

NORMA
BRASILEIRA

ABNT NBR
ISO/IEC
27005

Terceira edição
24.10.2019

**Tecnologia da informação — Técnicas de
segurança — Gestão de riscos de segurança da
informação**

*Information technology — Security techniques — Information security risk
management*

ICS 35.040

ISBN 978-85-07-08295-8



ASSOCIAÇÃO
BRASILEIRA
DE NORMAS
TÉCNICAS

Número de referência
ABNT NBR ISO/IEC 27005:2019
66 páginas

© ISO/IEC 2018 - © ABNT 2019



© ISO/IEC 2018

Todos os direitos reservados. A menos que especificado de outro modo, nenhuma parte desta publicação pode ser reproduzida ou utilizada por qualquer meio, eletrônico ou mecânico, incluindo fotocópia e microfilme, sem permissão por escrito da ABNT, único representante da IEC no território brasileiro.

© ABNT 2019

Todos os direitos reservados. A menos que especificado de outro modo, nenhuma parte desta publicação pode ser reproduzida ou utilizada por qualquer meio, eletrônico ou mecânico, incluindo fotocópia e microfilme, sem permissão por escrito da ABNT.

ABNT

Av. Treze de Maio, 13 - 28º andar

20031-901 - Rio de Janeiro - RJ

Tel.: + 55 21 3974-2300

Fax: + 55 21 3974-2346

abnt@abnt.org.br

www.abnt.org.br

Sumário

Página

Prefácio Nacional	vi
Introdução	vii
1 Escopo	1
2 Referência normativa	1
3 Termos e definições	1
4 Organização deste documento	1
5 Contextualização	2
6 Visão geral do processo de gestão de riscos de segurança da informação	3
7 Definição do contexto	7
7.1 Considerações gerais	7
7.2 Critérios básicos	7
7.2.1 Abordagem da gestão de riscos	7
7.2.2 Critérios para a avaliação de riscos	8
7.2.3 Critérios de impacto	8
7.2.4 Critérios para a aceitação do risco	8
7.3 Escopo e limites	9
7.4 Organização para gestão de riscos de segurança da informação	10
8 Processo de avaliação de riscos de segurança da informação	10
8.1 Descrição geral do processo de avaliação de riscos de segurança da informação	10
8.2 Identificação de riscos	11
8.2.1 Introdução à identificação de riscos	11
8.2.2 Identificação dos ativos	12
8.2.3 Identificação das ameaças	12
8.2.4 Identificação dos controles existentes	13
8.2.5 Identificação das vulnerabilidades	14
8.2.6 Identificação das consequências	15
8.3 Análise de riscos	15
8.3.1 Metodologias de análise de riscos	15
8.3.2 Avaliação das consequências	17
8.3.3 Avaliação da probabilidade dos incidentes	18
8.3.4 Determinação do nível de risco	19
8.4 Avaliação de riscos	19
9 Tratamento do risco de segurança da informação	20
9.1 Descrição geral do processo de tratamento do risco	20
9.2 Modificação do risco	22
9.3 Retenção do risco	23
9.4 Ação de evitar o risco	24
9.5 Compartilhamento do risco	24
10 Aceitação do risco de segurança da informação	24
11 Comunicação e consulta do risco de segurança da informação	25
12 Monitoramento e análise crítica de riscos de segurança da informação	26

12.1	Monitoramento e análise crítica dos fatores de risco	26
12.2	Monitoramento, análise crítica e melhoria do processo de gestão de riscos.....	27
Anexo A (informativo) Definindo o escopo e os limites do processo de gestão de riscos de		
	segurança da informação	29
A.1	Estudo da organização	29
A.2	Lista de restrições que afetam a organização.....	30
A.3	Lista de restrições que afetam o escopo.....	32
Anexo B (informativo) Identificação e valoração dos ativos e avaliação do impacto		
B.1	Exemplos de identificação de ativos.....	34
B.1.1	Generalidades.....	34
B.1.2	Identificação dos ativos primários	34
B.1.3	Lista e descrição de ativos de suporte	35
B.2	Valoração dos Ativos	39
B.2.1	Generalidades.....	39
B.2.2	Critérios.....	40
B.2.3	Definição de um denominador comum	40
B.2.4	Escala de medição	42
B.2.5	Dependências	42
B.2.6	Saída.....	43
B.3	Avaliação do Impacto.....	43
Anexo C (informativo) Exemplos de ameaças comuns.....		
Anexo D (informativo) Vulnerabilidades e métodos de avaliação de vulnerabilidades		
D.1	Exemplos de vulnerabilidades.....	49
D.2	Métodos para a avaliação de vulnerabilidades técnicas.....	53
Anexo E (informativo) Abordagens para o processo de avaliação de riscos de segurança da		
	informação	55
E.1	Processo de avaliação de riscos de segurança da informação – Enfoque de alto nível	55
E.2	Processo detalhado de avaliação de riscos de segurança da informação	57
E.2.1	Generalidades.....	57
E.2.2	Exemplo 1 – Matriz com valores predefinidos	57
E.2.3	Exemplo 2 – Ordenação de Ameaças em função do Risco	60
E.2.4	Exemplo 3 – Avaliando a probabilidade e as possíveis consequências dos riscos.....	60
Anexo F (informativo) Restrições para a modificação do risco		
Bibliografia.....		
66		

Figuras

Figura 1 – O processo de gestão de riscos	4
Figura 2 – Processo de gestão de riscos de segurança da informação	5
Figura 3 – A atividade de tratamento do risco	21

Tabelas

Tabela E.1	59
Tabela E.2	60
Tabela E.3	60
Tabela E.4	61
Tabela E.5	61



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 ABNT 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 Computadores e Processamento de Dados (ABNT/CB-021), pela Comissão de Estudo de Técnicas de Segurança (CE-021:000.027). O Projeto de Revisão circulou em Consulta Nacional conforme Edital nº 08, de 09.08.2019 a 09.09.2019.

A ABNT NBR ISO/IEC 27005 é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 27005:2018, que foi elaborada pelo *Technical Committee Information technology* (ISO/IEC JTC 1), *Subcommittee IT Security techniques* (SC 27).

A ABNT NBR ISO/IEC 27005:2019 cancela e substitui a ABNT NBR ISO/IEC 27005:2011, a qual foi tecnicamente revisada.

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

Scope

This document provides guidelines for information security risk management.

This document supports the general concepts specified in ABNT NBR ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Knowledge of the concepts, models, processes and terminologies described in ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 is important for a complete understanding of this document.

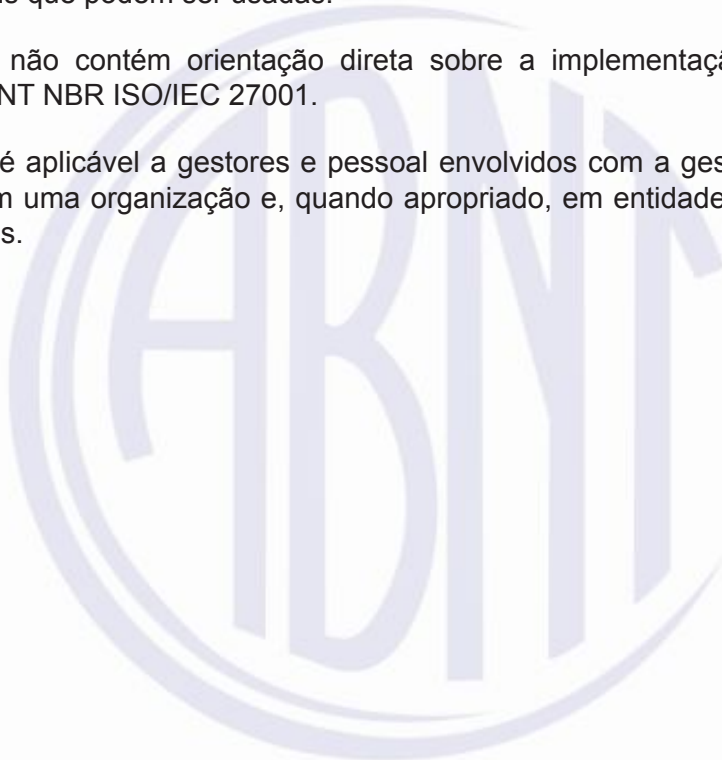
This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.

Introdução

Este documento fornece diretrizes para a gestão de riscos de segurança da informação em uma organização. Entretanto, este documento não fornece um método específico para a gestão de riscos de segurança da informação. Cabe à organização definir sua abordagem ao processo de gestão de riscos, considerando, por exemplo, o escopo de um sistema de gestão de segurança (SGSI), o contexto da gestão de riscos e o seu setor de atividade econômica. Há várias metodologias que podem ser utilizadas de acordo com a estrutura descrita neste documento para implementar os requisitos de um SGSI. Este documento é baseado no método de identificação de riscos de ativos, ameaças e vulnerabilidades, que não é mais requerido pela ABNT NBR ISO/IEC 27001. Existem outras abordagens que podem ser usadas.

Este documento não contém orientação direta sobre a implementação dos requisitos do SGSI fornecidos na ABNT NBR ISO/IEC 27001.

Este documento é aplicável a gestores e pessoal envolvidos com a gestão de riscos de segurança da informação em uma organização e, quando apropriado, em entidades externas que dão suporte a essas atividades.



Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação

1 Escopo

Este documento fornece diretrizes para o processo de gestão de riscos de segurança da informação.

Este documento estabelece os conceitos gerais especificados na ABNT NBR ISO/IEC 27001 e foi elaborado para facilitar uma implementação satisfatória da segurança da informação tendo como base uma abordagem de gestão de riscos.

O conhecimento dos conceitos, modelos, processos e terminologias descritos na ABNT NBR ISO/IEC 27001 e na ABNT NBR ISO/IEC 27002 é importante para um entendimento completo deste documento.

Este documento é aplicável a todos os tipos de organização (por exemplo: empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos), que pretendam gerenciar os riscos que podem comprometer a segurança da informação da organização.

2 Referência normativa

O seguinte documento é referenciado no texto de tal forma que partes ou todo o seu conteúdo constituem requisitos deste documento. Para as referências com datas, apenas a edição citada se aplica. Para as referências sem data, aplica-se apenas a edição mais recente do referido documento (incluindo quaisquer correções).

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 a seguir e os da ISO/IEC 27000.

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

- Plataforma de navegação online ISO: disponível em <https://www.iso.org/obp>
- IEC Electropedia: disponível em <http://www.electropedia.org/>

4 Organização deste documento

Este documento contém a descrição do processo de gestão de riscos de segurança da informação e das suas atividades.

As informações sobre o contexto histórico são apresentadas na Seção 5.

Uma visão geral do processo de gestão de riscos de segurança da informação é apresentada na Seção 6.

Todas as atividades de gestão de riscos de segurança da informação, apresentadas na Seção 6, são descritas nas seguintes seções:

- definição do contexto na Seção 7,
- processo de avaliação de riscos na Seção 8,
- tratamento do risco na Seção 9,
- aceitação do risco na Seção 10,
- comunicação e consulta do risco na Seção 11,
- monitoramento e análise crítica de riscos na Seção 12.

Informações adicionais para as atividades de gestão de riscos de segurança da informação são apresentadas nos Anexos. A definição do contexto é detalhada no Anexo A (Definindo o escopo e os limites do processo de gestão de riscos de segurança da informação). A identificação e valoração dos ativos e a avaliação do impacto são discutidas no Anexo B. O Anexo C fornece exemplos de ameaças típicas e o Anexo D apresenta vulnerabilidades e métodos para avaliação de vulnerabilidades. Exemplos de abordagens para o processo de avaliação de riscos de segurança da informação são apresentados no Anexo E.

Restrições relativas à modificação do risco são apresentadas no Anexo F.

As atividades de gestão de riscos, como apresentadas da Seção 7 até a Seção 12, estão estruturadas da seguinte forma:

Entrada: Identifica as informações necessárias para realizar a atividade.

Ação: Descreve a atividade.

Diretrizes para implementação: Fornece orientação para a execução da ação. Algumas destas orientações podem não ser adequadas em todos os casos e assim sendo, outras maneiras de se executar a ação podem ser mais apropriadas.

Saída: Identifica as informações resultantes da execução da atividade.

5 Contextualização

Uma abordagem sistemática de gestão de riscos de segurança da informação é necessária para se identificar as necessidades da organização em relação aos requisitos de segurança da informação e para criar um sistema de gestão de segurança da informação (SGSI) que seja eficaz. Convém que esta abordagem seja adequada ao ambiente da organização e em particular esteja alinhada com o processo maior de gestão de riscos corporativos. Convém que os esforços de segurança lidem com riscos de maneira efetiva e no tempo apropriado, onde e quando forem necessários. Convém que a gestão de riscos de segurança da informação seja parte integrante das atividades de gestão da segurança da informação e seja aplicada tanto à implementação quanto à operação cotidiana de um SGSI.

Convém que a gestão de riscos de segurança da informação seja um processo contínuo. Convém que o processo defina o contexto interno e externo, avalie os riscos e os trate usando um plano de tratamento a fim de implementar as recomendações e decisões. Convém que a gestão de riscos analise os possíveis acontecimentos e suas consequências, antes de decidir o que será feito e quando será feito, a fim de reduzir os riscos a um nível aceitável.

Convém que a gestão de riscos de segurança da informação contribua para o seguinte:

- identificação de riscos;
- processo de avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência;
- comunicação e entendimento da probabilidade e das consequências destes riscos;
- estabelecimento da ordem prioritária para tratamento do risco;
- priorização das ações para reduzir a ocorrência dos riscos;
- envolvimento das partes interessadas nas decisões de gestão de riscos tomadas e para informação sobre a situação da gestão de riscos;
- eficácia do monitoramento do tratamento do risco;
- monitoramento e análise crítica periódica dos riscos e do processo de gestão de riscos;
- coleta de informações de forma a melhorar a abordagem da gestão de riscos;
- treinamento de gestores e pessoal sobre os riscos e as ações para mitigá-los.

O processo de gestão de riscos de segurança da informação pode ser aplicado à organização como um todo, a uma área específica da organização (por exemplo: um departamento, um local físico, um serviço), a qualquer sistema de informações, a controles já existentes, planejados ou apenas a aspectos particulares de um controle (por exemplo: o plano de continuidade de negócios).

6 Visão geral do processo de gestão de riscos de segurança da informação

Uma visão de alto nível do processo de gestão de riscos é especificado na ABNT NBR ISO 31000 e apresentado na Figura 1.

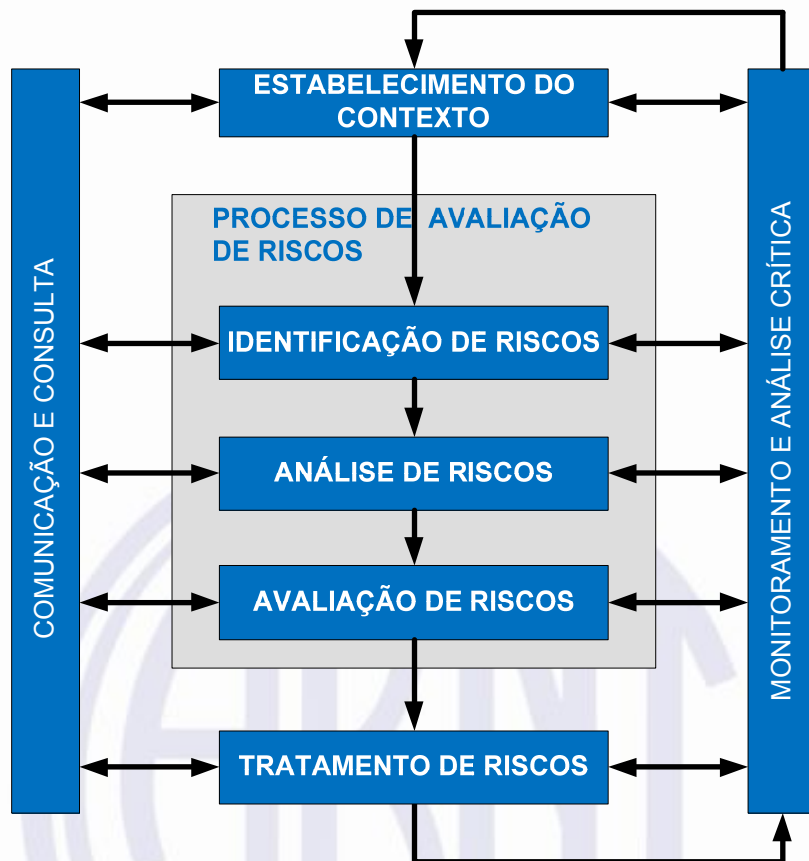


Figura 1 – O processo de gestão de riscos

A Figura 2 apresenta como este documento é aplicado ao processo de gestão de riscos.

O processo de gestão de riscos de segurança da informação consiste na definição do contexto (Seção 7), processo de avaliação de riscos (Seção 8), tratamento do risco (Seção 9), aceitação do risco (Seção 10), comunicação e consulta do risco (Seção 11) e monitoramento e análise crítica de riscos (Seção 12).

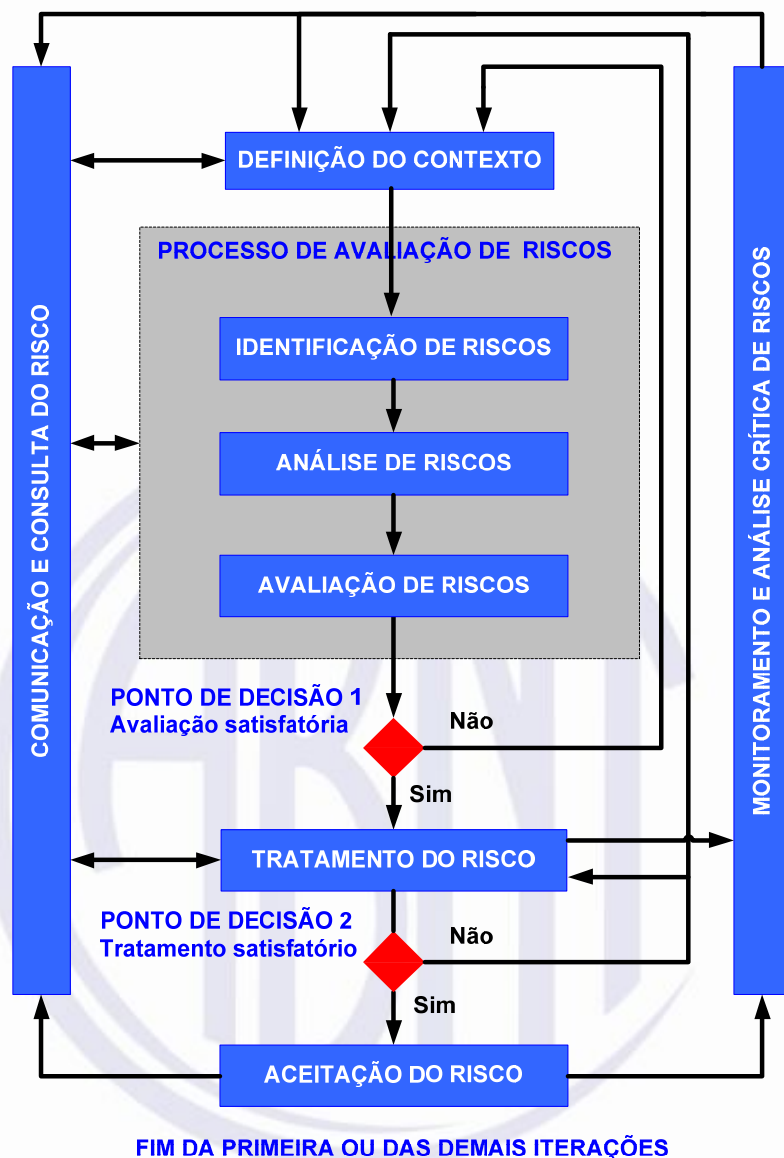


Figura 2 – Processo de gestão de riscos de segurança da informação

Como mostra a Figura 2, o processo de gestão de riscos de segurança da informação pode ser iterativo para o processo de avaliação de riscos e/ou para as atividades de tratamento do risco. Um enfoque iterativo na execução do processo de avaliação de riscos torna possível aprofundar e detalhar a avaliação em cada repetição. O enfoque iterativo permite minimizar o tempo e o esforço despendidos na identificação de controles e, ainda assim, assegura que riscos de alto impacto ou de alta probabilidade possam ser adequadamente avaliados.

Primeiramente, o contexto é estabelecido. Em seguida, executa-se um processo de avaliação de riscos. Se ele fornecer informações suficientes para que se determine de forma eficaz as ações necessárias para reduzir os riscos a um nível aceitável, então a tarefa está completa e o tratamento do risco pode ser realizado. Por outro lado, se as informações forem insuficientes, executa-se uma outra iteração do processo de avaliação de riscos, revisando-se o contexto (por exemplo: os critérios de avaliação de riscos, de aceitação do risco ou de impacto), possivelmente em partes limitadas do escopo (ver Figura 2, Ponto de Decisão 1).

A eficácia do tratamento do risco depende dos resultados do processo de avaliação de riscos.

Notar que o tratamento do risco envolve um processo cíclico para:

- avaliar um tratamento do risco;
- decidir se os níveis de risco residual são aceitáveis;
- gerar um novo tratamento do risco se os níveis de risco não forem aceitáveis; e
- avaliar a eficácia do tratamento.

É possível que o tratamento do risco não resulte em um nível de risco residual que seja aceitável. Nessa situação, pode ser necessária uma outra iteração do processo de avaliação de riscos, com mudanças nas variáveis do contexto (por exemplo: os critérios para o processo de avaliação de riscos, de aceitação do risco e de impacto), seguida por uma fase adicional de tratamento do risco (ver Figura 2, Ponto de Decisão 2).

A atividade de aceitação do risco tem de assegurar que os riscos residuais sejam explicitamente aceitos pelos gestores da organização. Isto é especialmente importante em uma situação em que a implementação de controles é omitida ou adiada, por exemplo, devido aos custos.

Durante o processo de gestão de riscos de segurança da informação, é importante que os riscos e a forma com que são tratados sejam comunicados ao pessoal das áreas operacionais e gestores apropriados. Mesmo antes do tratamento do risco, informações sobre riscos identificados podem ser muito úteis para gerenciar incidentes e ajudar a reduzir possíveis prejuízos. A conscientização dos gestores e pessoal em relação aos riscos, à natureza dos controles aplicados para mitigá-los e às áreas definidas como de interesse pela organização, auxiliam a lidar com os incidentes e eventos não previstos da maneira mais efetiva. Convém que os resultados detalhados de cada atividade do processo de gestão de riscos de segurança da informação, assim como as decisões sobre o processo de avaliação de riscos e sobre o tratamento do risco (representadas pelos dois pontos de decisão na Figura 2), sejam documentados.

A ABNT NBR ISO/IEC 27001 especifica que os controles implementados no escopo, limites e contexto do SGSI devem ser baseados em risco. A aplicação de um processo de gestão de riscos de segurança da informação pode satisfazer a esse requisito. Há várias abordagens pelas quais os controles podem ser determinados para implementar as opções de tratamento do risco escolhidas.

Convém que a organização estabeleça, implemente e mantenha um procedimento para identificar os requisitos legais aplicáveis a:

- a seleção de critérios para avaliação de riscos (7.2.2), impacto de riscos (7.2.3) e aceitação do risco (7.2.4);
- a definição do escopo e dos limites da gestão de riscos de segurança da informação (7.3 e A.2);
- a avaliação de riscos (8.4);
- o tratamento do risco de (9.1) e implementação de planos de redução de riscos (9.2 e Anexo F);
- o monitoramento, revisão e melhoria da gestão de riscos (12.2);
- a identificação de ativos (B.1.3) e avaliação de ativos (B.2.3); e
- a estimativa de risco (ver exemplos em E.2.1).

7 Definição do contexto

7.1 Considerações gerais

Entrada: Todas as informações sobre a organização relevantes para a definição do contexto da gestão de riscos de segurança da informação.

Ação: Convém que os contextos externo e interno para gestão de riscos de segurança da informação sejam estabelecidos, o que envolve a definição dos critérios básicos necessários para a gestão de riscos de segurança da informação (7.2), a definição do escopo e dos limites (7.3) e o estabelecimento de uma organização apropriada para operar a gestão de riscos de segurança da informação (7.4).

Diretrizes para implementação:

É essencial determinar o propósito da gestão de riscos de segurança da informação, pois ele afeta o processo em geral e a definição do contexto em particular. Esse propósito pode ser:

- suporte a um SGSI;
- conformidade legal e evidência da devida diligência (“*due diligence*”);
- preparação de um plano de continuidade de negócios;
- preparação de um plano de resposta a incidentes; e
- descrição dos requisitos de segurança da informação para um produto, um serviço ou um mecanismo.

As diretrizes para implementação dos elementos da definição do contexto necessários para dar suporte a um SGSI são discutidas detalhadamente nas Seções 7.2, 7.3 e 7.4 a seguir.

Saída: A especificação dos critérios básicos; o escopo e os limites do processo de gestão de riscos de segurança da informação; e a organização responsável pelo processo.

7.2 Critérios básicos

7.2.1 Abordagem da gestão de riscos

Dependendo do escopo e dos objetivos da gestão de riscos, diferentes métodos podem ser aplicados. O método também pode ser diferente para cada iteração do processo.

Convém que um método de gestão de riscos apropriado seja selecionado ou desenvolvido e considere critérios básicos, como: critérios de avaliação de riscos, critérios de impacto e critérios de aceitação do risco.

Além disso, convém que a organização avalie se os recursos necessários estão disponíveis para:

- executar o processo de avaliação de riscos e estabelecer um plano de tratamento dos riscos;
- definir e implementar políticas e procedimentos, incluindo implementação dos controles selecionados;
- monitorar controles, e

- monitorar o processo de gestão de riscos de segurança da informação.

7.2.2 Critérios para a avaliação de riscos

Convém que os critérios para a avaliação de riscos sejam desenvolvidos para avaliar os riscos de segurança da informação na organização, considerando o seguinte:

- o valor estratégico do processo que trata as informações de negócio;
- a criticidade dos ativos de informação envolvidos;
- importância do ponto de vista operacional e dos negócios, da disponibilidade, da confidencialidade e da integridade, e
- expectativas e percepções das partes interessadas e consequências negativas para o valor de mercado (e a reputação).

Além disso, critérios para avaliação de riscos podem ser usados para especificar as prioridades para o tratamento do risco.

7.2.3 Critérios de impacto

NOTA A ABNT NBR ISO/IEC 31000 usa um conceito de “critério de consequência” em vez de “critério de impacto”.

Convém que os critérios de impacto sejam desenvolvidos e especificados em função do montante dos danos ou custos à organização causados por um evento relacionado à segurança da informação, considerando o seguinte:

- nível de classificação do ativo de informação afetado;
- ocorrências de violação da segurança da informação (por exemplo: perda da disponibilidade, da confidencialidade e/ou da integridade);
- operações comprometidas (internas ou de terceiros);
- perda de oportunidades de negócio e de valor financeiro;
- interrupção de planos e não cumprimento de prazos;
- dano à reputação.

7.2.4 Critérios para a aceitação do risco

Convém que os critérios para a aceitação do risco sejam desenvolvidos e especificados. Os critérios de aceitação do risco dependem frequentemente das políticas, metas e objetivos da organização, assim como dos interesses das partes interessadas.

Convém que a organização defina sua própria escala de níveis de aceitação do risco. Convém que os seguintes tópicos sejam considerados durante o desenvolvimento:

- critérios para a aceitação do risco podem incluir mais de um limite, representando um nível desejável de risco, porém precauções podem ser tomadas por gestores seniores para aceitar riscos acima desse nível desde que sob circunstâncias definidas;

- critérios para a aceitação do risco podem ser expressos como a razão entre o lucro estimado (ou outro benefício ao negócio) e o risco estimado;
- diferentes critérios para a aceitação do risco podem ser aplicados a diferentes classes de risco;
- critérios para a aceitação do risco podem incluir requisitos para um tratamento adicional futuro, por exemplo: um risco pode ser aceito se for aprovado e houver o compromisso de que ações para reduzi-lo a um nível aceitável serão tomadas dentro de um determinado período de tempo.

Critérios para a aceitação do risco podem ser diferenciados de acordo com o tempo de existência previsto do risco, por exemplo: o risco pode estar associado a uma atividade temporária ou de curto prazo. Convém que os critérios para a aceitação do risco sejam estabelecidos, considerando os seguintes itens:

- critérios de negócio;
- operações;
- tecnologia;
- finanças;
- fatores sociais e humanitários.

Mais informações podem ser encontradas no Anexo A.

7.3 Escopo e limites

Convém que a organização defina o escopo e os limites da gestão de riscos de segurança da informação.

O escopo do processo de gestão de riscos de segurança da informação precisa ser definido para assegurar que todos os ativos relevantes sejam considerados no processo de avaliação de riscos. Além disso, os limites precisam ser identificados para permitir o reconhecimento dos riscos que possam transpor esses limites.

Convém que as informações sobre a organização sejam reunidas para que seja possível determinar o ambiente em que ela opera e a relevância desse ambiente para o processo de gestão de riscos de segurança da informação.

Ao definir o escopo e os limites, convém que a organização considere as seguintes informações:

- objetivos estratégicos, políticas e estratégias da organização;
- processos de negócio;
- funções e estrutura da organização;
- política de segurança da informação da organização;
- a abordagem da organização à gestão de riscos;
- ativos de informação;

- localidades em que a organização se encontra e suas características geográficas;
- restrições que afetam a organização;
- expectativas das partes interessadas;
- ambiente sociocultural;
- interfaces (ou seja, a troca de informação com o ambiente).

Além disso, convém que a organização forneça justificativa para quaisquer exclusões do escopo.

Exemplos do escopo da gestão de riscos podem ser: uma aplicação de TI, a infraestrutura de TI, um processo de negócios ou uma parte definida da organização.

Informações adicionais podem ser encontradas no Anexo A.

7.4 Organização para gestão de riscos de segurança da informação

Convém que a organização e as responsabilidades para o processo de gestão de riscos de segurança da informação sejam estabelecidas e mantidas. A seguir estão os principais papéis e responsabilidades dessa organização:

- desenvolvimento do processo de gestão de riscos de segurança da informação adequado à organização;
- identificação e análise das partes interessadas;
- definição dos papéis e responsabilidades de todas as partes, internas e externas à organização;
- estabelecimento das relações necessárias entre a organização e as partes interessadas, das interfaces com as funções de alto nível de gestão de riscos da organização (por exemplo: a gestão de riscos operacionais), assim como das interfaces com outros projetos ou atividades relevantes;
- definição de alçadas para a tomada de decisões;
- especificação dos registros a serem mantidos.

Convém que essa organização seja aprovada pelos gestores apropriados da organização.

8 Processo de avaliação de riscos de segurança da informação

8.1 Descrição geral do processo de avaliação de riscos de segurança da informação

Entrada: Critérios básicos, escopo e limites, e organização do processo de gestão de riscos de segurança da informação que se está definindo.

Ação: Convém que os riscos sejam identificados, quantificados ou descritos qualitativamente, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização.

Diretrizes para implementação:

Um risco é a combinação das consequências que podem seguir após a ocorrência de um evento indesejado e da probabilidade da ocorrência deste. O processo de avaliação de riscos quantifica ou descreve o risco qualitativamente e capacita os gestores a priorizar os riscos de acordo com a sua gravidade percebida ou com outros critérios estabelecidos.

O processo de avaliação de riscos consiste nas seguintes atividades:

- identificação de riscos (8.2);
- análise de riscos (8.3);
- avaliação de riscos (8.4).

O processo de avaliação de riscos determina o valor dos ativos de informação, identifica as ameaças e vulnerabilidades aplicáveis existentes (ou que possam existir), identifica os controles existentes e seus efeitos no risco identificado, determina as consequências possíveis e, finalmente, prioriza os riscos derivados e os ordena de acordo com os critérios de avaliação de riscos estabelecidos na definição do contexto.

O processo de avaliação de riscos é executado frequentemente em duas (ou mais) iterações. Primeiramente, uma avaliação de alto nível é realizada para identificar os riscos potencialmente altos, os quais merecem uma avaliação mais aprofundada. A segunda iteração pode considerar com mais profundidade esses riscos potencialmente altos revelados na primeira iteração. Se ela não fornecer informações suficientes para avaliar o risco, então análises adicionais detalhadas precisam ser executadas, provavelmente em partes do escopo total e possivelmente usando um outro método.

Cabe à organização selecionar seu próprio método para o processo de avaliação de riscos baseado nos objetivos e na meta do processo de avaliação de riscos.

Uma discussão sobre métodos utilizados no processo de avaliação de riscos de segurança da informação pode ser encontrada no Anexo E.

Saída: Uma lista de riscos avaliados, ordenados por prioridade de acordo com os critérios de avaliação de riscos.

8.2 Identificação de riscos

8.2.1 Introdução à identificação de riscos

O propósito da identificação de riscos é determinar o que possa causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer. As etapas descritas nas próximas subseções servem para coletar dados de entrada para a atividade de análise de riscos.

Convém que a identificação de riscos inclua os riscos cujas fontes estejam ou não sob controle da organização, mesmo que a fonte ou a causa dos riscos não seja evidente.

NOTA Atividades descritas nas subseções subsequentes podem ser executadas em uma ordem diferente dependendo da metodologia aplicada.

8.2.2 Identificação dos ativos

Entrada: Escopo e limites para o processo de avaliação de riscos a ser executado; lista de componentes com responsáveis, localidade, função etc.

Ação: Convém que os ativos dentro do escopo estabelecido sejam identificados.

Diretrizes para implementação:

Um ativo é algo que tem valor para a organização e que, portanto, requer proteção. Para a identificação dos ativos, convém que se tenha em mente que um sistema de informação compreende mais do que *hardware* e *software*.

Convém que a identificação dos ativos seja executada com um detalhamento adequado que forneça informações suficientes para o processo de avaliação de riscos. O nível de detalhe usado na identificação dos ativos influencia na quantidade geral de informações reunidas durante o processo de avaliação de riscos. O detalhamento pode ser aprofundado em cada iteração do processo de avaliação de riscos.

Convém que um responsável seja identificado para cada ativo, para fornecer responsabilidade e responsabilização pelo ativo. O responsável pelo ativo pode não ter direitos de propriedade sobre este, mas tem responsabilidade sobre sua produção, desenvolvimento, manutenção, utilização e segurança, conforme apropriado. O responsável pelo ativo é frequentemente a pessoa mais adequada para determinar o valor do ativo para a organização (ver 8.3.2 sobre a valoração dos ativos).

O limite da análise crítica é o perímetro dos ativos da organização a serem considerados pelo processo de gestão de riscos de segurança da informação.

Mais informações sobre a identificação e valoração dos ativos, sob a perspectiva da segurança da informação, podem ser encontradas no Anexo B.

Saída: Uma lista de ativos com riscos a serem gerenciados, e uma lista dos processos de negócio relacionados aos ativos e suas relevâncias.

8.2.3 Identificação das ameaças

Entrada: Informações sobre ameaças obtidas a partir da análise crítica de incidentes, dos responsáveis pelos ativos, de usuários e de outras fontes, incluindo catálogos externos de ameaças.

Ação: Convém que as ameaças e suas fontes sejam identificadas.

Diretrizes para implementação:

Uma ameaça tem o potencial de comprometer ativos como informações, processos e sistemas e, por isso, também as organizações. Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais. Convém que tanto as fontes das ameaças acidentais, quanto as intencionais, sejam identificadas. Uma ameaça pode surgir de dentro ou de fora da organização. Convém que as ameaças sejam identificadas genericamente e por classe (por exemplo: ações não autorizadas, danos físicos, falhas técnicas) e, quando apropriado, ameaças específicas identificadas dentro das classes genéricas. Isto significa que, nenhuma ameaça é ignorada, incluindo as não previstas, mas que o volume de trabalho requerido é limitado.

Algumas ameaças podem afetar mais de um ativo. Nesses casos, elas podem provocar impactos diferentes, dependendo de quais ativos são afetados.

Dados de entrada para a identificação das ameaças e estimativa da probabilidade de ocorrência (ver 8.3.3) podem ser obtidos dos responsáveis pelos ativos ou dos usuários, do pessoal, dos gestores das instalações e dos especialistas em segurança da informação, de peritos em segurança física, do departamento jurídico e de outras organizações relevantes, incluindo organismos legais, autoridades climáticas, companhias de seguros e autoridades governamentais nacionais. Aspectos culturais e relacionados ao ambiente precisam ser considerados quando as ameaças são examinadas.

Convém que experiências internas de incidentes e avaliações anteriores das ameaças sejam consideradas na avaliação atual. Pode ser útil a consulta a outros catálogos de ameaças (talvez mais específico a uma organização ou negócio) a fim de completar a lista de ameaças genéricas, quando relevante. Catálogos de ameaças e estatísticas são disponibilizados por organismos setoriais, governos, organismos legais, companhias de seguro etc.

Quando forem usados catálogos de ameaças ou os resultados de uma avaliação anterior das ameaças, convém que se tenha consciência de que as ameaças relevantes estão sempre mudando, especialmente se o ambiente de negócio ou se os sistemas de informações mudarem.

Mais informações sobre tipos de ameaças podem ser encontradas no Anexo C.

Saída: Uma lista de ameaças com a identificação do tipo e da fonte das ameaças.

8.2.4 Identificação dos controles existentes

Entrada: Documentação dos controles, planos de implementação do tratamento do risco.

Ação: Convém que os controles existentes e os planejados sejam identificados.

Diretrizes para implementação:

Convém que a identificação dos controles existentes seja realizada para evitar custos e trabalho desnecessários, por exemplo: na duplicação de controles. Além disso, enquanto os controles existentes estiverem sendo identificados, convém que seja feita uma verificação para assegurar que eles estão funcionando corretamente – uma referência aos relatórios já existentes de auditoria do SGSI pode reduzir o tempo gasto nesta tarefa. Um controle que não funcione como esperado pode provocar o surgimento de vulnerabilidades. Convém que seja levada em consideração a possibilidade de um controle selecionado (ou estratégia) falhar durante sua operação e, sendo assim, controles complementares são requeridos para tratar efetivamente o risco identificado.

Convém que os controles que estão planejados para serem implementados de acordo com os planos de implementação de tratamento do risco também sejam considerados, juntamente com aqueles que já estão implementados.

Controles existentes ou planejados podem ser considerados ineficazes, insuficientes ou não justificados. Convém que um controle insuficiente ou não justificado seja verificado para determinar se convém que este seja removido, substituído por outro controle mais adequado ou se convém que o controle permaneça em vigor, por exemplo, em função dos custos.

Para a identificação dos controles existentes ou planejados, as seguintes atividades podem ser úteis:

- analisar criticamente os documentos contendo informações sobre os controles (por exemplo: os planos de implementação de tratamento do risco) se os processos de gestão de segurança da informação estão bem documentados, convém que todos os controles existentes ou planejados e a situação de sua implementação estejam disponíveis;

- verificar com as pessoas responsáveis pela segurança da informação (por exemplo: o responsável pela segurança da informação, o responsável pela segurança do sistema da informação, o gestor das instalações prediais, o gerente de operações) e com os usuários quais controles, relacionados ao processo de informação ou ao sistema de informação sob consideração, estão realmente implementados;
- analisar criticamente, no local, os controles físicos, comparando os controles implementados com a lista de quais convém que estejam presentes; e verificar se aqueles implementados estão funcionando efetiva e corretamente, ou
- analisar criticamente os resultados de auditorias.

Saída: Uma lista de todos os controles existentes e planejados, sua implementação e a situação de utilização.

8.2.5 Identificação das vulnerabilidades

Entrada: Uma lista de ameaças conhecidas, listas de ativos e controles existentes.

Ação: Convém que as vulnerabilidades que podem ser exploradas por ameaças para comprometer os ativos ou a organização sejam identificadas.

Diretrizes para implementação:

Vulnerabilidades podem ser identificadas nas seguintes áreas:

- organização;
- processos e procedimentos;
- rotinas de gestão;
- recursos humanos;
- ambiente físico;
- configuração do sistema de informação;
- *hardware*, *software* ou equipamentos de comunicação;
- dependência de entidades externas.

A presença de uma vulnerabilidade não causa prejuízo por si só, pois precisa haver uma ameaça presente para explorá-la. Uma vulnerabilidade que não tem uma ameaça correspondente pode não requerer a implementação de um controle no presente momento, mas convém que ela seja reconhecida como tal e monitorada, no caso de haver mudanças. Notar que um controle implementado, funcionando incorretamente ou sendo usado incorretamente, pode, por si só, representar uma vulnerabilidade. Um controle pode ser eficaz ou não, dependendo do ambiente no qual ele opera. Inversamente, uma ameaça que não tenha uma vulnerabilidade correspondente pode não resultar em um risco.

Vulnerabilidades podem estar ligadas a propriedades do ativo, as quais podem ser usadas de uma forma ou para um propósito diferente daquele para o qual o ativo foi adquirido ou desenvolvido. Vulnerabilidades decorrentes de diferentes fontes precisam ser consideradas, por exemplo, as intrínsecas ao ativo e as extrínsecas.

Exemplos de vulnerabilidades e métodos para avaliação de vulnerabilidades podem ser encontrados no Anexo D.

Saída: Uma lista de vulnerabilidades associadas aos ativos, ameaças e controles; uma lista de vulnerabilidades que não se refere a nenhuma ameaça identificada para análise.

8.2.6 Identificação das consequências

Entrada: Uma lista de ativos, uma lista de processos do negócio e uma lista de ameaças e vulnerabilidades, quando aplicável, relacionadas aos ativos e sua relevância.

Ação: Convém que sejam identificadas as consequências que a perda de confidencialidade, de integridade e de disponibilidade possam ter sobre os ativos.

Diretrizes para implementação:

Uma consequência pode ser, por exemplo, a perda da eficácia, condições adversas de operação, a perda de oportunidades de negócio, reputação afetada, prejuízo etc.

Essa atividade identifica o prejuízo ou as consequências para a organização que podem decorrer de um cenário de incidente. Um cenário de incidente é a descrição de uma ameaça explorando uma certa vulnerabilidade ou um conjunto delas em um incidente de segurança da informação. O impacto dos cenários de incidentes é determinado considerando os critérios de impacto definidos durante a atividade de definição do contexto. Ele pode afetar um ou mais ativos ou apenas parte de um ativo. Assim, aos ativos podem ser atribuídos valores correspondendo tanto aos seus custos financeiros, quanto às consequências ao negócio se forem danificados ou comprometidos. Consequências podem ser de natureza temporária ou permanente como no caso da destruição de um ativo.

Convém que as organizações identifiquem as consequências operacionais de cenários de incidentes em função de (mas não limitado a):

- investigação e tempo de reparo;
- tempo (de trabalho) perdido;
- oportunidade perdida;
- saúde e segurança;
- custo financeiro das competências específicas necessárias para reparar o prejuízo, e
- imagem, reputação e valor de mercado.

Detalhes sobre a avaliação de vulnerabilidades técnicas podem ser encontrados em B.3.

Saída: Uma lista de cenários de incidentes com suas consequências associadas aos ativos e processos do negócio.

8.3 Análise de riscos

8.3.1 Metodologias de análise de riscos

A análise de riscos pode ser empreendida com diferentes graus de detalhamento, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores

envolvendo a organização. Uma metodologia para a análise de riscos pode ser qualitativa ou quantitativa ou uma combinação de ambos, dependendo das circunstâncias. Na prática, a análise qualitativa é frequentemente utilizada em primeiro lugar para obter uma indicação geral do nível de risco e para revelar os grandes riscos. Depois, pode ser necessário efetuar uma análise quantitativa ou mais específica, nos grandes riscos. Isso ocorre porque normalmente é menos complexo e menos oneroso realizar análises qualitativas do que quantitativas.

Convém que a forma da análise seja coerente com o critério de avaliação de riscos desenvolvido como parte da definição do contexto.

Detalhes adicionais sobre as metodologias para a análise estão descritos a seguir:

a) Análise qualitativa de riscos:

A análise qualitativa utiliza uma escala com atributos qualificadores que descrevem a magnitude das consequências potenciais (por exemplo: pequena, média e grande) e a probabilidade dessas consequências ocorrerem. Uma vantagem da análise qualitativa é sua facilidade de compreensão por todas as pessoas envolvidas enquanto que uma desvantagem é a dependência da escolha subjetiva da escala.

Essas escalas podem ser adaptadas ou ajustadas para se adequarem às circunstâncias e descrições diferentes podem ser usadas para riscos diferentes. A análise qualitativa pode ser utilizada:

- como uma verificação inicial a fim de identificar riscos que requeiram uma análise mais detalhada;
- quando esse tipo de análise é suficiente para a tomada de decisões;
- quando os dados numéricos ou recursos são inadequados para uma análise quantitativa.

Convém que a análise qualitativa utilize informações e dados factuais quando disponíveis.

b) Análise quantitativa de riscos:

A análise quantitativa utiliza uma escala com valores numéricos (e não as escalas descritivas usadas na análise qualitativa) tanto para consequências quanto para a probabilidade, usando dados de diversas fontes. A qualidade da análise depende da exatidão e da integralidade dos valores numéricos e da validade dos modelos utilizados. A análise quantitativa, na maioria dos casos, utiliza dados históricos dos incidentes, proporcionando a vantagem de poder ser relacionada diretamente aos objetivos da segurança da informação e interesses da organização. Uma desvantagem é a falta destes dados sobre novos riscos ou sobre fragilidades da segurança da informação, criando assim uma ilusão de valor e precisão da avaliação do risco.

A forma na qual as consequências e a probabilidade são expressas e a forma em que elas são combinadas para fornecer um nível de risco varia de acordo com o tipo de risco e do propósito para o qual os resultados do processo de avaliação de riscos são usados. Convém que a incerteza e a variabilidade tanto das consequências, quanto da probabilidade, sejam consideradas na análise e comunicadas de forma eficaz.

8.3.2 Avaliação das consequências

Entrada: Uma lista de cenários de incidentes identificados como relevantes, incluindo a identificação de ameaças, vulnerabilidades, ativos afetados e consequências para os ativos e processos do negócio.

Ação: Convém que o impacto sobre o negócio da organização, que pode ser causado por incidentes (possíveis ou reais) relacionados à segurança da informação, seja avaliado considerando as consequências de uma violação da segurança da informação, como por exemplo: a perda da confidencialidade, da integridade ou da disponibilidade dos ativos.

Diretrizes para implementação:

Depois de identificar todos os ativos relevantes, convém que os valores atribuídos a esses ativos sejam considerados durante a avaliação das consequências.

Um conceito de impacto no negócio é usado para medir consequências. O valor do impacto ao negócio pode ser expresso de forma qualitativa ou quantitativa, porém um método para designar valores monetários geralmente pode fornecer mais informações úteis para a tomada de decisões e, consequentemente, permitir que o processo de tomada de decisão seja mais eficiente.

A valoração dos ativos começa com a classificação destes de acordo com sua criticidade, em função da importância dos ativos para a realização dos objetivos de negócios da organização. A valoração é então determinada de duas maneiras:

- o valor de reposição do ativo: o custo da recuperação e da reposição da informação (se for possível); e
- as consequências ao negócio relacionadas à perda ou ao comprometimento do ativo, como as possíveis consequências adversas de caráter empresarial, legal ou regulatórias causadas pela divulgação indevida, modificação, indisponibilidade e/ou destruição de informações ou de outros ativos de informação

Essa valoração pode ser determinada a partir de uma análise de impacto no negócio. O valor, determinado em função da consequência para o negócio, normalmente é significativamente mais elevado do que o simples custo de reposição, dependendo da importância do ativo para a organização na realização dos objetivos de negócios.

A valoração dos ativos representa um dos aspectos mais importantes na avaliação do impacto de um cenário de incidente, pois o incidente pode afetar mais de um ativo (por exemplo: os ativos dependentes) ou somente parte de um ativo. Diferentes ameaças e vulnerabilidades causam diferentes impactos sobre os ativos, como perda da confidencialidade, da integridade ou da disponibilidade. A avaliação das consequências está, portanto, relacionada à valoração dos ativos baseada na análise de impacto no negócio.

As consequências ou o impacto ao negócio podem ser determinados por meio da criação de modelos com os resultados de um evento, um conjunto de eventos ou por meio da extrapolação a partir de estudos experimentais ou dados passados.

As consequências podem ser expressas em função dos critérios monetários, técnicos ou humanos, de impacto ou de outro critério relevante para a organização. Em alguns casos, mais de um valor numérico é necessário para especificar as consequências tendo em vista os diferentes momentos, lugares, grupos ou situações.

Convém que as consequências expressas em tempo e valor financeiro sejam medidas com a mesma abordagem utilizada para a probabilidade da ameaça e as vulnerabilidades. A consistência deve ser mantida em relação à abordagem quantitativa ou qualitativa.

Mais informações sobre valoração dos ativos e sobre a avaliação do impacto podem ser encontradas no Anexo B.

Saída: Uma lista de consequências avaliadas referentes a um cenário de incidente, relacionadas aos ativos e critérios de impacto.

8.3.3 Avaliação da probabilidade dos incidentes

Entrada: Uma lista de cenários de incidentes relevantes identificados, incluindo a identificação de ameaças, ativos afetados, vulnerabilidades exploradas e consequências para os ativos e processos do negócio. Além disso, listas com todos os controles existentes e planejados, sua eficácia, implementação e *status* de utilização.

Ação: Convém que a probabilidade dos cenários de incidentes seja avaliada.

Diretrizes para implementação:

Depois de identificar os cenários de incidentes, é necessário avaliar a probabilidade de cada cenário e do impacto correspondente, usando técnicas de análise qualitativas ou quantitativas. Convém considerar a frequência da ocorrência das ameaças e a facilidade com que as vulnerabilidades podem ser exploradas, considerando o seguinte:

- a experiência passada e estatísticas aplicáveis referentes à probabilidade da ameaça;
- para fontes de ameaças intencionais: a motivação e as competências, que mudam ao longo do tempo, os recursos disponíveis para possíveis atacantes, bem como a percepção da vulnerabilidade e o poder da atração dos ativos para um possível atacante;
- para fontes de ameaças acidentais: os fatores geográficos como, por exemplo, proximidade a fábricas e refinarias de produtos químicos e petróleo, a possibilidade de eventos climáticos extremos e os fatores que poderiam acarretar erros humanos e o mau funcionamento de equipamentos;
- vulnerabilidades, tanto individualmente como em conjunto;
- os controles existentes e a eficácia com que eles reduzem as vulnerabilidades.

Por exemplo, um sistema de informação pode ter uma vulnerabilidade relacionada às ameaças de se forjar a identidade de um usuário e de se fazer mau uso de recursos. A vulnerabilidade relacionada ao uso forjado da identidade de um usuário pode ser alta devido, por exemplo, à falta de um mecanismo de autenticação de usuário. Por outro lado, a probabilidade de utilização indevida dos recursos pode ser baixa, apesar da falta de autenticação, pois os meios disponíveis para que isso possa acontecer são limitados.

Dependendo da necessidade de exatidão, ativos podem ser agrupados ou pode ser necessário dividir um ativo em seus componentes e relacionar estes aos cenários. Por exemplo, conforme a localidade geográfica, a natureza das ameaças a um mesmo tipo de ativo ou a eficácia dos controles existentes podem variar.

Saída: Probabilidade dos cenários de incidentes (no método quantitativo ou no qualitativo).

8.3.4 Determinação do nível de risco

Entrada: Uma lista de cenários de incidentes com suas consequências associadas aos ativos, processos de negócio e suas probabilidades (no método quantitativo ou no qualitativo).

Ação: Convém que o nível de risco seja determinado para todos os cenários de incidentes relevantes.

Diretrizes para implementação:

A análise de riscos designa valores para a probabilidade e para as consequências de um risco. Esses valores podem ser de natureza quantitativa ou qualitativa. A análise de riscos é baseada nas consequências e na probabilidade avaliadas. Além disso, ela pode considerar o custo-benefício, as preocupações das partes interessadas e outras variáveis, conforme apropriado para a avaliação de riscos. O risco estimado é uma combinação da probabilidade de um cenário de incidente e suas consequências.

Exemplos de diferentes abordagens ou métodos para análise de riscos de segurança da informação podem ser encontrados no Anexo E.

Saída: Uma lista de riscos com níveis de valores designados.

8.4 Avaliação de riscos

Entrada: Uma lista de riscos com níveis de valores designados e critérios para a avaliação de riscos.

Ação: Convém que o nível dos riscos seja comparado com os critérios de avaliação de riscos e com os critérios para a aceitação do risco.

Diretrizes para implementação:

A natureza das decisões relativas à avaliação de riscos e os critérios de avaliação de riscos usados para tomar essas decisões são decididos durante a definição do contexto. Convém que essas decisões e o contexto sejam revisitados detalhadamente nesse estágio em que se conhece mais sobre os riscos identificados. Para avaliar os riscos, convém que as organizações comparem os riscos estimados (usando os métodos ou abordagens selecionadas como abordado no Anexo E) com os critérios de avaliação de riscos definidos durante a definição do contexto.

Convém que os critérios de avaliação de riscos utilizados na tomada de decisões sejam consistentes com o contexto definido, externo e interno, relativo à gestão de riscos de segurança da informação e considerem os objetivos da organização, o ponto de vista das partes interessadas etc. As decisões tomadas durante a atividade de avaliação de riscos são baseadas principalmente no nível de risco aceitável. No entanto, convém que as consequências, a probabilidade e o grau de confiança na identificação e análise de riscos também sejam considerados. A agregação de vários pequenos ou médios riscos pode resultar em um risco total bem mais significativo e convém que seja tratado adequadamente.

Convém que os seguintes itens sejam considerados:

- *Propriedades da segurança da informação:* se um critério não é relevante para a organização (por exemplo: a perda da confidencialidade), então todos os riscos que impactam este critério podem não ser relevantes;
- *A importância do processo de negócios ou da atividade suportada por um determinado ativo ou conjunto de ativos:* se o processo tiver sido julgado de baixa importância, convém que os

riscos associados a ele sejam menos considerados do que os riscos que causam impactos em processos ou atividades mais importantes;

A avaliação de riscos usa o entendimento do risco obtido por meio da análise de riscos para a tomada de decisões sobre ações futuras. Convém que as decisões incluam:

- se convém que uma atividade seja realizada;
- as prioridades para o tratamento do risco, levando-se em conta os níveis estimados de risco .

Saída: Uma lista de riscos priorizados de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos.

9 Tratamento do risco de segurança da informação

9.1 Descrição geral do processo de tratamento do risco

Entrada: Uma lista de riscos priorizados de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos.

Ação: Convém que controles para modificar, reter, evitar ou compartilhar os riscos sejam selecionados e o plano de tratamento do risco seja definido.

Diretrizes para implementação:

Há quatro opções disponíveis para o tratamento do risco: modificação do risco (ver 9.2), retenção do risco (ver 9.3), ação de evitar o risco (ver 9.4) e compartilhamento do risco (ver 9.5).

A Figura 3 ilustra a atividade de tratamento do risco dentro do processo de gestão de riscos de segurança da informação como apresentado na Figura 2.

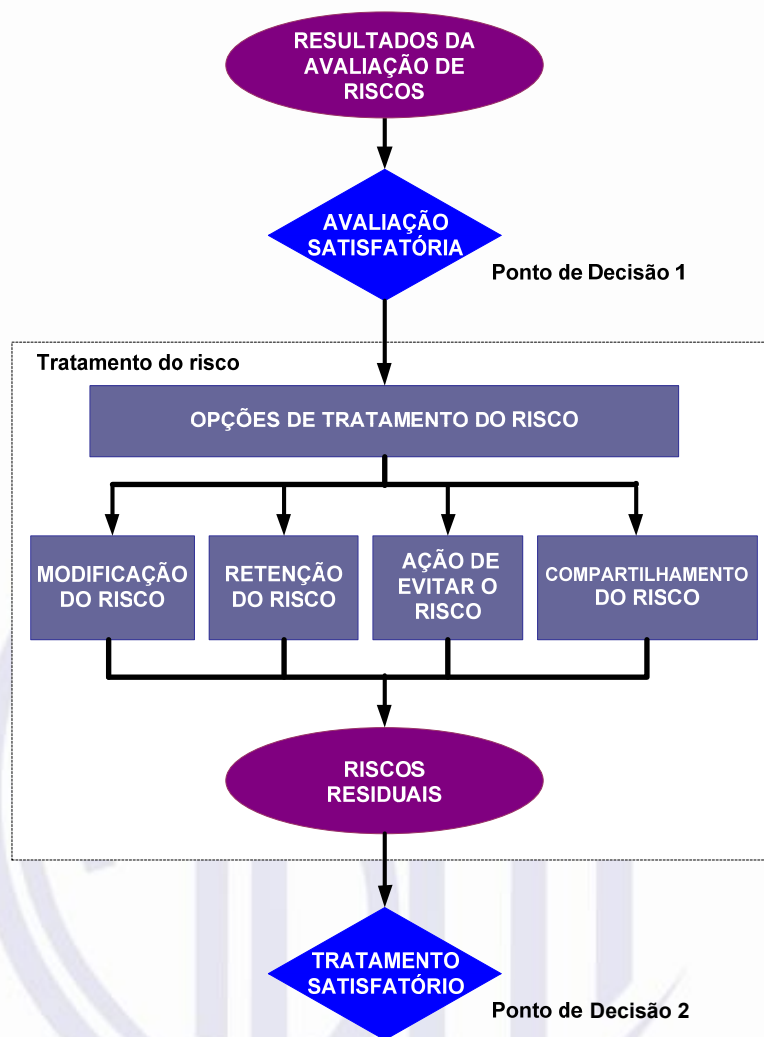


Figura 3 – A atividade de tratamento do risco

Convém que as opções de tratamento do risco sejam selecionadas com base no resultado do processo de avaliação de riscos, no custo esperado para implementação dessas opções e nos benefícios previstos.

Quando uma grande modificação do risco pode ser obtida com uma despesa relativamente pequena, convém que essas opções sejam implementadas. Outras opções para melhorias podem ser muito dispendiosas e uma análise precisa ser feita para verificar suas justificativas.

Em geral, convém que as consequências adversas do risco sejam reduzidas ao mínimo possível, independentemente de quaisquer critérios absolutos. Convém que os gestores considerem os riscos improváveis, porém graves. Nesse caso, controles que não forem justificáveis do ponto de vista estritamente econômico podem precisar ser implementados (por exemplo: controles de continuidade de negócios concebidos para tratar riscos de alto impacto específicos).

As quatro opções para o tratamento do risco não são mutuamente exclusivas. Às vezes, a organização pode se beneficiar substancialmente por uma combinação de opções, como a redução da probabilidade do risco, a redução de suas consequências e o compartilhamento ou retenção dos riscos residuais.

Algumas formas de tratamento do risco podem lidar com mais de um risco de forma efetiva (por exemplo: o treinamento e a conscientização em segurança da informação). Convém que um plano de tratamento do risco seja definido, identificando claramente a ordem de prioridade em que convém que as formas específicas de tratamento do risco sejam implementadas, assim como os seus prazos de execução. Prioridades podem ser estabelecidas usando várias técnicas, incluindo a ordenação dos riscos e a análise de custo-benefício. É de responsabilidade dos gestores da organização equilibrar os custos da implementação dos controles e o orçamento.

A identificação de controles existentes pode nos fazer concluir que estes excedem as necessidades atuais em função da comparação de custos, incluindo a manutenção. Se a remoção de controles redundantes e desnecessários tiver que ser considerada (especialmente se os controles têm altos custos de manutenção), convém que a segurança da informação e os fatores de custo sejam levados em conta. Devido à influência que os controles exercem uns sobre os outros, a remoção de controles redundantes pode reduzir a segurança em vigor como um todo. Além disso, talvez seja menos dispendioso deixar controles redundantes ou desnecessários em vigor do que removê-los.

Convém que as opções de tratamento do risco sejam consideradas levando-se em conta:

- como o risco é percebido pelas partes afetadas;
- as formas mais apropriadas de comunicação com as partes.

O risco para a organização é não estar em conformidade e convém que sejam implementadas opções de tratamento para limitar essa possibilidade. Convém que todas as restrições – organizacionais, técnicas, estruturais etc. – identificadas durante a atividade de definição do contexto, sejam levadas em conta durante o tratamento do risco.

Uma vez que o plano de tratamento do risco tenha sido definido, os riscos residuais precisam ser determinados. Isso envolve uma atualização ou uma repetição do processo de avaliação de riscos, considerando-se os efeitos previstos do tratamento do risco que foi proposto. Caso o risco residual ainda não satisfaça aos critérios para a aceitação do risco da organização, uma nova iteração do tratamento do risco pode ser necessária antes de se prosseguir à aceitação do risco.

Saída: O plano de tratamento do risco e os riscos residuais, sujeitos à decisão de aceitação por parte dos gestores da organização.

9.2 Modificação do risco

Ação: Convém que o nível de risco seja gerenciado por meio da inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e então considerado aceitável.

Diretrizes para implementação:

Convém que controles apropriados e devidamente justificados sejam selecionados para satisfazer aos requisitos identificados pelo processo de avaliação de riscos e do tratamento de riscos. Convém que essa seleção também leve em conta custos e prazos para a implementação de controles, além de aspectos técnicos, culturais e ambientais. Com frequência, é possível diminuir o custo total de propriedade de um sistema por meio de controles de segurança da informação apropriadamente selecionados.

Em geral, os controles podem fornecer um ou mais dos seguintes tipos de proteção: correção, eliminação, prevenção, minimização do impacto, dissuasão, detecção, recuperação, monitoramento e conscientização. Durante a seleção de controles, é importante pesar o custo da aquisição, implemen-

tação, administração, operação, monitoramento e manutenção dos controles em relação ao valor dos ativos sendo protegidos. Além disso, convém que o retorno do investimento, na forma da modificação do risco e da possibilidade de se explorar novas oportunidades de negócio em função da existência de certos controles, também seja considerado. Adicionalmente, convém considerar as competências especializadas que possam ser necessárias para definir e implementar novos controles ou modificar os existentes.

A ABNT NBR ISO/IEC 27002 fornece informações detalhadas sobre controles.

Há muitas restrições que podem afetar a seleção de controles. Restrições técnicas, como requisitos de desempenho, capacidade de gestão (requisitos de apoio operacional) e questões de compatibilidade podem dificultar a utilização de certos controles ou induzir erros humanos, chegando mesmo a anular o controle, a dar uma falsa sensação de segurança ou a tornar o risco ainda maior do que seria se o controle não existisse (por exemplo, exigir senhas complexas sem treinamento adequado leva os usuários a anotar as senhas por escrito). É importante lembrar também que um controle pode vir a afetar muito o desempenho. Convém que os gestores tentem encontrar uma solução que satisfaça aos requisitos de desempenho e que possa, ao mesmo tempo, garantir um nível suficiente de segurança da informação. O resultado dessa etapa é uma lista de controles possíveis, com seu custo, benefício e prioridade de implementação.

Convém que várias restrições sejam levadas em consideração durante a escolha e a implementação de controles. Normalmente, são consideradas as seguintes:

- restrições temporais;
- restrições financeiras;
- restrições técnicas;
- restrições operacionais;
- restrições culturais;
- restrições éticas;
- restrições ambientais;
- facilidade de uso;
- restrições de recursos humanos;
- restrições ligadas à integração dos controles novos aos já existentes.

Mais informações sobre as restrições relacionadas à modificação do risco podem ser encontradas no Anexo F.

9.3 Retenção do risco

Ação: Convém que as decisões sobre a retenção do risco, sem outras ações adicionais, sejam tomadas tendo como base a avaliação de riscos.

Diretrizes para implementação:

Se o nível de risco atende aos critérios para a aceitação do risco, não há necessidade de se implementar controles adicionais e pode haver a retenção do risco.

9.4 Ação de evitar o risco

Ação: Convém que a atividade ou condição que dá origem a um determinado risco seja evitada.

Diretrizes para implementação:

Quando os riscos identificados são considerados demasiadamente elevados e quando os custos da implementação de outras opções de tratamento do risco excederem os benefícios, pode-se decidir que o risco seja evitado completamente, seja pela eliminação de uma atividade planejada ou existente (ou de um conjunto de atividades), seja pelas mudanças nas condições em que a operação da atividade ocorre. Por exemplo: para riscos causados por fenômenos naturais, pode ser uma alternativa mais rentável mover fisicamente as instalações de processamento de informações para um local onde o risco não exista ou esteja sob controle.

9.5 Compartilhamento do risco

Ação: Convém que um determinado risco seja compartilhado com outra entidade que possa gerenciá-lo de forma mais eficaz, dependendo da avaliação de riscos.

Diretrizes para implementação:

O compartilhamento do risco envolve a decisão de se compartilhar certos riscos com entidades externas. O compartilhamento do risco pode criar novos riscos ou modificar riscos existentes e identificados. Portanto, um novo tratamento do risco pode ser necessário.

O compartilhamento pode ser feito por um seguro que cubra as consequências ou por meio da subcontratação de um parceiro cujo papel seja o de monitorar o sistema de informação e tomar medidas imediatas que impeçam um ataque antes que ele possa causar um determinado nível de dano.

Convém notar que é possível compartilhar a responsabilidade de gerenciar riscos, entretanto não é normalmente possível compartilhar a responsabilidade legal por um impacto. Os clientes provavelmente atribuem um impacto adverso como sendo falha da organização.

10 Aceitação do risco de segurança da informação

Entrada: O plano de tratamento do risco e o processo de avaliação do risco residual sujeito à decisão dos gestores da organização relativa à aceitação deste.

Ação: Convém que a decisão de aceitar os riscos seja feita e formalmente registrada, juntamente com a responsabilidade pela decisão.

Diretrizes para implementação:

Convém que os planos de tratamento do risco descrevam como os riscos avaliados serão tratados para que os critérios de aceitação do risco sejam atendidos (ver 7.2). É importante que gestores responsáveis façam uma análise crítica e aproveem os planos propostos de tratamento do risco, os riscos residuais resultantes e que registrem as condições associadas a essa aprovação.

Os critérios para a aceitação do risco podem ser mais complexos do que somente a determinação se o risco residual está, ou não, abaixo ou acima de um limite bem definido.

Em alguns casos, o nível de risco residual pode não satisfazer aos critérios de aceitação do risco, pois os critérios aplicados não estão levando em conta as circunstâncias predominantes no momento. Por exemplo, pode ser válido argumentar que é preciso que se aceite o risco, pois os benefícios que o acompanham são muito atraentes ou porque os custos de sua modificação são demasiadamente elevados. Estas circunstâncias indicam que os critérios para a aceitação do risco são inadequados e convém que sejam revistos, se possível. No entanto, nem sempre é possível rever os critérios para a aceitação do risco no tempo apropriado. Nesses casos, os tomadores de decisão podem aceitar riscos que não satisfaçam os critérios normais para o aceite. Se isso for necessário, convém que o tomador de decisão comente explicitamente sobre os riscos e inclua uma justificativa para a sua decisão de passar por cima dos critérios normais para a aceitação do risco.

Saída: Uma lista de riscos aceitos, incluindo uma justificativa para aqueles que não satisfaçam os critérios normais da organização para aceitação do risco.

11 Comunicação e consulta do risco de segurança da informação

Entrada: Todas as informações sobre os riscos obtidas por meio das atividades de gestão de riscos (ver Figura 2).

Ação: Convém que as informações sobre riscos sejam trocadas e/ou compartilhadas entre o tomador de decisão e as outras partes interessadas.

Diretrizes para implementação:

A comunicação do risco é uma atividade que objetiva alcançar um consenso sobre como gerenciar os riscos por meio da troca e/ou compartilhamento das informações sobre o risco entre os tomadores de decisão e as outras partes interessadas. A informação inclui, entre outros possíveis fatores, a existência, natureza, forma, probabilidade, severidade, tratamento e aceitabilidade dos riscos.

A comunicação eficaz entre as partes interessadas é importante, uma vez que isso pode ter um impacto significativo sobre as decisões a serem tomadas. A comunicação assegura que os responsáveis pela implementação da gestão de riscos, e aqueles com interesses reais de direito, tenham um bom entendimento do porquê as decisões são tomadas e dos motivos que tornam certas ações necessárias. A comunicação é bidirecional.

A percepção do risco pode variar devido a diferenças de suposições, conceitos, necessidades, interesses e preocupações das partes interessadas quando lidam com o risco ou quando tratam das questões sendo aqui discutidas. As partes interessadas irão, provavelmente, fazer julgamentos sobre a aceitabilidade do risco tendo como base sua própria percepção do risco. Isto é particularmente importante para garantir que a percepção do risco das partes interessadas bem como a sua percepção dos benefícios sejam identificadas e documentadas e que as razões subjacentes sejam claramente entendidas e consideradas.

Convém que a comunicação do risco seja realizada a fim de:

- fornecer garantia do resultado da gestão de riscos da organização;
- coletar informações sobre os riscos;

- compartilhar os resultados do processo de avaliação de riscos e apresentar o plano de tratamento do risco;
- evitar ou reduzir tanto a ocorrência quanto as consequências das violações da segurança da informação que aconteçam devido à falta de entendimento mútuo entre os tomadores de decisão e as partes interessadas;
- dar suporte ao processo decisório;
- obter novo conhecimento sobre a segurança da informação;
- coordenar com outras partes e planejar respostas para reduzir as consequências de um incidente;
- dar aos tomadores de decisão e às partes interessadas um senso de responsabilidade sobre riscos;
- melhorar a conscientização.

Convém que a organização desenvolva planos de comunicação dos riscos tanto para as operações rotineiras como também para situações emergenciais. Portanto, convém que a atividade de comunicação do risco seja realizada continuamente.

A coordenação entre os principais tomadores de decisão e as partes interessadas pode ser obtida mediante a formação de uma comissão em que os riscos, a sua priorização, as formas adequadas de tratá-los e a sua aceitação possam ser amplamente discutidos.

É importante cooperar com o escritório de relações públicas ou com o grupo de comunicação apropriado dentro da organização para coordenar as tarefas relacionadas com a comunicação e consulta do risco. Isso é vital no caso de ações de comunicação durante crises, por exemplo: em resposta a incidentes específicos.

Saída: Entendimento contínuo do processo de gestão de riscos de segurança da informação da organização e dos resultados obtidos.

12 Monitoramento e análise crítica de riscos de segurança da informação

12.1 Monitoramento e análise crítica dos fatores de risco

Entrada: Todas as informações sobre os riscos obtidas por meio das atividades de gestão de riscos (ver Figura 2).

Ação: Convém que os riscos e seus fatores (isto é, valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidade de ocorrência) sejam monitorados e analisados criticamente, a fim de se identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização e de se manter uma visão geral dos riscos.

Diretrizes para implementação:

Os riscos não são estáticos. As ameaças, as vulnerabilidades, a probabilidade ou as consequências podem mudar abruptamente, sem qualquer indicação. Portanto, o monitoramento constante é necessário para que se detectem essas mudanças. Isto pode ser apoiado por serviços de terceiros que forneçam informações sobre novas ameaças ou vulnerabilidades.

Convém que as organizações assegurem que os seguintes itens sejam monitorados continuamente:

- novos ativos que tenham sido incluídos no escopo da gestão de riscos;
- modificações necessárias dos valores dos ativos, por exemplo: devido à mudança nos requisitos de negócio;
- novas ameaças que podem estar ativas tanto fora quanto dentro da organização e que não tenham sido avaliadas;
- a possibilidade de que vulnerabilidades novas ou ampliadas venham a permitir que alguma ameaça as explore;
- as vulnerabilidades já identificadas, para determinar aquelas que estão se tornando expostas a ameaças novas ou ressurgentes;
- as consequências ou o impacto ampliado de ameaças, vulnerabilidades e riscos avaliados em conjunto em um todo agregado, resultando em um nível inaceitável de risco;
- incidentes relacionados à segurança da informação.

Novas ameaças, novas vulnerabilidades e mudanças na probabilidade ou nas consequências podem vir a ampliar os riscos anteriormente avaliados como baixos. Convém que a análise crítica dos riscos baixos e aceitos considere cada risco separadamente e também em conjunto a fim de avaliar seu impacto potencial agregado. Se os riscos não estiverem dentro da categoria “baixo” ou “aceitável”, convém que eles sejam tratados por meio de uma ou mais de uma das opções consideradas na Seção 9.

Fatores que afetam a probabilidade ou as consequências das ameaças já ocorridas podem mudar, assim como os fatores que afetam a adequação ou o custo das várias opções de tratamento. Convém que qualquer grande mudança que afete a organização seja seguida por uma análise crítica mais específica. Assim sendo, convém que as atividades de monitoramento de riscos sejam repetidas regularmente, e que as opções selecionadas para o tratamento do risco sejam analisadas criticamente periodicamente.

O resultado da atividade de monitoramento de riscos pode fornecer os dados de entrada para as atividades de análise crítica. Convém que a organização analise crítica e regularmente todos os riscos e também quando grandes mudanças ocorrerem.

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

12.2 Monitoramento, análise crítica e melhoria do processo de gestão de riscos

Entrada: Todas as informações sobre os riscos obtidas por meio das atividades de gestão de riscos (ver Figura 2).

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

Diretrizes para implementação:

O monitoramento cotidiano e a análise crítica são necessários para assegurar que o contexto, o resultado do processo de avaliação de riscos e do tratamento do risco, assim como os planos de gestão, permaneçam relevantes e adequados às circunstâncias.

Convém que a organização se certifique de que o processo de gestão de riscos de segurança da informação e as atividades relacionadas permaneçam apropriadas nas circunstâncias presentes e sejam acompanhadas. Convém que quaisquer melhorias ao processo ou quaisquer ações necessárias para melhorar a conformidade com o processo sejam comunicadas aos gestores apropriados, para que se possa ter garantia de que:

- nenhum risco ou elemento do risco é ignorado ou subestimado;
- as ações necessárias são executadas, e
- as decisões corretas estão sendo tomadas a fim de se garantir uma compreensão realista do risco e a capacidade de reação.

Além disso, convém que a organização verifique regularmente se os critérios utilizados para medir o risco e os seus elementos ainda são válidos e consistentes com os objetivos de negócios, estratégias e políticas. Convém verificar regularmente também se as mudanças no contexto do negócio são adequadamente consideradas durante o processo de gestão de riscos de segurança da informação. Convém que essa atividade de monitoramento e a análise crítica aborde (mas não seja limitada a):

- o contexto da concorrência;
- a abordagem do processo de avaliação de riscos;
- o valor e as categorias dos ativos;
- os critérios de impacto;
- os critérios para a avaliação de riscos;
- os critérios para a aceitação do risco;
- o custo total de propriedade;
- os recursos necessários.

Convém que a organização assegure que os recursos necessários para o processo de avaliação de riscos e o tratamento destes estejam sempre disponíveis para analisar criticamente os riscos, para lidar com ameaças ou vulnerabilidades novas ou alteradas e para aconselhar a direção da melhor forma possível.

O monitoramento da gestão de riscos pode resultar em modificação ou acréscimo da abordagem, metodologia ou ferramentas utilizadas, dependendo:

- das mudanças identificadas;
- da iteração do processo de avaliação de riscos;
- do objetivo do processo de gestão de riscos de segurança da informação (por exemplo: a continuidade de negócios, a resiliência diante dos incidentes, a conformidade); e
- do objeto de interesse do processo de gestão de riscos de segurança da informação (por exemplo: a organização, a unidade de negócios, o sistema de informação, a sua implementação técnica, a aplicação, a conexão à *Internet*).

Saída: Garantia permanente da relevância do processo de gestão de riscos de segurança da informação para os objetivos de negócios da organização ou a atualização do processo.

Anexo A (informativo)

Definindo o escopo e os limites do processo de gestão de riscos de segurança da informação

A.1 Estudo da organização

Avaliação da organização O estudo da organização destaca os elementos característicos que definem a identidade de uma organização. Ela se preocupa com o propósito, o negócio, a missão, os valores e as estratégias da organização. Convém que sejam identificados juntos com os elementos que contribuem com o seu desenvolvimento (por exemplo, a subcontratação).

A dificuldade aqui reside no entendimento exato de como a organização está estruturada. A identificação de sua real estrutura permite um entendimento do papel e da importância de cada área no alcance dos objetivos da organização.

Por exemplo, o fato de o gestor da segurança da informação se reportar à alta direção em vez de de aos gestores de TI pode indicar o envolvimento da alta direção nos assuntos relativos à segurança da informação.

O propósito principal da organização O seu propósito pode ser definido como a razão pela qual a organização existe (sua área de atividade, seu segmento de mercado etc.).

Seu negócio O negócio de uma organização, definido pelas técnicas e “*know-how*” de seus funcionários, viabiliza o cumprimento de sua missão. É específico à área de atividade da organização e frequentemente define sua cultura.

Sua missão A organização atinge seu propósito ao cumprir sua missão. Para bem identificá-la, convém que os serviços prestados e/ou produtos manufaturados sejam relacionados aos seus públicos-alvos.

Seus valores Valores consistem de princípios fundamentais ou de um código de conduta bem definido, aplicados na rotina de um negócio. Podem incluir os recursos humanos, as relações com agentes externos (clientes etc.), a qualidade dos produtos fornecidos ou dos serviços prestados.

Por exemplo, uma organização cujo propósito seja o serviço público, cujo negócio seja o transporte e cuja missão inclua o transporte de crianças de ida e de volta da escola pode ter como valores a pontualidade do serviço e a segurança durante o transporte.

A estrutura da organização Existem diferentes tipos de estrutura:

- Estrutura departamental baseada em divisões ou áreas: cada divisão fica sob a autoridade de um gestor de área responsável pelas decisões estratégicas, administrativas e operacionais relativas à sua unidade.
- Estrutura baseada em funções: a autoridade relativa a cada função é exercida na forma dos procedimentos adotados, na determinação da natureza do trabalho e algumas vezes nas decisões e no planejamento (por exemplo, produção, TI, recursos humanos, *marketing* etc.).

Observações:

- Uma área, em uma organização com estrutura departamental, pode ser estruturada com base em suas funções e vice-versa.
- Uma organização pode ser considerada como de estrutura matricial se possuir características de ambos os tipos de estrutura.
- Em qualquer tipo de estrutura organizacional, os seguintes níveis podem ser distinguidos:
 - o nível de tomada de decisão (estabelecimento da orientação estratégica);
 - o nível da liderança (coordenação e gestão);
 - o nível operacional (produção e atividades de apoio).

Organograma A estrutura da organização é esquematizada em seu organograma. Convém que essa representação destaque quem se reporta a quem e a delegação de autoridade, mas também convém que inclua outros tipos de relacionamentos, os quais, mesmo que não sejam baseados em uma autoridade oficial, criam de qualquer forma caminhos para o fluxo de informação.

A estratégia da organização Ela requer a expressão formalizada dos princípios que norteiam a organização. A estratégia determina a direção e o desenvolvimento necessários para que a organização possa se beneficiar das questões em pauta e das principais mudanças sendo planejadas.

A.2 Lista de restrições que afetam a organização

Convém que todas as restrições que afetam a organização e determinam o direcionamento da segurança da informação sejam consideradas. As suas origens podem ser encontradas na própria organização, o que lhe concede um certo controle sobre as restrições ou talvez sejam externas à organização, o que as tornam, provavelmente, “inegociáveis”. Recursos limitados (orçamento, recursos humanos) e restrições ligadas a emergências estão entre as mais importantes.

A organização define seus objetivos (relativos ao seu negócio, comportamento etc.) e se compromete a seguir um determinado caminho, possivelmente por um longo período. Ela define aquilo em que deseja se tornar e também os meios necessários para que isto possa ocorrer. Para especificar esse caminho, a organização considera a evolução das técnicas e do *know-how* disponíveis, assim como a vontade expressa de seus usuários, clientes, entre outros fatores. Esse objetivo pode ser expresso na forma de estratégias de operação ou de desenvolvimento com o fim de, por exemplo, cortar custos operacionais, melhorar a qualidade do serviço etc.

Essas estratégias provavelmente abrangem as informações e os sistemas de informação (SI), os quais auxiliam a aplicação das estratégias. Consequentemente, as características relacionadas à identidade, missão e estratégias da organização são elementos fundamentais para a análise do problema, pois a violação de qualquer aspecto da segurança da informação pode resultar na reformulação desses objetivos estratégicos. Além disso, é essencial que propostas de novos requisitos de segurança da informação sejam consistentes com as regras, o uso e os meios empregados na organização.

A lista de restrições inclui, mas não é limitada a:

Restrições de natureza política: Estas são relacionadas à administração governamental, às instituições públicas ou, mais genericamente, a qualquer organização que precise aplicar decisões

governamentais. Normalmente, trata-se de decisões relativas à orientação estratégica ou operacional determinada por uma área do governo ou por uma entidade responsável pelo processo decisório e convém que sejam aplicadas.

Por exemplo, a informatização de notas fiscais ou de documentos administrativos introduz questões de segurança da informação.

Restrições de natureza estratégica: Restrições podem surgir de mudanças, sejam planejadas ou não, na estrutura ou na orientação da organização. Elas são representadas nos planos estratégicos ou operacionais da organização.

Por exemplo, a cooperação internacional para o compartilhamento de informações sensíveis pode demandar acordos sobre a troca segura de dados.

Restrições territoriais: A estrutura e/ou o propósito da organização pode(m) implicar restrições específicas, como em relação à escolha de sua localização e distribuição geográfica, no país e no estrangeiro.

Exemplos incluem os serviços postais, embaixadas, bancos, subsidiárias de conglomerados industriais etc.

Restrições advindas do ambiente econômico e político: A operação de uma organização pode ser transformada por eventos específicos, como greves ou crises nacionais e internacionais.

Por exemplo, convém garantir a continuidade da prestação de alguns serviços mesmo em caso de crises.

Restrições estruturais: A natureza da estrutura de uma organização (departamental, funcional ou outra qualquer) pode levar a uma política de segurança da informação e a uma organização responsável pela segurança, adaptadas a essa estrutura.

Por exemplo, convém que uma estrutura internacional seja capaz de conciliar requisitos de segurança específicos de cada país.

Restrições funcionais: Restrições funcionais derivam diretamente das missões gerais ou específicas da organização .

Por exemplo, convém que uma organização que opera 24 h por dia seja capaz de assegurar que seus recursos estejam sempre disponíveis.

Restrições relativas aos recursos humanos: A natureza dessas restrições varia consideravelmente. Estão associadas ao: nível de responsabilidade, tipo de recrutamento, qualificação, treinamento, conscientização em segurança, motivação, disponibilidade etc.

Por exemplo, convém que todos os recursos humanos de uma organização de defesa do país tenham autorização para manipular informações altamente sigilosas.

Restrições advindas da agenda da organização: Esse tipo de restrição pode resultar da reestruturação ou da definição de novas políticas que imponham algumas datas-limite.

Por exemplo, a criação de uma área de segurança.

Restrições relacionadas a métodos: Métodos apropriados para o *know-how* da organização precisam ser impostos em relação a alguns tópicos, como o planejamento, a especificação e o desenvolvimento de projetos, entre outros.

Restrições de natureza cultural: Em algumas organizações, hábitos de trabalho ou as características do negócio dão origem a uma “cultura” específica da organização, a qual pode ser incompatível com o estabelecimento de controles de segurança. Essa cultura é usada pelos recursos humanos como sua principal referência e pode ser determinada por vários aspectos, incluindo educação, instrução, experiência profissional, experiência fora do trabalho, opiniões, filosofia, crenças, *status* social etc.

Restrições orçamentárias: Os controles de segurança recomendados podem, algumas vezes, ter um alto custo. Apesar de não ser sempre apropriado ter apenas a taxa de custo-benefício como base para os investimentos em segurança, uma justificativa econômica é normalmente necessária para o departamento financeiro da organização.

Por exemplo, no setor privado e em algumas organizações públicas, convém que o custo total dos controles de segurança não exceda o custo potencial das possíveis consequências dos riscos. Assim, convém que a alta direção avalie os riscos e aceite uma parcela deles de forma consciente e calculada, para se evitar custos excessivos em segurança.

A.3 Lista de restrições que afetam o escopo

Ao identificar as restrições, é possível enumerar aquelas que causam um impacto no escopo e determinar quais são passíveis de intervenção. Elas complementam e talvez venham a corrigir as restrições da organização discutidas anteriormente. Os parágrafos a seguir apresentam uma lista de tipos de restrições, sem esgotar todas as possibilidades.

Restrições derivadas de processos preexistentes

Projetos de aplicações não são desenvolvidos necessariamente de forma simultânea. Alguns dependem de processos preexistentes. Mesmo que um processo possa ser quebrado em subprocessos, o processo não é influenciado por todos os subprocessos de um outro processo.

Restrições técnicas

Restrições técnicas, relativas à infraestrutura, surgem normalmente em função do *software* e do *hardware* instalados e dos aposentos e instalações em que eles se encontram:

- arquivos (requisitos referentes à organização, gestão de mídia, gestão de regras de acesso etc.);
- arquitetura comum (requisitos referentes à topologia – centralizada, distribuída ou do tipo cliente-servidor –, à arquitetura física etc.);
- *software* aplicativo (requisitos referentes aos projetos de *software* específico, padrões de mercado etc.);
- *software* de prateleira (requisitos referentes a padrões, qualidade, conformidade com normas, segurança etc.);
- *hardware* (requisitos referentes a padrões, qualidade, conformidade com normas etc.);
- redes de comunicação (requisitos referentes à cobertura, padrões, capacidade, confiabilidade etc.);
- infraestrutura predial (requisitos referentes à engenharia civil, construção, alta voltagem, baixa voltagem etc.).

Restrições financeiras

A implementação de controles de segurança é frequentemente limitada pelo orçamento que a organização pode comprometer para tal. Entretanto, convém que restrições financeiras sejam consideradas por último já que alocações orçamentárias para segurança podem ser negociadas tendo como base a análise da própria segurança.

Restrições ambientais

Restrições ambientais surgem em função do ambiente geográfico ou econômico no qual os processos são implementados: país, clima, riscos naturais, situação geográfica, ambiente econômico etc.

Restrições temporais

Convém que o tempo requerido para a implementação de controles de segurança seja considerado em relação à capacidade de atualização do sistema de informação; se a implementação for muito demorada, os riscos para os quais os controles foram projetados podem já ter mudado. O tempo é um fator determinante na seleção de soluções e prioridades.

Restrições relacionadas a métodos

Convém que métodos apropriados para o *know-how* da organização sejam utilizados para o planejamento, a especificação e o desenvolvimento de projetos, entre outros.

Restrições organizacionais

Várias restrições podem ser causadas por requisitos de ordem organizacional:

- operação (requisitos referentes ao “tempo gasto na produção”, fornecimento de serviços, vigilância, monitoramento, planos em caso de emergência, operação reduzida etc.);
- manutenção (requisitos para a investigação e solução de incidentes, ações preventivas, correção rápida etc.);
- gestão de recursos humanos (requisitos referentes ao treinamento de operadores e usuários, qualificação para cargos como administrador de sistema ou de dados etc.);
- gestão administrativa (requisitos referentes a responsabilidades etc.);
- gestão do desenvolvimento (requisitos referentes a ferramentas de desenvolvimento, engenharia de *software* assistida por computador, cronograma de aceite, organização a ser estabelecida etc.);
- gestão de relacionamentos externos (requisitos referentes à organização das relações com terceiros, contratos etc.).

Anexo B (informativo)

Identificação e valoração dos ativos e avaliação do impacto

B.1 Exemplos de identificação de ativos

B.1.1 Generalidades

Para estabelecer o valor de seus ativos, uma organização precisa primeiro identificá-los (em um nível de detalhamento adequado). Dois tipos de ativos podem ser distinguidos:

- ativos primários:
 - processos e atividades do negócio;
 - informação;
- ativos de suporte (sobre os quais os elementos primários do escopo se apoiam), de todos os tipos:
 - *hardware*;
 - *software*;
 - rede;
 - recursos humanos;
 - instalações físicas;
 - estrutura da organização.

B.1.2 Identificação dos ativos primários

Para permitir a descrição do escopo de forma precisa, essa atividade consiste na identificação dos ativos primários (processos e atividades do negócio, informação). A identificação é conduzida por um grupo misto de trabalho que represente o processo (gestores, especialistas nos sistemas de informação e usuários).

Os ativos primários normalmente consistem dos principais processos e informações das atividades incluídas no escopo. Outros ativos primários, como os processos da organização, podem também ser considerados, os quais são úteis para a elaboração da política de segurança da informação ou do plano de continuidade de negócios. Dependendo de seus propósitos, alguns estudos não demandam uma análise exaustiva de todos os elementos presentes no escopo. Nesses casos, o estudo pode ser limitado aos elementos-chave incluídos no escopo.

Os ativos primários são de dois tipos:

- 1) Processos (ou subprocessos) e atividades do negócio, por exemplo:
 - processos cuja interrupção, mesmo que parcial, torna impossível cumprir a missão da organização;
 - processos que contêm procedimentos secretos ou processos envolvendo tecnologia proprietária;
 - processos que, se modificados, podem afetar significativamente o cumprimento da missão da organização;
 - processos necessários para que a organização fique em conformidade com requisitos contratuais, legais ou regulatórios identificados como tal na Seção 6;
- 2) Informação. Genericamente, informação primária compreende:
 - informação vital para o cumprimento da missão de uma organização ou para o desempenho de seu negócio;
 - informação de caráter pessoal, da forma em que é definida nas leis nacionais referentes à privacidade;
 - informação estratégica necessária para o alcance dos objetivos determinados pelo direcionamento estratégico;
 - informação de alto custo, cuja coleta, armazenamento, processamento e transmissão demandam um longo tempo ou incorrem em um alto custo de aquisição.

Processos e informação que não são identificadas como sensíveis após essa atividade não recebem uma classificação específica durante o restante do estudo. Isto significa que a organização pode cumprir sua missão com sucesso mesmo no caso desses processos ou informação terem sido comprometidos.

Entretanto, eles frequentemente herdam controles implementados para a proteção de processos e informação identificados como sensíveis.

B.1.3 Lista e descrição de ativos de suporte

Convém que o escopo consista de ativos que possam ser identificados e descritos. Estes ativos apresentam vulnerabilidades que podem ser exploradas por ameaças cujo objetivo é comprometer os ativos primários do escopo (processos e informação). Eles são de vários tipos:

- *Hardware*. O tipo *hardware* compreende os elementos físicos que dão suporte aos processos.
 - Equipamento de processamento de dados (ativo): Equipamento automático de processamento de dados incluindo os itens necessários para sua operação independente.
 - Equipamento móvel: Computadores portáteis.

EXEMPLO *Laptops*, agendas eletrônicas (*Personal Digital Assistants* – PDA).

- Equipamento fixo: Computadores utilizados nas instalações da organização.

EXEMPLOS Servidores, microcomputadores utilizados como estações de trabalho.

- Periféricos de processamento: Equipamento conectado a um computador por uma porta de comunicação (*serial, link paralelo* etc.) para a entrada, o transporte ou a transmissão de dados.

EXEMPLO Impressoras, unidades de disco removível.

- Mídia de dados (passiva): Este tipo compreende a mídia para o armazenamento de dados ou funções.

- Mídia eletrônica: Uma mídia com informações que pode ser conectada a um computador ou a uma rede de computadores para o armazenamento de dados. Apesar de seu tamanho reduzido, esse tipo de mídia pode conter um grande volume de dados e pode ser utilizada com equipamentos computadorizados comuns.

EXEMPLO Disco flexível, *CD-ROM*, cartucho de “*back-up*”, unidade de disco removível, cartão de memória, fita.

- Outros tipos de mídia: Mídia estática, não eletrônica, contendo dados.

EXEMPLO Papel, *slides*, transparências, documentação, fax.

- *Software*. O tipo *software* compreende todos os programas que contribuem para a operação de um sistema de processamento de dados.

- Sistema operacional: Este tipo inclui os programas que fornecem as operações básicas de um computador, a partir das quais os outros programas (serviços e aplicações) são executados. Nele encontramos um núcleo (“kernel”) e as funções ou serviços básicos. Dependendo de sua arquitetura, um sistema operacional pode ser monolítico ou formado por um “*micro-kernel*” e um conjunto de serviços do sistema. Os principais elementos de um sistema operacional são os serviços de gerenciamento do equipamento (CPU, memória, disco e interfaces de rede), os de gestão de tarefas ou processos e os serviços de gestão de direitos de usuário.

- *Software* de serviço, manutenção ou administração: *Software* caracterizado pelo fato de servir como complemento dos serviços do sistema operacional e não estar diretamente a serviço dos usuários ou aplicações (apesar de ser, normalmente, essencial e até mesmo indispensável para a operação do sistema de informação como um todo).

- *Software* de pacote ou *software*-padrão: *Software* de pacote ou *software*-padrão é aquele que é comercializado como um produto completo (e não como um serviço de desenvolvimento específico) com mídia, versão e manutenção. Ele fornece serviços para usuários e aplicações, mas não é personalizado ou específico como, por exemplo, aplicações de negócio o são.

EXEMPLO *Software* para o gerenciamento de bases de dados, *software* de mensagens eletrônicas, “*groupware*” (*software* de gerenciamento de fluxo de trabalho), *software* de diretório, servidores *web* etc.

- Aplicações de negócio:

- Aplicações de negócio padronizadas: Este tipo de *software* comercial é projetado para dar aos usuários acesso direto a serviços e funções que eles demandam de seus sistemas

de informação, em função das áreas em que atuam profissionalmente. Existe uma gama enorme, teoricamente ilimitada, de campos de atuação.

EXEMPLO *Software* de contabilidade, *software* para o controle de maquinário, *software* para administração do relacionamento com clientes, *software* para gestão de competências dos recursos humanos, *software* administrativo etc.

- Aplicações de negócio específicas: Vários aspectos desse tipo de *software* (principalmente o suporte, a manutenção e a atualização de versões etc.) são desenvolvidos especificamente para dar aos usuários acesso direto aos serviços e funções que eles demandam de seus sistemas de informação. Existe uma gama enorme, teoricamente ilimitada, de áreas em que esse tipo de *software* é encontrado.

EXEMPLO Administração das notas fiscais de clientes para as operadoras de telecomunicação, aplicação para monitoramento em tempo real do lançamento de foguetes.

- Rede. O tipo rede compreende os dispositivos de telecomunicação utilizados para interconectar computadores ou quaisquer outros elementos remotos de um sistema de informação.
- O meio físico e a infraestrutura: Os equipamentos de comunicação ou de telecomunicação são identificados principalmente pelas suas características físicas e técnicas (ponto a ponto, de “*broadcast*”) e pelos protocolos de comunicação utilizados (na camada de enlace de dados ou na camada de rede - níveis 2 e 3 do modelo OSI de 7 camadas).

EXEMPLO Rede telefônica pública comutada (“*Public Switching Telephone Network*” ou PSTN), “*Ethernet*”, “*GigabitEthernet*”, Linha digital assimétrica para assinante (“*Asymmetric Digital Subscriber Line*” ou ADSL), especificações de protocolo para comunicação sem fio (por exemplo, o WiFi 802.11), “*Bluetooth*”, “*FireWire*”.

- Pontes (“*relays*”) passivas ou ativas: Este subtipo compreende os dispositivos que não ficam nas extremidades lógicas da conexão (na perspectiva do sistema de informação), mas sim os que são intermediários no processo de comunicação, repassando o tráfego. Pontes são caracterizadas pelos protocolos de comunicação de rede com os quais funcionam. Além da função básica de repasse do tráfego, elas frequentemente são dotadas da capacidade de roteamento e/ou de serviços de filtragem, com o emprego de comutadores de comunicação (“*switches*”) e roteadores com filtros. Com frequência, elas podem ser administradas remotamente e são normalmente capazes de gerar arquivos de auditoria (“*logs*”).

EXEMPLO Pontes (“*bridges*”), roteadores, “*hubs*”, comutadores (“*switches*”), centrais telefônicas automáticas.

- Interface de comunicação: As interfaces de comunicação das unidades de processamento são conectadas às unidades de processamento, porém, caracterizadas pela mídia e protocolos com os quais funcionam; pelos serviços de filtragem, de auditoria e de alerta instalados, se houver, e por suas funcionalidades; e pela possibilidade e requisitos de administração remota.

EXEMPLO Serviço Geral de Pacotes por Rádio (“*General Packet Radio Service*” ou GPRS), adaptador “*Ethernet*”.

- Recursos humanos: O tipo de recursos humanos compreende todas as classes de pessoas envolvidas com os sistemas de informação.
- Tomador de decisão. Tomadores de decisão são aqueles responsáveis pelos ativos primários (informação e processos) e os gestores da organização ou, se for o caso, de um projeto específico.

EXEMPLO Alta direção, líderes de projeto.

- **Usuários.** Usuários são recursos humanos que manipulam material sensível no curso de suas atividades e que, portanto, possuem uma responsabilidade especial nesse contexto. Eles podem ter direitos especiais de acesso aos sistemas de informação para desempenhar suas atividades rotineiras.

EXEMPLO Gestores da área de recursos humanos, gerentes financeiros, gestores dos riscos.

- **Pessoal de produção/manutenção.** Estes são os recursos humanos responsáveis pela operação e manutenção dos sistemas de informação. Eles possuem direitos especiais de acesso aos sistemas de informação para desempenhar suas atividades rotineiras.

EXEMPLO Administradores de sistema; administradores de dados; operadores de “back-up”, “Help Desk” e de instalação de aplicativos; especialistas em segurança.

- **Desenvolvedores:** Desenvolvedores são responsáveis pelo desenvolvimento dos sistemas aplicativos da organização. Eles possuem acesso com alto privilégio a uma parte dos sistemas de informação, mas não interferem nos dados de produção.

EXEMPLO Desenvolvedores de aplicações de negócio

- **Instalações físicas:** O tipo instalações compreende os lugares onde encontramos o escopo (ou parte dele) e os meios físicos necessários para as operações nele contidas.

- **Localidade:**

- **Ambiente externo:** Compreende as localidades em que não é possível que as medidas de segurança de uma organização sejam aplicadas.

EXEMPLO Os lares das pessoas, as instalações de outra organização, o ambiente externo ao local da organização (áreas urbanas, zonas perigosas).

- **Edificações:** Esse local é limitado pelo perímetro externo da organização, isto é por aquilo que fica em contato direto com o exterior. Isto pode ser uma linha de proteção física formada por barreiras ou por mecanismos de vigilância ao redor dos prédios.

EXEMPLO Estabelecimentos, prédios.

- **Zona:** Uma zona é limitada por linhas de proteção física que criam partições dentro das instalações da organização. É obtida por meio da criação de barreiras físicas ao redor das áreas com a infraestrutura de processamento de informações da organização.

EXEMPLO Escritórios, áreas de acesso restrito, zonas de segurança.

- **Serviços essenciais:** Todos os serviços necessários para que os equipamentos da organização possam operar normalmente.

- **Comunicação:** Serviços de telecomunicação e equipamento fornecido por uma operadora.

EXEMPLO Linha telefônica, PABX, redes internas de telefonia.

- **Serviços de Utilidade Pública:**

- **Serviços e os meios (alimentação e fiação) necessários para o fornecimento de energia elétrica aos equipamentos de tecnologia da informação e aos seus periféricos.**

EXEMPLO Fonte de alimentação de baixa tensão, inversor, central de circuitos elétricos.

- Fornecimento de água
- Saneamento e esgoto
- Serviços e os meios (equipamento, controle) para refrigeração e purificação do ar.

EXEMPLO Tubulação de água refrigerada, ar-condicionados.

- Organização. O tipo organização descreve a estrutura da organização, compreendendo as hierarquias de pessoas voltadas para a execução de uma tarefa e os procedimentos que controlam essas hierarquias.
 - Autoridades: Essas são as organizações de onde a organização em questão obtém sua autoridade. Elas podem ser legalmente afiliadas ou ter um caráter mais externo. Isto impõe restrições à organização em questão relacionada a regulamentos, decisões e ações.

EXEMPLO Corpo administrativo, sede da organização.

- A estrutura da organização: Compreende os vários ramos da organização, incluindo suas atividades multidisciplinares, sob controle de sua direção.

EXEMPLO Gestão de recursos humanos, gestão de TI, gestão de compras, gerenciamento de unidade de negócio, serviço de segurança predial, serviço de combate a incêndios, gerenciamento da auditoria.

- Organização de projeto ou serviço: Compreende a organização montada para um projeto ou serviço específico.

EXEMPLO Projeto de desenvolvimento de uma nova aplicação, projeto de migração de sistema de informação.

- Subcontratados/ Fornecedores/ Fabricantes: Essas são organizações que fornecem serviços ou recursos para a organização em questão segundo os termos de um contrato.

EXEMPLO Empresa de gestão de instalações, empresa prestadora de serviços terceirizados, empresas de consultoria.

B.2 Valoração dos Ativos

B.2.1 Generalidades

O passo seguinte, após a identificação do ativo, é determinar a escala de medida a ser usada e os critérios que permitam posicionar um ativo no seu correto lugar nessa escala, em função de seu valor. Devido à diversidade de ativos encontrados em uma organização, é provável que alguns deles, aqueles que possuem um valor monetário conhecido, possam ser avaliados através da moeda corrente local, enquanto outros ativos, aqueles com um valor expresso em termos qualitativos, talvez precisem ser avaliados através de uma lista de valores a serem selecionados, por exemplo: “muito baixo”, “muito alto”. A decisão de se usar uma escala quantitativa em vez de uma qualitativa (ou vice-versa) depende da preferência da organização, porém convém que seja pertinente aos ativos em avaliação. Ambos os tipos de avaliação podem ser utilizados para se determinar o valor de um mesmo ativo.

Termos comuns usados em avaliações qualitativas do valor de ativos incluem expressões como as seguintes: insignificante, muito pequeno, pequeno, médio, alto, muito alto, e crítico. A escolha e o leque de termos adequados a uma organização depende muito da sua necessidade de segurança, do seu tamanho, e de outros aspectos específicos da organização.

B.2.2 Critérios

Convém que os critérios utilizados como base para atribuição do valor para cada ativo sejam redigidos de forma objetiva e sem ambiguidades. Esse é um dos aspectos mais difíceis da valoração dos ativos já que o valor de alguns deles talvez precise ser determinado de forma subjetiva, e também porque provavelmente várias pessoas participarão do processo. Entre os possíveis critérios utilizados para determinar o valor de um ativo estão: o seu custo original e o custo de sua substituição ou de sua recriação. Por outro lado, seu valor pode ser abstrato, por exemplo: o valor da reputação de uma organização.

Um outro enfoque para a valoração dos ativos é considerar os custos decorridos da perda da confidencialidade, integridade e disponibilidade resultante de um incidente. Convém que a garantia de não repúdio e de responsabilização, a autenticidade e a confiabilidade, se apropriadas, também sejam consideradas. Este enfoque acrescenta uma dimensão muito importante à atribuição do valor de um ativo, além do custo de sua substituição, pois considera as consequências adversas ao negócio causadas por incidentes de segurança, tendo como premissa um conjunto determinado de circunstâncias. Convém ressaltar também que as consequências que esse enfoque identifica precisarão ser consideradas durante o processo de avaliação de riscos.

Muitos ativos, durante o curso da avaliação, podem acabar recebendo vários valores. Por exemplo: um plano de negócios pode ser avaliado em função do esforço despendido no seu desenvolvimento, pode ter seu valor atribuído em função do trabalho de entrar com os dados, e pode ainda ser valorado de acordo com seu valor para um competidor. Provavelmente, os valores atribuídos serão consideravelmente diferentes. O valor atribuído pode ser o maior valor encontrado, a soma de alguns ou de todos os possíveis valores. Em última análise, convém pensar cuidadosamente quais ou qual valor são associados a um ativo, pois o valor final atribuído fará parte do processo de determinação dos recursos a serem investidos na proteção do ativo.

B.2.3 Definição de um denominador comum

Ao final do processo, a valoração dos ativos precisa ter como base um denominador comum. Isso pode ser feito com a ajuda de critérios como os seguintes. Critérios que podem ser utilizados para estimar as possíveis consequências resultantes da perda de confidencialidade, integridade, disponibilidade, assim como da capacidade de garantir o não repúdio, a responsabilização, a autenticidade, e a confiabilidade são os seguintes:

- redução do desempenho do negócio;
- perda de valor de mercado/efeito negativo sobre a imagem e a reputação;
- violação de segurança relacionada a informações pessoais;
- o perigo ocasionado à segurança física das pessoas;
- efeitos negativos relacionados à execução da lei;
- violação de confidencialidade;

- violação da ordem pública;
- perda financeira;
- interrupção de atividades do negócio, e
- o perigo ocasionado à segurança ambiental.

Um outro método para avaliar as consequências pode considerar o seguinte:

- interrupção dos serviços: incapacidade de prestar os serviços;
- perda da confiança do cliente:
 - perda da credibilidade no sistema interno de informação, e
 - dano à reputação;
- interrupção de operação interna:
 - interrupção dentro da própria organização, e
 - custo interno adicional;
- interrupção da operação de terceiros:
 - interrupção das transações entre a organização e terceiros, e
 - vários tipos de prejuízos ou danos;
- perigo ocasionado à segurança física dos recursos humanos / usuários: perigo para os recursos humanos e usuários da organização;
- ataque à vida privada de usuários;
- perda financeira;
- custos financeiros para emergências, reposição e consertos:
 - em termos de recursos humanos;
 - em termos de equipamentos;
 - em termos de estudo, relatórios de especialistas;
- perda de bens/ fundos/ ativos;
- perda de clientes, perda de fornecedores;
- procedimentos e penalidades judiciais;
- perda de vantagem competitiva;
- perda da liderança tecnológica/ técnica;

- perda de eficácia/ confiança;
- perda da reputação técnica;
- enfraquecimento da capacidade de negociação;
- crise industrial (greves);
- crise governamental;
- rejeição;
- dano material.

Esses critérios exemplificam os temas a serem considerados durante a valoração de ativos. Para a execução desse tipo de avaliação, uma organização precisa selecionar os critérios que sejam relevantes para o seu tipo de negócio e para os seus requisitos de segurança. Isso pode significar que alguns dos critérios listados anteriormente não sejam aplicáveis, e que outros talvez precisem ser adicionados à lista.

B.2.4 Escala de medição

Após estabelecer os critérios a serem considerados, convém que a organização adote uma escala de medição para ser utilizada em todas as suas áreas. O primeiro passo é definir a quantidade de níveis da escala. Não existem regras sobre qual é o número de níveis mais adequado. Quanto mais níveis, maior é a granularidade da medição, porém uma diferenciação muito tênue torna difícil garantir a consistência das avaliações realizadas nas diversas áreas da organização. Normalmente, qualquer quantidade de níveis entre 3 (por exemplo: baixo, médio e alto) e 10 pode ser utilizada, desde que ela seja consistente com a abordagem que a organização esteja usando para o processo de avaliação de riscos como um todo.

Uma organização pode definir seus próprios limites para os valores de seus ativos, como 'baixo', 'médio' e 'alto'. Convém que esses limites sejam estimados de acordo com o critério selecionado (por exemplo: para possíveis perdas financeiras, convém que eles sejam estabelecidos através de valores monetários; porém, para outros tipos de fatores, como o perigo ocasionado à segurança física das pessoas, uma estimativa monetária pode ser por demais complexa e não apropriada a muitas organizações). Por último, cabe inteiramente à organização a decisão sobre o que é considerado de 'pequena' ou 'grande' consequência. Uma consequência desastrosa para uma pequena organização pode ser pequena ou mesmo insignificante para uma grande organização.

B.2.5 Dependências

Quanto mais relevantes e numerosos os processos de negócio apoiados por um ativo, maior é o seu valor. Convém que a dependência de ativos a processos de negócio e a outros ativos também seja identificada, pois ela pode influenciar os valores dos ativos. Por exemplo: convém garantir a confidencialidade dos dados durante todo o seu ciclo de vida, inclusive durante o seu armazenamento e processamento. Em outras palavras, convém que os requisitos de segurança para o armazenamento de dados e para os programas que fazem o processamento correspondam ao valor da confidencialidade dos dados armazenados e processados. Da mesma forma, se um processo de negócios depende da integridade dos dados gerados por um programa, convém que os dados de entrada passados para o programa sejam confiáveis. Mais que isso, a integridade da informação depende do *hardware* e do *software* utilizados para seu armazenamento e processamento. Adicionalmente, o *hardware*

dependerá do suprimento de energia e, possivelmente, do ar-condicionado. Assim, informações sobre dependências ajudam na identificação de ameaças e, em particular, de vulnerabilidades. Além disso, ajudam a assegurar que o real valor dos ativos (considerando as relações de dependência) é atribuído a estes, dessa forma indicando o nível de proteção apropriado.

Convém que os valores dos ativos dos quais outros ativos dependem sejam modificados da seguinte maneira:

- se os valores dos ativos dependentes (por exemplo: os dados) forem menores ou iguais ao valor do ativo em questão (por exemplo: o *software*), o valor desse último permanece o mesmo;
- se os valores dos ativos dependentes (por exemplo: os dados) forem maiores do que o valor do ativo em questão (por exemplo: o *software*), convém que o valor desse último aumente de acordo com:
 - o grau de dependência, e
 - os valores dos outros ativos.

Uma organização pode possuir alguns ativos que são disponibilizados mais de uma vez, como cópias de programas de *software* ou o tipo de computador usado na maioria dos escritórios. É importante levar em conta esse fato quando estiver sendo executada a valoração dos ativos. Por um lado, esses ativos são facilmente ignorados e, por isso, convém que se tenha um cuidado especial em identificá-los. Por outro lado, eles podem ser usados para minimizar problemas ligados à falta de disponibilidade.

B.2.6 Saída

O resultado final dessa etapa é a lista de ativos e respectivos valores relativos à divulgação de informações (preservação da confidencialidade), a modificações (garantia de integridade, autenticidade, não repúdio e responsabilização), à indisponibilidade e destruição do ativo (preservação de sua disponibilidade e confiabilidade), e ao custo de sua reposição.

B.3 Avaliação do Impacto

Um incidente envolvendo a segurança da informação pode trazer consequências a vários ativos ou apenas a parte de um único ativo. O impacto está relacionado à medida do sucesso do incidente. Por conseguinte, existe uma diferença importante entre o valor do ativo e o impacto resultante do incidente. Considera-se que o impacto tem um efeito imediato (operacional) ou uma consequência futura (relativa ao negócio como um todo), a qual inclui aspectos financeiros e de mercado.

O impacto imediato (operacional) pode ser direto ou indireto.

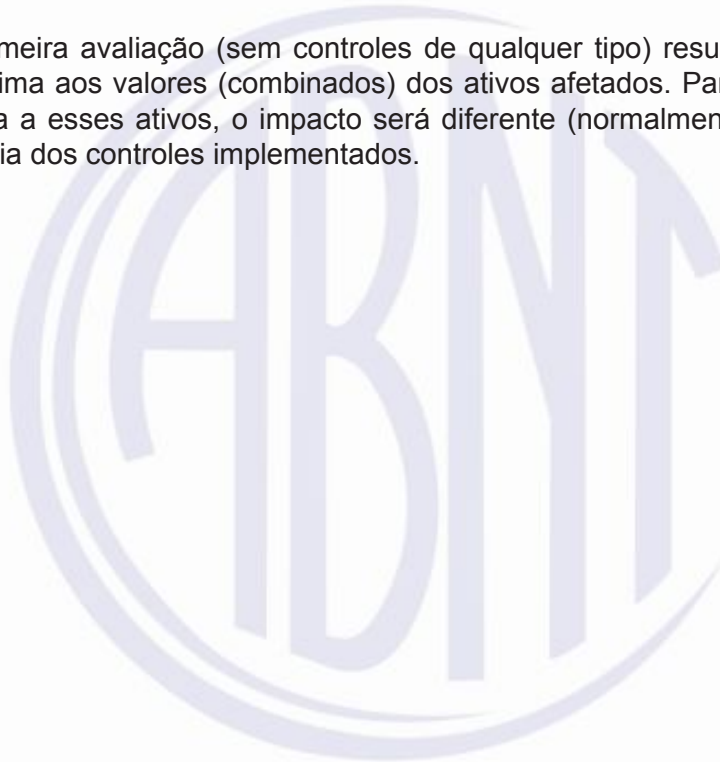
1) Direto:

- a) o valor financeiro de reposição do ativo perdido (ou parte dele);
- b) o custo de aquisição, configuração e instalação do novo ativo ou do “*back-up*”;
- c) o custo das operações suspensas devido ao incidente até que o serviço prestado pelos ativos afetados seja restaurado, e
- d) consequências resultantes de violações da segurança da informação.

2) Indireto:

- a) custo de oportunidade (recursos financeiros necessários para repor ou reparar um ativo poderiam estar sendo utilizados para outro fim);
- b) o custo das operações interrompidas;
- c) mau uso das informações obtidas por violação da segurança;
- d) violação de obrigações estatutárias ou regulatórias, e
- e) violação dos códigos éticos de conduta.

Dessa forma, a primeira avaliação (sem controles de qualquer tipo) resulta em uma estimativa do impacto muito próxima aos valores (combinados) dos ativos afetados. Para qualquer outra iteração que se faça relativa a esses ativos, o impacto será diferente (normalmente muito menor) devido à presença e à eficácia dos controles implementados.



Anexo C

(informativo)

Exemplos de ameaças comuns

A Tabela a seguir contém exemplos de ameaças comuns. A lista pode ser usada durante o processo de avaliação das ameaças. Ameaças podem ser intencionais, acidentais ou de origem ambiental (natural) e podem resultar, por exemplo, no comprometimento ou na paralisação de serviços essenciais. A lista também indica, para cada tipo de ameaça, se ela pode ser considerada I (intencional), A (acidental) ou N (natural). A letra I é utilizada para indicar as ações intencionais direcionadas contra os ativos de informação; a letra A é usada para indicar as ações de origem humana que podem comprometer acidentalmente os ativos de informação; e a letra N é utilizada para todos os incidentes que não são provocados pela ação dos seres humanos. Os grupos de ameaças não são apresentados em ordem de prioridade.

Tipo	Ameaças	Origem
Dano físico	Fogo	A, I, N
	Água	A, I, N
	Poluição	A, I, N
	Acidente grave	A, I, N
	Destruição de equipamento ou mídia	A, I, N
	Poeira, corrosão, congelamento	A, I, N
Eventos naturais	Fenômeno climático	N
	Fenômeno sísmico	N
	Fenômeno vulcânico	N
	Fenômeno meteorológico	N
	Inundação	N
Paralisação de serviços essenciais	Falha do ar-condicionado ou do sistema de suprimento de água	A, I
	Interrupção do suprimento de energia	A, I, N
	Falha do equipamento de telecomunicação	A, I
Distúrbio causado por radiação	Radiação eletromagnética	A, I, N
	Radiação térmica	A, I, N
	Pulsos eletromagnéticos	A, I, N

Tipo	Ameaças	Origem
Comprometimento da informação	Interceptação de sinais de interferência comprometedores	I
	Espionagem à distância	I
	Escuta não autorizada	I
	Furto de mídia ou documentos	I
	Furto de equipamentos	I
	Recuperação de mídia reciclada ou descartada	I
	Divulgação indevida	A, I
	Dados de fontes não confiáveis	A, I
	Alteração do <i>hardware</i>	I
	Alteração do <i>software</i>	A, I
	Determinação da localização	I
Falhas técnicas	Falha de equipamento	A
	Defeito de equipamento	A
	Saturação do sistema de informação	A, I
	Defeito de <i>software</i>	A
	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	A, I
Ações não autorizadas	Uso não autorizado de equipamento	I
	Cópia ilegal de <i>software</i>	I
	Uso de cópias de <i>software</i> falsificadas ou ilegais	A, I
	Comprometimento dos dados	I
	Processamento ilegal de dados	I
Comprometimento de funções	Erro durante o uso	A
	Abuso de direitos	A, I
	Forjamento de direitos	I
	Repúdio de ações	I
	Indisponibilidade de recursos humanos	A, I, N

Convém que atenção especial seja dada às fontes de ameaças representadas por seres humanos. A tabela a seguir enumera essas fontes:

Origem das Ameaças	Motivação	Possíveis Consequências
<i>Hacker, cracker</i>	Desafio Ego Rebeldia <i>Status</i> Dinheiro	<ul style="list-style-type: none"> • <i>Hacking</i> • Engenharia social • Invasão de sistemas, infiltrações e entradas não autorizadas • Acesso não autorizado ao sistema
Criminoso digital	Destruição de informações Divulgação ilegal de informações Ganho monetário Alteração de dados não autorizada	<ul style="list-style-type: none"> • Crime digital (por exemplo, perseguição no mundo digital) • Ato fraudulento (por exemplo, reutilização indevida de credenciais e dados transmitidos, fazer-se passar por uma outra pessoa, interceptação) • Suborno por informação • <i>Spoofing</i> (fazer-se passar por outro) • Invasão de sistemas
Terrorista	Chantagem Destruição Exploração Vingança Ganho político Cobertura da mídia	<ul style="list-style-type: none"> • Bomba/terrorismo • Guerra de informação • Ataque a sistemas (por exemplo, ataque distribuído de negação de serviço). • Invasão de sistema • Alteração do sistema
Espionagem industrial (serviços de inteligência, empresas, governos estrangeiros, outros grupos de interesse ligados ao governo)	Vantagem competitiva Espionagem econômica	<ul style="list-style-type: none"> • Garantir a vantagem de um posicionamento defensivo • Garantir uma vantagem política • Exploração econômica • Furto de informação • Violação da privacidade das pessoas • Engenharia social • Invasão de sistema • Acesso não autorizado ao sistema (acesso a informação restrita, de propriedade exclusiva, e/ou relativa à tecnologia)

Origem das Ameaças	Motivação	Possíveis Consequências
Pessoal interno (funcionários mal treinados, insatisfeitos, mal intencionados, negligentes, desonestos ou dispensados)	Curiosidade Ego Obtenção de informações úteis para serviços de inteligência Ganho monetário Vingança Erros e omissões não intencionais (por exemplo, erro na entrada de dados, erro de programação)	<ul style="list-style-type: none"> • Agressão a funcionário • Chantagem • Vasculhar informação de propriedade exclusiva • Uso impróprio de recurso computacional • Fraude e furto • Suborno por informação • Entrada de dados falsificados ou corrompidos • Interceptação • Código malicioso (por exemplo: vírus, bomba lógica, Cavalo de Tróia) • Venda de informações pessoais • Defeitos (“bugs”) no sistema • Invasão de sistemas • Sabotagem de sistemas • Acesso não autorizado ao sistema

Anexo D

(informativo)

Vulnerabilidades e métodos de avaliação de vulnerabilidades

D.1 Exemplos de vulnerabilidades

A Tabela a seguir fornece exemplos de vulnerabilidades em diversas áreas da segurança, incluindo exemplos de ameaças que poderiam explorar estas vulnerabilidades. As listas na Tabela D.1 podem ser de auxílio durante a avaliação das ameaças e vulnerabilidades a fim de se determinar os cenários relevantes de incidentes. Nota-se que, em alguns casos, outras ameaças são também capazes de explorar as mesmas vulnerabilidades.

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
<i>Hardware</i>	Manutenção insuficiente/Instalação defeituosa de mídia de armazenamento	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia
	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento
	Sensibilidade à radiação eletromagnética	Radiação eletromagnética
	Inexistência de um controle eficiente de mudança de configuração	Erro durante o uso
	Sensibilidade a variações de voltagem	Interrupção do suprimento de energia
	Sensibilidade a variações de temperatura	Fenômeno meteorológico
	Armazenamento não protegido	Furto de mídia ou documentos
	Falta de cuidado durante o descarte	Furto de mídia ou documentos
	Realização não controlada de cópias	Furto de mídia ou documentos

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Software	Procedimentos de teste de <i>software</i> insuficientes ou inexistentes	Abuso de direitos
	Falhas conhecidas no <i>software</i>	Abuso de direitos
	Não execução do “ <i>logout</i> ” ao se deixar uma estação de trabalho desassistida	Abuso de direitos
	Descarte ou reutilização de mídia de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados	Abuso de direitos
	Inexistência de uma trilha de auditoria	Abuso de direitos
	Atribuição errônea de direitos de acesso	Abuso de direitos
	<i>Software</i> amplamente distribuído	Comprometimento dos dados
	Utilizar programas aplicativos com um conjunto errado de dados (referentes a um outro período)	Comprometimento dos dados
	Interface de usuário complicada	Erro durante o uso
	Documentação inexistente	Erro durante o uso
	Configuração de parâmetros incorreta	Erro durante o uso
	Datas incorretas	Erro durante o uso
	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de usuários	Forjamento de direitos
	Tabelas de senhas desprotegidas	Forjamento de direitos
	Gerenciamento de senhas mal feito	Forjamento de direitos
	Serviços desnecessários permanecem habilitados	Processamento ilegal de dados
	<i>Software</i> novo ou imaturo	Defeito de <i>software</i>
	Especificações confusas ou incompletas para os desenvolvedores	Defeito de <i>software</i>
	Inexistência de um controle eficaz de mudança	Defeito de <i>software</i>
	<i>Download</i> e uso não controlado de <i>software</i>	Alteração do <i>software</i>
	Inexistência de cópias de segurança (“ <i>back-up</i> ”)	Alteração do <i>software</i>
	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de mídia ou documentos
	Inexistência de relatórios de gerenciamento	Uso não autorizado de equipamento

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Rede	Inexistência de evidências que comprovem o envio ou o recebimento de mensagens	Repúdio de ações
	Linhas de comunicação desprotegidas	Escuta não autorizada
	Tráfego sensível desprotegido	Escuta não autorizada
	Junções de cabeamento mal feitas	Falha do equipamento de telecomunicação
	Ponto único de falha	Falha do equipamento de telecomunicação
	Não identificação e não autenticação do emissor e do receptor	Forjamento de direitos
	Arquitetura insegura da rede	Espionagem à distância
	Transferência de senhas em claro	Espionagem à distância
	Gerenciamento de rede inadequado (quanto à flexibilidade de roteamento)	Saturação do sistema de informação
	Conexões de redes públicas desprotegidas	Uso não autorizado de equipamento
Recursos humanos	Ausência de recursos humanos	Indisponibilidade de recursos humanos
	Procedimentos de recrutamento inadequados	Destruição de equipamento ou mídia
	Treinamento insuficiente em segurança	Erro durante o uso
	Uso incorreto de <i>software</i> e <i>hardware</i>	Erro durante o uso
	Falta de conscientização em segurança	Erro durante o uso
	Inexistência de mecanismos de monitoramento	Processamento ilegal de dados
	Trabalho não supervisionado de pessoal de limpeza ou de terceirizados	Furto de mídia ou documentos
	Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens	Uso não autorizado de equipamento
Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controle do acesso físico a prédios e aposentos	Destruição de equipamento ou mídia
	Localização em área suscetível a inundações	Inundação
	Fornecimento de energia instável	Interrupção do suprimento de energia
	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de equipamentos

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Organização	Inexistência de um procedimento formal para o registro e a remoção de usuários	Abuso de direitos
	Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)	Abuso de direitos
	Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros	Abuso de direitos
	Inexistência de procedimento de monitoramento das instalações de processamento de informações	Abuso de direitos
	Inexistência de auditorias periódicas (supervisão)	Abuso de direitos
	Inexistência de procedimentos para a identificação, análise e avaliação de riscos	Abuso de direitos
	Inexistência de relatos de falha nos arquivos ("logs") de auditoria das atividades de administradores e operadores	Abuso de direitos
	Resposta inadequada do serviço de manutenção	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Acordo de nível de serviço (SLA - da sigla do termo em inglês) inexistente ou insuficiente	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Inexistência de procedimento de controle de mudanças	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Inexistência de um procedimento formal para o controle da documentação do SGSI	Comprometimento dos dados
	Inexistência de um procedimento formal para a supervisão dos registros do SGSI	Comprometimento dos dados
	Inexistência de um processo formal para a autorização das informações disponíveis publicamente	Dados de fontes não confiáveis
	Atribuição inadequada das responsabilidades pela segurança da informação	Repúdio de Ações
	Inexistência de um plano de continuidade	Falha de equipamento
	Inexistência de política de uso de correspondência eletrônica (<i>e-mail</i>)	Erro durante o uso
	Inexistência de procedimentos para a instalação de <i>software</i> em sistemas operacionais	Erro durante o uso
	Ausência de registros nos arquivos de auditoria ("logs") de administradores e operadores	Erro durante o uso
	Inexistência de procedimentos para a manipulação de informações classificadas	Erro durante o uso

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Organização	Ausência das responsabilidades ligadas à segurança da informação nas descrições de cargos e funções	Erro durante o uso
	Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com funcionários	Processamento ilegal de dados
	Inexistência de um processo disciplinar no caso de incidentes relacionados à segurança da informação	Furto de equipamentos
	Inexistência de uma política formal sobre o uso de computadores móveis	Furto de equipamentos
	Inexistência de controle sobre ativos fora das dependências	Furto de equipamentos
	Política de mesas e telas limpas (“ <i>clear desk and clear screen</i> ”) inexistente ou insuficiente	Furto de mídia ou documentos
	Inexistência de autorização para as instalações de processamento de informações	Furto de mídia ou documentos
	Inexistência de mecanismos estabelecidos para o monitoramento de violações da segurança	Furto de mídia ou documentos
	Inexistência de análises críticas periódicas por parte da direção	Uso não autorizado de equipamento
	Inexistência de procedimentos para o relato de fragilidades ligadas à segurança	Uso não autorizado de equipamento
	Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual	Uso de cópias de <i>software</i> falsificadas ou ilegais

D.2 Métodos para a avaliação de vulnerabilidades técnicas

Métodos proativos, como testar os sistemas de informação, podem ser utilizados para identificar as vulnerabilidades existentes, dependendo da criticidade do sistema de Tecnologia da Informação e Comunicação (TIC) e dos recursos disponíveis (por exemplo, verba alocada, tecnologia disponível, profissionais com a experiência necessária para a realização do teste). Entre os métodos de teste temos:

- ferramentas automatizadas de procura por vulnerabilidades;
- avaliação e testes da segurança;
- teste de invasão, e
- análise crítica de código.

Ferramentas automatizadas de procura por vulnerabilidades são utilizadas para varrer um grupo de computadores ou uma rede em busca de serviços reconhecidamente vulneráveis (por exemplo, o protocolo de transferência anônima de arquivos – “*anonymous FTP*” – e o recurso de retransmissão

do “*sendmail*” - “*sendmail relaying*”). Convém ressaltar, contudo, que nem todas as potenciais vulnerabilidades encontradas pela ferramenta necessariamente representam vulnerabilidades reais no contexto do sistema e de seu ambiente. Por exemplo, algumas dessas ferramentas de varredura avaliam as vulnerabilidades potenciais sem levar em consideração o ambiente da instalação e os seus requisitos. Algumas das vulnerabilidades encontradas pelo *software* de varredura podem não representar uma vulnerabilidade real em uma determinada instalação, mas sim o resultado de uma configuração requerida por seu ambiente. Assim, esse método de teste pode gerar falsos positivos.

A avaliação e testes da segurança (ATS) é uma outra técnica que pode ser utilizada na identificação de vulnerabilidades em sistemas de TIC durante o processo de avaliação de riscos. Ela inclui o desenvolvimento e a execução de planos de teste (por exemplo: roteiros e procedimentos para testes, lista de resultados previstos). O propósito dos testes da segurança do sistema é verificar a eficácia dos controles de segurança de um sistema de TIC, considerando-se a forma com que estão implementados no ambiente operacional. O objetivo é assegurar que os controles aplicados satisfazem às especificações de segurança do *software* e do *hardware*, implementam a política de segurança da organização, e/ou atendem aos padrões de mercado.

Testes de invasão podem ser usados para complementar o processo de análise crítica dos controles de segurança, assegurando-se que as diversas facetas do sistema de TIC estão protegidas. Testes de invasão, quando utilizados durante o processo de avaliação de riscos, servem para avaliar a capacidade do sistema de TIC de resistir a tentativas intencionais de se driblar a segurança do sistema. O objetivo é testar o sistema de TIC do ponto de vista da fonte da ameaça, identificando possíveis falhas no esquema de proteção do sistema.

A análise crítica de código é a mais minuciosa (embora também a mais dispendiosa) forma de avaliação de vulnerabilidades.

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

É importante notar que ferramentas e técnicas de invasão podem gerar resultados falsos quando a vulnerabilidade não é explorada com sucesso. Para explorar vulnerabilidades específicas, a exata configuração do sistema, da aplicação e das atualizações (“*patches*”) instaladas no sistema testado precisa ser conhecida. Se esses dados não são conhecidos quando o teste está sendo realizado, pode não ser possível explorar uma determinada vulnerabilidade com sucesso (por exemplo, o acesso remoto a “*shell*” reverso); no entanto, ainda assim, talvez seja possível causar uma pane no sistema ou processo testado ou mesmo forçar o seu reinício. Nesse caso, convém que o objeto testado seja considerado vulnerável.

Entre os métodos existentes, temos os seguintes:

- entrevistas com pessoas e usuários;
- questionários;
- inspeção física;
- análise de documentos.

Anexo E

(informativo)

Abordagens para o processo de avaliação de riscos de segurança da informação

E.1 Processo de avaliação de riscos de segurança da informação – Enfoque de alto nível

Uma avaliação de alto nível permite definir prioridades e uma cronologia para a execução das ações. Por várias razões, como por exemplo o orçamento, talvez não seja possível implementar todos os controles simultaneamente e, com isso, somente os riscos mais críticos podem ser tratados durante o processo de tratamento do risco. Da mesma forma, pode ser prematuro dar início a uma forma de gestão de riscos muito detalhada se a implementação só será contemplada após um ou dois anos. Para alcançar esse objetivo, uma avaliação de alto nível pode começar com um exame também de alto nível das consequências, em vez de começar por uma análise sistemática das ameaças, vulnerabilidades, ativos e consequências.

Outra razão para começar por uma avaliação de alto nível é permitir a sincronização com outros planos relacionados à gestão de mudanças (ou da continuidade de negócios). Por exemplo, não é razoável completar a implementação da segurança de um sistema ou aplicação se estiver sendo planejada a sua terceirização em um futuro próximo, embora possa ainda ser útil para a realização do processo de avaliação de riscos, para que se possa definir os termos do contrato da terceirização.

Características de um processo de avaliação de riscos alto nível pode incluir o seguinte:

- O processo de avaliação de riscos com enfoque de alto nível pode se preocupar com uma visão mais global da organização e de seus sistemas de informação, considerando os aspectos tecnológicos de forma independente das questões de negócio. Dessa forma, a análise do contexto incide mais sobre o negócio e o ambiente operacional do que sobre os elementos tecnológicos.
- O processo de avaliação de riscos com enfoque de alto nível pode se preocupar com uma lista menor de ameaças e vulnerabilidades, agrupando-as em domínios predefinidos, ou, para acelerar o processo, pode focar a sua atenção nos cenários de risco ou ataque, em vez de em seus elementos.
- Os riscos cobertos por uma avaliação com enfoque de alto nível podem ser entendidos mais como categorias (ou classes gerais) de risco do que, propriamente, como riscos identificados com especificidade. Como os cenários ou as ameaças são agrupados em domínios, o tratamento do risco propõe listas de controle para esses domínios. Então, em primeiro lugar, durante as atividades de tratamento do risco, propõe-se e selecionam-se os controles comuns válidos em todo o sistema.
- Contudo, por raramente tratar de detalhes tecnológicos, o processo de avaliação de riscos com enfoque de alto nível é mais adequado para fornecer controles organizacionais e não técnicos, além dos aspectos gerenciais de controles técnicos e mecanismos técnicos de proteção comuns e muito importantes, como cópias de segurança (“*back-ups*”) e antivírus.

As vantagens do processo de avaliação de riscos com um enfoque de alto nível são as seguintes:

- Com a incorporação de uma primeira abordagem simples é mais provável que se obtenha a aceitação do programa do processo de avaliação de riscos.
- Convém que seja possível criar uma visão estratégica de um programa corporativo de segurança da informação, ou seja, uma visão que possa auxiliar durante o planejamento.
- Recursos e verbas podem ser aplicados onde forem mais vantajosos, e os sistemas que estão, provavelmente, precisando de mais proteção são tratados primeiro.

Como as análises de risco iniciais são feitas com um enfoque de alto nível e potencialmente sendo menos exatas, a única potencial desvantagem é que alguns processos de negócio ou sistemas possam acabar, erroneamente, não sendo identificados entre aqueles que requerem um segundo processo de avaliação de riscos, mais detalhado. Isso pode ser evitado se houver informação adequada sobre todos os aspectos da organização, das informações que utiliza e de seus sistemas, incluindo dados obtidos por meio da avaliação dos incidentes de segurança da informação.

O processo de avaliação de riscos com enfoque de alto nível considera os valores para o negócio dos ativos de informação, e os riscos do ponto de vista de negócio da organização. No primeiro ponto de decisão (ver Figura 2), vários fatores ajudam a determinar se a avaliação de alto nível é adequada para o tratamento do risco; esses fatores podem incluir os seguintes itens:

- os objetivos de negócios a serem alcançados por meio de vários ativos de informação;
- o quanto o negócio da organização depende de cada ativo de informação, ou seja, o quanto as funções que a organização considera fundamentais para a sua sobrevivência ou para a condução eficaz do negócio depende dos ativos, ou da confidencialidade, da integridade, da disponibilidade, da garantia do não repúdio, da responsabilização, da autenticidade e da confiabilidade das informações armazenadas e processadas nesses ativos;
- o nível de investimento em cada ativo de informação, em termos do desenvolvimento, da manutenção ou da reposição do ativo, e
- os ativos de informação, para cada um dos quais a organização atribui um valor.

Quando esses fatores são avaliados, a decisão torna-se mais fácil. Se a função de um ativo é extremamente importante para a condução do negócio da organização ou se o ativo está exposto a riscos de alto impacto ou probabilidade, então convém que uma segunda iteração, com um processo de avaliação detalhado de riscos, seja executada tendo em vista o ativo de informação específico (ou parte dele).

Uma regra geral para ser aplicada é a seguinte: se a falta de segurança da informação puder resultar em consequências adversas significativas para a organização, para os seus processos de negócio ou para os seus ativos, uma segunda iteração, mais detalhada, do processo de avaliação de riscos será necessária para a identificação de riscos potenciais.

E.2 Processo detalhado de avaliação de riscos de segurança da informação

E.2.1 Generalidades

O processo de avaliação de riscos de segurança da informação detalhado envolve a minuciosa identificação e valoração dos ativos, a avaliação das ameaças aos ativos, e a avaliação das vulnerabilidades. Os resultados dessas atividades são, então, usados para avaliar os riscos e, depois, para identificar o tratamento do risco.

A etapa detalhada normalmente demanda bastante tempo, esforço e experiência, e pode, portanto, ser mais adequada para os sistemas de informação de alto risco.

A etapa final do processo de avaliação de riscos de segurança da informação detalhado consiste no cálculo do risco total, que é o assunto deste Anexo.

As consequências podem ser avaliadas de várias maneiras, incluindo a abordagem quantitativa (usando-se, por exemplo, uma unidade monetária), a qualitativa (que podem ser baseada no uso de adjetivos qualificadores tais como moderado ou severo) ou ainda uma combinação de ambas. Para avaliar a probabilidade de ocorrência de uma ameaça, convém que se estabeleça o período no qual o ativo é considerado como de valor ou durante o qual ele precisará ser protegido. A probabilidade da ocorrência de uma ameaça específica é afetada pelos seguintes itens:

- a atratividade do ativo ou do impacto potencial, aplicável quando uma ameaça intencional de origem humana estiver sendo considerada;
- a facilidade de converter a exploração de uma vulnerabilidade de um ativo em recompensa, aplicável quando uma ameaça intencional de origem humana está sendo considerada;
- a capacitação técnica do agente da ameaça, aplicável a ameaças intencionais de origem humana; e
- a susceptibilidade da vulnerabilidade à exploração, aplicável tanto a vulnerabilidades técnicas quanto a não técnicas.

Muitos métodos fazem uso de tabelas, e combinam medidas empíricas com medições subjetivas. É importante que a organização use um método com o qual ela se sinta confortável, no qual ela acredite, e que produza resultados reproduzíveis. Alguns exemplos de métodos baseados em tabelas são apresentados a seguir.

Para orientação adicional e técnicas que podem ser usadas para o processo de avaliação de riscos em segurança da informação ver ABNT NBR IEC 31010.

Os seguintes exemplos usam números para descrever processos de avaliação qualitativa. Convém que usuários destes métodos estejam cientes que pode ser inválido realizar operações matemáticas adicionais usando estes números que são resultados qualitativos produzidos por métodos qualitativos de avaliação de riscos.

E.2.2 Exemplo 1 – Matriz com valores predefinidos

Neste tipo de método para o processo de avaliação de riscos, ativos físicos, existentes ou planejados, são valorados conforme seus custos de reposição ou reconstrução (ou seja, medidas quantitativas). Esses custos são então convertidos para a mesma escala qualitativa usados para a valoração das informações (ver a seguir). Ativos do tipo *software*, existentes ou planejados, são valorados da

mesma forma que ativos físicos, com os custos de aquisição ou reposição sendo identificados e então convertidos para a mesma escala qualitativa usada para a valoração das informações. Além disso, se um *software* aplicativo tiver o seu próprio conjunto de requisitos de confidencialidade ou de integridade (por exemplo, se o seu código-fonte, por si só, for susceptível a questões comerciais), ele é valorado da mesma forma que as informações.

Os valores atribuídos às informações são obtidos por entrevista com gestores do negócio selecionados (os “responsáveis pelos dados”), que podem falar autoritativamente sobre os dados. Assim são determinados o valor e a sensibilidade dos dados em uso, armazenados, sendo processados ou acessados. As entrevistas facilitam a avaliação do valor e da sensibilidade da informação, tendo em vista os cenários com os piores impactos que possam ser previstos a partir das consequências adversas ao negócio causadas pela divulgação ou modificação não autorizadas da informação, por sua indisponibilidade durante diferentes períodos de tempo ou ainda por sua destruição.

A valoração é realizada usando diretrizes para a valoração da informação, as quais cobrem alguns temas, como:

- segurança física das pessoas;
- informações pessoais;
- obrigações legais e regulatórias;
- cumprimento das leis;
- interesses comerciais e econômicos;
- perda financeira/ interrupção de atividades;
- ordem pública;
- política e operações do negócio;
- perda de valor de mercado (em especial com referência a aspectos intangíveis), e
- contrato ou acordo com clientes.

As diretrizes facilitam a identificação dos valores em uma escala numérica, como a escala de 0 a 4 apresentada adiante na forma de uma matriz. Assim, permite-se o reconhecimento de valores quantitativos, sempre que possível e lógico, e de valores qualitativos quando valores quantitativos não são possíveis, por exemplo: em ocasiões em que a vida humana é colocada em perigo.

A próxima atividade importante é a conclusão de pares de questionários, para cada tipo de ameaça e para cada agrupamento de ativos relacionado a um tipo de ameaça, a fim de permitir a avaliação do nível das ameaças (probabilidade de ocorrência) e das vulnerabilidades (facilidade com que uma ameaça pode explorar uma vulnerabilidade e provocar consequências adversas). Cada questão respondida indica uma pontuação. Essas pontuações são acumuladas em uma base de conhecimento e comparadas a intervalos. Isso identifica o nível da ameaça em uma escala, digamos, de alto a baixo e, de forma similar, os níveis das vulnerabilidades - como ilustrado no exemplo da matriz mais adiante. Diferenciam-se os tipos de consequências na medida de suas relevâncias. Convém que informações para completar os questionários sejam reunidas a partir de entrevistas com as pessoas responsáveis pelas acomodações, os recursos humanos e os técnicos envolvidos, assim como também a partir de inspeções físicas dos locais e da análise crítica de documentos.

Os valores dos ativos, e os níveis de ameaça e vulnerabilidade, relacionados a cada tipo de consequência, são emparelhados em uma matriz como a apresentada a seguir, a fim de identificar, para cada combinação, a medida do risco em uma escala de 0 a 8. Os valores são colocados na matriz de uma maneira estruturada. Um exemplo é dado a seguir:

Tabela E.1

	Probabilidade da ocorrência – Ameaça	Baixa			Média			Alta		
	Facilidade de Exploração	B	M	A	B	M	A	B	M	A
Valor do Ativo	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Para cada ativo, as vulnerabilidades relevantes e respectivas ameaças são consideradas. Se houver uma vulnerabilidade sem uma ameaça correspondente, ou uma ameaça sem uma vulnerabilidade correspondente, então não há risco nesse momento (mas convém que cuidados sejam tomados no caso dessas situações mudarem). A linha apropriada é identificada na matriz pelo valor do ativo, e a coluna apropriada é identificada pela probabilidade da ocorrência da ameaça e a facilidade de exploração. Por exemplo, se o ativo tem o valor 3, a ameaça é “alta”, e a vulnerabilidade é “baixa”, a medida do risco é 5. Supondo-se que um ativo tenha um valor 2 (por exemplo, para modificações), o nível de ameaça é “baixo” e a facilidade de exploração é “alta”, logo, a medida de risco é 4. O tamanho da matriz pode ser adaptado às necessidades da organização, ajustando-se o número das colunas representando a probabilidade de ocorrência das ameaças ou daquelas que representam a facilidade de exploração, assim como as linhas que representam a valoração dos ativos. A adição de colunas e linhas implica em novas medidas de risco. A vantagem dessa abordagem está na ordenação dos riscos a serem tratados.

Uma matriz similar como apresentada na Tabela E.2 mostra a relação entre a probabilidade de um cenário de incidente e o impacto estimado, do ponto de vista do negócio. A probabilidade de um cenário de incidente é dada pela probabilidade de uma ameaça vir a explorar uma vulnerabilidade. A Tabela relaciona o impacto ao negócio, relativo ao cenário de incidente, àquela probabilidade. O risco resultante é medido em uma escala de 0 a 8, e pode ser avaliado tendo como base os critérios para a aceitação do risco. Essa escala de risco pode também ser convertida em uma classificação simples, mais genérica, do risco, como por exemplo:

- Baixo risco: 0 a 2;
- Médio risco: 3 a 5;
- Alto risco: 6 a 8.

Tabela E.2

	Probabilidade do cenário de incidente	Muito baixa (Muito improvável)	Baixa (Improvável)	Média (Possível)	Alta (Provável)	Muito alta (Frequente)
Impacto no negócio	Muito baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito alto	4	5	6	7	8

E.2.3 Exemplo 2 – Ordenação de Ameaças em função do Risco

Uma tabela ou matriz como apresentada na Tabela E.3 pode ser usada para relacionar as consequências (representadas pelo valor do ativo) à probabilidade de ocorrência de uma ameaça (incluindo assim os fatores ligados às vulnerabilidades). A primeira etapa consiste em avaliar as consequências (através do valor do ativo) em uma escala predefinida, por exemplo: de 1 a 5, para cada ativo ameaçado (coluna 'b' na Tabela). Na segunda etapa, estima-se a probabilidade de ocorrência da ameaça em uma escala predefinida, por exemplo: de 1 a 5, para cada ameaça (coluna 'c' na tabela). Na terceira etapa, calcula-se a medida de risco multiplicando ($b \times c$). Por último, as ameaças podem ser ordenadas em sequência conforme suas respectivas medidas de risco. Notar que nesse exemplo, 1 representa a menor consequência e a menor probabilidade de ocorrência.

Tabela E.3

Rótulo identificador da ameaça (a)	Valor da consequência (do ativo) (b)	Probabilidade de ocorrência da ameaça (c)	Medida do risco (d)	Ordem da ameaça (e)
Ameaça A	5	2	10	2
Ameaça B	2	4	8	3
Ameaça C	3	5	15	1
Ameaça D	1	3	3	5
Ameaça E	4	1	4	4
Ameaça F	2	4	8	3

Como mostrado anteriormente, esse procedimento permite que diferentes ameaças, com consequências e probabilidade de ocorrências distintas, sejam comparadas e ordenadas por prioridade. Em alguns casos, é necessário associar valores monetários às escalas empíricas utilizadas.

E.2.4 Exemplo 3 – Avaliando a probabilidade e as possíveis consequências dos riscos

Nesse exemplo, a ênfase é dada às consequências dos incidentes de segurança da informação (ou seja, aos cenários de incidentes) e convém que a atividade determine quais os sistemas priorizados.

Isso é feito estimando dois valores para cada par de ativo e risco, os quais, combinados, determinam a pontuação para cada ativo. Quando as pontuações de todos os ativos do sistema são somadas, uma medida do risco ao qual o sistema está submetido pode então ser determinada.

Primeiramente, um valor é designado para cada ativo. Esse valor é referente às possíveis consequências adversas que podem surgir quando o ativo é ameaçado. O valor (do ativo) é definido para cada ameaça aplicável ao ativo.

Depois, estima-se um valor para a probabilidade. Ela é avaliada combinando a probabilidade de ocorrência da ameaça e a facilidade com que a vulnerabilidade pode ser explorada. Ver, na Tabela E.4, a representação da probabilidade de um cenário de incidente.

Tabela E.4

4) Probabilidade da ameaça	5) Baixa			6) Média			7) Alta		
8) Nível da vulnerabilidade	B	M	A	B	M	A	B	M	A
9) Probabilidade do cenário de incidente	0	1	2	1	2	3	2	3	4

Em seguida, na Tabela E.5, uma pontuação referente ao par ativo/ameaça é definida pelo encontro da coluna com o valor do ativo e da linha com a probabilidade. As pontuações referentes aos pares ativos/ameaça são totalizadas para cada ativo, produzindo-se uma pontuação total do ativo. Esse valor pode ser usado para diferenciarmos os ativos que fazem parte de um mesmo sistema, entre si.

Tabela E.5

10) Valor do ativo	0	1	2	3	4
11) Probabilidade					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Na etapa final, somam-se as pontuações dos ativos do sistema, estabelecendo-se a pontuação do sistema. Isso pode ser usado para diferenciarmos os sistemas entre si, e determinar qual sistema convém que seja protegido com maior prioridade.

Nos exemplos a seguir, todos os valores foram escolhidos aleatoriamente.

Supondo-se que o Sistema S tenha três ativos A1, A2 e A3. Supondo-se também que existam duas ameaças, T1 e T2, aplicáveis ao sistema S. Estabelecendo que o valor de A1 é 3, que o valor do ativo A2 é 2 e que o valor do ativo A3 é 4.

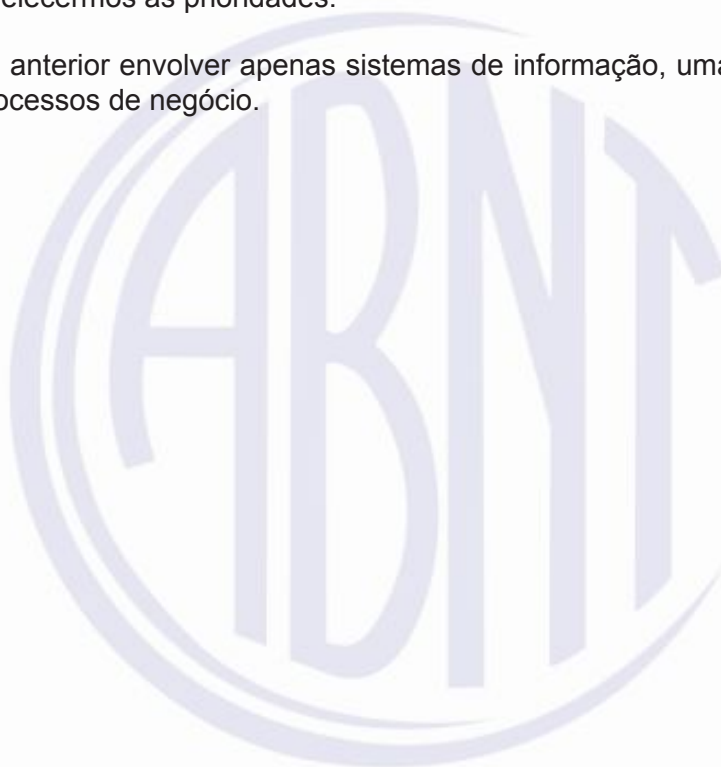
Se, para A1 e T1, a probabilidade da ameaça é baixa e a facilidade de exploração da vulnerabilidade é média, então o valor da probabilidade é 1 (ver Tabela E.4).

A pontuação referente ao par ativo/ameaça A1/T1 pode ser obtida na Tabela E.5, no encontro da coluna com o valor 3 (referente ao valor do ativo) e da linha com o valor 1 (referente à probabilidade). O valor assim obtido é 4. Do mesmo modo, para A1/T2, se a probabilidade da ameaça for média e a facilidade de exploração da vulnerabilidade for alta, o resultado será uma pontuação de 6, referente ao par A1/T2.

Agora, a pontuação total TA1 pode ser calculada, e o resultado é 10. A pontuação total do ativo é calculada para cada ativo considerando todas as ameaças aplicáveis. A pontuação total do sistema é calculada pela adição TA1 + TA2 + TA3, obtendo-se TS.

Assim, sistemas diferentes podem ser comparados, assim como diferentes ativos dentro do mesmo sistema, para estabelecermos as prioridades.

Apesar do exemplo anterior envolver apenas sistemas de informação, uma abordagem similar pode ser aplicada aos processos de negócio.



Anexo F (informativo)

Restrições para a modificação do risco

Ao considerar as restrições para a modificação do risco, convém que as seguintes restrições sejam consideradas:

— Restrições temporais

Pode haver muitos tipos de restrições de tempo. Por exemplo, convém que os controles sejam implementados dentro de um período de tempo aceitável para os gestores da organização. Outro tipo de restrição temporal é se um controle pode ser implementado durante o período de vida útil da informação ou do sistema. Um terceiro tipo de restrição temporal pode ser representado pelo período de tempo que os gestores da organização definem como aceitável para ficar exposto a um determinado risco.

— Restrições financeiras

Convém que a implementação ou a manutenção dos controles não sejam mais custosos do que o valor dos riscos que eles foram projetados para proteger. Convém que todos os esforços sejam feitos para que os orçamentos alocados não sejam excedidos, e também para que vantagens financeiras, pelo uso de controles, sejam obtidas. Contudo, em alguns casos, pode não ser possível implementar a segurança desejada e alcançar o nível de risco formalmente aceito, devido a restrições orçamentárias. Essa situação requer, então, uma decisão dos gestores da organização para a sua resolução.

Convém que se tenha muito cuidado no caso de restrições orçamentárias provocarem a redução do número ou da qualidade dos controles a serem implementados, pois isso pode levar à aceitação implícita de mais riscos do que o planejado. Convém que a utilização do orçamento alocado para os controles como fator limitante, se necessária, seja acompanhada por cuidados especiais.

— Restrições técnicas

Problemas técnicos, como a compatibilidade de *hardware* ou de programas, podem ser facilmente evitados se forem levados em conta durante a seleção dos controles. Além disso, a implementação retroativa dos controles em um processo ou sistema existente é frequentemente dificultada por restrições técnicas. Essas dificuldades podem deslocar o foco dos controles em direção aos aspectos procedurais e físicos da segurança. Pode ser necessário revisar os programas de segurança da informação, a fim de alcançar os objetivos de segurança. Isso pode ocorrer quando controles não conseguem atingir os resultados previstos na modificação do risco sem afetar a produtividade.

— Restrições operacionais

Restrições operacionais, como por exemplo, a necessidade de manter as operações em um regime de 24/7 e, ainda assim, executar “*back-ups*”, podem resultar em controles de implementação complexa e onerosa, a menos que eles sejam incorporados ao projeto desde o início.

— Restrições culturais:

As restrições culturais em relação à seleção de controles podem ser específicas a um país, a um setor, a uma organização ou mesmo a um departamento dentro de uma organização. Nem todos os controles podem ser aplicados em todos os países. Por exemplo, pode ser possível implementar buscas em bolsas e bagagens em partes da Europa, mas não em partes do Oriente Médio. Não é possível ignorar aspectos culturais, pois muitos controles contam com o apoio ativo do pessoal. Se o pessoal não compreende a necessidade do controle ou não acham que ele seja culturalmente aceitável, o controle se tornará ineficaz ao passar do tempo.

— Restrições éticas:

As restrições éticas podem ter grandes implicações sobre os controles na medida em que a ética muda tendo como base as normas sociais. Isso pode impedir a implementação de alguns controles em alguns países, como por exemplo, a varredura de correspondência eletrônica (“*email scanning*”). A privacidade das informações pode ser entendida de diferentes maneiras dependendo da ética da região ou do governo. Essas questões podem causar maiores preocupações em alguns setores de atividade econômica do que em outros, por exemplo: o setor governamental e o da saúde.

— Restrições ambientais

Fatores ambientais, como a disponibilidade de espaço, condições climáticas extremas e o meio geográfico natural ou urbano, podem influenciar a seleção de controles. Por exemplo, instalações à prova de terremoto podem ser necessárias em alguns países, porém desnecessárias em outros.

— Facilidade de uso:

Uma interface de usuário mal projetada resulta em erro humano e pode tornar o controle inútil. Convém que os controles selecionados sejam de fácil utilização, além de garantirem um nível aceitável de risco residual ao negócio. Os controles de difícil utilização têm sua eficácia prejudicada, já que os usuários tentarão contorná-los ou ignorá-los tanto quanto possível. Controles de acesso complexos dentro da organização podem estimular os usuários a acharem algum método de acesso alternativo não autorizado.

— Restrições de recursos humanos:

Convém que sejam considerados o custo salarial e a disponibilidade de profissionais com as competências especializadas necessárias para a implementação dos controles, bem como a capacidade de deslocar o pessoal em condições adversas de operação. O conhecimento necessário para a implementação dos controles planejados pode não estar prontamente disponível ou pode representar um custo excessivo para a organização. Outros aspectos como a tendência de parte do pessoal discriminar outros membros da equipe que não passaram por verificações de segurança, podem ter grandes implicações para as políticas e práticas de segurança. Além disso, a necessidade de achar e contratar as pessoas certas para o trabalho pode resultar na sua contratação antes que as verificações de segurança sejam concluídas. Requerer que a verificação de segurança seja finalizada antes da contratação é a prática normal e a mais segura.

— Restrições ligadas à integração dos controles novos aos já existentes:

A integração de controles novos a uma infraestrutura existente e a interdependência entre controles são fatores frequentemente ignorados. Controles novos podem não ser facilmente implementados

se houver incongruência ou incompatibilidade com controles existentes. Por exemplo, um plano para usar dispositivos de identificação biométrica para controle de acesso físico pode conflitar com um sistema que se baseie na digitação de números de identificação pessoal (PIN, conforme a sigla em Inglês) para o controle de acesso. Convém que o custo da mudança dos controles existentes para os planejados inclua também os itens a serem adicionados ao custo geral do tratamento do risco. Talvez não seja possível implementar alguns dos controles selecionados devido aos conflitos com os controles atuais.



Bibliografia

- [1] ABNT ISO Guia 73, *Gestão de riscos – Vocabulário – Recomendações para uso em normas*
- [2] ISO/IEC 16085, *Systems and software engineering – Life cycle processes – Risk management*
- [3] ABNT NBR ISO/IEC 27001, *Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação*
- [4] ABNT NBR ISO/IEC 27002, *Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação*
- [5] ABNT NBR ISO 31000, *Gestão de riscos – Princípios e diretrizes*
- [6] NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*
- [7] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology*