Apostila

NBR ISO IEC 27005:2011
Gestão de riscos de segurança da informação

Sumário

Página

Prefácio Nacional 4
Introdução 4
1 Escopo 4
2 Referências normativas 5
3 Termos e definições 5
4 Organização da Norma 10
5 Contextualização 11
6 Visão geral do processo de gestão de riscos de segurança da informação 11
7 Definição do contexto 15
7.1 Considerações Gerais 15
7.2 Critérios básicos 16
7.2.1 Abordagem da gestão de riscos 16
7.2.2 Critérios para a avaliação de riscos 16
7.2.3 Critérios de impacto 17
7.2.4 Critérios para a aceitação do risco 17
7.3 Escopo e limites 18
7.4 Organização para gestão de riscos de segurança da informação 19
8 Processo de avaliação de riscos de segurança da informação 20
8.1 Descrição geral do processo de avaliação de riscos de segurança da informação 20
8.2 Identificação de riscos 21
8.2.1 Introdução à identificação de riscos 21
8.2.2 Identificação dos ativos 21
8.2.3 Identificação das ameaças 22
8.2.4 Identificação dos controles existentes 22
8.2.5 Identificação das vulnerabilidades 24
8.2.6 Identificação das consequências 24
8.3 Análise de riscos 25
8.3.1 Metodologias de análise de riscos 25
8.3.2 Avaliação das consequências 27
8.3.3 Avaliação da probabilidade dos incidentes 28
8.3.4 Determinação do nível de risco 29
8.4 Avaliação de riscos 29
9 Tratamento do risco de segurança da informação 30
9.1 Descrição geral do processo de tratamento do risco 30
9.2 Modificação do risco 33
9.3 Retenção do risco 34
9.4 Ação de evitar o risco 34
9.5 Compartilhamento do risco 34
10 Aceitação do risco de segurança da informação 35
11 Comunicação e consulta do risco de segurança da informação 35
12 Monitoramento e análise crítica de riscos de segurança da informação 37

12.1 Monitoramento e análise crítica dos fatores de risco 37

12.2 Monitoramento, análise crítica e melhoria do processo de gestão de riscos 38

Anexo A (informativo) **Definindo o escopo e os limites do processo de gestão de riscos de segurança da informação 40**

A.1 A análise da organização 40

A.2 Restrições que afetam a organização 41

A.3 Referências legais e regulamentares aplicáveis à organização 44

A.4 Restrições que afetam o escopo 44

Anexo B (informativo) **Identificação e valoração dos ativos e avaliação do impacto 46**

B.1 Exemplos de identificação de ativos 46

B.1.1 Identificação dos ativos primários 46

B.1.2 Lista e descrição de ativos de suporte 47

B.2 Valoração dos Ativos 53

B.3 Avaliação do Impacto 57

Anexo C (informativo) **Exemplos de ameaças comuns 59**

Anexo D (informativo) **Vulnerabilidades e métodos de avaliação de vulnerabilidades 62**

D.1 Exemplos de vulnerabilidades 62

D.2 Métodos para a avaliação de vulnerabilidades técnicas 67

Anexo E (informativo) **Abordagens para o processo de avaliação de riscos de segurança da informação 69**

E.1 Processo de avaliação de riscos de segurança da informação - Enfoque de alto nível 69

E.2 Processo detalhado de avaliação de riscos de segurança da informação 71

E.2.1 Exemplo 1 Matriz com valores pré-definidos 71

E.2.2 Exemplo 2 Ordenação de Ameaças em função do Risco 74

E.2.3 Exemplo 3 Avaliando a probabilidade e as possíveis consequências dos riscos 75

Anexo F (informativo) **Restrições para a modificação do risco 77**

Anexo G (informativo) **Diferenças nas definições entre a ABNT NBR ISO/IEC 27005:2008 e a ABNT NBR ISO/IEC 27005:2011 80**

Bibliografia 94

Introdução

Esta apostila apresenta as diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a ABNT NBR ISO/IEC 27001:2006. Entretanto, esta não inclui um método específico para a gestão de riscos de segurança da informação. Cabe à organização definir sua abordagem ao processo de gestão de riscos, levando em conta, por exemplo, o escopo do seu 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 nesta Norma Internacional para implementar os requisitos de um SGSI.

A Norma 27005:2011 é do interesse de 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.

1 Escopo

A Norma 27005:2011 fornece diretrizes para o processo de gestão de riscos de segurança da informação.

A Norma 27005:2011 está de acordo com os conceitos especificados na ABNT NBR ISO/IEC 27001:2006 e foi elaborada 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 27001:2006 e na ABNT NBR ISO/IEC 27002:2005 é importante para um entendimento completo desta Norma Internacional.

A Norma 27005:2011 se aplica a todos os tipos de organização (por exemplo: empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos), que pretendam gerir os riscos que poderiam comprometer a segurança da informação da organização.

2 Referências normativas

Os documentos citados a seguir são indispensáveis para a correta aplicação desta Norma. Para as referências com datas, apenas a edição citada é válida. Para as referências sem data específica, vale apenas a versão oficial mais recente do referido documento (incluindo possíveis correções).

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

ABNT NBR ISO/IEC 27001: 2006, *Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.*

Termos e definições

3.1
consequência
resultado de um **evento** (3.3) que afeta os objetivos

[ABNT ISO GUIA 73:2009]

NOTA 1 Um evento pode levar a uma série de consequências.

NOTA 2 Uma consequência pode ser certa ou incerta e, no contexto da segurança da informação, é, normalmente, negativa..

NOTA 3 As consequências podem ser expressas qualitativa ou quantitativamente.

NOTA 4 As consequências iniciais podem desencadear reações em cadeia

3.2
controle
medida que está modificando o **risco** (3.9)

[ABNT ISO GUIA 73:2009]

NOTA 1 Os controles da segurança da informação incluem qualquer processo, política, procedimento, diretriz, prática ou estrutura organizaconal, que pode ser de natureza administrativa, técnica, gerencial ou legal que modificam o risco da segurança da informação.

NOTA 2 Os controles nem sempre conseguem exercer o efeito de modificação pretendido ou presumido.

NOTA 3 Controle também é usado como um sinônimo de salvaguarda ou contramedida.

