EIOPA-BoS-20/600

# Orientações sobre segurança e governação das tecnologias da informação e comunicação

EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Alemanha - Tel. + 49 69-951119-20;
Fax. + 49 69-951119-19; correio eletrónico: info@eiopa.europa.eu sítio Web: www.eiopa.europa.eu

# Índice

# Contexto

1. Ao abrigo do artigo 16.º do Regulamento (UE) n.º 1094/2010, a Autoridade Europeia dos Seguros e Pensões Complementares de Reforma (EIOPA) pode emitir orientações e recomendações dirigidas às autoridades competentes e a instituições financeiras, a fim de definir práticas de supervisão coerentes, eficientes e eficazes e garantir uma aplicação comum, uniforme e coerente da legislação da União.

2. 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 a essas orientações e recomendações.

3. A EIOPA identificou a necessidade de elaborar diretrizes específicas no domínio da segurança e governação das tecnologias da informação e comunicação (TIC) em relação aos artigos 41.º e 44.º da Diretiva 2009/138/CE, no contexto da análise efetuada para dar resposta ao Plano de Ação para a Tecnologia Financeira da Comissão Europeia [COM(2018) 109 final], do Plano de Convergência no domínio da Supervisão da EIOPA 2018-2019[1] e no seguimento de interações com várias outras partes interessadas[2].

4. Conforme referido no parecer conjunto das Autoridades Europeias de Supervisão dirigido à Comissão Europeia, as orientações da EIOPA sobre o sistema de governação «*não refletem adequadamente a importância de tratar da gestão dos riscos associados às TIC (incluindo riscos cibernéticos)*». Não existem diretrizes no que diz respeito a elementos essenciais que são geralmente aceites como parte da segurança e governação adequadas das TIC.

5. A análise da atual situação (legislativa) na UE, realizada no âmbito do parecer conjunto supramencionado, demonstrou que a maioria dos Estados-Membros da UE estabeleceu normas nacionais em matéria de segurança e governação das TIC. Embora os requisitos sejam semelhantes, o quadro regulamentar permanece fragmentado. Além disso, um inquérito sobre as atuais práticas de supervisão revelou uma ampla variedade de práticas – desde «sem supervisão específica» a «supervisão rigorosa» (incluindo «inspeções à distância» e «inspeções no local»).

6. Além do mais, as TIC são cada vez mais complexas e a frequência de incidentes relacionados com TIC (incluindo incidentes de cibersegurança) está igualmente a aumentar, bem como o impacto negativo de tais incidentes no funcionamento operacional das empresas. Por este motivo, a gestão dos riscos associados às TIC e à segurança é fundamental para que uma empresa atinja os seus objetivos em termos estratégicos, empresariais, operacionais e de reputação.

7. Adicionalmente, em todo o setor dos seguros, incluindo modelos empresariais tanto tradicionais como inovadores, verifica-se uma dependência crescente das TIC na prestação de serviços de seguros e no funcionamento operacional normal das empresas, por exemplo, digitalização do setor dos seguros (tecnologia dos seguros, IdC, etc.), bem como interligação através de canais de telecomunicação (Internet, ligações móveis e sem fios e redes de área alargada). Tal torna as atividades das empresas vulneráveis a incidentes de segurança, incluindo

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] É possível obter aqui o relatório publicado pela EIOPA em resposta ao Plano de Ação para a Tecnologia Financeira da Comissão Europeia.

ciberataques. Por conseguinte, importa garantir que as empresas se encontrem devidamente preparadas para gerir os riscos associados às TIC e à segurança.

8. Além disso, reconhecendo a necessidade de preparação para riscos cibernéticos[3] e de um quadro de cibersegurança sólido por parte das empresas, as presentes orientações abrangem igualmente a cibersegurança no âmbito das medidas de segurança da informação das empresas. Embora as presentes orientações reconheçam que a cibersegurança deve ser abordada no âmbito da gestão global dos riscos associados às TIC e à segurança das empresas, importa salientar que os ciberataques possuem determinadas características específicas, que devem ser tidas em conta a fim de garantir que as medidas de segurança da informação atenuam adequadamente os riscos cibernéticos:

   a) Os ciberataques são frequentemente mais difíceis de gerir (ou seja, de identificar, de proteger contra os mesmos, de detetar, de dar resposta aos mesmos e de recuperar totalmente dos mesmos) do que a maioria das outras fontes de riscos associados às TIC e à segurança, sendo que a extensão dos danos é igualmente difícil de determinar;

   b) Certos ciberataques podem tornar ineficazes os mecanismos comuns de gestão de riscos e de continuidade das atividades, bem como os procedimentos de recuperação em caso de catástrofes, uma vez que podem propagar programas informáticos maliciosos para os sistemas de segurança por forma a deixá-los indisponíveis ou a corromper os dados da cópia de segurança;

   c) Os prestadores de serviços, os corretores, os agentes (gestores) e os intermediários podem tornar-se canais de propagação de ciberataques. As ameaças silenciosas contagiosas podem utilizar a interligação através de ligações de telecomunicações de terceiros para aceder ao sistema de TIC da empresa. Assim, uma empresa interligada com relevância individual reduzida pode tornar-se vulnerável e uma fonte de propagação de riscos, o que pode resultar num impacto sistémico. Respeitando o princípio do elo mais fraco, a cibersegurança não deve ser apenas uma preocupação dos grandes participantes no mercado ou dos prestadores de serviços críticos.

9. As presentes orientações têm como objetivo o seguinte:

   a) Proporcionar esclarecimentos e transparência aos participantes no mercado relativamente às capacidades mínimas previstas em termos de informação e cibersegurança, ou seja, uma base de referência para a segurança;

   b) Evitar a potencial arbitragem regulamentar;

   c) Promover a convergência no domínio da supervisão no que diz respeito às expetativas e aos processos aplicáveis relativamente à segurança e governação das TIC enquanto elemento fundamental para a gestão adequada dos riscos associados às TIC e à segurança.

