como das reclamações de clientes relacionadas com segurança, à respetiva Direção de topo.

Orientação 6: Continuidade de negócio

6.1 Os prestadores de serviços de pagamento devem estabelecer uma sólida gestão da continuidade de negócio para maximizar, de forma permanente, a sua capacidade de prestar serviços de pagamento e para limitar as perdas em caso de perturbação grave do negócio.

6.2 A fim de estabelecer uma sólida gestão da continuidade de negócio, os prestadores de serviços de pagamento devem analisar cuidadosamente a sua exposição a perturbações graves do negócio e avaliar, quantitativa e qualitativamente, o seu potencial impacto, utilizando dados internos e/ou externos e a análise de cenários. Para as áreas, processos, sistemas, transações e interdependências identificados e classificados como críticos, em conformidade com as Orientações 3.1 a 3.3, os prestadores de serviços de pagamento devem prioritizar ações de continuidade de negócio que sigam uma abordagem orientada para o risco, a qual se pode basear nas avaliações de risco realizadas no âmbito da Orientação 3. Dependendo do modelo de negócio do prestador de serviços de pagamento, este pode, por exemplo, facilitar o processamento posterior de transações críticas, enquanto os esforços de recuperação continuam.

6.3 Com base na análise realizada no âmbito da Orientação 6.2, um prestador de serviços de pagamento deve pôr em prática:

a) Planos de continuidade de negócio para assegurar que é capaz de reagir adequadamente a emergências e de manter as suas atividades de negócio críticas; e

b) Medidas de mitigação para adotar em caso de cessação dos seus serviços de pagamento e de rescisão dos contratos existentes, de forma a evitar efeitos adversos nos sistemas de pagamento e nos utilizadores de serviços de pagamento e a assegurar a execução das transações de pagamento pendentes.

Plano de continuidade de negócio baseado em cenários

6.4 O prestador de serviços de pagamento deve considerar um conjunto de diferentes cenários, incluindo os mais extremos mas plausíveis, aos quais pode estar exposto, e avaliar o potencial impacto que tais cenários podem ter.

6.5 Com base na análise realizada no âmbito da Orientação 6.2 e nos cenários plausíveis identificados de acordo com a Orientação 6.4, o prestador de serviços de pagamento deve desenvolver planos de resposta e de recuperação que estejam:

a) focados no impacto no funcionamento de áreas, processos, sistemas, transações e interdependências críticos;

b) documentados e sejam disponibilizados às unidades de negócio e de suporte e facilmente acessíveis em caso de emergência; e

c) atualizados com as “lições aprendidas” retiradas dos testes, novos riscos identificados e ameaças e das alterações efetuadas aos objetivos de recuperação e prioridades.

Teste aos planos de continuidade de negócio

6.6 Os prestadores de serviços de pagamento devem testar os seus planos de continuidade de negócio e assegurar que o funcionamento das suas áreas, processos, sistemas, transações e interdependências críticos é testado pelo menos anualmente. Os planos devem suportar-se em objetivos para proteção e, se necessário, restabelecimento da integridade e disponibilidade das suas operações e da confidencialidade dos seus ativos de informação.

6.7 Os planos devem ser atualizados pelo menos anualmente, com base nos resultados dos testes, em ameaças atuais de informações, na partilha de informação e em lições aprendidas com eventos anteriores e nas alterações efetuadas aos objetivos de recuperação, bem como na análise de cenários operacional e tecnicamente plausíveis que ainda não tenham ocorrido e, se relevante, após a ocorrência de alterações nos sistemas e processos. Durante o desenvolvimento dos seus planos de continuidade de negócio, os prestadores de serviços de pagamento devem consultar e coordenar com as partes interessadas relevantes, internas e externas.

6.8 Os testes aos planos de continuidade de negócio dos prestadores de serviços de pagamento devem:

a) incluir um adequado conjunto de cenários, conforme referido na Orientação 6.4;

b) ser concebidos para desafiar os pressupostos sobre os quais se baseiam os planos de continuidade de negócio, incluindo acordos de governação e planos de comunicação de crises; e

c) incluir procedimentos para verificar a capacidade do seu pessoal e dos seus processos de responder adequadamente aos cenários acima mencionados.

6.9 Os prestadores de serviços de pagamento devem monitorizar periodicamente a eficácia dos seus planos de continuidade de negócio e documentar e analisar quaisquer desafios ou falhas resultantes dos testes.

Comunicação de crises

6.10 No caso de uma interrupção ou emergência, e durante a implementação dos planos de continuidade de negócio, os prestadores de serviços de pagamento devem assegurar que têm implementadas medidas eficazes de comunicação de crises para que todas as partes interessadas relevantes, internas e externas, incluindo prestadores de serviços externos, sejam informados de forma atempada e adequada.

Orientação 7: Teste às medidas de segurança

7.1 Os prestadores de serviços de pagamento devem estabelecer e implementar uma estrutura de teste que valide a robustez e a eficácia das medidas de segurança e assegurar que a estrutura de teste é adaptada para considerar novas ameaças e vulnerabilidades, identificadas através das atividades de monitorização de risco.