3.3
evento
ocorrência ou mudança em um conjunto específico de circunstâncias

[ABNT ISO GUIA 73:2009]

NOTA 1 Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas.

NOTA 2 Um evento pode consistir em alguma coisa não acontecer.

NOTA 3 Um evento pode algumas vezes ser referido como um "incidente" ou um "acidente".

3.4
contexto externo
ambiente externo no qual a organização busca atingir seus objetivos

[ABNT ISO GUIA 73:2009]

NOTA O contexto externo pode incluir:

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

— os fatores–chave e as tendências que tenham impacto sobre os objetivos da organização; e

— as relações com **partes interessadas** (3.2.1.1) externas e suas percepções e valores.

3.5
contexto interno
ambiente interno no qual a organização busca atingir seus objetivos

[ABNT ISO GUIA 73:2009]

NOTA O contexto interno pode incluir:

— governança, estrutura organizacional, funções e responsabilidades;

— políticas, objetivos e estratégias implementadas para atingi–los;

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

— sistemas de informação, fluxos de informação e processos de tomada de decisão (tanto formais como informais);

— relações com partes interessadas internas, e suas percepções e valores;

— cultura da organização;

— normas, diretrizes e modelos adotados pela organização; e

— forma e extensão das relações contratuais.

3.6
nível de risco
magnitude de um **risco** (3.9), expressa em termos da combinação das **consequências** (3.1) e de suas **probabilidades** (*likelihood*) (3.7)

[ABNT ISO GUIA 73:2009]

3.7
probabilidade (*likelihood*)
chance de algo acontecer

[ABNT ISO GUIA 73:2009]

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

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

3.8
risco residual
risco (3.9) remanescente após o **tratamento do risco** (3.17)

[ABNT ISO GUIA 73:2009]

NOTA 1 O risco residual pode conter riscos não identificados.

NOTA 2 O risco residual também pode ser conhecido como "risco retido".

3.9
risco
efeito da incerteza nos objetivos

[ABNT ISO GUIA 73:2009]

NOTA 1 Um efeito é um desvio em relação ao esperado – positivo e/ou negativo.

NOTA 2 Os objetivos podem ter diferentes aspectos (tais como metas financeiras, de saúde e segurança e ambientais) e podem aplicar–se em diferentes níveis (tais como estratégico, em toda a organização, de projeto, de produto e de processo).

NOTA 3 O risco é muitas vezes caracterizado pela referência aos **eventos** (3.3) potenciais e às **consequências** (3.1), ou uma combinação destes.

NOTA 4 O risco em segurança da informação é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a **probabilidade** (*likelihood*) (3.7) associada de ocorrência.

NOTA 5 A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

NOTA 6 O risco de segurança da informação está associado com o potencial de que ameaças possam explorar vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, consequentemente, causar dano a uma organização.

3.10
análise de riscos
processo de compreender a natureza do **risco** (3.9) e determinar o **nível de risco** (3.6)

[ABNT ISO GUIA 73:2009]

NOTA 1 A análise de riscos fornece a base para a **avaliação de riscos** (3.11) e para as decisões sobre o **tratamento de riscos** (3.17).

NOTA 2 A análise de riscos inclui a estimativa de riscos.

3.11
processo de avaliação de riscos[1)]
processo global de **identificação de riscos** (3.15), **análise de riscos** (3.10) e **avaliação de riscos** (3.14)

[ABNT ISO GUIA 73:2009]

3.12
comunicação e consulta
processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as **partes interessadas** (3.18), com relação a gerenciar **riscos** (3.9)

[ABNT ISO GUIA 73:2009]

NOTA 1 As informações podem referir-se à existência, natureza, forma, **probabilidade** (*likelihood*) (3.7), severidade, avaliação, aceitação e tratamento de riscos.

NOTA 2 A consulta é um processo bidirecional de comunicação sistematizada entre uma organização e suas partes interessadas ou outros, antes de tomar uma decisão ou direcionar uma questão específica. A consulta é:

— um processo que impacta uma decisão através da influência ao invés do poder; e

— uma entrada para o processo de tomada de decisão, e não uma tomada de decisão em conjunto.

3.13
critérios de risco
termos de referência contra os quais a significância de um **risco** (3.9) é avaliada

[ABNT ISO GUIA 73:2009]

NOTA 1 Os critérios de risco são baseados nos objetivos organizacionais e no **contexto externo** (3.4) e **contexto interno** (3.5).

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

3.14
avaliação de riscos
processo de comparar os resultados da **análise de riscos** (3.10) com os **critérios de risco** (3.13) para determinar se o **risco** (3.9) e/ou sua magnitude é aceitável ou tolerável

[ABNT ISO GUIA 73:2009]

NOTA A avaliação de riscos auxilia na decisão sobre o **tratamento de riscos** (3.17).

[1)] **NOTA DA TRADUÇÃO**: Para os efeitos deste documento o termo *risk assessment* foi traduzido como "processo de avaliação de riscos" (3.11) para evitar conflito com o termo *risk evaluation* que foi traduzido na ABNT NBR ISO 31000 como "avaliação de riscos" (3.14). Na ABNT NBR ISO/IEC 27001:2006, este termo está traduzido como "análise/avaliação de riscos".

3.15
identificação de riscos
processo de busca, reconhecimento e descrição de **riscos** (3.9)

[ABNT ISO GUIA 73:2009]

NOTA 1 A identificação de riscos envolve a identificação das fontes de risco, **eventos** (3.3), suas causas e suas **consequências** (3.1) potenciais.

NOTA 2 A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das **partes interessadas** (3.18).

3.16
gestão de riscos
atividades coordenadas para dirigir e controlar uma organização no que se refere a **riscos** (3.9)

[ABNT ISO GUIA 73:2009]

NOTA Esta Norma Internacional usa o termo "processo" para descrever toda a gestão de riscos. Os elementos contidos no processo de gestão de riscos foram chamados de "atividades".

3.17
tratamento de riscos
processo para modificar o **risco** (3.9)

[ABNT ISO GUIA 73:2009]

NOTA 1 O tratamento de risco pode envolver:

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

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

— a remoção da fonte de risco;

— a alteração da **probabilidade** (*likelihood*) (3.7);

— a alteração das **consequências** (3.1);

— o compartilhamento do risco com outra parte ou partes [incluindo contratos e financiamento do risco]; e

— a retenção do risco por uma escolha consciente.