[3] Para uma definição de «risco cibernético», consultar o Léxico Cibernético do CEF, de 12 de novembro de 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf

# Orientações sobre segurança e governação das tecnologias da informação e comunicação

# Introdução

1. Em conformidade com o artigo 16.º do Regulamento (UE) n.º 1094/2010[4], a EIOPA emite as presentes orientações dirigidas às autoridades de supervisão, a fim de fornecer diretrizes sobre a forma como as empresas de seguros e de resseguros (doravante, coletivamente «empresas») devem aplicar os requisitos em matéria de governação previstos na Diretiva 2009/138/CE[5] (doravante, «Diretiva Solvência II») e no Regulamento Delegado (UE) 2015/35 da Comissão[6] (doravante, «Regulamento Delegado») no contexto da segurança e governação das tecnologias da informação e comunicação (doravante, «TIC»). Para o efeito, as presentes orientações têm por base as disposições em matéria de governação previstas nos artigos 41.º, 44.º, 46.º, 47.º, 132.º e 246.º da Diretiva Solvência II e nos artigos 258.º a 260.º, 266.º, 268.º a 271.º e 274.º do Regulamento Delegado. Além disso, as presentes orientações têm igualmente por base as diretrizes fornecidas nas orientações da EIOPA sobre o sistema de governação (EIOPA-BoS-14/253)[7] e nas orientações da EIOPA sobre a subcontratação a prestadores de serviços de computação em nuvem (EIOPA-BoS-19/270)[8].

2. As orientações são aplicáveis a empresas individuais e, com as necessárias adaptações, a nível do grupo[9].

3. Ao cumprir ou supervisionar o cumprimento das presentes orientações, as autoridades competentes devem ter em conta o princípio da proporcionalidade[10], que deve garantir que os mecanismos de governação, incluindo os relacionados com a segurança e governação das TIC, são proporcionais à natureza, escala e complexidade dos riscos correspondentes com que as empresas estão ou podem vir a estar confrontadas.

4. As presentes orientações devem ser consideradas em conjunto com, e sem prejuízo de, a Diretiva Solvência II, o Regulamento Delegado, as orientações da EIOPA sobre o sistema de governação e as orientações da EIOPA sobre a subcontratação a prestadores de serviços de computação em nuvem. As presentes orientações devem ser neutras em termos de tecnologia e metodologia.

## Definições

5. Se não estiverem definidos nas presentes orientações, os termos utilizados têm a aceção que lhes é dada na Diretiva Solvência II.

6. Para efeitos das presentes orientações, são aplicáveis as seguintes definições:

---

[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).

[5] 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).

[6] Regulamento Delegado (UE) 2015/35 da Comissão, de 10 de outubro de 2014, que completa a Diretiva 2009/138/CE do Parlamento Europeu e do Conselho relativa ao acesso à atividade de seguros e resseguros e ao seu exercício (Solvência II) (JO L 12 de 17.1.2015, p. 1).

[7] https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

[8] https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-outsourcing-cloud-service-providers_en?source=search

[9] Artigo 212.º, n.º 1, da Diretiva 2009/138/CE.

[10] Artigo 29.º, n.º 3, da Diretiva 2009/138/CE.

| | |
|---|---|
| Proprietário do ativo | Pessoa ou entidade com responsabilidade e autoridade sobre um ativo de informação e de TIC. |
| Disponibilidade | Característica de ser acessível e utilizável a pedido (prontidão) por uma entidade autorizada. |
| Confidencialidade | Característica que inibe a disponibilização ou a divulgação de informação a particulares, entidades, processos ou sistemas não autorizados. |
| Ciberataque | Qualquer tipo de pirataria informática que conduza a uma tentativa prejudicial/maliciosa de destruir, expor, alterar, incapacitar, roubar ou obter acesso não autorizado ou fazer uma utilização não autorizada de um ativo de informação que tenha como alvo sistemas de TIC. |
| Cibersegurança | Preservação da confidencialidade, integridade e disponibilidade de informações e/ou sistemas de informação através do meio cibernético. |
| Ativo de TIC | Um ativo de programas informáticos ou de equipamentos informáticos que se encontra no ambiente empresarial. |
| Projetos de TIC | Qualquer projeto, ou parte do mesmo, em que os serviços e sistemas de TIC sejam alterados, substituídos ou aplicados. |
| Riscos associados às TIC e à segurança | Enquanto subcomponente do risco operacional, o risco de perdas por violação da confidencialidade, falta de integridade de sistemas e dados, inadequação ou indisponibilidade de sistemas e dados ou incapacidade para alterar as TIC num período e por um custo razoáveis quando o ambiente ou os requisitos empresariais sofram alterações (ou seja, agilidade).<br><br>Tal inclui riscos cibernéticos e riscos de segurança da informação resultantes de eventos externos ou processos internos inadequados ou deficientes, incluindo ciberataques ou uma segurança física inadequada. |
| Segurança da informação | Preservação da confidencialidade, integridade e disponibilidade de informações e/ou sistemas de informação. Podem ainda estar envolvidas outras características, tais como autenticidade, responsabilidade, não rejeição e fiabilidade. |

| | |
|---|---|
| Serviços de TIC | Serviços fornecidos através de sistemas e prestadores de serviços de TIC a um ou mais utilizadores internos ou externos. |
| Sistemas de TIC | Conjunto de aplicações, serviços, ativos de tecnologia da informação, ativos de TIC ou outros componentes do tratamento da informação, que inclui o ambiente de operação. |
| Ativo de informação | Um conjunto de informações, tangíveis ou intangíveis, que vale a pena proteger. |
| Integridade | Característica de exatidão e integralidade. |
| Incidente operacional ou de segurança | Um evento único ou uma série de eventos conexos e não previstos que têm, ou poderão vir a ter, um impacto negativo na integridade, disponibilidade e confidencialidade dos serviços e sistemas de TIC. |
| Prestador de serviços | Uma entidade terceira que desempenha, no todo ou em parte, uma atividade, um processo ou um serviço ao abrigo de um acordo de subcontratação. |
| Testes de penetração baseados em ameaças | Uma tentativa controlada de comprometer a ciber-resiliência de uma entidade mediante a simulação de táticas, técnicas e procedimentos de autores de ameaças reais. Tem por base informações sobre ameaças específicas e centra-se nos funcionários, processos e tecnologias de uma entidade, com conhecimento prévio mínimo e impacto reduzido nas atividades. |
| Vulnerabilidade | Uma deficiência, suscetibilidade ou falha de um ativo ou controlo que pode ser explorada por uma ou mais ameaças. |

7. As presentes orientações entram em vigor em 1 de julho de 2021.

## Orientação 1 – Proporcionalidade

8. As empresas devem aplicar as presentes orientações de forma proporcional à natureza, escala e complexidade dos riscos inerentes das suas atividades.

