EBA/GL/2017/05

11/09/2017

Orientações

Orientações relativas à avaliação do risco das TIC no âmbito do processo de revisão e avaliação pelo supervisor (SREP)

1. Obrigações de cumprimento e de comunicação de informação

Natureza das presentes Orientações

1. O presente documento contém orientações emitidas ao abrigo do artigo 16.o do Regulamento (UE) n.o 1093/20101. Nos termos do artigo 16.o, n.o 3, do referido Regulamento, as autoridades competentes e as instituições financeiras devem desenvolver todos os esforços para dar cumprimento às Orientações.

2. As Orientações refletem a posição da EBA sobre práticas de supervisão adequadas no âmbito do Sistema Europeu de Supervisão Financeira ou sobre o modo como a legislação da União deve ser aplicada num domínio específico. As autoridades competentes, na aceção do artigo 4.o, n.o 2, do Regulamento (UE) n.o 1093/2010, às quais as presentes Orientações se aplicam devem dar cumprimento às mesmas, incorporando-as nas suas práticas de supervisão conforme for mais adequado (por exemplo, alterando o seu enquadramento jurídico ou os seus processos de supervisão), incluindo nos casos em que as orientações são aplicáveis, em primeira instância, a instituições.

Requisitos de notificação

3. Nos termos do disposto no artigo 16.o, n.o 3, do Regulamento (UE) n.o 1093/2010, as autoridades competentes confirmam à EBA se dão ou tencionam dar cumprimento às presentes Orientações, ou, caso contrário, indicam as razões para o não cumprimento até 13.11.2017. Na ausência de qualquer notificação até à referida data, a EBA considerará que as autoridades competentes em causa não cumprem as Orientações. As notificações efetuam-se mediante o envio do modelo disponível no sítio Web da EBA para o endereço compliance@eba.europa.eu com a referência «EBA/GL/2017/05». As notificações devem ser apresentadas por pessoas devidamente autorizadas para o efeito pelas respetivas autoridades competentes. Qualquer alteração no que respeita à situação de cumprimento deve igualmente ser comunicada à EBA.

4. As notificações serão publicadas no sítio Web da EBA, em conformidade com o disposto no artigo 16.o, n.o 3.

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

2. Objeto, âmbito de aplicação e definições

Objeto e âmbito de aplicação

5. As presentes orientações, emitidas nos termos do n.º 3 do artigo 107.º da Diretiva 2013/36/UE[2], têm por objetivo garantir a convergência das práticas de supervisão na avaliação do risco das tecnologias da informação e comunicação (TIC) no âmbito do processo de revisão e avaliação pelo supervisor (SREP) referido no artigo 97.º da Diretiva 2013/36/UE e especificado mais pormenorizadamente nas orientações da EBA relativas aos procedimentos e metodologias comuns a seguir no âmbito do processo de revisão e avaliação pelo supervisor (SREP)[3]. As presentes orientações especificam, em particular, os critérios de avaliação que as autoridades competentes devem aplicar na avaliação de supervisão do governo e da estratégia das instituições em matéria de TIC, bem como na avaliação de supervisão das exposições das instituições ao risco das TIC e aos mecanismos de controlo desse risco. As presentes orientações fazem parte integrante das Orientações da EBA relativas ao SREP.

6. As autoridades competentes devem aplicar estas orientações em conformidade com o nível de aplicação do SREP especificado nas Orientações da EBA relativas ao SREP e de acordo com o modelo de compromisso mínimo e os requisitos de proporcionalidade estabelecidos.

Destinatários

7. As presentes orientações destinam-se às autoridades competentes, na aceção do artigo 4.º, n.º 2, alínea i), do Regulamento (UE) n.º 1093/2010.

[2] 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 (1) - JO L 176, de 27.6.2013.

[3] EBA/GL/2014/13

Definições

8. Salvo disposição em contrário, os termos utilizados e definidos na Diretiva 2013/36/UE, no Regulamento (UE) n.º 575/2013 e nas definições das Orientações da EBA relativas ao SREP têm a mesma aceção nas presentes orientações. Adicionalmente, para efeito das presentes orientações, aplicam-se as seguintes definições:

Sistemas de TIC	TIC implementadas no quadro de um mecanismo ou de uma rede de interligação que suporta as operações de uma instituição.
Serviços de TIC	Serviços fornecidos pelos sistemas de TIC a um ou mais utilizadores internos ou externos. Exemplificando, incluem-se os serviços de introdução, armazenamento, e processamento de dados, os serviços de reporte, mas também os serviços de monitorização e de suporte ao negócio e à tomada de decisão.
Risco de disponibilidade e continuidade das TIC	O risco de que o desempenho e a disponibilidade dos sistemas e dados das TIC sejam afetados negativamente, incluindo a incapacidade de recuperar atempadamente os serviços da instituição devido a uma falha dos componentes de *hardware* ou *software* das TIC, lacunas na gestão do sistema de TIC ou qualquer outro acontecimento, tal como explicado mais detalhadamente no Anexo.
Risco de segurança das TIC	O risco de acesso não autorizado a sistemas e dados das TIC a partir do interior ou do exterior da instituição (por exemplo, ciberataques), tal como explicado mais detalhadamente no Anexo.
Risco de alteração das TIC	O risco inerente à incapacidade da instituição em gerir de forma oportuna e controlada as alterações nos sistemas de TIC, em particular para programas de alteração profundos e complexos, tal como explicado mais detalhadamente no Anexo.
Risco de integridade de dados das TIC	O risco de que os dados armazenados e processados pelos sistemas de TIC estejam incompletos, incorretos ou inconsistentes em diferentes sistemas de TIC, por exemplo, em consequência de controlos de TIC insuficientes ou inexistentes durante as diferentes fases do ciclo de vida dos dados das TIC (*i.e.*, conceção da arquitetura de dados, criação do modelo de dados e/ou dicionários de dados, verificação de entradas de dados, controlo de extrações, transferências e processamento de dados, incluindo saídas de dados processados), comprometendo a capacidade de uma instituição fornecer

	serviços e produzir informações financeiras e de gestão (do risco) de forma correta e oportuna, tal como explicado mais detalhadamente no Anexo.
Risco de contratação externa de TIC	O risco de recorrer a uma entidade terceira ou a outra entidade do grupo (contratação externa intragrupo) para o fornecimento de sistemas de TIC ou de serviços conexos ter um impacto negativo no desempenho da instituição e da sua gestão de risco, tal como explicado mais detalhadamente no Anexo.

3. Aplicação

Data de aplicação

9. As presentes orientações são aplicáveis a partir de 1 de janeiro de 2018.

4. Requisitos para a avaliação de risco das TIC

Título 1 - Disposições gerais

10. As autoridades competentes devem realizar a avaliação do risco das TIC, do mecanismo de governo da TIC e da estratégia para as TIC no quadro do processo SREP, seguindo o modelo de compromisso mínimo e os requisitos de proporcionalidade especificados no Título 2 das Orientações da EBA relativas ao SREP. Tal significa, especificamente, que:

    a. a frequência da avaliação do risco das TIC depende do modelo de compromisso mínimo implementado com base na categoria SREP atribuída à instituição e do respetivo plano de atividades de supervisão; e

    b. a exaustividade, o detalhe e a intensidade da avaliação das TIC devem ser proporcionais à dimensão, à estrutura e ao ambiente operacional da instituição, bem como à natureza, à escala e à complexidade das suas atividades.

11. O princípio de proporcionalidade aplica-se ao longo das presentes orientações ao âmbito, à frequência e à intensidade do compromisso de supervisão e diálogo com uma instituição e às expectativas de supervisão das normas que a instituição deve cumprir.

12. As autoridades competentes podem basear-se no trabalho já levado a cabo pela instituição ou pela autoridade competente no contexto das avaliações de outros riscos ou elementos do SREP e ter em linha de conta esse trabalho a fim de atualizar a avaliação. Especificamente, ao realizarem as avaliações previstas nas presentes orientações, as autoridades competentes devem selecionar a abordagem de avaliação mais adequada e a metodologia mais apropriada e proporcional à instituição, e utilizar a documentação existente e disponível (por exemplo, relatórios relevantes e outros documentos, reuniões de gestão (de riscos), conclusões de inspeções *on-site*) para instruir a sua avaliação.

13. As autoridades competentes devem sintetizar as conclusões das suas avaliações dos critérios especificados nas presentes orientações e utilizá-las com o objetivo de chegarem a conclusões sobre a avaliação dos elementos do SREP, tal como especificado nas Orientações da EBA relativas ao SREP.

14. Em particular, a avaliação do governo e da estratégia de TIC efetuada nos termos do Título 2 das presentes orientações deve resultar em conclusões que instruam a síntese das conclusões da avaliação do elemento de governo interno e dos controlos ao nível da instituição, prevista no Título 5 das Orientações da EBA relativas ao SREP, e deve ser refletida na respetiva notação desse elemento SREP. Além disso, as autoridades competentes devem ter em consideração que qualquer impacto negativo significativo da avaliação da estratégia de TIC na estratégia de negócio da instituição, bem como

quaisquer preocupações de que a instituição possa não dispor de recursos e competências de TIC suficientes para realizar e suportar importantes alterações estratégicas planeadas, devem instruir a análise do modelo de negócio realizada nos termos do Título 4 das Orientações da EBA relativas ao SREP.

15. O resultado da avaliação do risco de TIC, tal como especificado no Título 3 das presentes orientações, deve instruir as conclusões da avaliação do risco operacional e deve ser considerado como elucidativo da notação relevante, conforme especificado no Título 6.4 das Orientações da EBA relativas ao SREP.