NOTA 2 Os tratamentos de riscos relativos a consequências negativas são muitas vezes referidos como "mitigação de riscos", "eliminação de riscos", "prevenção de riscos" e "redução de riscos".

NOTA 3 O tratamento de riscos pode criar novos riscos ou modificar riscos existentes.

3.18
parte interessada
pessoa ou organização que pode afetar, ser afetada, ou perceber–se afetada por uma decisão ou atividade

[ABNT ISO GUIA 73:2009]

NOTA Um tomador de decisão pode ser uma *parte interessada*.

4 Organização da Norma

Esta Norma Internacional 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 (exemplos de ativos), o Anexo C dá 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 diferenças nas definições entre as normas ABNT NBR ISO/IEC 27005:2008 e a ABNT NBR ISO/IEC 27005:2011 são apresentadas no Anexo G.

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 diretrizes para a execução da ação. Algumas destas diretrizes podem não ser adequadas em todos os casos. 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 essa 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 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 trate os riscos 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:

— 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 quando as decisões de gestão de riscos são tomadas e mantidas informadas sobre a situação da gestão de riscos

— Eficácia do monitoramento do tratamento do risco

— Monitoramento e a 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

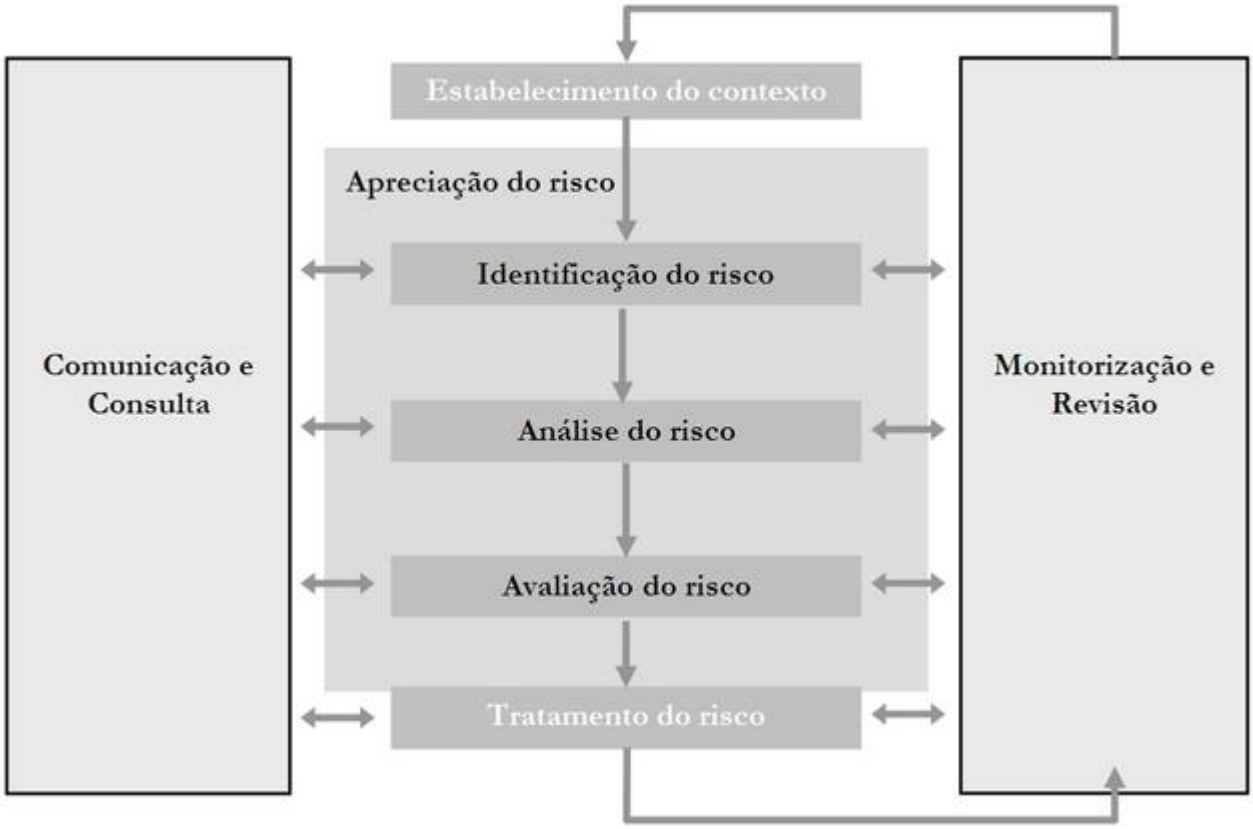
— Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los

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 31000:2009 e apresentado na Figura 1.

Figura 1 – O processo de gestão de riscos



A Figura 2 apresenta como esta Norma Internacional se aplica 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 determinem 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 continuar. 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.

Note que o tratamento de riscos 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 (veja 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. Isso 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 o gerenciamento de incidentes e ajudar a reduzir possíveis prejuízos. A conscientização dos gestores e pessoal no que diz respeito 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 27001:2006 especifica que os controles implementados no escopo, limites e contexto do SGSI devem ser baseados no risco. A aplicação de um processo de gestão de riscos de segurança da informação pode satisfazer esse requisito. Há vários métodos através dos quais o processo pode ser implementado com sucesso em uma organização. Convém que a organização use o método que melhor se adeque a suas circunstâncias, para cada aplicação específica do processo.

Em um SGSI, a definição do contexto, o processo de avaliação de riscos, o desenvolvimento do plano de tratamento do risco e a aceitação do risco fazem parte da fase "planejar". Na fase "executar" do SGSI, as ações e controles necessários para reduzir os riscos para um nível aceitável são implementados de acordo com o plano de tratamento do risco. Na fase “verificar” do SGSI, os gestores determinarão a necessidade de revisão da avaliação e tratamento do risco à luz dos incidentes e mudanças nas circunstâncias. Na fase “agir”, as ações necessárias são executadas, incluindo a reaplicação do processo de gestão de riscos de segurança da informação.

