REGULAMENTO DELEGADO (UE) 2024/1774 DA COMISSÃO

de 13 de março de 2024

que complementa o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeito às normas técnicas de regulamentação que especificam as ferramentas, métodos, processos e políticas de gestão do risco associado às TIC e ao quadro simplificado de gestão do risco associado às TIC

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 ([1]), nomeadamente o artigo 15.º, quarto parágrafo, e o artigo 16.º, n.º 3, quarto parágrafo,

Considerando o seguinte:

(1) O Regulamento (UE) 2022/2554 abrange uma grande variedade de entidades financeiras que diferem em termos de dimensão, estrutura e organização interna, bem como em termos de natureza e complexidade das suas atividades, pelo que têm elementos de maior ou menor complexidade ou de maior ou menor risco. Para assegurar que essa variedade é devidamente tida em conta, importa assegurar que quaisquer requisitos em matéria de políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC, bem como em matéria de um quadro simplificado de gestão do risco associado às TIC, sejam proporcionados a essa dimensão, estrutura, organização interna, natureza e complexidade dessas entidades financeiras, bem como aos riscos correspondentes.

(2) Pela mesma razão, é importante que as entidades financeiras sujeitas ao Regulamento (UE) 2022/2554 disponham de uma certa flexibilidade na forma como cumprem quaisquer requisitos relativos às políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC, bem como no que respeita a qualquer quadro simplificado de gestão do risco associado às TIC. Por esse motivo, as entidades financeiras devem ser autorizadas a utilizar os documentos de que já dispõem para cumprir quaisquer requisitos de documentação decorrentes desses requisitos. Daqui resulta que só será adequado exigir o desenvolvimento, a documentação e a aplicação de políticas específicas de segurança das TIC para determinados elementos essenciais, tendo em conta, nomeadamente, as melhores práticas e normas do setor. Além disso, a fim de abranger aspetos técnicos específicos da execução, é necessário desenvolver, documentar e aplicar procedimentos de segurança das TIC que abranjam aspetos técnicos específicos da execução, designadamente a gestão da capacidade e do desempenho, a gestão de vulnerabilidades e as correções, a segurança dos dados e dos sistemas e as atividades de registo.

(3) Com vista a assegurar a correta aplicação, ao longo do tempo, das políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC referidas no título II, capítulo I, do presente regulamento, é importante que as entidades financeiras atribuam e mantenham corretamente as funções e responsabilidades relacionadas com a segurança das TIC e definam as consequências do incumprimento das políticas ou dos procedimentos de segurança no domínio das TIC.

(4) Para limitar o risco de conflitos de interesses, as entidades financeiras devem assegurar a segregação de funções aquando da atribuição de funções e responsabilidades no domínio das TIC.

(5) Para assegurar flexibilidade e simplificar o quadro de controlo das entidades financeiras, estas não devem ser obrigadas a desenvolver disposições específicas relativas às consequências do incumprimento das políticas, procedimentos e protocolos de segurança das TIC referidos no título II, capítulo I, do presente regulamento, caso essas disposições já estejam estabelecidas noutra política ou procedimento.

([1]) JO L 333 de 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj

(6) Num ambiente dinâmico, em que os riscos associados às TIC evoluem constantemente, é importante que as entidades financeiras desenvolvam o seu conjunto de políticas de segurança das TIC com base nas melhores práticas e, se for caso disso, nas normas definidas no artigo 2.º, ponto 1, do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho ([2]), o que deverá permitir que as entidades financeiras referidas no título II do presente regulamento se mantenham informadas e preparadas num cenário em mutação.

(7) Com visa a assegurar a sua resiliência operacional digital, as entidades financeiras referidas no título II do presente regulamento devem, no âmbito das suas políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC, desenvolver e aplicar uma política de gestão dos ativos de TIC, procedimentos de gestão da capacidade e do desempenho, bem como políticas e procedimentos para as operações no domínio das TIC. Essas políticas e procedimentos são necessários para assegurar a monitorização do estado dos ativos de TIC ao longo de todo o seu ciclo de vida, de modo que esses ativos sejam utilizados e mantidos de forma eficaz (gestão dos ativos de TIC). Essas políticas e procedimentos devem igualmente assegurar a otimização do funcionamento dos sistemas de TIC e garantir que o desempenho e a capacidade dos sistemas de TIC cumprem os objetivos de segurança estabelecidos para a atividade e para a informação (gestão da capacidade e do desempenho). Por último, essas políticas e esses procedimentos devem assegurar a gestão e o funcionamento quotidianos eficazes e harmoniosos dos sistemas de TIC (funcionamento das TIC), minimizando assim o risco de perda de confidencialidade, integridade e disponibilidade de dados. Essas políticas e procedimentos são, por conseguinte, necessários para garantir a segurança das redes, proporcionar salvaguardas adequadas contra intrusões e utilizações abusivas dos dados e preservar a disponibilidade, autenticidade, integridade e confidencialidade dos dados.

(8) Para assegurar uma gestão adequada do risco dos sistemas de TIC legados, as entidades financeiras devem registar e monitorizar as datas de termo dos serviços de apoio prestados por terceiros no domínio das TIC. Devido ao potencial impacto que uma perda de confidencialidade, integridade e disponibilidade de dados pode ter, as entidades financeiras devem concentrar-se nos ativos ou sistemas de TIC que sejam críticos para o funcionamento das empresas, aquando do registo e da monitorização dessas datas de termo.

(9) A disponibilidade, autenticidade, integridade e confidencialidade dos dados podem ser garantidos através de controlos criptográficos. Por conseguinte, as entidades financeiras referidas no título II do presente regulamento devem identificar e aplicar esses controlos com base numa abordagem baseada no risco. Para o efeito, as entidades financeiras devem encriptar os dados em causa quando estão conservados, em trânsito ou, se necessário, em utilização, com base nos resultados de um processo em duas vertentes, a saber, a classificação dos dados e uma avaliação exaustiva do risco associado às TIC. Dada a complexidade da encriptação dos dados em utilização, as entidades financeiras referidas no título II do presente regulamento só devem encriptar os dados em utilização se tal for adequado tendo em conta os resultados da avaliação do risco associado às TIC. Contudo, é importante que as entidades financeiras referidas no título II do presente regulamento possam, caso a encriptação dos dados em utilização não seja viável ou seja demasiado complexa, proteger a confidencialidade, integridade e disponibilidade dos dados em causa através de outras medidas de segurança das TIC. Tendo em conta a rápida evolução tecnológica no domínio das técnicas criptográficas, as entidades financeiras referidas no título II do presente regulamento devem manter-se a par dos desenvolvimentos relevantes em matéria de criptoanálise e ter em consideração as melhores práticas e normas. Assim sendo, as entidades financeiras referidas no título II do presente regulamento devem seguir uma abordagem flexível, baseada na mitigação e monitorização dos riscos, para lidar com o panorama dinâmico das ameaças criptográficas, incluindo as ameaças decorrentes de avanços quânticos.

(10) A segurança das operações de TIC e as políticas, procedimentos, protocolos e ferramentas operacionais são essenciais para garantir a confidencialidade, integridade e disponibilidade dos dados. Um aspeto central é a separação estrita entre os ambientes de produção de TIC e os ambientes em que os sistemas de TIC são desenvolvidos e testados ou outros ambientes não produtivos. Essa separação deverá constituir uma importante medida de segurança das TIC contra o acesso não intencional e não autorizado a dados e contra alterações e supressões de dados no ambiente de produção, que podem resultar em perturbações graves nas operações comerciais das entidades financeiras referidas no título II do presente regulamento. Contudo, tendo em conta as atuais práticas de desenvolvimento dos sistemas de TIC, em circunstâncias excecionais, as entidades financeiras devem ser autorizadas a realizar testes em ambientes de produção, desde que justifiquem esses testes e obtenham a aprovação necessária.

([2]) Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) A rápida evolução dos ambientes TIC, as vulnerabilidades das TIC e as ciberameaças exigem uma abordagem proativa e abrangente para identificar, avaliar e dar resposta às vulnerabilidades das TIC. Sem essa abordagem, as entidades financeiras, os seus clientes, utilizadores ou contrapartes podem ficar gravemente expostos a riscos que poriam em risco a sua resiliência operacional digital, a segurança das suas redes e a disponibilidade, autenticidade, integridade e confidencialidade dos dados que as políticas e os procedimentos de segurança das TIC devem proteger. Por conseguinte, importa que as entidades financeiras referidas no título II do presente regulamento identifiquem e corrijam as vulnerabilidades no seu ambiente de TIC e que tanto as entidades financeiras como os terceiros que lhes prestem serviços no domínio das TIC adiram a um quadro de gestão das vulnerabilidades coerente, transparente e responsável. Pela mesma razão, as entidades financeiras devem monitorizar as vulnerabilidades das TIC utilizando recursos fiáveis e ferramentas automatizadas, verificando se os terceiros prestadores de serviços de TIC asseguram uma ação rápida em relação às vulnerabilidades nos serviços de TIC prestados.

(12) A gestão das correções informáticas deve ser uma parte crucial das políticas e procedimentos de segurança das TIC que, através de testes e implantação num ambiente controlado, visam resolver as vulnerabilidades identificadas e evitar perturbações na instalação de correções.

(13) A fim de assegurar uma comunicação atempada e transparente de potenciais ameaças à segurança que possam afetar a entidade financeira e as suas partes interessadas, as entidades financeiras devem estabelecer procedimentos para a divulgação responsável das vulnerabilidades no domínio das TIC aos clientes, às contrapartes e ao público. Ao estabelecerem esses procedimentos, as entidades financeiras devem ter em conta alguns fatores, nomeadamente a gravidade da vulnerabilidade, o potencial impacto dessa vulnerabilidade nas partes interessadas e a prontidão para adotar uma correção ou medidas de mitigação.

(14) Com vista a permitir a atribuição de direitos de acesso aos utilizadores, as entidades financeiras referidas no título II do presente regulamento devem estabelecer medidas sólidas para confirmar a identificação única das pessoas e dos sistemas que terão acesso às informações da entidade financeira. Se tal não acontecer, as entidades financeiras ficam expostas a potenciais acessos não autorizados, violações de dados e atividades fraudulentas, comprometendo assim a confidencialidade, integridade e disponibilidade de dados financeiros sensíveis. Embora a utilização de contas genéricas ou partilhadas deva ser autorizada a título excecional em circunstâncias especificadas pelas entidades financeiras, as entidades financeiras devem assegurar que permaneça assegurada a responsabilização pelas ações tomadas através dessas contas. Sem essa salvaguarda, os potenciais utilizadores mal-intencionados podem prejudicar a aplicação de medidas de investigação e corretivas, deixando as entidades financeiras vulneráveis a atividades maliciosas não detetadas ou a sanções por incumprimento.

(15) Para gerir a rápida evolução dos ambientes de TIC, é importante que as entidades financeiras referidas no título II do presente regulamento apliquem políticas e procedimentos sólidos de gestão dos projetos de TIC para manter a disponibilidade, autenticidade, integridade e confidencialidade dos dados. Essas políticas e procedimentos de gestão dos projetos de TIC devem identificar os elementos necessários para gerir com êxito esses projetos, em especial as alterações, aquisições, manutenção e evolução dos sistemas de TIC da entidade financeira, independentemente da metodologia de gestão dos projetos de TIC escolhida pela entidade financeira. No contexto dessas políticas e procedimentos, as entidades financeiras devem adotar práticas e métodos para a realização de testes que correspondam às suas necessidades, aderindo simultaneamente a uma abordagem baseada no risco e assegurando a manutenção de um ambiente de TIC seguro, fiável e resiliente. A fim de garantir a execução segura de um projeto de TIC, as entidades financeiras devem assegurar que o pessoal de setores de atividade ou funções específicos influenciados ou afetados por esse projeto de TIC possa fornecer as informações e os conhecimentos especializados necessários. Para assegurar uma supervisão eficaz, deverão ser apresentados ao órgão de administração relatórios sobre os projetos de TIC, em especial sobre aqueles que afetem funções críticas ou importantes e sobre os riscos que lhes estão associados. As entidades financeiras devem adaptar a frequência e os pormenores das revisões e dos relatórios sistemáticos e contínuos à importância e à dimensão dos projetos de TIC em causa.

(16) É necessário assegurar que os pacotes de programas informáticos que as entidades financeiras referidas no título II do presente regulamento adquiram e desenvolvam sejam integrados no ambiente das TIC existente de forma eficaz e segura, em conformidade com os objetivos empresariais e de segurança da informação estabelecidos. Por conseguinte, as entidades financeiras devem avaliar exaustivamente esses pacotes de programas informáticos. Para o efeito, e a fim de identificar vulnerabilidades e potenciais lacunas de segurança tanto nos pacotes de programas informáticos como nos sistemas TIC num sentido mais lato, as entidades financeiras devem realizar testes de segurança das TIC. Com vista a avaliar a integridade dos programas informáticos e assegurar que a utilização desses programas informáticos não coloca riscos à segurança das TIC, as entidades financeiras devem também analisar os códigos-fonte dos programas informáticos adquiridos, designadamente, sempre que possível, dos programas informáticos patenteados fornecidos por terceiros prestadores de serviços de TIC, utilizando métodos estáticos e dinâmicos para a realização dos testes.

(17) Efetuar alterações, independentemente da sua escala, comporta riscos inerentes e pode representar riscos significativos de perda de confidencialidade, integridade e disponibilidade de dados, podendo, por conseguinte, conduzir a graves perturbações das atividades. A fim de proteger as entidades financeiras de potenciais vulnerabilidades e fragilidades das TIC suscetíveis de as expor a riscos significativos, é necessário um processo de verificação rigoroso para confirmar que todas as alterações cumprem os requisitos de segurança das TIC necessários. Por conseguinte, as entidades financeiras referidas no título II do presente regulamento devem dispor de políticas e procedimentos sólidos de gestão das alterações das TIC, enquanto elemento essencial das suas políticas e procedimentos de segurança das TIC. Com vista a manter a objetividade e a eficácia do processo de gestão das alterações das TIC, prevenir conflitos de interesses e assegurar que as alterações das TIC são avaliadas de forma objetiva, é necessário separar as funções responsáveis pela aprovação dessas alterações das funções que solicitam e implementam essas alterações. Para alcançar transições eficazes, uma aplicação controlada das alterações das TIC e perturbações mínimas no funcionamento dos sistemas de TIC, as entidades financeiras devem atribuir funções e responsabilidades claras que assegurem que as alterações das TIC são planeadas, testadas adequadamente e que a qualidade é assegurada. Por forma a assegurar que os sistemas de TIC continuam a funcionar eficazmente e a proporcionar uma rede de segurança às entidades financeiras, estas devem também desenvolver e aplicar procedimentos alternativos. As entidades financeiras devem identificar claramente esses procedimentos alternativos e atribuir responsabilidades para assegurar uma resposta rápida e eficaz caso as alterações das TIC não sejam bem-sucedidas.

