REGULAMENTO DELEGADO (UE) 2025/1190 DA COMISSÃO

de 13 de fevereiro de 2025

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 utilizados para identificar as entidades financeiras obrigadas a realizar testes de penetração baseados em ameaças, os requisitos e normas que regem a utilização de testadores internos, os requisitos relativos ao âmbito, metodologia e abordagem para cada uma das fases de realização dos testes, os resultados, as fases de conclusão e de correção e o tipo de cooperação em matéria de supervisão e outra cooperação relevante e necessária para a realização dos TLPT e para facilitar o reconhecimento mútuo

(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 26.º, n.º 11, quarto parágrafo,

Considerando o seguinte:

(1) O presente regulamento foi elaborado em conformidade com o quadro TIBER-EU e reflete a metodologia, o processo e a estrutura dos testes de penetração baseados em ameaças (TLPT), tal como descrito no TIBER-EU. As entidades financeiras sujeitas aos TLPT podem referenciar ou aplicar o quadro TIBER-EU, ou uma das respetivas aplicações nacionais, na medida em que esse quadro ou essas aplicações sejam coerentes com os requisitos estabelecidos nos artigos 26.º e 27.º do Regulamento (UE) 2022/2554 e no presente regulamento. A designação de uma única autoridade pública do setor financeiro responsável pelas questões relacionadas com os TLPT a nível nacional, em conformidade com o artigo 26.º, n.º 9, do Regulamento (UE) 2022/2554, não deverá prejudicar a competência das autoridades competentes confiada a nível da União para a supervisão de determinadas entidades financeiras nos termos do artigo 46.º desse regulamento, como por exemplo o Banco Central Europeu, para as instituições de crédito significativas, que devem ser consideradas competentes para as questões relacionadas com os TLPT. Se apenas algumas das funções relacionadas com os TLPT forem delegadas noutra autoridade nacional do setor financeiro nos termos do artigo 26.º, n.º 10, do Regulamento (UE) 2022/2554, a autoridade competente da entidade financeira a que se refere o artigo 46.º desse regulamento deve continuar a ser a autoridade responsável pelas funções relacionadas com os TLPT que não tenham sido delegadas.

(2) Tendo em conta a complexidade dos TLPT e os riscos que lhes estão associados, a sua utilização deve ser limitada às entidades financeiras para as quais se justifica. Por conseguinte, as autoridades responsáveis pelas questões relativas aos TLPT (autoridades TLPT, quer a nível da União quer a nível nacional) devem excluir do âmbito dos TLPT as entidades financeiras que operam em subsetores com serviços financeiros fundamentais para os quais não se justifica a sua realização. Tal significa que as instituições de crédito, as instituições de pagamento e de moeda eletrónica, as centrais de valores mobiliários, as contrapartes centrais, as plataformas de negociação e as empresas de seguros e de resseguros, mesmo que cumpram os critérios quantitativos, podem ser dispensadas do requisito de realização de TLPT à luz de uma avaliação global do seu perfil de risco e da sua maturidade no domínio das TIC, do impacto no setor financeiro e de preocupações conexas em matéria de estabilidade financeira.

(3) As autoridades TLPT devem avaliar, à luz de uma apreciação global do perfil de risco e da maturidade no domínio das TIC, do impacto no setor financeiro, bem como de preocupações conexas em matéria de estabilidade financeira, se qualquer outro tipo de entidade financeira que não as instituições de crédito, instituições de pagamento, instituições de moeda eletrónica, contrapartes centrais, centrais de valores mobiliários, plataformas de negociação e empresas de seguros e de resseguros deve ser sujeito à realização de TLPT. A avaliação para determinar se essas entidades financeiras cumprem os referidos critérios qualitativos deve ter como objetivo identificar as entidades financeiras para as quais é adequado realizar os TLPT, utilizando indicadores intersetoriais e objetivos. Ao mesmo tempo, a avaliação para determinar se uma entidade financeira cumpre esses critérios qualitativos deve limitar as entidades

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

sujeitas aos TLPT àquelas para as quais os testes se justificam. A questão de saber se uma entidade financeira cumpre esses critérios qualitativos deve também ser avaliada à luz do desenvolvimento de novos mercados e da importância crescente dos novos intervenientes no mercado para o setor financeiro no futuro, incluindo os prestadores de serviços de criptoativos autorizados em conformidade com o artigo 59.º do Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho ([2]).

(4) As entidades financeiras podem ter um mesmo prestador de serviços de TIC intragrupo ou pertencer a um mesmo grupo e utilizar sistemas de TIC partilhados. Nesse caso, é importante que as autoridades TLPT tenham em conta a estrutura e o caráter sistémico ou a importância dessa entidade financeira para o setor financeiro a nível nacional ou da União quando avaliam se deve ser sujeita aos TLPT e se esses TLPT devem ser realizados a nível da entidade ou a nível do grupo (através de um TLPT conjunto).

(5) Para refletir o quadro TIBER-EU, é necessário que a metodologia dos testes preveja o envolvimento dos principais participantes indicados a seguir: a entidade financeira, com uma equipa de controlo (que reflete a «equipa de controlo» do quadro TIBER-EU) e uma equipa azul (que reflete a «equipa azul» do quadro TIBER-EU), e a autoridade TLPT, sob a forma de uma equipa cibernética TLPT (que reflete as «equipas cibernéticas TIBER» do quadro TIBER-EU), um prestador de informações sobre as ameaças e testadores (testadores esses que refletem o «prestador da equipa vermelha» do quadro TIBER-EU).

(6) A fim de assegurar que os TLPT beneficiam da experiência desenvolvida no âmbito da aplicação do TIBER-EU e de reduzir os riscos associados à realização dos TLPT, importa garantir que as responsabilidades das equipas cibernéticas TLPT que serão criadas a nível das autoridades TLPT correspondem tão estreitamente quanto possível às das equipas cibernéticas do quadro TIBER-EU. Por conseguinte, as equipas cibernéticas dos TLPT devem ter gestores dos testes responsáveis pela supervisão dos TLPT individuais e pelo planeamento e coordenação dos testes individuais. As equipas cibernéticas dos TLPT devem servir de ponto de contacto único para a comunicação relacionada com os testes às partes interessadas internas e externas, para a recolha e o tratamento das observações e ensinamentos retirados dos testes realizados anteriormente e para o apoio às entidades financeiras submetidas aos testes TLPT.

(7) A fim de refletir a metodologia do quadro TIBER-EU, os gestores dos testes devem dispor das competências e capacidades necessárias para prestar aconselhamento e contestar as propostas dos testadores. A experiência no âmbito do quadro TIBER-EU demonstrou que é útil dispor de uma equipa de pelo menos dois gestores dos testes para cada teste. A fim de refletir que os TLPT são utilizados para incentivar a experiência de aprendizagem, as autoridades TLPT, a menos que tenham problemas de recursos ou de conhecimentos especializados, são fortemente incentivadas a ter em conta que, no decurso de um TLPT, os gestores dos testes não devem exercer atividades de supervisão referentes à mesma entidade financeira sujeita a um TLPT, de modo a salvaguardar a confidencialidade dos testes.

(8) Por razões de coerência com o quadro TIBER-EU, é importante que a autoridade TLPT acompanhe de perto todas as fases dos testes. Tendo em conta a natureza dos testes e os riscos que lhes estão associados, é fundamental que a autoridade TLPT esteja envolvida em cada fase específica dos testes. A autoridade TLPT deve, em particular, ser consultada e validar as avaliações ou decisões das entidades financeiras que possam, por um lado, influenciar a eficácia do teste e, por outro, ter impacto nos riscos associados ao teste. As etapas fundamentais em que é necessária uma participação específica da autoridade TLPT incluem a validação de determinados documentos fundamentais dos testes, bem como a seleção dos prestadores de informações sobre as ameaças e testadores e das medidas de gestão dos riscos. A participação das autoridades TLPT, especialmente nas validações, não deve resultar num encargo excessivo para essas autoridades, devendo por conseguinte limitar-se à documentação e às decisões que afetam diretamente a realização dos TLPT. Através da participação ativa em cada fase dos testes, as autoridades TLPT podem avaliar eficazmente a conformidade das entidades financeiras com os requisitos pertinentes, o que deverá permitir a emissão, por parte dessas autoridades, dos comprovativos referidos no artigo 26.º, n.º 7, do Regulamento (UE) 2022/2554.

([2]) Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho, de 31 de maio de 2023, relativo aos mercados de criptoativos e que altera os Regulamentos (UE) n.º 1093/2010 e (UE) n.º 1095/2010 e as Diretivas 2013/36/UE e (UE) 2019/1937 (JO L 150 de 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) O sigilo dos TLPT é da maior importância para garantir que as condições dos testes sejam realistas. Por esse motivo, os testes devem ser secretos e devem ser tomadas precauções para manter a confidencialidade dos TLPT, incluindo a escolha dos nomes de código que devem ser criados para impedir a identificação dos TLPT por terceiros. Se os membros do pessoal responsáveis pela segurança da equipa financeira tiverem conhecimento de um TLPT planeado ou em curso, é provável que estejam mais atentos e alerta do que em condições normais de trabalho, o que alterará o resultado dos testes. Por conseguinte, os membros do pessoal da entidade financeira que não fazem parte da equipa de controlo só devem ser informados de quaisquer TLPT planeados ou em curso se existirem motivos convincentes para o fazer e mediante o acordo prévio dos gestores dos testes, nomeadamente para garantir o sigilo do teste caso um membro da equipa azul tenha detetado as atividades de teste.

(10) Tal como demonstrado pela experiência adquirida no quadro do TIBER-EU no que respeita à «equipa de controlo», a seleção de um chefe de equipa adequado para a equipa de controlo é indispensável para a realização segura dos TLPT. O chefe da equipa de controlo deve possuir a autoridade necessária no seio da entidade financeira para orientar todos os aspetos dos testes, sem comprometer a sua confidencialidade. Pela mesma razão, os membros da equipa de controlo devem ter um conhecimento profundo da entidade financeira, das funções profissionais e posicionamento estratégico do chefe da equipa de controlo, possuir a antiguidade exigida e ter acesso ao conselho de administração. Para reduzir o risco de comprometer os TLPT, a equipa de controlo deve ser o mais pequena possível.