A Tabela 1 resume as atividades relevantes de gestão de riscos de segurança da informação para as quatro fases do processo do SGSI:

Tabela 1 – Alinhamento do processo do SGSI e do processo de gestão de riscos de segurança da informação

Processo do SGSI	Processo de gestão de riscos de segurança da informação
Planejar	Definição do contexto Processo de avaliação de riscos Definição do plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

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 o contexto externo e interno para gestão de riscos de segurança da informação seja estabelecido, 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

— 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.

NOTA A ABNT NBR ISO/IEC 27001:2006 não usa o termo "contexto". No entanto, a Seção 7 refere-se aos requisitos "definir o escopo e limites do SGSI" [4.2.1.a)], "definir uma política para o SGSI" [4.2.1.b)] e "definir a abordagem de análise/avaliação de riscos" [4.2.1.c)], especificados na ABNT NBR ISO/IEC 27001:2006.

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 leve em conta critérios básicos, tais 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 de riscos

— Definir e implementar políticas e procedimentos, incluindo implementação dos controles selecionados

— Monitorar controles

— Monitorar o processo de gestão de riscos de segurança da informação

NOTA Ver também a ABNT NBR ISO/IEC 27001:2006 (Seção 5.2.1) com relação à provisão de recursos para a implementação e operação de um SGSI.

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 os seguintes itens:

— O valor estratégico do processo que trata as informações de negócio

— A criticidade dos ativos de informação envolvidos

— Requisitos legais e regulatórios, bem como as obrigações contratuais

— Importância do ponto de vista operacional e dos negócios, da disponibilidade, da confidencialidade e da integridade

— Expectativas e percepções das partes interessadas e consequências negativas para o valor de mercado (em especial, no que se refere aos fatores intangíveis desse valor), a imagem 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

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 com a 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 o não cumprimento de prazos

— Dano à reputação

— Violações de requisitos legais, regulatórios ou contratuais

NOTA Veja também a ABNT NBR ISO/IEC 27001:2006 [Seção 4.2.1 d) 4] com relação à identificação dos critérios de impacto, considerando aperda da confidencialidade, da integridade e/ou da disponibilidade.

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, por exemplo: riscos que podem resultar em não conformidade com regulamentações ou leis podem não ser aceitos, enquanto riscos de alto impacto poderão ser aceitos se isto for especificado como um requisito contratual

— Critérios para a aceitação do risco podem incluir requisitos para um tratamento adicional futuro, por exemplo: um risco poderá 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

— Aspectos legais e regulatórios

— Operações

— Tecnologia

— Finanças

— Fatores sociais e humanitários

NOTA Os critérios para a aceitação do risco correspondem aos “critérios para aceitação do risco e identificação do nível aceitável dos mesmos” especificados na ABNT NBR ISO/IEC 27001:2006 Seção 4.2.1.c) 2).

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 [ver também a ABNT NBR ISO/IEC 27001:2006 Seção 4.2.1.a)] 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:

— Os objetivos estratégicos, políticas e estratégias da organização

— Processos de negócio

— As funções e estrutura da organização

— Requisitos legais, regulatórios e contratuais aplicáveis à organização

— A 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.

NOTA O escopo e os limites da gestão de riscos de segurança da informação estão relacionados ao escopo e aos limites do SGSI, conforme requerido na ABNT NBR ISO/IEC 27001:2006 4.2.1.a).

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.

NOTA A ABNT NBR ISO/IEC 27001:2006 requer a identificação e a provisão dos recursos necessários para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI [5.2.1.a)]. A organização das operações de gestão de riscos pode ser considerada como um dos recursos necessários, segundo a ABNT NBR ISO/IEC 27001:2006.

8 Processo de avaliação de riscos de segurança da informação

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

NOTA A atividade do processo de avaliação de riscos é referida como processo de análise/avaliação de riscos na ABNT NBR ISO/IEC 27001:2006.

Entrada: Critérios básicos, o escopo e os limites, e a 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 advindas da ocorrência de um evento indesejado e da probabilidade da ocorrência do mesmo. 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 (Seção 8.2)

— Análise de riscos (Seção 8.3)

— Avaliação de riscos (Seção 8.4)

O processo de avaliação de riscos determina o valor dos ativos de informação, identifica as ameaças e vulnerabilidades aplicáveis existentes (ou que poderiam existir), identifica os controles existentes e seus efeitos no risco identificado, determina as consequências possíveis e, finalmente, prioriza os riscos derivados e ordena-os 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 precisarão 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 eventos que possam causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer. As etapas descritas nas próximas subseções de 8.2 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 seções 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 (refere-se à ABNT NBR ISO/IEC 27001:2006, Seção 4.2.1.d) 1)).

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 influenciará 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, a fim de oficializar sua responsabilidade e garantir a possibilidade da respectiva prestação de contas. O responsável pelo ativo pode não ter direitos de propriedade sobre o mesmo, 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 mesmo 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 (refere-se à ABNT NBR ISO/IEC 27001:2006, Seção 4.2.1 d) 2)).

Diretrizes para implementação:

Uma ameaça tem o potencial de comprometer ativos (tais 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. Isso significa que, nenhuma ameaça é ignorada, incluindo as não previstas, mas que o volume de trabalho exigido 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 análise da probabilidade de ocorrência (ver 8.2.2.2) podem ser obtidos dos responsáveis pelos ativos ou dos usuários, do pessoal, dos administradores das instalações e dos especialistas em segurança da informação, de peritos em segurança física, do departamento jurídico e de outras organizações, incluindo organismos legais, autoridades climáticas, companhias de seguros e autoridades governamentais nacionais. Aspectos culturais e relacionados ao ambiente precisam ser considerados quando se examina as ameaças.

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 nacionais, 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 estão 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. Sendo assim, controles complementares são necessários para tratar efetivamente o risco identificado. Em um SGSI, de acordo com a ABNT NBR ISO/IEC 27001:2006, isso é auxiliado pela medição da eficácia dos controles. Uma maneira para estimar o efeito do controle é ver o quanto ele reduz, por um lado, a probabilidade da ameaça e a facilidade com que uma vulnerabilidade pode ser explorada ou, por outro lado, o impacto do incidente. A análise crítica pela direção e relatórios de auditoria também fornecem informações sobre a eficácia dos controles existentes.