## Orientação 2 – TIC no âmbito do sistema de governação

9. O órgão de direção, administração ou supervisão deve garantir que o sistema de governação das empresas, nomeadamente o sistema de gestão de riscos e o sistema de controlo interno, gere adequadamente os riscos associados às TIC e à segurança das empresas.

10. O órgão de direção, administração ou supervisão deve assegurar que a quantidade e as competências dos funcionários das empresas são adequadas para apoiar as suas necessidades operacionais de TIC e os seus processos de gestão dos riscos associados às TIC e à segurança numa base contínua e para garantir a aplicação da sua estratégia em matéria de TIC. Além disso, os funcionários devem receber regularmente formação adequada em matéria de riscos associados às TIC e à segurança, incluindo segurança da informação, conforme estabelecido na orientação 13.

11. O órgão de direção, administração ou supervisão deve garantir que os recursos atribuídos são adequados para o cumprimento dos requisitos supramencionados.

## Orientação 3 – Estratégia em matéria de TIC

12. O órgão de direção, administração ou supervisão é globalmente responsável por elaborar e aprovar a estratégia escrita em matéria de TIC das empresas como parte da sua estratégia comercial global e alinhada com esta, bem como por supervisionar a sua comunicação e aplicação.

13. A estratégia em matéria de TIC deve definir, no mínimo, o seguinte:

    a) A forma como as TIC das empresas devem evoluir para apoiar e aplicar eficazmente a sua estratégia comercial, incluindo a evolução da estrutura organizacional, modelos empresariais, sistema de TIC e principais dependências em relação aos prestadores de serviços;

    b) A evolução da arquitetura das TIC, incluindo a dependência de prestadores de serviços; e

    c) Objetivos claros em matéria de segurança da informação, centrados nos sistemas e serviços de TIC, nos funcionários e nos processos.

14. As empresas devem garantir que a estratégia em matéria de TIC é aplicada, adotada e comunicada atempadamente a todos os funcionários e prestadores de serviços pertinentes, sempre que aplicável e pertinente.

15. As empresas devem criar um processo para monitorizar e medir a eficácia da aplicação da estratégia em matéria de TIC. Tal processo deve ser revisto e atualizado regularmente.

## Orientação 4 – Riscos associados às TIC e à segurança no âmbito do sistema de gestão de riscos

16. O órgão de direção, administração ou supervisão é globalmente responsável por criar um sistema efetivo para a gestão dos riscos associados às TIC e à segurança como parte do sistema de gestão global de riscos da empresa. Tal inclui a determinação da tolerância face ao risco em relação aos riscos em causa, de acordo com a estratégia em matéria de TIC da empresa, e um relatório escrito periódico sobre o resultado do processo de gestão dos riscos dirigido ao órgão de direção, administração ou supervisão.

17. No âmbito do respetivo sistema de gestão global de riscos, as empresas devem ter em consideração, no que diz respeito aos riscos associados às TIC e à segurança (definindo simultaneamente os requisitos de proteção das TIC conforme descrito em seguida), pelo menos, o seguinte:

    a) As empresas devem estabelecer e atualizar regularmente um levantamento dos respetivos processos e atividades empresariais, funções empresariais, papéis e ativos (por exemplo, ativos de informação e ativos de TIC), a fim de

identificar a importância de cada um destes e as suas interdependências relativamente aos riscos associados às TIC e à segurança;

b) As empresas devem identificar e medir todos os riscos pertinentes associados às TIC e à segurança a que estão expostas e classificar, em termos de criticidade, os processos e atividades empresariais identificados, as funções empresariais, os papéis e os ativos (por exemplo, ativos de informação e ativos de TIC). As empresas devem avaliar igualmente, pelo menos, os requisitos em matéria de proteção da confidencialidade, integridade e disponibilidade de tais processos e atividades empresariais, funções empresariais, papéis e ativos (por exemplo, ativos de informação e ativos de TIC). Os proprietários dos ativos, responsáveis pela classificação dos mesmos, devem ser identificados;

c) Os métodos utilizados para determinar a criticidade e o nível de proteção exigido – nomeadamente no que se refere aos objetivos no domínio da proteção da integridade, disponibilidade e confidencialidade – devem garantir que os requisitos resultantes em matéria de proteção são coerentes e abrangentes;

d) A medição dos riscos associados às TIC e à segurança deve ser efetuada com base nos critérios definidos em matéria de riscos associados às TIC e à segurança, tendo em conta a criticidade dos respetivos processos e atividades empresariais, funções empresariais, papéis e ativos (por exemplo, ativos de informação e ativos de TIC), a extensão das vulnerabilidades conhecidas e os incidentes anteriores que afetaram a empresa;

e) A avaliação dos riscos associados às TIC e à segurança deve ser realizada e documentada regularmente. Tal avaliação deve ser igualmente efetuada antes de qualquer alteração significativa na infraestrutura, nos processos ou nos procedimentos que afete os processos e atividades empresariais, as funções empresariais, os papéis e os ativos (por exemplo, ativos de informação e ativos de TIC);

f) Com base na avaliação do risco, as empresas devem, no mínimo, definir e aplicar medidas para gerir os riscos identificados associados às TIC e à segurança e para proteger os ativos de informação de acordo com a sua classificação. O que precede deve incluir a definição de medidas para gerir os restantes riscos residuais.