7.2 Os prestadores de serviços de pagamento devem assegurar que os testes são realizados no caso de ocorrerem alterações ao nível das infraestruturas, processos ou procedimentos e no caso de essas alterações serem efetuadas em consequência da ocorrência de incidentes operacionais ou de segurança de carácter severo.

7.3 A estrutura de teste deve também abranger as medidas de segurança relevantes para (i) terminais de pagamento e dispositivos utilizados para a prestação de serviços de pagamento, (ii) terminais de pagamento e dispositivos utilizados para autenticar o utilizador de serviços de pagamento e (iii) dispositivos e *software* fornecidos pelo prestador de serviços de pagamento para o utilizador de serviços de pagamento gerar/receber um código de autenticação.

7.4 A estrutura de teste deve assegurar que os testes:

a) são realizados como parte do processo de gestão de alterações formal do prestador de serviços de pagamento de forma a garantir a sua robustez e eficácia;

b) são efetuados por pessoal independente com conhecimentos, competências e experiência suficientes para testar medidas de segurança relativas a serviços de pagamento e que não está envolvido no desenvolvimento das medidas de segurança relativas aos respetivos serviços ou sistemas de pagamento a testar, pelo menos nos testes finais antes da implementação das medidas de segurança; e

c) incluem análises de vulnerabilidade e testes de penetração adequados ao nível de risco identificado para os serviços de pagamento.

7.5 Os prestadores de serviços de pagamento devem realizar testes, de forma contínua e repetida, às medidas de segurança dos seus serviços de pagamento. Para os sistemas considerados críticos para a prestação dos serviços de pagamento (conforme descrito na Orientação 3.2), estes testes devem ser realizados pelo menos anualmente. Os sistemas não críticos devem ser testados regularmente seguindo uma abordagem orientada para o risco, mas no mínimo a cada três anos.

7.6 Os prestadores de serviços de pagamento devem monitorizar e avaliar os resultados dos testes realizados e atualizar as suas medidas de segurança em conformidade e sem demora indevida no caso dos sistemas críticos.

Orientação 8: Conhecimento da situação e aprendizagem contínua

Cenário de ameaças e conhecimento da situação

8.1 Os prestadores de serviços de pagamento devem estabelecer e implementar processos e estruturas organizacionais de forma a identificar e monitorizar constantemente as ameaças de segurança e operacionais que podem afetar materialmente a sua capacidade de prestar serviços de pagamento.

8.2 Os prestadores de serviços de pagamento devem analisar os incidentes operacionais ou de segurança identificados ou ocorridos dentro e/ou fora da organização. Os prestadores de serviços

de pagamento devem retirar destas análises as principais lições aprendidas e atualizar as medidas de segurança em conformidade.

8.3 Os prestadores de serviços de pagamento devem monitorizar ativamente os desenvolvimentos tecnológicos para assegurar que têm conhecimento dos riscos de segurança.

Programas de formação e sensibilização para a segurança

8.4 Os prestadores de serviços de pagamento devem estabelecer um programa de formação para todo o pessoal que assegure que são formados para desempenhar os seus deveres e responsabilidades de forma consistente com as políticas e procedimentos de segurança relevantes, tendo por objetivo reduzir o erro humano, roubo, fraude, uso indevido ou perda. Os prestadores de serviços de pagamento devem assegurar que o programa oferece formação ao pessoal pelo menos uma vez por ano, ou com maior frequência, se necessário.

8.5 Os prestadores de serviços de pagamento devem assegurar que os membros do pessoal identificado no âmbito da Orientação 3.1 com funções essenciais recebem formação específica em segurança da informação, numa base anual, ou com maior frequência, se necessário.

8.6 Os prestadores de serviços de pagamento devem estabelecer e implementar programas periódicos de sensibilização para a segurança de forma a educar o seu pessoal e a abordar os riscos relacionados com a segurança da informação. Estes programas devem exigir a comunicação de qualquer incidente e atividade fora do comum por parte do seu pessoal.

Orientação 9: Gestão da relação com os utilizadores de serviços de pagamento

Sensibilização dos utilizadores de serviços de pagamento para os riscos de segurança e ações de mitigação de risco

9.1 Os prestadores de serviços de pagamento devem estabelecer e implementar processos para aumentar a sensibilização dos utilizadores de serviços de pagamento quanto aos riscos de segurança associados aos serviços de pagamento através da prestação de assistência e orientação aos utilizadores de serviços de pagamento.

9.2 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.

9.3 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 pelo prestador de serviços de pagamento ao utilizador de serviços de pagamento.

9.4 Quando, em conformidade com o n.º 1 do artigo 68.º da DSP2, um prestador de serviços de pagamento tiver acordado com o ordenante limites de despesa para as transações 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.

9.5 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 transações de pagamento, permitindo assim detetar a utilização fraudulenta ou maliciosa da sua conta.

9.6 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.

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