# Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação

## APRESENTAÇÃO

**1)** Este Projeto de Revisão foi elaborado pela Comissão de Estudo de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade (CE-021:004.027) do Comitê Brasileiro de Tecnologias da Informação e Transformação Digital (ABNT/CB-021), nas reuniões de:

| | | |
|---|---|---|
| 31.08.2022 | 06.12.2022 | 24.01.2023 |

a) é previsto para cancelar e substituir a ABNT NBR ISO/IEC 27005:2019, a qual foi tecnicamente revisada, quando aprovado, sendo que, nesse ínterim, a referida norma continua em vigor;

b) é previsto para ser idêntico à ISO/IEC 27005:2022, que foi elaborada pelo *Joint Technical Committee Information security, cybersecurity and privacy protection* (ISO/JTC 1), *Subcommittee Information security, cybersecurity and privacy protection* (SC 27);

c) .

**2)** Aqueles que tiverem conhecimento de qualquer direito de patente devem apresentar esta informação em seus comentários, com documentação comprobatória.

**3)** Analista ABNT – Carolina Martins de Oliveira.

# Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação

*Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

## Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas pelas partes interessadas no tema objeto da normalização.

Os Documentos Técnicos internacionais adotados são elaborados conforme as regras da ABNT Diretiva 3.

A ABNT chama a atenção para que, apesar de ter sido solicitada manifestação sobre eventuais direitos de patentes durante a Consulta Nacional, estes podem ocorrer e devem ser comunicados à ABNT a qualquer momento (Lei nº 9.279, de 14 de maio de 1996).

Os Documentos Técnicos ABNT, assim como as Normas Internacionais (ISO e IEC), são voluntários e não incluem requisitos contratuais, legais ou estatutários. Os Documentos Técnicos ABNT não substituem Leis, Decretos ou Regulamentos, aos quais os usuários devem atender, tendo precedência sobre qualquer Documento Técnico ABNT.

Ressalta-se que os Documentos Técnicos ABNT podem ser objeto de citação em Regulamentos Técnicos. Nestes casos, os órgãos responsáveis pelos Regulamentos Técnicos podem determinar as datas para exigência dos requisitos de quaisquer Documentos Técnicos ABNT.

A ABNT NBR ISO/IEC 27005 foi elaborada no Comitê Brasileiro de Tecnologias da Informação e Transformação Digital (ABNT/CB-021), pela Comissão de Estudo de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade (CE-021:004.027). O Projeto de Revisão circulou em Consulta Nacional conforme Edital nº XX, de XX.XX.XXXX a XX.XX.XXXX.

A ABNT NBR ISO/IEC 27005 é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 27005:2022, que foi elaborada pelo *Joint Technical Committee Information security, cybersecurity and privacy protection* (ISO/JTC 1), *Subcommittee Information security, cybersecurity and privacy protection* (SC 27).

A ABNT NBR ISO/IEC 27005:2023 cancela e substitui a ABNT ISO/IEC 27005:2019, a qual foi tecnicamente revisada.

O Escopo da ABNT NBR ISO/IEC 27005 em inglês é o seguinte:

## *Scope*

*This document provides guidance to assist organizations to:*

— *fulfil the requirements of ABNT NBR ISO/IEC 27001 concerning actions to address information security risks;*

— *perform information security risk management activities, specifically information security risk assessment and treatment.*

*This document is applicable to all organizations, regardless of type, size or sector.*

# Introdução

Este documento fornece orientações para:

— implementação dos requisitos de riscos de segurança da informação especificados na ABNT NBR ISO/IEC 27001;

— referências essenciais dentro das normas desenvolvidas pelo ISO/IEC JTC 1/SC 27 para apoiar atividades de gestão de riscos de segurança da informação;

— ações que abordem riscos relacionados à segurança da informação (ver ABNT NBR ISO/IEC 27001:2022, 6.1 e Seção 8);

— implementação das orientações de gestão de riscos da ABNT NBR ISO 31000 no contexto da segurança da informação.

Este documento contém orientações detalhadas para a gestão de riscos e complementa as orientações da ABNT NBR ISO/IEC 27003.

Este documento destina-se a ser usado por:

— organizações que pretendam estabelecer e implementar um sistema de gestão de segurança da informação (SGSI) de acordo com a ABNT NBR ISO/IEC 27001;

— pessoas que atuem ou estejam envolvidas na gestão de riscos de segurança da informação (por exemplo, profissionais do SGSI, proprietários de riscos e outras partes interessadas);

— organizações que pretendam melhorar seu processo de gestão de riscos de segurança da informação.

# Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação

## 1 Escopo

Este documento fornece orientações para ajudar as organizações a:

— cumprir os requisitos da ABNT NBR ISO/IEC 27001 em relação às ações para abordar riscos de segurança da informação;

— realizar atividades de gestão de riscos de segurança da informação, especificamente avaliação e tratamento de riscos de segurança da informação.

Este documento é aplicável a todas as organizações, independentemente do tipo, tamanho ou setor.

## 2 Referência normativa

O documento a seguir é citado no texto de tal forma que seu conteúdo, total ou parcial, constitui requisitos para este Documento. Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do referido documento (incluindo emendas).

ISO/IEC 27000, *Information Technology – Security Techniques – Information security management systems - Overview and vocabulary*

## 3 Termos e definições

Para os efeitos deste documento, aplicam-se os termos e definições da ISO/IEC 27000 e os seguintes.

A ISO e a IEC mantêm bases de dados terminológicos para uso na normalização nos seguintes endereços:

ISO *Online browsing plataform*: disponível em https://www.iso.org/obp

IEC *Eletropedia*: disponível em https://www.electropedia.org/

### 3.1 Termos relacionados ao risco de segurança da informação

**3.1.1**
**contexto externo**
ambiente externo no qual a organização busca atingir seus objetivos

Nota 1 de entrada: O contexto externo pode incluir:

— o ambiente social, cultural, político, legal, regulatório, financeiro, tecnológico, econômico, ambiente geológico, seja internacional, nacional, regional ou local;

— os fatores-chave e as tendências que afetam os objetivos da organização;

— as relações, percepções, valores, necessidades e expectativas das partes interessadas externas;

— as relações e compromissos contratuais;

— a complexidade das redes e dependências.

[FONTE: ABNT ISO Guia 73:2009, 3.3.1.1, modificada – A Nota 1 de entrada foi modificada.]

**3.1.2**
**contexto interno**
ambiente interno no qual a organização busca atingir seus objetivos

Nota 1 de entrada: O contexto interno pode incluir:

— visão, missão e valores;

— governança, estrutura organizacional, papéis e responsabilidades;

— estratégia, objetivos e políticas;

— a cultura da organização;

— normas, diretrizes e modelos adotados pela organização;

— capacidades compreendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);

— dados, sistemas de informação e fluxos de informações;

— relações com as partes interessadas internas, levando em consideração suas percepções e valores;

— relações e compromissos contratuais;

— interdependências e interconexões internas.

[FONTE: ABNT ISO Guia 73:2009, 3.3.1.2, modificada – A Nota 1 de entrada foi modificada.]

**3.1.3**
**risco**
efeito da incerteza nos objetivos

Nota 1 de entrada: Um efeito é um desvio em relação ao esperado, positivo ou negativo.

Nota 2 de entrada: Objetivos podem possuir diferentes aspectos e categorias, e podem ser aplicados em diferentes níveis.

Nota 3 de entrada: A incerteza é o estado, mesmo parcial, de deficiência de informações relacionadas àcompreensão ou conhecimento de um *evento* (3.1.11), sua *consequência* (3.1.14) ou *probabilidade* (3.1.13).

Nota 4 de entrada: Risco é normalmente expresso em termos de *fontes de risco* (3.1.6), eventos potenciais, suas consequências e suas probabilidades.

Nota 5 de entrada: No contexto dos sistemas de gestão de segurança da informação, os riscos de segurança da informação podem ser expressos como o efeito da incerteza nos objetivos de segurança da informação.

Nota 6 de entrada: Os riscos de segurança da informação geralmente estão associados a um efeito negativo da incerteza nos objetivos de segurança da informação.

Nota 7 de entrada: Os riscos de segurança da informação podem estar associados ao potencial de que as *ameaças* (3.1.9) explorem *vulnerabilidades* (3.1.10) de um ativo de informação ou grupo de ativos de informação e, assim, causem danos a uma organização.

[FONTE: ABNT NBR ISO 31000:2018, 3.1, modificada – a frase: “Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças” foi substituída por “positivo ou negativo” na Nota 1 de entrada; a entrada original da Nota 3 foi renumerada como Nota 4 de entrada; e as Notas 3, 5, 6 e 7 de entrada foram adicionadas.]

**3.1.4**
**cenário de risco**
sequência ou combinação de *eventos* (3.1.11) que levam da causa inicial à consequência indesejada (3.1.14)

[FONTE: ISO 17666:2016, 3.1.13, modificada – Nota 1 de entrada foi excluída.]

**3.1.5**
**proprietário do risco**
pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um *risco* (3.1.3)

[FONTE: ABNT ISO Guia 73:2009, 3.5.1.5]

**3.1.6**
**fonte de risco**
elemento que, individualmente ou combinado, tem o potencial para dar origem ao *risco* (3.1.3)

Nota 1 de entrada: Uma fonte de risco pode ser um desses três tipos:

— humano;

— ambiental;

— técnico.

Nota 2 de entrada: Uma fonte de risco do tipo humano pode ser intencional ou não.

[FONTE: ABNT NBR ISO 31000:2018, 3.4, modificada – As notas 1 e 2 de entrada foram adicionadas.]

**3.1.7**
**critérios de risco**
termos de referência contra os quais a significância de um *risco* (3.1.3) é avaliada

Nota 1 de entrada: Os critérios de risco são baseados nos objetivos organizacionais e em *contexto externo* (3.1.1) e *contexto interno* (3.1.2).

Nota 2 de entrada: Os critérios de risco podem ser derivados de normas, leis, políticas e outros requisitos.

[FONTE: ABNT ISO Guia 73:2009, 3.3.1.3]

**3.1.8**
**apetite pelo risco**
quantidade e tipo de *riscos* (3.1.3) que uma organização está preparada para buscar ou reter

[FONTE: ABNT ISO Guia 73:2009, 3.7.1.2]

**3.1.9**
**ameaça**
causa potencial de um *incidente de segurança da informação* (3.1.12) que pode resultar em danos a um sistema ou prejuízos a uma organização

**3.1.10**
**vulnerabilidade**
fraqueza de um ativo ou *controle* (3.1.16) que pode ser explorada e então pode ocorrer um *evento* (3.1.11) com uma *consequência* (3.1.14) negativa

**3.1.11**
**evento**
ocorrência ou mudança em um conjunto específico de circunstâncias

Nota 1 de entrada: Um evento pode consistir em uma ou mais ocorrências, e pode ter várias causas e várias *consequências* (3.1.14).

Nota 2 de entrada: Um evento pode também ser algo que é esperado, mas não acontece, ou algo que é inesperado, mas acontece.

[FONTE: ABNT NBR ISO 31000:2018, 3.5, modificada – A Nota 3 de entrada foi excluída.]

**3.1.12**
**incidente de segurança da informação**
um único ou uma série de eventos de segurança da informação indesejados ou inesperados que têm uma probabilidade significativa de comprometer as operações do negócio e ameaçar a segurança da informação

**3.1.13**
**probabilidade (*likelihood*)**
chance de algo acontecer

Nota 1 de entrada: Na terminologia de gestão de riscos, a palavra “probabilidade” é utilizada para referir-se à chance de algo acontecer, não importando se, de forma definida, medida ou determinada, objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (tal como probabilidade ou frequência durante um determinado período de tempo).

Nota 2 de entrada: O termo em inglês “*likelihood*” não tem um equivalente direto em algumas línguas; em vez disso, o equivalente ao termo “*probability*” é frequentemente utilizado. Entretanto, em inglês, “*probability*” é muitas vezes interpretado estritamente como uma expressão matemática. Portanto, na terminologia de gestão de riscos, “*likelihood*” é utilizado com a mesma ampla interpretação que o termo “*probability*” têm em muitos outros idiomas além do inglês.

[FONTE: ABNT NBR ISO 31000:2018, 3.7]

**3.1.14**
**consequência**
resultado de um *evento* (3.1.11) que afeta os objetivos

Nota 1 de entrada: Uma consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos, diretos ou indiretos, nos objetivos.

Nota 2 de entrada: As consequências podem ser expressas qualitativa ou quantitativamente.

Nota 3 de entrada: Qualquer consequência pode escalar por meio de efeitos cascata e cumulativos.

[FONTE: ABNT NBR ISO 31000:2018, 3.6]

**3.1.15**
**nível de risco**
significância de um risco (3.1.3), expressa em termos da combinação das *consequências* (3.1.14) e de suas *probabilidades* (3.1.13)

[FONTE: ABNT ISO Guia 73:2009, 3.6.1.8, modificado – a frase: “magnitude de um risco ou combinação de riscos” foi substituída por “significância de um risco”.]

**3.1.16**
**controle**
medida que mantém e/ou modifica o *risco* (3.1.3)

Nota 1 de entrada: Controles incluem, mas não estão limitados a, qualquer processo, política, dispositivo, prática ou outras condições e/ou ações que mantêm e/ou modificam o risco.

Nota 2 de entrada: Controles podem nem sempre exercer o efeito modificador pretendido ou presumido.

[FONTE: ABNT NBR ISO 31000:2018, 3.8]

**3.1.17**
**risco residual**
*risco* (3.1.3) remanescente após o *tratamento do risco* (3.2.7)

Nota 1 de entrada: O risco residual pode conter riscos não identificados.

Nota 2 de entrada: Os riscos residuais também podem conter riscos retidos.

[FONTE: ABNT ISO Guia 73:2009, 3.8.1.6, modificado – A Nota 2 de entrada foi modificada.]

## 3.2 Termos relacionados à gestão de riscos de segurança da informação

**3.2.1**
**processo de gestão de riscos**
aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos *riscos* (3.1.3)

[FONTE: ABNT ISO Guia 73:2009, 3.1]

**3.2.2**
**comunicação e consulta de risco**
conjunto de processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e dialogar com as partes interessadas, com a relação a gerenciar *riscos* (3.1.3)

Nota 1 de entrada: As informações podem referir-se à existência, natureza, forma, *probabilidade* (3.1.13), significância, avaliação, aceitação e tratamento de riscos.

Nota 2 de entrada: A consulta é um processo bidirecional de comunicação sistematizada entre uma organização e suas partes interessadas sobre um assunto antes de tomar uma decisão ou determinar uma orientação sobre essa questão. A consulta é:

— um processo que impacta uma decisão por meio da influência em vez do poder;

— uma entrada para a tomada de decisões, e não uma tomada de decisão em conjunto.

**3.2.3**
**processo de avaliação de riscos (*risk assessment*)**
processo global de *identificação de riscos* (3.2.4), *análise de riscos* (3.2.5) e *avaliação de riscos* (3.2.6)

[FONTE: ABNT ISO Guia 73:2009, 3.4.1]

**3.2.4**
**identificação de riscos**
processo de busca, reconhecimento e descrição de *riscos* (3.1.3)

Nota 1 de entrada: A identificação de riscos envolve a identificação das *fontes de risco* (3.1.6), *eventos* (3.1.1.11), suas causas e suas *consequências* (3.1.14) potenciais.

Nota 2 de entrada: A identificação de riscos pode envolver dados históricos, análise teórica, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas.

[FONTE: ABNT ISO Guia 73:2009, 3.5.1, modificado – “parte interessada” substituiu “*stakeholder*” na Nota 2 de entrada.]

**3.2.5**
**análise de riscos**
processo de compreender a natureza do *risco* (3.1.3) e determinar o *nível de risco* (3.1.15)

Nota 1 de entrada: A análise de riscos fornece a base para a *avaliação de riscos* (3.2.6) e para as decisões sobre o *tratamento de riscos* (3.2.7).

Nota 2 de entrada: A análise de riscos inclui a estimativa de risco.

[FONTE: ABNT ISO Guia 73:2009, 3.6.1]

**3.2.6**
**avaliação de riscos (*risk evaluation*)**
processo de comparar os resultados da *análise de riscos* (3.2.5) com os *critérios de risco* (3.1.7) para determinar se o *risco* (3.1.3) e/ou sua significância é aceitável ou tolerável

Nota 1 de entrada: Avaliação de riscos auxilia na decisão sobre o *tratamento de riscos* (3.2.7).

[FONTE: ABNT ISO Guia 73:2009, 3.7.1, modificado – “significância” substituiu “magnitude”.]

**3.2.7**
**tratamento de riscos**
processo para modificar o *risco* (3.1.3)

Nota 1 de entrada: O tratamento de riscos pode envolver:

— a ação de evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco;

— assumir ou aumentar o risco, a fim de buscar uma oportunidade;

— a remoção da *fonte de risco* (3.1.6);

— a alteração da *probabilidade* (3.1.13);

— a alteração das *consequências* (3.1.14);

— o compartilhamento do risco com outra parte ou partes (incluindo contratos e financiamento do risco); e

— a retenção do risco por decisão consciente.

Nota 2 de entrada: O tratamento de riscos de segurança da informação não inclui “assumir ou aumentar o risco, a fim de buscar uma oportunidade”, mas a organização pode ter essa opção para gestão geral de riscos.

Nota 3 de entrada: Tratamentos de risco que lidam com consequências negativas às vezes são chamados de “mitigação de riscos”, “eliminação de riscos”, “prevenção de riscos” e “redução de riscos”.

Nota 4 de entrada: O tratamento de riscos pode criar novos riscos ou modificar riscos existentes.

[FONTE: ABNT ISO Guia 73:2009, 3.8.1, modificado - Nota 1 de entrada foi adicionada e as Nota 1 de entrada e Nota 2 de entrada originais foram renumeradas como Nota 2 de entrada e Nota 3 de entrada.]

**3.2.8**
**aceitação do risco**
decisão consciente de assumir um *risco* (3.1.3) específico

Nota 1 de entrada: A aceitação do risco pode ocorrer sem o *tratamento do risco* (3.2.7), ou durante o processo de tratamento de riscos.

Nota 2 de entrada: Riscos aceitos estão sujeitos a monitoramento e análise crítica.

[FONTE: ABNT ISO Guia 73:2009, 3.7.1.6]

**3.2.9**
**compartilhamento de risco**
forma de *tratamento de riscos* (3.2.7) que envolve a distribuição acordada de *riscos* (3.1.3) com outras partes

Nota 1 de entrada: Requisitos legais ou regulatórios podem limitar, proibir ou ordenar o compartilhamento de risco.

Nota 2 de entrada: O compartilhamento de risco pode ser realizado por meio de seguros ou outras formas de contrato.

Nota 3 de entrada: A extensão em que o risco é distribuído pode depender da confiabilidade e clareza dos acordos de compartilhamento.

Nota 4 de entrada: A transferência de risco é uma forma de compartilhamento de risco.

[FONTE: ABNT ISO Guia 73:2009, 3.8.1.3]

**3.2.10**
**retenção de riscos**
aceitação temporária do benefício potencial de ganho, ou do ônus da perda, a partir de um *risco* (3.1.3) específico

Nota 1 de entrada: A retenção pode ser restrita a um determinado período de tempo.

Nota 2 de entrada: O *nível de risco* (3.1.15) retido pode depender de *critérios de risco* (3.1.7).

[FONTE: ABNT ISO Guia 73:2009, 3.8.1.5, modificado — A palavra “temporária” foi adicionada no início da definição e da frase; “A retenção de riscos inclui a aceitação de riscos residuais” foi substituída por “A retenção pode ser restrita a um determinado período de tempo” na Nota 1 de entrada.]

## 4 Estrutura deste documento

Este documento está estruturado da seguinte forma:

— Seção 5: Gestão de riscos de segurança da informação;

— Seção 6: Estabelecimento de contexto;

— Seção 7: Processo de avaliação de riscos de segurança da informação;

— Seção 8: Processo de tratamento de riscos de segurança da informação;

— Seção 9: Operação;

— Seção 10: Alavancagem dos processos relacionados ao SGSI.

Com exceção das descrições dadas nas subseções gerais, todas as atividades de gestão de riscos apresentadas da Seção 7 à Seção 10 estão estruturadas da seguinte forma:

Entrada: Identifica todas as informações necessárias para realizar a atividade.

Ação: Descreve a atividade.

Gatilho: Fornece orientações sobre quando iniciar a atividade, por exemplo, por causa de uma mudança dentro da organização, ou conforme um plano ou uma mudança no contexto externo da organização.

Saída: Identifica qualquer informação derivada após a realização da atividade, bem como quaisquer critérios que convém que tal saída satisfaça.

Orientação: Fornece orientações sobre a realização da atividade, palavra-chave e conceito-chave.

# 5 Gestão de riscos de segurança da informação

## 5.1 Processo de gestão de riscos de segurança da informação

O processo de gestão de riscos de segurança da informação é apresentado na Figura 1.

NOTA Esse processo é baseado no processo geral de gestão de riscos definido na ABNT NBR ISO 31000.

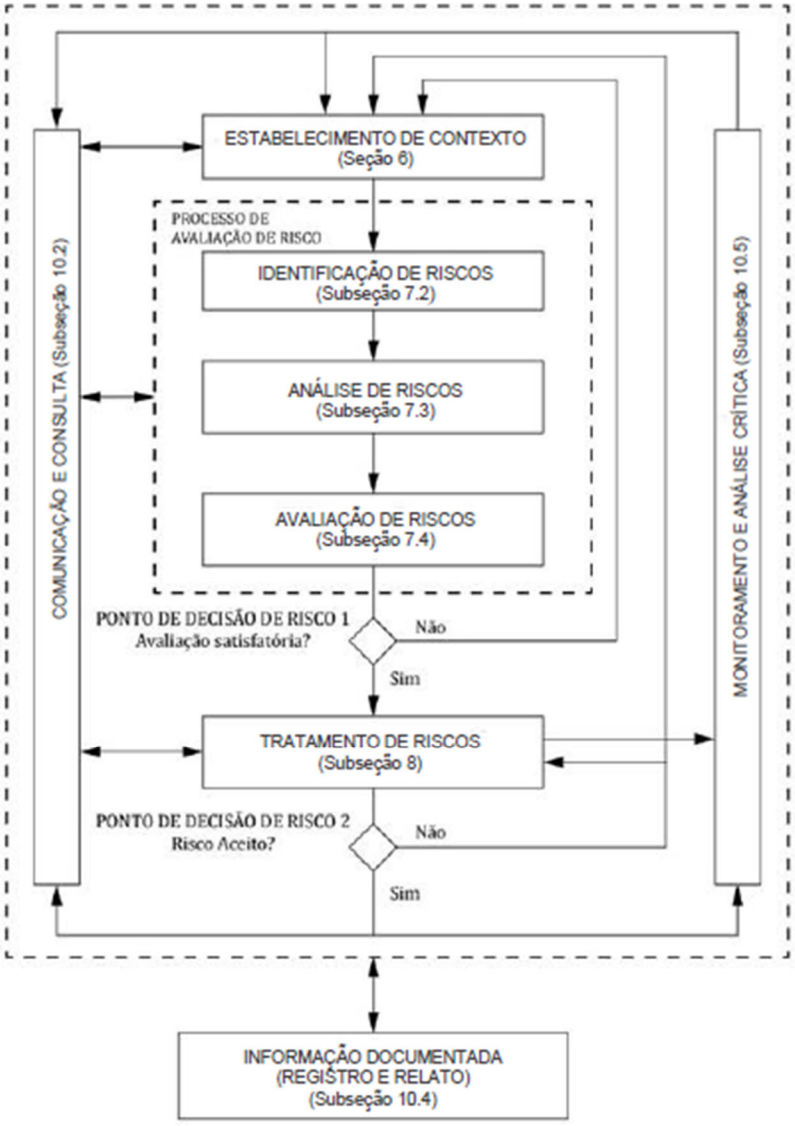



**Figura 1 – Processo de gestão de riscos de segurança da informação**

Como apresenta a Figura 1, o processo de gestão de riscos de segurança da informação pode ser iterativo para atividades do processo de avaliação de riscos e/ou tratamento de riscos. Uma abordagem iterativa para a realização do processo de avaliação de riscos pode aumentar a profundidade e os detalhes da avaliação em cada iteração. A abordagem iterativa proporciona um bom equilíbrio entre minimizar o tempo e o esforço gasto na identificação de controles, ao mesmo tempo em que assegura que os riscos sejam devidamente avaliados.