(11) Existem elementos de risco inerentes aos TLPT, uma vez que as funções críticas são testadas num ambiente de produção «ao vivo», o que pode causar incidentes de negação de serviço, falhas inesperadas do sistema, danos em sistemas críticos de produção «ao vivo» ou a perda, alteração ou divulgação de dados. Esses riscos sublinham a necessidade de medidas de gestão dos riscos sólidas. A fim de assegurar que os TLPT são realizados de forma controlada durante todo o período de testes, é muito importante que as entidades financeiras estejam sempre cientes dos riscos específicos que surgem num TLPT e que esses riscos sejam atenuados. A este respeito, sem prejuízo dos processos internos da entidade financeira e das responsabilidades e delegações já atribuídas ao chefe da equipa de controlo, pode ser adequado fornecer informações sobre as medidas de gestão dos riscos dos TLPT ou, em casos específicos, assegurar a aprovação dessas medidas de gestão de riscos pelo próprio órgão de administração da entidade financeira. Para poderem prestar serviços profissionais eficazes e mais qualificados e reduzir esses riscos, é também essencial que os testadores e os prestadores de informações sobre as ameaças (em conjunto, os prestadores TLPT) possuam o mais elevado nível de competências, conhecimentos especializados e experiência adequada em matéria de informações sobre as ameaças e os TLPT no setor dos serviços financeiros.

(12) Os testes de penetração convencionais proporcionam uma avaliação pormenorizada e útil das vulnerabilidades técnicas e de configuração, frequentemente de um único sistema ou ambiente de forma isolada, mas, ao contrário dos testes da equipa vermelha com base em informações, não avaliam o cenário completo de um ataque direcionado contra a entidade no seu conjunto, incluindo todos os seus funcionários, processos e tecnologias. Durante o processo de seleção dos prestadores TLPT, as entidades financeiras devem, assim, assegurar que esses prestadores possuem as competências necessárias para realizar testes da equipa vermelha com base em informações, e não apenas testes de penetração. Por conseguinte, é necessário estabelecer critérios abrangentes para os testadores, tanto internos como externos, e para os prestadores de informações sobre as ameaças, que são sempre externos. Se os prestadores TLPT pertencerem à mesma empresa, o pessoal afetado a um TLPT deve ser adequadamente separado.

(13) Pode haver circunstâncias excecionais em que as entidades financeiras não possam contratar prestadores TLPT que cumpram os critérios abrangentes. Assim, as entidades financeiras, após comprovarem a indisponibilidade desses prestadores de informações sobre as ameaças, deverão ser autorizadas a contratar pessoas que não preencham todos os critérios abrangentes, desde que atenuem adequadamente quaisquer riscos adicionais daí resultantes e que a autoridade TLPT avalie todos esses critérios.

(14) Sempre que várias entidades financeiras e várias autoridades TLPT estejam envolvidas num TLPT, há que especificar as funções de todas as partes no processo do TLPT por forma a garantir que seja o mais eficiente e seguro possível. Para efeitos dos testes agrupados, são necessários requisitos específicos para especificar o papel da entidade financeira designada, nomeadamente o facto de que será responsável por fornecer toda a documentação necessária à autoridade TLPT principal e pelo acompanhamento do processo do teste. A entidade financeira designada deverá também ser responsável pelos aspetos comuns da avaliação da gestão dos riscos. Não obstante o papel da entidade financeira designada, as obrigações de cada entidade financeira participante no processo de TLPT agrupado não devem ser afetadas durante a realização desse teste. Aplica-se o mesmo princípio aos TLPT conjuntos.

(15) Tal como demonstrado pela experiência adquirida com a aplicação do quadro TIBER-EU, a realização de reuniões presenciais ou virtuais que incluam todas as partes interessadas (entidades financeiras, autoridades, testadores e prestadores de informações sobre as ameaças) é a forma mais eficiente de assegurar a realização adequada dos testes. Por conseguinte, devem ser realizadas reuniões presenciais e virtuais em várias fases do processo, em especial durante a fase de preparação do lançamento do TLPT, para delimitar o seu âmbito, durante a fase de testes, para finalizar o relatório de informações sobre as ameaças e o plano de testes da equipa vermelha e para as atualizações semanais, bem como durante a fase de conclusão, para reproduzir as ações dos testadores e da equipa azul, para proceder à associação de equipas (equipa roxa) e para trocar observações sobre o TLPT.

(16) A fim de assegurar o bom desempenho dos TLPT, a autoridade TLPT deve apresentar claramente à entidade financeira as suas expectativas em relação aos testes. A este respeito, os gestores dos testes devem assegurar o estabelecimento de um fluxo adequado de informações com a equipa de controlo na entidade financeira e com os prestadores TLPT.

(17) A entidade financeira deve selecionar as funções críticas ou importantes que serão abrangidas pelos TLPT. Ao selecionar essas funções, a entidade financeira deve basear-se em vários critérios relacionados com a importância de cada função para a própria entidade financeira e para o setor financeiro, a nível da União e a nível nacional, não só em termos económicos como também tendo em conta a natureza simbólica ou política da função. A fim de facilitar uma transição harmoniosa para a fase de recolha de informações sobre as ameaças, a equipa de controlo deve fornecer aos testadores e ao prestador de informações sobre as ameaças que não estejam envolvidos no processo de delimitação do âmbito informações pormenorizadas sobre a delimitação acordada.

(18) A fim de fornecer aos testadores as informações necessárias para simular um ataque realista aos sistemas «ao vivo» da entidade financeira subjacentes às suas funções críticas ou importantes, o prestador de informações sobre as ameaças deve recolher informações que abranjam pelo menos dois domínios de interesse fundamentais: os alvos, identificando potenciais superfícies de ataque em toda a entidade financeira, e as ameaças, identificando os autores relevantes e os cenários prováveis de ameaça. A fim de assegurar que o prestador de informações sobre as ameaças tem em conta as ameaças relevantes para a entidade financeira, os testadores, a equipa de controlo e os gestores dos testes devem apresentar as suas observações sobre o projeto de relatório de informações sobre as ameaças. O prestador de informações sobre as ameaças pode utilizar, se estiver disponível, um cenário de ameaças genérico fornecido pela autoridade TLPT para o setor financeiro de um Estado-Membro como referência para o cenário de ameaças nacional. Com base na aplicação do quadro TIBER-EU, o processo de recolha de informações sobre as ameaças dura normalmente cerca de quatro semanas.

(19) Para que os testadores possam conhecer e rever mais aprofundadamente o documento de especificação do âmbito e o relatório de informações específicas sobre as ameaças para finalizarem o plano de testes da equipa vermelha, é essencial que, antes da fase de testes da equipa vermelha do TLPT, os testadores recebam do prestador de informações explicações pormenorizadas quanto ao relatório de informações específicas sobre as ameaças e uma análise dos possíveis cenários de ameaça.

(20) A fim de permitir que os testadores realizem testes realistas e abrangentes, em que todas as fases de ataque são executadas e os alertas são desencadeados, deve ser atribuído tempo suficiente à fase ativa dos testes da equipa vermelha. Com base na experiência adquirida com o quadro TIBER-EU, o tempo atribuído deve ser de pelo menos 12 semanas e deve ser determinado tendo em conta o número de partes envolvidas, o âmbito dos TLPT, os recursos da entidade ou entidades financeiras envolvidas, quaisquer requisitos externos e a disponibilidade das informações de apoio fornecidas pela entidade financeira.

(21) Durante a fase ativa dos testes da equipa vermelha, os testadores devem utilizar uma série de táticas, técnicas e procedimentos (TTP) para testar adequadamente os sistemas de produção «ao vivo» da entidade financeira. Os TTP devem conter, consoante o caso, o reconhecimento (ou seja, a recolha do maior número possível de informações sobre um alvo), a instrumentalização (ou seja, a análise das informações sobre as infraestruturas, as instalações e os trabalhadores e a preparação das operações especificamente destinadas ao alvo visado), a execução (ou seja, o lançamento ativo da operação completa sobre o alvo), a exploração (ou seja, as situações em que o objetivo dos testadores é comprometer os servidores e as redes da entidade financeira e explorar o seu pessoal através da engenharia social), o controlo e movimento (ou seja, tentativas de passar dos sistemas comprometidos para outros mais vulneráveis ou de elevado valor) e as ações relativas ao alvo (ou seja, obter maior acesso aos sistemas comprometidos e acesso às informações e dados acordados anteriormente no âmbito do plano de testes da equipa vermelha).

(22) Ao realizarem um TLPT, os testadores devem atuar tendo em conta o tempo disponível para realizar o ataque, os recursos utilizados e os limites éticos e jurídicos. Caso os testadores não consigam avançar para a próxima fase programada do ataque, a equipa de controlo deverá prestar assistência ocasional, mediante acordo da autoridade TLPT, sob a forma de «ajudas». As ajudas podem, de um modo geral, ser categorizadas em informações e ajudas ao acesso e podem consistir na disponibilização de acesso a sistemas de TIC ou redes internas para que o teste possa prosseguir e centrar-se nas etapas de ataque seguintes.

(23) Durante a fase ativa dos testes da equipa vermelha, se tal for necessário para permitir a continuação do TLPT como último recurso, em circunstâncias excecionais e uma vez esgotadas todas as opções alternativas, deve ser utilizada uma atividade de teste colaborativa que envolva tanto os testadores como a equipa azul. No contexto deste exercício limitado de associação de equipas (equipa roxa), podem ser utilizados os seguintes métodos: «captura e libertação», em que os testadores tentam dar seguimento aos cenários, são detetados e, em seguida, retomam o teste, «jogos de guerra», que permite cenários mais complexos para testar a tomada de decisões estratégicas, ou «prova de conceito colaborativa», que permite que os testadores e os membros da equipa azul validem conjuntamente medidas, ferramentas ou técnicas de segurança específicas num ambiente controlado e cooperativo.

(24) Os TLPT devem ser utilizados como experiência de aprendizagem para reforçar a resiliência operacional digital das entidades financeiras. A este respeito, a equipa azul e os testadores devem reproduzir o ataque e rever as medidas tomadas para retirar ilações dos testes em colaboração com os testadores. Para o efeito, e a fim de permitir uma preparação adequada, os relatórios de testes da equipa vermelha e da equipa azul devem ser disponibilizados a todas as partes envolvidas nas atividades de reprodução dos ataques, antes da realização de quaisquer dessas atividades. Além disso, na fase de conclusão, deve ser realizado um exercício de associação de equipas (equipa roxa) para maximizar a experiência de aprendizagem. Os métodos que podem ser utilizados para a associação de equipas (equipa roxa) na fase de conclusão devem incluir a discussão de cenários de ataque alternativos, a exploração dos sistemas «ao vivo» dos cenários alternativos ou a reexploração de cenários planeados em sistemas «ao vivo» que os testadores não tenham podido concluir ou executar durante a fase de testes.