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 o mesmo 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 de forma crítica os documentos contendo informações sobre os controles (por exemplo: os planos de implementação de tratamento do risco). Se os processos de gestão da 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 gerente 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;

— Revisar, 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 status 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 se exploradas por ameaças para comprometer os ativos ou a organização sejam identificadas (refere-se à ABNT NBR ISO/IEC 27001:2006, Seção 4.2.1 d) 3)).

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. Note-se 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 as consequências que a perda de confidencialidade, de integridade e de disponibilidade podem ter sobre os ativos sejam identificadas (ver a ABNT NBR ISO/IEC 27001:2006 4.2.1 d)4)).

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 (ver ABNT NBR ISO/IEC 27002, Seção 13). O impacto dos cenários de incidentes é determinado considerando-se 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.

NOTA A ABNT NBR ISO/IEC 27001:2006 descreve a ocorrência de cenários de incidentes como “falhas de segurança”.

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

— Imagem, reputação e valor de mercado

Detalhes sobre a avaliação de vulnerabilidades técnicas podem ser encontrados em B.3 - Avaliação do Impacto.

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 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, poderá 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 desenvolvida como parte da definição do contexto.

Detalhes adicionais a respeito das 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 à 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 exigirão uma análise mais detalhada

— Quando esse tipo de análise é suficiente para a tomada de decisões

— Quando os dados numéricos ou recursos são insuficientes 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 de tais dados sobre novos riscos ou sobre fragilidades da segurança da informação. Uma desvantagem da abordagem quantitativa ocorre quando dados factuais e auditáveis não estão disponíveis. Nesse caso, a exatidão do processo de avaliação de riscos e os valores associados tornam-se ilusórios.

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 irá variar de acordo com o tipo de risco e do propósito para o qual os resultados do processo de avaliação de riscos serão 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 levando-se em conta as consequências de uma violação da segurança da informação, como por exemplo: a perda da confidencialidade, da integridade ou da disponibilidade dos ativos (refere-se à ABNT NBR ISO/IEC 27001:2006, Seção 4.2.1 e)1)).

Diretrizes para implementação:

Depois de identificar todos os ativos relevantes, convém que os valores atribuídos a esses ativos sejam levados em consideração durante a avaliação das 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 dos mesmos 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, tais 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 causarão diferentes impactos sobre os ativos, tais 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 através 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 com respeito 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 identificados como relevantes, 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 (refere-se à ABNT NBR ISO/IEC 27001:2006, Seção 4.2.1 e) 2)).

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 levar em conta 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: fatores geográficos (como por exemplo: proximidade a fábricas e refinarias de produtos químicos e petróleo), a possibilidade de eventos climáticos extremos e 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 pudesse 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 estimado para todos os cenários de incidentes considerados relevantes (refere-se à ABNT NBR ISO/IEC 27001:2006, Seção 4.2.1 e) 4)).

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 estimadas. 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 (refere-se à ABNT NBR ISO/IEC 27001:2006, Seção 4.2.1 e) 4)).

Diretrizes para implementação:

A natureza das decisões relativas à avaliação de riscos e os critérios de avaliação de riscos que irão ser usados para tomar essas decisões teriam sido decididos durante a definição do contexto. Convém que essas decisões e o contexto sejam revisados 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 levem em conta 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 precisa ser tratada adequadamente.

Convém que os seguintes itens sejam considerados:

— *Propriedades da segurança da informação:* se um critério não for relevante para a organização (por exemplo: a perda da confidencialidade), logo, todos os riscos que provocam esse tipo de impacto podem ser considerados irrelevantes

— *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 através da análise de riscos para a tomada de decisões sobre ações futuras. Convém que as seguintes questões sejam decididas:

— Convém que uma atividade seja empreendida

— As prioridades para o tratamento do risco, levando-se em conta os níveis estimados de risco

Durante a etapa de avaliação de riscos, além dos riscos estimados, convém que requisitos contratuais, legais e regulatórios também sejam considerados.

Saída: Uma lista de riscos priorizada, 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 priorizada, 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).

NOTA A ABNT NBR ISO/IEC 27001:2006 4.2.1.f) 2) usa o termo “aceitação do risco” em vez de “retenção do risco”.

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: 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 são 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 beneficiar-se substancialmente de uma combinação de opções, tais 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 as formas específicas de tratamento do risco convém ser 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 os mesmos 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 sobres 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

A definição do contexto (ver 7.2 - Critérios de avaliação de riscos) fornece informações sobre requisitos legais e regulatórios com os quais a organização precisa estar em conformidade. Nesse caso, o risco para 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 os 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. Mais informações podem ser encontradas na ABNT NBR ISO/IEC 27002, Seção 0.3.

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 através 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 os requisitos identificados através do processo de avaliação de riscos e do tratamento dos mesmos. Convém que essa escolha leve em conta os critérios para a aceitação do risco assim como requisitos legais, regulatórios e contratuais. 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, implementação, 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, tais como requisitos de desempenho, capacidade de gerenciamento (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 o desempenho sobremaneira. Convém que os gestores tentem encontrar uma solução que satisfaça os 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
- Restrições legais
- Facilidade de uso
- Restrições de recursos humanos
- Restrições ligadas à integração dos controles novos aos já existentes.

Mais informações sobre as restrições que dizem respeito 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.

NOTA O tópico ABNT NBR ISO/IEC 27001:2006 4.2.1 f 2) "aceitação do risco, consciente e objetiva, desde que claramente satisfazendo as políticas da organização e os critérios para aceitação do risco" descreve a mesma atividade.

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 através da eliminação de uma atividade planejada ou existente (ou de um conjunto de atividades), seja através de 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 existe ou está 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 através da subcontratação de um parceiro cujo papel seria 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 ou prejuízo.

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 irão atribuir 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 do mesmo.

Ação: Convém que a decisão de aceitar os riscos seja feita e formalmente registrada, juntamente com a responsabilidade pela decisão (isso se refere ao parágrafo 4.2.1 h) da ABNT NBR ISO/IEC 27001:2006).

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 Seção 7.2 Critérios para a aceitação do risco). É importante que gestores responsáveis façam uma análise crítica e aprovem, se for o caso, 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 os 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. Tais 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 ter que 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 para aceitação do risco.