(18) Para detetar, gerir e comunicar incidentes relacionados com as TIC, as entidades financeiras referidas no título II do presente regulamento devem estabelecer uma política em matéria de incidentes relacionados com as TIC que abranja os componentes de um processo de gestão de incidentes relacionados com as TIC. Para o efeito, as entidades financeiras devem identificar todos os contactos pertinentes dentro e fora da organização que possam facilitar a correta coordenação e execução das diferentes fases desse processo. Para otimizar a deteção e a resposta a incidentes relacionados com as TIC e identificar tendências desses incidentes, uma fonte de informação valiosa que permitirá às entidades financeiras identificar e resolver as causas profundas e os problemas de forma eficaz, as entidades financeiras devem, em especial, analisar pormenorizadamente os incidentes relacionados com as TIC que considerem mais significativos, em especial, devido à sua recorrência regular.

(19) Para garantir uma deteção precoce e eficaz das atividades anómalas, as entidades financeiras referidas no título II do presente regulamento devem recolher, monitorizar e analisar as diferentes fontes de informação e atribuir funções e responsabilidades conexas. No que respeita às fontes internas de informação, os registos são uma fonte extremamente relevante, mas as entidades financeiras não devem basear-se apenas nos mesmos. Em vez disso, é importante que as entidades financeiras considerem informações mais amplas por forma a incluir o que é comunicado por outras funções internas, uma vez que essas funções são frequentemente uma fonte valiosa de informações relevantes. Pela mesma razão, as entidades financeiras devem analisar e monitorizar as informações recolhidas de fontes externas, nomeadamente informações fornecidas por terceiros prestadores de serviços de TIC sobre incidentes que afetem os seus sistemas e redes, bem como outras fontes de informação que as entidades financeiras considerem relevantes. Na medida em que essas informações constituam dados pessoais, aplica-se o direito da União em matéria de proteção de dados. Os dados pessoais devem limitar-se ao necessário para a deteção de incidentes.

(20) A fim de facilitar a deteção de incidentes relacionados com as TIC, as entidades financeiras devem conservar provas desses incidentes. Para assegurar, por um lado, que esses elementos de prova são conservados durante um tempo suficientemente longo e evitar, por outro lado, encargos regulamentares excessivos, as entidades financeiras devem determinar o período de conservação tendo em conta, entre outros aspetos, o caráter crítico dos dados e os requisitos de conservação decorrentes do direito da União.

(21) Com vista a assegurar que os incidentes relacionados com as TIC são detetados a tempo, as entidades financeiras referidas no título II do presente regulamento devem considerar não exaustivos os critérios identificados para desencadear a deteção e as respostas a incidentes relacionados com as TIC. Além disso, embora as entidades financeiras devam considerar cada um desses critérios, as circunstâncias descritas nos critérios não devem ter de ocorrer simultaneamente e a importância dos serviços de TIC afetados deve ser devidamente tida em conta para desencadear processos de deteção e resposta a incidentes relacionados com as TIC.

(22) Ao desenvolverem uma política de continuidade das atividades no domínio das TIC, as entidades financeiras referidas no título II do presente regulamento devem ter em conta os componentes essenciais da gestão do risco associado às TIC, designadamente as estratégias de gestão e comunicação de incidentes relacionados com as TIC, o processo de gestão das alterações das TIC e os riscos associados aos terceiros prestadores de serviços de TIC.

(23) É necessário definir o conjunto de cenários que as entidades financeiras referidas no título II do presente regulamento devem ter em conta tanto para a execução dos planos de resposta e recuperação no domínio das TIC como para a realização de testes dos planos de continuidade das atividades no domínio das TIC. Esses cenários devem servir de ponto de partida para as entidades financeiras analisarem tanto a pertinência e a plausibilidade de cada cenário como a necessidade de desenvolver cenários alternativos. As entidades financeiras devem concentrar-se nos cenários em que o investimento em medidas de resiliência pode ser mais eficiente e eficaz. Ao testar as transições entre a infraestrutura de TIC primária e qualquer capacidade redundante, cópias de segurança e equipamentos redundantes, as instituições financeiras devem avaliar se essa capacidade, essas cópias de segurança e esses equipamentos funcionam eficazmente durante um período suficiente e assegurar que o funcionamento normal da infraestrutura de TIC primária é restabelecido em conformidade com os objetivos de recuperação.

(24) É necessário estabelecer requisitos em matéria de risco operacional e, mais especificamente, requisitos relativos à gestão das alterações e dos projetos de TIC e à gestão da continuidade das atividades no domínio das TIC, com base nos que já se aplicam às contrapartes centrais, às centrais de valores mobiliários e às plataformas de negociação nos termos dos Regulamentos (UE) n.º 648/2012 ([3]), (UE) n.º 600/2014 ([4]) e (UE) n.º 909/2014 ([5]) do Parlamento Europeu e do Conselho, respetivamente.

(25) O artigo 6.º, n.º 5, do Regulamento (UE) 2022/2554 exige que as entidades financeiras revejam o seu quadro de gestão do risco associado às TIC e apresentem à sua autoridade competente um relatório sobre essa análise. A fim de permitir que as autoridades competentes tratem facilmente as informações contidas nesses relatórios e garantam uma transmissão adequada das mesmas, as entidades financeiras devem apresentar esses relatórios num formato eletrónico pesquisável.

(26) Os requisitos aplicáveis às entidades financeiras sujeitas ao quadro simplificado de gestão do risco associado às TIC referido no artigo 16.º do Regulamento (UE) 2022/2554 devem centrar-se nos domínios e elementos essenciais que, tendo em conta a escala, o risco, a dimensão e a complexidade dessas entidades financeiras, sejam, no mínimo, necessários para assegurar a confidencialidade, integridade, disponibilidade e autenticidade dos dados e serviços dessas entidades financeiras. Nesse contexto, essas entidades financeiras devem dispor de um quadro interno de governação e controlo com responsabilidades claras, a fim de permitir a existência de um quadro de gestão dos riscos eficaz e sólido. Além disso, a fim de reduzir os encargos administrativos e operacionais, essas entidades financeiras devem desenvolver e documentar apenas uma política, ou seja, uma política de segurança da informação, que especifique os princípios e regras de alto nível necessários para proteger a confidencialidade, integridade, disponibilidade e autenticidade dos dados e serviços dessas entidades financeiras.

(27) As disposições do presente regulamento dizem respeito ao domínio do quadro de gestão do risco associado às TIC, especificando os elementos específicos aplicáveis às entidades financeiras, em conformidade com o artigo 15.º do Regulamento (UE) 2022/2554, e concebendo o quadro simplificado de gestão do risco associado às TIC para as entidades financeiras previsto no artigo 16.º, n.º 1, do mesmo regulamento. A fim de assegurar a coerência entre o quadro ordinário e o quadro simplificado de gestão do risco associado às TIC, e tendo em conta que essas disposições devem tornar-se aplicáveis ao mesmo tempo, é conveniente incluí-las num único ato legislativo.

(28) O presente regulamento baseia-se nos projetos de normas técnicas de regulamentação apresentados à Comissão pela Autoridade Bancária Europeia, pela Autoridade Europeia dos Seguros e Pensões Complementares de Reforma e pela Autoridade Europeia dos Valores Mobiliários e dos Mercados (Autoridades Europeias de Supervisão), em consulta com a Agência da União Europeia para a Cibersegurança (ENISA).

([3]) Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, de 4 de julho de 2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações (JO L 201 de 27.7.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) Regulamento (UE) n.º 600/2014 do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativo aos mercados de instrumentos financeiros e que altera o Regulamento (UE) n.º 648/2012 (JO L 173 de 12.6.2014, p. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) Regulamento (UE) n.º 909/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à melhoria da liquidação de valores mobiliários na União Europeia e às Centrais de Valores Mobiliários (CSDs) e que altera as Diretivas 98/26/CE e 2014/65/UE e o Regulamento (UE) n.º 236/2012 (JO L 257 de 28.8.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) O Comité Conjunto das Autoridades Europeias de Supervisão referido no artigo 54.º do Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho ([6]), no artigo 54.º do Regulamento (UE) n.º 1094/2010 do Parlamento Europeu e do Conselho ([7]) e no artigo 54.º do Regulamento (UE) n.º 1095/2010 do Parlamento Europeu e do Conselho ([8]) realizou consultas públicas abertas sobre os projetos de normas técnicas de regulamentação em que se baseia o presente regulamento, analisou os potenciais custos e benefícios das normas propostas e solicitou o parecer do Grupo das Partes Interessadas do Setor Bancário criado em conformidade com o artigo 37.º do Regulamento (UE) n.º 1093/2010, do Grupo de Interessados do Setor dos Seguros e Resseguros e do Grupo de Interessados do Setor das Pensões Complementares de Reforma criados em conformidade com o artigo 37.º do Regulamento (UE) n.º 1094/2010 e do Grupo de Interessados do Setor dos Valores Mobiliários e dos Mercados criado em conformidade com o artigo 37.º do Regulamento (UE) n.º 1095/2010.

(30) Na medida em que o tratamento de dados pessoais seja necessário para cumprir as obrigações estabelecidas no presente ato, aplicam-se plenamente o Regulamento (UE) 2016/679 ([9]) e o Regulamento (UE) 2018/1725 ([10]) do Parlamento Europeu e do Conselho. A título de exemplo, o princípio da minimização dos dados deve ser respeitado quando os dados pessoais são recolhidos para assegurar uma deteção adequada de incidentes. A Autoridade Europeia para a Proteção de Dados foi igualmente consultada sobre o projeto de texto do presente ato,

ADOTOU O PRESENTE REGULAMENTO:

TÍTULO I

PRINCÍPIOS GERAIS

Artigo 1.º

Perfil de risco global e complexidade

Ao desenvolver e aplicar as políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC referidos no título II e o quadro simplificado de gestão do risco associado às TIC referido no título III, devem ser tidos em conta a dimensão e o perfil de risco global da entidade financeira, bem como a natureza, escala e os elementos de maior ou menor complexidade dos seus serviços, atividades e operações, incluindo os elementos relacionados com:

a) Encriptação e criptografia;

b) Segurança das operações de TIC;

c) Segurança da rede;

([6]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Regulamento (UE) n.º 1094/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Europeia dos Seguros e Pensões Complementares de Reforma), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/79/CE da Comissão (JO L 331 de 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Regulamento (UE) n.º 1095/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Europeia dos Valores Mobiliários e dos Mercados), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/77/CE da Comissão (JO L 331 de 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) Regulamento (UE) 2016/679 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d) Gestão das alterações e dos projetos de TIC;

e) O potencial impacto do risco associado às TIC na confidencialidade, integridade e disponibilidade dos dados, bem como das perturbações na continuidade e disponibilidade das atividades da entidade financeira.

TÍTULO II

MAIOR HARMONIZAÇÃO DAS FERRAMENTAS, MÉTODOS, PROCESSOS E POLÍTICAS DE GESTÃO DO RISCO ASSOCIADO ÀS TIC, EM CONFORMIDADE COM O ARTIGO 15.º DO REGULAMENTO (UE) 2022/2554

CAPÍTULO I

Políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC

Secção 1

Artigo 2.º

Elementos gerais das políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC

1. As entidades financeiras devem assegurar que as suas políticas de segurança das TIC, segurança da informação e os procedimentos, protocolos e ferramentas conexos referidos no artigo 9.º, n.º 2, do Regulamento (UE) 2022/2554 estão incorporados no seu quadro de gestão do risco associado às TIC. As entidades financeiras devem estabelecer as políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC previstos no presente capítulo de modo que:

a) Assegurem a segurança das redes;

b) Contenham proteções contra as intrusões e a utilização abusiva de dados;

c) Preservem a disponibilidade, autenticidade, integridade e confidencialidade dos dados, nomeadamente através da utilização de técnicas criptográficas;

d) Garantam uma transmissão rigorosa e rápida dos dados, sem grandes perturbações e atrasos indevidos.

2. As entidades financeiras devem assegurar que as políticas de segurança das TIC referidas no n.º 1:

a) Estão alinhadas com os objetivos de segurança da informação da entidade financeira incluídos na estratégia de resiliência operacional digital referida no artigo 6.º, n.º 8, do Regulamento (UE) 2022/2554;

b) Indicam a data da aprovação formal das políticas de segurança das TIC pelo órgão de administração;

c) Contêm indicadores e medidas para:

   i) monitorizar a aplicação das políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC,

   ii) registar as exceções a essa aplicação,

   iii) garantir que a resiliência operacional digital da entidade financeira é assegurada em caso de exceções, tal como referido na subalínea ii);

d) Especificam as responsabilidades do pessoal a todos os níveis no sentido de garantir a segurança das TIC da entidade financeira;

e) Especificam as consequências do incumprimento, por parte do pessoal da entidade financeira, das políticas de segurança das TIC, caso as disposições para o efeito não estejam previstas noutras políticas da entidade financeira;

f) Enumeram a documentação que deve ser conservada;

g) Especificam as disposições relativas à segregação de funções no contexto do modelo das três linhas de defesa ou de outro modelo interno de gestão e controlo dos riscos, conforme aplicável, a fim de evitar conflitos de interesses;

h) Têm em conta as melhores práticas e, se for caso disso, as normas definidas no artigo 2.º, ponto 1, do Regulamento (UE) n.º 1025/2012;

i) Identificam as funções e responsabilidades no quadro do desenvolvimento, aplicação e manutenção de políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC;

j) São revistas em conformidade com o artigo 6.º, n.º 5, do Regulamento (UE) 2022/2554;

k) Têm em conta as alterações significativas relativas à entidade financeira, nomeadamente alterações significativas das suas atividades ou processos, do panorama das ciberameaças ou das obrigações jurídicas aplicáveis.

Secção 2

Artigo 3.º

Gestão do risco associado às TIC

As entidades financeiras devem desenvolver, documentar e aplicar políticas e procedimentos de gestão do risco associado às TIC que incluam todos os elementos seguintes:

a) Uma indicação da aprovação do nível de tolerância ao risco associado às TIC estabelecido em conformidade com o artigo 6.º, n.º 8, alínea b), do Regulamento (UE) 2022/2554;

b) Um procedimento e uma metodologia para realizar a avaliação do risco associado às TIC, que identifiquem:

   i) as vulnerabilidades e ameaças que afetem ou possam afetar as funções operacionais apoiadas, os sistemas de TIC e os ativos de TIC que apoiam essas funções,

   ii) os indicadores quantitativos ou qualitativos para medir o impacto e a probabilidade das vulnerabilidades e ameaças referidas na subalínea i);

c) O procedimento para identificar, aplicar e documentar medidas de tratamento do risco associado às TIC para os riscos associados às TIC identificados e avaliados, designadamente a determinação das medidas de tratamento do risco associado às TIC necessárias para manter esse risco dentro do nível de tolerância referido na alínea a);

d) Para os riscos residuais associados às TIC que ainda estejam presentes na sequência da aplicação das medidas de tratamento do risco associado às TIC referido na alínea c):

   i) disposições relativas à identificação desses riscos residuais associados às TIC,

   ii) a atribuição de funções e responsabilidades no que respeita:

      (1) à aceitação dos riscos residuais associados às TIC que excedem o nível de tolerância ao risco da entidade financeira referido na alínea a);

      (2) ao processo de revisão referido na subalínea iv) da presente alínea d);

   iii) a elaboração de um inventário dos riscos residuais associados às TIC aceites, incluindo uma justificação para a sua aceitação,

   iv) disposições relativas à revisão dos riscos residuais associados às TIC aceites, pelo menos uma vez por ano, nomeadamente:

      (1) a identificação de quaisquer alterações dos riscos residuais associados às TIC;

      (2) a avaliação das medidas de mitigação disponíveis;

      (3) uma avaliação para determinar se as razões que justificam a aceitação dos riscos residuais associados às TIC continuam a ser válidas e aplicáveis à data da revisão;

e) Disposições relativas à monitorização:

   i) de quaisquer alterações do panorama dos riscos associados às TIC e das ciberameaças,

   ii) das vulnerabilidades e ameaças internas e externas,

   iii) do risco associado às TIC da entidade financeira, de um modo que permita a deteção rápida de alterações que possam afetar o seu perfil de risco associado às TIC;

f) Disposições relativas a um processo para assegurar que quaisquer alterações da estratégia empresarial e da estratégia de resiliência operacional digital da entidade financeira são tidas em conta.

Para efeitos da alínea c), primeiro parágrafo, o procedimento referido nessa alínea deve assegurar:

a) A monitorização da eficácia das medidas de tratamento do risco associado às TIC aplicadas;

b) Uma avaliação para determinar se os níveis de tolerância ao risco estabelecidos pela entidade financeira foram atingidos;

c) Uma avaliação para determinar se a entidade financeira tomou medidas para corrigir ou melhorar essas medidas, quando necessário.

Secção 3

Gestão dos ativos de TIC

Artigo 4.º

Política de gestão dos ativos de TIC

1. No âmbito das políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC referidas no artigo 9.º, n.º 2, do Regulamento (UE) 2022/2554, as entidades financeiras devem elaborar, documentar e aplicar uma política de gestão dos ativos de TIC.

2. A política de gestão dos ativos de TIC referida no n.º 1 deve:

a) Prescrever a monitorização e gestão do ciclo de vida dos ativos de TIC identificados e classificados em conformidade com o artigo 8.º, n.º 1, do Regulamento (UE) 2022/2554;

b) Prescrever que a entidade financeira mantenha registos de todos os elementos seguintes:

   i) o identificador único de cada ativo de TIC,

   ii) informações sobre a localização, física ou lógica, de todos os ativos de TIC,

   iii) a classificação de todos os ativos de TIC, tal como referido no artigo 8.º, n.º 1, do Regulamento (UE) 2022/2254,

   iv) a identidade dos titulares dos ativos de TIC,

   v) as funções ou serviços operacionais apoiados pelo ativo de TIC,

   vi) os requisitos de continuidade das atividades no domínio das TIC, incluindo os objetivos em termos de tempo de recuperação e ponto de recuperação,

   vii) se o ativo de TIC pode ser ou está exposto a redes externas, designadamente a Internet,

   viii) as ligações e interdependências entre os ativos de TIC e as funções operacionais que utilizam cada ativo de TIC,

   ix) quando aplicável, para todos os ativos de TIC, as datas de termo dos serviços de apoio regulares, alargados e personalizados prestados pelo terceiro prestador de serviços de TIC, após a qual esses ativos de TIC deixam de ser apoiados pelo seu fornecedor ou por um terceiro prestador de serviços de TIC;

c) No caso das entidades financeiras que não sejam microempresas, prescrever que essas entidades financeiras conservem registos das informações necessárias para realizar uma avaliação específica do risco associado às TIC relativamente a todos os sistemas de TIC legados referidos no artigo 8.º, n.º 7, do Regulamento (UE) 2022/2554.

Artigo 5.º

Procedimento de gestão dos ativos de TIC

1. As entidades financeiras devem elaborar, documentar e aplicar um procedimento de gestão dos ativos de TIC.

2. O procedimento de gestão dos ativos de TIC referido no n.º 1 deve especificar os critérios para a realização de uma avaliação do caráter crítico dos ativos de informação e dos ativos de TIC que apoiam funções operacionais. Essa avaliação deve ter em conta:

a) O risco associado às TIC relacionado com essas funções operacionais e as suas dependências em relação aos ativos de informação ou aos ativos de TIC;

b) A forma como a perda de confidencialidade, integridade e disponibilidade desses ativos de informação e ativos de TIC afetaria os processos operacionais e as atividades das entidades financeiras.

Secção 4

Encriptação e criptografia

Artigo 6.º

Encriptação e controlos criptográficos

1. No âmbito das suas políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC a que se refere o artigo 9.º, n.º 2, do Regulamento (UE) 2022/2554, as entidades financeiras devem elaborar, documentar e aplicar uma política em matéria de encriptação e controlos criptográficos.

2. As entidades financeiras devem conceber a política em matéria de encriptação e controlos criptográficos referida no n.º 1 com base nos resultados de uma classificação de dados aprovada e de uma avaliação do risco associado às TIC. Essa política deve conter regras em relação a todos os elementos seguintes:

a) A encriptação dos dados conservados e em trânsito;

b) A encriptação dos dados em utilização, se necessário;

c) A encriptação das ligações à rede interna e do tráfego com partes externas;

d) A gestão de chaves criptográficas a que se refere o artigo 7.º, estabelecendo regras relativas à utilização correta, à proteção e ao ciclo de vida dessas mesmas chaves criptográficas.

Para efeitos da alínea b), caso não seja possível a encriptação dos dados em utilização, as entidades financeiras devem tratar os dados em utilização num ambiente separado e protegido ou tomar medidas equivalentes para garantir a confidencialidade, integridade, autenticidade e disponibilidade dos dados.

3. As entidades financeiras devem incluir na política em matéria de encriptação e controlos criptográficos referida no n.º 1 critérios para a seleção de técnicas criptográficas e práticas de utilização, tendo em conta as melhores práticas e as normas definidas no artigo 2.º, ponto 1, do Regulamento (UE) n.º 1025/2012, e a classificação dos ativos de TIC relevantes estabelecida em conformidade com o artigo 8.º, n.º 1, do Regulamento (UE) 2022/2554. As entidades financeiras que não consigam aderir às melhores práticas ou normas, ou utilizar as técnicas mais fiáveis, devem adotar medidas de mitigação e monitorização que assegurem a resiliência contra ciberameaças.

4. As entidades financeiras devem incluir na política em matéria de encriptação e controlos criptográficos referida no n.º 1 disposições relativas à atualização ou alteração, se necessário, da tecnologia criptográfica com base na evolução da criptoanálise. Essas atualizações ou alterações devem assegurar que a tecnologia criptográfica permanece resiliente às ciberameaças, tal como exigido pelo artigo 10.º, n.º 2, alínea a). As entidades financeiras que não consigam atualizar ou alterar a tecnologia criptográfica devem adotar medidas de mitigação e monitorização que assegurem a resiliência contra ciberameaças.

5. As entidades financeiras devem incluir na política em matéria de encriptação e controlos criptográficos referida no n.º 1 a obrigação de registar a adoção de medidas de mitigação e monitorização em conformidade com os n.ºs 3 e 4 e apresentar uma explicação fundamentada para tal.

Artigo 7.º

Gestão das chaves criptográficas

1. As entidades financeiras devem incluir na política em matéria de gestão das chaves criptográficas referida no artigo 6.º, n.º 2, alínea d), requisitos relativos à gestão das chaves criptográficas ao longo de todo o seu ciclo de vida, nomeadamente a geração, renovação, conservação, criação de cópias de segurança, arquivamento, recuperação, transmissão, retirada, revogação e destruição dessas chaves criptográficas.

2. As entidades financeiras devem identificar e aplicar controlos para proteger as chaves criptográficas ao longo de todo o seu ciclo de vida contra a perda, o acesso não autorizado, a divulgação e a alteração. As entidades financeiras devem conceber esses controlos com base nos resultados da classificação dos dados aprovada e da avaliação do risco associado às TIC.

3. As entidades financeiras devem desenvolver e aplicar métodos para substituir as chaves criptográficas em caso de perda, ou quando essas chaves estejam comprometidas ou danificadas.

4. As entidades financeiras devem criar e manter um registo de todos os certificados e dispositivos de armazenamento de certificados para, pelo menos, os ativos de TIC que apoiam funções críticas ou importantes. As entidades financeiras devem manter esse registo atualizado.

5. As entidades financeiras devem assegurar a rápida renovação dos certificados antes de estes expirarem.

Secção 5

Segurança das operações de TIC

Artigo 8.º

Políticas e procedimentos ao nível do funcionamento das TIC

1. No âmbito das políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC a que se refere o artigo 9.º, n.º 2, do Regulamento (UE) 2022/2554, as entidades financeiras devem elaborar, documentar e aplicar políticas e procedimentos para gerir o funcionamento das TIC. Essas políticas e procedimentos devem especificar a forma como as entidades financeiras operam, monitorizam, controlam e restauram os seus ativos de TIC, incluindo a documentação relativa ao funcionamento das TIC.

2. As políticas e os procedimentos relativos ao funcionamento das TIC referidos no n.º 1 devem incluir todos os elementos seguintes:

a) Uma descrição dos ativos de TIC, incluindo todos os elementos seguintes:

   i) requisitos relativos à instalação, manutenção, configuração e desinstalação seguras de um sistema de TIC,

   ii) requisitos relativos à gestão dos ativos de informação utilizados pelos ativos de TIC, incluindo o seu tratamento, tanto automatizado como manual,

   iii) requisitos relativos à identificação e ao controlo dos sistemas de TIC legados;

b) Controlos e monitorização dos sistemas de TIC, incluindo todos os elementos seguintes:

   i) requisitos relativos a cópias de segurança e restauração dos sistemas de TIC,

   ii) requisitos de calendarização, tendo em conta as interdependências entre os sistemas de TIC,

   iii) protocolos relativos às pistas de auditoria e ao registo de informações no sistema,

   iv) requisitos para assegurar que a realização da auditoria interna e de outros testes causa o mínimo de perturbações nas operações comerciais,

   v) requisitos relativos à separação entre os ambientes de produção de TIC e os ambientes de desenvolvimento, realização de testes e outros ambientes não produtivos,

   vi) requisitos para proceder ao desenvolvimento e à realização de testes em ambientes separados do ambiente de produção,

   vii) requisitos para proceder ao desenvolvimento e à realização de testes em ambientes de produção;

c) Tratamento de erros relativos aos sistemas de TIC, incluindo todos os elementos seguintes:

i) procedimentos e protocolos para o tratamento de erros,

ii) contactos de apoio e de ativação, incluindo contactos externos de apoio em caso de problemas operacionais ou técnicos imprevistos,

iii) procedimentos para reiniciar, retomar e recuperar o sistema de TIC, a utilizar em caso de perturbação desse mesmo sistema.

Para efeitos da alínea b), subalínea v), a separação deve ter em conta todos os componentes do ambiente, incluindo contas, dados ou ligações, conforme exigido pelo artigo 13.º, primeiro parágrafo, alínea a).

Para efeitos da alínea b), subalínea vii), as políticas e os procedimentos referidos no n.º 1 devem prever que os casos em que os testes são realizados num ambiente de produção sejam claramente identificados e fundamentados, sejam realizados por períodos limitados e aprovados pela função pertinente em conformidade com o artigo 16.º, n.º 6. As entidades financeiras devem assegurar a disponibilidade, confidencialidade, integridade e autenticidade dos sistemas de TIC e dos dados de produção durante as atividades de desenvolvimento e teste no ambiente de produção.

Artigo 9.º

Gestão da capacidade e do desempenho

1. No âmbito das políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC a que se refere o artigo 9.º, n.º 2, do Regulamento (UE) 2022/2554, as entidades financeiras devem elaborar, documentar e aplicar procedimentos para gerir a capacidade e o desempenho em relação ao seguinte:

a) A identificação dos requisitos de capacidade dos seus sistemas de TIC;

b) A aplicação da otimização dos recursos;

c) Os procedimentos de monitorização para manter e melhorar:

i) a disponibilidade de dados e os sistemas de TIC,

ii) a eficiência dos sistemas de TIC,

iii) a prevenção da escassez de capacidade no domínio das TIC.

2. Os procedimentos de gestão da capacidade e do desempenho referidos no n.º 1 devem assegurar que as entidades financeiras tomam as medidas adequadas para ter em conta as especificidades dos sistemas de TIC com processos de adjudicação ou aprovação longos ou complexos ou de sistemas de TIC com utilização intensiva de recursos.

Artigo 10.º

Gestão das vulnerabilidades e correções informáticas

1. No âmbito das políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC referidas no artigo 9.º, n.º 2, do Regulamento (UE) 2022/2554, as entidades financeiras devem elaborar, documentar e aplicar procedimentos de gestão das vulnerabilidades.

2. Os procedimentos de gestão das vulnerabilidades referidos no n.º 1 devem:

a) Identificar e atualizar recursos de informação pertinentes e fiáveis para desenvolver e manter a sensibilização para as vulnerabilidades;

b) Assegurar a realização de análises automatizadas da vulnerabilidade e de avaliações dos ativos de TIC, devendo a frequência e o âmbito dessas atividades ser proporcionais à classificação estabelecida em conformidade com o artigo 8.º, n.º 1, do Regulamento (UE) 2022/2554 e ao perfil de risco global do ativo de TIC;

c) Verificar se:

i) os terceiros prestadores de serviços de TIC tratam as vulnerabilidades relacionadas com os serviços de TIC prestados à entidade financeira,

ii) esses prestadores de serviços comunicam atempadamente à entidade financeira, pelo menos, as vulnerabilidades críticas, bem como estatísticas e tendências;

d) Acompanhar a utilização de:

i) bibliotecas de terceiros, incluindo bibliotecas de fonte aberta, utilizadas por serviços de TIC que apoiem funções críticas ou importantes,

ii) serviços de TIC desenvolvidos pela própria entidade financeira ou especificamente personalizados ou desenvolvidos para a entidade financeira por um terceiro prestador de serviços de TIC;

e) Estabelecer procedimentos para a divulgação responsável das vulnerabilidades aos clientes, às contrapartes e ao público;

f) Dar prioridade à implantação de correções e de outras medidas de mitigação para dar resposta às vulnerabilidades identificadas;

g) Monitorizar e verificar a correção das vulnerabilidades;

h) Exigir o registo de quaisquer vulnerabilidades detetadas que afetem os sistemas de TIC e a monitorização da sua resolução.

Para efeitos da alínea b), as entidades financeiras devem realizar, pelo menos semanalmente, uma análise automatizada da vulnerabilidade e avaliações dos ativos de TIC para os ativos de TIC que apoiam funções críticas ou importantes.

Para efeitos da alínea c), as entidades financeiras devem solicitar que os terceiros prestadores de serviços de TIC investiguem as vulnerabilidades relevantes, determinem as causas profundas e apliquem medidas de mitigação adequadas.

Para efeitos da alínea d), as entidades financeiras devem, se for caso disso em colaboração com o terceiro prestador de serviços de TIC, monitorizar a versão e eventuais atualizações das bibliotecas de terceiros. No caso dos ativos de TIC prontos a utilizar (*off-the-shelf*) ou de componentes de ativos de TIC adquiridos e utilizados no funcionamento de serviços de TIC que não apoiem funções críticas ou importantes, as entidades financeiras devem acompanhar a utilização, na medida do possível, das bibliotecas de terceiros, incluindo bibliotecas de fonte aberta.