(25) A fim de facilitar ainda mais a experiência de aprendizagem de todas as partes envolvidas nos TLPT, em prol de testes futuros, e reforçar a resiliência operacional digital das entidades financeiras, as partes em causa devem trocar observações sobre o processo global e, em especial, identificar quais as atividades que decorreram de forma positiva ou poderiam ter sido melhoradas e que aspetos do processo TLPT funcionaram bem ou poderiam ser melhorados.

(26) As autoridades competentes referidas no artigo 46.º do Regulamento (UE) 2022/2554 e as autoridades TLPT, caso sejam diferentes, devem cooperar para incorporar testes avançados através dos TLPT nos processos de supervisão existentes. A este respeito, e a fim de partilhar a correta compreensão das conclusões dos TLPT e da forma como devem ser interpretadas, é conveniente que, em especial no que respeita ao relatório de síntese dos testes e aos planos corretivos, seja estabelecida uma estreita cooperação entre os gestores dos testes que participaram nos TLPT e os supervisores responsáveis.

(27) Nos termos do artigo 26.º, n.º 8, primeiro parágrafo, do Regulamento (UE) 2022/2554, as entidades financeiras devem contratar testadores externos de três em três testes. Sempre que as entidades financeiras incluam testadores internos e externos na equipa, deve considerar-se, para efeitos do referido artigo, que um TLPT é realizado com testadores internos.

(28) O presente regulamento tem por base os 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 concertação com o Banco Central Europeu.

(29) As Autoridades Europeias de Supervisão realizaram consultas públicas abertas sobre os projetos de normas técnicas de regulamentação que estão na base do presente regulamento, analisaram os potenciais custos e benefícios associados e solicitaram 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 Parlamento Europeu e do Conselho ([3]), 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 do Parlamento Europeu e do Conselho ([4]), 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 do Parlamento Europeu e do Conselho ([5]).

(30) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([6]) e emitiu parecer em 20 de agosto de 2024,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Equipa de controlo»: a equipa composta por pessoal da entidade financeira testada e, se for caso disso tendo em conta o âmbito do TLPT, por pessoal dos seus terceiros prestadores de serviços e de qualquer outra parte, envolvidos na gestão do teste;

2) «Chefe da equipa de controlo»: o membro do pessoal da entidade financeira responsável pela realização de todas as atividades relacionadas com o TLPT para a entidade financeira no contexto de um determinado teste;

3) «Equipa azul»: o pessoal da entidade financeira e, se for caso disso, dos terceiros prestadores de serviços da entidade financeira e de qualquer outra parte considerada relevante tendo em conta o âmbito dos TLPT, que defende a vertente da utilização das redes e dos sistemas de informação por uma entidade financeira mantendo a sua posição de segurança contra ataques simulados ou reais e que não tem conhecimento do TLPT;

4) «Funções da equipa azul»: as funções tipicamente realizadas pela equipa azul, tais como o centro de operações de segurança, os serviços das infraestruturas das TIC, os serviços de assistência e os serviços de gestão de incidentes a nível operacional;

5) «Equipa vermelha»: os testadores, internos ou externos, contratados para um TLPT ou afetados ao mesmo;

6) «Associação de equipas (equipa roxa)»: uma atividade de teste colaborativa que envolve tanto os testadores como a equipa azul;

([3]) 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).

([4]) 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).

([5]) 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).

([6]) 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).

7) «Autoridade TLPT»: qualquer uma das seguintes entidades:

   a) A autoridade pública única para o setor financeiro designada em conformidade com o artigo 26.º, n.º 9, do Regulamento (UE) 2022/2554,

   b) A autoridade do setor financeiro na qual é delegado o exercício de algumas ou de todas as funções relacionadas com os TLPT, em conformidade com o artigo 26.º, n.º 10, do Regulamento (UE) 2022/2554,

   c) Qualquer uma das autoridades competentes a que se refere o artigo 46.º do Regulamento (UE) 2022/2554;

8) «Equipa cibernética TLPT» ou «TCT»: o pessoal das autoridades TLPT responsável pelas questões relacionadas com os TLPT;

9) «Gestores dos testes»: o pessoal designado para liderar as atividades da autoridade TLPT destinadas a controlar o cumprimento do presente regulamento para um TLPT específico;

10) «Prestador de informações sobre as ameaças»: os peritos, contratados pela entidade financeira para cada TLPT e externos à entidade financeira e aos prestadores de serviços de TIC intragrupo, se for caso disso, que recolhem e analisam informações específicas sobre as ameaças pertinentes para as entidades financeiras no âmbito de um exercício específico de TLPT e desenvolvem os correspondentes cenários de ameaça pertinentes e realistas;

11) «Prestadores TLPT»: os testadores e os prestadores de informações sobre as ameaças;

12) «Ajudas»: a assistência ou as informações fornecidas pela equipa de controlo aos testadores para que estes possam continuar a executar uma via de ataque caso não consigam fazê-lo autonomamente e quando não exista outra alternativa razoável, nomeadamente por falta de tempo ou recursos num determinado TLPT;

13) «Via de ataque»: a trajetória seguida pelos testadores durante a fase ativa dos testes da equipa vermelha dos TLPT para desencadear os alertas especificados para esse TLPT;

14) «Alertas»: os objetivos fundamentais nos sistemas de TIC que apoiam funções críticas ou importantes de uma entidade financeira que os testadores tentam desencadear através do teste;

15) «Informações sensíveis»: informações que podem ser facilmente aproveitadas para realizar ataques contra os sistemas de TIC da entidade financeira, propriedade intelectual, dados comerciais confidenciais ou dados pessoais, que podem direta ou indiretamente prejudicar a entidade financeira e o seu ecossistema se caírem nas mãos de intervenientes mal-intencionados;

16) «Agrupamento»: todas as entidades financeiras que participam num TLPT agrupado nos termos do artigo 26.º, n.º 4, do Regulamento (UE) 2022/2554;

17) «Estado-Membro de acolhimento»: o Estado-Membro de acolhimento em conformidade com o direito setorial da União aplicável a cada entidade financeira;

18) «TLPT conjunto»: um TLPT, que não seja um TLPT agrupado a que se refere o artigo 26.º, n.º 4, do Regulamento (UE) 2022/2554, que envolva várias entidades financeiras que utilizem o mesmo prestador de serviços de TIC intragrupo ou pertençam ao mesmo grupo e partilhem sistemas de TIC.

Artigo 2.º

Identificação das entidades financeiras obrigadas a realizar TLPT

1. As autoridades TLPT devem avaliar se uma entidade financeira é obrigada a realizar TLPT, tendo em conta o impacto dessas entidades financeiras, o caráter sistémico das mesmas e o seu perfil de risco associado às TIC, com base em todos os critérios indicados a seguir:

a) Fatores relacionados com o impacto e o caráter sistémico:

   i) a dimensão da entidade financeira, determinada com base no facto de a entidade financeira prestar serviços financeiros num ou mais Estados-Membros e comparando as atividades da entidade financeira com as de outras entidades financeiras que prestam serviços semelhantes,

   ii) a extensão e a natureza da interligação da entidade financeira com outras entidades financeiras do setor financeiro num ou mais Estados-Membros,

   iii) o caráter crítico ou a importância dos serviços que a entidade financeira presta ao setor financeiro,

iv) a possibilidade de substituição dos serviços prestados pela entidade financeira,

v) a complexidade do modelo de negócios da entidade financeira e dos serviços e processos conexos,

vi) se a entidade financeira faz parte de um grupo de caráter sistémico a nível da União ou nacional no setor financeiro que partilha sistemas de TIC;

b) Fatores relacionados com o risco associado às TIC:

i) o perfil de risco da entidade financeira,

ii) o cenário de ameaças da entidade financeira,

iii) o grau de dependência das funções críticas ou importantes ou respetivas funções de apoio da entidade financeira em relação a sistemas e processos de TIC,

iv) a complexidade da arquitetura das TIC da entidade financeira,

v) os serviços e funções de TIC apoiados por terceiros prestadores de serviços de TIC e a quantidade e o tipo de acordos contratuais com terceiros prestadores de serviços de TIC ou prestadores de serviços de TIC intragrupo,

vi) os resultados de quaisquer análises de supervisão relevantes para a avaliação da maturidade das TIC da entidade financeira,

vii) a maturidade dos planos de continuidade das atividades no domínio das TIC e dos planos de resposta e recuperação no domínio das TIC,

viii) a maturidade das medidas operacionais de deteção e mitigação no domínio da segurança das TIC, incluindo a capacidade de:

1) Monitorizar permanentemente a infraestrutura de TIC da entidade financeira;

2) Detetar eventos relacionados com as TIC em tempo real;

3) Analisar os eventos referidos no ponto 2;

4) Responder aos eventos referidos no ponto 2 de forma atempada e eficaz,

ix) se a entidade financeira faz parte de um grupo ativo no setor financeiro a nível da União ou a nível nacional que partilha sistemas de TIC.

Para efeitos da alínea a), subalínea i), a autoridade TLPT deve, sempre que possível, considerar:

a) A posição em termos de quota de mercado da entidade financeira a nível da União e a nível nacional,

b) O leque de atividades oferecidas pela entidade financeira,

c) A quota de mercado dos serviços prestados pela entidade financeira ou das atividades realizadas a nível da União e a nível nacional;

Para efeitos da alínea a), subalínea v), a autoridade TLPT deve, sempre que possível, considerar:

a) Se a entidade financeira tem mais do que um modelo de negócios,

b) A interligação dos diferentes processos operacionais e dos serviços conexos.