11 Comunicação e consulta do risco de segurança da informação

Entrada: Todas as informações sobre os riscos obtidas através 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 os riscos devem ser gerenciados, fazendo uso para tal da troca e/ou partilha 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 que devem ser tomadas. A comunicação assegurará que os responsáveis pela implementação da gestão de riscos, e aqueles com interesses reais de direito, tenham um bom entendimento do por que 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. Assim, é particularmente importante 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 as 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 através 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. Serviços de terceiros que forneçam informações sobre novas ameaças ou vulnerabilidades podem prestar um auxílio valioso.

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 pequenos. Convém que a análise crítica dos riscos pequenos 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 utilizando-se 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 não só as atividades de monitoramento de riscos sejam repetidas regularmente, mas também as opções selecionadas para o tratamento do risco sejam periodicamente revistas.

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 critica e regularmente todos os riscos e também quando grandes mudanças ocorrerem (de acordo com a ABNT NBR ISO/IEC 27001:2006, Seção 4.2.3)).

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 através 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 que o processo de gestão de riscos de segurança da informação e as atividades relacionadas permaneçam apropriadas nas circunstâncias presentes. Convém também assegurar que as atividades 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 certeza que nenhum risco ou elemento do risco será ignorado ou subestimado, que as ações necessárias estão sendo executadas e que 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 e 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 análise crítica lide com (mas não seja limitada ao(s)):

— Contexto legal e ambiental

— Contexto da concorrência

— Abordagem do processo de avaliação de riscos

— Valor e as categorias dos ativos

— Critérios de impacto

— Critérios para a avaliação de riscos

— Critérios para a aceitação do risco

— Custo total de propriedade

— Recursos necessários

Convém que a organização assegure que os recursos necessários para o processo de avaliação de riscos e o tratamento dos mesmos estejam sempre disponíveis para rever 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)

— 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 A análise da organização

A análise da organização Este tipo de análise 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 esses elementos sejam identificados ao lado daqueles 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 do gestor da segurança da informação se reportar à alta direção ao invés de fazê-lo 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 e outros), a qualidade dos produtos fornecidos ou dos serviços prestados.

Tomemos o exemplo de 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. Os seus valores poderiam ser 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 a 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.).

Notas:

— Uma área, em uma organização com estrutura departamental, pode estruturar-se baseando-se 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 gerenciamento);

  — o nível operacional (produção e atividades de apoio).

Organograma A estrutura da organização é esquematizada em seu organograma. Convém que essa representação deixe claro quem se reporta a quem, destacando também a linha de comando que legitimiza a delegação de autoridade. Convém que inclua também 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 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 dá um certo controle sobre as restrições ou talvez sejam externas à organização, o que as tornariam, 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 compromete-se a seguir um determinado caminho, possivelmente por um longo período. Ela define aquilo na qual deseja se tornar e também os meios necessários para que tal 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 dizem respeito à administração governamental, às instituições públicas ou, 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 implicar restrições, tais como com 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 transtornada por eventos específicos, tais 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 são aquelas derivadas diretamente da missão da organização (seja nos seus aspectos gerais, seja nos específicos).

Por exemplo, convém que uma organização que opera 24 horas por dia seja capaz de assegurar que seus recursos estarão 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 resulta, por exemplo, da reestruturação ou da definição de novas políticas nacionais ou internacionais que imponham algumas datas limites.

Por exemplo, a criação de uma área de segurança.

Restrições relacionadas a métodos

Métodos apropriados para o *know-how* da organização precisarão ser impostos com relação a alguns tópicos, tais como o planejamento, a especificação e o desenvolvimento de projetos, entre outros.

Por exemplo, uma restrição desse tipo bastante comum é a necessidade das obrigações legais da organização serem incorporadas à política de segurança.

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 Referências legais e regulamentares aplicáveis à organização

Convém que os requisitos regulatórios aplicáveis à organização sejam identificados. Eles consistem das leis, decretos, regulamentações específicas que dizem respeito à área de atividade da organização ou regulamentos internos e externos. Englobam também contratos, acordos e, mais genericamente, qualquer obrigação de natureza legal ou regulatória.

A.4 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 mais acima. Os parágrafos a seguir apresentam uma lista de tipos de restrições, sem esgotar todas as possibilidades.

Restrições derivadas de processos pré-existentes

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

Restrições técnicas

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

— Arquivos (requisitos referentes à organização, gestão de mídia, gerenciamento 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, nível de avaliação, 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.)

— Gerenciamento administrativo (requisitos referentes a responsabilidades etc.)

— Gerenciamento do desenvolvimento (requisitos referentes a ferramentas de desenvolvimento, engenharia de software assistida por computador, cronograma de aceite, organização a ser estabelecida etc.)

— Gerenciamento 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

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

- Ativos primários:
  - Processos e atividades do negócio
  - Informação
- Ativos de suporte e infraestrutura (sobre os quais os elementos primários do escopo se apoiam), de todos os tipos:
  - Hardware
  - Software
  - Rede
  - Recursos humanos
  - Instalações físicas
  - A estrutura da organização

B.1.1 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, tais como os processos da organização, podem também ser considerados, os quais serão úteis para a elaboração da política de segurança da informação ou do plano de continuidade de negócios. Dependendo de seus propósitos, alguns estudos não irão demandar 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

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 demanda um longo tempo ou incorre em um alto custo de aquisição

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

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

B.1.2 Lista e descrição de ativos de suporte

Convém que o escopo consista de ativos que podem ser identificados e descritos. Esses 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.

Exemplos: *laptops*, agendas eletrônicas (Personal Digital Assistants - PDAs).

Equipamento fixo

Computadores utilizados nas instalações da organização.

Exemplos: servidores, microcomputadores utilizados como estações de trabalho.

Periféricos de processamento

Equipamento conectado a um computador através de uma porta de comunicação (serial, paralela etc.) para a entrada, o transporte ou a transmissão de dados.

Exemplos: 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.

Exemplos: 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.

Exemplos: 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 gerenciamento de tarefas ou processos e os serviços de gerenciamento 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 de prateleira

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.

Exemplos: 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.

Exemplos: 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.

Exemplos: 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).

Exemplos: 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 não compreende os dispositivos que 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*").

Exemplos: pontes ("*bridges*"), roteadores, "*hubs*", comutadores ("*switches*"), centrais telefônicas automáticas.