Para efeitos da alínea f), as entidades financeiras devem ter em conta o caráter crítico da vulnerabilidade, a classificação estabelecida em conformidade com o artigo 8.º, n.º 1, do Regulamento (UE) 2022/2554 e o perfil de risco dos ativos de TIC afetados pelas vulnerabilidades identificadas.

3. No âmbito das políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC a que se refere o artigo 9.º, n.º 2, do Regulamento (UE) 2022/2554, as entidades financeiras devem elaborar, documentar e aplicar procedimentos de gestão das correções.

4. Os procedimentos de gestão das correções referidos no n.º 3 devem:

a) Identificar e avaliar, na medida do possível, as correções e atualizações dos programas informáticos e equipamentos informáticos disponíveis utilizando ferramentas automatizadas;

b) Identificar procedimentos de emergência para a correção e atualização dos ativos de TIC;

c) Testar e implantar as correções dos programas informáticos e dos equipamentos informáticos e as atualizações referidas no artigo 8.º, n.º 2, alínea b), subalíneas v), vi) e vii);

d) Fixar prazos para a instalação de correções e atualizações de programas informáticos e equipamentos informáticos e procedimentos de ativação caso esses prazos não possam ser cumpridos.

Artigo 11.º

Segurança dos dados e do sistema

1. No âmbito das políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC a que se refere o artigo 9.º, n.º 2, do Regulamento (UE) 2022/2554, as entidades financeiras devem elaborar, documentar e aplicar um procedimento de segurança dos dados e do sistema.

2. O procedimento de segurança dos dados e do sistema referido no n.º 1 deve conter todos os elementos indicados a seguir relacionados com a segurança dos dados e do sistema de TIC, de acordo com a classificação estabelecida em conformidade com o artigo 8.º, n.º 1, do Regulamento (UE) 2022/2554:

a) As restrições de acesso referidas no artigo 21.º do presente regulamento, que apoiem os requisitos de proteção para cada nível de classificação;

b) A identificação de uma base de referência de configuração segura para os ativos de TIC que minimize a exposição desses ativos de TIC a ciberameaças e medidas para verificar regularmente se essas bases de referência são efetivamente implantadas;

c) A identificação de medidas de segurança para garantir que apenas sejam instalados programas informáticos autorizados nos sistemas TIC e dispositivos terminais;

d) A identificação de medidas de segurança contra códigos maliciosos;

e) A identificação de medidas de segurança para assegurar que apenas se utilizam suportes externos, sistemas e dispositivos terminais de armazenamento de dados autorizados para transferir e conservar dados da entidade financeira;

f) Os seguintes requisitos para garantir a utilização de dispositivos terminais portáteis e de dispositivos terminais não portáteis privados:

   i) o requisito de utilizar uma solução de gestão para gerir os dispositivos terminais à distância e limpar remotamente os dados da entidade financeira,

   ii) o requisito de utilizar mecanismos de segurança que não possam ser modificados, removidos ou contornados por membros do pessoal ou terceiros prestadores de serviços de TIC de forma não autorizada,

   iii) o requisito de utilizar dispositivos de armazenamento de dados amovíveis apenas se o risco residual associado às TIC permanecer dentro do nível de tolerância ao risco da entidade financeira referido no artigo 3.º, primeiro parágrafo, alínea a);

g) O processo de apagamento seguro de dados, presentes nas instalações da entidade financeira ou conservados externamente, que a entidade financeira já não precisa de recolher nem conservar;

h) O processo de eliminação ou desativação segura de dispositivos de armazenamento de dados presentes nas instalações da entidade financeira ou conservados externamente que contenham informações confidenciais;

i) A identificação e aplicação de medidas de segurança para evitar a perda e fuga de dados de sistemas e dispositivos terminais;

j) A aplicação de medidas de segurança para garantir que o teletrabalho e a utilização de dispositivos terminais privados não têm um impacto negativo na segurança das TIC da entidade financeira;

k) No caso dos ativos ou serviços de TIC operados por um terceiro prestador de serviços de TIC, a identificação e aplicação de requisitos para manter a resiliência operacional digital, de acordo com os resultados da classificação dos dados e da avaliação do risco associado às TIC.

Para efeitos da alínea b), a base de referência da configuração segura referida nessa alínea deve ter em conta as melhores práticas e as técnicas adequadas previstas nas normas definidas no artigo 2.º, ponto 1, do Regulamento (UE) n.º 1025/2012.

Para efeitos da alínea k), as entidades financeiras devem considerar o seguinte:

a) A implementação dos parâmetros recomendados pelo vendedor nos elementos operados pela entidade financeira;

b) Uma repartição clara das funções e responsabilidades em matéria de segurança da informação entre a entidade financeira e o terceiro prestador de serviços de TIC, em conformidade com o princípio da total responsabilidade da entidade financeira em relação ao terceiro prestador de serviços de TIC, referido no artigo 28.º, n.º 1, alínea a), do Regulamento (UE) 2022/2554, no caso das entidades financeiras referidas no artigo 28.º, n.º 2, do mesmo regulamento e de acordo com a política da entidade financeira em matéria de utilização de serviços de TIC que apoiem funções críticas ou importantes;

c) A necessidade de assegurar e manter competências adequadas no seio da entidade financeira na gestão e segurança do serviço utilizado;

d) Medidas técnicas e organizativas para minimizar os riscos relacionados com a infraestrutura utilizada pelo terceiro prestador de serviços de TIC para os seus serviços de TIC, tendo em conta as melhores práticas e as normas definidas no artigo 2.º, ponto 1, do Regulamento (UE) n.º 1025/2012.

Artigo 12.º

Registos

1. No âmbito das salvaguardas contra intrusões e utilização abusiva de dados, as entidades financeiras devem desenvolver, documentar e aplicar procedimentos, protocolos e ferramentas de registo.

2. Os procedimentos, protocolos e ferramentas de registo referidos no n.º 1 devem conter todos os elementos seguintes:

a) A identificação dos eventos a registar, o período de conservação dos registos e as medidas para proteger e tratar os dados dos registos, tendo em conta a finalidade para a qual os registos são criados;

b) O alinhamento do nível de pormenor dos registos com a sua finalidade e utilização, a fim de permitir a deteção eficaz de atividades anómalas, tal como referido no artigo 24.º;

c) O requisito de registar eventos relacionados com todos os elementos seguintes:

   i) controlo lógico e físico do acesso, tal como referido no artigo 21.º, e gestão da identidade,

   ii) gestão da capacidade,

   iii) gestão das alterações,

   iv) funcionamento das TIC, incluindo as atividades dos sistemas de TIC,

   v) atividades de tráfego da rede, incluindo o desempenho da rede de TIC;

d) Medidas para proteger os sistemas de registo e as informações que constam dos registos contra a manipulação, a supressão e o acesso não autorizado aos dados conservados, em trânsito e, se for caso disso, em utilização;

e) Medidas para detetar uma falha nos sistemas de registo;

f) Sem prejuízo de quaisquer requisitos regulamentares aplicáveis ao abrigo do direito da União ou nacional, a sincronização dos relógios de cada um dos sistemas de TIC da entidade financeira com base numa referência temporal fiável e documentada.

Para efeitos da alínea a), as entidades financeiras devem estabelecer o período de conservação, tendo em conta os objetivos empresariais e de segurança da informação, o motivo para registar o evento nos registos e os resultados da avaliação do risco associado às TIC.

Secção 6

Segurança das redes

Artigo 13.º

Gestão da segurança das redes

No âmbito das salvaguardas que garantem a segurança das redes contra intrusões e a utilização abusiva de dados, as entidades financeiras devem desenvolver, documentar e aplicar políticas, procedimentos, protocolos e ferramentas em matéria de gestão da segurança das redes, incluindo todos os elementos seguintes:

a) A segregação e segmentação dos sistemas de TIC e redes, tendo em conta:

   i) o caráter crítico ou a importância da função que esses sistemas de TIC e redes apoiam,

   ii) a classificação estabelecida em conformidade com o artigo 8.º, n.º 1, do Regulamento (UE) 2022/2554,

   iii) o perfil de risco global dos ativos de TIC que utilizam esses sistemas e redes de TIC;

b) A documentação de todas as ligações à rede e fluxos de dados da entidade financeira;

c) A utilização de uma rede separada e específica para a administração dos ativos de TIC;

d) A identificação e implementação de controlos de acesso à rede para prevenir e detetar ligações à rede da entidade financeira por qualquer dispositivo ou sistema não autorizado ou por qualquer terminal que não cumpra os requisitos de segurança da entidade financeira;

e) A encriptação das ligações à rede que passem por redes empresariais, redes públicas, redes domésticas, redes de terceiros e redes sem fios, para os protocolos de comunicação utilizados, tendo em conta os resultados da classificação de dados aprovada, os resultados da avaliação do risco associado às TIC e a encriptação das ligações à rede a que se refere o artigo 6.º, n.º 2;

f) A conceção das redes em consonância com os requisitos de segurança das TIC estabelecidos pela entidade financeira, tendo em conta as melhores práticas para garantir a confidencialidade, integridade e disponibilidade da rede;

g) A segurança do tráfego de rede entre as redes internas e a Internet e outras ligações externas;

h) A identificação das funções e responsabilidades e das etapas para a especificação, aplicação, aprovação, alteração e revisão das regras relativas às barreiras de segurança e aos filtros de ligação;

i) A realização de análises da arquitetura da rede e da conceção da segurança da rede uma vez por ano, e periodicamente para as microempresas, a fim de identificar potenciais vulnerabilidades;

j) As medidas para isolar temporariamente, se necessário, as sub-redes e os componentes e dispositivos de rede;

k) A implementação de uma base de referência para a configuração segura de todos os componentes da rede e o aumento da solidez da rede e dos dispositivos de rede em consonância com as instruções do vendedor, se for caso disso, respeitando as normas aplicáveis, tal como definidas no artigo 2.º, ponto 1, do Regulamento (UE) n.º 1025/2012, e as melhores práticas;

l) Os procedimentos para limitar, bloquear e encerrar o sistema e as sessões à distância após um determinado período de inatividade;

m) Para os acordos de serviços de rede:

   i) a identificação e especificação das medidas de segurança da informação e das TIC, dos níveis de serviço e dos requisitos de gestão de todos os serviços de rede,

   ii) se esses serviços são prestados por um prestador de serviços de TIC intragrupo ou por terceiros prestadores de serviços de TIC.

Para efeitos da alínea h), as entidades financeiras devem proceder regularmente à revisão das regras relativas às barreiras de segurança e aos filtros de ligação, de acordo com a classificação estabelecida em conformidade com o artigo 8.º, n.º 1, do Regulamento (UE) 2022/2554 e com o perfil de risco global dos sistemas de TIC envolvidos. No caso dos sistemas de TIC que suportem funções críticas ou importantes, as entidades financeiras devem verificar a adequação das regras existentes em matéria de barreiras de segurança e dos filtros de ligação, pelo menos, a cada seis meses.

Artigo 14.º

Garantir a segurança das informações em trânsito

1. No âmbito das salvaguardas destinadas a preservar a disponibilidade, autenticidade, integridade e confidencialidade dos dados, as entidades financeiras devem desenvolver, documentar e aplicar as políticas, procedimentos, protocolos e ferramentas para proteger as informações em trânsito. As entidades financeiras devem, em especial, assegurar todos os elementos seguintes:

a) A disponibilidade, autenticidade, integridade e confidencialidade dos dados durante a transmissão na rede e o estabelecimento de procedimentos para avaliar o cumprimento desses requisitos;

b) A prevenção e deteção de fugas de dados e a transferência segura de informações entre a entidade financeira e partes externas;

c) Que os requisitos relativos a acordos de confidencialidade ou de não divulgação que reflitam as necessidades da entidade financeira em matéria de proteção da informação, tanto para o pessoal da entidade financeira como para terceiros, sejam implementados, documentados e revistos regularmente.

2. As entidades financeiras devem conceber as políticas, procedimentos, protocolos e ferramentas para proteger as informações em trânsito referidas no n.º 1 com base nos resultados de uma classificação dos dados aprovada e de uma avaliação do risco associado às TIC.

Secção 7

Gestão das alterações e dos projetos de TIC

Artigo 15.º

Gestão dos projetos de TIC

1. No âmbito das salvaguardas destinadas a preservar a disponibilidade, autenticidade, integridade e confidencialidade dos dados, as entidades financeiras devem desenvolver, documentar e aplicar uma política de gestão dos projetos de TIC.

2. A política de gestão dos projetos de TIC referida no n.º 1 deve especificar os elementos que asseguram a gestão eficaz dos projetos de TIC relacionados com a aquisição, manutenção e, se for caso disso, o desenvolvimento dos sistemas de TIC da entidade financeira.

3. A política de gestão dos projetos de TIC referida no n.º 1 deve conter todos os elementos seguintes:

a) Objetivos dos projetos de TIC;

b) Governação dos projetos de TIC, nomeadamente as funções e as responsabilidades;

c) Planeamento, calendário e etapas dos projetos de TIC;

d) Avaliação dos riscos dos projetos de TIC;

e) Objetivos intermédios relevantes;

f) Requisitos de gestão das alterações;

g) A realização de testes de todos os requisitos, nomeadamente de segurança, e o respetivo processo de aprovação aquando da implantação de um sistema de TIC no ambiente de produção.

4. A política de gestão de projetos de TIC referida no n.º 1 deve assegurar a execução segura dos projetos de TIC através da prestação das informações e dos conhecimentos especializados necessários da área de atividade ou das funções afetadas pelo projeto de TIC.

5. Em conformidade com a avaliação dos riscos dos projetos de TIC referida no n.º 3, alínea d), a política de gestão dos projetos de TIC referida no n.º 1 deve prever que o estabelecimento e os progressos realizados no âmbito dos projetos de TIC com impacto nas funções críticas ou importantes da entidade financeira e os riscos que lhes estão associados sejam comunicados ao órgão de administração do seguinte modo:

a) Individualmente ou de forma agregada, dependendo da importância e da dimensão dos projetos de TIC;

b) Periodicamente e, se necessário, com base em determinados eventos.

Artigo 16.º

Aquisição, desenvolvimento e manutenção dos sistemas de TIC

1. No âmbito das salvaguardas destinadas a preservar a disponibilidade, autenticidade, integridade e confidencialidade dos dados, as entidades financeiras devem desenvolver, documentar e aplicar uma política que regule a aquisição, desenvolvimento e manutenção dos sistemas de TIC. Essa política deve:

a) Identificar as práticas e metodologias de segurança relacionadas com a aquisição, desenvolvimento e manutenção dos sistemas de TIC;

b) Exigir a identificação de:

   i) especificações técnicas e especificações técnicas no domínio das TIC, tal como definidas no artigo 2.º, pontos 4 e 5, do Regulamento (UE) n.º 1025/2012,

   ii) requisitos relativos à aquisição, desenvolvimento e manutenção dos sistemas de TIC, com especial destaque para os requisitos de segurança das TIC e a sua aprovação pela função empresarial competente e pelo titular dos ativos de TIC, de acordo com os mecanismos de governação interna da entidade financeira;

c) Especificar medidas para mitigar o risco de alteração não intencional ou manipulação intencional dos sistemas de TIC durante o desenvolvimento, manutenção e implantação desses sistemas de TIC no ambiente de produção.

2. As entidades financeiras devem desenvolver, documentar e aplicar um procedimento de aquisição, desenvolvimento e manutenção dos sistemas necessários para testar e aprovar todos os sistemas de TIC antes da sua utilização e após manutenção, em conformidade com o artigo 8.º, n.º 2, alínea b), subalíneas v), vi) e vii). O nível dos testes deve ser proporcionado ao caráter crítico dos procedimentos operacionais e dos ativos de TIC em causa. Os testes devem ser concebidos para verificar se os novos sistemas de TIC são adequados ao desempenho pretendido, incluindo a qualidade dos programas informáticos desenvolvidos internamente.

Para além dos requisitos estabelecidos no primeiro parágrafo, as contrapartes centrais devem envolver as seguintes entidades, conforme adequado, na conceção e realização dos testes referidos no primeiro parágrafo:

a) Membros compensadores e clientes;

b) Contrapartes centrais interoperáveis;

c) Outras partes interessadas.

Para além dos requisitos estabelecidos no primeiro parágrafo, as centrais de valores mobiliários devem envolver as seguintes entidades, conforme adequado, na conceção e realização dos testes referidos no primeiro parágrafo:

a) Utilizadores;

b) Prestadores de serviços de utilidade pública críticos e de outros serviços críticos;

c) Outras centrais de valores mobiliários;

d) Outras infraestruturas de mercado;

e) Quaisquer outras instituições com as quais as centrais de valores mobiliários tenham identificado interdependências na sua política de continuidade das atividades.

3. O procedimento referido no n.º 2 deve incluir o desempenho das análises do código-fonte que abranjam testes estáticos e dinâmicos. Esses testes devem incluir testes de segurança para os sistemas e aplicações expostos à Internet, em conformidade com o artigo 8.º, n.º 2, alínea b), subalíneas v), vi) e vii). As entidades financeiras devem:

a) Identificar e analisar as vulnerabilidades e anomalias no código-fonte;

b) Adotar um plano de ação para corrigir essas vulnerabilidades e anomalias;

c) Monitorizar a execução desse plano de ação.

4. O procedimento referido no n.º 2 deve incluir testes de segurança dos pacotes de programas informáticos o mais tardar na fase de integração, em conformidade com o artigo 8.º, n.º 2, alínea b), subalíneas v), vi) e vii).

5. O procedimento referido no n.º 2 deve prever que:

a) Os ambientes não produtivos apenas conservem dados de produção anonimizados, pseudonimizados ou aleatorizados;

b) As entidades financeiras protegem a integridade e a confidencialidade dos dados em ambientes não produtivos.

6. Em derrogação do n.º 5, o procedimento referido no n.º 2 pode prever que os dados relativos à produção sejam conservados apenas para ocasiões específicas de realização de testes, durante períodos limitados e após a aprovação pela função pertinente e a comunicação dessas ocasiões à função de gestão do risco associado às TIC.

7. O procedimento referido no n.º 2 deve incluir a execução de controlos para proteger a integridade do código-fonte dos sistemas de TIC que são desenvolvidos internamente ou por um terceiro prestador de serviços de TIC e entregues à entidade financeira por um terceiro prestador de serviços de TIC.

8. O procedimento referido no n.º 2 deve prever que os programas informáticos patenteados e, sempre que possível, o código-fonte fornecido por terceiros prestadores de serviços de TIC ou proveniente de projetos de fonte aberta, sejam analisados e testados em conformidade com o n.º 3 antes da sua implantação no ambiente de produção.

9. Os n.os 1 a 8 do presente artigo são igualmente aplicáveis aos sistemas de TIC desenvolvidos ou geridos por utilizadores fora da função de TIC, utilizando uma abordagem baseada no risco.

Artigo 17.º

Gestão das alterações das TIC

1. No âmbito das salvaguardas destinadas a preservar a disponibilidade, autenticidade, integridade e confidencialidade dos dados, as entidades financeiras devem incluir nos procedimentos de gestão das alterações das TIC referidos no artigo 9.º, n.º 4, alínea e), do Regulamento (UE) 2022/2554, no que respeita a todas as alterações de programas informáticos, equipamentos informáticos, componentes de microprogramas, sistemas ou parâmetros de segurança, todos os elementos seguintes:

a) Uma verificação do cumprimento dos requisitos de segurança das TIC;

b) Mecanismos para assegurar a independência das funções que aprovam as alterações e das funções responsáveis pelo pedido e pela aplicação dessas alterações;

c) Uma descrição clara das funções e responsabilidades, a fim de assegurar que:

   i) as alterações são especificadas e planeadas,

   ii) foi concebida uma transição adequada,

   iii) as alterações são testadas e concluídas de forma controlada,

   iv) existe uma garantia de qualidade eficaz;

d) A documentação e a comunicação das especificidades das alterações, nomeadamente:

   i) o objetivo e o âmbito da alteração,

   ii) o prazo para a implementação da alteração,

   iii) os resultados esperados;

e) A identificação de procedimentos e responsabilidades alternativos, designadamente procedimentos e responsabilidades para abortar alterações ou recuperar de alterações não implementadas com êxito;

f) Procedimentos, protocolos e ferramentas para gerir alterações de emergência que proporcionem salvaguardas adequadas;

g) Procedimentos para documentar, reavaliar, avaliar e aprovar alterações de emergência após a sua aplicação, incluindo formas de contornar os problemas e implementar correções informáticas;

h) A identificação do potencial impacto de uma alteração nas medidas de segurança das TIC existentes e uma avaliação da necessidade de adotar medidas de segurança das TIC adicionais.

2. Após terem introduzido alterações significativas nos seus sistemas de TIC, as contrapartes centrais e as centrais de valores mobiliários devem submeter os seus sistemas de TIC a testes rigorosos, simulando condições de tensão.

As contrapartes centrais devem envolver as seguintes entidades, conforme adequado, na conceção e realização dos testes referidos no primeiro parágrafo:

a) Membros compensadores e clientes;

b) Contrapartes centrais interoperáveis;

c) Outras partes interessadas.

As centrais de valores mobiliários devem envolver as seguintes entidades, conforme adequado, na conceção e realização dos testes referidos no primeiro parágrafo:

a) Utilizadores;

b) Prestadores de serviços de utilidade pública críticos e de outros serviços críticos;

c) Outras centrais de valores mobiliários;

d) Outras infraestruturas de mercado;

e) Quaisquer outras instituições com as quais as centrais de valores mobiliários tenham identificado interdependências na sua política de continuidade das atividades no domínio das TIC.

SECÇÃO 8

Artigo 18.º

Segurança física e ambiental

1. No âmbito das salvaguardas destinadas a preservar a disponibilidade, autenticidade, integridade e confidencialidade dos dados, as entidades financeiras devem especificar, documentar e aplicar uma política de segurança física e ambiental. As entidades financeiras devem conceber essa política tendo em conta o panorama das ciberameaças, de acordo com a classificação estabelecida nos termos do artigo 8.º, n.º 1, do Regulamento (UE) 2022/2554, e o perfil de risco global dos ativos de TIC e dos ativos de informação acessíveis.

2. A política de segurança física e ambiental referida no n.º 1 deve conter todos os elementos seguintes:

a) Uma referência à secção da política relativa ao controlo da gestão dos direitos do acesso referida no artigo 21.º, primeiro parágrafo, alínea g);

b) Medidas para proteger contra ataques, acidentes e ameaças e perigos ambientais as instalações, os centros de dados da entidade financeira e as áreas consideradas sensíveis identificadas pela entidade financeira onde se encontrem ativos de TIC e ativos de informação;

c) Medidas para garantir a segurança dos ativos de TIC, tanto dentro como fora das instalações da entidade financeira, tendo em conta os resultados da avaliação do risco associado às TIC relacionada com os ativos de TIC pertinentes;

d) Medidas destinadas a garantir a disponibilidade, autenticidade, integridade e confidencialidade dos ativos de TIC, dos ativos de informação e dos dispositivos de controlo do acesso físico da entidade financeira através de uma manutenção adequada;

e) Medidas para preservar a disponibilidade, autenticidade, integridade e confidencialidade dos dados, nomeadamente:

   i) uma política clara em relação à documentação,

   ii) uma política clara de controlo das instalações de tratamento da informação.

Para efeitos da alínea b), as medidas de proteção contra ameaças e perigos ambientais devem ser proporcionadas à importância das instalações, dos centros de dados e das áreas consideradas sensíveis e ao caráter crítico das operações ou dos sistemas de TIC aí localizados.

Para efeitos da alínea c), a política de segurança física e ambiental referida no n.º 1 deve conter medidas destinadas a proporcionar uma proteção adequada aos ativos de TIC sem vigilância.

CAPÍTULO II

Política de recursos humanos e controlo do acesso

Artigo 19.º

Política de recursos humanos

As entidades financeiras devem incluir na sua política de recursos humanos ou noutras políticas relevantes todos os elementos seguintes relacionados com a segurança das TIC:

a) A identificação e atribuição de quaisquer responsabilidades específicas em matéria de segurança das TIC;

b) Os requisitos aplicáveis aos membros do pessoal da entidade financeira e dos terceiros prestadores de serviços de TIC que utilizam ou acedem a ativos de TIC da entidade financeira para:

i) estarem informados e aderirem às políticas, procedimentos e protocolos de segurança das TIC da entidade financeira,

ii) terem conhecimento dos canais de comunicação criados pela entidade financeira para a deteção de comportamentos anómalos, incluindo, se for caso disso, os canais de comunicação estabelecidos em conformidade com a Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho ([11]),

iii) no que toca aos membros do pessoal, devolverem à entidade financeira, após a cessação do contrato de trabalho, todos os ativos de TIC e ativos de informação tangíveis na sua posse que pertençam à entidade financeira.

Artigo 20.º

Gestão da identidade

1. No âmbito do seu controlo da gestão dos direitos de acesso, as entidades financeiras devem desenvolver, documentar e aplicar políticas e procedimentos de gestão da identidade que assegurem a identificação e autenticação únicas das pessoas singulares e dos sistemas que acedem às informações das entidades financeiras, a fim de permitir a atribuição de direitos de acesso aos utilizadores em conformidade com o artigo 21.º.

2. As políticas e os procedimentos relativos à gestão da identidade referidos no n.º 1 devem conter todos os elementos seguintes:

a) Sem prejuízo do artigo 21.º, primeiro parágrafo, alínea c), é atribuída a cada membro do pessoal da entidade financeira ou do pessoal dos terceiros prestadores de serviços de TIC que acedam aos ativos de informação e aos ativos de TIC da entidade financeira uma identidade única correspondente a uma conta de utilizador única;

b) Um processo de gestão do ciclo de vida das identidades e das contas que faça a gestão da criação, alteração, revisão e atualização, desativação temporária e encerramento de todas as contas.

Para efeitos da alínea a), as entidades financeiras devem manter registos de todas as atribuições de identidade. Esses registos devem ser conservados na sequência de uma reorganização da entidade financeira ou após o termo da relação contratual, sem prejuízo dos requisitos de retenção estabelecidos no direito da União e no direito nacional aplicáveis.

Para efeitos da alínea b), as entidades financeiras devem utilizar, sempre que possível e adequado, soluções automatizadas para o processo de gestão da identidade ao longo do ciclo de vida.

Artigo 21.º

Controlo do acesso

No âmbito do seu controlo da gestão dos direitos de acesso, as entidades financeiras devem desenvolver, documentar e aplicar uma política que contenha todos os elementos seguintes:

a) A atribuição de direitos de acesso a ativos de TIC com base nos princípios da necessidade de tomar conhecimento, da necessidade de utilizar e do menor privilégio, nomeadamente para o acesso à distância e de emergência;

b) A segregação de funções destinada a impedir o acesso injustificado a dados críticos ou impedir a atribuição de combinações de direitos de acesso que possam ser utilizadas para contornar os controlos;

c) Uma disposição sobre a responsabilização dos utilizadores, limitando, na medida do possível, a utilização de contas de utilizador genéricas e partilhadas e assegurando que os utilizadores sejam sempre identificáveis nas ações realizadas nos sistemas de TIC;

([11]) Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União (JO L 305 de 26.11.2019, p. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) Uma disposição em matéria de restrições de acesso a ativos de TIC, estabelecendo controlos e ferramentas para impedir o acesso não autorizado;

e) Procedimentos de gestão das contas para conceder, alterar ou revogar direitos de acesso a contas de utilizador e a contas genéricas, nomeadamente contas de administrador genéricas, incluindo disposições relativas a todos os aspetos seguintes:

   i) atribuição de funções e responsabilidades para a concessão, revisão e revogação de direitos de acesso,

   ii) atribuição de acesso privilegiado, de emergência e de administrador com base na necessidade de utilização ou numa base *ad hoc* para todos os sistemas de TIC,

   iii) retirada dos direitos de acesso sem demora injustificada após a cessação do contrato de trabalho ou quando o acesso deixar de ser necessário,

   iv) atualização dos direitos de acesso sempre que sejam necessárias alterações e, pelo menos, uma vez por ano para todos os sistemas de TIC que não sejam sistemas de TIC que apoiem funções críticas ou importantes, e pelo menos a cada seis meses para os sistemas de TIC que apoiem funções críticas ou importantes;

f) Métodos de autenticação, incluindo todos os elementos seguintes:

   i) a utilização de métodos de autenticação proporcionados à classificação estabelecida em conformidade com o artigo 8.º, n.º 1, do Regulamento (UE) 2022/2554 e ao perfil de risco global dos ativos de TIC e tendo em conta as melhores práticas,

   ii) a utilização de métodos de autenticação forte em conformidade com as melhores práticas e técnicas para o acesso remoto à rede da entidade financeira, para o acesso privilegiado e ainda para o acesso a ativos de TIC que apoiem funções críticas ou importantes ou ativos de TIC acessíveis ao público;

g) Medidas de controlo do acesso físico, nomeadamente:

   i) a identificação e o registo de pessoas singulares autorizadas a aceder a instalações, centros de dados e áreas consideradas sensíveis identificadas pela entidade financeira onde se encontrem os ativos de TIC e de informação,

   ii) a concessão de direitos de acesso físico a ativos de TIC críticos apenas a pessoas autorizadas, de acordo com os princípios da necessidade de tomar conhecimento e do menor privilégio, e numa base *ad hoc*,

   iii) a monitorização do acesso físico a instalações, centros de dados e áreas consideradas sensíveis identificadas pela entidade financeira onde se encontrem os ativos de TIC e de informação ou ambos,

   iv) a revisão dos direitos de acesso físico, a fim de assegurar que os direitos de acesso desnecessários são imediatamente revogados.

Para efeitos da alínea e), subalínea i), as entidades financeiras devem estabelecer o período de conservação, tendo em conta os objetivos empresariais e de segurança da informação, o motivo para registar o evento nos registos e os resultados da avaliação do risco associado às TIC.

Para efeitos da alínea e), subalínea ii), as entidades financeiras devem utilizar, sempre que possível, contas específicas para a execução de tarefas administrativas relativas aos sistemas de TIC. Sempre que possível e adequado, as entidades financeiras devem utilizar soluções automatizadas para a gestão do acesso privilegiado.

Para efeitos da alínea g), subalínea i), a identificação e o registo devem ser proporcionados à importância das instalações, dos centros de dados e das áreas consideradas sensíveis e ao caráter crítico das operações ou dos sistemas de TIC aí localizados.

Para efeitos da alínea g), subalínea iii), a monitorização deve ser proporcionada à classificação estabelecida em conformidade com o artigo 8.º, n.º 1, do Regulamento (UE) 2022/2554 e ao caráter crítico da área acedida.

CAPÍTULO III

Deteção e resposta a incidentes relacionados com as TIC

Artigo 22.º

Política de gestão de incidentes relacionados com as TIC

No âmbito dos mecanismos de deteção de atividades anómalas, incluindo problemas de desempenho das redes de TIC e incidentes relacionados com as TIC, as entidades financeiras devem desenvolver, documentar e aplicar uma política em matéria de incidentes relacionados com as TIC através da qual devem:

a) Documentar o processo de gestão de incidentes relacionados com as TIC a que se refere o artigo 17.º do Regulamento (UE) 2022/2554;

b) Estabelecer uma lista de contactos pertinentes com funções internas e partes interessadas externas diretamente envolvidas na segurança das operações de TIC, nomeadamente no que respeita:

   i) à deteção e monitorização de ciberameaças,

   ii) à deteção de atividades anómalas,

   iii) à gestão das vulnerabilidades;

c) Estabelecer, aplicar e operar mecanismos técnicos, organizativos e operacionais para apoiar o processo de gestão de incidentes relacionados com as TIC, incluindo mecanismos que permitam a rápida deteção de atividades e comportamentos anómalos, em conformidade com o artigo 23.º do presente regulamento;

d) Conservar todos os elementos de prova relativos a incidentes relacionados com as TIC durante um período que não exceda o necessário para as finalidades para as quais os dados são recolhidos, proporcionada à criticalidade das funções operacionais, dos processos de apoio e dos ativos de TIC e de informação afetados, em conformidade com o artigo 15.º do Regulamento Delegado (UE) 2024/1772 da Comissão ([12]) e com qualquer requisito de conservação aplicável nos termos do direito da União;

e) Estabelecer e aplicar mecanismos para analisar incidentes e padrões significativos ou recorrentes relacionados com as TIC em termos de número e da ocorrência de incidentes relacionados com as TIC.

Para efeitos da alínea d), as entidades financeiras devem conservar os elementos de prova referidos nessa alínea de forma segura.

Artigo 23.º

Deteção de atividades anómalas e critérios para a deteção e resposta a incidentes relacionados com as TIC

1. As entidades financeiras devem definir funções e responsabilidades claras para detetar e responder eficazmente a incidentes e atividades anómalas relacionados com as TIC.

2. O mecanismo para detetar prontamente atividades anómalas, designadamente problemas de desempenho das redes de TIC e incidentes relacionados com as TIC, tal como referido no artigo 10.º, n.º 1, do Regulamento (UE) 2022/2554, deve permitir às entidades financeiras:

a) Recolher, monitorizar e analisar todos os elementos seguintes:

   i) fatores internos e externos, incluindo, pelo menos, os registos recolhidos em conformidade com o artigo 12.º do presente regulamento, informações provenientes de funções operacionais e de TIC e qualquer problema comunicado pelos utilizadores da entidade financeira,

   ii) potenciais ciberameaças internas e externas, tendo em conta os cenários geralmente utilizados pelos autores de ameaças e os cenários baseados na atividade de informações sobre ameaças,

([12]) Regulamento Delegado (UE) 2024/1772 da Comissão, 13 de março de 2024, que complementa o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação que especificam os critérios de classificação dos incidentes relacionados com as TIC e das ciberameaças, estabelecem limiares de materialidade e especificam os pormenores das notificações dos incidentes de caráter severo (JO L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) notificação de incidentes relacionados com as TIC por parte de um terceiro prestador de serviços de TIC da entidade financeira detetados nos sistemas e redes de TIC do terceiro prestador de serviços de TIC e que possam afetar a entidade financeira;

b) Identificar atividades e comportamentos anómalos e implementar ferramentas geradoras de alertas para atividades e comportamentos anómalos, pelo menos para os ativos de TIC e de informação que apoiem funções críticas ou importantes;

c) Atribuir prioridade aos alertas a que se refere a alínea b), a fim de permitir a gestão dos incidentes relacionados com as TIC detetados dentro do prazo de resolução previsto, conforme especificado pelas entidades financeiras, tanto durante como fora do horário de expediente;

d) Registar, analisar e avaliar, automática ou manualmente, quaisquer informações pertinentes sobre todas as atividades e comportamentos anómalos.

Para efeitos da alínea b), as ferramentas referidas nessa alínea devem incluir as ferramentas que emitem alertas automatizados com base em regras predefinidas para identificar anomalias que afetem a exaustividade e a integridade das fontes de dados ou da recolha de registos.

3. As entidades financeiras devem proteger qualquer registo das atividades anómalas contra a manipulação ilícita e o acesso não autorizado a dados inativos, em trânsito e, se for caso disso, em uso.

4. As entidades financeiras devem registar todas as informações pertinentes para cada atividade anómala detetada que permitam:

a) A identificação da data e da hora da ocorrência da atividade anómala;

b) A identificação da data e da hora de deteção da atividade anómala;

c) A identificação do tipo de atividade anómala.

5. As entidades financeiras devem ter em conta os seguintes critérios para desencadear os processos de deteção e resposta a incidentes relacionados com as TIC a que se refere o artigo 10.º, n.º 2, do Regulamento (UE) 2022/2554:

a) Indicações de que possam ter sido levadas a cabo atividades mal-intencionadas num sistema ou rede de TIC, ou de que esse sistema ou rede de TIC possa ter sido comprometido;

b) Perdas de dados detetadas em relação à disponibilidade, autenticidade, integridade e confidencialidade dos dados;

c) Impacto negativo detetado nas transações e operações da entidade financeira;

d) Indisponibilidade de sistemas e redes de TIC.

6. Para efeitos do n.º 5, as entidades financeiras devem também ter em conta a criticalidade dos serviços afetados.

CAPÍTULO IV

Gestão da continuidade das atividades no domínio das TIC

Artigo 24.º

Componentes da política de continuidade das atividades no domínio das TIC

1. As entidades financeiras devem incluir na sua política de continuidade das atividades no domínio das TIC a que se refere o artigo 11.º, n.º 1, do Regulamento (UE) 2022/2554 todos os elementos seguintes:

a) Uma descrição:

i) dos objetivos da política de continuidade das atividades no domínio das TIC, incluindo a inter-relação entre as TIC e a continuidade global das atividades, e tendo em conta os resultados da análise de impacto na atividade (BIA) a que se refere o artigo 11.º, n.º 5, do Regulamento (UE) 2022/2554,

ii) do âmbito das disposições, planos, procedimentos e mecanismos de continuidade das atividades no domínio das TIC, incluindo limitações e exclusões,

iii) do calendário a abranger pelas disposições, planos, procedimentos e mecanismos de continuidade das atividades no domínio das TIC

iv) dos critérios para ativar e desativar os planos de continuidade das atividades no domínio das TIC, os planos de resposta e recuperação no domínio das TIC e os planos de comunicação em situações de crise;

b) Disposições relativas:

i) à governação e à organização para aplicar a política de continuidade das atividades no domínio das TIC, incluindo funções, responsabilidades e procedimentos escalonados que garantam a disponibilidade de recursos suficientes,

ii) ao alinhamento entre os planos de continuidade das atividades no domínio das TIC e os planos globais de continuidade das atividades, no que respeita, pelo menos, a todos os elementos seguintes:

(1) potenciais cenários de falha, incluindo os cenários referidos no artigo 26.º, n.º 2, do presente regulamento,

(2) objetivos de recuperação, especificando que a entidade financeira deve ser capaz de recuperar as operações das suas funções críticas ou importantes após a ocorrência de perturbações de acordo com um objetivo de tempo de recuperação e um objetivo de ponto de recuperação,

iii) à elaboração de planos de continuidade das atividades no domínio das TIC em caso de perturbações graves das atividades no âmbito desses planos e à atribuição de prioridade às ações de continuidade das atividades no domínio das TIC utilizando uma abordagem baseada no risco,

iv) à elaboração, testes e revisão dos planos de resposta e recuperação no domínio das TIC, em conformidade com os artigos 25.º e 26.º do presente regulamento,

v) à análise da eficácia das disposições, planos, procedimentos e mecanismos de continuidade das atividades no domínio das TIC aplicados, em conformidade com o artigo 26.º do presente regulamento,

vi) ao alinhamento da política de continuidade das atividades no domínio das TIC com:

(1) a política de comunicação a que se refere o artigo 14.º, n.º 2, do Regulamento (UE) 2022/2554,

(2) as ações de comunicação e gestão de crises a que se refere o artigo 11.º, n.º 2, alínea e), do Regulamento (UE) 2022/2554.

2. Para além dos requisitos a que se refere o n.º 1, as contrapartes centrais devem assegurar que a sua política de continuidade das atividades no domínio das TIC:

a) Inclua um tempo máximo de recuperação das suas funções críticas não superior a duas horas;

b) Tenha em conta as ligações e interdependências externas no âmbito das infraestruturas financeiras, incluindo as plataformas de negociação compensadas pela contraparte central, os sistemas de liquidação e pagamento de valores mobiliários e as instituições de crédito utilizadas pela contraparte central ou por uma contraparte central ligada;

c) Exija a adoção de disposições para:

i) assegurar a continuidade das funções críticas ou importantes da contraparte central com base em cenários de catástrofe,

ii) manter um local de tratamento de dados secundário capaz de assegurar a continuidade de funções críticas ou importantes da contraparte central de forma idêntica às do local principal,

iii) manter ou ter acesso imediato a um local de atividade secundário, a fim de permitir que o pessoal assegure a continuidade do serviço se a localização principal da atividade não estiver disponível,

iv) ponderar a necessidade de instalações suplementares de tratamento de dados, em particular se a diversidade dos perfis de risco dos locais primário e secundário não proporcionar confiança suficiente em que os objetivos de continuidade das atividades da contraparte central serão atingidos em todos os cenários.

Para efeitos da alínea a), as contrapartes centrais devem realizar os procedimentos e os pagamentos de fim de dia no dia e na hora devidos em todas as circunstâncias.

Para efeitos da alínea c), subalínea i), as disposições referidas nessa alínea devem abordar a disponibilidade de recursos humanos adequados, o tempo máximo de indisponibilidade de funções críticas, bem como a comutação e recuperação para um local secundário.

Para efeitos da alínea c), subalínea ii), o local de tratamento de dados secundário referido nessa alínea deve ter um perfil de risco geográfico distinto do perfil do local primário.

3. Para além dos requisitos a que se refere o n.º 1, as centrais de depósito de valores mobiliários devem assegurar que a sua política de continuidade das atividades no domínio das TIC:

a) Tenha em conta quaisquer ligações e interdependências com utilizadores, serviços públicos críticos e prestadores de serviços críticos, outras centrais de depósito de valores mobiliários e outras infraestruturas de mercado;

b) Exija que as suas disposições de continuidade das atividades no domínio das TIC assegurem que o objetivo do tempo de recuperação das suas funções críticas ou importantes não seja superior a duas horas.

4. Para além dos requisitos a que se refere o n.º 1, as plataformas de negociação devem garantir que a sua política de continuidade das atividades no domínio das TIC assegure que:

a) A negociação possa ser retomada num período de duas horas ou próximo de duas horas após um incidente que perturbe as atividades;

b) A quantidade máxima de dados que possam ser perdidos em qualquer serviço informático da plataforma de negociação após um incidente que perturbe as atividades seja praticamente nula.

Artigo 25.º

Testes dos planos de continuidade das atividades no domínio das TIC

1. Ao testar os planos de continuidade das atividades no domínio das TIC em conformidade com o artigo 11.º, n.º 6, do Regulamento (UE) 2022/2554, as entidades financeiras devem ter em conta a análise de impacto na atividade (BIA) da entidade financeira e a avaliação do risco associado às TIC a que se refere o artigo 3.º, n.º 1, alínea b), do presente regulamento.

2. As entidades financeiras devem avaliar, através dos testes dos seus planos de continuidade das atividades no domínio das TIC a que se refere o n.º 1, se são capazes de assegurar a continuidade das funções críticas ou importantes da entidade financeira. Esses testes devem:

a) Ser realizados com base em cenários de teste que simulem potenciais perturbações, incluindo um conjunto adequado de cenários graves mas plausíveis;

b) Incluir os testes dos serviços de TIC prestados por terceiros prestadores de serviços de TIC, se for caso disso;

c) No caso de entidades financeiras que não sejam microempresas, como referido no artigo 11.º, n.º 6, segundo parágrafo, do Regulamento (UE) 2022/2554, incluir cenários de passagem entre a infraestrutura primária de TIC e a capacidade redundante, cópias de segurança e equipamentos redundantes;

d) Ser concebidos para desafiar os pressupostos em que se baseiam os planos de continuidade das atividades, incluindo mecanismos de governação e planos de comunicação em situações de crise;

e) Incluir procedimentos para verificar a capacidade do pessoal das entidades financeiras, dos terceiros prestadores de serviços de TIC, dos sistemas de TIC e dos serviços de TIC para responder de forma adequada aos cenários tidos devidamente em conta nos termos do artigo 26.º, n.º 2.

Para efeitos da alínea a), as entidades financeiras devem sempre incluir nos testes os cenários considerados para a elaboração dos planos de continuidade das atividades.

Para efeitos da alínea b), as entidades financeiras devem ter devidamente em conta cenários associados à insolvência ou a falhas dos terceiros prestadores de serviços de TIC ou associados a riscos políticos nas jurisdições dos terceiros prestadores de serviços de TIC, se for caso disso.

Para efeitos da alínea c), os testes devem verificar se é possível executar de forma adequada pelo menos as funções críticas ou importantes durante um período suficiente e se o funcionamento normal pode ser restabelecido.

3. Para além dos requisitos a que se refere o n.º 2, as contrapartes centrais devem envolver as seguintes entidades nos testes dos seus planos de continuidade das atividades no domínio das TIC a que se refere o n.º 1:

a) Membros compensadores;

b) Prestadores externos;

c) Instituições relevantes nas infraestruturas financeiras com as quais as contrapartes centrais tenham identificado interdependências nas suas políticas de continuidade das atividades.

4. Para além dos requisitos a que se refere o n.º 2, as centrais de depósito de valores mobiliários devem envolver as seguintes entidades na testagem dos seus planos de continuidade das atividades no domínio das TIC a que se refere o n.º 1, conforme adequado:

a) Utilizadores das centrais de depósito de valores mobiliários;

b) Prestadores de serviços de utilidade pública críticos e de outros serviços críticos;

c) Outras centrais de valores mobiliários;

d) Outras infraestruturas de mercado;

e) Quaisquer outras instituições com as quais as centrais de valores mobiliários tenham identificado interdependências na sua política de continuidade das atividades.

5. As entidades financeiras devem documentar os resultados dos testes a que se refere o n.º 1. As eventuais deficiências identificadas resultantes desses testes devem ser analisadas, corrigidas e comunicadas ao órgão de administração.

Artigo 26.º

Planos de resposta e recuperação no domínio das TIC

1. Ao elaborar os planos de resposta e recuperação no domínio das TIC a que se refere o artigo 11.º, n.º 3, do Regulamento (UE) 2022/2554, as entidades financeiras devem ter em conta os resultados da análise de impacto na atividade (BIA) da entidade financeira. Esses planos de resposta e recuperação no domínio das TIC devem:

a) Especificar as condições que desencadeiam a sua ativação ou desativação, bem como quaisquer exceções a essa ativação ou desativação;

b) Descrever as medidas a tomar para assegurar a disponibilidade, integridade, continuidade e recuperação, pelo menos, dos sistemas e serviços de TIC que apoiam funções críticas ou importantes da entidade financeira;

c) Ser concebidos de modo a cumprir os objetivos de recuperação das operações das entidades financeiras;

d) Ser documentados e disponibilizados ao pessoal envolvido na execução dos planos de resposta e recuperação no domínio das TIC e ser facilmente acessíveis numa situação de emergência;

e) Prever opções de recuperação a curto e a longo prazo, incluindo a recuperação parcial dos sistemas;

f) Estabelecer os objetivos dos planos de resposta e recuperação no domínio das TIC e as condições para declarar a execução eficaz desses planos.

Para efeitos da alínea d), as entidades financeiras devem especificar claramente as funções e responsabilidades.

2. Os planos de resposta e recuperação no domínio das TIC a que se refere o n.º 1 devem identificar cenários pertinentes, incluindo cenários de perturbações graves da atividade e de maior probabilidade de ocorrência de perturbações. Esses planos devem desenvolver cenários com base nas informações atuais sobre as ameaças e nos ensinamentos retirados de anteriores ocorrências de perturbações da atividade. As entidades financeiras devem ter devidamente em conta todos os cenários seguintes:

a) Ciberataques e transições entre a infraestrutura de TIC primária e a capacidade redundante, cópias de segurança e equipamentos redundantes;

b) Cenários em que a qualidade da prestação de uma função crítica ou importante se deteriore para um nível inaceitável ou falhe, considerando devidamente o potencial impacto da insolvência, ou de outras falhas, de qualquer terceiro prestador de serviços de TIC relevante;

c) Falha total ou parcial das instalações, incluindo instalações administrativas e comerciais, e de centros de dados;

d) Falha substancial dos ativos de TIC ou das infraestruturas de comunicação;

e) Indisponibilidade de um número crítico de pessoal ou de membros do pessoal encarregados de garantir a continuidade das operações;

f) Impacto de eventos relacionados com as alterações climáticas e a degradação do ambiente, catástrofes naturais, pandemias e ataques físicos, incluindo intrusões e ataques terroristas;

g) Ataques internos;

h) Instabilidade política e social, incluindo, se for caso disso, na jurisdição do terceiro prestador de serviços de TIC e no local onde os dados são conservados e tratados;

i) Cortes generalizados de energia.

3. Caso as principais medidas de recuperação possam não ser exequíveis a curto prazo devido a custos, riscos, logística ou circunstâncias imprevistas, os planos de resposta e recuperação no domínio das TIC a que se refere o n.º 1 devem considerar opções alternativas.

4. No âmbito dos planos de resposta e recuperação no domínio das TIC a que se refere o n.º 1, as entidades financeiras devem considerar e aplicar medidas de continuidade para atenuar as falhas de terceiros prestadores de serviços de TIC de apoio a funções críticas ou importantes da entidade financeira.

CAPÍTULO V

Relatório sobre a revisão do quadro de gestão do risco associado às TIC

Artigo 27.º

Formato e conteúdo do relatório sobre a revisão do quadro de gestão do risco associado às TIC

1. As entidades financeiras devem apresentar o relatório sobre a revisão do quadro de gestão do risco associado às TIC a que se refere o artigo 6.º, n.º 5, do Regulamento (UE) 2022/2554 num formato eletrónico pesquisável.

2. As entidades financeiras devem incluir todas as informações seguintes no relatório a que se refere o n.º 1:

a) Uma secção introdutória que:

   i) identifique claramente a entidade financeira objeto do relatório e descreva a sua estrutura de grupo, se aplicável,

   ii) descreva o contexto do relatório em termos da natureza, escala e complexidade dos serviços, atividades e operações da entidade financeira, da sua organização, das funções críticas identificadas, da estratégia, dos projetos ou atividades de envergadura em curso, das relações e da sua dependência de serviços e sistemas de TIC internos e contratados, ou das implicações que uma perda total ou uma degradação grave desses sistemas teria em termos de funções críticas ou importantes e de eficiência do mercado,

   iii) sintetize as principais alterações do quadro de gestão do risco associado às TIC desde o relatório anterior apresentado,

   iv) apresente um resumo do perfil de risco atual e a curto prazo associado às TIC, do panorama das ameaças, da eficácia avaliada dos seus controlos e da postura de segurança da entidade financeira;

b) A data de aprovação do relatório pelo órgão de administração da entidade financeira;

c) Uma descrição do motivo para a revisão do quadro de gestão do risco associado às TIC, em conformidade com o artigo 6.º, n.º 5, do Regulamento (UE) 2022/2554;

d) As datas de início e de termo do período de revisão;

e) Uma indicação da função responsável pela revisão;

f) Uma descrição das principais alterações e melhorias introduzidas no quadro de gestão do risco associado às TIC desde a revisão anterior;

g) Um resumo das conclusões da revisão e da análise e avaliação aprofundadas da gravidade das vulnerabilidades, deficiências e lacunas no quadro de gestão do risco associado às TIC durante o período de revisão;

h) Uma descrição das medidas destinadas a corrigir as vulnerabilidades, deficiências e lacunas, incluindo todos os elementos seguintes:

   i) um resumo das medidas tomadas para identificar as vulnerabilidades, deficiências e lacunas,

   ii) uma data prevista para a aplicação das medidas e as datas relacionadas com o controlo interno da aplicação, incluindo informações sobre o estado de progresso da aplicação dessas medidas à data de elaboração do relatório, explicando, se for caso disso, se existe o risco de os prazos não serem respeitados,

   iii) as ferramentas a utilizar e a identificação da função responsável pela aplicação das medidas, especificando se essas ferramentas e funções são internas ou externas,

   iv) uma descrição do impacto das alterações previstas das medidas relativas aos recursos orçamentais, humanos e materiais da entidade financeira, incluindo os recursos dedicados à aplicação de eventuais medidas corretivas,

   v) informações sobre o processo de informação da autoridade competente, se for caso disso,

   vi) se as vulnerabilidades, deficiências ou lacunas identificadas não forem objeto de medidas corretivas, uma explicação pormenorizada dos critérios utilizados para analisar o impacto dessas vulnerabilidades, deficiências ou lacunas, bem como para avaliar o risco residual associado às TIC, e dos critérios utilizados para aceitar o risco residual conexo;

i) Informações sobre os desenvolvimentos futuros previstos do quadro de gestão do risco associado às TIC;

j) Conclusões decorrentes da revisão do quadro de gestão do risco associado às TIC;

k) Informações sobre revisões anteriores, incluindo:

   i) uma lista das revisões anteriores até à data,

   ii) a situação relativa à aplicação das medidas corretivas identificadas no último relatório, se aplicável,

   iii) caso as medidas corretivas propostas em revisões anteriores se tenham revelado ineficazes ou tenham criado dificuldades imprevistas, uma descrição da forma como essas medidas corretivas podem ser melhoradas ou dessas dificuldades imprevistas;

l) Fontes de informação utilizadas na elaboração do relatório, incluindo todos os elementos seguintes:

   i) no caso das entidades financeiras que não sejam microempresas a que se refere o artigo 6.º, n.º 6, do Regulamento (UE) 2022/2554, os resultados das auditorias internas,

   ii) os resultados das avaliações de conformidade,

   iii) os resultados dos testes de resiliência operacional digital e, se for caso disso, os resultados dos testes avançados, com base em testes de penetração baseados em ameaças (TLPT) às ferramentas, sistemas e processos de TIC,

   iv) fontes externas.

Para efeitos da alínea c), caso a revisão tenha sido iniciada na sequência de instruções de supervisão ou de conclusões decorrentes de testes de resiliência operacional digital ou de processos de auditoria pertinentes, o relatório deve conter referências explícitas a essas instruções ou conclusões, de modo a permitir identificar o motivo para dar início à revisão. Caso a revisão tenha sido iniciada na sequência da ocorrência de incidentes relacionados com as TIC, o relatório deve incluir a lista de todos esses incidentes relacionados com as TIC, juntamente com uma análise das respetivas causas profundas.

Para efeitos da alínea f), a descrição deve incluir uma análise do impacto das alterações na estratégia de resiliência operacional digital da entidade financeira, no quadro de controlo interno das TIC da entidade financeira e na governação da gestão do risco associado às TIC da entidade financeira.

TÍTULO III

QUADRO SIMPLIFICADO DE GESTÃO DO RISCO ASSOCIADO ÀS TIC PARA AS ENTIDADES FINANCEIRAS A QUE SE REFERE O ARTIGO 16.º, N.º 1, DO REGULAMENTO (UE) 2022/2554

CAPÍTULO I

Quadro simplificado de gestão do risco associado às TIC

Artigo 28.º

Governação e organização

1. As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem dispor de um quadro interno de governação e controlo que assegure uma gestão eficaz e prudente do risco associado às TIC, a fim de alcançar um elevado nível de resiliência operacional digital.

2. As entidades financeiras a que se refere o n.º 1 devem assegurar, no âmbito do seu quadro simplificado de gestão do risco associado às TIC, que o seu órgão de administração:

a) Assuma a responsabilidade global de assegurar que o quadro simplificado de gestão do risco associado às TIC permita a consecução da estratégia operacional da entidade financeira, de acordo com a sua apetência pelo risco, e garanta que o risco associado às TIC seja tido em conta nesse contexto;

b) Estabeleça competências e responsabilidades claras para todas as funções relacionadas com as TIC;

c) Defina objetivos de segurança da informação e requisitos em matéria de TIC;

d) Aprove, supervisione e reveja periodicamente:

   i) a classificação dos ativos de informação da entidade financeira a que se refere o artigo 30.º, n.º 1, do presente regulamento, a lista dos principais riscos identificados e a análise do impacto na atividade e políticas conexas,

   ii) os planos de continuidade das atividades da entidade financeira e as medidas de resposta e recuperação a que se refere o artigo 16.º, n.º 1, alínea f), do Regulamento (UE) 2022/2554;

e) Atribua e reveja pelo menos uma vez por ano o orçamento necessário para suprir as necessidades da entidade financeira em matéria de resiliência operacional digital a respeito de todos os tipos de recursos, incluindo programas pertinentes de sensibilização para a segurança das TIC e a formação em matéria de resiliência operacional digital, bem como competências no domínio das TIC para todos os funcionários;

f) Especifique e aplique as políticas e medidas incluídas nos capítulos I, II e III do presente título para identificar, avaliar e gerir o risco associado às TIC a que a entidade financeira está exposta;

g) Identifique e aplique os procedimentos, protocolos de TIC e ferramentas necessários para proteger todos os ativos de informação e de TIC;

h) Garanta a atualização do pessoal da entidade financeira através de conhecimentos e competências suficientes para compreender e avaliar o risco associado às TIC e o seu impacto nas operações da entidade financeira, proporcionados ao risco associado às TIC que é gerido;

i) Estabeleça disposições em matéria de comunicação de informações, incluindo a frequência, a forma e o conteúdo dos relatórios ao órgão de administração sobre a segurança da informação e a resiliência operacional digital.

3. As entidades financeiras a que se refere o n.º 1 podem, em conformidade com o direito da União e o direito setorial nacional, subcontratar as tarefas de verificação do cumprimento dos requisitos de gestão do risco associado às TIC a prestadores de serviços de TIC intragrupo ou a terceiros prestadores de serviços de TIC. Nesse caso, as entidades financeiras continuam a ser plenamente responsáveis pela verificação do cumprimento dos requisitos de gestão do risco associado às TIC.

4. As entidades financeiras a que se refere o n.º 1 devem assegurar a segregação e independência adequadas entre as funções de controlo e de auditoria interna.

5. As entidades financeiras a que se refere o n.º 1 devem assegurar que o seu quadro simplificado de gestão do risco associado às TIC seja objeto de uma auditoria interna por parte de auditores, em conformidade com o plano de auditoria das entidades financeiras. Os auditores devem possuir conhecimentos, competências e especialização suficientes em matéria de risco associado às TIC e ser independentes. A frequência e a ênfase das auditorias às TIC devem ser proporcionadas ao risco associado às TIC da entidade financeira.

6. Com base nas conclusões da auditoria a que se refere o n.º 5, as entidades financeiras a que se refere o n.º 1 devem assegurar a verificação e correção atempadas dos resultados críticos das auditorias às TIC.

Artigo 29.º

Política e medidas de segurança das informações

1. As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem elaborar, documentar e aplicar uma política de segurança das informações no contexto do quadro simplificado de gestão do risco associado às TIC. Essa política de segurança das informações deve especificar os princípios e regras de alto nível para proteger a confidencialidade, integridade, disponibilidade e autenticidade dos dados e dos serviços prestados pelas entidades financeiras.

2. Com base na sua política de segurança das informações a que se refere o n.º 1, as entidades financeiras a que se refere esse número devem estabelecer e aplicar medidas de segurança das TIC para atenuar a sua exposição ao risco associado às TIC, incluindo medidas de atenuação aplicadas por terceiros prestadores de serviços de TIC.

As medidas de segurança das TIC incluem todas as medidas referidas nos artigos 30.º a 38.º.

Artigo 30.º

Classificação dos ativos de informação e dos ativos de TIC

1. No âmbito do quadro simplificado de gestão do risco associado às TIC a que se refere o artigo 16.º, n.º 1, alínea a), do Regulamento (UE) 2022/2554, as entidades financeiras a que se refere o n.º 1 desse artigo devem identificar, classificar e documentar todas as funções críticas ou importantes, os ativos de informação e os ativos de TIC que as apoiam e as respetivas interdependências. As entidades financeiras devem rever essa identificação e classificação conforme necessário.

2. As entidades financeiras a que se refere o n.º 1 devem identificar todas as funções críticas ou importantes apoiadas por terceiros prestadores de serviços de TIC.

Artigo 31.º

Gestão do risco associado às TIC

1. As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem incluir no seu quadro simplificado de gestão do risco associado às TIC todos os elementos seguintes:

a) Uma determinação dos níveis de tolerância ao risco associados às TIC, de acordo com a apetência pelo risco da entidade financeira;

b) A identificação e avaliação dos riscos associados às TIC a que a entidade financeira está exposta;

c) A especificação das estratégias de atenuação, pelo menos para os riscos associados às TIC que não se encontram dentro dos níveis de tolerância ao risco da entidade financeira;

d) O acompanhamento da eficácia das estratégias de atenuação a que se refere a alínea c);

e) A identificação e avaliação de eventuais riscos para a segurança das TIC e da informação decorrentes de alterações importantes do sistema de TIC ou dos serviços, processos ou procedimentos de TIC, bem como dos resultados dos testes de segurança das TIC e após qualquer incidente de caráter severo relacionado com as TIC.

2. As entidades financeiras a que se refere o n.º 1 devem realizar e documentar periodicamente a avaliação do risco associado às TIC, de forma proporcionada ao seu perfil de risco associado às TIC.

3. As entidades financeiras a que se refere o n.º 1 devem monitorizar continuamente as ameaças e vulnerabilidades relevantes para as suas funções críticas ou importantes, bem como os ativos de informação e os ativos de TIC, e rever regularmente os cenários de risco que afetam essas funções críticas ou importantes.

4. As entidades financeiras a que se refere o n.º 1 devem estabelecer limiares de alerta e critérios para desencadear e iniciar processos de resposta a incidentes relacionados com as TIC.

Artigo 32.º

Segurança física e ambiental

1. As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem identificar e aplicar medidas de segurança física elaboradas com base no panorama de ameaças e de acordo com a classificação a que se refere o artigo 30.º, n.º 1, do presente regulamento, com o perfil de risco global dos ativos de TIC e com os ativos de informação acessíveis.

2. As medidas a que se refere o n.º 1 devem proteger as instalações das entidades financeiras e, se for caso disso, os centros de dados das entidades financeiras que detêm os ativos de TIC e os ativos de informação contra acesso não autorizado, ataques e acidentes, bem como contra ameaças e perigos ambientais.

3. A proteção contra ameaças e perigos ambientais deve ser proporcionada à importância das instalações em causa e, se for caso disso, dos centros de dados e da criticalidade das operações ou dos sistemas de TIC aí localizados.

CAPÍTULO II

Outros elementos dos sistemas, protocolos e ferramentas para minimizar o impacto do risco associado às TIC

Artigo 33.º

Controlo do acesso

As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem elaborar, documentar e aplicar procedimentos de controlo do acesso lógico e físico, bem como fazer cumprir, acompanhar e rever periodicamente esses procedimentos. Esses procedimentos devem incluir os seguintes elementos de controlo do acesso lógico e físico:

a) Os direitos de acesso a ativos de informação, ativos de TIC e respetivas funções apoiadas, bem como a locais críticos de funcionamento da entidade financeira, são geridos com base nos princípios da necessidade de conhecer, da necessidade de utilizar e do menor privilégio, nomeadamente para o acesso remoto e de emergência;

b) Responsabilização dos utilizadores, que garanta que os mesmos possam ser identificados no respeitante às ações realizadas nos sistemas de TIC;

c) Procedimentos de gestão de contas para conceder, alterar ou revogar direitos de acesso a contas de utilizador e a contas genéricas, incluindo contas de administrador genéricas;

d) Métodos de autenticação que sejam proporcionados à classificação a que se refere o artigo 30.º, n.º 1, e ao perfil de risco global dos ativos de TIC, e que se baseiem nas melhores práticas;

e) Os direitos de acesso são revistos periodicamente e revogados quando deixarem de ser necessários.

Para efeitos da alínea c), a entidade financeira atribui acesso privilegiado, de emergência e de administrador com base na necessidade de utilizar ou numa base pontual a todos os sistemas de TIC, que deve ser registado em conformidade com o artigo 34.º, primeiro parágrafo, alínea f).

Para efeitos da alínea d), as entidades financeiras devem utilizar métodos de autenticação forte baseados nas melhores práticas para o acesso remoto à rede das entidades financeiras, para o acesso privilegiado e para o acesso a ativos de TIC que apoiam funções críticas ou importantes publicamente disponíveis.

Artigo 34.º

Segurança das operações de TIC

As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem, no âmbito dos seus sistemas, protocolos e ferramentas, e em relação a todos os ativos de TIC:

a) Acompanhar e gerir o ciclo de vida de todos os ativos de TIC;

b) Verificar se os ativos de TIC são apoiados por terceiros prestadores de serviços de TIC de entidades financeiras, se for caso disso;

c) Identificar as necessidades de capacidade dos seus ativos de TIC e as medidas para manter e melhorar a disponibilidade e a eficiência dos sistemas de TIC e evitar défices de capacidade das TIC antes da sua ocorrência;

d) Realizar análises automatizadas das vulnerabilidades e avaliações de ativos de TIC proporcionadas à sua classificação, tal como referido no artigo 30.º, n.º 1, e ao perfil de risco global do ativo de TIC, bem como aplicar correções para resolver as vulnerabilidades identificadas;

e) Gerir os riscos relacionados com ativos de TIC obsoletos, não apoiados ou legados;

f) Registar eventos relacionados com o controlo lógico e físico do acesso e com as operações de TIC, incluindo atividades de tráfego nos sistemas e redes e a gestão de alterações das TIC;

g) Identificar e aplicar medidas para monitorizar e analisar informações sobre atividades e comportamentos anómalos em operações críticas ou importantes no domínio das TIC;

h) Aplicar medidas para monitorizar informações pertinentes e atualizadas sobre as ciberameaças;

i) Aplicar medidas para identificar possíveis fugas de informação, códigos maliciosos e outras ameaças à segurança, bem como vulnerabilidades do conhecimento público em *software* e *hardware*, e verificar se existem novas atualizações de segurança correspondentes.

Para efeitos da alínea f), as entidades financeiras devem alinhar o nível de pormenor dos registos com a sua finalidade e a utilização do ativo de TIC que dá origem a esses registos.

Artigo 35.º

Segurança dos dados, dos sistemas e das redes

As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem, no âmbito dos seus sistemas, protocolos e ferramentas, desenvolver e aplicar salvaguardas que garantam a segurança das redes contra intrusões e a utilização indevida de dados e que preservem a disponibilidade, autenticidade, integridade e confidencialidade dos dados. Em especial, as entidades financeiras, tendo em conta a classificação a que se refere o artigo 30.º, n.º 1, do presente regulamento, devem estabelecer todos os elementos seguintes:

a) A identificação e aplicação de medidas de proteção dos dados em uso, em trânsito e inativos;

b) A identificação e aplicação de medidas de segurança relativas à utilização de *software*, a suportes de armazenamento de dados, bem como a sistemas e dispositivos terminais que transferem e armazenam dados da entidade financeira;

c) A identificação e implementação de medidas para prevenir e detetar ligações não autorizadas à rede da entidade financeira e para proteger o tráfego na rede entre as redes internas da entidade financeira e a Internet e outras ligações externas;

d) A identificação e aplicação de medidas que garantam a disponibilidade, autenticidade, integridade e confidencialidade dos dados durante as transmissões da rede;

e) Um processo de apagamento seguro de dados nas instalações ou armazenados externamente, que a entidade financeira já não tenha necessidade de recolher ou armazenar;

f) Um processo de eliminação ou desativação segura de dispositivos de armazenamento de dados nas instalações ou de dispositivos de armazenamento de dados armazenados externamente que contenham informações confidenciais;

g) A identificação e aplicação de medidas destinadas a assegurar que o teletrabalho e a utilização de dispositivos terminais privados não afetam negativamente a capacidade da entidade financeira para exercer as suas atividades críticas de forma adequada, atempada e segura.

Artigo 36.º

Testes de segurança das TIC

1. As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem estabelecer e aplicar um plano de testes de segurança das TIC para validar a eficácia das suas medidas de segurança das TIC desenvolvido em conformidade com os artigos 33.º, 34.º e 35.º e com os artigos 37.º e 38.º do presente regulamento. As entidades financeiras devem assegurar que esse plano tenha em conta as ameaças e vulnerabilidades identificadas no âmbito do quadro simplificado de gestão do risco associado às TIC a que se refere o artigo 31.º do presente regulamento.

2. As entidades financeiras a que se refere o n.º 1 devem rever, avaliar e testar as medidas de segurança das TIC, tendo em conta o perfil de risco global dos ativos de TIC da entidade financeira.

3. As entidades financeiras a que se refere o n.º 1 devem acompanhar e avaliar os resultados dos testes de segurança e atualizar as suas medidas de segurança em conformidade, sem demora injustificada, no caso dos sistemas de TIC que apoiem funções críticas ou importantes.

Artigo 37.º

Aquisição, desenvolvimento e manutenção dos sistemas de TIC

As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem conceber e aplicar, se for caso disso, um procedimento que regule a aquisição, o desenvolvimento e a manutenção de sistemas de TIC de acordo com uma abordagem baseada no risco. Esse procedimento deve:

a) Assegurar que, antes de qualquer aquisição ou desenvolvimento de sistemas de TIC, os requisitos funcionais e não funcionais, incluindo os requisitos de segurança das informações, sejam claramente especificados e aprovados pela função operacional em causa;

b) Assegurar a realização de testes e a aprovação dos sistemas de TIC antes da sua primeira utilização e antes da introdução de alterações no ambiente de produção;

c) Identificar medidas para atenuar o risco de alteração não intencional ou de manipulação intencional dos sistemas de TIC durante o desenvolvimento e a aplicação no ambiente de produção.

Artigo 38.º

Gestão das alterações e projetos de TIC

1. As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem elaborar, documentar e aplicar um procedimento de gestão de projetos de TIC e especificar as funções e responsabilidades pela sua execução. Esse procedimento deve abranger todas as fases dos projetos de TIC, desde o seu início até ao seu encerramento.

2. As entidades financeiras a que se refere o n.º 1 devem elaborar, documentar e aplicar um procedimento de gestão das alterações das TIC para assegurar que todas essas alterações sejam registadas, testadas, avaliadas, aprovadas, aplicadas e verificadas de forma controlada e com as salvaguardas adequadas para preservar a resiliência operacional digital da entidade financeira.

CAPÍTULO III

Gestão da continuidade das atividades no domínio das TIC

Artigo 39.º

Componentes da política de continuidade das atividades no domínio das TIC

1. As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem elaborar os seus planos de continuidade das atividades no domínio das TIC tendo em conta os resultados da análise das suas exposições a perturbações graves da atividade e do potencial impacto das mesmas, bem como dos cenários a que os seus ativos de TIC que apoiam funções críticas ou importantes possam estar expostos, incluindo um cenário de ciberataque.

2. Os planos de continuidade das atividades a que se refere o n.º 1 devem:

a) Ser aprovados pelo órgão de administração da entidade financeira;

b) Ser documentados e facilmente acessíveis em caso de emergência ou crise;

c) Afetar recursos suficientes para a sua execução;

d) Estabelecer os níveis e prazos de recuperação previstos para a recuperação e o relançamento de funções e as principais dependências internas e externas, nomeadamente em relação a terceiros prestadores de serviços de TIC;

e) Identificar as condições que podem desencadear a ativação dos planos de continuidade das atividades no domínio das TIC e as medidas a tomar para assegurar a disponibilidade, a continuidade e a recuperação dos ativos de TIC de apoio a funções críticas ou importantes das entidades financeiras;

f) Identificar as medidas de restauração e recuperação de funções operacionais críticas ou importantes, processos de apoio, ativos de informação e respetivas interdependências, a fim de evitar efeitos adversos no funcionamento das entidades financeiras;

g) Identificar procedimentos e medidas de salvaguarda que especifiquem o âmbito dos dados abrangidos e a frequência mínima com que são geradas as cópias de segurança, em função da natureza crítica da função que utiliza esses dados;

h) Considerar opções alternativas quando a recuperação possa não ser viável a curto prazo devido a custos, riscos, logística ou circunstâncias imprevistas;

i) Especificar as modalidades de comunicação interna e externa, incluindo os planos de escalonamento;

j) Ser atualizados em consonância com os ensinamentos retirados de incidentes, testes, novos riscos e ameaças identificados, alterações dos objetivos de recuperação, alterações importantes da organização da entidade financeira e dos ativos de TIC que apoiam funções críticas ou operacionais.

Para efeitos da alínea f), as medidas referidas nessa alínea devem prever a atenuação das falhas de terceiros prestadores críticos.

Artigo 40.º

Testes dos planos de continuidade das atividades

1. As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem testar os seus planos de continuidade das atividades a que se refere o artigo 39.º do presente regulamento, incluindo os cenários referidos nesse artigo, pelo menos uma vez por ano no caso dos procedimentos de salvaguarda e restauração, ou em função de qualquer alteração importante do plano de continuidade das atividades.

2. Os testes dos planos de continuidade das atividades a que se refere o n.º 1 devem demonstrar que as entidades financeiras a que se refere esse número são capazes de manter a viabilidade das suas atividades até ao restabelecimento das operações críticas e de identificar eventuais deficiências nesses planos.

3. As entidades financeiras a que se refere o n.º 1 devem documentar os resultados dos testes dos planos de continuidade das atividades, devendo quaisquer deficiências identificadas na sequência desses testes ser analisadas, corrigidas e comunicadas ao órgão de administração.

CAPÍTULO IV

Relatório sobre a revisão do quadro simplificado de gestão do risco associado às TIC

Artigo 41.º

Formato e conteúdo do relatório sobre a revisão do quadro simplificado de gestão do risco associado às TIC

1. As entidades financeiras a que se refere o artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554 devem apresentar o relatório sobre a revisão do quadro de gestão do risco associado às TIC a que se refere o n.º 2 desse artigo num formato eletrónico pesquisável.

2. O relatório a que se refere o n.º 1 deve incluir todas as informações seguintes:

a) Uma secção introdutória que apresente:

   i) uma descrição do contexto do relatório em termos da natureza, escala e complexidade dos serviços, atividades e operações da entidade financeira, da sua organização, das funções críticas identificadas, da estratégia, dos projetos ou atividades de envergadura em curso e das relações e dependência da entidade financeira de serviços e sistemas de TIC internos e subcontratados, ou das implicações que uma perda total ou uma degradação grave desses sistemas teria nas funções críticas ou importantes e na eficiência do mercado,

   ii) um resumo do perfil de risco atual e a curto prazo associado às TIC identificado, do panorama de ameaças, da eficácia avaliada dos seus controlos e da postura de segurança da entidade financeira,

   iii) informações sobre o domínio notificado,

   iv) um resumo das principais alterações do quadro de gestão do risco associado às TIC desde o relatório anterior,

   v) um resumo e uma descrição do impacto das principais alterações do quadro simplificado de gestão do risco associado às TIC desde o relatório anterior;

b) A data de aprovação do relatório pelo órgão de administração da entidade financeira, se aplicável;

c) Uma descrição dos motivos da revisão, incluindo:

   i) caso a revisão tenha sido iniciada de acordo com instruções de supervisão, elementos comprovativos dessas instruções,

   ii) caso a revisão tenha sido iniciada na sequência da ocorrência de incidentes relacionados com as TIC, a lista de todos esses incidentes relacionados com as TIC, juntamente com uma análise das causas profundas de incidentes conexos;

d) A data do início e do termo do período de revisão;

e) A pessoa responsável pela revisão;

f) Um resumo das conclusões e uma autoavaliação da gravidade das vulnerabilidades, deficiências e lacunas identificadas no quadro de gestão do risco associado às TIC no período de revisão, incluindo uma análise pormenorizada das mesmas;

g) Medidas corretivas identificadas para resolver as vulnerabilidades, deficiências e lacunas do quadro simplificado de gestão do risco associado às TIC, bem como a data prevista para a aplicação dessas medidas, incluindo o seguimento das vulnerabilidades, deficiências e lacunas identificadas em relatórios anteriores, sempre que essas vulnerabilidades, deficiências e lacunas ainda não tenham sido corrigidas;

h) Conclusões gerais sobre a revisão do quadro simplificado de gestão do risco associado às TIC, incluindo eventuais desenvolvimentos futuros.

TÍTULO IV

DISPOSIÇÕES FINAIS

Artigo 42.º

Entrada em vigor

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 13 de março de 2024.

Pela Comissão
A Presidente
Ursula VON DER LEYEN