2. As autoridades TLPT devem exigir que todas as entidades financeiras indicadas a seguir realizem TLPT, a menos que a avaliação a que se refere o n.º 1 relativamente a uma entidade financeira indique que o seu impacto, as preocupações em matéria de estabilidade financeira relacionadas com essa entidade financeira ou o seu perfil de risco associado às TIC não justificam a realização de um TLPT:

a) Instituições de crédito que preencham qualquer uma das seguintes condições:

i) tenham sido identificadas como instituições de importância sistémica global (G-SII) em conformidade com o artigo 131.º da Diretiva 2013/36/UE do Parlamento Europeu e do Conselho ([7]),

ii) tenham sido identificadas como outras instituições de importância sistémica (O-SII) em conformidade com o artigo 131.º da Diretiva 2013/36/UE,

iii) façam parte de uma G-SII ou de O-SII;

([7]) Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176 de 27.6.2013, p. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) instituições de pagamento que excederam, em cada um dos dois anos civis anteriores à avaliação pela autoridade TLPT, 150 mil milhões de EUR de valor total das operações de pagamento na aceção do artigo 4.º, ponto 5, da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho ([8]);

c) Instituições de moeda eletrónica que excederam, em cada um dos dois anos civis anteriores à avaliação pela autoridade TLPT, 150 mil milhões de EUR de valor total das operações de pagamento na aceção do artigo 4.º, ponto 5, da Diretiva (UE) 2015/2366 ou 40 mil milhões de EUR de valor total do montante de moeda eletrónica em circulação;

d) Centrais de valores mobiliários;

e) Contrapartes centrais;

f) Plataformas de negociação com um sistema de negociação eletrónico que preencham qualquer um dos seguintes critérios:

i) a plataforma de negociação teve a quota de mercado mais elevada em termos de volume de negócios a nível nacional em cada um dos dois anos civis anteriores à avaliação pela autoridade TLPT em qualquer dos seguintes casos:

1) Valores mobiliários na aceção do artigo 4.º, n.º 1, ponto 44, alínea a), da Diretiva 2014/65/UE do Parlamento Europeu e do Conselho ([9]);

2) Valores mobiliários na aceção do artigo 4.º, n.º 1, ponto 44, alínea b), da Diretiva 2014/65/UE;

3) Derivados na aceção do artigo 2.º, n.º 1, ponto 29, do Regulamento (UE) n.º 600/2014 do Parlamento Europeu e do Conselho ([10]);

4) Produtos financeiros estruturados na aceção do artigo 2.º, n.º 1, ponto 28, do Regulamento (UE) n.º 600/2014;

5) Licenças de emissão na aceção do anexo I, secção C, ponto 11, da Diretiva 2014/65/UE,

ii) a plataforma de negociação teve uma quota de mercado em termos de volume de negócios a nível da União que ultrapassa os 5 % em cada um dos dois anos civis anteriores à avaliação pela autoridade TLPT em qualquer dos seguintes casos:

1) Ações de sociedades e outros títulos equivalentes a ações de sociedades, de sociedades de responsabilidade ilimitada, parcerias ou de outras entidades, bem como certificados de depósito de ações;

2) Obrigações ou outras formas de dívida titularizada, incluindo certificados de depósito de tais títulos;

3) Derivados na aceção do artigo 2.º, n.º 1, ponto 29, do Regulamento (UE) n.º 600/2014;

4) Produtos financeiros estruturados na aceção do artigo 2.º, n.º 1, ponto 28, do Regulamento (UE) n.º 600/2014;

5) Licenças de emissão na aceção do anexo I, secção C, ponto 11, da Diretiva 2014/65/UE;

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

([9]) Diretiva 2014/65/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa aos mercados de instrumentos financeiros e que altera a Diretiva 2002/92/CE e a Diretiva 2011/61/UE (JO L 173 de 12.6.2014, p. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) 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).

g) Empresas de seguros e de resseguros que preencham cumulativamente os seguintes critérios:

i) prémios brutos emitidos superiores a 1 500 000 000 EUR,

ii) provisões técnicas superiores a 10 000 000 000 EUR,

iii) empresas de seguros que exercem apenas atividades de seguro de vida ou que exercem cumulativamente atividades de seguro de vida e não vida e que têm um total de ativos superior a 3,5 % da soma dos ativos totais, avaliados em conformidade com o artigo 75.º da Diretiva 2009/138/CE do Parlamento Europeu e do Conselho ([11]), das empresas de seguros e de resseguros estabelecidas no Estado-Membro;

Para efeitos da alínea f), subalínea ii), se a plataforma de negociação fizer parte de um grupo que partilha sistemas de TIC ou o mesmo prestador de serviços de TIC intragrupo, deve ser tido em conta o volume de negócios dos contratos de valores mobiliários e derivados em todas as plataformas de negociação pertencentes ao mesmo grupo e estabelecidas na União.

Para efeitos da alínea g), as autoridades TLPT devem identificar um subconjunto de todas as empresas de seguros e de resseguros aplicando os critérios estabelecidos na alínea g), subalíneas i), ii) e iii). As empresas de seguros e de resseguros incluídas nesse subconjunto são obrigadas a realizar TLPT se preencherem igualmente qualquer um dos seguintes critérios:

a) Prémios brutos emitidos superiores a 3 000 000 000 EUR;

b) Provisões técnicas superiores a 30 000 000 000 EUR;

c) Ativos totais que excedam 10 % da soma dos ativos totais, avaliados em conformidade com o artigo 75.º da Diretiva 2009/138/CE, das empresas de seguros e de resseguros estabelecidas no Estado-Membro.

3. Se mais do que uma entidade financeira pertencente ao mesmo grupo e que partilha sistemas de TIC, ou mais do que uma entidade financeira que utiliza o mesmo prestador de serviços de TIC intragrupo, preencher os critérios estabelecidos no n.º 2, as autoridades TLPT dessas entidades financeiras devem decidir, nos termos do artigo 16.º, n.º 2, se o requisito de realização de TLPT numa base individual se aplica a essas entidades financeiras.

Se a autoridade TLPT da empresa-mãe de um grupo de entidades financeiras a que se refere o primeiro parágrafo for diferente das autoridades TLPT das entidades financeiras do grupo, essa autoridade deve ser consultada pelas autoridades TLPT das entidades financeiras pertencentes a esse grupo sobre a conveniência de realizar TLPT numa base individual.

Artigo 3.º

TCT e gestores dos testes dos TLPT

1. Uma autoridade TLPT deve atribuir a responsabilidade pela coordenação das atividades relacionadas com os TLPT a uma TCT. Uma TCT é composta pelos gestores dos testes designados para supervisionar um TLPT individual.

2. Para cada teste, a autoridade TLPT deve designar um gestor dos testes e, pelo menos, um suplente.

3. Os gestores dos testes devem monitorizar e assegurar o cumprimento dos requisitos estabelecidos no presente regulamento.

([11]) Diretiva 2009/138/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, relativa ao acesso à atividade de seguros e resseguros e ao seu exercício (Solvência II) (JO L 335 de 17.12.2009, p. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. O gestor dos testes deve comunicar os dados de contacto da TCT à entidade financeira através da notificação a que se refere o artigo 9.º, n.º 1.

5. A autoridade TLPT deve participar em todas as fases dos TLPT.

Artigo 4.º

Disposições organizativas aplicáveis às entidades financeiras

1. As entidades financeiras devem nomear uma equipa de controlo que será responsável pela gestão corrente do TLPT e pelas decisões e ações da equipa de controlo.

2. As entidades financeiras devem estabelecer medidas organizativas e processuais para assegurar que:

a) O acesso às informações relativas a qualquer TLPT planeado ou em curso é limitado, com base na necessidade de conhecer, à equipa de controlo, ao órgão de administração, aos testadores, ao prestador de informações sobre as ameaças e à autoridade TLPT;

b) A equipa de controlo consulta os gestores dos testes antes de envolver qualquer membro da equipa azul num TLPT;

c) A equipa de controlo é informada de qualquer deteção do TLPT por membros do pessoal da entidade financeira ou dos seus terceiros prestadores de serviços; em caso de propagação da reação a incidentes daí resultante a equipa de controlo contém, se necessário, essa propagação;

d) Estão em vigor disposições relativas ao sigilo dos TLPT, aplicáveis ao pessoal da entidade financeira, ao pessoal dos terceiros prestadores de serviços de TIC em causa, aos testadores e ao prestador de informações sobre as ameaças;

e) A equipa de controlo fornece aos gestores dos testes, mediante pedido, todas as informações relativas aos TLPT;

f) Sempre que possível, as partes envolvidas no TLPT mencionam-no apenas pelo nome de código.

Artigo 5.º

Gestão dos riscos associados aos TLPT

1. Durante a fase de preparação a que se refere o artigo 9.º, a equipa de controlo deve avaliar os riscos associados aos testes dos sistemas de produção «ao vivo» de funções críticas ou importantes da entidade financeira, nomeadamente os potenciais impactos sobre:

a) O setor financeiro;

b) A estabilidade financeira a nível da União ou a nível nacional.

A equipa de controlo deve analisar esses impactos ao longo dos testes.

2. Para efeitos da avaliação e gestão dos riscos, a equipa de controlo deve ter em conta, pelo menos, os seguintes tipos de riscos relacionados com:

a) A concessão de acesso a informações sensíveis sobre a entidade financeira ao prestador de informações sobre as ameaças e aos testadores externos, se for caso disso;

b) A falta de conformidade dos TLPT com o Regulamento (UE) 2022/2554 e com o presente regulamento, se essa falta de conformidade resultar na falta do comprovativo referido no artigo 26.º, n.º 7, do Regulamento (UE) 2022/2554, nomeadamente quando essa falta de conformidade se dever a violações da confidencialidade do TLPT ou a uma conduta não ética;

c) A propagação dos incidentes e crises;

d) A fase ativa da equipa vermelha, nomeadamente os riscos relacionados com a interrupção de atividades críticas e a corrupção de dados devido às atividades dos testadores, bem como os seus potenciais impactos em terceiros;

e) A atividade da equipa azul, nomeadamente os riscos relacionados com a interrupção de atividades críticas e a corrupção de dados devido às suas atividades, bem como os seus potenciais impactos em terceiros;

f) A restauração incompleta dos sistemas afetados pelo TLPT.

Artigo 6.º

Gestão de riscos associados aos TLPT agrupados ou conjuntos

1. No caso de um TLPT conjunto ou de um TLPT agrupado, a equipa de controlo de cada entidade financeira deve realizar a sua própria avaliação dos riscos e estabelecer as suas próprias medidas de gestão dos riscos.

2. A equipa de controlo da entidade financeira designada a que se refere o artigo 16.º, n.º 3, alínea b), do presente regulamento, ou a entidade financeira designada em conformidade com o artigo 26.º, n.º 4, do Regulamento (UE) 2022/2554, deve avaliar os riscos relacionados com a participação de várias entidades financeiras nos TLPT. As equipas de controlo das entidades financeiras envolvidas devem cooperar com a equipa de controlo da entidade financeira designada para identificar potenciais riscos conjuntos.

Artigo 7.º

Seleção dos prestadores TLPT

1. A equipa de controlo deve tomar medidas para gerir os riscos relacionados com os TLPT e assegurar, em especial, que, para cada TLPT:

a) O prestador de informações sobre as ameaças e os testadores externos fornecem à equipa de controlo um *curriculum vitae* pormenorizado e cópias das certificações que, de acordo com as normas de mercado reconhecidas, são adequadas para o desempenho das suas atividades;

b) O prestador de informações sobre as ameaças e os testadores externos estão devida e totalmente cobertos por seguros de indemnização profissional adequados, nomeadamente contra riscos de conduta irregular e negligência;

c) O prestador de informações sobre as ameaças fornece pelo menos três referências de missões anteriores no contexto de testes de penetração e dos testes da equipa vermelha;

d) Os testadores externos fornecem pelo menos cinco referências de missões anteriores relacionadas com testes de penetração e testes da equipa vermelha;

e) O pessoal do prestador de informações sobre as ameaças afetado ao TLPT:

   i) é composto por pelo menos um gestor com pelo menos cinco anos de experiência em informações sobre as ameaças e pelo menos um membro adicional com pelo menos dois anos de experiência em informações sobre as ameaças,

   ii) apresenta um vasto leque e um nível adequado de conhecimentos e competências profissionais, nomeadamente:

      1) Táticas, técnicas e procedimentos de recolha de informações;

      2) Conhecimentos geopolíticos, técnicos e setoriais;

      3) Competências de comunicação adequadas para apresentar e comunicar claramente os resultados do trabalho,

   iii) tem uma participação combinada em pelo menos três missões anteriores de informações sobre as ameaças no contexto de testes de penetração e testes da equipa vermelha,

   iv) não executa simultaneamente quaisquer tarefas da equipa azul ou outros serviços que possam constituir um conflito de interesses no que respeita à entidade financeira, à entidade terceira prestadora de serviços no domínio das TIC ou a um prestador de serviços de TIC intragrupo envolvido em TLPT a que esteja afetado,

   v) está separado do pessoal do mesmo prestador TLPT que fornece testes externos para o mesmo TLPT e não presta contas a esse pessoal;

f) Para os testadores externos, a equipa vermelha afetada ao TLPT:

i) é composta por pelo menos um gestor com pelo menos cinco anos de experiência em testes de penetração e testes da equipa vermelha, bem como por pelo menos dois testadores adicionais, cada um com pelo menos dois anos de experiência em testes de penetração e testes da equipa vermelha,

ii) apresenta um vasto leque e um nível adequado de conhecimentos e competências profissionais, nomeadamente conhecimentos sobre a atividade da entidade financeira, o reconhecimento e a gestão dos riscos, o desenvolvimento de exploração, a penetração física, a engenharia social, a análise das vulnerabilidades, bem como competências de comunicação adequadas para apresentar e comunicar claramente o resultado do trabalho,

iii) teve uma participação combinada em pelo menos cinco missões anteriores relacionadas com testes de penetração e testes da equipa vermelha,

iv) não foi contratada nem presta serviços a um prestador de informações sobre as ameaças que desempenhe simultaneamente funções na equipa azul de uma entidade financeira, um terceiro prestador de serviços de TIC ou um prestador de serviços de TIC intragrupo que esteja envolvido no TLPT,

v) é separada de qualquer pessoal do mesmo prestador TLPT que preste simultaneamente serviços de informações sobre as ameaças para o mesmo TLPT;

g) Os testadores e o prestador de informações sobre as ameaças realizam procedimentos de restauração no final dos testes, incluindo a supressão segura de informações relacionadas com senhas, credenciais e outras chaves secretas comprometidas durante o TLPT, a comunicação segura às entidades financeiras das contas comprometidas, bem como a recolha, armazenamento, gestão e eliminação seguros de outros dados recolhidos durante os testes;

h) Os testadores, para além dos procedimentos de restauração no final do teste a que se refere a alínea g), realizam os seguintes procedimentos de restauração:

i) desativação do comando e controlo,

ii) determinação do âmbito e da data dos dispositivos de segurança (*kill switches*),

iii) remoção de portas de acesso não autorizadas e de outros programas maliciosos,

iv) notificação de potenciais violações,

v) procedimentos para a futura restauração de cópias de segurança que possam dizer respeito a programas maliciosos ou ferramentas instalados durante o teste,

vi) monitorização das atividades da equipa azul e informação à equipa de controlo sobre eventuais deteções;

i) Os testadores e o prestador de informações sobre as ameaças não realizam nem participam em nenhuma das seguintes atividades:

i) destruição não autorizada de equipamento da entidade financeira e dos seus terceiros prestadores de serviços de TIC, se for caso disso,

ii) modificação não controlada das informações e dos ativos de TIC da entidade financeira e dos seus terceiros prestadores de serviços de TIC, se for caso disso,

iii) perturbação intencional da continuidade de funções críticas ou importantes da entidade financeira,

iv) inclusão não autorizada de sistemas fora do âmbito de aplicação,

v) divulgação não autorizada dos resultados dos testes.

2. A equipa de controlo deve manter um registo da documentação facultada pelos testadores e pelos fornecedores de informações sobre as ameaças, para comprovar o cumprimento do disposto no n.º 1, alíneas a) a f).

Em circunstâncias excecionais, as entidades financeiras podem contratar testadores externos e prestadores de informações sobre as ameaças que não cumpram um ou mais dos requisitos estabelecidos no n.º 1, alíneas a) a f), desde que essas entidades financeiras adotem medidas adequadas para atenuar os riscos relacionados com o incumprimento dessas alíneas e registem essas medidas.

Artigo 8.º

Especificidades dos TLPT agrupados ou conjuntos

1. Salvo decisão em contrário da autoridade TLPT principal, caso várias entidades financeiras, identificadas em conformidade com o artigo 16.º, n.ºs 2 ou 4, estejam envolvidas num TLPT agrupado ou conjunto, cada entidade financeira deve seguir cada uma das etapas estabelecidas nos artigos 9.º a 15.º.

2. Salvo disposição em contrário do presente regulamento, caso várias autoridades TLPT estejam envolvidas num TLPT conjunto ou num TLPT agrupado, tal como referido no artigo 16.º, n.ºs 3 ou 5, as referências nos artigos 9.º a 15.º à «autoridade TLPT» devem ser entendidas como referências à autoridade TLPT principal para esses TLPT agrupados ou conjuntos.

Artigo 9.º

Fase de preparação

1. Uma entidade financeira identificada nos termos do artigo 26.º, n.º 8, terceiro parágrafo, do Regulamento (UE) 2022/2554 deve dar início a um TLPT na sequência de uma notificação da autoridade TLPT nesse sentido.

2. Uma entidade financeira deve, no prazo de três meses a contar da receção da notificação a que se refere o n.º 1, apresentar aos gestores dos testes todas as informações indicadas a seguir relativamente ao lançamento do TLPT:

a) Uma carta de projeto que inclua um plano de projeto de alto nível, contendo as informações previstas no anexo I;

b) Os dados de contacto do chefe da equipa de controlo;

c) As informações sobre a utilização prevista de testadores internos ou externos, ou ambos, se for caso disso, conforme especificado no artigo 15.º;

d) As informações sobre os canais de comunicação a utilizar durante o TLPT;

e) O nome de código do TLPT.

3. Se as informações referidas no n.º 2, alíneas a) a e), estiverem completas e garantirem a adequação e a realização efetiva do TLPT, a autoridade TLPT deve validar as informações relativas ao início do TLPT da entidade financeira e notificar a entidade financeira desse facto.

4. Na sequência da validação das informações relativas ao início do TLPT pela autoridade TLPT, a entidade financeira deve criar uma equipa de controlo para apoiar o chefe da equipa de controlo nas suas seguintes funções:

a) Especificar, no âmbito da equipa de controlo, os canais e processos de comunicação com os testadores e os prestadores de informações sobre as ameaças para todas as questões relacionadas com o TLPT;

b) Informar o órgão de administração da entidade financeira sobre os progressos do TLPT e os riscos associados;

c) Tomar decisões com base em conhecimentos especializados na matéria ao longo de todo o TLPT;

d) Executar o TLPT em conformidade com o presente regulamento;

e) Selecionar o prestador de informações sobre as ameaças para o TLPT;

f) Selecionar os testadores externos, os testadores internos ou ambos;

g) Elaborar o documento de especificação do âmbito.

5. Se a autoridade TLPT considerar que a composição inicial da equipa de controlo e quaisquer alterações subsequentes da mesma são adequadas para o desempenho das funções referidas no n.º 4, deve validar a equipa de controlo e notificar do facto o chefe da equipa de controlo.

6. A entidade financeira deve apresentar aos gestores dos testes um documento de especificação do âmbito que contenha todas as informações previstas no anexo II, no prazo de seis meses a contar da receção da notificação da autoridade TLPT a que se refere o n.º 1. O órgão de administração da entidade financeira deve aprovar o documento de especificação do âmbito.

7. As entidades financeiras devem ter em conta os seguintes critérios para a inclusão de funções críticas ou importantes no âmbito dos TLPT:

a) O caráter crítico ou a importância da função e o seu possível impacto no setor financeiro e na estabilidade financeira a nível da União e a nível nacional;

b) A importância da função para as operações comerciais diárias da entidade financeira;

c) A permutabilidade da função;

d) A interligação com outras funções;

e) A localização geográfica da função;

f) A dependência setorial de outras entidades em relação à função;

g) Se disponíveis, informações sobre as ameaças relacionadas com a função.

8. A equipa de controlo deve partilhar as informações relativas ao início do TLPT e o documento de especificação do âmbito com os testadores e os prestadores de informações sobre as ameaças, após a sua contratação. A equipa de controlo deve informar os testadores e os prestadores de informações sobre as ameaças acerca do processo de teste que deve ser seguido.

9. A entidade financeira deve assegurar que a contratação ou afetação de testadores e prestadores de informações sobre as ameaças é concluída antes do início da fase de testes.

10. Antes do início da fase de testes, a equipa de controlo deve consultar os gestores dos testes sobre a avaliação dos riscos TLPT e sobre as medidas de gestão dos riscos. A equipa de controlo deve rever a avaliação dos riscos ou as medidas de gestão dos riscos se a autoridade TLPT considerar que estas não dão uma resposta adequada aos riscos do TLPT.

11. A equipa de controlo deve avaliar a conformidade dos prestadores de informações sobre as ameaças e dos testadores que ponderem integrar nos TLPT com os requisitos estabelecidos no artigo 27.º do Regulamento (UE) 2022/2554 e no artigo 7.º, n.º 1, do presente regulamento, e devem documentar o resultado dessa avaliação. A equipa de controlo deve selecionar os prestadores de informações sobre as ameaças em conformidade com essa avaliação e com as suas práticas de gestão de riscos. Antes de contratar os prestadores de informações sobre as ameaças e os testadores externos selecionados, a equipa de controlo deve fornecer aos gestores dos testes provas da conformidade desses prestadores de informações sobre as ameaças e testadores com os requisitos estabelecidos no artigo 27.º do Regulamento (UE) 2022/2554 e no artigo 7.º, n.º 1, do presente regulamento. A equipa de controlo não pode contratar os prestadores de informações sobre as ameaças e os testadores externos selecionados se a autoridade TLPT considerar que os mesmos não cumprem os requisitos estabelecidos no artigo 27.º do Regulamento (UE) 2022/2554, os requisitos estabelecidos no artigo 7.º, n.º 1, do presente regulamento ou os requisitos adicionais decorrentes das legislações nacionais de segurança em conformidade com o direito da União, se a entidade financeira não cumprir o artigo 7.º, n.º 2, primeiro parágrafo, do presente regulamento ou se as circunstâncias referidas no artigo 7.º, n.º 2, segundo parágrafo, do presente regulamento não se verificarem.

12. Se o documento de especificação do âmbito estiver completo e garantir a realização de um TLPT adequado e eficaz, a autoridade TLPT deve aprovar esse documento e informar do facto o chefe da equipa de controlo.

Artigo 10.º

Fase de testes: informações sobre as ameaças

1. Na sequência da aprovação do documento de especificação do âmbito pela autoridade TLPT, o prestador de informações sobre as ameaças deve analisar informações genéricas e setoriais sobre as ameaças relevantes para a entidade financeira. Caso a autoridade TLPT forneça um cenário de ameaças genérico para o setor financeiro de um Estado-Membro, o prestador de informações sobre as ameaças pode utilizar esse cenário como base de referência para o cenário de ameaças nacional. O prestador de informações sobre as ameaças deve identificar ciberameaças e vulnerabilidades existentes ou potenciais relativas à entidade financeira. Além disso, o prestador de informações sobre as ameaças deve recolher e analisar informações concretas, acionáveis e contextualizadas sobre alvos e ameaças relativamente à entidade financeira, nomeadamente através da consulta da equipa de controlo e dos gestores dos testes.

2. O prestador de informações sobre as ameaças deve apresentar as ameaças pertinentes e as informações específicas sobre as ameaças e propor os cenários necessários à equipa de controlo, aos testadores e aos gestores dos testes. Os cenários propostos devem diferir no que respeita aos autores de ameaças identificados e às táticas, técnicas e procedimentos associados e devem visar cada função crítica ou importante no âmbito do TLPT.

3. O chefe da equipa de controlo deve selecionar pelo menos três cenários para realizar o TLPT com base em todos os elementos indicados a seguir:

a) A recomendação do prestador de informações sobre as ameaças e a natureza baseada em ameaças de cada cenário;

b) Os contributos dos gestores dos testes;

c) A viabilidade dos cenários de execução propostos, com base na opinião especializada dos testadores;

d) A dimensão, complexidade e perfil de risco global da entidade financeira e a natureza, escala e complexidade dos seus serviços, atividades e operações.

4. Dos cenários selecionados, só um pode não ser baseado em ameaças, mas eventualmente numa ameaça prospetiva e potencialmente fictícia com um elevado valor preditivo, antecipatório, oportunista ou prospetivo, tendo em conta a evolução prevista do cenário de ameaças no que respeita à entidade financeira.

No caso dos TLPT agrupados, sem prejuízo dos cenários que visam diretamente as funções críticas ou importantes das entidades financeiras envolvidas nos testes, pelo menos um cenário deve incluir os sistemas, processos e tecnologias de TIC subjacentes relevantes do terceiro prestador de serviços de TIC que apoiam as funções críticas ou importantes das entidades financeiras abrangidas.

Se o teste for um TLPT conjunto que envolva um prestador de serviços de TIC intragrupo, sem prejuízo dos cenários que visem diretamente as funções críticas ou importantes das entidades financeiras envolvidas no teste, pelo menos um cenário deve incluir os sistemas, processos e tecnologias de TIC subjacentes relevantes do prestador de serviços de TIC intragrupo que apoiam as funções críticas ou importantes das entidades financeiras abrangidas.

5. O prestador de informações sobre as ameaças deve fornecer o relatório de informações sobre as ameaças específicas à equipa de controlo, incluindo os cenários selecionados em conformidade com os n.os 3 e 4. O relatório de informações sobre as ameaças deve conter as informações previstas no anexo III.

6. A equipa de controlo deve apresentar o relatório de informações sobre as ameaças específicas ao gestor do teste para aprovação. Se o relatório de informações sobre as ameaças específicas estiver completo e garantir a realização de um TLPT eficaz, a autoridade TLPT deve aprovar o relatório de informações sobre as ameaças específicas e informar do facto o chefe da equipa de controlo.

Artigo 11.º

Fase de testes: teste da equipa vermelha

1. Após a aprovação do relatório de informações sobre as ameaças específicas pela autoridade TLPT, os testadores devem elaborar o plano de testes da equipa vermelha, que deve conter as informações previstas no anexo IV. Os testadores devem utilizar o documento de especificação do âmbito e o relatório de informações sobre as ameaças específicas como base para a elaboração dos cenários de ataque.

2. Os testadores devem consultar a equipa de controlo, o prestador de informações sobre as ameaças e os gestores dos testes sobre o plano de testes da equipa vermelha, incluindo as disposições em matéria de comunicação, procedimentos e gestão de projetos, a preparação e os casos de utilização para ativação das ajudas e os acordos de comunicação de informações à equipa de controlo e aos gestores dos testes.

3. Se o plano de testes da equipa vermelha estiver completo e garantir a realização de um TLPT eficaz, a equipa de controlo e a autoridade TLPT devem aprovar o plano de testes da equipa vermelha e o TLPT deve informar do facto o chefe da equipa de controlo.

4. Após a aprovação do plano de testes da equipa vermelha em conformidade com o n.º 3, os testadores devem realizar o TLPT durante a fase ativa de testes da equipa vermelha.

5. A duração da fase ativa de testes da equipa vermelha deve ser proporcionada ao âmbito do TLPT e à dimensão, atividade, complexidade e número das entidades financeiras e terceiros prestadores de serviços de TIC ou prestadores de serviços de TIC intragrupo envolvidos no TLPT, devendo, em qualquer caso, ser de pelo menos 12 semanas. Os cenários de ataque podem ser executados sequencialmente ou em simultâneo. A equipa de controlo, o prestador de informações sobre as ameaças, os testadores e os gestores dos testes devem chegar a acordo sobre a conclusão da fase ativa de testes da equipa vermelha.

6. Sob reserva de assegurar que o plano de testes da equipa vermelha permanece completo e permite a realização de um TLPT eficaz, o chefe da equipa de controlo e os gestores dos testes devem aprovar quaisquer alterações no plano de testes da equipa vermelha subsequentes à sua aprovação, que afetem nomeadamente o calendário, âmbito, os sistemas-alvo ou o desencadeamento dos alertas.

7. Durante toda a fase ativa de testes da equipa vermelha, os testadores devem informar pelo menos semanalmente a equipa de controlo e os gestores dos testes sobre os progressos realizados no TLPT, e o prestador de informações sobre as ameaças deve permanecer disponível para consulta e informações adicionais quando a equipa de controlo as solicitar.

8. A equipa de controlo deve fornecer atempadamente as ajudas concebidas com base no plano de testes da equipa vermelha. As ajudas podem ser acrescentadas ou adaptadas mediante aprovação da equipa de controlo e dos gestores dos testes.

9. Caso as atividades de teste sejam detetadas por qualquer membro do pessoal da entidade financeira ou dos seus terceiros prestadores de serviços de TIC ou prestador de serviços de TIC intragrupo, se for caso disso, a equipa de controlo, em consulta com os testadores e sem prejuízo do disposto no n.º 10, deve propor e apresentar medidas que permitam prosseguir o TLPT, assegurando ao mesmo tempo o seu sigilo, aos gestores dos testes para validação.

10. Em circunstâncias excecionais que desencadeiem riscos de impacto nos dados, danos nos ativos e perturbações nas funções, serviços ou operações críticos ou importantes da própria entidade financeira, dos seus terceiros prestadores de serviços de TIC ou prestadores de serviços de TIC intragrupo, ou perturbações nas suas contrapartes ou no setor financeiro, o chefe da equipa de controlo pode suspender o TLPT ou, como último recurso, caso a continuação do TLPT não seja de outro modo possível, e sob reserva de validação prévia pela autoridade TLPT, prosseguir o TLPT utilizando um exercício limitado de associação de equipas (equipa roxa). A duração do exercício limitado de associação de equipas (equipa roxa) deve ser contabilizada para efeitos da duração mínima de 12 semanas, referida no n.º 5, para a fase ativa de testes da equipa vermelha.

Artigo 12.º

Fase de conclusão

1. Após a conclusão da fase ativa de testes da equipa vermelha, o chefe da equipa de controlo deve informar a equipa azul de que teve lugar um TLPT.

2. No prazo de quatro semanas a contar do final da fase ativa de testes da equipa vermelha, os testadores devem apresentar à equipa de controlo um relatório de testes da equipa vermelha com as informações previstas no anexo V.

3. A equipa de controlo deve apresentar o relatório de testes da equipa vermelha à equipa azul e aos gestores dos testes sem demora injustificada.

Caso os gestores dos testes o solicitem, o relatório a que se refere o primeiro parágrafo não deve conter informações sensíveis.

4. Após receção do relatório de testes da equipa vermelha, e o mais tardar 10 semanas após o final da fase ativa de testes da equipa vermelha, a equipa azul deve apresentar à equipa de controlo um relatório de testes da equipa azul com as informações previstas no anexo VI. A equipa de controlo deve apresentar o relatório de testes da equipa azul aos testadores e aos gestores dos testes sem demora injustificada.

Caso os gestores dos testes o solicitem, o relatório a que se refere o primeiro parágrafo não deve conter informações sensíveis.

5. O mais tardar 10 semanas após o final da fase ativa de testes da equipa vermelha, a equipa azul e os testadores devem reproduzir as ações ofensivas e defensivas realizadas durante o TLPT. A equipa de controlo deve também realizar um exercício de associação de equipas (equipa roxa) sobre temas identificados conjuntamente pela equipa azul e pelos testadores, com base nas vulnerabilidades identificadas durante o teste e, se for caso disso, em questões que não puderam ser testadas durante a fase ativa de testes da equipa vermelha.

6. Após a conclusão dos exercícios de reprodução das ações e de associação de equipas (equipa roxa), a equipa de controlo, a equipa azul, os testadores e os prestadores de informações sobre as ameaças devem trocar observações sobre o processo TLPT. Os gestores dos testes podem apresentar observações.

7. Logo que a autoridade TLPT tenha notificado o chefe da equipa de controlo da sua avaliação no sentido de que o relatório de testes da equipa azul e o relatório de testes da equipa vermelha contêm as informações previstas nos anexos V e VI, a entidade financeira deve, no prazo de oito semanas, apresentar à autoridade TLPT, tal como referido no artigo 26.º, n.º 6, do Regulamento (UE) 2022/2554, o relatório que resume os resultados pertinentes do TLPT, contendo os elementos constantes do anexo VII, para aprovação.

Caso a autoridade TLPT o solicite, o relatório a que se refere o primeiro parágrafo não deve conter informações sensíveis.

Artigo 13.º

Plano corretivo

1. No prazo de oito semanas a contar da notificação a que se refere o artigo 12.º, n.º 7, do presente regulamento, a entidade financeira deve fornecer os planos corretivos e a documentação referida no artigo 26.º, n.º 6, do Regulamento (UE) 2022/2554 à autoridade TLPT e, se for diferente, à autoridade competente da entidade financeira.

2. O plano corretivo a que se refere o n.º 1 deve incluir, para cada conclusão retirada no âmbito do TLPT:

a) Uma descrição das deficiências identificadas;

b) Uma descrição das medidas corretivas propostas e da sua priorização e conclusão prevista, incluindo, se for caso disso, medidas para melhorar as capacidades de identificação, proteção, deteção e resposta;

c) Uma análise das causas profundas;

d) O pessoal ou as funções da entidade financeira responsáveis pela aplicação das medidas corretivas ou melhorias propostas;

e) Os riscos associados à não aplicação das medidas referidas na alínea b) e, se for caso disso, os riscos associados à aplicação dessas medidas.

Artigo 14.º

Comprovativo

1. O comprovativo referido no artigo 26.º, n.º 7, do Regulamento (UE) 2022/2554 deve conter as informações previstas no anexo VIII.

2. Caso várias autoridades TLPT tenham estado envolvidas num TLPT, a autoridade TLPT principal deve fornecer o comprovativo referido no artigo 26.º, n.º 7, do Regulamento (UE) 2022/2554 às entidades financeiras testadas.

Artigo 15.º

Utilização de testadores internos

1. As entidades financeiras devem estabelecer todos os mecanismos indicados a seguir para a utilização de testadores internos:

a) O estabelecimento e a aplicação de uma política de gestão dos testadores internos num TLPT;

b) Medidas destinadas a assegurar que a utilização de testadores internos para realizar um TLPT não afeta negativamente as capacidades gerais defensivas ou de resiliência da entidade financeira no que respeita a incidentes relacionados com as TIC nem afeta significativamente a disponibilidade de recursos dedicados a funções relacionadas com as TIC durante um TLPT;

c) Medidas para assegurar que os testadores internos dispõem de recursos e capacidades suficientes para realizar um TLPT.

A política referida na alínea a) deve:

a) conter critérios para avaliar a adequação, competência e os potenciais conflitos de interesses dos testadores internos e especificar as responsabilidades de gestão no processo de teste;

b) ser documentada e periodicamente revista;

c) prever que a equipa de testadores internos inclua um chefe dos testadores e pelo menos dois membros adicionais;

d) exigir que todos os membros da equipa de testadores tenham um vínculo contratual com a entidade financeira ou com um prestador de serviços de TIC intragrupo há pelo menos 12 meses;

e) incluir disposições sobre a formação dos testadores internos em relação à forma de realizar testes de penetração e testes da equipa vermelha.

2. Se uma autoridade TLPT aprovar a utilização de testadores internos em conformidade com o artigo 27.º, n.º 2, alínea a), do Regulamento (UE) 2022/2554, deve ter em conta os requisitos estabelecidos no artigo 7.º, n.º 1, do presente regulamento.

3. Ao utilizar testadores internos, a entidade financeira deve assegurar que essa utilização é mencionada nos documentos seguintes:

a) As informações relativas ao início dos testes a que se refere o artigo 9.º;

b) O relatório de testes da equipa vermelha a que se refere o artigo 12.º, n.º 2;

c) O relatório que resume as conclusões pertinentes do TLPT a que se refere o artigo 26.º, n.º 6, do Regulamento (UE) 2022/2554.

4. Os testadores que tenham vínculo contratual com o prestador de serviços de TIC intragrupo são considerados testadores internos da entidade financeira.

Artigo 16.º

Cooperação e reconhecimento mútuo

1. Para efeitos da realização de um TLPT em relação a uma entidade financeira que preste serviços em mais do que um Estado-Membro, nomeadamente através de uma sucursal, a autoridade TLPT dessa entidade financeira deve:

a) Determinar quais as autoridades TLPT nos Estados-Membros de acolhimento que devem estar envolvidas, tendo em conta se uma ou mais funções críticas ou importantes são geridas ou partilhadas entre os Estados-Membros de acolhimento;

b) Informar as autoridades TLPT identificadas em conformidade com a alínea a) da decisão de realizar um teste TLPT à entidade financeira;

c) Salvo acordo em contrário das autoridades TLPT, cabe à autoridade TLPT da entidade financeira dirigir o TLPT.

As autoridades TLPT dos Estados-Membros de acolhimento podem, no prazo de 20 dias úteis a contar da receção das informações sobre a realização futura de um TLPT, manifestar o seu interesse em acompanhar o TLPT na qualidade de observadoras ou designar um gestor dos testes para participar no TLPT. A autoridade TLPT principal deve fornecer a todas as autoridades TLPT que atuem na qualidade de observadores no TLPT o documento de especificação do âmbito, o relatório de síntese do teste, o plano corretivo e o comprovativo.

A autoridade TLPT principal deve coordenar todas as autoridades TLPT participantes ao longo de todo o teste e adotar todas as decisões necessárias para realizar o TLPT de forma adequada e eficaz. A autoridade TLPT principal pode fixar um número máximo de autoridades TLPT participantes, sempre que, de outro modo, a eficiência do TLPT possa ficar comprometida.

2. Se uma entidade financeira utilizar o mesmo prestador de serviços de TIC intragrupo que entidades financeiras estabelecidas noutros Estados-Membros, ou pertencer a um grupo e partilhar sistemas de TIC com entidades financeiras do mesmo grupo estabelecidas noutros Estados-Membros, a autoridade TLPT da entidade financeira deve contactar as autoridades TLPT das outras entidades financeiras que utilizam o mesmo prestador de serviços de TIC intragrupo ou partilham sistemas de TIC como parte do grupo e avaliar com elas a viabilidade e adequação da realização de um TLPT conjunto a seu respeito. Deve privilegiar-se um TLPT conjunto em relação a um TLPT individual caso o primeiro possa resultar numa redução dos custos e dos recursos para as entidades financeiras e para as autoridades TLPT, desde que a solidez e a eficácia dos testes não sejam prejudicadas.

3. Para efeitos da realização de um TLPT conjunto:

a) As autoridades TLPT das entidades financeiras devem chegar a acordo sobre a entidade financeira que deve ser designada para realizar o TLPT, tendo em conta a estrutura do grupo e a eficiência do teste;

b) A autoridade TLPT da entidade financeira designada em conformidade com a alínea a) deve dirigir o TLPT, salvo acordo em contrário das autoridades TLPT das entidades financeiras que participam nos TLPT conjuntos;

c) As autoridades TLPT das entidades financeiras que não a entidade financeira designada para dirigir os TLPT conjuntos podem manifestar o seu interesse em acompanhar o TLPT na qualidade de observadoras ou designar um gestor dos testes para esse TLPT.

A autoridade TLPT principal deve coordenar todas as autoridades TLPT envolvidas no TLPT conjunto e adotar todas as decisões necessárias para realizar o TLPT conjunto de forma sólida e eficaz.

4. Sempre que uma entidade financeira tencione realizar um TLPT agrupado, tal como referido no artigo 26.º, n.º 4, do Regulamento (UE) 2022/2554, eventualmente envolvendo entidades financeiras estabelecidas noutros Estados-Membros, a autoridade TLPT dessa entidade financeira deve contactar as autoridades TLPT das outras entidades financeiras e avaliar com elas a viabilidade e adequação da realização do TLPT agrupado a seu respeito, em conformidade com o artigo 26.º, n.º 4, do Regulamento (UE) 2022/2554.

5. Para efeitos da realização de um TLPT agrupado tal como referido no artigo 26.º, n.º 4, do Regulamento (UE) 2022/2554:

a) As autoridades TLPT das entidades financeiras devem chegar a acordo sobre a entidade financeira que deve ser designada para conduzir o TLPT agrupado, tendo em conta os serviços de TIC prestados pelo terceiro prestador de serviços de TIC às entidades financeiras e a eficiência do teste;

b) A autoridade TLPT da entidade financeira designada em conformidade com a alínea a) deve dirigir o TLPT, salvo acordo em contrário das autoridades TLPT das entidades financeiras que participam nos TLPT conjuntos;

c) As autoridades TLPT das entidades financeiras que não a entidade financeira designada para dirigir o TLPT agrupado podem manifestar o seu interesse em acompanhar o TLPT na qualidade de observadoras ou designar um gestor dos testes para esse TLPT.

A autoridade TLPT principal deve coordenar todas as autoridades TLPT envolvidas no TLPT agrupado e adotar todas as decisões necessárias para que seja realizado TLPT de forma sólida e eficaz.

6. Se, em relação a uma entidade financeira obrigada a realizar um TLPT, a autoridade TLPT dessa entidade financeira for diferente da sua autoridade competente nos termos do artigo 46.º do Regulamento (UE) 2022/2554, essas autoridades devem partilhar todas as informações pertinentes sobre todas as questões relacionadas com os TLPT para efeitos da realização dos TLPT ou para o exercício das suas funções em conformidade com esse regulamento.

Artigo 17.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 fevereiro de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO I

Conteúdo da carta de projeto [artigo 9.º, n.º 2, alínea a)]

Elemento de informação	Informações necessárias
Pessoa responsável pelo plano do projeto, ou seja, o chefe da equipa de controlo	Nome Dados de contacto
Testadores	☐ internos ☐ externos ☐ ambos
Canais de comunicação selecionados em conformidade com o artigo 9.º, n.º 2, alínea d), e o artigo 9.º, n.º 4, alínea a), incluindo: a) Encriptação de correio eletrónico a utilizar b) Salas de dados em linha a utilizar c) Mensagens instantâneas a utilizar	
Nome de código do TLPT	
Se existirem, funções críticas ou importantes que a entidade financeira gere noutros Estados-Membros	1. Lista de funções críticas ou importantes geridas noutro Estado-Membro 2. Para cada função crítica ou importante, indicação do Estado-Membro ou dos Estados-Membros onde são geridas
Se existirem, funções críticas ou importantes apoiadas por terceiros prestadores de serviços de TIC	3. Lista de funções críticas ou importantes apoiadas por terceiros prestadores de serviços de TIC 4. Para cada função, identificação do terceiro prestador de serviços de TIC
Prazos previstos para a conclusão do(a):	
1) Fase de preparação, em conformidade com o artigo 9.º	aaaa-mm-dd
2) Fase de testes, em conformidade com os artigos 10.º e 11.º	aaaa-mm-dd
3) Fase de conclusão, em conformidade com o artigo 12.º	aaaa-mm-dd
4) Plano corretivo, em conformidade com o artigo 13.º	aaaa-mm-dd

ANEXO II

Conteúdo do documento de especificação do âmbito (artigo 9.º, n.º 6)

1. O documento de especificação do âmbito deve conter uma lista de todas as funções críticas ou importantes identificadas pela entidade financeira.

2. Para cada função crítica ou importante identificada, devem ser incluídas as seguintes informações:
   a) Se a função crítica ou importante não estiver incluída no âmbito do TLPT, a explicação dos motivos para tal exclusão;
   b) Se a função crítica ou importante estiver incluída no âmbito do TLPT:
      i) a explicação dos motivos da sua inclusão,
      ii) o(s) sistema(s) de TIC identificado(s) que apoia(m) essa função crítica ou importante,
      iii) para cada sistema de TIC identificado:
         1. Se foi externalizada e, em caso afirmativo, o nome do terceiro prestador de serviços de TIC;
         2. As jurisdições em que o sistema de TIC é utilizado;
         3. Uma descrição de alto nível do(s) sinal(is) de alerta preliminar(es), indicando que aspeto de segurança da confidencialidade, integridade, autenticidade ou disponibilidade é abrangido por cada sinal de alerta.

ANEXO III

Conteúdo do relatório de informações sobre as ameaças específicas (artigo 10.º, n.º 5)

O relatório de informações sobre as ameaças específicas deve conter informações sobre todos os elementos indicados a seguir:

1. O âmbito global da investigação de informações, incluindo pelo menos:
   a) As funções críticas ou importantes abrangidas;
   b) A sua localização geográfica;
   c) A língua oficial da UE utilizada;
   d) Os terceiros prestadores de serviços de TIC pertinentes;
   e) O período durante o qual as informações são recolhidas;
2. A avaliação global das informações acionáveis concretas que é possível obter sobre a entidade financeira, incluindo:
   a) Os nomes de utilizador e senhas do trabalhador;
   b) Os domínios parecidos que podem ser confundidos com os domínios oficiais da entidade financeira;
   c) Reconhecimento técnico: s*oftware*, sistemas e tecnologias vulneráveis ou que possam ser exploradas;
   d) Informações publicadas pelos trabalhadores na Internet, relacionadas com a entidade financeira, que possam ser utilizadas para efeitos de um ataque;
   e) Informações para venda na Web obscura;
   f) Quaisquer outras informações pertinentes disponíveis na Internet ou em redes públicas;
   g) Se for caso disso, informações sobre ataques físicos, incluindo formas de acesso às instalações da entidade financeira;
3. Análise das informações sobre as ameaças, tendo em conta o cenário de ameaças geral e a situação específica da entidade financeira, incluindo pelo menos:
   a) O ambiente geopolítico;
   b) O ambiente económico;
   c) As tendências tecnológicas e quaisquer outras tendências relacionadas com as atividades no setor dos serviços financeiros;
4. Perfis de ameaça dos intervenientes maliciosos (indivíduos/grupos específicos ou categoria genérica) que possam visar a entidade financeira, nomeadamente os sistemas da entidade financeira que os intervenientes maliciosos serão mais suscetíveis de comprometer ou visar, a possível motivação, intenção e lógica subjacentes ao potencial ataque e o possível *modus operandi* dos atacantes;
5. Cenários de ameaça: pelo menos três cenários de ameaça de extremo a extremo para os perfis de ameaça identificados em conformidade com o ponto 4 que apresentem as classificações mais elevadas em termos de gravidade da ameaça. Os cenários de ameaça devem descrever a via de ataque de extremo a extremo e incluir pelo menos:
   a) Um cenário que inclua, nomeadamente, a colocação em causa da disponibilidade dos serviços;
   b) Um cenário que inclua, nomeadamente, a colocação em causa da integridade dos dados;
   c) Um cenário que inclua, nomeadamente, a colocação em causa da confidencialidade das informações;
6. Se for caso disso, uma descrição do cenário não baseado em ameaças a que se refere o artigo 10.º, n.º 4.

ANEXO IV

Conteúdo do plano de testes da equipa vermelha (artigo 11.º, n.º 1)

O plano de testes da equipa vermelha deve conter informações sobre todos os elementos indicados a seguir:

a) Canais e procedimentos de comunicação;

b) As táticas, técnicas e procedimentos que é permitido ou não utilizar no ataque, nomeadamente os limites éticos em termos de engenharia social;

c) As medidas de gestão dos riscos a seguir pelos testadores;

d) Uma descrição de cada cenário que inclua:

   i) o autor da ameaça simulada,

   ii) a sua intenção, motivação e objetivos,

   iii) a(s) função(ões) visada(s) e o(s) sistema(s) de TIC de apoio,

   iv) os aspetos específicos de confidencialidade, integridade, disponibilidade e autenticidade,

   v) alertas;

e) Uma descrição pormenorizada de cada via de ataque prevista, nomeadamente os pré-requisitos e as eventuais ajudas a fornecer pela equipa de controlo, incluindo prazos para a sua disponibilização e potencial utilização;

f) A programação das atividades da equipa vermelha, nomeadamente o planeamento temporal da execução de cada cenário, com uma repartição mínima de acordo com as três fases que um testador executa ao longo da fase de testes, respetivamente, ao entrar nos sistemas de TIC das entidades financeiras, no seu percurso pelos sistemas de TIC e, por último, na execução de ações para alcançar os objetivos e, em seguida, sair dos sistemas de TIC (fases de entrada, passagem e saída);

g) Especificidades da infraestrutura das entidades financeiras a ter em conta durante os testes;

h) Se for caso disso, informações adicionais ou outros recursos necessários aos testadores para a execução dos cenários.

ANEXO V

Conteúdo do relatório de testes da equipa vermelha (artigo 12.º, n.º 2)

O relatório de testes da equipa vermelha deve conter informações sobre, pelo menos, todos os elementos indicados a seguir:

a) Informações sobre o ataque realizado, incluindo:

   i) as funções críticas ou importantes visadas e os sistemas, processos e tecnologias de TIC identificados que apoiam a função crítica ou importante, tal como identificados no plano de testes da equipa vermelha,

   ii) resumo de cada cenário,

   iii) alertas desencadeados e não desencadeados,

   iv) vias de ataque seguidas com êxito e sem êxito,

   v) táticas, técnicas e procedimentos utilizados com êxito e sem êxito,

   vi) eventuais desvios em relação ao plano de testes da equipa vermelha,

   vii) ajudas concedidas, se for caso disso;

b) Todas as ações de que os testadores tenham conhecimento e que foram executadas pela equipa azul para reconstituir o ataque e atenuar os seus efeitos;

c) Vulnerabilidades detetadas e outras conclusões, incluindo:

   i) a descrição da vulnerabilidade e das outras conclusões, nomeadamente o seu caráter crítico,

   ii) análise das causas profundas dos ataques bem-sucedidos,

   iii) recomendações de correção, nomeadamente a indicação da respetiva prioridade.

ANEXO VI

Conteúdo do relatório de testes da equipa azul (artigo 12.º, n.º 4)

O relatório de testes da equipa azul deve conter informações sobre, pelo menos, todos os elementos indicados a seguir:

1. Para cada etapa de ataque descrita pelos testadores no relatório de testes da equipa vermelha:
   a) Lista das ações de ataque detetadas,
   b) Registos correspondentes a estas deteções;
2. Avaliação das conclusões e recomendações dos testadores;
3. Provas do ataque dos testadores recolhidas pela equipa azul;
4. Análise pela equipa azul das causas profundas dos ataques bem-sucedidos por parte dos testadores;
5. Lista das ilações retiradas e potencial de melhorias identificado;
6. Lista de temas a abordar aquando da associação de equipas (equipa roxa).

ANEXO VII

Pormenores do relatório que resume as conclusões pertinentes do TLPT referido no artigo 26.º, n.º 6, do Regulamento (UE) 2022/2554

O relatório de síntese dos testes deve conter informações sobre, pelo menos, todos os elementos indicados a seguir:

a) As partes envolvidas;

b) O plano do projeto;

c) O âmbito validado, nomeadamente a lógica subjacente à inclusão ou exclusão de funções críticas ou importantes e de sistemas, processos e tecnologias de TIC identificados que apoiem as funções críticas ou importantes abrangidas pelo TLPT;

d) Os cenários selecionados e qualquer desvio significativo em relação ao relatório de informações sobre as ameaças específicas;

e) As vias de ataque executadas e as táticas, técnicas e procedimentos utilizados;

f) Os alertas desencadeados e não desencadeados;

g) eventuais desvios em relação ao plano de testes da equipa vermelha,

h) Deteções da equipa azul, caso tenham ocorrido;

i) Associação de equipas (equipa roxa) na fase de testes, se realizada, e as condições conexas;

j) Ajudas utilizadas, se for caso disso;

k) Medidas de gestão dos riscos adotadas;

l) Vulnerabilidades identificadas e outras conclusões, nomeadamente quanto ao seu caráter crítico;

m) análise das causas profundas dos ataques bem-sucedidos;

n) Plano corretivo de alto nível, ligando as vulnerabilidades e outras conclusões, as suas causas profundas e a prioridade de correção;

o) Ilações retiradas das observações recebidas.

ANEXO VIII

Pormenores do comprovativo do TLPT referido no artigo 26.º, n.º 7, do Regulamento (UE) 2022/2554

O comprovativo deve incluir, pelo menos, todas as informações indicadas a seguir:

a) Sobre o TLPT realizado:

   i) as datas de início e de fim do TLPT,

   ii) as funções críticas ou importantes abrangidas pelo teste,

   iii) se for caso disso, informações sobre funções críticas ou importantes abrangidas pelo teste em relação às quais o TLPT não foi realizado,

   iv) se for caso disso, outras entidades financeiras que estiveram envolvidas no TLPT,

   v) se for caso disso, os terceiros prestadores de serviços de TIC que participaram no TLPT,

   vi) No que respeita aos testadores:

      1. Se foram utilizados testadores internos;

      2. Se a entidade financeira utilizou o artigo 5.º, n.º 3, segundo parágrafo,

   vii) a duração, em dias de calendário, da fase ativa de testes da equipa vermelha;

b) Nos casos em que várias autoridades TLPT tenham estado envolvidas no TLPT, as outras autoridades TLPT e a qualidade em que participaram;

c) Lista dos documentos examinados pela autoridade TLPT para efeitos do comprovativo.