Interface de Comunicação

As interfaces de comunicação conectadas às unidades de processamento são, 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.

Exemplos: Serviço Geral de Pacotes por Rádio ("*General Packet Radio Service*" ou GPRS), adaptador "*Ethernet*".

Recursos humanos

O tipo 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.

Exemplos: 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.

Exemplos: 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.

Exemplos: 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 com os dados de produção.

Exemplos: 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 as medidas de segurança de uma organização não podem ser aplicadas.

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

Edificações

Esse lugar é limitado pelo perímetro externo da organização, isto é por aquilo que fica em contato direto com o exterior.

Isso pode ser uma linha de proteção física formada por barreiras ou por mecanismos de vigilância ao redor dos prédios.

Exemplos: 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.

Exemplos: 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.

Exemplos: linha telefônica, PABX, redes internas de telefonia.

Serviços de Infraestrutura

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

Exemplos: 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.

Exemplos: 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. Isso impõe restrições à organização em questão com relação a regulamentos, decisões e ações.

Exemplos: corpo administrativo, sede da organização.

A estrutura da organização

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

Exemplos: gestão de recursos humanos, gestão te 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.

Exemplos: 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.

Exemplos: empresa de gerenciamento de instalações, empresa prestadora de serviços terceirizados, empresas de consultoria.

B.2 Valoração dos Ativos

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" etc. A decisão de se usar uma escala quantitativa ao invés 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.

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. Tal 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 mesmo 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.

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 que se seguem. 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:

— Violação da legislação e/ou das regulamentações

— 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

— O perigo ocasionado à segurança ambiental

Um outro método para avaliar as consequências poderia levar em conta o seguinte:

— Interrupção dos serviços

  - incapacidade de prestar os serviços
- Perda da confiança do cliente
  - perda da credibilidade no sistema interno de informação
  - dano à reputação
- Interrupção de operação interna
  - descontinuidade dentro da própria organização
  - custo interno adicional
- Interrupção da operação de terceiros:
  - descontinuidade das transações entre a organização e terceiros
  - vários tipos de prejuízos ou danos
- Infração de leis / regulamentações:
  - incapacidade de cumprir obrigações legais
- Violação de cláusulas contratuais
  - incapacidade de cumprir obrigações contratuais
- 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 acima não sejam aplicáveis, e que outros talvez precisem ser adicionados à lista.

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 a respeito de qual seria 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, tais 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, tais 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 a respeito do que é considerado de 'pequena', 'média' ou 'grande' consequência. Uma consequência desastrosa para uma pequena organização pode ser pequena ou mesmo insignificante para uma grande organização.

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 importante do que isso, a integridade da informação dependerá do hardware e software utilizados para seu armazenamento e processamento. Adicionalmente, o hardware dependerá do suprimento de energia e, possivelmente, do ar condicionado. Assim, informações sobre dependências serão de grande ajuda na identificação de ameaças e, em particular, de vulnerabilidades. Além disso, ajudarão a assegurar que o real valor dos ativos (considerando as relações de dependência) ser-lhes-á atribuído, 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

  — os valores dos outros ativos

Uma organização pode possuir alguns ativos que são disponibilizados mais de uma vez, tais 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 todos. Por outro lado, eles podem ser usados para minimizar problemas ligados à falta de disponibilidade.

Saída

O resultado final dessa etapa é a lista de ativos e respectivos valores relativos à divulgação indevida de informações (preservação da confidencialidade), a modificações não autorizadas (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.

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.

d) Consequências resultantes de violações da segurança da informação

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 através da violação da segurança

d) Violação de obrigações estatutárias ou regulatórias

e) Violação dos códigos éticos de conduta

Dessa forma, a primeira avaliação (sem controles de qualquer tipo) resultará 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 contém exemplos de ameaças típicas. A lista na Tabela 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
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

Tipo	Ameaças	Origem
	Alteração do hardware	I
	Alteração do software	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 software	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 software	I
	Uso de cópias de software 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 C.2 enumera essas fontes:

Origem das Ameaças	Motivação	Possíveis Consequências
Hacker, cracker	Desafio Ego Rebeldia Status Dinheiro	• Hacking • 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	• Crime digital (p. ex.: perseguição no mundo digital) • Ato fraudulento (p. ex.: reutilização indevida de credenciais e dados transmitidos, fazer-se passar por uma outra pessoa, interceptação) • Suborno por Informação • *Spoofing* (fazer-se passar por outro) • Invasão de sistemas
Terrorista	Chantagem Destruição	• Bomba/Terrorismo • Guerra de Informação

Origem das Ameaças	Motivação	Possíveis Consequências
	Exploração Vingança Ganho Político Cobertura da Mídia	• Ataque a sistemas (p. ex.: ataque distribuído de negação de serviço). • Invasão de sistema • Alteração do sistema

Fonte de Ameaças	Motivação	Ações que representam Ameaças:
Espionagem industrial (serviços de inteligência, empresas, governos estrangeiros, outros grupos de interesse ligados ao governo)	Vantagem competitiva Espionagem econômica	• 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)
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 (p. ex.: erro na entrada de dados, erro de programação)	• 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 (p. ex.: 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 fornece exemplos de vulnerabilidades em diversas áreas da segurança, incluindo exemplos de ameaças que poderiam explorar tais 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
Hardware	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 de cópias não controlada	Furto de mídia ou documentos
Software	Procedimentos de teste de software insuficientes ou inexistentes	Abuso de direitos
	Falhas conhecidas no software	Abuso de direitos
	Não execução do "logout" 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	Abuso de direitos

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
	dados	
	Inexistência de uma trilha de auditoria	Abuso de direitos

	Atribuição errônea de direitos de acesso	Abuso de direitos
	Software 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
	Software novo ou imaturo	Defeito de software
	Especificações confusas ou incompletas para os desenvolvedores	Defeito de software
	Inexistência de um controle eficaz de mudança	Defeito de software
	Download e uso não controlado de software	Alteração do software
	Inexistência de cópias de segurança (“back-up”)	Alteração do software
	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

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

Tabela D.1 – Exemplos de vulnerabilidades (continuação)

	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 software e hardware	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	Uso não autorizado de equipamento

	mensagens	
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
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

Organização	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 ("l*ogs*") 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 (e-mail)	Erro durante o uso
	Inexistência de procedimentos para a instalação de software em sistemas operacionais	Erro durante o uso
	Ausência de registros nos arquivos de auditoria ("l*ogs*") de administradores e operadores	Erro durante o uso
	Inexistência de procedimentos para a manipulação de informações classificadas	Erro durante o uso
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	Furto de equipamentos

	segurança da informação	
	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 ("*clear desk and clear screen*") 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 software falsificadas ou ilegais

D.2 Métodos para a avaliação de vulnerabilidades técnicas

Métodos pró-ativos, tal 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

— 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 exigida 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 as 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 a realização do processo de avaliação de riscos, para que se possa definir os termos do contrato da terceirização.