Estabelecimento de contexto significa a montagem do contexto interno e externo para a gestão de riscos de segurança da informação, ou uma avaliação de riscos de segurança da informação.

Se o processo de avaliação de riscos fornecer informações suficientes para determinar efetivamente as ações necessárias para modificar os riscos a um nível aceitável, então a tarefa está completa e o tratamento de riscos segue. Se as informações forem insuficientes, convém que outra iteração do processo de avaliação de riscos seja realizada. Isso pode envolver uma mudança de contexto do processo de avaliação de riscos (por exemplo, escopo revisado), envolvimento de especialistas na área específica, ou outras formas de coletar as informações necessárias para permitir a modificação de risco a um nível aceitável (ver “ponto de decisão de risco 1” na Figura 1).

O tratamento de riscos envolve um processo iterativo de:

— formular e selecionar opções de tratamento de riscos;

— planejar e implementar o tratamento de riscos;

— avaliar a eficácia desse tratamento;

— decidir se o risco restante é aceitável;

— tomar o tratamento adicional, se não for aceitável.

É possível que o tratamento de riscos não leve imediatamente a um nível aceitável de riscos residuais. Nesta situação, outra tentativa de encontrar mais tratamento de riscos pode ser realizada, ou pode haver outra iteração do processo de avaliação de riscos, seja como um todo ou em partes. Isso pode envolver uma mudança de contexto da avaliação de riscos (por exemplo, por um escopo analisado criticamente), e o envolvimento de especialistas na área específica. O conhecimento sobre ameaças ou vulnerabilidades relevantes pode levar às melhores decisões sobre atividades adequadas de tratamento de riscos na próxima iteração da avaliação de riscos (ver “ponto de decisão de risco 2” na Figura 1).

O estabelecimento de contexto é apresentado detalhadamente na Seção 6, atividades de avaliação de riscos são apresentadas na Seção 7 e atividades de tratamento de riscos são apresentadas na Seção 8.

Outras atividades necessárias à gestão de riscos de segurança da informação são apresentadas na Seção 10.

## 5.2 Ciclos de gestão de riscos de segurança da informação

Convém que o processo de avaliação de riscos e o tratamento de riscos sejam atualizados regularmente e fundamentados em mudanças. Convém que isto se aplique a todo o processo de avaliação de riscos e as atualizações podem ser divididas em dois ciclos de gestão de riscos:

— ciclo estratégico, em que ativos de negócios, fontes de risco e ameaças, objetivos ou consequências para eventos de segurança da informação estão evoluindo a partir de mudanças no contexto geral da organização. Isso pode resultar em insumos para uma atualização geral do processo de avaliação de riscos ou avaliações de risco e dos tratamentos de riscos. Também pode servir como um insumo para identificar novos riscos e iniciar processos de avaliação de risco completamente novos;

— ciclo operacional, em que os elementos mencionados anteriormente servem como informações de entrada ou critérios de mudança que afetarão um processo de avaliação de riscos ou avaliação na qual convém que os cenários sejam analisados criticamente e atualizados. Convém que a análise crítica inclua a atualização do tratamento de riscos correspondente, conforme aplicável.

Convém que o ciclo estratégico seja conduzido em períodos mais longos de tempo, ou quando grandes mudanças ocorrem, enquanto para o ciclo operacional convém que seja mais curto dependendo dos riscos detalhados que são identificados e avaliados, bem como do tratamento de riscos relacionado.

O ciclo estratégico se aplica ao ambiente em que a organização busca alcançar seus objetivos, enquanto o ciclo operacional se aplica a todos os processos de avaliação de riscos considerando o contexto do processo de gestão de riscos. Em ambos os ciclos, pode haver muitos processos de avaliação de risco com contextos e escopo diferentes em cada avaliação.

# 6 Estabelecimento de contexto

## 6.1 Considerações organizacionais

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 4.1.

Uma organização é definida como uma pessoa ou grupo de pessoas que tem suas próprias funções com responsabilidades, autoridades e relacionamentos para alcançar seus objetivos. Uma organização não é necessariamente uma empresa, outro órgão societário ou pessoa jurídica, também pode ser um subconjunto de uma pessoa jurídica (por exemplo, o departamento de TI de uma empresa), e pode ser considerada como a “organização” no contexto do SGSI.

É importante entender que o apetite pelo risco, definido como a quantidade de risco que uma organização está disposta a buscar ou aceitar, pode variar consideravelmente de organização para organização. Por exemplo, fatores que afetam o apetite pelo risco de uma organização incluem tamanho, complexidade e setor. Convém que o apetite pelo risco seja definido e regularmente analisado criticamente pela Alta Direção.

Convém que a organização assegure que o papel do proprietário de risco seja determinado em termos das atividades de gestão em relação aos riscos identificados. Convém que os proprietários de risco tenham responsabilidade e autoridade adequadas para gerenciar riscos identificados.

## 6.2 Identificação de requisitos básicos das partes interessadas

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 4.2.

Convém que sejam identificados os requisitos básicos das partes interessadas relevantes, bem como o *status* de cumprimento desses requisitos. Isso inclui identificar todos os documentos de referência que estabelecem regras e controles de segurança e que se aplicam no âmbito da avaliação de riscos de segurança da informação.

Esses documentos de referência podem incluir, mas não se limitam a:

a) ABNT NBR ISO/IEC 27001:2022, Anexo A;

b) normas adicionais que abrangem o SGSI;

c) normas adicionais aplicáveis a um setor específico (por exemplo, financeiro, saúde);

d) regulamentos internacionais e/ou nacionais específicos;

e) regras de segurança interna da organização;

f) regras e controles de segurança de contratos ou acordos;

g) controles de segurança implementados com base em atividades anteriores de tratamento de riscos.

Convém que qualquer descumprimento dos requisitos básicos seja explicado e justificado. Convém que esses requisitos básicos e sua conformidade sejam a entrada para a avaliação da probabilidade e para o tratamento de riscos.

## 6.3 Aplicação da avaliação de riscos

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 4.3.

As organizações podem realizar processos de avaliação de risco incorporados em diversos processos, como gerenciamento de projetos, gestão de vulnerabilidades, gestão de incidentes, gestão de problemas ou até mesmo de forma improvisada para um determinado tópico específico identificado. Independentemente de como os processos de avaliação de risco são realizados, convém que cubram coletivamente todas as questões relevantes para a organização no âmbito de um SGSI.

Convém que o processo de avaliação de riscos ajude a organização a tomar decisões sobre a gestão dos riscos que afetam o alcance de seus objetivos. Convém, portanto, que isto seja direcionado a esses riscos e controles que, se gerenciados com sucesso, melhorarão a probabilidade de a organização atingir seus objetivos.

Mais informações sobre o contexto de um SGSI e as questões a serem compreendidas por meio do processo de avaliação de riscos são dadas na ABNT NBR ISO/IEC 27003.

## 6.4 Estabelecimento e manutenção de critérios de risco de segurança da informação

### 6.4.1 Geral

A ABNT NBR ISO/IEC 27001:2022, 6.1.2-a), especifica requisitos para que as organizações definam seus critérios de risco, ou seja, os termos de referência pelos quais avaliam a significância dos riscos que identificam e tomam decisões sobre riscos.

A ABNT NBR ISO/IEC 27001 especifica os requisitos para que uma organização estabeleça e mantenha critérios de risco de segurança da informação que incluem:

a) os critérios de aceitação de riscos;

b) os critérios para a realização de processos de avaliação de riscos de segurança da informação.

Em geral, para definir critérios de risco, convém que os seguintes sejam considerados:

— a natureza e os tipos de incertezas que podem afetar desfechos e objetivos (tangíveis e intangíveis);

— como a consequência e a probabilidade serão definidas, previstas e medidas;

— os fatores relacionados ao tempo;

— a consistência no uso de medidas;

— como o nível de risco será determinado;

— como as combinações e sequências de múltiplos riscos serão levadas em conta;

— a capacidade da organização.

Outras considerações sobre critérios de risco são apresentadas no Anexo A.

### 6.4.2 Critérios de aceitação de riscos

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-a)-1).

Na avaliação de riscos, convém que os critérios de aceitação de riscos sejam usados para determinar se um risco é aceitável ou não.

No tratamento de riscos, os critérios de aceitação de riscos podem ser usados para determinar se o tratamento de riscos proposto é suficiente para atingir um nível aceitável de risco ou se é necessário um tratamento de riscos adicional.

Convém que a organização defina níveis de aceitação de risco. Convém que o seguinte seja considerado durante o desenvolvimento:

a) a consistência entre os critérios de aceitação de riscos de segurança da informação e os critérios gerais de aceitação de riscos da organização;

b) o nível de gestão com autoridade delegada é identificado para tomar decisões de aceitação de riscos;

c) os critérios de aceitação de riscos podem incluir múltiplos limites e a autoridade para aceitação pode ser atribuída a diferentes níveis de gestão;

d) os critérios de aceitação de riscos podem basear-se apenas na probabilidade e consequência, ou podem ser estendidos para considerar também o equilíbrio custo/benefício entre perdas prospectivas e o custo dos controles;

e) diferentes critérios de aceitação de riscos podem se aplicar a diferentes classes de risco (por exemplo, riscos que podem resultar em não conformidade com regulamentos ou leis nem sempre são retidos, enquanto a aceitação de riscos pode ser permitida se a aceitação for resultado de uma exigência contratual);

f) os critérios de aceitação de riscos podem incluir requisitos para tratamento adicional futuro (por exemplo, um risco pode ser retido em uma base de curto prazo, mesmo quando o nível de risco excede os critérios de aceitação de riscos, se houver aprovação e compromisso para tomar medidas para implementar um conjunto de controles escolhidos para atingir um nível aceitável dentro de um período de tempo definido);

g) convém que os critérios de aceitação de risco sejam definidos com base no apetite pelo risco que indique quantidade e tipo de risco que a organização está disposta a perseguir ou reter;

h) os critérios de aceitação de riscos podem ser absolutos ou condicionais, dependendo do contexto.

Convém que os critérios de aceitação de riscos sejam estabelecidos considerando os seguintes fatores influenciadores:

— objetivos organizacionais;

— oportunidades organizacionais;

— aspectos legais e regulatórios;

— atividades operacionais;

— restrições tecnológicas;

— restrições financeiras;

— processos;

— relações com fornecedores;

— fatores humanos (por exemplo, relacionados à privacidade).

A lista de fatores influenciadores não é exaustiva. Convém que a organização considere os fatores influenciadores com base no contexto.

Um simples critério de aceitação (sim/não) nem sempre é suficiente na prática.

Em muitos casos, a decisão de aceitar o risco pode ser tomada em níveis específicos de risco (combinações específicas de probabilidade e consequência). No entanto, pode haver circunstâncias em que é necessário estabelecer limites de aceitação para consequências extremas, independentemente de sua probabilidade, ou probabilidades extremamente altas, independentemente das consequências, em que o efeito sobre a organização resulta principalmente de um ou outro.

Por exemplo, convém que a aceitação de um evento raro que aniquile o valor das ações de uma empresa, ou um dreno constante de recursos resultantes da necessidade de controlar infrações menores frequentes de uma política, seja considerada principalmente com base em quais dos dois fatores têm o efeito dominante sobre a organização.

Consequentemente, convém que os critérios de aceitação de riscos, idealmente, incluam a consideração da probabilidade e das consequências de forma independente, bem como os custos de gestão, em vez de meramente nível de risco como uma combinação de probabilidade e consequência.

Uma organização com apetite pelo risco aguçado pode estabelecer um limite maior de aceitação, aceitando assim mais riscos que uma organização com menor apetite pelo risco. Isso protege a organização do excesso de controle, ou seja, ter tantos controles de segurança da informação que impedem a capacidade da organização de alcançar seus objetivos.

Os critérios de aceitação de riscos podem diferir, dependendo de quanto tempo se espera que os riscos existam (por exemplo, os riscos podem estar associados a uma atividade temporária ou de curto prazo).

Convém que os critérios de risco sejam mantidos sob análise crítica e atualizados conforme necessário, como resultado de quaisquer alterações no contexto da gestão de riscos de segurança da informação.

EXEMPLO Uma pequena empresa pode inicialmente ter um apetite pelo risco aguçado, mas à medida que ela cresce, pode diminuir seu apetite pelo risco.

Convém que os critérios de aceitação de riscos sejam aprovados pelo nível de gestão autorizado.

### 6.4.3 Critérios para a realização de processos de avaliação de riscos de segurança da informação

#### 6.4.3.1 Geral

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-a)-2).

Os critérios de avaliação de riscos especificam como a significância de um risco é determinada em termos de suas consequências, probabilidade e nível de risco.

Convém que os critérios de avaliação de riscos de segurança da informação levem em conta a adequação das atividades de gestão de riscos.

As considerações para isso incluem:

a) o nível de classificação das informações;

b) a quantidade e qualquer concentração de informação;

c) o valor estratégico dos processos de negócios que fazem uso das informações;

d) a criticidade das informações e ativos relacionados às informações envolvidas;

e) a importância operacional e empresarial de disponibilidade, a confidencialidade e a integridade;

f) as expectativas e percepções das partes interessadas (por exemplo, Alta Direção);

g) as consequências negativas, como perda de boa vontade e reputação;

h) a consistência com os critérios de riscos organizacionais.

Convém que os critérios de avaliação de riscos, ou uma base formal para defini-los, sejam padronizados em toda a organização para todos os tipos de processos de avaliação de riscos, pois isso pode facilitar a comunicação, comparação e agregação de riscos associados a múltiplos domínios de negócios.

Os critérios de avaliação de riscos de segurança da informação normalmente incluem:

— consequências;

— probabilidade;

— nível de risco.

#### 6.4.3.2 Critérios de consequência

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-a)-2).

A ABNT NBR ISO/IEC 27001 está relacionada com as consequências que são direta ou indiretamente afetadas pela preservação ou perda de confidencialidade, integridade e disponibilidade de informações no âmbito do SGSI. Convém que os critérios de consequência sejam desenvolvidos e especificados em termos de extensão de dano ou perda, ou danos a uma organização ou indivíduo resultante da perda de confidencialidade, integridade e disponibilidade de informações. Ao definir critérios de consequência, convém que sejam considerados principalmente:

a) perda de vidas ou danos aos indivíduos ou grupos;

b) perda de liberdade, dignidade ou direito à privacidade;

c) perda de pessoal e capital intelectual (habilidades e expertise);

d) operações internas ou de terceiros prejudicadas (por exemplo, danos a uma função ou processo de negócios);

e) efeitos aos planos e prazos;

f) perda de valor empresarial e financeiro;

g) perda de vantagem empresarial ou participação de mercado;

h) danos à confiança ou reputação pública;

i) violações de requisitos legais, regulatórios ou estatutários;

j) violações de contratos ou níveis de serviço;

k) impacto adverso sobre as partes interessadas;

l) impacto negativo sobre o meio ambiente, poluição.

Os critérios de consequência definem como uma organização categoriza a significância de potenciais eventos de segurança da informação para a organização. É essencial determinar quantas categorias de consequências são utilizadas, como são definidas e quais as consequências associadas a cada categoria. Geralmente, os critérios de consequência são diferentes para diferentes organizações, dependendo do contexto interno e externo da organização.

EXEMPLO 1 O valor máximo que a organização está preparada para abater em um ano fiscal e o valor mínimo no mesmo período que a forçaria à liquidar, pode criar limites superiores e inferiores realistas da escala de consequências de uma organização expressa em termos monetários.

Essa faixa dependente do contexto pode então ser dividida em várias categorias de consequências, das quais convém que o número e a distribuição dependam da percepção de risco e do apetite da organização. As escalas de consequência monetária são comumente expressas em escala logarítmica, como em décadas ou poderes de dez (por exemplo, 100 a 1000; 1 a 10 000 etc.), mas esquemas alternativos de quantização podem ser usados onde se encaixam melhor no contexto da organização.

Como as consequências em diferentes domínios ou departamentos de uma organização podem ser expressas inicialmente de várias maneiras e não estritamente em termos monetários, é útil se essas várias expressões podem ser cruzadas a uma escala de ancoragem comum para assegurar que níveis aproximadamente equivalentes de consequência nos diferentes domínios sejam corretamente comparados entre si. Convém que isso permita que uma agregação de riscos entre os domínios seja realizada.

EXEMPLO 2 A violação de dados pode resultar na perda de confidencialidade, integridade ou disponibilidade de informações no escopo do SGSI, bem como possivelmente impactar a privacidade individual. Isso também pode levar ao descumprimento da legislação de proteção de dados aplicável. As consequências potenciais vão desde a perda de informações, perda de ativos relacionados a informações e ao processo de informações, perda de metas operacionais de negócios e negócios projetados.

#### 6.4.3.3 Critérios de probabilidade

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-a)-2).

Determinar critérios de probabilidade depende de aspectos como:

a) eventos acidentais ou naturais;

b) grau de exposição à ameaça de informações relevantes ou do ativo relacionado às informações;

c) grau em que a vulnerabilidade da organização é explorada;

d) falha tecnológica;

e) atos ou omissões humanas.

A probabilidade pode ser expressa em termos probabilísticos (a chance de um evento ocorrer em um determinado período de tempo) ou em termos frequentes (o número médio de ocorrências notórias em um determinado período de tempo). A probabilidade expressa em termos relacionados à frequência é frequentemente usada quando é comunicada, embora apenas a probabilidade expressa em termos probabilísticos possa ser usada quando a agregação de probabilidades é realizada.

Convém que os critérios de probabilidade cubram a faixa previsível e gerenciável das probabilidades de eventos antecipadas. Além dos limites da gerenciabilidade praticável, normalmente só é necessário reconhecer que um ou outro limite foi excedido para tomar uma decisão adequada de gestão de riscos (designação como um caso extremo). Se as escamas finitas forem muito largas, isso normalmente resulta em quantização excessivamente grosseira e pode levar a erros na avaliação. Este é particularmente o caso em que as probabilidades caem na extremidade alta de escalas exponencialmente representadas, já que os incrementos nas faixas superiores são intrinsecamente muito amplos.

Embora quase tudo seja “possível”, convém que as fontes de risco que recebem atenção primária sejam aquelas com probabilidades mais relevantes para o contexto da organização e o escopo de seu SGSI.

#### 6.4.3.4 Critérios para determinação do nível de risco

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-a)-2).

O objetivo das escalas para o nível de risco é ajudar os proprietários de risco a decidir sobre reter ou tratar riscos e priorizá-los para o tratamento de riscos. Convém que o nível avaliado de um determinado risco ajude a organização a determinar a urgência de lidar com esse risco.

Dependendo da situação, recomenda-se considerar o nível de risco inerente (sem considerar quaisquer controles) ou o nível atual de risco (permitindo a eficácia de quaisquer controles já implementados). Convém que a organização desenvolva um *ranking* de riscos, levando em conta o seguinte:

a) os critérios de consequência e os critérios de probabilidade;

b) as consequências que os eventos de segurança da informação podem ter em níveis estratégicos, táticos e operacionais (isso pode ser definido como pior caso ou em outros termos, desde que a mesma base seja usada de forma consistente);

c) os requisitos legais e regulatórios e obrigações contratuais;

d) os riscos que aparecem além dos limites do escopo da organização, incluindo efeitos imprevistos sobre terceiros.

Critérios para nível de risco são necessários para avaliar os riscos analisados.

Os critérios para nível de risco podem ser qualitativos (por exemplo, muito altos, altos, médios, baixos) ou quantitativos (por exemplo, expressos em termos de valor esperado de perda monetária, perda de vidas ou participação de mercado durante um determinado período de tempo).

EXEMPLOS Os riscos podem ser quantificados como expectativa de perda anual, ou seja, o valor monetário médio da consequência por ano tomada ao longo do próximo ano.

Se forem utilizados critérios quantitativos ou qualitativos, convém que as escalas de avaliação, em última análise, ancorem-se em uma escala de referência que é compreendida por todas as partes interessadas, e convém que tanto a análise de riscos quanto a avaliação de riscos incluam, pelo menos, calibração formal periódica em relação à escala de referência para garantir validade, consistência e comparabilidade dos resultados.

Se uma abordagem qualitativa for usada, convém que os níveis de qualquer escala qualitativa sejam inequívocos, seus incrementos sejam claramente definidos, as descrições qualitativas para cada nível sejam expressas em linguagem objetiva e os níveis não se sobreponham. Quando diferentes escalas são usadas (por exemplo, para lidar com riscos em diferentes domínios de negócios), convém que haja uma equivalência para permitir resultados comparáveis.

## 6.5 Escolha de um método apropriado

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-b).

Em geral, convém que a abordagem e os métodos de gestão de riscos de segurança da informação estejam alinhados com a abordagem e os métodos utilizados para gerenciar os outros riscos da organização.

Convém que a abordagem escolhida seja documentada.

De acordo com a ABNT NBR ISO/IEC 27001:2022, 6.1.2 b), a organização no âmbito do SGSI é necessária para assegurar que avaliações repetidas de risco de segurança da informação produzam resultados consistentes, válidos e comparáveis. Isso significa que convém que o método escolhido assegure as seguintes propriedades dos resultados:

— consistência: convém que avaliações dos mesmos riscos praticados por pessoas diferentes, ou pelas mesmas pessoas em diferentes ocasiões, no mesmo contexto, produzam resultados semelhantes;

— comparabilidade: convém que sejam definidos critérios de avaliação de riscos para assegurar que as avaliações realizadas para diferentes riscos produzam resultados comparáveis quando representam níveis equivalentes de risco;

— validade: convém que as avaliações produzam os resultados conforme o mais próximo possível da realidade.

Os métodos operacionais de gestão de riscos são usados normalmente para a gestão de riscos de segurança da informação. O método escolhido pode utilizar qualquer abordagem adequada em relação ao uso de risco residual. As abordagens mais utilizadas para a gestão de riscos de segurança da informação usam o risco atual ao avaliar a probabilidade e a consequência dos riscos.

# 7 Processo de avaliação de riscos de segurança da informação

## 7.1 Geral

Convém que a organização use o processo de avaliação de riscos organizacionais (se estabelecido) para avaliar riscos às informações ou para definir um processo de avaliação de riscos de segurança da informação.

O processo de avaliação de riscos permite aos proprietários de risco darem prioridade aos riscos alinhados à perspectiva do tratamento, com base principalmente em suas consequências e probabilidades, ou outros critérios estabelecidos.

Convém que o contexto da avaliação de riscos seja determinado, incluindo uma descrição do escopo e do propósito, bem como questões internas e externas que afetam a avaliação de riscos.

A avaliação de riscos consiste nas seguintes atividades:

a) identificação de riscos, que é um processo para encontrar, reconhecer e descrever riscos (mais detalhes sobre a identificação de riscos são fornecidos em 7.2);

b) análise de riscos, que é um processo para compreender os tipos de risco e determinar o nível de risco. A análise de riscos envolve a consideração das causas e fontes de risco, a probabilidade de ocorrer um evento específico, a probabilidade de que este evento tenha consequências e a gravidade dessas consequências (mais detalhes sobre análise de riscos são fornecidos em 7.3);

c) avaliação de riscos, que é um processo para comparar os resultados da análise de riscos com critérios de risco para determinar se o risco e/ou sua significância é aceitável e priorizar os riscos analisados para o tratamento de riscos. Com base nesta comparação, a necessidade de tratamento pode ser considerada (mais detalhes sobre a avaliação de riscos são fornecidos em 7.4).

Convém que o processo de avaliação de riscos seja baseado em métodos (ver 6.5) e ferramentas projetadas em detalhes suficientes para assegurar, diante das possibilidades, resultados consistentes, válidos e reprodutíveis. Além disso, convém que o resultado seja comparável, por exemplo, para determinar se o nível de risco aumentou ou diminuiu.

Convém que a organização assegure que sua abordagem de gestão de riscos de segurança da informação esteja alinhada com a abordagem de gestão de riscos organizacional, de modo que quaisquer riscos de segurança da informação possam ser comparados com outros riscos organizacionais e não apenas considerados isoladamente.

A ABNT NBR ISO/IEC 27001 não obriga uma abordagem específica a ser usada para cumprir os requisitos na ABNT NBR ISO/IEC 27001:2022, 6.1.2. Entretanto, existem duas abordagens principais para avaliação: uma abordagem com base em eventos e uma abordagem baseada em ativos. Elas são discutidas com mais detalhes em 7.2.1.

## 7.2 Identificação de riscos de segurança da informação

### 7.2.1 Identificação e descrição de riscos de segurança da informação

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-c)-1).

Entrada: Eventos que podem influenciar negativamente o alcance dos objetivos de segurança da informação na organização ou em outras organizações.

Ação: Convém que sejam identificados riscos associados à perda de confidencialidade, integridade e disponibilidade de informações.

Gatilho: Proprietários de riscos, partes interessadas e/ou especialistas detectam, ou têm a necessidade de procurar, eventos ou situações novas ou alteradas que possam afetar o alcance dos objetivos de segurança da informação.

Saída: Uma lista de riscos identificados.

Orientação de implementação:

Identificação de riscos é o processo de encontrar, reconhecer e descrever riscos. Isto envolve a identificação de fontes de risco e eventos.

O objetivo da identificação de riscos é gerar uma lista de riscos com base em eventos que possam prevenir, afetar ou retardar o alcance dos objetivos de segurança da informação.

Convém que os riscos identificados sejam aqueles que, caso se materializem, podem ter efeito na realização dos objetivos.

A ABNT NBR ISO/IEC 27001:2022, 6.1.2-c) requer que a organização defina e aplique um processo de avaliação de riscos de segurança da informação que identifique os riscos de segurança da informação. Existem duas abordagens comumente utilizadas para realizar identificação de riscos.

a) Abordagem com base em eventos: identificar cenários estratégicos por meio de uma consideração de fontes de risco e como elas usam ou impactam as partes interessadas para atingir o objetivo desejado por esses riscos.

b) Abordagem com base em ativos: identificar cenários operacionais, detalhados em termos de ativos, ameaças e vulnerabilidades.

Em uma abordagem com base em eventos, o conceito subjacente é que os riscos podem ser identificados e avaliados por meio de uma avaliação de eventos e consequências. Os eventos e as consequências muitas vezes podem ser determinados pela descoberta das preocupações da Alta Direção, dos proprietários de riscos e dos requisitos identificados na determinação do contexto da organização (ABNT NBR ISO/IEC 27001:2022, Seção 4). Entrevistas com a Alta Direção e as pessoas da organização que têm a responsabilidade por um processo de negócios podem auxiliar na identificação dos eventos e consequências relevantes e na identificação dos proprietários de riscos.

Uma abordagem com base em eventos pode estabelecer cenários de alto nível ou estratégicos sem gastar um tempo considerável na identificação de ativos em um nível detalhado. Isto permite que a organização concentre seus esforços de tratamento de riscos nos riscos críticos. A avaliação dos eventos que utilizam essa abordagem pode fazer uso de dados históricos em que os riscos permanecem imutáveis por longos períodos, e permite que os interessados alcancem seus objetivos. Entretanto, no caso de riscos para os quais os dados históricos não estão disponíveis ou não são confiáveis, a assessoria com base no conhecimento e experiência de especialistas ou na investigação de fontes de risco pode auxiliar na avaliação.

Com uma abordagem com base em ativos, o conceito subjacente é que os riscos podem ser identificados e avaliados através de uma inspeção de ativos, ameaças e vulnerabilidades. Um ativo é qualquer coisa que tenha valor para a organização e, portanto, requer proteção. Convém que os ativos sejam identificados, tendo em vista que um sistema de informação consiste em atividades, processos e informações a serem protegidas. Os ativos podem ser identificados como ativos primários

e de suporte de acordo com seu tipo e prioridade, destacando suas dependências, bem como suas interações com suas fontes de risco e as partes interessadas da organização. Uma ameaça explora uma vulnerabilidade de um ativo para comprometer a confidencialidade, integridade e/ou disponibilidade de informações correspondentes. Se todas as combinações válidas de ativos, ameaças e vulnerabilidades puderem ser enumeradas no âmbito do SGSI, então, em teoria, todos os riscos seriam identificados. Para etapas adicionais do processo de avaliação de riscos, convém que seja elaborada uma lista de ativos associados a recursos de informação e processamento de informações.

A abordagem com base em ativos pode identificar ameaças e vulnerabilidades específicas de ativos e permite que a organização determine um tratamento de riscos específico em um nível detalhado.

Mais informações sobre ambas as abordagens são apresentadas no Anexo A.

Em princípio, as duas abordagens diferem apenas em relação ao nível em que a identificação é iniciada. Ambas as abordagens podem descrever o mesmo cenário de risco, por exemplo, quando um ativo de informação está no nível de detalhes e uma exposição ao negócio está no nível geral. Identificar as fontes de risco contributivos usando uma avaliação com base em eventos normalmente requer aprofundamento do nível geral do cenário para o nível de detalhe, mas uma avaliação com base em ativos normalmente pesquisa do ativo para o cenário, a fim de fornecer visibilidade sobre como as consequências se acumulam.

A identificação de riscos é fundamental, pois um risco de segurança da informação que não é identificado nesta fase não está incluído em análises posteriores.

Convém que a identificação de riscos considere riscos independentemente de sua fonte estar sob o controle da organização, mesmo que não haja fontes de risco específicas. Especialmente na avaliação de cenários de risco complexos, convém que seja realizado um processo de avaliação de riscos iterativo. Convém que a primeira rodada se concentre em observações de alto nível e que as rodadas sucessivas considerem níveis adicionais de detalhes, até que as causas básicas dos riscos possam ser identificadas.

Qualquer outra abordagem de identificação de riscos pode ser utilizada, desde que assegure a produção de resultados consistentes, válidos e comparáveis, atendendo ao requisito da ABNT NBR ISO/IEC 27001:2022, 6.1.2-b).

Não convém que a gestão de riscos de segurança da informação seja restringida por visões arbitrárias ou restritivas de como convém que os riscos sejam estruturados, agrupados, agregados, divididos ou descritos. Os riscos podem parecer se sobrepor ou ser subconjuntos ou instâncias específicas de outros riscos. No entanto, convém que os controles para riscos individuais sejam considerados e identificados separadamente de riscos mais amplos ou riscos agregados para fins de tratamento de riscos.

EXEMPLO 1 Um exemplo de dois riscos sobrepostos: (1) há risco de incêndio na sede; (2) há o risco de um incêndio afetar o funcionamento do departamento de contabilidade que está na sede, mas também em vários outros edifícios.

Um exemplo de casos específicos de risco: (1) há um incidente de perda de dados; (2) há um incidente de perda de dados pessoais.

O segundo risco é uma instância específica do primeiro risco, mas é provável que tenha atributos e controles diferentes para o primeiro risco, e pode ser importante gerenciá-lo separadamente do primeiro risco muito mais amplo.

Convém que a agregação de riscos não seja realizada, a menos que sejam pertinentes uns com os outros no nível em que o contexto da organização está sendo considerado. Pode ser necessário considerar separadamente os riscos que são mesclados com o propósito de orçamento global de gestão de riscos, ao planejar opções de tratamento, pois diferentes controles podem ser necessários para gerenciá-los.

EXEMPLO 2 Um *data center* pode estar sujeito a vários perigos independentes: inundações, incêndios, picos de energia elétrica e vandalismo.

Para estimar o nível geral de risco corporativo, os riscos individuais desses eventos podem ser combinados em um nível global de risco, mas como cada um desses eventos requer controles diferentes para gerenciar o risco, convém que sejam considerados e identificados separadamente para fins de tratamento de riscos. Os riscos (combinações de probabilidades e consequências) nem sempre podem ser agregados diretamente.

### 7.2.2 Identificação de proprietários de riscos

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-c)-2).

Entrada: Lista de riscos identificados.

Ação: Convém que os riscos estejam associados aos proprietários de riscos.

Gatilho: A identificação dos proprietários de riscos torna-se necessária quando:

— não foi feito antes;

— houver uma mudança de pessoal na área de negócios pertinente em que os riscos residem;

Saída: Lista de proprietários de risco com riscos associados.

Orientação de implementação:

A Alta Direção, o comitê de segurança, os proprietários de processos, os proprietários funcionais, os gerentes de departamento e os proprietários de ativos podem ser os proprietários de riscos.

Convém que uma organização utilize o processo de avaliação de riscos organizacionais (se estabelecido) no que diz respeito à identificação de proprietários de riscos e, caso contrário, convém estabelecer critérios para identificar proprietários de riscos. Convém que estes critérios levem em consideração que os proprietários de riscos:

— são responsáveis e têm autoridade para gerenciar os riscos que possuem, ou seja, convém que tenham uma posição na organização que lhes permita exercer realmente essa autoridade;

— entendam os problemas em questão e que estão em posição de tomar decisões informadas (por exemplo, sobre como tratar os riscos).

O nível de risco e a qual ativo convém que o risco seja aplicado, podem servir de base para identificar os proprietários de risco.

Convém que a alocação ocorra como parte do processo de avaliação de riscos.

## 7.3 Análise de riscos de segurança da informação

### 7.3.1 Geral

A análise de riscos tem o objetivo de determinar o nível do risco.

A ABNT NBR ISO 31000 é referenciada na ABNT NBR ISO/IEC 27001 como modelo geral. A ABNT NBR ISO/IEC 27001:2022, 6.1.2, requer que, para cada risco identificado, a análise de riscos se fundamente na avaliação das consequências decorrentes do risco e na avaliação da probabilidade do risco, para a determinação de um nível de risco.

Técnicas para análise de riscos com base em consequências e probabilidades podem ser:

a) qualitativa, utilizando uma escala de atributos de qualificação (por exemplo, alto, médio, baixo); ou

b) quantitativa, utilizando uma escala com valores numéricos (por exemplo, custo monetário, frequência ou probabilidade de ocorrência); ou

c) semiquantitativo, utilizando escalas qualitativas com valores atribuídos.

Convém que a análise de riscos seja direcionada a esses riscos e controles que, se gerenciados com sucesso, melhoram a probabilidade de a organização atingir seus objetivos. É fácil gastar um tempo significativo em uma avaliação de riscos, notadamente na avaliação de probabilidades e consequências. Para permitir uma tomada de decisão eficiente sobre a gestão de riscos, pode ser suficiente para usar estimativas iniciais e aproximadas de probabilidade e consequência.

### 7.3.2 Avaliação das possíveis consequências

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-d)-1).

Entrada: Uma lista de cenários de eventos ou riscos relevantes identificados, incluindo a identificação das fontes de risco e processos de negócios, objetivos de negócios e critérios de consequência. Além disso, listas de todos os controles existentes, sua eficácia, implementação e status de uso.

Ação: Convém que as consequências decorrentes da falha em preservar adequadamente a confidencialidade, integridade ou disponibilidade de informações sejam identificadas e avaliadas.

Gatilho: A avaliação das consequências torna-se necessária quando:

— não foi realizada previamente;

— a lista produzida pela “identificação de riscos” é alterada;

— os proprietários de risco ou as partes interessadas das unidades em que desejam que as consequências sejam especificadas, mudaram; ou

— são determinadas mudanças no escopo ou contexto que afetam as consequências.

Saída: Uma lista de potenciais consequências relacionadas a cenários de risco, considerando-se as suas consequências relacionadas a ativos ou eventos, dependendo da abordagem aplicada.

Orientação de implementação:

A não preservação adequada da segurança das informações pode levar à perda de sua confidencialidade, integridade ou disponibilidade. A perda de confidencialidade, integridade ou disponibilidade pode ter consequências adicionais para a organização e seus objetivos. A análise de consequências pode ser realizada após a análise das consequências da segurança da informação, considerando o que pode acontecer se houver perda de confidencialidade, integridade ou disponibilidade das informações em questão. Normalmente, o proprietário de risco pode estimar a consequência se o evento ocorrer. Convém que os seguintes elementos sejam levados em consideração:

— estimativa (ou medida com base na experiência) das perdas (tempo ou dados) devido ao evento como resultado de operações interrompidas ou afetadas;

— estimativa/percepção da gravidade da consequência (por exemplo, expressa em valores financeiros);

— custos de recuperação, dependendo se a recuperação pode ser realizada internamente (pela equipe do proprietário de risco), ou se há a necessidade do envolvimento de uma entidade externa.

### 7.3.3 Avaliação da probabilidade

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-d)-2).

Entrada: Uma lista de cenários de eventos ou riscos relevantes identificados, incluindo a identificação de fontes de risco e processos de negócios, objetivos de negócios e critérios de probabilidade. Além disso, listas de todos os controles existentes, sua eficácia, implementação e *status* de uso.

Ação: Convém que a probabilidade de ocorrência de cenários possíveis ou reais seja avaliada e expressa utilizando critérios de probabilidade estabelecidos.

Gatilho: Além da consequência, avaliar a probabilidade é uma atividade-chave do processo de avaliação de riscos ao se determinar o nível de risco.

A avaliação da probabilidade torna-se necessária quando:

— não foi realizada previamente;

— determinadas alterações no escopo ou no contexto ocorreram e podem afetar a probabilidade;

— vulnerabilidades são descobertas em controles implementados;

— testes/auditorias de eficácia de controle resultam em resultados inesperados;

— mudanças são descobertas no ambiente de ameaças (por exemplo, novos atores/fontes de ameaças).

Saída: Uma lista de eventos ou cenários de risco complementados pelas probabilidades de que estes ocorram.

Orientação de implementação:

Após a identificação dos cenários de risco, é necessário analisar a probabilidade de cada cenário e a consequência de ocorrerem, utilizando técnicas de análise qualitativa ou quantitativa. Avaliar a probabilidade nem sempre é fácil e convém que a avaliação seja expressa de diferentes formas.

Convém que o processo de avaliação leve em conta a frequência com que as fontes de risco ocorrem ou quão facilmente algumas delas (por exemplo, vulnerabilidades) podem ser exploradas, considerando:

— experiência e estatísticas aplicáveis para a probabilidade de fonte de risco;

— para fontes de risco deliberadas: o grau de motivação [por exemplo, a viabilidade (custo/benefício) do ataque] e as capacidades (por exemplo, o nível da habilidade dos possíveis atacantes), que mudam ao longo do tempo, recursos disponíveis para possíveis atacantes e as influências sobre possíveis atacantes, por exemplo, crimes graves, organizações terroristas ou inteligência estrangeira, bem como a percepção de atratividade e vulnerabilidade de informações para um possível atacante;

— para fontes de risco acidentais: fatores geográficos (por exemplo, proximidade a instalações ou atividades perigosas), a possibilidade de desastres naturais como clima extremo, atividade vulcânica, terremotos, inundações, tsunami e fatores que podem influenciar erros humanos e mau funcionamento do equipamento;

— fraquezas conhecidas e quaisquer controles compensadores, tanto individualmente quanto em agregação;

— controles existentes e quão efetivamente reduzem as fraquezas conhecidas.

A estimativa de probabilidade é intrinsecamente incerta, não apenas porque considera coisas que ainda não aconteceram e, portanto, não são totalmente conhecidas, mas também porque a probabilidade é uma medida estatística e não é diretamente representativa de eventos individuais. As três fontes básicas de incerteza de avaliação são:

— incerteza pessoal originada no julgamento do avaliador, que deriva da variabilidade na heurística mental da tomada de decisão;

— incerteza metodológica, que deriva do uso de ferramentas que inevitavelmente modelam eventos de forma simples;

— incerteza sistêmica sobre o evento em si antecipado, que deriva do conhecimento insuficiente (em particular, se a evidência é limitada ou se uma fonte de risco muda com o tempo).

Para aumentar a confiabilidade da estimativa de probabilidade, convém que as organizações considerem o uso de:

a) avaliações de equipe em vez de avaliações individuais;

b) fontes externas, como relatórios de violação de segurança da informação;

c) escalas com alcance e resolução adequadas à abordagem da organização;

d) categorias inequívocas, como “uma vez por ano”, em vez de “pouco frequentes”.

Ao avaliar a probabilidade de eventos, é importante reconhecer a diferença entre eventos independentes e dependentes. A probabilidade de eventos que dependem uns dos outros é condicionada pela relação entre eles (por exemplo, um segundo evento pode ser inevitável se um primeiro evento ocorrer) de modo que a avaliação separada de ambas as suas probabilidades não é necessária. A probabilidade de eventos independentes relevantes são todos contribuintes essenciais para a probabilidade de uma consequência à qual contribuem.

EXEMPLO A probabilidade de um ataque de Negação de Serviço em um servidor depende do cenário de ameaça atual e da vulnerabilidade e acessibilidade do servidor. No entanto, a probabilidade de pacotes

maliciosos pode ser de 100 %, uma vez que o ataque tenha começado e sua avaliação não ajuda na avaliação da probabilidade do ataque de Negação de Serviço.

Para evitar a complexidade desnecessária da avaliação, é importante identificar quaisquer dependências entre os eventos que contribuem para um cenário de risco e, em primeira instância, avaliar as probabilidades daqueles eventos independentes uns dos outros.

A probabilidade geral de consequências comerciais de um evento de segurança da informação normalmente depende da probabilidade de, possivelmente, vários eventos contributivos de nível inferior e suas consequências. Em vez de tentar estimar a probabilidade de consequências dos negócios em uma única avaliação de alto nível, pode ser mais efetivo iniciar agregando as probabilidades dos eventos de nível inferior avaliados individualmente que contribuem para isso.

### 7.3.4 Determinação dos níveis de risco

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-d)-3).

Entrada: Uma lista de cenários de risco com suas consequências relacionadas a ativos ou eventos e sua probabilidade (quantitativa ou qualitativa).

Ação: Convém que o nível de risco seja determinado como uma combinação da probabilidade avaliada e das consequências avaliadas para todos os cenários de risco relevantes.

Gatilho: A determinação dos níveis de risco torna-se necessária para que os riscos de segurança da informação sejam avaliados.

Saída: Uma lista de riscos com valores de nível atribuídos.

Orientação de implementação:

O nível de risco pode ser determinado de diversas formas. É comumente determinado como uma combinação da probabilidade avaliada e das consequências avaliadas para todos os cenários de risco relevantes. Cálculos alternativos podem incluir um valor de ativo, bem como a probabilidade e a consequência. Além disso, o cálculo não é necessariamente linear, por exemplo, pode ser a probabilidade ao quadrado combinada com a consequência. Em qualquer caso, convém que o nível de risco seja determinado utilizando-se os critérios estabelecidos, conforme descrito em 6.4.3.4.

## 7.4 Avaliação de riscos de segurança da informação

### 7.4.1 Comparação dos resultados da análise de riscos com os critérios de risco

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-e)-1).

Entrada: Uma lista de critérios de risco e de riscos com valores de nível atribuídos.

Ação: Convém que o nível de riscos seja comparado com critérios de avaliação de riscos, particularmente critérios de aceitação de riscos.

Gatilho: Comparar os resultados da análise de riscos com os critérios de risco torna-se necessário se os riscos de segurança da informação forem priorizados para o tratamento.

Saída: Uma lista de sugestões de decisões sobre ações adicionais relativas à gestão de riscos.

Orientação de implementação:

Uma vez identificados os riscos e a probabilidade e a gravidade dos valores de consequência atribuídos, convém que as organizações apliquem seus critérios de aceitação de risco, para determinar se os riscos podem ou não ser aceitos. Se eles não podem ser aceitos, então convém que sejam priorizados para o tratamento.

Para avaliar os riscos, convém que as organizações comparem os riscos avaliados com os critérios de risco determinados durante o estabelecimento do contexto.

Convém que as decisões de avaliação de riscos se fundamentem na comparação do risco avaliado com critérios de aceitação definidos, idealmente levando-se em conta o grau de confiança na avaliação. Em alguns casos, como é frequente a ocorrência de eventos de consequência relativamente baixa, pode ser útil considerar seu efeito cumulativo em algum período de tempo de interesse, ao invés de se considerar o risco de cada evento individualmente, pois isso pode fornecer uma representação mais realista dos riscos globais.

Pode haver incertezas na definição do limite entre os riscos que requerem tratamento e os que não requerem. Em certas circunstâncias, adotar um único nível como o nível aceitável de risco que divide riscos que requerem tratamento daqueles que não requerem, nem sempre é apropriado. Em alguns casos, pode ser mais eficaz incluir um elemento de flexibilidade nos critérios, incorporando parâmetros adicionais, como custo e eficácia de possíveis controles.

Os níveis de risco podem ser validados com base no consenso entre proprietários de risco e especialistas empresariais e técnicos. É importante que os proprietários de risco tenham uma boa compreensão dos riscos pelos quais são responsáveis, de acordo com os resultados da avaliação objetiva. Consequentemente, convém que qualquer disparidade entre os níveis de risco avaliados e aqueles percebidos pelos proprietários de risco seja investigada para determinar qual melhor se aproxima da realidade.

### 7.4.2 Priorização dos riscos analisados para o tratamento de riscos

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.2-e)-2).

Entrada: Uma lista dos resultados dos riscos em comparação com os critérios de risco.

Ação: Convém que os riscos da lista sejam priorizados para o tratamento de riscos, considerando os níveis avaliados de riscos.

Gatilho: Priorizar os riscos analisados para o tratamento de riscos torna-se necessário para que os riscos de segurança da informação sejam tratados.

Saída: Uma lista de riscos priorizados com cenários de risco que levam a esses riscos.

Orientação de implementação:

A avaliação de riscos utiliza o entendimento do risco obtido pela análise de riscos para fazer propostas de atuação para se decidir sobre o próximo passo a ser tomado. Convém que estes se refiram a:

— se um tratamento de riscos é necessário;

— prioridades para o tratamento de riscos, considerando níveis de riscos avaliados.

Convém que os critérios de risco utilizados para priorizar riscos considerem os objetivos da organização, os requisitos contratuais, legais e regulatórios e as opiniões das partes interessadas relevantes. A priorização da atividade de avaliação de riscos fundamenta-se principalmente nos critérios de aceitação.

# 8 Processo de tratamento de riscos de segurança da informação

## 8.1 Geral

A entrada do tratamento de riscos de segurança da informação fundamenta-se nos resultados do processo de avaliação de riscos na forma de um conjunto priorizado de riscos a serem tratados, com base em critérios de risco.

A saída desse processo é um conjunto de controles necessários de segurança da informação [ver ABNT NBR ISO/IEC 27001:2022, 6.1.3-b)] que convém que sejam implantados ou aprimorados em relação uns aos outros, de acordo com o plano de tratamento de riscos [ver ABNT NBR ISO/IEC 27001:2022, 6.1.3 -e)]. Implantado dessa forma, a eficácia do plano de tratamento de riscos deve modificar o risco de segurança da informação enfrentado pela organização para que ela atenda aos critérios de aceitação da organização.

## 8.2 Seleção de opções apropriadas de tratamento de riscos de segurança da informação

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.3-a).

Entrada: Uma lista de riscos priorizados com cenários de eventos ou riscos que levem a esses riscos.

Ação: Convém que sejam escolhidas opções de tratamento de riscos.

Gatilho: Selecionar opções adequadas de tratamento de riscos de segurança da informação torna-se necessário se nenhum plano de tratamento de riscos existir ou se o plano estiver incompleto.

Saída: Uma lista de riscos priorizados com as opções de tratamento de riscos selecionadas.

Orientação de implementação:

Várias opções para tratamento de riscos incluem:

— evitar riscos, decidindo não iniciar ou continuar com a atividade que gera risco;

— modificação de risco, alterando a probabilidade da ocorrência de um evento ou uma consequência, ou alterando a gravidade da consequência;

— retenção de risco, por escolha informada;

— compartilhamento de riscos, dividindo responsabilidades com outras partes, interna ou externamente (por exemplo, compartilhando as consequências via seguro);

EXEMPLO 1 Um exemplo de prevenção de risco é um local de escritório situado em uma zona de inundação, onde há o potencial de uma inundação, danos resultantes ao escritório e restrições à disponibilidade e/ou acesso ao escritório. Os controles físicos pertinentes podem ser insuficientes para reduzir esse risco, nesse caso, a opção de tratamento de evitar o risco pode ser a melhor opção disponível. Isso pode envolver o fechamento ou a interrupção da operação daquele escritório.

EXEMPLO 2 Outro exemplo de evitar o risco é optar por não coletar certas informações de indivíduos para que não seja necessário que a organização gerencie, armazene e transmita as informações em seus sistemas de informação.

No caso do compartilhamento de riscos, pelo menos um controle é necessário para modificar a probabilidade ou consequência, mas a organização delega a responsabilidade de implementar o controle à outra parte.

Convém que as opções de tratamento de riscos sejam selecionadas com base no resultado do processo de avaliação de riscos, nos custos esperados para a implementação dessas opções e nos benefícios esperados dessas opções, tanto individualmente quanto no contexto de outros controles. Convém que o tratamento de riscos seja priorizado de acordo com os níveis de risco definidos, restrições de tempo e sequência necessária de implementações e resultados de avaliação de riscos estabelecidos em 7.4. Ao escolher a opção, pode-se considerar como um determinado risco é percebido pelas partes afetadas e as formas mais adequadas de comunicar risco a essas partes.

## 8.3 Determinação dos controles necessários para implementação das opções de tratamento de riscos de segurança da informação

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.3 b).

Entrada: Uma lista de riscos priorizados com as opções de tratamento de riscos selecionadas.

Ação: Determinar todos os controles, desde os conjuntos de controle escolhidos, selecionados a partir de uma fonte adequada, que sejam necessários para tratar os riscos com base nas opções de tratamento de riscos escolhidas, como modificar, reter, evitar ou compartilhar os riscos.

Gatilho: conformidade com o SGSI; gestão de riscos de segurança da informação.

Saída: Todos os controles necessários.

Orientação de implementação:

Convém que seja dada atenção especial para determinar os controles necessários. Convém que cada controle seja verificado para determinar se é necessário, perguntando:

— que efeito esse controle tem sobre a probabilidade ou consequência desse risco;

— de que forma o controle mantém o nível de risco.

Convém que apenas controles que tenham mais do que um efeito insignificante sobre o risco sejam designados como “necessários”. Convém que um ou mais controles sejam aplicados a todos os riscos avaliados como necessitando de tratamento.

Há muitas fontes de controle. Elas podem ser encontradas na ABNT NBR ISO/IEC 27001:2022, Anexo A, em códigos de prática específicos do setor (por exemplo, ABNT NBR ISO/IEC 27017) e outros conjuntos de controle nacional, regional e industrial. Uma organização também pode determinar um ou mais controles “personalizados” (ver ABNT NBR ISO/IEC 27003).

Se um controle personalizado for definido, convém que a redação do controle descreva com exatidão e clareza o que é o controle e como ele opera. Conforme aplicável e apropriado, essa redação pode incluir de forma útil aspectos como:

— se é um controle documentado;

— quem é o dono do controle;

— como é monitorado;

— como isso pode ser evidenciado;

— quaisquer exceções;

— frequência de operação do controle;

— tolerância para o controle;

— se não é óbvio, então, a razão pela qual o controle existe.

Se o controle estiver fora da tolerância, o controle não está operando efetivamente o suficiente para gerenciar o risco identificado.

EXEMPLO 1 “Um processo documentado de gestão de *malware* está em vigor, tendo o gerente de segurança de TI como proprietário. O processo não considera computadores Macs e é monitorado por meio do console do fornecedor por meio de relatórios de desempenho enviados semanalmente ao CIO.”

Tal abordagem detalhada para controlar a redação pode ser útil se os controles personalizados também forem destinados a apoiar a organização em relatórios de qualidade de controles. No entanto, é mais importante que a redação dos controles tenha significado para as pessoas da organização e as ajude a tomar decisões sobre a gestão desses controles e riscos associados.

A determinação dos controles pode incluir novos controles ainda não implementados, ou pode incluir o uso de controles existentes na organização. No entanto, não convém que um controle que já está em operação seja automaticamente incluído no processo de avaliação de riscos porque:

— o controle não é necessário para gerenciar um ou mais riscos de segurança da informação;

— pode ser um controle que, de alguma forma, ajude a gerenciar um ou mais riscos de segurança da informação, mas não é suficientemente eficaz para ser incluído no processo de avaliação de riscos ou gerenciado pelo SGSI, ou;

— pode estar operando atualmente por razões não relacionadas à segurança da informação (por exemplo, qualidade, eficiência, eficácia ou conformidade) ou;

— atualmente está operando, mas do ponto de vista da segurança da informação pode ser removido, pois não tem efeito suficiente para justificar seu *status* contínuo como um controle essencial.

Se um controle for usado para outros fins que não seja apenas a gestão de riscos de segurança da informação, convém tomar cuidado para assegurar que o controle seja gerenciado para alcançar os objetivos de segurança da informação, bem como os objetivos não relacionados à segurança da informação.

EXEMPLO 2 CFTV interno para controlar a qualidade do processo de produção, bem como por razões de segurança da informação (para proteger contra fraudes).

Ao determinar controles de um conjunto de controles existente (por exemplo, ABNT NBR ISO/IEC 27001:2022, Anexo A, ou uma lista de controles específica do setor), convém que a redação do controle corresponda ao necessário para gerenciar o risco e refletir com exatidão o que é ou convém que seja o controle. Se a abordagem geral for usar um conjunto de controles existente (por exemplo,

ABNT NBR ISO/IEC 27001:2022, Anexo A, ou uma lista de controles específica do setor) e o conjunto de controles não tiver um controle que descreva com precisão o controle necessário, então convém considerar a definição de um controle personalizado que descreva o controle com exatidão.

Os controles podem ser classificados como preventivos, detectivos e corretivos:

a) controle preventivo: um controle que visa evitar a ocorrência de um evento de segurança da informação que possa levar à ocorrência de uma ou mais consequências;

b) controle detectivos: um controle que se destina a detectar a ocorrência de um evento de segurança da informação;

c) controle corretivo: um controle que se destina a limitar as consequências de um evento de segurança da informação.

O tipo de controle descreve se um controle age, ou pretende agir, para prevenir ou detectar um evento ou reagir às suas consequências.

EXEMPLO 3 A política de segurança da informação é um controle que mantém o risco, mas o cumprimento da política visa reduzir a probabilidade de ocorrência de risco e, portanto, pode ser categorizado como sendo preventivo.

A utilidade de categorizar controles como preventivos, detectivos e corretivos reside em seu uso, para assegurar que a construção de planos de tratamento de riscos sejam resilientes a falhas nos controles. Desde que haja uma mistura apropriada de controles preventivos, detectivos e corretivos:

— convém que os controles detectivos mitiguem o risco se os controles preventivos falharem;

— convém que os controles corretivos mitiguem o risco se os controles detectivos falharem;

— convém que os controles preventivos reduzam a probabilidade de que os controles corretivos tenham que ser usados.

Ao utilizar controles, convém que as organizações primeiro decidam se é possível detectar a ocorrência de um evento. Se for esse o caso, convém que os controles detectivos sejam implementados. Se não for possível detectar um evento, os controles detectivos podem ser ineficazes, sem nenhuma maneira de dizer se um controle preventivo está funcionando.

EXEMPLO 4 Se não estiver claro se um computador se tornou parte de uma "*botnet*", não é possível saber se os controles que estão sendo usados para evitar que ele se torne parte de uma "*botnet*" funcionam como pretendido.

Os controles detectivos podem funcionar como apropriado, mas ainda podem ser ineficazes.

EXEMPLO 5 A implementação de sistemas de detecção/prevenção de invasões pode ser uma forma eficaz de evitar que o *malware* se propague pela rede, mas eles não são úteis se não houver monitoramento dos sistemas/alertas para a ação, no caso de ocorrer uma propagação que não esteja contida.

Em geral, os controles detectivos são, em última análise, ineficazes em casos em que podem ser ignorados, ou quando sua notificação não resulta em ação apropriada. Convém que os controles corretivos sejam examinados a seguir. Se os controles detectivos falharem, então é provável que haja uma ou mais consequências indesejáveis. A implementação dos controles corretivos pode auxiliar na limitação dessas consequências. Embora os controles corretivos tenham efeito após o início da consequência, muitas vezes é necessário implantá-los bem antes da ocorrência de qualquer evento.

EXEMPLO 6 A criptografia de disco rígido não impede que um *laptop* seja roubado ou que sofra tentativas subsequentes de extrair os dados. No entanto, reduz a gravidade das consequências ligadas a uma divulgação. O controle, é claro, precisa ser implantado antes que o *laptop* seja roubado.

A categorização dos controles não é absoluta e depende do contexto em que o uso de um controle é descrito.

EXEMPLO 7 O *backup* não impede a ocorrência de um evento que de outra forma resultaria em perda de dados (por exemplo, um dano no disco rígido ou perda de um *laptop*), mas ajuda a reduzir a consequência. Algumas organizações podem, portanto, considerar isso como um controle corretivo e não um controle preventivo. Da mesma forma, a criptografia não impede a perda de informações, mas se o evento é descrito como “dados pessoais revelados ao invasor”, então a criptografia é um controle preventivo, e não um controle corretivo.

A ordem em que os controles que abordam os riscos são organizados depende de vários fatores. Muitas técnicas podem ser usadas. É responsabilidade dos respectivos proprietários de risco decidir o equilíbrio entre os custos de investir em controles e assumir consequências, caso os riscos se materializem.

A identificação dos controles existentes pode determinar que esses controles excedem as necessidades atuais. Convém que uma análise de custo-benefício seja realizada antes de remover controles redundantes ou desnecessários (especialmente se os controles possuírem altos custos de manutenção). Uma vez que os controles podem influenciar uns aos outros, remover controles redundantes pode reduzir a segurança geral no local. Não convém que os controles sejam incluídos no tratamento de riscos, a menos que sejam necessários controles para gerenciar um ou mais riscos de segurança da informação identificados. Convém que um controle tenha um efeito sobre a consequência ou probabilidade dos riscos identificados de segurança da informação. Não convém que os controles sejam incluídos no tratamento de riscos se estiverem operando por razões não relacionadas à segurança da informação.

Convém adotar considerações para os controles que são implementados, mas que sejam conhecidos por terem algumas fraquezas. Se a avaliação de todos os riscos que um controle com fraquezas está gerenciando está dentro dos critérios de aceitação, então não é necessário melhorar o controle. Mesmo que o controle não esteja funcionando de forma totalmente eficaz, nem sempre é necessário melhorá-lo para torná-lo totalmente eficaz, portanto, não necessariamente todos os controles precisam operar com total eficácia para que a organização gerencie seus riscos com sucesso. É possível especificar que cada controle individual tem um nível de tolerância para falha abaixo do qual o controle pode ser considerado como não operando efetivamente o suficiente para gerenciar os riscos identificados. Enquanto o controle estiver operando dentro da tolerância, ele não precisa de nenhuma melhoria.

## 8.4 Comparação dos controles determinados com os da ABNT NBR ISO/IEC 27001:2022, Anexo A

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.3-c).

Entrada: Todos os controles necessários (ver 8.3).

Ação: Comparar todos os controles necessários com os listados na ABNT NBR ISO/IEC 27001:2022, Anexo A.

Gatilho: A identificação de quaisquer controles ausentes torna-se necessária se os planos de tratamento de riscos forem formulados.

Saída: Todos os controles aplicáveis ao tratamento de riscos.

Orientação de implementação:

A ABNT NBR ISO/IEC 27001:2022, 6.1.3-c) requer que uma organização compare os controles que determinou como sendo necessários para implementar suas opções de tratamento de riscos escolhidas com os controles listados na ABNT NBR ISO/IEC 27001:2022, Anexo A. O objetivo disso é agir como uma verificação de segurança para verificar se nenhum controle necessário foi omitido da avaliação de riscos. Esta verificação de segurança não está em vigor para identificar quaisquer controles omitidos da ABNT NBR ISO/IEC 27001:2022, Anexo A, na avaliação de riscos. É uma verificação de segurança para identificar quaisquer controles necessários ausentes de qualquer fonte, comparando os controles com outras normas e listas de controles. Os controles omitidos identificados durante esta verificação podem ser controles específicos ou personalizados do setor ou da ABNT NBR ISO/IEC 27001:2022, Anexo A. Convém que as diretrizes para determinar controles em 8.3 sejam seguidas quando considerar-se que algum controle perdido seja adicionado à avaliação de riscos.

EXEMPLO É importante que um controle que já está operando na organização não seja adicionado automaticamente à avaliação de riscos sem maiores considerações.

É importante lembrar que essa comparação dos controles é realizada por meio da avaliação de riscos e não é realizada por meio da Declaração de Aplicabilidade. O princípio é olhar para cada risco por sua vez, e comparar os controles determinados conforme necessário para o risco com os controles na ABNT NBR ISO/IEC 27001:2022, Anexo A, para ajudar a identificar se há algum controle necessário faltante para cada risco.

## 8.5 Produção de uma Declaração de Aplicabilidade

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.3-d).

Entrada: Todos os controles aplicáveis ao tratamento de riscos (ver 8.4).

Ação: Produzir uma Declaração de Aplicabilidade.

Gatilho: Documentação de todos os controles necessários, sua justificativa e *status* de implementação.

Saída: Declaração de Aplicabilidade.

Orientação de implementação:

De acordo com a ABNT NBR ISO/IEC 27001:2022, 6.1.3-d), convém que a Declaração de Aplicabilidade (*Statement of Applicability – SOA*) contenha pelo menos:

a) os controles necessários;

b) a justificativa para sua inclusão;

c) se são implementados ou não;

d) a justificativa para exclusões de controles da ABNT NBR ISO/IEC 27001:2022, Anexo A.

O SOA pode ser facilmente produzido examinando o processo de avaliação de riscos para identificar os controles necessários e o plano de tratamento de riscos para identificar aqueles que estão planejados para serem implementados. Somente controles identificados na avaliação de riscos podem ser incluídos no SOA. Os controles não podem ser adicionados ao SOA independentemente da avaliação de riscos. Convém que haja consistência entre os controles necessários para realizar opções de tratamento de

riscos selecionadas e o SOA. O SOA pode afirmar que a justificativa para a inclusão de um controle é a mesma para todos os controles e que eles foram identificados na avaliação de riscos conforme necessário para tratar um ou mais riscos a um nível aceitável. Não são necessárias mais justificativas para a inclusão de um controle para qualquer um dos controles. O *status* de implementação de todos os controles contidos no SOA pode ser declarado como “implementado”, “parcialmente implementado” ou “não implementado”. Isso pode ser individualmente para cada controle ou para toda a declaração.

EXEMPLO O SOA contém a instrução: “Todos os controles foram implementados”. Nenhuma análise adicional ou informação é necessária para completar o SOA.

## 8.6 Plano de tratamento de riscos de segurança da informação

### 8.6.1 Formulação do plano de tratamento de riscos

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.3-e).

Entrada: Resultados de avaliações de risco.

Ação: Formular plano de tratamento de riscos.

Gatilho: A necessidade da organização para tratar riscos.

Saída: Plano de tratamento de riscos.

Orientação de implementação:

O objetivo desta atividade é criar planos para o tratamento de conjuntos específicos dos riscos que estão na lista de riscos priorizados (ver Seção 7). Um plano de tratamento de riscos é um plano para modificar o risco de tal forma que atenda aos critérios de aceitação de risco da organização (ver 6.4.2). Há duas interpretações possíveis do termo “plano” no contexto do tratamento de riscos. A primeira interpretação é um plano de projeto, ou seja, um plano para implementar os controles necessários da organização. A segunda é um plano de *design*, ou seja, o plano que não apenas identifica os controles necessários, mas também descreve como os controles interagem com seu ambiente e entre si para modificar riscos. Na prática, ambos podem ser usados.

Uma vez que os controles estão em vigor, o plano de projeto deixa de ter qualquer valor que não seja como um registro histórico, enquanto o plano de *design* ainda é útil.

Convém que todo risco que precisa de tratamento seja tratado em um dos planos de tratamento de riscos. Uma organização pode optar por ter vários planos de tratamento de riscos, que juntos implementam todos os aspectos necessários do tratamento de riscos. Estas podem ser organizadas com base em onde as informações residem (por exemplo, um plano para o *data center*, outro para computação móvel etc.), por ativo (por exemplo, planos diferentes para diferentes classificações de ativos) ou por eventos (por exemplo, aqueles usados na avaliação do risco usando o método com base em eventos).

Ao criar o plano de tratamento de riscos, convém que as organizações considerem o seguinte:

— prioridades em relação ao nível de risco e urgência do tratamento;

— se diferentes tipos de controles (preventivos, detectivos, corretivos) ou sua composição são aplicáveis;

— se é necessário esperar que um controle seja estabelecido antes de começar a implementar um novo no mesmo ativo;

— se há um atraso entre o tempo em que o controle é implementado e o momento em que ele é totalmente eficaz e operacional.

Para cada risco tratado, convém que o plano de tratamento inclua as seguintes informações:

— a justificativa para a seleção das opções de tratamento, incluindo os benefícios esperados a serem obtidos;

— aqueles que são responsabilizados e responsáveis pela aprovação e implementação do plano;

— as ações propostas;

— os recursos necessários, incluindo contingências;

— os indicadores de desempenho;

— as restrições;

— os relatórios e monitoramento necessários;

— quando  espera-se que as ações sejam realizadas e concluídas;

— *o status* de implementação.

Convém que as ações do plano de tratamento de riscos sejam classificadas prioritariamente em relação ao nível de risco e urgência do tratamento. Quanto maior o nível de risco e, em alguns casos, a frequência de ocorrência de risco, convém que o controle seja implementado mais cedo.

Para cada risco listado dentro do plano de tratamento de riscos, convém que informações detalhadas de implementação sejam rastreadas, e elas podem incluir, mas não se limitam a:

— nomes de proprietários de risco e responsáveis pela implementação;

— datas ou cronogramas de implementação;

— atividades de controle planejadas para testar o resultado da implementação;

— *status* de implementação;

— nível de custo (investimento, operação).

### 8.6.2 Aprovação pelos proprietários de risco

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.3-f).

Entrada: Plano(s) de tratamento de riscos.

Ação: Aprovação de plano(s) de tratamento de riscos por proprietários de risco.

Gatilho: A necessidade de aprovação de plano(s) de tratamento de riscos.

Saída: Plano(s) de tratamento de riscos aprovado(s).

Orientação de implementação:

Convém que o plano de tratamento de riscos de segurança da informação seja aprovado pelos proprietários de risco assim que for formulado. Convém que os proprietários de risco também decidam sobre a aceitação de riscos residuais de segurança da informação. Convém que essa decisão se fundamente em critérios definidos de aceitação de riscos.

Convém que os resultados do processo avaliação de riscos, o plano de tratamento de riscos e os riscos restantes sejam compreensíveis para os proprietários de risco para que possam quitar suas contas adequadamente.

### 8.6.3 Aceitação dos riscos residuais de segurança da informação

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 6.1.3 f).

Entrada: Plano(s) de tratamento de riscos aprovado(s) e critérios de aceitação de risco.

Ação: Determinar se os riscos residuais são aceitáveis.

Gatilho: A necessidade da organização decidir sobre a retenção de riscos residuais.

Saída: Riscos residuais aceitos.

Orientação de implementação:

Para determinar os riscos residuais, convém que os planos de tratamento de riscos se alimentem do acompanhamento da avaliação da probabilidade e consequência residuais. Convém que os controles propostos descritos nos planos de tratamento de riscos e eficácia relacionada sejam considerados à luz se reduzirão a probabilidade ou a consequência, ou ambos, e se o nível de riscos residuais é alocado aos riscos. O nível de riscos residuais é, então, considerado pelo proprietário de risco para determinar se os riscos residuais são aceitáveis.

Convém que os planos de tratamento de riscos descrevam como os riscos avaliados precisam ser tratados para atender aos critérios de aceitação de riscos.

Em alguns casos, o nível de risco residual nem sempre atende aos critérios de aceitação de riscos, pois os critérios a serem aplicados não levam em conta as circunstâncias vigentes.

EXEMPLO Pode-se argumentar que é necessário reter riscos porque os benefícios que acompanham os riscos são uma importante oportunidade de negócio, ou porque o custo de modificação de risco é muito alto.

No entanto, nem sempre é possível rever os critérios de aceitação de risco em tempo hábil. Nesses casos, os proprietários de risco podem reter riscos que não atendem aos critérios normais de aceitação. Se isso for necessário, convém que o proprietário de risco comente explicitamente sobre os riscos e inclua uma justificativa para a decisão de anular critérios normais de aceitação de risco.

A aceitação de riscos pode envolver um processo para endossar o tratamento antes de uma decisão final de aceitação de risco. É importante que os proprietários de risco analisem criticamente e aprovem planos de tratamento de riscos propostos e riscos residuais resultantes, e registrem quaisquer condições associadas a essa aprovação. Dependendo do processo de avaliação de riscos e dos critérios de aceitação de riscos, isso pode requerer que um gestor com um nível de autoridade mais alto do que o proprietário de risco concorde com a aceitação do risco.

Pode levar algum tempo para implementar um plano para tratar os riscos avaliados. Os critérios de risco podem permitir que os níveis de risco excedam um limiar desejado em uma medida definida se houver um plano em vigor para reduzir esse risco em um tempo aceitável. As decisões de aceitação de riscos podem levar em conta prazos nos planos de tratamento de riscos e se o progresso da implementação do tratamento de riscos está ou não em consonância com o que está planejado.

Alguns riscos podem variar ao longo do tempo (independentemente de essa mudança ser devido à implementação de um plano de tratamento de riscos). Os critérios de aceitação de riscos podem considerar isso e ter limiares de aceitação de risco que dependem do tempo que uma organização pode ser exposta a um risco avaliado.

# 9 Operação

## 9.1 Execução do processo de avaliação de riscos de segurança da informação

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 8.2.

Entrada: Documentos sobre o processo de avaliação de riscos de segurança da informação, incluindo avaliação de riscos e critérios de aceitação de riscos.

Ação: Convém que o processo de avaliação de riscos seja realizado conforme a Seção 7.

Gatilho: A necessidade da organização avaliar riscos, em intervalos planejados ou com base em eventos.

Saída: Riscos avaliados.

Orientação de implementação:

Convém que o processo de avaliação de riscos de segurança da informação definido e aplicado na ABNT NBR ISO/IEC 27001:2022, 6.1, seja integrado às operações organizacionais e que seja realizado em intervalos planejados ou quando mudanças significativas forem propostas ou ocorrerem. Convém que o processo de avaliação de riscos de segurança da informação leve em conta os critérios estabelecidos na ABNT NBR ISO/IEC 27001:2022, 6.1.2 a). Convém que os intervalos em que a avaliação de riscos é realizada sejam adequados ao SGSI. Quando ocorrer uma mudança significativa do SGSI (ou seu contexto), ou uma mudança no cenário de ameaças (por exemplo, um novo tipo de ataque de segurança da informação), convém que a organização determine se essa alteração requer uma avaliação adicional do risco de segurança da informação.

Ao fazer planos para avaliações rotineiras de risco, convém que as organizações levem em conta qualquer calendário que se aplique aos seus processos gerais de negócios e aos ciclos orçamentários associados.

EXEMPLO Se houver um ciclo orçamentário anual, a organização pode ser obrigada a enviar solicitações de financiamento em uma determinada época do ano. Os fundos são então concedidos (diminuídos ou negados) posteriormente.

Se os processos de aquisição estiverem envolvidos, pode haver outro ciclo orçamentário antes que as recomendações de tratamento de riscos possam ser implementadas e sua eficácia avaliada antes do próximo processo de avaliação de riscos de rotina. Nesses casos, convém que os processos de avaliação de riscos sejam agendados:

a) para fazer suas recomendações de tratamento de riscos a tempo de aplicação de financiamento;

b) para ser reavaliado após os resultados das dotações orçamentárias;

c) para realizar a avaliação de rotina, uma vez implementadas as recomendações, após qualquer atividade de aquisição.

### 9.2 Realização do processo de tratamento de riscos de segurança da informação

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 8.3.

Entrada: Risco(s) avaliado(s).

Ação: Convém que o processo de tratamento de riscos seja realizado conforme a Seção 8.

Gatilho: A necessidade da organização de tratar riscos, em intervalos planejados ou com base em eventos.

Saída: Riscos residuais retidos ou aceitos.

Orientação de implementação:

A ABNT NBR ISO/IEC 27001:2022, 8.3, estabelece requisitos para que as organizações implementem seus planos de tratamento de riscos. Considerações incluídas em 8.6 também são pertinentes para esta Subseção.

## 10 Aproveitamento dos processos relacionados ao SGSI

### 10.1 Contexto da organização

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, Seção 4.

Entrada: Informações sobre a organização, seu contexto interno e externo.

Ação: Convém que todos os dados relevantes sejam considerados para identificar e descrever questões internas e externas que influenciam a gestão de riscos de segurança da informação e os requisitos das partes interessadas.

Gatilho: A ABNT NBR ISO/IEC 27001:2022 estabelece requisitos para que essas informações sejam capazes de estabelecer objetivos de segurança da informação.

Saída: Questões internas e externas relacionadas a riscos que influenciam a gestão de riscos de segurança da informação.

Orientação de implementação:

Convém que a organização tenha uma compreensão de alto nível (por exemplo, estratégica) das questões importantes que podem afetar o SGSI, positiva ou negativamente. Convém conhecer ainda o contexto interno e externo que é pertinente para o seu propósito e que afete sua capacidade de alcançar o resultado pretendido do seu SGSI. Convém que os resultados pretendidos assegurem a preservação da confidencialidade, integridade e disponibilidade das informações, aplicando o processo de gestão de riscos e sabendo quais riscos são adequadamente gerenciados.

Para identificar de forma confiável os riscos, convém que a organização entenda com detalhes suficientes as circunstâncias em que atua. Isto significa que convém que a organização reúna

informações sobre seus contextos interno e externo, suas partes interessadas e requisitos delas (ver ABNT NBR ISO/IEC 27001:2022, 4.1 e 4.2). Convém que a coleta dessas informações seja feita antes de qualquer tentativa da organização de avaliar seus riscos de segurança da informação, ou mesmo quaisquer outros riscos que possam afetar o resultado pretendido do SGSI (ver ABNT NBR ISO/IEC 27001:2022, 6.1.1).

Convém que a organização considere todas as fontes de risco internas e externas. O entendimento da organização sobre as partes interessadas que se opõem à organização e seus interesses é altamente relevante.

EXEMPLO 1 Um exemplo de uma parte interessada com interesses que se opõem aos objetivos da organização é o atacante. O atacante deseja uma organização com baixo nível de segurança. A organização leva em conta o interesse desta parte por ter o oposto (forte nível de segurança), ou seja, a organização considera possíveis conflitos com os objetivos do SGSI. A organização assegura, por meio de controles eficazes de segurança da informação, que esses interesses não sejam atendidos.

Convém que interfaces com serviços ou atividades que não estejam completamente dentro do escopo do SGSI sejam consideradas no processo de avaliação de riscos de segurança da informação da organização.

EXEMPLO 2 Um exemplo dessa situação é o compartilhamento de ativos (por exemplo, instalações, sistemas de TI e bancos de dados) com outras organizações ou a terceirização de uma função de negócio.

A forma como outros fatores relevantes que influenciam a segurança da informação são considerados, depende da escolha da organização quanto aos métodos de identificação e análise de riscos.

Os objetivos de segurança da informação da organização (ver ABNT NBR ISO/IEC 27001:2022, 6.2) podem restringir os critérios de aceitação de risco (por exemplo, o nível aceitável de risco pode ser uma função das recompensas potenciais associadas a diferentes atividades comerciais). Além disso, a política de segurança da informação pode restringir o tratamento de riscos (por exemplo, certas opções de tratamento de riscos podem ser excluídas por essa política).

## 10.2 Liderança e comprometimento

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 5.1.

Entrada: Informações sobre resultados de avaliação de riscos de segurança da informação ou resultados de tratamento de riscos de segurança da informação que requerem aprovação ou endosso.

Ação: Convém que o nível adequado de gestão considere os resultados relacionados aos riscos de segurança da informação, decidir ou endossar outras ações.

Gatilho: A ABNT NBR ISO/IEC 27001 requer que um nível adequado de gestão esteja envolvido em todas as atividades relacionadas ao risco de segurança da informação.

Saída: Decisões relacionadas ao risco de segurança da informação ou endosso.

Orientação de implementação:

A Alta Direção é responsável por gerenciar riscos e convém que lidere e conduza processos de avaliação de riscos, incluindo:

— assegurar que os recursos necessários sejam alocados para gerenciar riscos;

— atribuir autoridade, responsabilidade e responsabilização em níveis adequados dentro da organização no que se refere à gestão de riscos;

— comunicar-se com as partes interessadas apropriadas.

## 10.3 Comunicação e consulta

NOTA 1 Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 7.4.

NOTA 2 A ABNT NBR ISO/IEC 27001 refere-se diretamente à parte de comunicação desta atividade.

Entrada: Informações sobre riscos, suas causas, consequências e sua probabilidade identificada por meio dos processos de gestão de riscos.

Ação: Convém que informações sobre riscos, suas causas, consequências, sua probabilidade e os controles que estão sendo tomados para tratá-los sejam comunicados ou obtidos das partes interessadas externas e internas.

Gatilho: A ABNT NBR ISO/IEC 27001 requer tal comunicação.

Saída: Percepções e resultados relevantes das partes interessadas sobre o processo e resultados de gestão de riscos de segurança da informação da organização.

Orientação de implementação:

A atividade de comunicação e consulta visa chegar a um acordo sobre como gerenciar riscos, trocando e/ou compartilhando informações sobre riscos com os proprietários de riscos e outras partes interessadas relevantes. As informações incluem, mas não se limitam à existência, natureza, forma, probabilidade, consequência, significância, tratamento e aceitação de riscos.

A ABNT NBR ISO/IEC 27001:2022, 6.1.2-c)-2), requer que os proprietários de riscos de segurança da informação sejam identificados. A propriedade do risco pode ser deliberadamente confusa ou ocultada. Mesmo quando os proprietários de riscos podem ser identificados, eles podem ser relutantes em reconhecer que são responsáveis pelos riscos que possuem, e obter sua participação no processo de gestão de riscos pode ser difícil. Convém que haja um procedimento de comunicação definido para informar os interessados sobre a propriedade de riscos.

A ABNT NBR ISO/IEC 27001:2022, 6.1.3-f), requer que os proprietários de risco aprovem o(s) plano(s) de tratamento de riscos e decidam sobre a aceitação de riscos residuais. A comunicação entre proprietários de riscos e funcionários responsáveis pela implantação do SGSI é uma atividade importante. Convém que haja um acordo sobre como gerenciar riscos trocando e/ou compartilhando informações sobre riscos com os proprietários de riscos e, talvez, outras partes interessadas e tomadores de decisão. As informações incluem, mas não se limitam à existência, natureza, forma, probabilidade, significância, tratamento e aceitação de riscos. Convém que a comunicação seja bidirecional.

Dependendo da natureza e sensibilidade do(s) risco(s), pode haver a necessidade de limitar algumas informações sobre risco(s), sua avaliação e tratamento com base na necessidade de conhecimento para os responsáveis por identificá-los, avaliá-los e tratá-los. Convém que a comunicação de risco seja controlada de forma "*need to know*", levando em conta o nível de detalhe requerido por diferentes partes interessadas, em consulta com os proprietários de risco ou potenciais proprietários, com o objetivo de evitar a divulgação dos riscos mais sensíveis e suas fraquezas conhecidas associadas.

As percepções de risco podem variar devido a diferenças de suposições, conceitos, necessidades, questões e preocupações das partes interessadas adequadas no que se refere ao risco ou às questões em discussão. As partes interessadas provavelmente farão julgamentos sobre a aceitação do risco, com base em sua percepção de risco. Isso é particularmente importante para assegurar que a percepção de risco das partes interessadas, bem como suas percepções sobre benefícios, possam ser identificadas e documentadas, e as razões subjacentes claramente compreendidas e abordadas.

A comunicação e a consulta sobre os riscos podem resultar em um melhor engajamento das partes interessadas com o que está sendo feito e nas partes interessadas adequadas apropriando-se de decisões e resultados. A comunicação e consulta com as partes interessadas, à medida que os critérios são desenvolvidos e à medida que os métodos de avaliação de riscos são selecionados, também podem melhorar a propriedade dos resultados pelas partes interessadas. As partes interessadas são menos propensas a questionar os resultados dos processos que ajudaram a projetar. Como resultado, a probabilidade de aceitarem descobertas e apoiar planos de ação é frequentemente aumentada. Nos casos em que as partes interessadas são gestores, isso cria comprometimento para atingir os objetivos da gestão de riscos e fornecer os recursos necessários.

Convém que a comunicação de risco seja realizada para efeito de:

— assegurar o resultado da gestão de riscos da organização;

— coletar informações de risco;

— compartilhar os resultados do processo de avaliação de riscos e apresentar o plano de tratamento de riscos;

— evitar ou reduzir tanto a ocorrência quanto a consequência de violações da segurança da informação devido à falta de entendimento mútuo entre proprietários de risco e partes interessadas;

— apoiar proprietários de risco;

— obter novos conhecimentos de segurança da informação;

— coordenar com outras partes e planejar respostas para reduzir as consequências de qualquer incidente;

— dar um senso de responsabilidade aos proprietários de risco e outras partes interessadas em risco;

— melhorar a conscientização.

Convém que uma organização desenvolva planos de comunicação de risco para operações normais, bem como para emergências. Convém que a atividade de comunicação e consulta de risco seja realizada continuamente.

A coordenação entre os principais proprietários de riscos e as partes interessadas relevantes pode ser alcançada pela formação de um comitê no qual o debate sobre riscos, sua priorização e tratamento adequado e aceitação podem ocorrer.

As comunicações de risco podem ser encaminhadas voluntariamente a terceiros externos para permitir uma melhor coordenação ou conscientização de gestão de riscos ou resposta e também podem ser exigidas por reguladores ou parceiros de negócios em determinadas circunstâncias.

É importante cooperar com as relações públicas ou a unidade de comunicação adequada dentro da organização para coordenar todas as tarefas relacionadas à comunicação de risco. Isso é crucial no caso de ativação da comunicação de crise, por exemplo, em resposta a incidentes específicos.

## 10.4 Informações documentadas

### 10.4.1 Geral

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 7.5.

A ABNT NBR ISO/IEC 27001 estabelece os requisitos para que as organizações retenham informações documentadas sobre o processo de avaliação de riscos (ver a ABNT NBR ISO/IEC 27001:2022, 6.1.2) e resultados (ver a ABNT NBR ISO/IEC 27001:2022, 8.2); o processo de tratamento de riscos (ABNT NBR ISO/IEC 27001:2022, 6.1.3) e resultados (ABNT NBR ISO/IEC 27001:2022, 8.3).

### 10.4.2 Informações documentadas sobre processos

Entrada: Conhecimento sobre os processos de avaliação e tratamento de riscos de segurança da informação conforme as Seções 7 e 8, definidos pela organização.

Ação: Convém que informações sobre os processos de avaliação e tratamento de riscos de segurança da informação sejam documentadas e retidas.

Gatilho: A ABNT NBR ISO/IEC 27001 requer informações documentadas sobre os processos de avaliação e tratamento de riscos de segurança da informação.

Saída: Informações documentadas requeridas pelas partes interessadas (por exemplo, órgão de certificação) ou determinadas pela organização como necessárias para a eficácia do processo de avaliação de riscos de segurança da informação ou processo de tratamento de riscos de segurança da informação.

Orientação de implementação:

Convém que informações documentadas sobre o processo de avaliação de riscos de segurança da informação contenham:

a) uma definição dos critérios de risco (incluindo os critérios de aceitação de riscos e os critérios para a realização de avaliações de risco de segurança da informação);

b) fundamentação da consistência, validade e comparabilidade dos resultados;

c) uma descrição do método de identificação de riscos (incluindo a identificação de proprietários de risco);

d) uma descrição do método de análise dos riscos à segurança da informação (incluindo a avaliação de potenciais consequências, probabilidade realista e nível de risco resultante);

e) uma descrição do método para comparar os resultados com os critérios de risco e a priorização de riscos para o tratamento de riscos.

Convém que as informações documentadas sobre o processo de tratamento de riscos de segurança da informação contenham descrições de:

— método para selecionar opções adequadas de tratamento de riscos de segurança da informação;

— método para determinar os controles necessários;

— como a ABNT NBR ISO/IEC 27001:2022, Anexo A, é usada para determinar que os controles necessários não foram inadvertidamente negligenciados;

— como os planos de tratamento de riscos são produzidos;

— como a aprovação dos proprietários de risco é obtida.

### 10.4.3 Informações documentadas sobre resultados

Entrada: A avaliação de riscos de segurança da informação e os resultados do tratamento.

Ação: Convém que informações sobre a avaliação de riscos de segurança da informação e os resultados do tratamento sejam documentadas e retidas.

Gatilho: A ABNT NBR ISO/IEC 27001 requer informações documentadas sobre o processo de avaliação de riscos de segurança da informação e os resultados do tratamento.

Saída: Informações documentadas sobre a avaliação de riscos de segurança da informação e os resultados do tratamento.

Orientação de implementação:

Como as organizações são requeridas a realizar processos de avaliação de riscos em intervalos planejados, ou quando mudanças significativas são propostas ou ocorrem, convém que haja pelo menos evidências de um cronograma, e que os processos de avaliação de riscos sejam realizados de acordo com esse cronograma. Se uma mudança for proposta ou tiver ocorrido, então convém que haja evidências da execução de um processo de avaliação de riscos associado. Caso contrário, convém que a organização explique por que a mudança é significativa ou não.

Convém que as informações documentadas sobre os resultados de processos de avaliação de riscos de segurança da informação contenham:

a) os riscos identificados, suas consequências e probabilidades;

b) a identidade do proprietário de risco(s);

c) os resultados da aplicação dos critérios de aceitação de riscos;

d) a prioridade para o tratamento de riscos.

O registro da justificativa das decisões de risco também é recomendado, a fim de aprender com o erro em casos individuais e facilitar a melhoria contínua.

Convém que as informações documentadas sobre os resultados do tratamento de riscos de segurança da informação contenham:

— identificação dos controles necessários;

— quando apropriado e disponível, evidências de que esses controles necessários atuam para modificar riscos, de modo a atender aos critérios de aceitação de riscos da organização.

## 10.5 Monitoramento e análise crítica

### 10.5.1 Geral

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 9.1.

Convém que o processo de monitoramento da organização (ver a ABNT NBR ISO/IEC 27001:2022, 9.1) abranja todos os aspectos dos processos de avaliação de riscos e tratamento de riscos para efeito de:

a) garantia de que os tratamentos de risco sejam eficazes, eficientes e econômicos tanto no projeto quanto na operação;

b) obtenção de informações para melhorar avaliações futuras de risco;

c) análise e aprendizado das lições de incidentes (incluindo erros próximos), mudanças, tendências, sucessos e fracassos;

d) detecção de alterações no contexto interno e externo, incluindo alterações nos critérios de risco e os próprios riscos, que podem requerer análise crítica de tratamentos e prioridades de risco;

e) identificação de riscos emergentes.

Cenários de risco retidos, provenientes das atividades de gestão de riscos, podem ser transpostos em cenários de monitoramento, a fim de assegurar um processo de monitoramento eficaz. Mais detalhes sobre os cenários de monitoramento são apresentados em A.2.7.

### 10.5.2 Monitoramento e análise crítica de fatores que influenciam os riscos

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 9.1.

Entrada: Todas as informações de risco obtidas das atividades de gestão de riscos.

Ação: Convém que os riscos e seus fatores (ou seja, valor dos ativos, consequências, ameaças, vulnerabilidades, probabilidade de ocorrência) sejam monitorados e analisados criticamente para identificar quaisquer alterações no contexto da organização em um estágio inicial, e manter uma visão geral do quadro completo de risco.

Gatilho: Análise crítica da política organizacional e qualquer detecção de alterações no ambiente operacional ou de ameaça atual.

Saída: Alinhamento contínuo da gestão de riscos com os objetivos de negócios da organização e com critérios de aceitação de riscos.

Orientação de implementação:

A ABNT NBR ISO/IEC 27001:2022, 9.1, requer que as organizações avaliem seu desempenho de segurança da informação e eficácia do SGSI. De acordo com esse requisito, convém que as organizações utilizem seu(s) plano(s) de tratamento de riscos como assunto para suas avaliações de desempenho. Para isso, convém que uma organização primeiro determine uma ou mais necessidades de informação, por exemplo, para descrever o que a Alta Direção deseja saber sobre a capacidade da organização de se defender contra ameaças. Usando isso como uma especificação de alto nível, convém que uma organização então determine as medições que precisa realizar e como tais medidas sejam combinadas para satisfazer a necessidade de informações.

Riscos não são estáticos. Cenários de eventos, valores de ativos, ameaças, vulnerabilidades, probabilidades e consequências podem mudar abruptamente sem qualquer indicação. Convém que o monitoramento constante seja realizado para detectar essas alterações. Isso pode ser suportado por serviços externos que fornecem informações sobre novas ameaças ou vulnerabilidades. Convém que as organizações assegurem o monitoramento contínuo de fatores relevantes como:

a) novas fontes de risco, incluindo vulnerabilidades recentemente relatadas na TI;

b) novos ativos que foram incluídos no escopo de gestão de riscos;

c) modificação necessária dos valores dos ativos (por exemplo, devido às alterações nos requisitos de negócios);

d) vulnerabilidades identificadas para determinar aquelas que estão expostas a ameaças novas ou ressurgindo;

e) mudanças nos padrões de uso de tecnologias existentes ou novas que possam abrir novas oportunidades possíveis de ataque;

f) mudanças nas leis e regulamentos;

g) mudanças no apetite pelo risco e percepções do que agora é aceitável e do que não é mais aceitável;

h) incidentes de segurança da informação, dentro e fora da organização.

Novas fontes de risco ou mudanças de probabilidade ou consequências podem aumentar os riscos previamente avaliados. Convém que a análise crítica dos riscos baixos e retidos examinem cada risco separadamente, e todos esses riscos como um agregado também, para avaliar sua potencial consequência acumulada. Se os riscos não se enquadrarem mais na categoria de risco baixo ou aceitável, convém que sejam tratados usando uma ou mais das opções em 8.2.

Fatores que afetam a probabilidade da ocorrência de eventos e suas consequências correspondentes podem mudar, assim como fatores que afetam a adequação ou custo das diversas opções de tratamento. Convém que grandes mudanças que afetam a organização sejam uma razão para uma análise crítica mais específica. Convém que as atividades de monitoramento de risco sejam repetidas regularmente e as opções selecionadas para tratamento de riscos sejam analisadas criticamente de forma periódica.

Novas ameaças, vulnerabilidades ou mudanças de probabilidade ou consequências podem aumentar os riscos previamente avaliados como baixos. Convém que a análise crítica dos riscos baixos e retidos considere cada risco separadamente, e todos esses riscos como um agregado também, para avaliar sua potencial consequência acumulada. Se os riscos não se enquadrarem na categoria de risco baixo ou aceitável, convém que sejam tratados utilizando uma ou mais das opções consideradas na Seção 8.

Fatores que afetam a probabilidade da ocorrência de ameaças e suas consequências correspondentes podem mudar, assim como fatores que afetam a adequação ou o custo das diversas opções de tratamento. Convém que as principais mudanças que afetam a organização sejam motivos para uma análise crítica mais específica. Convém que as atividades de monitoramento de risco sejam repetidas regularmente e as opções selecionadas para tratamento de riscos sejam analisadas criticamente de forma periódica.

A saída das atividades de monitoramento de riscos pode ser entrada para outras atividades de análise crítica de risco. Convém que a organização analise criticamente todos os riscos de forma regular e quando grandes alterações forem propostas ou ocorrerem de acordo com a ABNT NBR ISO/IEC 27001:2022, Seção 8.

## 10.6 Análise crítica da direção

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 9.3.

Entrada: Resultados do(s) processo(s) de avaliação de risco de segurança da informação, *status* do plano de tratamento de riscos de segurança da informação.

Ação: Convém que os resultados do processo de avaliação de riscos de segurança da informação e o *status* do plano de tratamento de riscos de segurança da informação sejam analisados criticamente para confirmar que os riscos residuais atendem aos critérios de aceitação de riscos e que o plano de tratamento de riscos aborda todos os riscos relevantes e suas opções de tratamento de riscos.

Gatilho: Uma parte do calendário programado de atividades de análise crítica.

Saída: Alterações dos critérios de aceitação de riscos e dos critérios para a realização de avaliações de risco de segurança da informação, plano de tratamento de riscos de segurança da informação atualizado ou SOA.

## 10.7 Ação corretiva

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 10.1.

Entrada: O plano de tratamento de riscos está se mostrando ineficaz, o que significa que o risco residual permanecerá em níveis inaceitáveis após a conclusão do plano de tratamento.

Ação: Revisar o plano de tratamento de riscos e implementá-lo para modificar o risco residual a um nível aceitável.

Gatilho: A decisão de revisar o plano de tratamento de riscos.

Saída: Um plano de tratamento de riscos analisado criticamente e sua implementação.

Orientação de implementação:

As inconformidades relacionadas à eficácia do plano de tratamento de riscos podem ser levantadas por meio de uma auditoria interna ou externa, ou por meio de monitoramento e indicadores. Convém que o plano de tratamento seja analisado criticamente para refletir:

— os resultados do processo de tratamento de riscos de segurança da informação;

— a implementação progressiva do plano (por exemplo, um controle é implementado conforme especificado, conforme projetado, conforme construído);

— as dificuldades identificadas na implementação de controles (por exemplo, questões técnicas ou financeiras, inconsistências com fatores internos ou externos, como considerações de privacidade).

Há também casos em que, mesmo que os riscos residuais sejam aceitáveis após a conclusão do plano de tratamento, os usuários rejeitarão seu uso ou tentarão contornar porque esses controles

não são aceitos pelos usuários em termos de facilidade de uso (por exemplo, não ergonômico, muito complicado ou muito longo).

Convém que a organização analise criticamente a eficácia do plano de tratamento revisado.

## 10.8 Melhoria contínua

NOTA Esta subseção refere-se à ABNT NBR ISO/IEC 27001:2022, 10.2

Entrada: Todas as informações de risco obtidas das atividades de gestão de riscos.

Ação: Convém que o processo de gestão de riscos de segurança da informação seja continuamente monitorado, analisado criticamente e aprimorado conforme necessário.

Gatilho: Organização busca melhorar e amadurecer a partir das lições aprendidas durante o processo de gestão de riscos de segurança da informação.

Saída: Relevância contínua do processo de gestão de riscos de segurança da informação para os objetivos de negócios da organização ou atualização do processo.

Orientação de implementação:

O monitoramento e a análise crítica contínua de que o contexto, o resultado da avaliação de riscos e o tratamento de riscos, bem como os planos de gestão, permanecem relevantes e adequados às circunstâncias é necessário para assegurar que o processo de gestão de riscos de segurança da informação esteja correto.

Convém que a organização assegure que o processo de gestão de riscos de segurança da informação e as atividades relacionadas, permaneçam apropriadas nas circunstâncias atuais e sejam seguidas. Convém que quaisquer melhorias acordadas no processo, ou ações necessárias para melhorar o cumprimento do processo, sejam notificadas aos gestores responsáveis. Convém que esses gestores tenham a garantia de que nenhum elemento de risco ou risco é negligenciado ou subestimado, que as ações necessárias são tomadas, e que as decisões são tomadas para fornecer uma compreensão realista do risco e a capacidade de resposta.

Convém notar que o processo de gestão de mudanças precisará fornecer *feedback* continuamente ao processo de gestão de riscos, a fim de assegurar que as variações nos sistemas de informação capazes de modificar riscos sejam prontamente levadas em conta, mesmo modificando as atividades de avaliação de riscos para avaliá-los adequadamente.

Além disso, convém que a organização verifique regularmente os critérios utilizados para medir o risco. Convém que essa verificação assegure que todos os elementos ainda sejam válidos e consistentes com objetivos, estratégias e políticas de negócios, e que as mudanças no contexto dos negócios sejam levadas em consideração adequadamente durante o processo de gestão de riscos de segurança da informação. Convém que esta atividade de monitoramento e análise crítica aborde, mas não se limite a:

— contexto legal e ambiental;

— contexto de competição;

— abordagem do processo de avaliação de riscos;

— valor e categorias dos ativos;

— critérios de consequência;

— critérios de probabilidade;

— critérios de avaliação de riscos;

— critérios de aceitação de riscos;

— custo total de propriedade;

— recursos necessários.

Convém que a organização assegure que os recursos do processo de avaliação de riscos e tratamento de riscos estejam continuamente disponíveis para analisar criticamente riscos, abordar ameaças ou vulnerabilidades novas ou alteradas e aconselhar a direção de acordo.

O monitoramento da gestão de riscos pode resultar em modificar ou adicionar à abordagem, metodologia ou ferramentas utilizadas dependendo de:

— a maturidade de risco da organização;

— as alterações identificadas;

— a iteração de avaliação de riscos;

— o objetivo do processo de gestão de riscos de segurança da informação (por exemplo, continuidade de negócios, resiliência a incidentes, conformidade);

— o objeto do processo de gestão de riscos de segurança da informação (por exemplo, organização, unidade de negócios, processo de informação, sua implementação técnica, aplicação, conexão com a *internet*).

Os ciclos de gestão de riscos relacionados ao escopo do processo de avaliação de riscos e tratamento de riscos são apresentados em 5.2.

# Anexo A
(informativo)

# Exemplos de técnicas de apoio ao processo de avaliação de riscos

## A.1 Critérios de risco de segurança da informação

### A.1.1 Critérios relacionados ao processo de avaliação de riscos

#### A.1.1.1 Considerações gerais do processo de avaliação de riscos

Em geral, a incerteza pessoal domina o processo de avaliação de riscos de informação, e diversos analistas apresentam tendências diferentes ao interpretar pontos sobre escalas de probabilidade e consequências. Convém que as escalas de referência relacionem as categorias de consequência, probabilidade e risco a valores objetivos comuns inequivocamente especificados, possivelmente expressos em termos como perda financeira em unidades monetárias, e frequência nocional de ocorrência em período finito específico para a abordagem quantitativa.

Particularmente quando a abordagem qualitativa é adotada, convém que os analistas de riscos passem, periodicamente, por treinamentos e práticas, contra uma escala de referência de ancoragem, a fim de manter a calibração de seu julgamento.

#### A.1.1.2 Abordagem qualitativa

##### A.1.1.2.1 Escala de consequências

A Tabela A.1 apresenta um exemplo de escala de consequência.

**Tabela A.1 – Exemplo de escala de consequência** (continua)

| Consequências | Descrição |
|---|---|
| **5 – Catastrófica** | **Consequências setoriais ou regulatórias além da organização**<br>Os ecossistemas setoriais impactaram substancialmente, com consequências que podem ser duradouras.<br>E/ou: dificuldade para o Estado, e até mesmo uma incapacidade, para assegurar uma função regulatória ou uma de suas missões de vital importância.<br>E/ou: consequências críticas na segurança das pessoas e da propriedade (crise sanitária, poluição ambiental significativa, destruição de infraestruturas essenciais etc.). |

**Tabela A.1** (conclusão)

| Consequências | Descrição |
|---|---|
| **4 – Crítica** | **Consequências desastrosas para a organização**<br>Incapacidade para a organização de assegurar toda ou uma parte de sua atividade, com possíveis sérias consequências na segurança das pessoas e dos bens. A organização provavelmente não superará a situação (sua sobrevivência está ameaçada), os setores de atividade ou setores estatais em que opera provavelmente serão afetados ligeiramente, sem consequências duradouras. |
| **3 – Séria** | **Consequências substanciais para a organização**<br>Alta degradação no desempenho da atividade, com possíveis consequências significativas na segurança das pessoas e do patrimônio. A organização vai superar a situação com sérias dificuldades (operação em um modo altamente degradado), sem qualquer impacto do setor ou do Estado. |
| **2 – Significativa** | **Consequências significativas, porém, limitadas para a organização**<br>Degradação no desempenho da atividade sem consequências na segurança das pessoas e do patrimônio. A organização vai superar a situação apesar de algumas dificuldades (operação no modo degradado). |
| **1 – Menor** | **Consequências insignificantes para a organização**<br>Não há consequências nas operações ou no desempenho da atividade ou na segurança das pessoas e dos bens. A organização vai superar a situação sem muita dificuldade (as margens serão consumidas). |

#### A.1.1.2.2 Escala de probabilidade

A Tabela A.2 e a Tabela A.4 apresentam exemplos de formas alternativas para representar escalas de probabilidade. A probabilidade pode ser expressa em termos probabilísticos como na Tabela A.2, ou em termos frequentes como na Tabela A.4. A representação probabilística indica a probabilidade média de um evento de risco ocorrer em um período determinado, enquanto a representação frequente indica a média do número de vezes de o evento de risco ocorrer em um período de tempo especificado. Como as duas abordagens expressam a mesma coisa a partir de duas perspectivas diferentes, qualquer representação pode ser usada, a depender de qual a organização achar mais conveniente para uma determinada categoria de riscos.

No entanto, se ambas as abordagens forem usadas como alternativas dentro da mesma organização, é importante que cada classificação nocionalmente equivalente em ambas as escalas representem a mesma probabilidade real. Caso contrário, os resultados da avaliação dependem de qual escala é utilizada, e não da probabilidade real da fonte de risco ser avaliada. Se ambas as abordagens foram utilizadas, convém que o nível probabilístico para cada classificação nocional seja calculado matematicamente a partir do valor frequente da classificação equivalente ou vice-versa, dependendo de qual abordagem é usada para definir a escala primária.

Se qualquer uma das duas abordagens for utilizada, não é necessário que os incrementos da escala sejam tão bem definidos, pois a priorização das probabilidades ainda pode ser alcançada independentemente dos valores absolutos utilizados. Embora a Tabela A.2 e a Tabela A.4 utilizem incrementos e faixas de probabilidade completamente diferentes, dependendo do contexto da organização e da categoria de risco que está sendo avaliada, ambos podem ser igualmente eficazes para análise se utilizados exclusivamente. Eles não seriam, no entanto, utilizáveis com segurança,

pois alternativas no mesmo contexto que os valores ligados a classificações equivalentes não se correlacionam.

As categorias e valores utilizados na Tabela A.2 e na Tabela A.4 são apenas exemplos. O valor mais adequado para atribuir a cada nível de probabilidade depende do perfil de risco e do apetite de risco da organização.

**Tabela A.2 – Exemplo de escala de probabilidade**

| Probabilidade | Descrição |
|---|---|
| **5 – Quase certo** | A fonte de risco certamente atingirá seu objetivo usando um dos métodos de ataque.<br>A probabilidade do cenário de risco é muito alta. |
| **4 – Muito provável** | A fonte de risco provavelmente atingirá seu objetivo usando um dos métodos de ataque.<br>A probabilidade do cenário de risco é alta. |
| **3 – Provável** | A fonte de risco é capaz de atingir seu objetivo usando um dos métodos de ataque.<br>A probabilidade do cenário de risco é significativa. |
| **2 – Bastante improvável** | A fonte de risco tem relativamente pouca chance de atingir seu objetivo usando um dos métodos de ataque.<br>A probabilidade do cenário de risco é baixa. |
| **1 – Improvável** | A fonte de risco tem muito pouca chance de atingir seu objetivo usando um dos métodos de ataque.<br>A probabilidade do cenário de risco é muito baixa. |

Classificações como “baixo”, “médio” e “alto” podem ser anexadas às classificações ao usar qualquer abordagem para avaliação de probabilidade. Estas podem ser úteis quando se discute níveis de probabilidade com as partes interessadas que não são especialistas em risco. No entanto, são subjetivos e, portanto, inevitavelmente ambíguos. Consequentemente, não convém que sejam usados como descritores primários ao realizar ou relatar avaliações.

#### A.1.1.2.3 Nível de risco

O uso das escalas qualitativas e a consistência dos processos de avaliação de riscos que derivam delas dependem inteiramente, da coerência com que os rótulos da categoria são interpretados por todas as partes interessadas. Convém que os níveis de qualquer escala qualitativa sejam inequívocos, seus incrementos claramente definidos, as descrições qualitativas para cada nível expressas em linguagem objetiva e as categorias não se sobreponham entre si.

Consequentemente, ao utilizar classificações de probabilidade, consequência ou risco, convém que estes sejam formalmente referenciados a escalas inequívocas ancoradas em numéricas (conforme a Tabela A.4) ou em pontos de referência radiométricos (conforme a Tabela A.2). Convém que todas as partes interessadas estejam cientes das escalas de referência para garantir que a interpretação dos dados e resultados de avaliação qualitativa seja consistente.

A Tabela A.3 apresenta um exemplo de abordagem qualitativa.

**Tabela A.3 – Exemplo de abordagem qualitativa aos critérios de risco**

| Probabilidade | Consequência | | | | |
|---|---|---|---|---|---|
| | Catastrófico | Crítico | Sério | Significativo | Menor |
| **Quase certo** | Muito alto | Muito alto | Alto | Alto | Médio |
| **Muito provavelmente** | Muito alto | Alto | Alto | Médio | Baixo |
| **Provável** | Alto | Alto | Médio | Baixo | Baixo |
| **Bastante improvável** | Médio | Médio | Baixo | Baixo | Muito baixo |
| **Improvável** | Baixo | Baixo | Baixo | Muito baixo | Muito baixo |

Convém que a criação de uma matriz de risco qualitativa seja orientada pelos critérios de aceitação de risco da organização (ver 6.4.2 e A.1.2).

EXEMPLO Às vezes uma organização está mais preocupada com consequências extremas, apesar de sua improvável ocorrência, ou principalmente com eventos de alta frequência com consequências menores.

Ao criar uma matriz de risco, seja qualitativa ou quantitativa, o perfil de risco de uma organização é normalmente assimétrico. Eventos triviais geralmente são os mais frequentes e a frequência esperada geralmente diminui à medida que as consequências aumentam, culminando em probabilidades muito baixas de consequências extremas. Também é incomum que a exposição ao negócio, representada por um evento de alta probabilidade/baixa consequência, seja equivalente à representada por um evento de baixa probabilidade/alta consequência. Embora uma matriz de risco que seja simétrica em relação à sua diagonal baixa/baixa para alta/alta possa parecer fácil de criar e ingenuamente aceitável, é improvável que ela represente com precisão o perfil de risco real de qualquer organização e, portanto, pode gerar resultados inválidos. Para assegurar que uma matriz de risco seja realista e possa cumprir o requisito de melhoria contínua (ver a ABNT NBR ISO/IEC 27001:2022, 10.2), convém que o raciocínio tanto para alocar cada categoria para as escalas de probabilidade e consequência e para a matriz de risco, quanto sobre a forma como as categorias estão de acordo com o perfil de risco da organização, sejam documentados quando as escalas e matrizes forem definidas ou alteradas. Convém que no mínimo as incertezas intrínsecas ao uso de matrizes em escala incremental sejam descritas com as devidas advertências aos seus usuários.

A utilidade das escalas qualitativas e a consistência das avaliações de risco que derivam delas dependem inteiramente da consistência com que as classificações sejam interpretadas por todas as partes interessadas. Convém que os níveis de qualquer escala qualitativa sejam inequívocos, seus incrementos estejam claramente definidos, as descrições para cada nível sejam expressas em linguagem objetiva e as categorias não se sobreponham entre si.

### A.1.1.3 Abordagem quantitativa

#### A.1.1.3.1 Escalas finitas

O nível de risco pode ser calculado usando qualquer método e levando em conta quaisquer fatores relevantes, mas geralmente é apresentado multiplicando a probabilidade pela consequência.

A probabilidade representa a possibilidade ou a frequência de um evento ocorrer dentro de um determinado período de tempo. Esse prazo é normalmente anual (por ano), mas pode ser maior (por exemplo, por século) ou menor (por exemplo, por segundo) de acordo com a pretensão da organização.

Convém que as escalas de probabilidade sejam definidas em termos práticos para que representem o contexto da organização, a fim de gerenciar riscos e sejam de fácil compreensão por todas as partes interessadas. Isso significa, principalmente, estabelecer limites realistas para a gama de probabilidades representadas. Se os limites máximos e mínimos da escala estiverem muito distantes, cada categoria dentro dela inclui uma gama excessivamente ampla de probabilidades, tornando incerta a avaliação.

EXEMPLO 1 O ponto de maior probabilidade finita na escala pode ser definido de forma apropriada em termos do tempo que normalmente a organização leva para responder aos eventos, e o ponto finito mais baixo em termos da duração do planejamento estratégico de longo prazo.

As probabilidades acima e abaixo dos limites definidos da escala podem ser expressas de forma apropriada como “maior que o máximo da escala” e “inferior ao mínimo da escala”, indicando claramente que as probabilidades, além dos limites da escala definida, são casos extremos a serem considerados excepcionalmente (possivelmente usando critérios especiais “fora dos limites”). Fora desses limites, a probabilidade específica é menos importante que o fato de ser uma exceção na direção concedida.

Geralmente, é útil medir as consequências utilizando um valor financeiro, pois permite agregar informações ao relato de risco.

EXEMPLO 2 Escalas de consequências monetárias são tipicamente baseadas em fatores de dez (100 a 1 000; 1 000 a 10 000 etc.). Convém que as distâncias das categorias de uma escala de probabilidade sejam selecionadas com referência às escalas de consequência, a fim de evitar uma faixa excessiva de risco acessando cada categoria.

EXEMPLO 3 Se a probabilidade e a consequência forem representadas pelos índices de escala exponencial (ou seja, os logaritmos dos valores na escala), convém que estes sejam somados.

O valor de risco pode, então, ser calculado da seguinte forma: antilog [log (valor de probabilidade) + log (valor de consequência)].

**Tabela A.4 – Exemplo de escala de probabilidade logarítmica**

| Frequência média aproximada | Expressão em log | Valor de escala |
|---|---|---|
| A cada hora | (aproximadamente $10^5$) | 5 |
| A cada 8 horas | (aproximadamente $10^4$) | 4 |
| Duas vezes por semana | (aproximadamente $10^3$) | 3 |
| Uma vez por mês | (aproximadamente $10^2$) | 2 |
| Uma vez por ano | ($10^1$) | 1 |
| Uma vez por década | ($10^0$) | 0 |

EXEMPLO 4 Na Tabela A.4, um exemplo de evento de alta frequência, é um ataque de senha feito por computador, ou um ataque *Distributed Denial-of-Service* feito por *botnet*. De fato, as frequências de ataque podem ser muito maiores.

EXEMPLO 5 Na Tabela A.4, um exemplo de evento de baixa frequência, são as erupções vulcânicas. Mesmo que seja previsto ocorrer apenas uma vez por século, não significa que não ocorreria durante a vida de um SGSI.

A Tabela A.5 apresenta um exemplo de escala de consequência logarítmica. O propósito de considerar a frequência é assegurar que as medidas de proteção sejam fortes o suficiente para suportar sequências de ataque de alta frequência, mesmo quando a probabilidade de tal sequência de ataque é baixa.

**Tabela A.5 – Exemplo de escala de consequência logarítmica**

| Consequência (uma perda de) | Expressão em log | Valor de escala |
|---|---|---|
| R$ 1000 000 | ($10^6$) | 6 |
| R$ 100.000 | ($10^5$) | 5 |
| R$ 10.000 | ($10^4$) | 4 |
| R$ 1000 | ($10^3$) | 3 |
| R$ 100 | ($10^2$) | 2 |
| Menos de R$ 100 | ($10^1$) | 1 |

Se as escalas de probabilidade e consequência utilizarem uma base logarítmica 10 para atribuir nível, os analistas de risco podem acabar com muitos riscos no mesmo nível de risco e serem incapazes de tomar uma decisão apropriada para priorização ou investimento em segurança. Nesse caso, pode ser útil reduzir a base e aumentar o número de níveis considerados. Convém notar que, se diferentes bases para probabilidade e consequências forem selecionadas, então não pode ser aplicada uma fórmula considerável para resumir dois fatores.

EXEMPLO 6 Se a probabilidade for duplicada ao passar de um nível para o outro enquanto a consequência é um fator 10 mais elevado, a fórmula resultará em riscos a) e b), em que o risco b) tem um nível de consequência 10 vezes mais elevado que o risco a), porém apenas metade da probabilidade de risco a) acabará no mesmo nível de risco. Isso é economicamente incorreto.

As Tabela A.4 e Tabela A.5 listam faixas de probabilidade e consequência que englobam a maioria das eventualidades entre organizações amplamente diferentes. É provável que nenhuma organização encontre a gama de risco representada pela totalidade dessas escalas de exemplo. Convém que o contexto da organização e do escopo do SGSI seja utilizado a fim de definir limites realistas superiores e inferiores para probabilidades e consequências, tendo em vista que quantificar faixas de risco superiores a 1 000 para 1 provavelmente será de valor prático limitado.

### A.1.2 Critérios de aceitação de riscos

Os critérios para a aceitação do risco podem ser simplesmente um valor acima do qual os riscos são considerados inaceitáveis.

EXEMPLO 1 Na Tabela A.3, se o valor médio for selecionado, todos os riscos com valor muito baixo, baixo ou médio seriam considerados aceitáveis pela organização, e todos os riscos com valor alto ou muito alto seriam considerados inaceitáveis.

Ao utilizar uma matriz de risco codificada por cores, espelhando as escalas para consequência e probabilidade, as organizações podem apresentar graficamente a distribuição de risco de uma ou várias avaliações de risco. Esta matriz de risco também pode ser utilizada para sinalizar a atitude da organização com relação aos valores de risco, e indicar se convém que um risco seja normalmente aceito ou tratado.

EXEMPLO 2 A matriz de risco utilizando três cores (por exemplo, vermelho, amarelo e verde) pode ser aplicada para representar três graus de avaliação de riscos, conforme apresentado na Tabela A.6.

Pode ser benéfico escolher outros modelos utilizando cores para uma matriz de risco.

EXEMPLO 3 Se uma matriz de risco for utilizada para comparar os resultados de uma avaliação de riscos, originalmente realizada com os resultados de uma reavaliação para os mesmos riscos, a redução do risco pode ser mais facilmente apresentada se mais cores forem aplicadas aos níveis atuais de riscos.

Também é possível adicionar qual nível de gestão está autorizado a aceitar um risco com determinado valor.

A Tabela A.6 apresenta um exemplo de escala de avaliação.

**Tabela A.6 – Exemplo de escala de avaliação associada à matriz de risco de três cores**

| Nível de risco | Avaliação de riscos | Descrição |
|---|---|---|
| **Baixo (verde)** | Aceitável como é apresentado | O risco pode ser aceito sem mais ações. |
| **Moderado (amarelo)** | Tolerável sob controle | Convém que um acompanhamento em termos de gestão de riscos seja realizado, e que ações sejam criadas no quadro de melhoria contínua a médio e longo prazo. |
| **Alto (vermelho)** | Inaceitável | Convém que medidas para reduzir o risco sejam tomadas absolutamente no curto prazo. Caso contrário, convém que toda ou parte da atividade seja recusada. |

## A.2 Técnicas práticas

### A.2.1 Componentes de risco de segurança da informação

Ao identificar e avaliar os riscos de segurança da informação, convém que sejam levados em conta os seguintes componentes:

— componentes relacionados ao passado:

  — eventos de segurança e incidentes (dentro e fora da organização);

  — fontes de risco;

  — vulnerabilidades exploradas;

  — consequências medidas;

— componentes relacionados ao futuro:

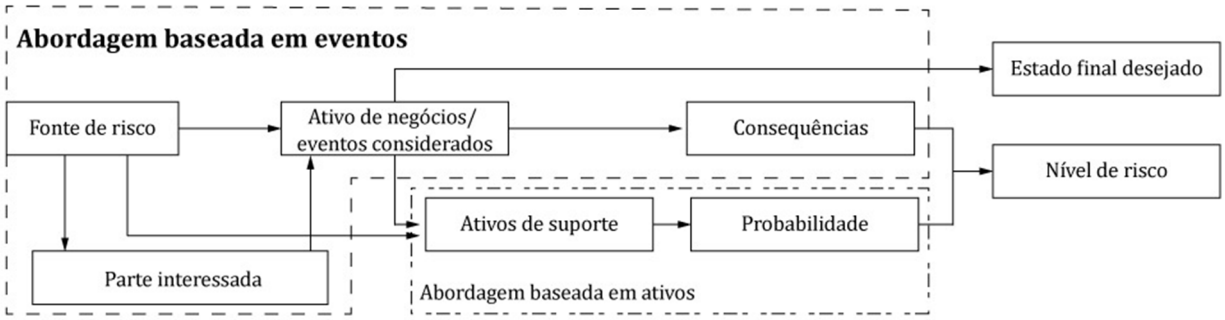
— ameaças;

— vulnerabilidades;

— consequências;

— cenários de risco.

As relações entre os componentes de risco de segurança da informação são apresentadas na Figura A.1 e discutidas em A.2.2 a A.2.7.




**Legenda**

→ ameaça

**Figura A.1 – Componentes de avaliação de riscos de segurança da informação**

Detalhes sobre “Estado final desejado” podem ser encontrados em A.2.3-b).

## A.2.2 Ativos

Ao aplicar a abordagem com base em ativos para a identificação de riscos, convém que os ativos sejam identificados.

No processo de avaliação de riscos, dentro do desenvolvimento de cenários de risco, convém que a identificação de eventos, consequências, ameaças e vulnerabilidades estejam vinculadas aos ativos.

No processo de tratamento de riscos, cada controle é aplicável a um subconjunto dos ativos.

Os ativos podem ser divididos em duas categorias:

— ativos primários/de negócio – informações ou processos de valor para uma organização;

— ativos de suporte – componentes do sistema de informações em que um ou vários ativos de negócios estão fundamentados.

Os ativos primários/de negócio são frequentemente usados na abordagem com base em eventos (identificação de eventos e suas consequências sobre os ativos de negócio).

Os ativos de suporte são frequentemente utilizados na abordagem com base em ativos (identificação e análise de vulnerabilidades e ameaças sobre esses ativos) e no processo de tratamento de riscos (especificação dos ativos aos quais convém que cada controle seja aplicado).

Os ativos de negócio e de suporte estão relacionados, portanto, às fontes de risco identificadas para os ativos de suporte que podem impactar os ativos de negócio

Por isso, é importante identificar as relações entre os ativos e entender seu valor para a organização. O erro de julgamento do valor do ativo pode levar a um erro de julgamento das consequências relacionadas ao risco, mas também pode afetar o entendimento da probabilidade de ameaças em consideração.

EXEMPLO 1 Um ativo de suporte está hospedando um ativo de negócios (informações, neste caso).

Os dados são protegidos por controles internos e externos, a fim de evitar que uma fonte de risco atinja seu objetivo relacionado ao ativo de negócio, explorando uma vulnerabilidade no ativo de suporte. Ao distinguir diferentes tipos de ativos, convém que as dependências entre os ativos sejam documentadas e a propagação de riscos avaliada, de modo que possa ser documentado que o mesmo risco não seja avaliado duas vezes, uma vez quando ocorre no ativo de suporte, e uma vez quando afeta os ativos primários. Os gráficos de dependência de ativos são ferramentas úteis para representar estas dependências e assegurar que todas as dependências tenham sido consideradas.

EXEMPLO 2 O gráfico na Figura A.2 indica ativos dependentes para o ativo de negócio “mostrando pedido e processamento de faturas” e pode ser lido da seguinte forma:

— “Administrador” (tipo: recurso humano), que, se não for devidamente treinado, propaga um risco para o ativo.

— Manutenção de TI” (tipo: serviço), que propaga o risco para o ativo.

— “Servidor” (tipo: *hardware*) ou para o ativo “Rede” (tipo de conectividade de rede). O servidor, se ele parar de operar ou a rede desconfigurada impacta o ativo.

— “Portal da *Web*” (tipo: aplicativo), para parar de rodar ou ficar indisponível.

Sem o “portal da *web*”, o processo de negócio “mostrando pedido e processamento de faturas” não oferece o processo pretendido aos clientes.

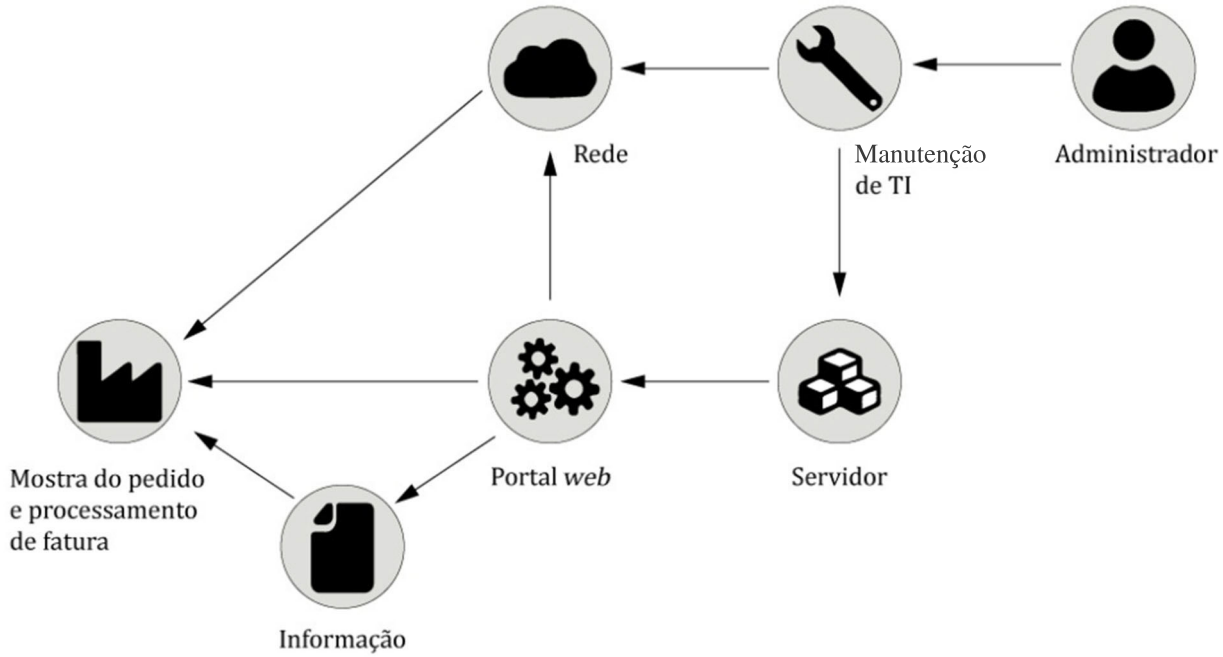



**Figura A.2 – Exemplo de um gráfico de dependência de ativos**

### A.2.3 Fontes de risco e estado final desejado

Este parágrafo propõe caracterizar esse tipo de fontes de risco. Dois critérios principais estruturam essa abordagem descritiva:

— a motivação;

— a capacidade de agir.

a) Identificação de fonte de risco

A Tabela A.7 apresenta exemplos e métodos habituais de ataque.

**Tabela A.7 – Exemplos e métodos habituais de ataque** (continua)

| Fonte de risco | Exemplos e métodos habituais de ataque |
|---|---|
| **Relacionado ao Estado** | Estados, agências de inteligência<br>Método: Ataques geralmente conduzidos por profissionais, trabalhando sob um calendário e um método de ataque que são predefinidos. Este perfil de atacante é caracterizado por sua capacidade de realizar uma operação ofensiva por um longo período de tempo (recursos estáveis, procedimentos) e adaptar suas ferramentas e métodos à topologia do alvo. Por extensão, esses atores têm os meios de comprar ou descobrir vulnerabilidades de 0-*Day* e alguns são capazes de se infiltrar em redes isoladas e realizar ataques sucessivos a fim de atingir um alvo ou alvos (por exemplo, por meio de um ataque direcionado à cadeia de suprimentos). |
| **Crime organizado** | Organizações de cibercriminosos (máfias, gangues, ferramentas criminosas)<br>Método: Golpes *on-line* ou pessoalmente, solicitação de resgate ou ataque via *ransomware*, uso de *botnets* etc. Devido, em particular, à proliferação de *kits* de ataque que estão prontamente disponíveis *on-line*, os cibercriminosos estão realizando operações cada vez mais sofisticadas e organizadas para fins lucrativos ou fraudulentos. Alguns têm os meios de comprar ou descobrir vulnerabilidades de *0-Day*. |
| **Terrorista** | Ciberterroristas, cibermilícias<br>Método: Ataques que geralmente não são muito sofisticados, mas que são conduzidos com determinação para efeitos de desestabilização e destruição: negação de serviço (visando, por exemplo, tornar os serviços de emergência de um centro hospitalar indisponíveis, paralisações prematuras de um sistema industrial de produção de energia), desfiguração e exploração de vulnerabilidades de *sites* de *Internet*. |
| **Ativista ideológico** | Cyber-hacktivistas, grupos de interesse, seitas<br>Método: Os métodos e sofisticação dos ataques são relativamente semelhantes aos dos ciberterroristas, mas são motivados por intenções menos destrutivas. Alguns atores realizam esses ataques a fim de transmitir uma ideologia, uma mensagem (por exemplo, uso maciço das redes sociais como meio de manifestação). |
| **Ferramentas especializadas** | Perfil “cibermercenário” com conhecimento em tecnologia que geralmente são altas do ponto de vista técnico. Por causa disso, convém que seja distinguido dos *script-kids* com quem compartilha, no entanto, o espírito de um desafio e busca por reconhecimento, mas com um objetivo lucrativo. Esses grupos podem ser organizados como ferramentas especializadas que propõem verdadeiros serviços de *hackers*.<br>Método: Este tipo de *hacker* experiente está muitas vezes na origem da concepção e criação de kits de ataque e ferramentas que estão disponíveis online (possivelmente custando uma taxa) que podem então ser usados, mediante disponibilização, por outros grupos de invasores. Não há motivações particulares além do ganho financeiro. |
| **Amador** | Perfil do *hacker script-kiddies* ou que tenha bom conhecimento em tecnologia; motivado pela busca por reconhecimento social, diversão, desafio.<br>Método: Ataques básicos, mas com a capacidade de uso dos *kits* de ataque que estão disponíveis *on-line*. |

**Tabela A.7** (conclusão)

| Fonte de risco | Exemplos e métodos habituais de ataque |
|---|---|
| **Vingador** | As motivações desse perfil de agressor são guiadas por um espírito de vingança aguda ou um sentimento de injustiça (por exemplo, funcionário demitido por falta grave, provedor de serviços descontente após um contrato que não foi renovado etc.).<br>Método: Esse perfil de atacante é caracterizado por sua determinação e seu conhecimento interno dos sistemas e processos organizacionais. Isso pode torná-lo formidável e fornecer-lhe um poder substancial para causar danos. |
| **Atacante patológico** | As motivações desse perfil de agressor são de natureza patológica ou oportunista e às vezes são guiadas pelo motivo de um ganho (por exemplo, concorrente injusto, cliente desonesto, golpista e fraudador).<br>Método: Aqui, os atacantes têm uma base de conhecimento em computação que os leva a tentar comprometer a segurança da informação de seu alvo, ou eles usam os *kits* de ataque disponíveis *on-line*, ou decidem subcontratar o ataque de tecnologia, chamando uma equipe especializada. Em certos casos, os invasores podem direcionar sua atenção para uma fonte interna (funcionário descontente, provedor de serviços inescrupuloso) e tentar corromper este último. |

b) Modelar a motivação de uma fonte de risco — estado final desejado

Há uma ampla gama de motivações: podem ser motivações políticas, financeiras, ideológicas, mas também sociais ou até mesmo representar uma condição psicológica pontual ou patológica.

Embora não seja possível expressar diretamente uma motivação, ela pode ser apresentada por meio da intenção da fonte de risco e expressa na forma de um estado final desejado (*Desired End State* - DES): a situação geral que a fonte de risco quer alcançar após o confronto. Uma classificação sistemática de situações, associadas a categorias gerais de ação, pode orientar a análise contextualizada.

A Tabela A.8 apresenta um exemplo de classificação de motivações para expressar o DES.

**Tabela A.8 – Exemplo de classificação de motivações para expressar o DES**

| | |
|---|---|
| **Conquistar** | Captura de recursos a longo prazo ou mercados econômicos, ganhando poder político ou impondo valores |
| **Adquirir** | Abordagem predatória, resolutamente ofensiva, impulsionada pela captura de recursos ou benefícios |
| **Impedir** | Abordagem ofensiva para limitar as ações de terceiros |
| **Manter** | Esforços para manter uma situação ideológica, política, econômica ou social |
| **Defender** | Adotando uma postura de recuo estritamente defensiva, ou uma atitude explicitamente ameaçadora (por exemplo, intimidação) a fim de evitar o comportamento agressivo de um oponente claramente designado ou impedir sua ação, atrasando-os etc. |
| **Sobreviver** | Proteger uma entidade a todo custo, o que pode levar a ações extremamente agressivas |

c) Objetivos de alvo

Para chegar ao DES, a fonte de risco se concentra em um ou vários objetivos que impactam os ativos de negócios do sistema pretendido. Estes são os objetivos-alvo da fonte de risco.

A Tabela A.9 apresenta exemplos de objetivos-alvo.

**Tabela A.9 – Exemplos de objetivos-alvo**

| Objetivo-alvo | Descrição |
|---|---|
| **Espionagem** | Operação de inteligência (estatal, econômica). Em muitos casos, o invasor visa uma instalação de longo prazo no sistema de informações e com total discrição. Armas, espaço, aeronáutica, setor farmacêutico, energia e certas atividades do Estado (economia, finanças e relações exteriores) são alvos privilegiados. |
| **Pré-posicionamento estratégico** | O pré-posicionamento geralmente visa um ataque a longo prazo, sem que o propósito final seja claramente estabelecido (por exemplo, comprometendo redes de operadoras de telecomunicações, infiltração massiva de sites de *internet,* a fim de lançar uma operação de influência política ou econômica com um forte eco). O comprometimento repentino e maciço de computadores para formar uma *botnet* pode ser vinculado a esta categoria. |
| **Influência** | Operação com objetivo de difundir informações falsas ou alterá-las, mobilizando formadores de opinião nas redes sociais, destruindo reputações, divulgando informações confidenciais, degradando a imagem de uma organização ou de um Estado. O objetivo final é, geralmente, desestabilizar ou modificar percepções. |
| **Obstáculo ao funcionamento** | Operação de sabotagem com o objetivo de, por exemplo, tornar um *site* da *internet* indisponível, causando saturação de informações, impedindo o uso de um recurso digital, tornando uma instalação física indisponível. Os sistemas industriais podem ser particularmente expostos e vulneráveis por meio de redes de tecnologia com as quais estejam interconectados (por exemplo, enviando comandos a fim de gerar danos de *hardware* ou uma quebra que exija manutenção extensiva). Os ataques de negação de serviço distribuídos (DDoS) são técnicas comumente usadas para neutralizar recursos digitais. |
| **Lucrativo** | Operação visando um ganho financeiro, direta ou indiretamente. Geralmente ligado ao crime organizado, pode-se mencionar: fraude na *internet*, lavagem de dinheiro, extorsão ou peculato, manipulação do mercado financeiro, falsificação de documentos administrativos, roubo de identidade etc. Certas operações para fins lucrativos podem fazer uso de um método de ataque que faz parte das categorias *hereinabove* (por exemplo, espionagem e roubo de dados, *ransomware* a fim de neutralizar uma atividade), mas o propósito final permanece financeiro. |
| **Desafio, diversão** | Operação destinada a realizar uma exploração para fins de reconhecimento social, desafio ou simplesmente para diversão.<br>Embora o objetivo seja principalmente para a diversão e sem qualquer desejo particular de prejudicar, esse tipo de operação pode ter sérias consequências para a vítima. |

A diferença entre um DES e um objetivo-alvo pode ser ilustrada pelo exemplo de uma fonte de risco cujo objetivo é ganhar um acordo (DES) que busca roubar informações confidenciais sobre negociações de seu concorrente (objetivo estratégico). Às vezes, o alvo em questão (as informações desejadas) não resulta no DES.

Pode-se considerar que o valor do alvo do ponto de vista da fonte de risco baseia-se na sua contribuição ao DES.

Em termos gerais, os objetivos-alvo da fonte de risco são divididos em duas classes principais:

— explorando recursos alvo para seu próprio benefício (por exemplo, espionagem, roubo, trapaça, fraude, tráfico);

— impedindo que o alvo use seus recursos (o confronto é sempre relativo) (por exemplo, guerra, terrorismo, sabotagem, subversão, desestabilização).

### A.2.4 Abordagem com base em eventos

#### A.2.4.1 Ecossistema

Em uma abordagem com base em eventos, convém que os cenários sejam construídos analisando os diferentes caminhos, relevantes para as interações entre a organização e as partes interessadas, que formam um ecossistema que as fontes de risco podem usar para alcançar os ativos do negócio e seus DES.

Um número crescente de métodos de ataque usam os *links* mais vulneráveis em tal ecossistema para atingir seus objetivos.

As partes interessadas no escopo do SGSI que convém que sejam consideradas ao analisar cenários de risco, podem ser de dois tipos:

— partes externas, incluindo:

  — clientes;

  — sócios, cocontratantes;

  — prestadores de serviços (subcontratados, fornecedores).

— partes internas, incluindo:

  — prestadores de serviços técnicos (por exemplo, serviços de suporte propostos pela gestão de TI);

  — prestadores de serviços de negócios (por exemplo, entidade comercial que utiliza dados de negócios);

  — subsidiárias (em particular, localizadas em outros países).

O objetivo da identificação das partes interessadas é obter uma visão clara do ecossistema, a fim de identificar os mais vulneráveis. Convém que a conscientização do ecossistema seja tratada como um estudo preliminar de risco. A Figura A.3 mostra a identificação das partes interessadas do ecossistema.

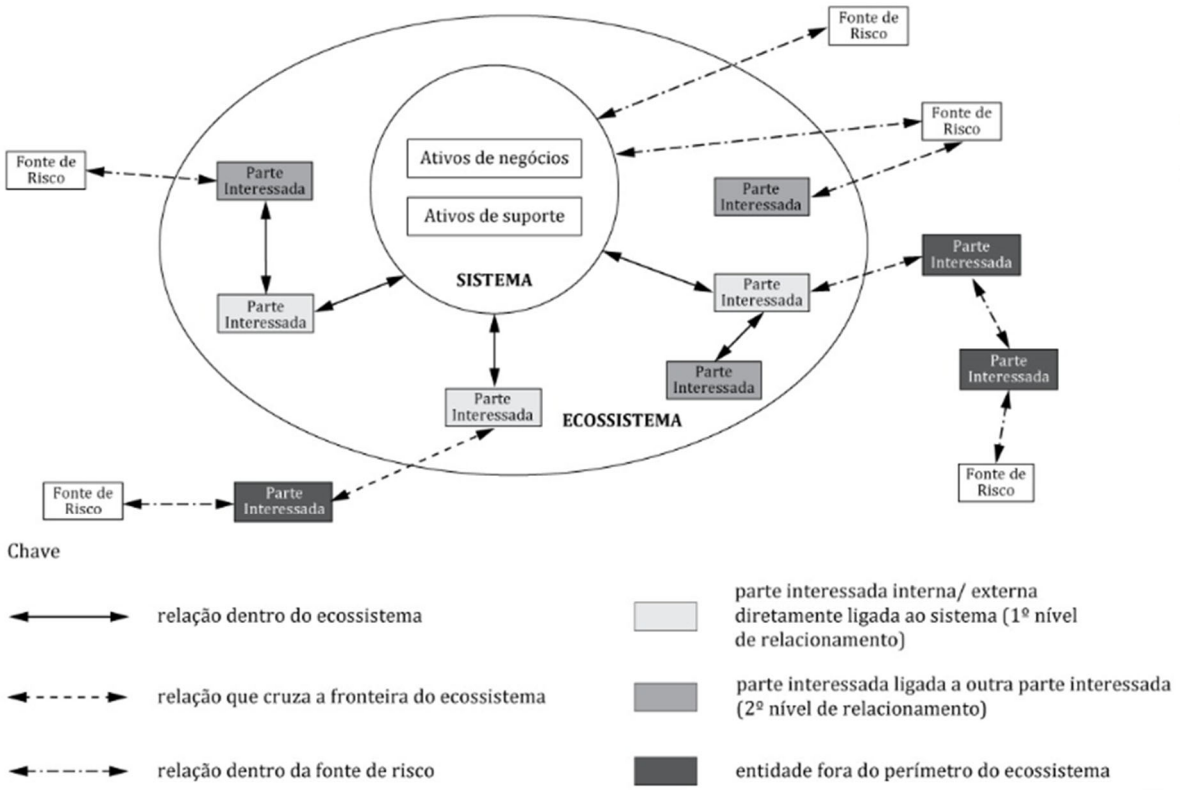



**Figura A.3 – Identificação das partes interessadas do ecossistema**

### A.2.4.2 Cenários estratégicos

Com base em informações sobre fontes de risco e eventos envolvidos, cenários realistas de alto nível (cenários estratégicos) podem ser imaginados, indicando de que forma uma fonte de risco pode proceder para chegar ao seu DES. Ele pode, por exemplo, passar pelo ecossistema ou desviar alguns processos de negócios. Esses cenários são identificados por dedução, a partir das fontes de risco e de seus DES: para cada uma delas, podem ser feitas as seguintes perguntas, do ponto de vista da fonte de risco:

— Quais são os ativos de negócios da organização que convém que as fontes de risco mirem para chegar ao seu DES?

— Para tornar possível o ataque ou facilitá-lo, é provável que ataquem a parte interessada crítica do ecossistema que tenha acesso privilegiado aos ativos do negócio?

Uma vez identificados os elementos mais expostos, o cenário estratégico pode ser desenhado, descrevendo o sequenciamento dos eventos gerados pela fonte de risco para chegar ao seu DES. A infração aos ativos de negócio corresponde a eventos finais, enquanto os eventos relativos ao ecossistema são eventos intermediários. O cenário estratégico reflete uma avaliação de consequências herdada diretamente  dos eventos envolvidos.

Esses cenários podem ser representados na forma de gráficos de ataque ou diretamente na visão ecossistêmica do mapeamento do sistema de informações, superpondo o caminho de ataque.

Cenários estratégicos requerem uma consideração adicional da probabilidade dos eventos. A abordagem baseada em ativos e os cenários operacionais associados podem ser usados para determinar a probabilidade de eventos. Os exemplos de ameaças apresentados em A.2.5.1 podem ser utilizados para obter avaliações necessárias.

## A.2.5 Abordagem com base em ativos

### A.2.5.1 Exemplos de ameaças

A Tabela A.10 fornece exemplos de ameaças típicas. A lista pode ser usada durante o processo de avaliação de ameaças. Ameaças consideradas como fontes de risco podem ser deliberadas, como acidentais ou ambientais (naturais) e podem resultar, por exemplo, em danos ou perda de serviços essenciais. A lista indica para cada tipo de ameaça onde D (deliberada), A (acidental), E (ambiental) é relevante. D é usado para todas as ações deliberadas voltadas para informações e ativos relacionados à informação, A é usado para todas as ações humanas que podem danificar acidentalmente informações e ativos relacionados à informação, e E é usado para todos os incidentes que não são baseados em ações humanas. Os grupos de ameaças não estão em ordem prioritária.

Os controles podem mitigar ameaças dissuadindo ou impedindo que essas ameaças atuem ou ocorram. A seleção de controles para reduzir o risco também requer a consideração de controles detectivos e responsivos que identifiquem, respondam, contenham e recuperem de eventos. Controles detectivos e responsivos estão associados a consequências ao invés de ameaças.

EXEMPLO O registro e o monitoramento permitem a identificação e a resposta de eventos de segurança.

**Tabela A.10 – Exemplos de ameaças típicas** (continua)

| Categoria | Nº | Descrição da ameaça | Tipo de fonte de risco[a] |
|---|---|---|---|
| Ameaças físicas | TP01 | Fogo | A, D, E |
| | TP02 | Água | A, D, E |
| | TP03 | Poluição, radiação nociva | A, D, E |
| | TP04 | Acidente grave | A, D, E |
| | TP05 | Explosão | A, D, E |
| | TP06 | Poeira, corrosão, congelamento | A, D, E |
| Ameaças naturais | TN01 | Fenômeno climático | E |
| | TN02 | Fenômeno sísmico | E |
| | TN03 | Fenômeno vulcânico | E |
| | TN04 | Fenômeno meteorológico | E |
| | TN05 | Inundação | E |
| | TN06 | Fenômeno pandemia/epidêmico | E |
| Falhas na infraestrutura | TI01 | Falha de um sistema de abastecimento | A, D |
| | TI02 | Falha no sistema de resfriamento ou ventilação | A, D |
| | TI03 | Perda de fornecimento de energia | A, D, E |
| | TI04 | Falha de uma rede de telecomunicações | A, D, E |
| | TI05 | Falha nos equipamentos de telecomunicações | A, D |
| | TI06 | Onda eletromagnética | A, D, E |
| | TI07 | Radiação térmica | A, D, E |
| | TI08 | Pulsos eletromagnéticos | A, D, E |
| Falhas técnicas | TT01 | Falha do dispositivo ou sistema | Um |
| | TT02 | Saturação do sistema de informação | A, D |
| | TT03 | Violação da capacidade de manutenção do sistema de informações | A, D |

**Tabela A.10** (continuação)

| Categoria | Nº | Descrição da ameaça | Tipo de fonte de risco[a] |
|---|---|---|---|
| Ações humanas | TH01 | Terror, ataque, sabotagem | D |
| | TH02 | Engenharia Social | D |
| | TH03 | Interceptação de radiação de um dispositivo | D |
| | TH04 | Espionagem remota | D |
| | TH05 | Escutas | D |
| | TH06 | Roubo de mídia ou documentos | D |
| | TH07 | Roubo de equipamentos | D |
| | TH08 | Roubo de identidade digital ou credenciais | D |
| | TH09 | Recuperação de mídia reciclada ou descartada | D |
| | TH10 | Divulgação de informações | A, D |
| | TH11 | Entrada de dados de fontes não confiáveis | A, D |
| | TH12 | Adulteração de *hardware* | D |
| | TH13 | Adulteração de *software* | A, D |
| | TH14 | *Drive-by-exploits* usando comunicação baseada na *Web* | D |
| | TH15 | *Replay attack* e *man-in-the-middle*) | D |
| | TH16 | Tratamento não autorizado de dados pessoais | A, D |
| | TH17 | Entrada não autorizada nas instalações | D |
| | TH18 | Uso não autorizado de dispositivos | D |
| | TH19 | Uso incorreto de dispositivos | A, D |
| | TH20 | Dispositivos ou mídia prejudiciais | A, D |
| | TH21 | Cópia fraudulenta de *software* | D |
| | TH22 | Uso de *software* falsificado ou copiado | A, D |
| | TH23 | Corrupção de dados | D |
| | TH24 | Processamento ilegal de dados | D |
| | TH25 | Envio ou distribuição de *malware* | A, D, R. |
| | TH26 | Detecção de posição | D |

**Tabela A.10** (conclusão)

| Categoria | Nº | Descrição da ameaça | Tipo de fonte de risco[a] |
|---|---|---|---|
| Comprometimento de funções ou serviços | TC01 | Erro de uso | Um |
| | TC02 | Abuso de direitos ou permissões | A, D |
| | TC03 | Falsificação de direitos ou permissões | D |
| | TC04 | Negação de ações | D |
| Ameaças organizacionais | TO01 | Falta de pessoal | A, E |
| | TO02 | Falta de recursos | A, E |
| | TO03 | Falha dos prestadores de serviços | A, E |
| | TO04 | Violação de leis ou regulamentos | A, D |

[a] D = deliberada; A = acidental; E = ambiental.

### A.2.5.2 Exemplos de vulnerabilidades

A Tabela A.11 fornece exemplos de vulnerabilidades em diversas áreas de segurança, incluindo exemplos de ameaças que podem explorar essas vulnerabilidades. As listas podem fornecer ajuda durante a avaliação de ameaças e vulnerabilidades, para determinar cenários de risco relevantes. Em alguns casos, outras ameaças também podem explorar essas vulnerabilidades.

**Tabela A.11 – Exemplos de vulnerabilidades típicas** (continua)

| Categoria | Nº | Exemplos de vulnerabilidades |
|---|---|---|
| *Hardware* | VH01 | Manutenção insuficiente/instalação defeituosa de mídia de armazenamento |
| | VH02 | Esquemas de substituição periódica insuficientes para equipamentos |
| | VH03 | Suscetibilidade à umidade, poeira, sujeira |
| | VH04 | Sensibilidade à radiação eletromagnética |
| | VH05 | Controle de alteração de configuração insuficiente |
| | VH06 | Suscetibilidade a variações de tensão |
| | VH07 | Suscetibilidade a variações de temperatura |
| | VH08 | Armazenamento desprotegido |
| | VH09 | Falta de cuidado à disposição |
| | VH10 | Cópia descontrolada |

**Tabela A.11** (continuação)

| Categoria | Nº | Exemplos de vulnerabilidades |
|---|---|---|
| *Software* | VS01 | Nenhum ou teste de *software* insuficiente |
| | VS02 | Falhas bem conhecidas no *software* |
| | VS03 | Sem "*logout*" ao sair da estação de trabalho |
| | VS04 | Descarte ou reutilização de mídia de armazenamento sem a devida eliminação |
| | VS05 | Configuração insuficiente de *logs* para fins de trilha de auditoria |
| | VS06 | Alocação errada de direitos de acesso |
| | VS07 | *Software* amplamente distribuído |
| | VS08 | Aplicando programas de aplicativos aos dados errados em termos de tempo |
| | VS09 | Interface de usuário complicada |
| | VS10 | Insuficiente ou falta de documentação |
| | VS11 | Parâmetro incorreto configurado |
| | VS12 | Datas incorretas |
| | VS13 | Mecanismos insuficientes de identificação e autenticação (por exemplo, para autenticação do usuário) |
| | VS14 | Tabelas de senhas desprotegidas |
| | VS15 | Má gestão de senhas |
| | VS16 | Serviços desnecessários habilitados |
| | VS17 | *Software* imaturo ou novo |
| | VS18 | Especificações não claras ou incompletas para desenvolvedores |
| | VS19 | Controle de mudança ineficaz |
| | VS20 | *Download* e uso de *software* descontrolados |
| | VS21 | Falta de cópias de *backup* ou incompletas |
| | VS22 | Falha na produção de relatórios de gestão |
| Rede | VN01 | Mecanismos insuficientes para a prova de enviar ou receber uma mensagem |
| | VN02 | Linhas de comunicação desprotegidas |
| | VN03 | Tráfego sensível desprotegido |
| | VN04 | Acoplamentos de baixa qualidade |
| | VN05 | Único ponto de falha |
| | VN06 | Ineficaz ou sem mecanismos de identificação e autenticação de remetente e receptor |
| | VN07 | Arquitetura de rede insegura |
| | VN08 | Transferência de senhas em claro |
| | VN09 | Gestão de rede inadequada (resiliência do roteamento) |
| | VN10 | Conexões de rede pública desprotegidas |

**Tabela A.11** (continuação)

| Categoria | Nº | Exemplos de vulnerabilidades |
|---|---|---|
| Pessoal | VP01 | Ausência de pessoal |
| | VP02 | Procedimentos inadequados de recrutamento |
| | VP03 | Treinamento de segurança insuficiente |
| | VP04 | Uso incorreto de *software* e *hardware* |
| | VP05 | Má consciência de segurança |
| | VP06 | Mecanismos insuficientes ou sem mecanismos de monitoramento |
| | VP07 | Trabalho não supervisionado por funcionários externos ou de limpeza |
| | VP08 | Ineficaz ou sem políticas para o uso correto de mídia de telecomunicações e mensagens |
| Local | VS01 | Uso inadequado ou descuidado do controle de acesso físico a edifícios e salas |
| | VS02 | Localização em uma área suscetível a inundações |
| | VS03 | Rede de energia instável |
| | VS04 | Proteção física insuficiente do prédio, portas e janelas |
| Organização | VO01 | Procedimento formal para registro e descadastramento do usuário não desenvolvido, ou sua implementação é ineficaz |
| | VO02 | Processo formal para análise crítica de direito de acesso (supervisão) não desenvolvido, ou sua implementação é ineficaz |
| | VO03 | Disposições insuficientes (relativas à segurança) em contratos com clientes e/ou terceiros |
| | VO04 | Procedimento de monitoramento de instalações de processamento de informações não desenvolvidas, ou sua implementação é ineficaz |
| | VO05 | Auditorias (supervisão) não realizadas regularmente |
| | VO06 | Procedimentos de identificação e avaliação de riscos não desenvolvidos, ou sua implementação é ineficaz |
| | VO07 | Relatórios insuficientes ou sem falhas registrados em registros de administradores e operadores |
| | VO08 | Resposta inadequada de manutenção de serviços |
| | VO09 | Acordo de nível de serviço insuficiente ou falta |
| | VO10 | Procedimento de controle de mudança não desenvolvido, ou sua implementação é ineficaz |
| | VO11 | Procedimento formal para controle de documentação do SGSI não desenvolvido, ou sua implementação é ineficaz |
| | VO12 | Procedimento formal para supervisão de registro do SGSI não desenvolvido, ou sua implementação é ineficaz |
| | VO13 | Processo formal para autorização de informações disponíveis publicamente não desenvolvidas, ou sua implementação é ineficaz |
| | VO14 | Alocação indevida de responsabilidades de segurança da informação |

**Tabela A.11** (conclusão)

| Categoria | Nº | Exemplos de vulnerabilidades |
|---|---|---|
| Organização | VO15 | Planos de continuidade não existem, ou estão incompletos, ou estão desatualizados |
| | VO16 | Política de uso de e-mails não desenvolvida, ou sua implementação é ineficaz |
| | VO17 | Procedimentos para introduzir *software* em sistemas operacionais não desenvolvidos, ou sua implementação é ineficaz |
| | VO18 | Procedimentos para o processamento de informações classificadas não desenvolvidos, ou sua implementação é ineficaz |
| | VO19 | Responsabilidades de segurança da informação não estão presentes nas descrições do trabalho |
| | VO20 | Insuficiência ou falta de provisões (relativas à segurança da informação) em contratos com funcionários |
| | VO21 | Processo disciplinar em caso de incidente de segurança da informação não determinado, ou não funcionando corretamente |
| | VO22 | Política formal sobre uso de computador móvel não desenvolvida, ou sua implementação é ineficaz |
| | VO23 | Controle insuficiente de ativos fora do local |
| | VO34 | Política insuficiente ou sem “mesa limpa e tela limpa” |
| | VO25 | Autorização de processamento de informações não implementadas ou não funcionando corretamente |
| | VO26 | Mecanismos de monitoramento de violações de segurança não implementadas adequadamente |
| | VO27 | Procedimentos para relatar fraquezas de segurança não desenvolvidas, ou sua implementação é ineficaz |
| | VO28 | Procedimentos de disposições de conformidade com direitos intelectuais não desenvolvidos, ou sua implementação é ineficaz |

### A.2.5.3 Métodos para avaliação de vulnerabilidades técnicas

Métodos proativos, como testes de sistema de informações, podem ser usados para identificar vulnerabilidades, dependendo da criticidade do sistema de Tecnologia da Informação e Comunicações (TIC) e dos recursos disponíveis (por exemplo, fundos alocados, tecnologia disponível, pessoas com experiência para realizar o teste). Os métodos de teste incluem:

— ferramenta automatizada de varredura de vulnerabilidades;

— testes de segurança e avaliação;

— teste de penetração;

— análise crítica de código.

Uma ferramenta automatizada de varredura de vulnerabilidades é usada para analisar um grupo de *hosts* ou uma rede em busca de serviços vulneráveis conhecidos [por exemplo, o sistema permite o FTP (*Anonymous File Transfer Protocol*, protocolo de transferência de arquivos” anônimo,

retransmissão de Sendmail] No entanto, algumas das vulnerabilidades potenciais identificadas pela ferramenta de digitalização automatizada não representam necessariamente vulnerabilidades reais no contexto do ambiente do sistema (por exemplo, algumas dessas ferramentas de digitalização avaliam vulnerabilidades potenciais sem considerar o ambiente e os requisitos do *site*). Algumas das vulnerabilidades sinalizadas pelo *software* de digitalização automatizado podem realmente não ser vulneráveis para um determinado *site*, mas podem ser configuradas dessa forma porque seu ambiente requer isso. Este método de teste pode, portanto, produzir falsos positivos.

O teste e avaliação de segurança (STE) é outra técnica que pode ser usada na identificação de vulnerabilidades do sistema de TIC durante o processo de avaliação de riscos. Inclui o desenvolvimento e execução de um plano de teste (por exemplo, *script* de teste, procedimentos de teste e resultados esperados de testes). O objetivo dos testes de segurança do sistema é testar a eficácia dos controles de segurança de um sistema de TIC, pois eles foram aplicados em um ambiente operacional. O objetivo é assegurar que os controles aplicados atendam à especificação de segurança aprovada para o *software* e *hardware* e implementem a política de segurança da organização ou atendam aos padrões do setor.

Os testes de penetração podem ser usados para complementar a análise crítica dos controles de segurança e garantir que diferentes facetas do sistema de TIC estejam protegidas. Os testes de penetração, quando utilizados no processo de avaliação de riscos, podem ser usados para avaliar a capacidade de um sistema de TIC de suportar tentativas intencionais de burlar a segurança do sistema. O objetivo é testar o sistema de TIC do ponto de vista de uma fonte de ameaça e identificar possíveis falhas nos esquemas de proteção do sistema de TIC.

A análise crítica de código é a maneira mais completa (mas também mais cara) de avaliação de vulnerabilidade.

Os resultados desses tipos de testes de segurança ajudam a identificar as vulnerabilidades de um sistema.

Ferramentas e técnicas de penetração podem dar resultados falsos, a menos que a vulnerabilidade seja explorada com sucesso. Para explorar vulnerabilidades específicas, é necessário saber a configuração exata do sistema/aplicativo/*patches* no sistema testado. Se esses dados não forem conhecidos no momento do teste, não é necessariamente possível explorar uma determinada vulnerabilidade com sucesso (por exemplo, obter *shell* reversa remota). No entanto, ainda é possível travar ou reiniciar um processo ou sistema testado. Nesse caso, convém que o objeto testado também seja considerado vulnerável.

Os métodos podem incluir as seguintes atividades:

— entrevistas com pessoas e usuários;

— questionários;

— inspeção física;

— análise documental.

### A.2.5.4 Cenários operacionais

Em uma abordagem baseada em ativos, cenários operacionais podem ser construídos analisando os diferentes caminhos, dentro dos ativos de suporte, que as fontes de risco podem usar para alcançar os ativos do negócio e seu DES.

Analisar esses cenários pode ajudar a investigar a abordagem baseada em eventos.

Um ataque bem-sucedido é muitas vezes o resultado da exploração de várias falhas. Ataques intencionais geralmente seguem uma abordagem sequenciada. Este último explora de forma coordenada várias vulnerabilidades de natureza de TI, organizacional ou física. Tal abordagem baseada na exploração simultânea de falhas separadas pode ter pesadas consequências, embora as vulnerabilidades exploradas possam ser insignificantes quando são consideradas individualmente.

Os cenários analisados podem ser estruturados de acordo com uma sequência típica de ataque. Vários modelos existem e podem ser usados (por exemplo, o modelo da cadeia de *cyber kill chain*). Convém que a abordagem permita identificar os ativos críticos de suporte que podem ser usados como vetores de entrada ou exploração, ou como um ponto de propagação para o ataque modelado.

Esses cenários podem ser representados na forma de gráficos ou diagramas de ataque, úteis para representar os métodos de ataque do atacante.

### A.2.6 Exemplos de cenários aplicáveis em ambas as abordagens

Os cenários de risco podem ser construídos usando uma abordagem baseada em eventos, uma abordagem baseada em ativos ou ambos.

A Figura A.4 apresenta o processo de avaliação de riscos com base em cenários de risco.

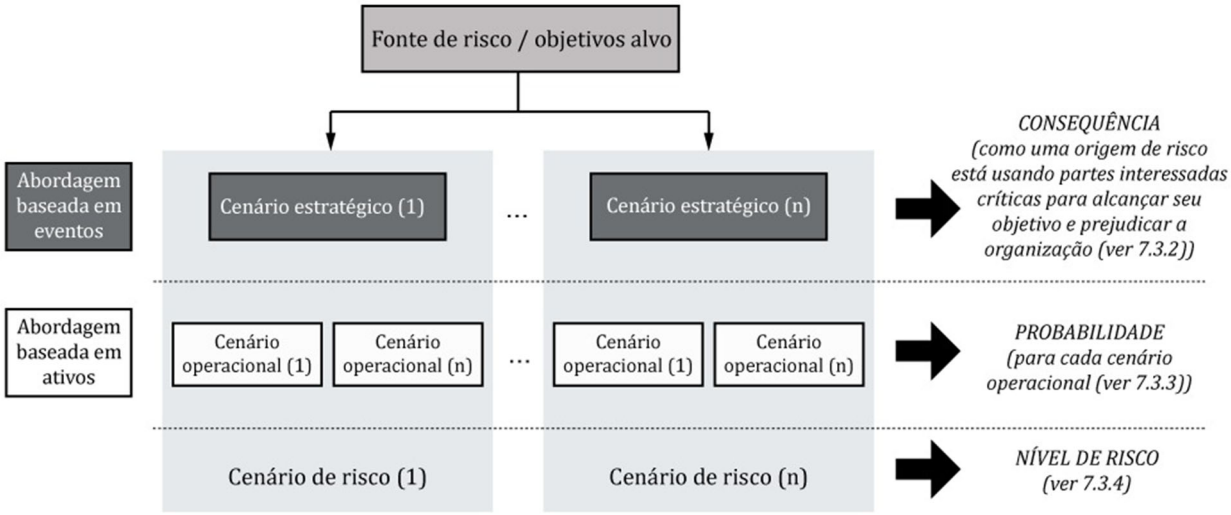



**Figura A.4 – Processo de avaliação de riscos com base em cenários de risco**

A Tabela A.12 mostra exemplos de cenários de risco e os *links* com as abordagens baseadas em ativos/eventos e fontes de risco.

**Tabela A.12 – Exemplos de cenários de risco em ambas as abordagens**

| Fonte de risco | Objetivo de alvo DES | Cenário estratégico de risco (Abordagem baseada em eventos) | Cenário de risco operacional (Abordagem baseada em ativos) |
|---|---|---|---|
| Estado autoritário | Aquisição de um vetor de ataque estratégico | Subvertendo infraestrutura crítica | Implantação de *malware* oculto e persistente na cadeia de suprimentos |
| Crime organizado | Desenvolvimento de atividades ilegais | Exploração da infraestrutura portuária | Infiltração do sindicato dos portuários |
| | | | Assunção do controle de um sistema informatizado de gestão de fluxo |
| | | Fraude de carrossel fiscal | Criação empresas de fachada para realizar trocas falsas no mercado de impostos sobre o carbono |
| | | Extorsão | Distribuição de *ransomware* |
| Negócios agressivos | Obtenção de um monopólio de mercado | Influência sobre o regulador | Corrompendo um tomador de decisão |
| | | Remoção de concorrentes | Campanha de difamação nas redes sociais |

### A.2.7 Monitoramento de eventos relacionados a riscos

O monitoramento de eventos relacionados ao risco é a identificação de fatores que podem influenciar um cenário de risco de segurança da informação definido em 10.5.2.

Nesse contexto, os fatores são identificados como um conjunto de elementos que permitem detectar um comportamento inesperado em relação a um determinado ativo e que podem ser integrados às capacidades de monitoramento e ferramentas da organização para determinar o gatilho de um cenário de risco de segurança da informação.

O monitoramento de eventos relacionados ao risco pode ser definido utilizando diversos indicadores provenientes de cenários operacionais ou cenários estratégicos, ambos introduzidos em 7.2.1. Podem ser de natureza diferente (técnica, organizacional, comportamental, resultados de auditorias, etc.). Os eventos são monitorados de acordo com prioridades definidas, como magnitude das consequências e probabilidade do evento.

A Tabela A.13 fornece um exemplo de uma descrição do cenário de risco de segurança da informação com seus eventos relacionados ao monitoramento associados.

**Tabela A.13 – Exemplo de cenário de risco e monitoramento da relação de eventos relacionados ao risco**

| Componentes de risco | Exemplos | Eventos para monitorar |
|---|---|---|
| Cenário estratégico (com base em eventos) | Documentos confidenciais são destruídos por um administrador | |
| Eventos em causa | Perda de documentos críticos | |
| Gravidade da consequência | Medida descritiva: alta | |
| Cenários operacionais (com base em ativos) | Uso dos direitos do administrador para destruir os documentos confidenciais acessando diretamente o banco de dados | → Detecção de um acesso direto ao banco de dados fora do horário normal de trabalho |
| | Acesso raiz para modificar a data/hora do sistema | |
| | Infecção por *malware* da estação de trabalho do administrador com uma propagação no banco de dados | → Detecção de operações que impactam um grande volume de dados (Destruição) |
| Probabilidade | Medida descritiva: média | |
| Fonte de risco | Administrador | |
| Objetivo de alvo | Comprometendo a disponibilidade de documentos sensíveis | |
| DES | Comprometendo o sistema | |
| Controles de segurança | Implementação de estratégia de *backup* | |
| | Solução *anti-malware* | |
| | Implementação de NTP | |
| | Endurecimento do SO | |
| | Restrição de direitos de acesso aos dados operacionais | |

O modelo SFDT (*Source-Function-Destination-Trigger,* Fonte-Função-Destino-Gatilho) permite construir eventos relacionados ao risco de monitoramento, onde:

— fonte: indica de onde vem o evento/técnica (quem e por quê?) e pode estar associado aos recursos A.2.3;

— função: indica o tipo de evento/técnica realizada pelo atacante (o quê?);

— destino: indica sobre qual é a técnica ou evento (em qual principal dos ativos de suporte?);

— gatilho: indica quais condições permitem detectar e identificar o cenário de risco (resultados do ataque).

Um exemplo da aplicação do modelo SFDT é apresentado na Figura A.5.

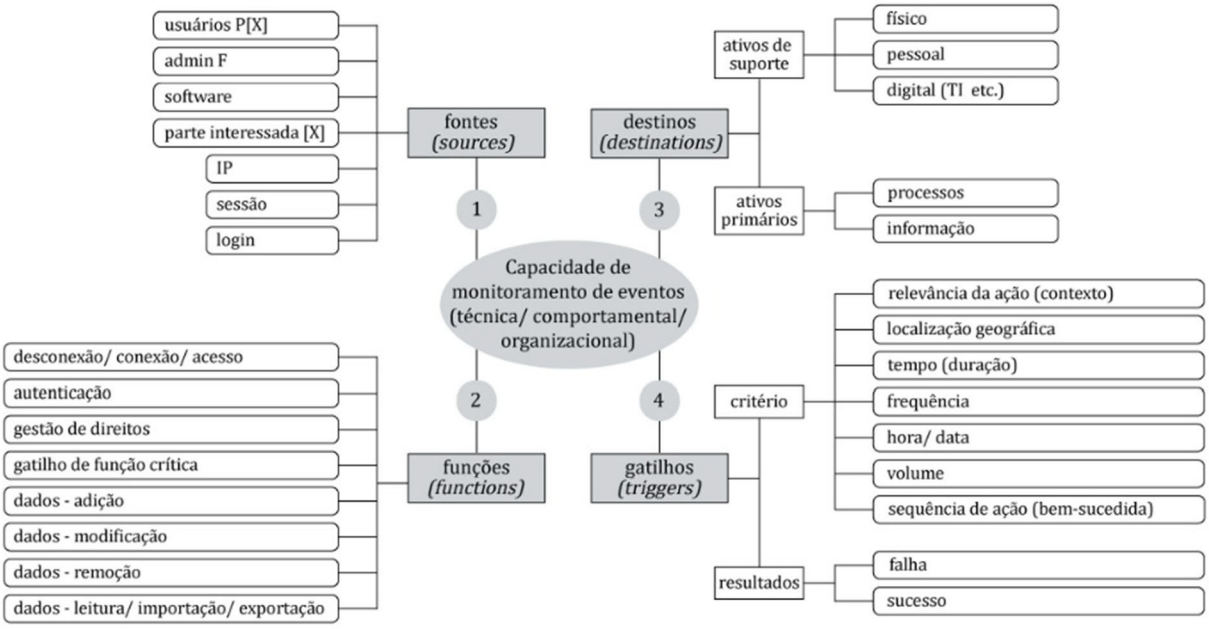



**Figura A.5 – Exemplo de aplicação do modelo SFDT**

Para assegurar que um evento relacionado ao risco de monitoramento seja eficaz e eficiente para monitorar um cenário de risco de segurança da informação, é necessário determinar seus indicadores.

Os indicadores de eventos relacionados ao risco de monitoramento são:

— nível de risco do cenário de risco que está sendo monitorado;

— eficácia, capacidade dos eventos relacionados ao risco para monitorar um cenário de risco;

— eficiência, relação entre alerta positivo verdadeiro e falso positivo, ou o custo da caracterização.

# Bibliografia

[1] ISO 17666:2016, *Space systems – Risk management*

[2] ABNT NBR ISO/IEC 27001:2022, *Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos*

[3] ABNT NBR ISO/IEC 27003, *Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Orientação*

[4] ABNT NBR ISO/IEC 27004, *Tecnologia da Informação – Técnicas de segurança – Gestão de segurança da informação – Monitoramento, medição, análise e avaliação*

[5] ABNT NBR ISO/IEC 27014, *Segurança da Informação, segurança cibernética e proteção à privacidade – Governança da segurança da informação*

[6] ISO/IEC/TR 27016, *Information technology – Security techniques – Information security management – Organizational economics*

[7] ABNT NBR ISO/IEC 27017, *Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação com base na ABNT NBR ISO/IEC 27002 para serviços em nuvem*

[8] ABNT NBR ISO/IEC 27701, *Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes*

[9] ABNT NBR ISO 31000:2018, *Gestão de riscos – Diretrizes*

[10] ABNT NBR IEC 31010:2021, *Gestão de riscos – Técnicas para o processo de avaliação de riscos*

[11] ABNT ISO Guia 73:2009, *Gestão de riscos – Vocabulário*