16. Cabe notar que as autoridades competentes, ainda que devam, regra geral, avaliar as subcategorias de riscos no quadro das principais categorias (*i.e.*, o risco das TIC deve ser avaliado no quadro do risco operacional), podem avaliar individualmente as subcategorias que considerem significativas. Para o efeito, caso o risco das TIC seja identificado como risco significativo pela autoridade competente, estas orientações também fornecem um quadro de notação (Quadro 1) que deve ser utilizado para a atribuição de uma notação de subcategoria autónoma para o risco das TIC, seguindo a abordagem global para atribuir uma notação aos riscos de capital definida nas Orientações da EBA relativas ao SREP.

17. Para chegar a uma conclusão sobre se o risco de TIC deve ser considerado significativo e, consequentemente, sobre a possibilidade desse risco ser avaliado e classificado como uma subcategoria individual do risco operacional, as autoridades competentes podem utilizar os critérios especificados na secção 6.1 das Orientações da EBA relativas ao SREP.

18. Ao aplicarem as presentes orientações, as autoridades competentes devem, quando relevante, ter em conta a lista não exaustiva de subcategorias de risco das TIC e os cenários de risco indicados no Anexo, tendo em consideração que o Anexo se centra nos riscos de TIC suscetíveis de resultar em perdas graves. As autoridades competentes podem excluir os riscos de TIC incluídos na taxonomia que não sejam pertinentes para a sua avaliação. Espera-se que as instituições tenham as suas próprias taxonomias de riscos das TIC e não que utilizem a taxonomia de riscos das TIC indicada no Anexo.

19. Sempre que as presentes orientações sejam aplicadas em relação a grupos bancários transfronteiriços e respetivas entidades e que tenha sido criado um colégio de entidades de supervisão, as autoridades competentes envolvidas devem, no contexto da sua cooperação para a avaliação do SREP em conformidade com a secção 11.1 das Orientações da EBA relativas ao SREP, coordenar, tanto quanto possível e de uma forma coerente para todas as entidades do grupo, o âmbito exato e detalhado de cada elemento de informação.

Título 2 - Avaliação do governo e da estratégia das instituições para as TIC

2.1 Princípios gerais

20. As autoridades competentes devem avaliar se a estrutura global de governo e controlo interno da instituição abrange devidamente os sistemas de TIC e os riscos conexos e se o órgão de administração endereça e gere adequadamente estes aspetos, visto que as TIC são parte integrante do bom funcionamento de uma instituição.

21. Ao efetuarem esta avaliação, as autoridades competentes devem ter como referência os requisitos e normas relativos à boa governação interna e às disposições de gestão de riscos, conforme especificado nas Orientações da EBA sobre a governação interna das instituições (GL 44)[4], e as orientações internacionais nesta matéria, na medida em que sejam aplicáveis, dada a especificidade dos sistemas e riscos das TIC.

22. A avaliação no presente Título não abrange os elementos específicos do governo, da gestão de riscos e dos controlos dos sistemas de TIC que se centram na gestão de riscos específicos das TIC abordados no Título 3 das presentes orientações, centrando-se nas seguintes áreas:

    a. estratégia de TIC – se a instituição tem uma estratégia das TIC adequadamente gerida e em conformidade com a estratégia de negócio da instituição;

    b. governo interno global – se os mecanismos de governo interno global da instituição são adequados em relação aos sistemas de TIC da instituição; e

    c. risco de TIC na estrutura de gestão de risco da instituição – se a estrutura de gestão de risco e controlo interno da instituição salvaguarda adequadamente os sistemas de TIC da instituição.

23. A alínea a) do n.º 22, fornecendo simultaneamente informações sobre elementos do governo da instituição, deve principalmente contribuir para a avaliação do modelo de negócio endereçado no Título 4 das Orientações da EBA relativas ao SREP. As alíneas b) e c) complementam as avaliações dos tópicos cobertos pelo Título 5 das Orientações da EBA relativas ao SREP e a avaliação descrita nas presentes orientações deve contribuir para a respetiva avaliação nos termos do Título 5 das Orientações da EBA relativas ao SREP.

24. O resultado desta avaliação deve instruir, quando relevante, a avaliação da gestão de risco e dos controlos nos termos do Título 3 das presentes orientações.

[4] Orientações da EBA sobre a governação interna das instituições, GL 44, de 27 de setembro de 2011.

2.2 Estratégia de TIC

25. Nos termos da presente secção, as autoridades competentes devem avaliar se a instituição implementou uma estratégia de TIC que: está sujeita a uma fiscalização adequada pelo órgão de administração da instituição; é consistente com a estratégia de negócio, em particular para manter as TIC atualizadas e planear ou implementar alterações importantes e complexas ao nível das TIC; e suporta o modelo de negócio da instituição.

2.2.1 Desenvolvimento e adequação da estratégia de TIC

26. As autoridades competentes devem avaliar se a instituição dispõe de uma estrutura, proporcional à natureza, escala e complexidade das suas atividades de TIC, para a preparação e o desenvolvimento da estratégia de TIC da instituição. Ao conduzirem esta avaliação, as autoridades competentes devem ter em consideração se:

    a. a direção de topo[5] do(s) segmento(s)de atividade está devidamente envolvida na definição das prioridades estratégicas de TIC da instituição e se, por sua vez, a direção de topo da função de TIC está ciente do desenvolvimento, da conceção e da criação de estratégias e iniciativas de negócio para garantir o alinhamento contínuo entre os sistemas , os serviços e a função de TIC (*i.e.*, os responsáveis pela gestão e implementação destes sistemas e serviços), da estratégia de negócio da instituição, e de que as TIC estão efetivamente atualizadas.

    b. a estratégia de TIC está documentada e apoiada por planos de implementação concretos, em particular no que diz respeito a metas importantes e ao planeamento de recursos (incluindo recursos financeiros e humanos) para garantir que tais metas são realistas e permitem a execução da estratégia de TIC;

    c. a instituição atualiza periodicamente a sua estratégia para as TIC, em particular aquando de alterações da estratégia de negócio, para assegurar o alinhamento contínuo entre as TIC e os objetivos, planos e atividades de negócio a médio e a longo prazo; e

    d. o órgão de administração da instituição aprova a estratégia para as TIC e os planos de implementação e monitoriza a respetiva implementação.

2.2.2 Implementação da estratégia de TIC

27. Se a estratégia de TIC da instituição exigir a implementação de alterações importantes e complexas ao nível das TIC ou com implicações significativas para o modelo de negócio da instituição, as autoridades competentes devem avaliar se a instituição implementou uma estrutura de controlo, adequada à sua dimensão, às suas atividades de TIC, assim como ao nível de atividades de alteração, para apoiar a implementação efetiva da estratégia de TIC da instituição. Ao levaram a cabo esta avaliação, as autoridades competentes devem ter em consideração se a estrutura de controlo:

[5] Direção de topo e órgão de administração tal como definidos na Diretiva 2013/36/UE de 26 de junho de 2013; «órgão de administração» no n.º 7 do artigo 3.º e «direção de topo» no n.º 9 do artigo 3.º.

a. inclui processos de governo (por exemplo, a monitorização e reporte do progresso e dos orçamentos) e órgãos relevantes (por exemplo, um gabinete de gestão de projetos (PMO), um grupo diretor das TIC ou equivalente) para apoiar de forma efetiva a implementação de programas estratégicos de TIC;

b. definiu e atribuiu papéis e responsabilidades para a implementação dos programas estratégicos de TIC, tendo em particular atenção à experiência das principais partes interessadas na organização, direção e monitorização de alterações importantes e complexas ao nível das TIC e a gestão de impactos organizacionais e humanos mais gerais (tais como, gestão da resistência à mudança, formação, comunicação);

c. envolve as funções de controlo independente e auditoria interna para garantir que os riscos associados à implementação da estratégia de TIC foram identificados, avaliados e efetivamente mitigados e que a estrutura de governo em vigor para implementar a estratégia de TIC é eficaz; e

d. contém um processo de planeamento e de revisão do planeamento que proporciona flexibilidade para responder a questões importantes identificadas (por exemplo, problemas ou atrasos encontrados na implementação) ou a desenvolvimentos externos (por exemplo, alterações importantes no ambiente de negócio, problemas tecnológicos ou inovações) para garantir uma adaptação oportuna do plano de implementação estratégico.

2.3 Governo interno global

28. Nos termos do Título 5 das Orientações da EBA relativas ao SREP, as autoridades competentes devem avaliar se a instituição possui uma estrutura empresarial apropriada e transparente adequada à sua finalidade e se implementou os mecanismos de governo adequados. No que diz respeito especificamente aos sistemas de TIC e em conformidade com as Orientações da EBA sobre a governação interna, esta avaliação deve incluir uma avaliação sobre se a instituição demonstra:

    a. possuir uma estrutura organizacional sólida e transparente, com responsabilidades claras relativamente às TIC, incluindo o órgão de administração e os seus comités, e que os principais responsáveis no domínio das TIC (por exemplo, o diretor dos sistemas de informação - CIO- , o diretor de operações - COO ou uma função equivalente) dispõem de acesso indireto ou direto adequado ao órgão de administração, para garantir que as informações ou os problemas importantes relacionados com as TIC são comunicados, discutidos e decididos adequadamente ao nível do órgão de administração; e

    b. que o órgão de administração tem conhecimento e endereça os riscos associados às TIC.

29. Em conformidade com a secção 5.2 das Orientações da EBA relativas ao SREP, as autoridades competentes devem avaliar se a política e a estratégia de contratação externa ao nível das TIC da instituição tem em conta, quando relevante, o impacto da contratação externa de TIC no negócio e no modelo de negócio da instituição.

2.4 Risco de TIC na estrutura de gestão de risco da instituição

30. Na avaliação da gestão de risco e de controlos internos a nível da instituição, tal como previsto no Título 5 das Orientações da EBA relativas ao SREP, as autoridades competentes devem ter em consideração se a estrutura de gestão de risco e de controlo interno da instituição salvaguarda adequadamente os sistemas de TIC da instituição de uma forma que seja proporcional à dimensão e às atividades da instituição e ao seu perfil de risco de TIC tal como definido no Título 3. As autoridades competentes devem determinar, em particular, se:

    a. a apetência pelo risco e o processo de autoavaliação da adequação do capital interno (ICAAP) cobrem os riscos de TIC, no quadro da categoria mais ampla de risco operacional, para a definição da estratégia global de risco e para a determinação do capital interno; e

    b. os riscos de TIC estão incluídos no âmbito das estruturas de gestão de risco e de controlo interno da instituição.

31. As autoridades competentes devem realizar a avaliação referida na alínea a) tendo em conta quer os cenários previstos quer os cenários adversos, tais como os cenários incluídos no teste de esforço específico da instituição ou no teste de esforço de supervisão.

32. No que se refere especificamente à alínea b), as autoridades competentes devem avaliar se as funções de controlo independente e de auditoria interna, detalhadas no n.º 104, alíneas a) e d), e no n.º 105, alíneas a) e c) das Orientações da EBA relativas ao SREP, são apropriadas para assegurar um nível suficiente de independência entre as TIC e as funções de controlo e auditoria, tendo em conta a dimensão e o perfil de risco de TIC da instituição.

2.5 Síntese das conclusões

33. Estes resultados devem ser refletidos na síntese das conclusões nos termos do Título 5 das Orientações da EBA relativas ao SREP e devem fazer parte da respetiva notação em conformidade com as considerações no Quadro 3 das Orientações da EBA relativas ao SREP.

34. Para a avaliação da estratégia para as TIC, devem ser tidos em consideração os pontos abaixo na realização da avaliação acima referida:

    a. se as autoridades competentes chegarem à conclusão de que a estrutura de governo da instituição é inadequada para o desenvolvimento e a implementação da estratégia da instituição para as TIC nos termos do ponto 2.2, essa conclusão deve instruir a avaliação do governo interno da instituição nos termos do Título 5, ponto 87, alínea a), das Orientações da EBA relativas ao SREP;

    b. se as autoridades competentes chegarem à conclusão, com base nas avaliações nos termos do ponto 2.2, de que haverá um desalinhamento significativo entre a estratégia de TIC e a estratégia de negócio, suscetível de ter um impacto negativo significativo nos objetivos de negócio e/ou financeiros a longo prazo da instituição, na sustentabilidade e/ou no modelo de negócio da instituição ou nas áreas de negócio/linhas de produto da instituição que forem considerados como mais significativos na aceção do n.º 62, alínea a) das Orientações da EBA

relativas ao SREP, essa conclusão deve instruir a avaliação do modelo de negócio nos termos do Título 4, n.º 70, alíneas b) e c) das referidas orientações; e

c. se as autoridades competentes chegarem à conclusão, com base nas avaliações referidas no ponto 2.2 *supra*, de que a instituição não possui recursos de TIC e competências de implementação de TIC suficientes para executar e apoiar as alterações estratégicas importantes planeadas, essa conclusão deve instruir a avaliação do modelo de negócio do Título 4, n.º 70, alínea b), das Orientações da EBA relativas ao SREP.

Título 3 - Avaliação das exposições e dos controlos dos riscos de TIC das instituições

3.1 Considerações gerais

35. As autoridades competentes devem avaliar se a instituição identificou, avaliou e mitigou devidamente os riscos de TIC a que está exposta. Este processo deve fazer parte da estrutura de gestão de riscos operacionais e ser coerente com a abordagem aplicável ao risco operacional.

36. As autoridades competentes devem, em primeiro lugar, identificar os riscos de TIC inerentes significativos aos quais a instituição esteja ou possa estar exposta e, em seguida, efetuar uma avaliação da eficácia da estrutura de gestão dos riscos de TIC da instituição e dos procedimentos e controlos para mitigar esses riscos. O resultado da avaliação deve ser refletido na síntese das conclusões que contribui para a notação de risco operacional nas Orientações relativas ao SREP. Nos casos em que o risco de TIC seja considerado significativo e as autoridades competentes pretendam atribuir uma notação individual, deve ser utilizado o Quadro 1 para atribuir uma notação como um sub-risco do risco operacional.

37. Ao realizarem a avaliação em conformidade com o presente Título, as autoridades competentes devem utilizar todas as fontes de informação disponíveis, tal como previsto no n.º 127 do Título 6 das Orientações da EBA relativas ao SREP, por exemplo, atividades de gestão de risco da instituição, reportes e resultados, como base para a identificação das suas prioridades de avaliação de supervisão. As autoridades competentes devem também utilizar outras fontes de informação para realizar esta avaliação, designadamente, quando relevante, as fontes seguintes:

    a. autoavaliações de risco e de controlos das TIC (se forem fornecidas no âmbito do ICAAP);
    b. Informação de gestão (MI) relacionada com o risco de TIC comunicada ao órgão de administração da instituição, por exemplo reportes de riscos de TIC periódicos e relacionados com incidentes (incluindo na base de dados de perdas operacionais), dados de exposição ao risco de TIC derivados da função de gestão de risco da instituição;
    c. conclusões de auditorias internas e externas referentes a TIC comunicadas ao comité de auditoria da instituição.

3.2 Identificação de riscos de TIC significativos

38. As autoridades competentes devem identificar os riscos de TIC significativos aos quais a instituição esteja ou possa vir a estar exposta seguindo os procedimentos descritos abaixo.

3.2.1 Revisão do perfil de risco de TIC da instituição

39. Ao reverem o perfil de risco de TIC da instituição, as autoridades competentes devem ter em consideração todas as informações relevantes sobre as exposições da instituição ao risco de TIC,

incluindo as informações nos termos do n.º 37 e as deficiências ou lacunas significativas identificadas na organização das TIC e nos controlos ao nível da instituição, nos termos do Título 2 das presentes orientações e, quando relevante, devem rever estas informações de forma proporcionada. No quadro desta revisão, as autoridades competentes devem ter em consideração:

a. o impacto potencial de uma perturbação significativa dos sistemas de TIC da instituição no sistema financeiro a nível nacional ou internacional;
b. se a instituição pode estar exposta a riscos de segurança das TIC ou a riscos de disponibilidade e continuidade das TIC devido a dependências à Internet, a adoção massiva de soluções de TIC inovadoras ou de outros canais de distribuição empresariais que possam torná-la um alvo mais suscetível a ciberataques;
c. se a instituição pode estar mais exposta a riscos de segurança, de disponibilidade e continuidade, de integridade de dados ou alteração de TIC devido à complexidade (tal como na sequência de fusões ou aquisições) ou à desatualização dos seus sistemas de TIC;
d. se a instituição está a implementar alterações significativas aos seus sistemas de TIC e/ou à função de TIC (por exemplo na sequência de fusões, aquisições, alienações ou substituição dos seus sistemas de TIC *core*), o que pode ter impacto negativo na estabilidade ou no bom funcionamento dos sistemas de TIC, podendo resultar em riscos de disponibilidade e continuidade, de segurança, de alteração e de integridade de dados de TIC significativos;
e. se a instituição contratou externamente serviços ou sistemas de TIC dentro ou fora do grupo, que a possa expor a riscos significativos associados a essa contratação externa;
f. se a instituição está a implementar medidas agressivas de redução de custos ao nível das TIC que possam levar à redução de investimentos, recursos e competências em TIC que sejam necessários e possam aumentar a exposição a todos os tipos de riscos de TIC na taxonomia;
g. se a localização de operações de TIC/centros de dados importantes (por exemplo, regiões, países) pode expor a instituição a catástrofes naturais (como cheias, sismos), instabilidade política ou conflitos laborais e distúrbios civis que possam levar a um aumento significativo dos riscos de disponibilidade e continuidade das TIC e dos riscos de segurança das TIC.

3.2.2 Revisão dos sistemas e serviços de TIC críticos

40. No quadro do processo para a identificação dos riscos de TIC com um potencial impacto prudencial significativo na instituição, as autoridades competentes devem rever a documentação da instituição e formar uma opinião sobre os sistemas e serviços de TIC considerados críticos para a disponibilidade, continuidade, segurança e funcionamento adequados das atividades essenciais da instituição.

41. Para esse efeito, as autoridades competentes devem rever a metodologia e os processos aplicados pela instituição para identificar os sistemas e serviços de TIC críticos, tendo em conta que alguns sistemas e serviços de TIC podem ser considerados críticos pela instituição de uma perspetiva de continuidade do negócio e disponibilidade, de uma perspetiva de segurança (como prevenção de fraudes) e/ou de uma perspetiva de confidencialidade (como dados confidenciais). Aquando da revisão, as autoridades competentes devem efetuar a revisão tendo em consideração que os sistemas e serviços de TIC críticos devem satisfazer pelo menos uma das seguintes condições:

a. suportam as operações de negócio e canais de distribuição (por exemplo, caixas automáticas, serviços bancários *online* e móveis) da instituição;

b. suportam os processos de governo e as funções empresariais fundamentais, incluindo a gestão de riscos (por exemplo, sistemas de gestão de riscos e gestão de tesouraria);

c. enquadram-se em requisitos legais ou regulamentares especiais (se existentes) que impõem requisitos de disponibilidade, resistência, confidencialidade ou segurança reforçados (nomeadamente legislação de proteção de dados ou «Objetivos de tempo de recuperação» (RTO, o tempo máximo durante o qual um sistema ou processo tem de ser restabelecido após um incidente) e «Objetivo de ponto de recuperação» (RPO, o período máximo de perda de dados em caso de incidente)) para alguns serviços importantes do ponto de vista sistémico (se e quando aplicável);

d. processam ou armazenam dados confidenciais ou sensíveis aos quais o acesso não autorizado poderia ter impacto significativo na reputação da instituição, nos resultados financeiros ou na solidez e continuidade da respetiva atividade (como bases de dados com dados confidenciais sobre clientes); e/ou

e. disponibilizam funcionalidades base que são vitais para o bom funcionamento da instituição (como serviços de telecomunicações e conectividade, serviços de TIC e de cibersegurança).

3.2.3 Identificação de riscos de TIC significativos para os sistemas e serviços de TIC críticos

42. Tendo em conta as revisões realizadas do perfil de risco de TIC da instituição e dos sistemas e serviços de TIC críticos acima indicados, as autoridades competentes devem formar uma opinião sobre os riscos de TIC significativos que, segundo a sua avaliação de supervisão, possam ter um impacto prudencial significativo nos sistemas e serviços de TIC críticos da instituição.

43. Ao avaliarem o potencial impacto dos riscos de TIC nos sistemas e serviços de TIC críticos de uma instituição, as autoridades competentes devem ter em consideração:

a. o impacto financeiro, incluindo, entre outros, a perda de fundos ou ativos, a potencial compensação de clientes, os custos legais ou de recuperação, os danos contratuais e a perda de receitas;

b. a potencial perturbação das atividades, tendo em consideração, entre outros, a criticidade dos serviços financeiros afetados, o número de clientes e/ou sucursais e funcionários potencialmente afetados;

c. o potencial impacto na reputação da instituição com base na criticidade do serviço bancário ou atividade operacional afetada (como roubo de dados de clientes); o perfil/visibilidade externa dos sistemas e serviços de TIC afetados (como sistemas bancários *online* ou móveis, pontos de venda, caixas automáticas ou sistemas de pagamento);

d. o impacto regulamentar, incluindo o potencial de censura pública por parte do regulador, multas ou mesmo alteração das autorizações;

e. o impacto estratégico na instituição, por exemplo, se o produto ou os planos de negócio estratégicos forem comprometidos ou roubados.

44. As autoridades competentes devem em seguida mapear os riscos de TIC identificados que sejam considerados significativos nas categorias de risco de TIC indicadas abaixo para as quais são fornecidas descrições adicionais do risco e exemplos no Anexo. As autoridades competentes devem debruçar-se sobre os riscos de TIC referidos no Anexo, no quadro da avaliação nos termos do Título 3:

a. Risco de disponibilidade e continuidade das TIC
b. risco de segurança das TIC
c. risco de alteração das TIC
d. risco de integridade de dados das TIC
e. risco de contração externa de TIC

A mapeamento visa auxiliar as autoridades competentes na determinação dos riscos significativos (se existentes) e, por conseguinte, deve ser objeto de uma revisão mais rigorosa e/ou aprofundada nos seguintes procedimentos de avaliação.

3.3 Avaliação dos controlos para reduzir os riscos de TIC significativos

45. Para avaliaram a exposição a riscos de TIC residuais da instituição, as autoridades competentes devem rever a forma como a instituição identifica, monitoriza, avalia e mitiga os riscos significativos identificados pelas autoridades competentes na avaliação supramencionada.

46. Para o efeito, para os riscos de TIC significativos identificados, as autoridades competentes devem rever os elementos aplicáveis:

a. política de gestão de risco, processos e limiares de tolerância ao risco de TIC;
b. gestão organizacional e estrutura de supervisão;
c. cobertura e conclusões da auditoria interna; e
d. controlos de risco de TIC específicos para o risco de TIC significativo identificado.

47. A avaliação deve ter em conta o resultado da análise da estrutura global de gestão de risco e controlo interno tal como referido no Título 5 das Orientações da EBA relativas ao SREP, assim como o governo e a estratégia da instituição abordados no Título 2 das presentes orientações, uma vez que as deficiências significativas identificadas nestas áreas podem ter influência na capacidade da instituição gerir e mitigar as respetivas exposições a riscos de TIC. Quando relevante, as autoridades competentes devem também utilizar as fontes de informação referidas no n.º 37 das presentes orientações.

48. As autoridades competentes devem executar os seguintes procedimentos de avaliação de uma forma que seja proporcional à natureza, à escala e à complexidade das atividades da instituição e através da aplicação de uma revisão de supervisão apropriada ao perfil de risco de TIC da instituição.

3.3.1 Política de gestão de risco, processos e limiares de tolerância ao risco de TIC

49. As autoridades competentes devem rever se a instituição possui políticas de gestão de risco, processos e limiares de tolerância adequados em vigor para os riscos de TIC significativos identificados. Estes podem fazer parte de uma estrutura de gestão de risco operacional ou constituírem um documento separado. Para esta avaliação, as autoridades competentes devem ter em consideração se:

    a. a política de gestão de risco está formalizada e foi aprovada pelo órgão de administração e contém orientações suficientes sobre a apetência pelo risco de TIC da instituição e sobre os principais objetivos de gestão de risco de TIC pretendidos e/ou os limiares de tolerância ao risco de TIC aplicados. A política de gestão de risco de TIC pertinente deve ser igualmente comunicada a todas as partes interessadas relevantes;

    b. a política aplicável abrange todos os elementos importantes para a gestão de risco referente aos riscos de TIC significativos identificados;

    c. a instituição implementou um processo e os procedimentos subjacentes para a identificação (por exemplo, «autoavaliações de controlo do risco » (RCSA), análise de cenários de risco) e a monitorização dos riscos de TIC significativos envolvidos; e

    d. a instituição tem em vigor reportes de gestão de risco de TIC que fornecem informações atempadas à direção de topo e ao órgão de administração e que permitem que a direção de topo e/ou órgão de administração avalie e monitorize se os planos e medidas de mitigação de risco de TIC da instituição são consistentes com a apetência pelo risco e/ou os limiares de tolerância aprovados (quando relevante) e monitorize também as alterações de riscos de TIC significativos.

3.3.2 Gestão organizacional e estrutura de supervisão

50. As autoridades competentes devem avaliar a forma como os papéis e responsabilidades a nível da gestão de riscos aplicáveis estão incluídas e integradas na organização interna para gerir e controlar os riscos de TIC significativos identificados. A este respeito, as autoridades competentes devem avaliar se a instituição demonstra:

    a. possuir papéis e responsabilidades claras para a identificação, avaliação, monitorização, mitigação, reporte e supervisão dos riscos de TIC significativos envolvidos;

    b. que as responsabilidades e papéis relativos aos riscos são comunicados, atribuídos e integrados de forma explícita em todos os setores (por exemplo, segmentos de atividade, TI) e processos relevantes da organização, incluindo os papéis e responsabilidades para reunir e agregar a informação sobre os riscos e reportá-la à direção de topo e/ou órgão de administração;

    c. que as atividades de gestão de risco de TIC são efetuadas com recursos humanos e técnicos suficientes e adequados do ponto de vista qualitativo e quantitativo. Para a avaliação da credibilidade dos planos de redução de riscos aplicáveis, as autoridades competentes devem avaliar também se a instituição atribuiu orçamentos financeiros suficientes e/ou outros recursos necessários para a sua implementação;

d. dar um seguimento e resposta apropriados por parte do órgão de administração relativamente às conclusões importantes das funções de controlo independente referentes ao risco de TIC, tendo em conta a possível delegação de alguns aspetos a um comité, caso exista; e
e. que as exceções às regulamentações e políticas de TIC aplicáveis são registadas e submetidas a uma revisão documentada e reportadas pela função de controlo independente com ênfase nos riscos associados.

3.3.3 Cobertura e conclusões da auditoria interna

51. As autoridades competentes devem ter em consideração se a função de auditoria interna é eficaz no que se refere à auditoria da estrutura de controlo de risco de TIC aplicável, revendo se:

    a. a estrutura de controlo de risco de TIC é auditada com a qualidade, exaustividade e frequência exigidas e é proporcional à dimensão, às atividades e ao perfil de risco de TIC da instituição;
    b. o plano de auditoria inclui auditorias dos riscos de TIC críticos identificados pela instituição;
    c. as conclusões importantes da auditoria de TIC, incluindo as ações acordadas, são comunicadas ao órgão de administração; e
    d. as conclusões de auditorias de TIC, incluindo as ações acordadas, são acompanhadas e os relatórios do progresso são revistos periodicamente pela direção de topo e/ou o comité de auditoria.

3.3.4 Controlos de risco de TIC específicos para o risco de TIC significativo identificado

52. Relativamente aos riscos de TIC significativos identificados, as autoridades competentes devem avaliar se a instituição tem em vigor controlos específicos para endereçar esses riscos. As secções que se seguem apresentam uma lista não exaustiva dos controlos específicos que devem ser tidos em consideração aquando da avaliação dos riscos significativos identificados nos termos do 3.2.3 que foram mapeados às seguintes categorias de risco de TIC:

    a. riscos de disponibilidade e continuidade das TIC;
    b. riscos de segurança das TIC;
    c. riscos de alteração das TIC;
    d. riscos de integridade de dados das TIC;
    e. riscos de contratação externa das TIC.

(a) Controlos para a gestão de riscos significativos de disponibilidade e continuidade das TIC

53. Para além dos requisitos estabelecidos nas Orientações da EBA relativas ao SREP (números 279 - 281), as autoridades competentes devem avaliar se a instituição implementou a estrutura adequada para identificar, compreender, medir e mitigar os riscos de disponibilidade e continuidade das TIC.

54. Para esta avaliação, as autoridades competentes devem ter em consideração, em particular, se a estrutura:

a. identifica os processos de TIC críticos e os sistemas de TIC de apoio relevantes que devem fazer parte dos planos de resiliência e continuidade do negócio com:

i. uma análise detalhada das dependências entre os processos de negócio críticos e os sistemas de suporte;

ii. a determinação de objetivos de recuperação para os sistemas de TIC de suporte (por exemplo, tipicamente determinados pela empresa e/ou regulamentações em termos de RTO e RPO);

iii. um plano de contingência apropriado para permitir a disponibilidade, a continuidade e a recuperação de sistemas e serviços de TIC críticos por forma a minimizar a perturbação das operações da instituição dentro de limites aceitáveis.

b. demonstra a resiliência do negócio e possui políticas e normas referentes ao ambiente de controlo da continuidade e controlos operacionais que incluem:

i. medidas para evitar que um único cenário, incidente ou catástrofe possa ter impacto nos sistemas de produção e recuperação das TIC;

ii. procedimentos de salvaguarda e recuperação do sistema de TIC para *software* e dados críticos que garantam que as cópias de salvaguarda sejam guardadas num local seguro e suficientemente remoto para que um incidente ou uma catástrofe não destruam ou corrompam estes dados críticos;

iii. soluções de monitorização para a deteção atempada de incidentes de disponibilidade ou continuidade das TIC;

iv. um processo documentado de gestão de incidentes e escalonamento, que também forneça orientações sobre os diferentes papéis e responsabilidades ao nível da gestão de incidentes e escalonamento, os membros dos comités de crise e a cadeia de comando em caso de emergência;

v. medidas físicas para proteger a infraestrutura de TIC crítica da instituição (como centros de dados) de riscos ambientais (como cheias e outras catástrofes naturais) e assegurar um ambiente operacional apropriado para sistemas de TIC (como ar condicionado);

vi. processos, papéis e responsabilidades para garantir que os sistemas e serviços de TIC contratados externamente estão igualmente abrangidos pelas soluções e planos de resiliência e continuidade do negócio;

vii. soluções de planeamento e monitorização do desempenho e da capacidade das TIC para sistemas e serviços de TIC críticos com requisitos de disponibilidade definidos, para deteção de restrições importantes a nível de desempenho e capacidade atempadamente;

viii. soluções para proteger atividades ou serviços críticos na Internet (como serviços de banca eletrónica), quando necessário e apropriado, contra a negação de serviço e outros ciberataques

provenientes da Internet, com o objetivo de impedirem ou perturbarem o acesso a estas atividades e serviços.

c. testa soluções de disponibilidade e continuidade das TIC face a um conjunto de cenários realistas incluindo ciberataques, testes a falhas e testes de cópias de salvaguarda para *software* e dados críticos que:

   i. são planeados, formalizados e documentados, sendo os resultados dos testes utilizados para reforçar a eficácia das soluções de disponibilidade e continuidade das TIC;

   ii. incluem partes interessadas e funções dentro da organização, como gestão de linhas de produtos incluindo equipas de continuidade do negócio e de resposta a incidentes e crises, bem como partes interessadas externas relevantes no ecossistema;

   iii. a direção de topo e o órgão de administração estão devidamente envolvidos no processo (como parte das equipas de gestão de crises) e são informados sobre os resultados dos testes.

(b) Controlos para a gestão de riscos de segurança das TIC significativos

55. As autoridades competentes devem avaliar se a instituição implementou uma estrutura eficaz para identificar, compreender, medir e mitigar os riscos de segurança das TIC. Para esta avaliação, as autoridades competentes devem ter em consideração, em particular, se a estrutura tem em conta:

a. papéis e responsabilidades claramente definidos no que se refere a:
   i. pessoas e/ou comités que são encarregados e/ou responsáveis pela gestão diária da segurança das TIC e pela elaboração das políticas de segurança globais de TIC, tendo em especial atenção a sua necessária independência;
   ii. conceção, implementação, gestão e monitorização dos controlos de segurança das TIC;
   iii. proteção de sistemas e serviços de TIC críticos através da adoção, por exemplo, de um processo de avaliação da vulnerabilidades, gestão de correções de segurança de *software*, proteção de pontos terminais (nomeadamente, vírus *malware*), deteção de intrusão e ferramentas de prevenção;
   iv. monitorização, classificação e tratamento de incidentes de segurança das TIC externos ou internos, incluindo a resposta a incidentes e o restabelecimento e recuperação dos sistemas e serviços de TIC;
   v. avaliações regulares e pró-ativas de ameaças para manutenção de controlos de segurança apropriados.

b. uma política de segurança de TIC que tenha em consideração e, quando apropriado, siga as normas de segurança de TIC e os princípios de segurança reconhecidos internacionalmente (como o «princípio dos privilégios mínimos», ou seja, limitando o acesso ao nível mínimo que permite o normal funcionamento para a gestão de direitos de acesso, e o princípio de «defesa em profundidade», *i.e.*, mecanismos de segurança por camadas visando aumentar a segurança do sistema como um todo para a criação de uma arquitetura de segurança);

c. um processo para identificar sistemas, serviços e requisitos de segurança das TIC compatíveis que reflitam o potencial risco de fraude e/ou possíveis utilizações indevidas e/ou abusos de dados confidenciais, juntamente com expectativas de segurança documentadas que devem ser seguidos para os sistemas, serviços e dados das TIC identificados, em conformidade com a tolerância ao risco da instituição, e monitorizados quanto à sua correta implementação;

d. um processo documentado de gestão de incidentes de segurança e escalonamento, que forneça orientações sobre os diferentes papéis e responsabilidades a nível da gestão de incidentes e escalonamento, os membros do(s) comité(s) de crise e a cadeia de comando em caso de emergências de segurança;

e. um registo das atividades dos utilizadores e dos administradores para permitir uma monitorização eficaz e a deteção e resposta atempadas a atividades não autorizadas; para apoiar ou realizar investigações forenses de incidentes de segurança. A instituição deve ter em vigor políticas de registo que definam os tipos indicados de registo que devem ser mantidos e o respetivo período de retenção;

f. campanhas ou iniciativas de sensibilização e informação para informar todos os níveis da instituição sobre a utilização segura e a proteção dos sistemas de TIC da instituição e os principais riscos de segurança (e outros) das TIC dos quais devem estar cientes, em particular no que se refere a ciberameaças existentes e emergentes (como vírus informáticos, possíveis abusos ou ataques internos ou externos, ciberataques) e a sua função na mitigação das falhas de segurança;

g. medidas de segurança física adequadas (como CCTV, alarme anti-roubo, portas de segurança) para prevenção de acesso físico não autorizado a sistemas de TIC críticos e sensíveis (como centros de dados);

h. medidas para proteger os sistemas de TIC de ataques via Internet (*i.e.*, ciberataques) ou outras redes externas (como ligações tradicionais de telecomunicações ou ligações a parceiros fidedignos). As autoridades competentes devem analisar se a estrutura da instituição tem em consideração:

    i. um processo e soluções para manter um inventário completo e atualizado e uma descrição de todos os pontos de ligação de rede virados para o exterior (como *websites*, aplicações da Internet, redes sem fios, acesso remoto) através dos quais terceiros possam entrar nos sistemas de TIC internos;

    ii. medidas de segurança rigorosamente geridas e monitorizadas (como *firewalls*, servidores *proxy*, retransmissores de correio, detetores antivírus e de conteúdo) para proteger o tráfego de rede recebido e enviado (por exemplo, e-mail) e as ligações de rede viradas para o exterior através das quais terceiros possam entrar nos sistemas de TIC internos;

    iii. processos e soluções para proteger *websites* e aplicações que possam ser atacados diretamente a partir da Internet e/ou do exterior, podendo servir de ponto de entrada nos sistemas de TIC internos. Em geral, incluem um conjunto de práticas de desenvolvimento seguras reconhecidas, proteção do sistema de TIC e práticas de deteção de vulnerabilidades e/ou a implementação de soluções de segurança adicionais como, por exemplo, *firewalls* de aplicações e/ou sistemas de deteção de intrusão (IDS) e/ou de prevenção de intrusão (IPS);

    iv. testes de penetração de segurança periódicos para avaliar a eficácia da implementação de medidas e processos de cibersegurança e de segurança interna das TIC. Estes testes devem

ser realizados por funcionários e/ou peritos externos com as competências necessárias, com resultados de testes documentados e conclusões reportadas à direção de topo e/ou ao órgão de administração. Quando necessário e aplicável, a instituição deve ter conhecimento destes testes para melhorar os controlos e processos de segurança e/ou para obter mais garantias da sua eficácia.

(c) Controlos para a gestão de riscos de alteração das TIC significativos

56. As autoridades competentes devem avaliar se a instituição possui uma estrutura eficaz para identificar, compreender, medir e mitigar o risco de alteração das TIC proporcional à natureza, à escala e à complexidade das atividades da instituição e ao perfil de risco de TIC da instituição. A estrutura da instituição deve abranger os riscos associados ao desenvolvimento, teste e aprovação de alterações aos sistemas de TIC, incluindo o desenvolvimento ou alteração de *software*, antes da sua migração para o ambiente de produção, garantindo uma gestão adequada do ciclo de vida das TIC. Para esta avaliação, as autoridades competentes devem ter em consideração, em particular, se a estrutura tem em conta:

a. processos documentados para a gestão e controlo de alterações aos sistemas de TIC (como configuração e gestão de correções de segurança) e dados (como correção de erros ou de dados), garantindo o envolvimento apropriado da gestão de riscos de TIC para importantes alterações das TIC que possam ter um impacto significativo no perfil de risco ou exposição da instituição;

b. especificações referentes à necessária segregação de funções durante as diferentes fases dos processos de alteração das TIC implementados (como conceção e desenvolvimento de soluções, testes e aprovação de novo *software* e/ou de alterações, migração e implementação no ambiente de produção, e correção de erros), com ênfase nas soluções implementadas e na segregação de funções para gerir e controlar as alterações aos sistemas de TIC de produção e dados pela equipa de TIC (como programadores, administradores de sistemas de TIC, administradores de bases de dados) ou outras partes (como utilizadores de negócio, prestadores de serviços);

c. ambientes de teste que reflitam adequadamente os ambientes de produção;

d. um inventário de ativos das aplicações e sistemas de TIC existentes no ambiente de produção, assim como no ambiente de testes e desenvolvimento, para que as alterações necessárias (como atualizações de versões, aplicação de correções de segurança a sistemas, alterações de configuração) possam ser geridas, implementadas e monitorizadas apropriadamente para os sistemas de TIC envolvidos;

e. um processo para monitorizar e gerir o ciclo de vida dos sistemas de TIC utilizados, para garantir que continuam a satisfazer e a apoiar os requisitos atuais de gestão de negócio e de riscos e para assegurar que as soluções e os sistemas de TIC utilizados ainda são suportados pelos respetivos fornecedores e que este processo é acompanhado por procedimentos adequados do ciclo de vida de desenvolvimento de *software* (SDLC);

f. um sistema de controlo de código fonte de *software* e procedimentos apropriados para evitar alterações não autorizadas no código fonte de *software* desenvolvido internamente;

g. um processo para realizar a deteção de segurança e de vulnerabilidades de sistemas e *software* de TIC novos ou com alterações significativas, antes de serem enviados para produção e expostos a possíveis ciberataques;

h. um processo e soluções para prevenir a divulgação não autorizada ou não intencional de dados confidenciais ao substituir, arquivar, eliminar ou destruir sistemas de TIC;

i. processos independentes de revisão e validação para reduzir os riscos de erros humanos ao serem efetuadas alterações aos sistemas de TIC que possam ter um importante efeito negativo na disponibilidade, continuidade ou segurança da instituição (por exemplo, alterações importantes na configuração da *firewall*) ou na segurança da instituição (como alterações às *firewalls*).

(d) Controlos para a gestão de riscos de integridade de dados das TIC significativos

57. As autoridades competentes devem avaliar se a instituição possui uma estrutura eficaz para identificar, compreender, medir e mitigar o risco de integridade de dados das TIC proporcional à natureza, à escala e à complexidade das atividades da instituição e ao perfil de risco de TIC da instituição. A estrutura da instituição deve ter em conta os riscos associados à preservação da integridade dos dados guardados e processados pelos sistemas de TIC. Para esta avaliação, as autoridades competentes devem ter em consideração, em particular, se o modelo tem em conta:

a. uma política que defina os papéis e responsabilidades para a gestão da integridade dos dados nos sistemas de TIC (como arquiteto de dados, responsáveis pelos dados[6], responsáveis pela conservação de dados[7], proprietários/responsáveis pela gestão de dados[8]) e forneça orientações sobre os dados considerados críticos de uma perspetiva de integridade dos dados e que deve ser submetida a controlos de TIC específicos (como controlos de validação de introdução automática, controlos de transferência de dados, reconciliações, etc.) ou revisões (como uma verificação da compatibilidade com a arquitetura de dados) nas diferentes fases do ciclo de vida dos dados de TIC;

b. uma arquitetura de dados, modelo de dados e/ou dicionário documentados e validados pelas partes interessadas relevantes ao nível do negócio e de TIC para apoiar a consistência de dados necessária nos sistemas de TIC e para garantir que a arquitetura de dados, modelo de dados e/ou dicionário permanecem alinhados com as necessidades de negócio e de gestão de riscos;

c. uma política referente à utilização autorizada da informática na ótica do utilizador final e à respetiva fiabilidade, em particular no que se refere à identificação, registo e documentação de soluções importantes de informática na ótica do utilizador final (por exemplo, ao processar dados importantes) e aos níveis de segurança esperados para prevenção de alterações não autorizadas, tanto na própria ferramenta como nos dados aí armazenados;

d. processos documentados de tratamento de exceções para resolver problemas de integridade de dados de TIC identificados de acordo com a respetiva criticidade e sensibilidade.

[6] Um responsável pelos dados tem como responsabilidades o processamento e a gestão de dados.

[7] Um responsável pela conservação dos dados tem como responsabilidades a conservação, transporte e armazenamento seguros de dados.

[8] Um responsável pela gestão de dados tem como responsabilidades a gestão e adequação de elementos de dados – conteúdo e metadados.

58. Para as instituições supervisionadas que estão abrangidas pelo âmbito dos princípios do Regulamento n.º 239 do BCBS para a agregação eficaz de dados sobre riscos e o reporte de informações sobre riscos[9], as autoridades competentes devem rever a análise de risco da instituição relativamente às suas capacidades de reporte de informações sobre riscos e de agregação de dados, em comparação com os princípios e a documentação preparada sobre o assunto, tendo em consideração o calendário de implementação e as medidas transitórias nesses princípios.

(e) Controlos para a gestão de riscos de contratação externa de TIC significativos

59. As autoridades competentes devem avaliar se a estratégia de contratação externa da instituição, em conformidade com as Orientações do CEBS relativas à contratação externa (2006) e com o requisito no n.º 85, alínea d) das Orientações da EBA relativas ao SREP, é aplicada corretamente à contratação externa de TIC, incluindo contratação externa intragrupo para o fornecimento de serviços de TIC dentro do grupo. Ao avaliarem os riscos de contratação externa de TIC, as autoridades competentes devem ter em consideração que os riscos de contratação externa de TIC podem também ser tratados como parte da avaliação dos riscos operacionais inerentes, nos termos do n.º 240, alínea j) das Orientações da EBA relativas ao SREP, para evitar qualquer duplicação de trabalho ou contagem dupla.

60. As autoridades competentes devem avaliar, especificamente, se a instituição tem uma estrutura eficaz em vigor para identificar, compreender e medir o risco de contratação externa de TIC e, em particular, controlos e um ambiente de controlo implementados para mitigar riscos significativos relacionados com serviços de TIC contratados externamente, proporcionais à dimensão, às atividades e ao perfil de risco de TIC da instituição e que incluam:

    a. uma avaliação do impacto da contratação externa de TIC sobre a gestão de riscos da instituição relativamente ao recurso a prestadores de serviço (por exemplo, fornecedores de serviço em nuvem) e aos respetivos serviços durante o processo de aquisição documentado e tido em conta pela direção de topo ou o órgão de administração para a decisão de contratar ou não externamente os serviços. A instituição deve rever as políticas de gestão de riscos de TIC, os controlos de TIC e o ambiente de controlo do prestador de serviço para garantir que cumprem os objetivos de gestão de riscos internos e a apetência pelo risco da instituição. Esta revisão deve ser atualizada periodicamente durante o período contratual de contratação externa, tendo em conta as características dos serviços contratados externamente;

    b. uma monitorização dos riscos de TIC dos serviços contratados externamente durante o período contratual como parte da gestão de riscos da instituição, que contribui para os reportes de gestão de risco de TIC da instituição (como reportes sobre a continuidade da atividade, reportes de segurança);

    c. uma monitorização e comparação dos níveis de serviço recebidos comparativamente aos níveis de serviço acordados contratualmente que devem fazer parte do contrato de contratação externa ou do acordo de nível de serviço (SLA); e

[9] Comité de Basileia de Supervisão Bancária, Princípios para a agregação eficaz de dados sobre o risco e a prestação eficaz de informação sobre o risco, janeiro de 2013, disponível *online*: http://www.bis.org/publ/bcbs239.pdf.

d. pessoal, recursos e competências adequadas para monitorizar e gerir os riscos de TIC dos serviços contratados externamente.

3.4 Síntese das conclusões e da notação

61. Na sequência da avaliação supramencionada, as autoridades competentes devem formar uma opinião sobre o risco de TIC da instituição. Esta opinião deve estar refletida numa síntese das conclusões que as autoridades competentes devem ter em consideração na atribuição da notação do risco operacional no Quadro 6 das Orientações da EBA relativas ao SREP. As autoridades competentes devem basear a sua opinião nos riscos de TIC significativos tendo em conta as seguintes considerações que serão integradas na avaliação de risco operacional:

a. Considerações relativas aos riscos

i. O perfil e as exposições ao risco de TIC da instituição;
ii. Os sistemas e serviços de TIC críticos identificados; e
iii. A relevância do risco de TIC relativamente a sistemas de TIC críticos.

b. Considerações sobre gestão e controlos

i. Se existe coerência entre a política e a estratégia de gestão de risco de TIC da instituição e a estratégia e a apetência globais pelo risco;
ii. Se a estrutura organizacional para gestão de risco de TIC é sólido, com responsabilidades claramente definidas e uma separação nítida de tarefas entre os responsáveis pela assunção de riscos e as funções de gestão e controlo;
iii. Se os sistemas de medição, monitorização e reporte de risco de TIC são adequados; e
iv. Se as estruturas de controlo para riscos de TIC significativos são sólidos.

62. Se as autoridades competentes considerarem que o risco de TIC é significativo e a autoridade competente decidir avaliar e atribuir uma notação a este risco como uma subcategoria de risco operacional, o quadro abaixo (Quadro 1) apresenta as considerações sobre notação de riscos de TIC.

Quadro 1: Considerações do supervisor relativas à atribuição de uma notação de risco de TIC

Notação atribuída ao risco	Opinião do supervisor	Considerações relativas ao risco inerente	Considerações relativas à gestão e aos controlos adequados
1	Não foram identificados riscos de impacto prudencial significativo na instituição, tendo	• As fontes de informação que devem ser consideradas nos termos do n.º 37 não revelaram quaisquer exposições significativas a riscos de TIC. • A natureza do perfil de risco de	

	em conta o nível de risco inerente, a gestão e os controlos.	TIC da instituição, em conjunto com a revisão dos sistemas de TIC críticos e os riscos de TIC significativos para os sistemas e serviços de TIC, não revelaram quaisquer riscos significativos das TIC.	
2	Existe um risco baixo de impacto prudencial significativo na instituição, tendo em conta o nível de risco inerente, a gestão e os controlos.	• As fontes de informação que devem ser consideradas nos termos do n.º 37 não revelaram quaisquer exposições significativas a riscos de TIC. • A natureza do perfil de risco de TIC da instituição, em conjunto com a revisão dos sistemas de TIC críticos e os riscos de TIC significativos para os sistemas e serviços de TIC, revelaram uma exposição limitada a riscos das TIC (por exemplo, a não mais do que em 2 das 5 categorias de riscos de TIC predefinidas).	• A política e a estratégia de gestão de risco de TIC da instituição são proporcionais à sua estratégia e à apetência globais pelo risco. • A estrutura organizacional para risco de TIC é sólido, com responsabilidades claramente definidas e uma separação nítida de tarefas entre os responsáveis pela assunção de riscos e as funções de gestão e controlo. • Os sistemas de medição, monitorização e reporte de riscos de TIC são adequados. • A estrutura de controlo para riscos de TIC é sólido.
3	Existe um risco médio de impacto prudencial significativo na instituição, tendo em conta o nível de risco inerente, a gestão e os controlos.	• As fontes de informação que devem ser consideradas nos termos do n.º 37 revelaram indícios de possíveis exposições significativas a riscos de TIC. • A natureza do perfil de risco de TIC da instituição, em conjunto com a revisão dos sistemas de TIC críticos e os riscos de TIC significativos para os sistemas e serviços de TIC, revelaram uma exposição aumentada a riscos das TIC (por exemplo, a 3 ou mais das 5 categorias de riscos de TIC predefinidas).	
4	Existe um risco elevado de impacto prudencial significativo na instituição, tendo em conta o nível de risco inerente, a	• As fontes de informação que devem ser consideradas nos termos do n.º 37 forneceram vários indícios de exposições significativas a riscos de TIC. • A natureza do perfil de risco de TIC da instituição, em conjunto	

	gestão e os controlos.	com a revisão dos sistemas de TIC críticos e os riscos de TIC significativos para os sistemas e serviços de TIC, revelaram uma exposição elevada a riscos das TIC (por exemplo, a 4 ou 5 das 5 categorias de riscos de TIC predefinidas).	

Anexo – Taxonomia de risco das TIC

5 categorias de risco das TIC com uma lista não exaustiva de riscos de TIC com uma potencial gravidade elevada e/ou impacto operacional, reputacional ou financeiro

Categorias de risco das TIC	Riscos de TIC (lista não exaustiva[10])	Descrição do risco	Exemplos
Riscos de disponibilidade e continuidade das TIC	Gestão inadequada da capacidade	Uma falta de recursos (como *hardware*, *software*, pessoal, prestadores de serviços) pode resultar numa incapacidade de escalar o serviço para responder às necessidades do negócio, interrupções do sistema, degradação do serviço e/ou erros operacionais.	• Um défice de capacidade pode afetar as taxas de transmissão e a disponibilidade da rede (Internet) para serviços como banca eletrónica. • Uma falta de pessoal (interno ou de terceiros) pode resultar em interrupções do sistema e/ou erros operacionais.
	Falhas do sistema de TIC	Uma perda de disponibilidade devido a falhas de *hardware*.	• Falhas/anomalias de armazenamento (discos rígidos), servidor ou outros equipamentos de TIC causadas por falta de manutenção, por exemplo.
		Uma perda de disponibilidade devido a falhas de *software* e erros.	• Um ciclo infinito numa aplicação evita a execução de transações. • Interrupções devido à utilização continuada de sistemas e soluções de TIC desatualizados que já não cumprem os atuais requisitos de disponibilidade e resiliência e/ou já não são suportados pelos fornecedores.
	Planeamento inadequado de continuidade das TIC e recuperação após desastre	Falha da disponibilidade planeada das TIC e/ou das soluções de continuidade e/ou da recuperação após desastre (como num centro de dados de recuperação após falha) quando ativadas em resposta a um incidente.	• As diferenças de configuração entre o centro de dados primário e secundário podem resultar na incapacidade do centro de dados de recuperação fornecer a continuidade planeada do serviço.
	Ciberataques	Ataques com diferentes fins (como ativismo,	• Os ataques de Negação de serviço distribuído são

[10] Os riscos das TIC são listados na categoria de risco onde têm maior impacto, mas também podem ter impacto em outras categorias de risco

Categorias de risco das TIC	Riscos de TIC (lista não exaustiva[10])	Descrição do risco	Exemplos
	disruptivos e destrutivos	chantagem), que resultem numa sobrecarga de sistemas e de rede, impedindo o acesso a serviços *online* pelos seus utilizadores legítimos.	realizados através de vários sistemas informáticos na Internet controlados por piratas informáticos, que enviam uma grande quantidade de pedidos de serviço aparentemente legítimos para serviços *online* (como banca eletrónica).
Riscos de segurança das TIC	Ciberataques e outros ataques com base em TIC externas	Ataques efetuados a partir da Internet ou de redes externas para diferentes fins (como fraude, espionagem, ativismo/sabotagem, ciberterrorismo) com recurso a várias técnicas (como engenharia social, tentativas de intrusão através da exploração de vulnerabilidades, desenvolvimento de *software* malicioso) para assumir o controlo de sistemas de TIC internos.	Diferentes tipos de ataques: • APT (Ameaça avançada persistente) para assumir o controlo de sistemas internos ou roubar informações (como informações relacionadas com roubo de identidade, informações de cartões de crédito). • *Software* malicioso (como *ransomware*) que cifra dados com o objetivo de fazer chantagem. • Infeção de sistemas de TIC internos com cavalos de Troia para cometer ações maliciosas no sistema de forma oculta. • Exploração de vulnerabilidades do sistema de TIC e/ou aplicações (*web*) (como injeção de SQL, etc.) para obter acesso ao sistema de TIC interno.
		Execução de transações de pagamento fraudulentas por piratas informáticos através da quebra ou violação da segurança de serviços de banca eletrónica e pagamento e/ou através do ataque e exploração das vulnerabilidades de segurança nos sistemas de pagamento internos da instituição.	• Ataques a serviços de banca eletrónica ou de pagamento, com o objetivo de efetuar transações não autorizadas. • A criação e o envio de transações de pagamento fraudulentas a partir dos sistemas de pagamento interno da instituição (como mensagens *SWIFT* fraudulentas).
		Execução de transações de títulos fraudulentas por piratas informáticos através da quebra ou violação da segurança de serviços de banca eletrónica que também dão acesso às contas de títulos do cliente.	• Ataques «pump and dump» em que os atacantes obtêm acesso a contas de títulos de clientes através da banca eletrónica e colocam ordens de compra ou venda fraudulentas para influenciar o preço de mercado e/ou obter lucros com base nas posições

Categorias de risco das TIC	Riscos de TIC (lista não exaustiva[10])	Descrição do risco	Exemplos
			dos títulos estabelecidas anteriormente.
		Ataques a ligações de comunicação e conversas de todos os tipos ou sistemas de TIC com o objetivo de recolher informações e/ou cometer fraudes.	• Escuta clandestina/interceção de transmissão não protegida de dados de autenticação em texto simples.
	Segurança interna inadequada das TIC	Obtenção de acesso não autorizado a sistemas de TIC críticos a partir da instituição para diferentes fins (como fraude, realização e ocultação de atividades comerciais fraudulentas, roubo de dados, ativismo/sabotagem) através de várias técnicas (como abuso e/ou obtenção de privilégios, usurpação de identidade, engenharia social, exploração de vulnerabilidades em sistemas de TIC, criação de *software* malicioso).	• Instalação de aplicações de monitorização da atividade do teclado (*key loggers*) para roubar os nomes de utilizador e respetivas palavras-passe do utilizador para obter acesso não autorizado a dados confidenciais e/ou cometer fraude. • Decifragem/deteção de palavras-passe fracas para obter direitos de acesso ilegítimos ou privilegiados. • O administrador do sistema utiliza sistemas operativos ou utilitários de bases de dados (para alterações diretas a bases de dados) para cometer fraudes.
		Manipulações não autorizadas das TIC devido a procedimentos e práticas de gestão de acesso a TIC inadequadas.	• Falha na desativação ou eliminação de contas desnecessárias, como contas de funcionários que mudaram de funções e/ou saíram da instituição, incluindo convidados ou fornecedores que já não precisam de acesso, que dão acesso não autorizado a sistemas de TIC. • Concessão de direitos e privilégios de acesso excessivos, permitindo acessos não autorizados e/ou a ocultação de atividades fraudulentas.
		Ameaças de segurança devido à falta de sensibilização para a questão da segurança em situações em que os funcionários não compreendem, negligenciam ou não cumprem as políticas e procedimentos de segurança das TIC.	• Funcionários que são enganados para prestar assistência a um atacante (*i.e.*, engenharia social). • Más práticas no que se refere a credenciais: partilha de palavras-passe, utilização de palavras-passe «fáceis» de adivinhar, utilização da mesma palavra-

Categorias de risco das TIC	Riscos de TIC (lista não exaustiva[10])	Descrição do risco	Exemplos
			passe para diferentes fins, etc. • Armazenamento de dados confidenciais não cifrados em computadores portáteis e soluções de armazenamento de dados portáteis (como *pens* USB) que se podem perder ou ser roubados.
		O armazenamento ou a transferência não autorizados de informações confidenciais para fora da instituição.	• Pessoas que roubam ou divulgam deliberadamente ou clandestinamente informações confidenciais a pessoas não autorizadas ou ao público.
	Segurança física inadequada das TIC	Utilização indevida ou roubo de ativos de TIC através de acesso físico, causando danos, perda de ativos ou dados ou para permitir outras ameaças.	• Entrada forçada em escritórios e/ou centros de dados para roubar equipamentos de TIC (como computadores, portáteis, soluções de armazenamento) e/ou para copiar dados através do acesso físico a sistemas de TIC.
		Danos deliberados ou acidentais a ativos de TIC físicos causados por terrorismo, acidentes ou manipulações não intencionais/erradas por funcionários da instituição e/ou por terceiros (fornecedores, pessoal que faz reparações).	• Terrorismo físico (*i.e.*, atendados terroristas à bomba) ou sabotagem de ativos de TIC. • Destruição de centros de dados causada por incêndio, fugas de água ou outros fatores.
		Proteção física insuficiente contra catástrofes naturais que originem a destruição parcial ou completa de sistemas de TIC/centros de dados devido a catástrofes naturais.	• Sismos, calor extremo, tempestades de ventos, tempestades de neve, inundações, incêndios, relâmpagos.
Riscos de alteração das TIC	Controlos inapropriados às alterações ao sistema de TIC e desenvolvimento das TIC	Incidentes causados por erros não detetados ou vulnerabilidades resultantes de alterações (como efeitos não previstos de uma alteração ou uma alteração gerida incorretamente devido a falta de testes ou práticas impróprias de gestão de alterações) a, por exemplo, *software*, sistemas e dados das TIC.	• Lançamento para utilização em produção de *software* submetido a testes insuficientes ou alterações de configurações com efeitos negativos inesperados nos dados (como corrupção, eliminação) e/ou desempenho do sistema de TIC (como interrupção, redução do desempenho). • Alterações não controladas e sistemas ou dados das TIC no ambiente de produção. • Lançamento para utilização em produção de

Categorias de risco das TIC	Riscos de TIC (lista não exaustiva[10])	Descrição do risco	Exemplos
			sistemas de TIC e aplicações de Internet pouco seguros, criando oportunidades para os piratas informáticos atacarem os serviços de Internet fornecidos e/ou entrarem nos sistemas de TIC internos. • Alterações não controladas no código fonte de *software* desenvolvido internamente. • Testes insuficientes devido à falta de ambientes de teste adequados.
	Arquitetura de TIC inadequada	Uma má gestão da arquitetura de TIC ao conceber, criar e efetuar a manutenção de sistemas de TIC (como *software*, *hardware*, dados) pode, ao longo do tempo, tornar complexa, difícil e dispendiosa a gestão de sistemas de TIC rígidos, que já não dão uma resposta suficiente às necessidades do negócio e são insuficientes em comparação com os requisitos reais de gestão de riscos.	• Alterações geridas inadequadamente a sistemas de TIC, *software* e/ou dados durante um período de tempo prolongado, dando origem a arquiteturas e sistemas de TIC complexos, heterogéneos e difíceis de gerir, causando muitos impactos negativos na gestão do negócio e dos riscos (como falta de flexibilidade e agilidade, falhas e incidentes a nível das TIC, custos operacionais elevados, menor segurança e resiliência das TIC, qualidade dos dados e capacidades de reporte reduzidas). • Personalização excessiva e extensão de pacotes de *software* comercial com *software* desenvolvido internamente, que dão origem à incapacidade de implementar futuros lançamentos e atualizações do *software* comercial e ao risco de já não ser suportado pelo fornecedor.
	Ciclo de vida e gestão de correções de segurança inadequados	A incapacidade de manter um inventário adequado de todos os ativos de TIC como forma de apoiar, e em conjunto com, um ciclo de vida sólido e práticas de gestão de correções de segurança. Tal origina sistemas de TIC com correções de segurança insuficientes (e, como tal, mais vulneráveis) e desatualizados que	• Sistemas de TIC sem aplicação de correções de segurança e desatualizados que podem causar impactos negativos na gestão do negócio e dos riscos (como falta de flexibilidade e agilidade, interrupções das TIC, menor segurança e resiliência das TIC).

Categorias de risco das TIC	Riscos de TIC (lista não exaustiva[10])	Descrição do risco	Exemplos
		podem não atender às necessidades da gestão do negócio e dos riscos.	
Riscos de integridade de dados das TIC	Processamento ou tratamento disfuncional de dados das TIC	Devido a erros ou falhas do sistema, de comunicação e/ou aplicação, ou a um processo de extração, transferência e carregamento (ETL) de dados executados incorretamente, os dados podem ser corrompidos ou perdidos.	• Erro do sistema de TIC no processamento em *batch*, originando saldos incorretos nas contas bancárias do cliente. • Consultas executadas incorretamente. • Perda de dados devido a erro de replicação de dados (cópia de salvaguarda).
	Controlos de validação de dados concebidos incorretamente em sistemas de TIC	Erros relacionados com a inexistência ou ineficácia de introdução de dados automática e controlos de aceitação (como para dados de entidades terceiras utilizados), transferência de dados, controlos de processamento e de saída nos sistemas de TIC (como controlos de validade de dados de entrada, reconciliações de dados).	• Formatação/validação insuficiente ou inválida de entradas de dados em aplicações e/ou interfaces do utilizador. • Inexistência de controlos de reconciliação sobre os dados produzidos • Inexistência de controlos em processos de extração de dados executados (como consultas a bases de dados) que dão origem a dados errados. • Utilização de dados externos com erros.
	Alterações mal controladas a dados nos sistemas de TIC de produção.	Erros de dados introduzidos devido à falta de controlos relativamente à precisão e à natureza justificada de manipulações de dados realizadas na produção de sistemas de TIC	• Programadores ou administradores de bases de dados que acedem diretamente e alteram os dados nos sistemas de TIC de produção de uma forma não controlada, como no caso de um incidente ao nível das TIC.
	Arquitetura, fluxos, modelos ou dicionários de dados concebidos e/ou geridos incorretamente	Arquiteturas, modelos, fluxos ou dicionários de dados geridos incorretamente podem resultar em várias versões dos mesmos dados nos sistemas de TIC, que já não são consistentes devido a modelos de dados ou definições de dados aplicados de forma diferente e/ou a diferenças no processo de criação e alteração de dados subjacente.	• A existência de diferentes bases de dados de clientes por produto ou unidade de negócios com diferentes definições e campos de dados, resultando em dados de clientes integrados não reconciliados e difíceis de comparar ao nível de toda a instituição financeira ou grupo.
Riscos de	Resiliência inadequada de	A indisponibilidade de serviços de TIC críticos, serviços de telecomunicações e utilitários contratados	• Indisponibilidade de serviços fundamentais como resultado de falhas nos sistemas ou aplicações de

Categorias de risco das TIC	Riscos de TIC (lista não exaustiva[10])	Descrição do risco	Exemplos
contratação externa de TIC	serviços de terceiros ou de outra entidade do Grupo	externamente. Perda ou corrupção de dados críticos/sensíveis confiados ao prestador de serviços	TIC de fornecedores (contratados externamente). • Perturbação de ligações de telecomunicações. • Falta de energia.
	Governo inadequado da contratação externa	Degradação ou falhas graves no serviço devido à preparação ou processos de controlo ineficazes do prestador de serviços contratado externamente. Governo ineficaz da contratação externa que pode resultar numa falta de competências e capacidades apropriadas para identificar, avaliar, mitigar e monitorizar totalmente os riscos de TIC e que pode limitar as capacidades operacionais da instituição.	• Procedimentos de gestão de incidentes, mecanismos de controlo contratual e garantias insuficientes integrados no contrato de prestação de serviços que aumentam a dependência para com funcionários chave de entidades terceiras e fornecedores. • Controlos de gestão de alterações inapropriados referentes ao ambiente de TIC do prestador de serviços que podem causar uma degradação ou falha grave do serviço.
	Segurança inadequada de terceiros ou de outra entidade do Grupo	Pirataria dos sistemas de TIC dos prestadores de serviço, com um impacto direto nos serviços contratados externamente ou nos dados críticos/confidenciais armazenados no prestador de serviços. Obtenção de acesso não autorizado por funcionários do prestador de serviços a dados críticos/sensíveis armazenados no prestador de serviços	• Pirataria aos prestadores de serviço por criminosos ou terroristas, como um ponto de entrada para os sistemas de TIC das instituições ou para aceder/destruir dados críticos ou sensíveis armazenados nos prestadores de serviço. • Funcionários internos mal-intencionados do lado do prestador de serviços que tentam roubar e vender dados sensíveis.