18. Os resultados do processo de gestão dos riscos associados às TIC e à segurança devem ser aprovados pelo órgão de direção, administração ou supervisão e incluídos no processo de gestão do risco operacional como parte da gestão global de riscos da empresa.

## Orientação 5 – Auditoria

19. A governação, os sistemas e os processos das empresas no âmbito dos riscos associados às TIC e à segurança devem ser periodicamente objeto de auditoria, em consonância com o plano de auditoria[11] da empresa, a ser realizada por auditores com competências, conhecimentos e experiência suficientes no domínio dos riscos associados às TIC e à segurança, a fim de fornecer uma garantia independente da sua eficácia ao órgão de direção, administração ou supervisão. A frequência e o

[11] Artigo 271.º do Regulamento Delegado.

objetivo de tais auditorias devem ser proporcionais aos riscos pertinentes associados às TIC e à segurança.

## Orientação 6 – Política e medidas de segurança da informação

20. As empresas devem estabelecer por escrito uma política de segurança da informação aprovada pelo órgão de direção, administração ou supervisão, que deve definir os princípios e regras de alto nível para a proteção da confidencialidade, integridade e disponibilidade da informação das empresas, a fim de apoiar a aplicação da estratégia em matéria de TIC.

21. A política deve incluir uma descrição das principais funções e responsabilidades da gestão da segurança da informação, devendo estabelecer os requisitos aplicáveis aos funcionários, aos processos e à tecnologia em relação à segurança da informação, reconhecendo que os funcionários a todos os níveis têm a responsabilidade de garantir a segurança da informação das empresas.

22. A política deve ser comunicada a nível da empresa e ser aplicável a todos os funcionários. Sempre que aplicável e pertinente, a política de segurança da informação, ou partes da mesma, deve ser igualmente comunicada e aplicável aos prestadores de serviços.

23. Com base na política, as empresas devem estabelecer e aplicar procedimentos de segurança da informação mais específicos e medidas de segurança da informação, a fim de, *inter alia*, atenuar os riscos associados às TIC e à segurança a que estão expostas. Os procedimentos em causa e as medidas de segurança da informação devem incluir todos os processos descritos nas presentes orientações, se for caso disso.

## Orientação 7 – Função de segurança da informação

24. As empresas devem estabelecer, no âmbito do respetivo sistema de governação e de acordo com o princípio da proporcionalidade, uma função de segurança da informação, cujas responsabilidades devem ser atribuídas a uma pessoa designada. As empresas devem assegurar a independência e a objetividade da função de segurança da informação, separando-a devidamente do desenvolvimento e dos processos operacionais de TIC. A função deve informar o órgão de direção, administração ou supervisão.

25. As tarefas da função de segurança da informação englobam, habitualmente, o seguinte:

    a) Apoiar o órgão de direção, administração ou supervisão aquando da definição e atualização da política de segurança da informação das empresas e controlar a sua execução;

    b) Informar e aconselhar o órgão de direção, administração ou supervisão numa base regular e *ad hoc* relativamente ao estado da segurança da informação e à sua evolução;

    c) Acompanhar e rever a aplicação das medidas de segurança da informação;

    d) Garantir o cumprimento dos requisitos em matéria de segurança da informação ao utilizar prestadores de serviços;

    e) Garantir que todos os funcionários e prestadores de serviços com acesso à informação e aos sistemas são devidamente informados sobre a política de segurança da informação, por exemplo, através de sessões de formação e de sensibilização no domínio da segurança da informação;

f) Coordenar a análise de incidentes operacionais ou de segurança e informar o órgão de direção, administração ou supervisão dos incidentes pertinentes.

## Orientação 8 – Segurança lógica

26. As empresas devem definir, documentar e aplicar procedimentos para controlo do acesso lógico ou para segurança lógica (identidade e gestão de acesso) em consonância com os requisitos de proteção, conforme definido na orientação 4. Os procedimentos em causa devem ser aplicados, executados, monitorizados e revistos periodicamente, devendo incluir igualmente controlos para a monitorização de anomalias. Estes procedimentos devem, no mínimo, aplicar os seguintes elementos, nos quais o termo «utilizador» inclui igualmente os utilizadores técnicos:

    a) Necessidade de tomar conhecimento, menor privilégio e segregação de funções: as empresas devem gerir os direitos de acesso, incluindo o acesso remoto aos ativos de informação e aos seus sistemas de apoio, com base na «necessidade de tomar conhecimento». Devem ser concedidos aos utilizadores os direitos mínimos de acesso estritamente necessários para a execução das suas funções (princípio do «menor privilégio»), ou seja, para evitar o acesso injustificado aos dados ou para impedir a atribuição de combinações de direitos de acesso que possam ser utilizadas para contornar os controlos (princípio da «segregação de funções»);

    b) Responsabilização dos utilizadores: as empresas devem limitar, tanto quanto possível, a utilização de contas de utilizador genéricas e partilhadas, bem como garantir que os utilizadores possam ser permanentemente identificados e a sua origem rastreada até uma tarefa autorizada ou uma pessoa singular responsável pelas ações executadas nos sistemas de TIC;

    c) Direitos de acesso privilegiado: as empresas devem aplicar controlos rigorosos sobre o acesso privilegiado ao sistema, limitando estritamente e supervisionando de perto as contas com um nível elevado de acesso ao sistema (por exemplo, as contas de administrador);

    d) Acesso remoto: a fim de assegurar uma comunicação segura e reduzir o risco, apenas deve ser concedido acesso remoto administrativo aos sistemas críticos de TIC com base na necessidade de tomar conhecimento e quando são utilizadas soluções de autenticação forte;

    e) Registo das atividades do utilizador: as atividades dos utilizadores devem ser registadas e monitorizadas de uma forma proporcional ao risco, incluindo, no mínimo, as atividades dos utilizadores privilegiados. Os registos de acesso devem ser protegidos para evitar alterações ou eliminações não autorizadas e mantidos durante um período proporcional à criticidade das funções empresariais, processos de apoio e ativos de informação identificados, sem prejuízo dos requisitos de retenção estabelecidos no direito nacional ou comunitário. As empresas devem utilizar esta informação para facilitar a identificação e investigação de atividades anómalas que tenham sido detetadas durante a prestação de serviços;

    f) Gestão de acesso: os direitos de acesso devem ser concedidos, suprimidos e alterados atempadamente, de acordo com rotinas de aprovação predefinidas, sempre que o proprietário do ativo de informação esteja envolvido. Caso o acesso deixe de ser necessário, os direitos de acesso devem ser imediatamente revogados;

g) Avaliação do acesso: os direitos de acesso devem ser revistos periodicamente para assegurar que os utilizadores não possuam privilégios excessivos e que os direitos de acesso sejam retirados/suprimidos quando já não são necessários;

h) A concessão, alteração e revogação dos direitos de acesso devem ser documentadas de um modo que facilite a compreensão e a análise; e

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

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

## Orientação 9 – Segurança física

28. As medidas de segurança física das empresas (por exemplo, proteção contra falhas de energia, incêndios, água e acesso físico não autorizado) devem ser definidas, documentadas e aplicadas tendo em vista a proteção das suas instalações, centros de dados e áreas sensíveis contra acesso não autorizado e riscos ambientais.

29. O acesso físico aos sistemas de TIC deve ser permitido apenas a pessoas autorizadas. A autorização deve ser atribuída de acordo com as tarefas e responsabilidades da pessoa em causa, bem como limitada a pessoas que sejam devidamente formadas e supervisionadas. O acesso físico deve ser revisto regularmente, a fim de garantir que os direitos de acesso desnecessários sejam imediatamente retirados/suprimidos.

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

## Orientação 10 – Segurança das operações de TIC

31. As empresas devem aplicar procedimentos para garantir a confidencialidade, integridade e disponibilidade dos sistemas de TIC e dos serviços de TIC, com vista a minimizar, respetivamente, o impacto das questões de segurança na prestação de serviços de TIC. Estes procedimentos devem incluir, de forma adequada, as seguintes medidas:

a) Identificação de potenciais vulnerabilidades, que devem ser avaliadas e corrigidas, assegurando que os sistemas de TIC estão atualizados, incluindo os programas informáticos fornecidos pelas empresas aos seus utilizadores internos e externos, através da implementação de correções críticas de segurança (incluindo atualizações das definições de antivírus) ou da aplicação de controlos compensatórios;

b) Aplicação de configurações de base seguras para todos os componentes críticos, tais como sistemas operativos, bases de dados, encaminhadores (*routers*), comutadores;

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

d) Aplicação da proteção de terminais, incluindo servidores, estações de trabalho e dispositivos móveis. As empresas devem determinar se um terminal cumpre as normas de segurança definidas pelas próprias antes de lhe ser concedido acesso à rede empresarial;

e) Garantia da existência de mecanismos de verificação da integridade para verificar a integridade dos sistemas de TIC;

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

## Orientação 11 – Monitorização da segurança

32. As empresas devem criar e aplicar procedimentos e processos para monitorizar continuamente as atividades que afetem a segurança da informação das empresas. A monitorização deve abranger, pelo menos, o seguinte:

    a) Fatores internos e externos, incluindo as funções administrativas das empresas e das TIC;

    b) Operações efetuadas por prestadores de serviços, outras entidades e utilizadores internos; e

    c) Potenciais ameaças internas e externas.

33. Com base na monitorização, as empresas devem aplicar recursos adequados e eficazes para detetar, comunicar e dar resposta a atividades anómalas e ameaças, tais como intrusões físicas ou lógicas, violações da confidencialidade, integridade e disponibilidade dos ativos de informação, códigos maliciosos e vulnerabilidades publicamente conhecidas em termos de programas informáticos ou de equipamentos informáticos.

34. A comunicação decorrente da monitorização da segurança deve ajudar as empresas a compreender a natureza dos incidentes operacionais ou de segurança, a identificar tendências e a apoiar as investigações internas das empresas, permitindo-lhes tomar decisões adequadas.

## Orientação 12 – Revisões, avaliação e testes da segurança da informação

35. As empresas devem realizar uma série de diversas revisões, avaliações e testes da segurança da informação, por forma a garantir a identificação efetiva de vulnerabilidades nos respetivos sistemas e serviços de TIC. Por exemplo, as empresas podem realizar análises de lacunas em relação às normas de segurança da informação, revisões de conformidade, auditorias internas e externas dos sistemas de informação ou revisões da segurança física.

36. As empresas devem estabelecer e aplicar um quadro de testes da segurança da informação que valide a robustez e a eficácia das medidas de segurança da informação, devendo garantir que tal quadro tenha em consideração as ameaças e vulnerabilidades, identificadas através da monitorização das ameaças e do processo de avaliação dos riscos associados às TIC e à segurança.

37. Os testes devem ser efetuados de modo seguro por pessoal independente com conhecimentos, competências e experiência suficientes para testar medidas de segurança da informação.

38. As empresas devem realizar testes regularmente. O âmbito, a frequência e o método dos testes (tal como testes de penetração, incluindo testes de penetração baseados em ameaças) devem ser proporcionais ao nível de risco identificado. Os testes dos sistemas críticos de TIC e a verificação de vulnerabilidades devem ser realizados anualmente.

39. As empresas devem garantir que os testes às medidas de segurança são realizados no caso de alterações da infraestrutura, dos processos ou dos procedimentos e se forem efetuadas alterações devido a incidentes operacionais ou de segurança de caráter severo ou devido ao lançamento de aplicações críticas novas ou significativamente alteradas. As empresas devem monitorizar e avaliar os resultados dos testes de segurança e atualizar as suas medidas de segurança em conformidade, sem demora indevida no caso dos sistemas críticos de TIC.

## Orientação 13 – Formação e sensibilização no domínio da segurança da informação

40. As empresas devem criar programas de formação no domínio da segurança da informação para todos os funcionários, incluindo o órgão de direção, administração ou supervisão, a fim de assegurar que os mesmos possuam formação para desempenhar as suas funções e responsabilidades para reduzir o erro humano, o roubo, a fraude, a utilização indevida ou a perda. As empresas devem garantir que o programa de formação proporcione regularmente formação a todos os funcionários.

41. As empresas devem criar e aplicar programas periódicos de sensibilização no domínio da segurança para educar os seus funcionários, incluindo o órgão de direção, administração ou supervisão, sobre a forma como devem abordar os riscos relacionados com a segurança da informação.

## Orientação 14 – Gestão de operações de TIC

42. As empresas devem gerir as suas operações de TIC com base na estratégia em matéria de TIC. Devem existir documentos que definam a forma como as empresas operam, monitorizam e controlam os seus sistemas e serviços de TIC, incluindo a documentação de processos, procedimentos e operações críticos de TIC.

43. As empresas devem aplicar procedimentos de registo e de monitorização de operações críticas de TIC para permitir a deteção, análise e correção de erros.

44. As empresas devem manter um inventário atualizado dos seus ativos de TIC. O inventário de ativos de TIC deve ser suficientemente pormenorizado para permitir uma rápida identificação de um ativo de TIC, bem como da sua localização, classificação de segurança e propriedade.

45. As empresas devem monitorizar e gerir o ciclo de vida dos ativos de TIC, a fim de garantir que estes continuem a cumprir e a apoiar os requisitos empresariais e de gestão dos riscos. As empresas devem monitorizar se os ativos de TIC são apoiados pelos seus fornecedores ou promotores internos e se todas as correções e atualizações pertinentes são aplicadas com base num processo documentado. Os riscos decorrentes de ativos de TIC desatualizados ou não apoiados devem ser avaliados e reduzidos. Os ativos de TIC desativados devem ser processados e cedidos de forma segura.

46. As empresas devem aplicar processos de monitorização e de planeamento da capacidade e do desempenho para prevenir, detetar e responder atempadamente a importantes questões de desempenho dos sistemas de TIC e de escassez de capacidade em matéria de TIC.

47. As empresas devem definir e aplicar procedimentos de segurança e de recuperação de dados e de sistemas de TIC para garantir que possam ser recuperados conforme necessário. O âmbito e a frequência das cópias de segurança devem ser definidos em consonância com os requisitos de recuperação empresariais e a criticidade dos dados e dos sistemas de TIC, avaliados de acordo com a avaliação dos riscos realizada. Os testes dos procedimentos de segurança e de recuperação devem ser efetuados regularmente.

48. As empresas devem garantir que as cópias de segurança dos sistemas de TIC e dos dados sejam armazenadas num ou mais locais fora da localização primária, que sejam seguros e estejam suficientemente afastados da localização primária, de modo que não estejam expostos aos mesmos riscos.

## Orientação 15 - Gestão de problemas e incidentes em matéria de TIC

49. As empresas devem estabelecer e aplicar um processo de gestão de problemas e incidentes para monitorizar e registar incidentes operacionais ou de segurança e para permitir que as empresas continuem ou retomem funções empresariais e processos críticos quando ocorrerem perturbações.

50. As empresas devem determinar critérios e limites adequados para a classificação de um evento como um incidente operacional ou de segurança, bem como indicadores de alerta prévio que permitam à empresa ser capaz de detetar rapidamente este tipo de incidentes.

51. Para minimizar o impacto de eventos adversos e permitir uma recuperação atempada, as empresas devem estabelecer processos e estruturas organizacionais adequados para assegurar uma monitorização, um tratamento e um acompanhamento coerentes e integrados dos incidentes operacionais e de segurança com vista a garantir que as causas profundas sejam identificadas e tratadas e sejam tomadas ações/medidas corretivas para evitar a ocorrência repetida de incidentes. O processo de gestão de problemas e incidentes deve, pelo menos, estabelecer o seguinte:

    a) Os procedimentos para identificar, detetar, registar, categorizar e classificar os incidentes de acordo com uma prioridade definida pela empresa e baseada na criticidade empresarial e em contratos de serviço;

    b) As funções e responsabilidades para diferentes cenários de incidentes (por exemplo, erros, mau funcionamento, ciberataques);

    c) Um procedimento de gestão de problemas para identificar, analisar e resolver a causa profunda subjacente a um ou mais incidentes; as empresas devem analisar os incidentes operacionais ou de segurança que tenham sido identificados ou que tenham ocorrido dentro e/ou fora da organização, bem como devem ter em consideração os principais ensinamentos retirados destas análises e atualizar as medidas de segurança em conformidade;

    d) Planos de comunicação interna eficazes, incluindo procedimentos por etapas em caso de incidentes e de notificação de incidentes — abrangendo igualmente as reclamações de clientes relacionadas com a segurança — para garantir que:

i. os incidentes com um impacto adverso potencialmente elevado nos sistemas e serviços críticos de TIC sejam comunicados à direção de topo pertinente,

ii. o órgão de direção, administração ou supervisão seja informado numa base *ad hoc* em caso de incidentes significativos e, pelo menos, informado do impacto, da resposta e dos controlos adicionais a definir em resultado dos incidentes;

e) Procedimentos de resposta a incidentes para atenuar os impactos relacionados com os mesmos e para assegurar que o serviço se torne operacional e seguro em tempo útil;

f) Planos de comunicação externa específicos para processos e funções empresariais críticos, a fim de:

i. colaborar com as partes interessadas pertinentes para responder eficazmente ao incidente e recuperar do mesmo,

ii. fornecer informações oportunas, incluindo comunicação de incidentes, a partes externas (por exemplo, clientes, outros participantes no mercado, autoridades de supervisão competentes), conforme adequado e em consonância com a regulamentação aplicável.

## Orientação 16 – Gestão de projetos de TIC

52. As empresas devem aplicar uma metodologia de projetos de TIC (incluindo considerações sobre requisitos de segurança independentes) com um processo de governação e uma liderança de execução de projetos que sejam adequados para apoiar eficazmente a aplicação da estratégia em matéria de TIC através de projetos de TIC.

53. As empresas devem monitorizar e reduzir adequadamente os riscos decorrentes da carteira de projetos de TIC, tendo igualmente em consideração os riscos que possam resultar de interdependências entre diferentes projetos e de dependências de múltiplos projetos em relação aos mesmos recursos e/ou conhecimentos especializados.

## Orientação 17 – Aquisição e desenvolvimento de sistemas de TIC

54. As empresas devem desenvolver e aplicar um processo que regule a aquisição, o desenvolvimento e a manutenção de sistemas de TIC, a fim de garantir a proteção integral da confidencialidade, integridade e disponibilidade dos dados a tratar e o cumprimento dos requisitos de proteção definidos. Este processo deve ser concebido utilizando uma abordagem baseada no risco.

55. As empresas devem garantir que, antes de efetuar aquisições de sistemas ou atividades de desenvolvimento, os requisitos funcionais e não funcionais (incluindo os requisitos de segurança da informação) e os objetivos técnicos sejam claramente definidos.

56. As empresas devem assegurar a aplicação de medidas para evitar a alteração não intencional ou a manipulação intencional dos sistemas de TIC durante o desenvolvimento.

57. As empresas devem dispor de uma metodologia para testar e aprovar os sistemas de TIC, os serviços de TIC e as medidas de segurança da informação.

58. As empresas devem testar, de forma adequada, sistemas de TIC, serviços de TIC e medidas de segurança da informação, a fim de identificar potenciais fragilidades, violações e incidentes em matéria de segurança.

59. As empresas devem assegurar a segregação dos ambientes de produção em relação aos ambientes de desenvolvimento, aos ambientes de teste e a outros ambientes de não produção.

60. As empresas devem aplicar medidas para proteger a integridade dos códigos fonte (quando disponíveis) dos sistemas de TIC. Devem também documentar exaustivamente o desenvolvimento, a aplicação, o funcionamento e/ou a configuração dos sistemas de TIC para reduzir qualquer dependência desnecessária de peritos na matéria.

61. Os processos de aquisição e desenvolvimento de sistemas de TIC das empresas devem igualmente aplicar-se a sistemas de TIC desenvolvidos ou geridos pelos utilizadores finais da função empresarial fora da organização de TIC (por exemplo, aplicações de gestão empresarial ou aplicações informáticas para utilizadores finais), utilizando uma abordagem baseada no risco. As empresas devem manter um registo das aplicações em causa que apoiam funções empresariais ou processos críticos.

## Orientação 18 – Gestão de alterações em matéria de TIC

62. As empresas devem estabelecer e aplicar um processo de gestão de alterações em matéria de TIC para assegurar que todas as alterações introduzidas nos sistemas de TIC sejam registadas, avaliadas, testadas, aprovadas, autorizadas e aplicadas de forma controlada. As alterações em matéria de TIC efetuadas durante situações de urgência ou emergência devem poder ser rastreadas e ser notificadas *ex post* ao proprietário do ativo pertinente para análise *ex post*.

63. As empresas devem averiguar se as alterações do ambiente operacional existente afetam as medidas de segurança em vigor ou exigem a adoção de medidas adicionais para atenuar os riscos envolvidos. Estas alterações devem estar em conformidade com o processo formal de gestão de alterações das empresas.

## Orientação 19 – Gestão da continuidade das atividades

64. Como parte da política global de continuidade das atividades da empresa, o órgão de direção, administração ou supervisão é responsável por definir e aprovar a política de continuidade das TIC das empresas. A política de continuidade das TIC deve ser devidamente comunicada a nível das empresas e ser aplicável a todos os funcionários pertinentes e, se pertinente, aos prestadores de serviços.

## Orientação 20 – Análise de impacto nas atividades

65. Como parte de uma gestão sólida da continuidade das atividades, as empresas devem realizar uma análise de impacto nas atividades para avaliar a sua exposição a perturbações graves nas atividades e os seus potenciais impactos, a nível quantitativo e qualitativo, recorrendo a dados internos e/ou externos e à análise de cenários. A análise de impacto nas atividades deve ter igualmente em consideração a criticidade dos processos e atividades empresariais, funções empresariais, papéis e ativos (por exemplo, ativos de informação e ativos de TIC) que tenham sido identificados e classificados, bem como as suas interdependências, em conformidade com a orientação 4.

66. As empresas devem assegurar que os seus sistemas e serviços de TIC sejam concebidos e alinhados com as suas análises de impacto nas atividades, por exemplo, através da redundância de determinados componentes críticos para evitar perturbações causadas por eventos que tenham impacto nos componentes em causa.

## Orientação 21 – Planeamento da continuidade das atividades

67. Os planos de continuidade das atividades (PCA) das empresas a nível global devem ter em consideração os riscos substanciais que possam ter um impacto negativo nos sistemas e serviços de TIC. Os planos devem apoiar objetivos para proteger e, se necessário, restabelecer a confidencialidade, integridade e disponibilidade dos processos e atividades empresariais, funções empresariais, papéis e ativos das empresas (por exemplo, ativos de informação e ativos de TIC). As empresas devem coordenar-se com as partes interessadas internas e externas pertinentes, se for caso disso, durante a elaboração destes planos.

68. As empresas devem criar PCA para garantir que conseguem reagir adequadamente a potenciais cenários de falha dentro de um objetivo de tempo de recuperação (o intervalo de tempo máximo dentro do qual um sistema ou processo deve ser restaurado após um incidente) e de um objetivo de ponto de recuperação (o intervalo de tempo máximo durante o qual é aceitável que os dados se percam em caso de incidente a um nível de serviço predefinido).

69. As empresas devem considerar um conjunto de diferentes cenários nos seus PCA (incluindo cenários extremos mas plausíveis e cenários de ciberataque), bem como devem avaliar o potencial impacto de tais cenários. Com base nos cenários em questão, as empresas devem descrever a forma como a continuidade dos sistemas e serviços de TIC, bem como a segurança da informação das empresas, são asseguradas.

## Orientação 22 – Planos de recuperação e resposta

70. Com base nas análises de impacto nas atividades e nos cenários plausíveis, as empresas devem elaborar planos de recuperação e resposta. Tais planos devem especificar as condições que podem exigir a ativação do plano e as ações que devem ser tomadas para assegurar a integridade, disponibilidade, continuidade e recuperação, pelo menos, de sistemas de TIC, serviços de TIC e dados críticos das empresas. Os planos de recuperação e resposta devem visar o cumprimento dos objetivos de recuperação das operações das empresas.

71. Os planos de recuperação e resposta devem ter em consideração as opções de recuperação a curto e, sempre que necessário, a longo prazo. No mínimo, os planos devem:

    a) centrar-se na recuperação das operações de serviços importantes de TIC, funções empresariais, processos de apoio, ativos de informação e respetivas interdependências para evitar efeitos adversos no funcionamento da empresa;

    b) ser documentados e disponibilizados às unidades de negócio e de apoio e facilmente acessíveis em caso de emergência, incluindo uma clara definição das funções e responsabilidades; e

    c) ser continuamente atualizados em consonância com os ensinamentos retirados dos incidentes, testes, riscos recentemente identificados e ameaças, bem como com as alterações introduzidas nos objetivos de recuperação e prioridades.

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

73. Como parte dos planos de recuperação e resposta, as empresas devem ter em consideração e aplicar medidas de continuidade para atenuar as falhas de prestadores de serviços, que são de importância fundamental para a continuidade dos serviços de TIC das empresas (em consonância com as disposições das orientações da EIOPA sobre o sistema de governação e as orientações da EIOPA sobre a subcontratação a prestadores de serviços de computação em nuvem).

## Orientação 23 – Teste dos planos

74. As empresas devem testar os seus PCA e garantir que a operação dos seus processos e atividades empresariais críticos, funções empresariais, papéis e ativos (por exemplo, ativos de informação e ativos de TIC) e respetivas interdependências (incluindo os fornecidos por prestadores de serviços) sejam testadas regularmente com base no perfil de risco das empresas.

75. Os PCA devem ser atualizados regularmente, com base nos resultados dos testes, nas informações sobre ameaças atuais e nos ensinamentos retirados de eventos anteriores. Devem ser igualmente incluídas quaisquer alterações pertinentes dos objetivos de recuperação (incluindo o objetivo de tempo de recuperação e o objetivo de ponto de recuperação) e/ou alterações dos processos e atividades empresariais, funções empresariais, papéis e ativos (por exemplo, ativos de informação e ativos de TIC).

76. Os testes dos PCA devem demonstrar que estes são capazes de manter a viabilidade das atividades até ao restabelecimento das operações críticas a um nível de serviço predefinido ou de tolerância face ao impacto.

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

## Orientação 24 – Comunicação de crises

78. No caso de uma interrupção ou emergência, e durante a aplicação dos PCA, as empresas devem garantir que dispõem de medidas eficazes de comunicação de crises, de modo que todas as partes interessadas internas e externas pertinentes, incluindo as autoridades de supervisão competentes quando tal for exigido pela regulamentação nacional, bem como os prestadores de serviços pertinentes, sejam informados de forma atempada e adequada.

## Orientação 25 – Subcontratação de serviços de TIC e sistemas de TIC

79. Sem prejuízo das orientações da EIOPA sobre a subcontratação a prestadores de serviços de computação em nuvem, em caso de subcontratação dos serviços e sistemas de TIC, as empresas devem assegurar o cumprimento dos requisitos pertinentes aplicáveis aos serviços de TIC ou aos sistemas de TIC.

80. Em caso de subcontratação de funções críticas ou importantes, as empresas devem garantir que as obrigações contratuais do prestador de serviços (por exemplo, contratos, acordos de nível de serviço, disposições de rescisão nos contratos pertinentes) incluam, pelo menos, o seguinte:

    a) Objetivos e medidas adequados e proporcionais relacionados com a segurança da informação, incluindo requisitos como requisitos mínimos de

segurança da informação; especificações do ciclo de vida dos dados das empresas; direitos de acesso e auditoria; bem como quaisquer requisitos relativos à localização dos centros de dados e requisitos relativos à cifragem de dados, à segurança da rede e aos processos de monitorização da segurança;

b) Acordos de nível de serviço, a fim de assegurar a continuidade dos serviços e sistemas de TIC e as metas de desempenho em condições normais, bem como as previstas em planos de contingência no caso de interrupção do serviço; e

c) Procedimentos de tratamento de incidentes operacionais e de segurança, incluindo procedimentos por etapas e de comunicação de informações.

81. As empresas devem monitorizar e assegurar o nível de conformidade de tais prestadores de serviços com os seus objetivos de segurança, medidas e metas de desempenho definidos.

## Regras em matéria de conformidade e comunicação de informações

82. O presente documento contém orientações emitidas ao abrigo do artigo 16.º do Regulamento (UE) n.º 1094/2010. Nos termos do artigo 16.º, n.º 3, do referido regulamento, as autoridades competentes e as empresas devem desenvolver todos os esforços para dar cumprimento às orientações e recomendações.

83. As autoridades competentes que deem ou tencionem dar cumprimento às presentes orientações devem incorporá-las de forma adequada no seu quadro regulamentar ou de supervisão.

84. As autoridades competentes devem confirmar perante a EIOPA se dão ou tencionam dar cumprimento às presentes orientações, indicando as razões para o não cumprimento, no prazo de dois meses a contar da data de publicação das versões traduzidas.

85. Na ausência de resposta no prazo referido, as autoridades competentes serão consideradas incumpridoras da obrigação de comunicação e declaradas como tal.

## Disposição final relativa à revisão

86. As presentes orientações devem ser objeto de revisão pela EIOPA.