Entre as características de uma iteração, com um enfoque de alto nível, do processo de avaliação de riscos temos que:

— 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 pré-definidos, 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, tais 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 serão tratados primeiro.

Como as análises de risco iniciais são feitas com um enfoque de alto nível (potencialmente, portanto, sendo menos exatas), há o perigo de que alguns processos de negócio ou sistemas possam acabar, erroneamente, não sendo identificados entre aqueles que requerem uma 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 através 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 (veja 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 através 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

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 desegurança 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 está sendo considerada

— A facilidade de se 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.

E.2.1 Exemplo 1 Matriz com valores pré-definidos

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 (veja abaixo). À ativos do tipo software, existentes ou planejados, valores são atribuídos da mesma forma que à ativos físicos, com os custos de aquisição ou redesenvolvimento 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 deve ser valorado da mesma forma que as informações.

Os valores atribuídos às informações são obtidos entrevistando-se uma parte seleta da direção do negócio (os "responsáveis pelos dados"), aqueles que podem falar autoritativamente sobre os dados. Assim determinam-se 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, tais 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)

— 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 a)

	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**. Suponha 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 implicará novas medidas de risco. A vantagem dessa abordagem está na ordenação dos riscos a serem tratados.

Uma matriz similar como apresentada na Tabela E.1 b) mostra a relação entre 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 escada 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: 0-2
- Médio Risco: 3-5
- Alto Risco: 6-8

Tabela E.1 b)

	Probabilidade do cenário de incidente	Muito baixa (Muito improvável)	Baixa (Improvável)	Média (Possível)	Alta (Provável)	Muito Alta (Frequente)
Impacto ao 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.2.2 Exemplo 2 Ordenação de Ameaças em função do Risco

Uma tabela ou matriz como apresentada na tabela E.2 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 pré-definida, 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 pré-definida, por exemplo: de 1 a 5, para cada ameaça (coluna 'c' na tabela). Na terceira etapa, calcula-se a medida de risco multiplicando (b x c). Por último, as ameaças podem ser ordenadas em sequência conforme suas respectivas medidas de risco. Note que nesse exemplo, 1 representa a menor consequência e a menor probabilidade de ocorrência.

Tabela E.2

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

E.2.3 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 sistemas sejam priorizados. Isso é feito estimando-se dois valores para cada par de ativo e risco, os quais, combinados, irão determinar 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 refere-se 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-se a probabilidade de ocorrência da ameaça e a facilidade com que a vulnerabilidade pode ser explorada. Veja, na Tabela 3, a representação da probabilidade de um cenário de incidente.

Tabela E.3

Probabilidade da Ameaça	Baixa			Média			Alta		
Nível da vulnerabilidade	B	M	A	B	M	A	B	M	A
Probabilidade do cenário de incidente	0	1	2	1	2	3	2	3	4

Em seguida, na Tabela E.4, 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.4

Valor do ativo	0	1	2	3	4
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 convém determinar qual sistema seja protegido com maior prioridade.

Nos exemplos a seguir todos os valores foram escolhidos aleatoriamente.

Suponha que o Sistema S tenha três ativos A1, A2 e A3. Suponha também que existam duas ameaças, T1 e T2, aplicáveis ao sistema S. Estabeleçamos 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.3).

A pontuação referente ao par ativo/ameaça A1/T1 pode ser obtida na Tabela E.4, 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, TA1, que é a pontuação total do ativo A1, pode ser calculada, e o resultado é 10. A pontuação total do ativo é calculada para cada ativo levando-se em conta todas as ameaças aplicáveis. A pontuação total do sistema é calculada através da 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 acima 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-se exposto a um determinado risco.

Restrições financeiras:

Convém que a implementação ou a manutenção dos controles sejam menos dispendiosas do que o valor dos riscos que eles foram projetados para combater, exceto nos casos em que a conformidade é obrigatória (por exemplo, no caso de legislações específicas). Convém que todos os esforços sejam feitos para que os orçamentos alocados não sejam excedidos, e também para que vantagens financeiras, através do uso de controles, sejam obtidas. Contudo, em alguns casos, talvez não seja possível implementar a segurança desejada e alcançar o nível de risco formalmente aceito, devido a restrições orçamentárias. Essa situação exigirá, 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 24x7 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. Aspectos culturais não podem ser ignorados, 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, tais 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.

Restrições legais:

Fatores legais tais como provisões relativas à proteção de dados pessoais ou do código penal referentes ao processamento de informações, podem afetar a seleção de controles. A conformidade à legislação e a normas pode exigir certos tipos de controles, como por exemplo, a proteção de dados e a auditoria financeira. Por outro lado, ela pode também impedir o uso de alguns controles, por exemplo: a criptografia. Outras leis e regulamentações, tais como a legislação do trabalho, as normas do corpo de bombeiros, da área da saúde e da segurança, e regulamentações do setor econômico, também podem afetar a escolha de controles.

Facilidade de uso:

Uma interface de usuário mal projetada resultará 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 tais 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. Exigir 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: 2009, *Gestão de riscos – Vocabulário – Recomendações para uso em normas*

[2] ISO/IEC 16085: 2006, *Systems and Software Engineering — Life Cycle Processes — Risk Management*

[3] ABNT NBR ISO/IEC 27002:2005*, Tecnologia da informação — Técnicas de segurança — Código de pratica para a gestão de segurança da informação*

[4] ABNT NBR ISO 31000:2009, *Gestão de riscos — Princípios e diretrizes*

[5] NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handboo*k

[6] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology*