INTRODUÇÃO À GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

VERSÃO 1.2

GSIC302

Jorge Henrique Cabral Fernandes

Luiz Inácio Lula da Silva
Presidente da República

Jorge Armando Félix
Ministro do Gabinete de Segurança Institucional

Antonio Sergio Geromel
Secretário Executivo

Raphael Mandarino Junior
Diretor do Departamento de Segurança da Informação e Comunicações

Reinaldo Silva Simião
Coordenador Geral de Gestão da Segurança da Informação e Comunicações

Fernando Haddad
Ministro da Educação

UNIVERSIDADE DE BRASÍLIA

José Geraldo de Sousa Junior
Reitor

João Batista de Sousa
Vice-Reitor

Denise Bomtempo Birche de Carvalho
Decana de Pesquisa e Pós-Graduação

Noraí Romeu Rocco
Instituto de Ciências Exatas

Priscila Barreto
Departamento de Ciência da Computação

CEGSIC

Coordenação
Jorge Henrique Cabral Fernandes

Secretaria Pedagógica
Marcelo Felipe Moreira Persegona
Ana Cristina Santos Moreira
Eduardo Loureiro Jr.

Assessoria Técnica
Ricardo Sampaio
Gabriel Velasco
Odacyr Luiz Timm

Secretaria Administrativa
Adriana Rodrigues Pereira Moura
Gelsilane Cruvinel Menezes

Equipe de Produção Multimídia
Alex Harlen
Estéfano Pietragalla
Lizane Leite
Rodrigo Moraes

Equipe de Tecnologia da Informação
Douglas Ferlini
Osvaldo Corrêa
Maicon Braga Freitas

Revisão de Língua Portuguesa
Davi Miranda

Texto e Ilustrações
Jorge Henrique Cabral Fernandes

Capa e projeto gráfico
Alex Harlen

Diagramação
Estéfano Pietragalla

Desenvolvido em atendimento ao plano de trabalho do Programa de Formação de Especialistas para a Elaboração da Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações – CEGSIC 2009-2011.

UnB

Sumário

CURRÍCULO RESUMIDO DO AUTOR

Jorge Henrique Cabral Fernandes

Jorge Henrique Cabral Fernandes é Doutor e Mestre em Ciência da Computação pela Universidade Federal de Pernambuco (2000 e 1992). É especialista em Engenharia de Sistemas pela Universidade Federal do Rio Grande do Norte (1998). Possui graduação em Ciências Biológicas - Habilitação em Bioquímica pela Universidade Federal do Rio Grande do Norte (1986). Foi Agente Administrativo, Analista de Sistemas e Professor de Engenharia de Software pela Universidade Federal do Rio Grande do Norte. Atualmente é Professor Adjunto do Departamento de Ciência da Computação da Universidade de Brasília e Professor da Pós-Graduação em Ciência da Informação no Departamento de Ciência da Informação da Universidade de Brasília. É Presidente do Conselho de Informática da UnB e Coordenador do Curso de Especialização em Gestão de Segurança da Informação e Comunicações. Tem experiência na área de Engenharia de Software, Programação Orientada a Objetos, Ciência da Informação, Segurança da Informação, Gestão da Segurança da Informação, Sistemas de Inventário de Ciclo de Vida de Produtos e Bancos de Dados.

Resumo

O objetivo deste texto é apresentar uma introdução conceitual à gestão da segurança, com base na gestão de riscos de segurança da informação. O modelo conceitual de segurança, apresentado no Capítulo 2, é desenvolvido pelo próprio autor. O modelo de gestão de riscos de segurança é baseado na abordagem da norma ABNT NBR ISO/IEC 27005:2008 (ABNT, 2008) e apresentado nos capítulos 3 a 10. A base para a apresentação da norma foi a versão draft (ISO/IEC, 2007) da norma produzida pela ISO/IEC. A monografia contém uma compilação de vários elementos descritos na referida norma e na versão brasileira da ISO/IEC (ABNT, 2008), mas não a substitui. Por fim, o texto apresenta algumas orientações para a introdução da gestão de riscos nas organizações, baseadas na Norma AS-NZS 4360 (Standards Australia and Standards New Zealand, 2004), da qual deriva a ISO/IEC 31000 (ISO/IEC, 2009). O texto foi produzido para suporte às atividades do CEGSIC 2009-2011, a partir de aprimoramento de material previamente desenvolvido em versões anteriores do CEGSIC. Comentários, críticas, sugestões e propostas de correções para aprimoramento deste material devem ser encaminhadas ao autor, que antecipa agradecimentos pelo retorno.

1 Introdução

Risco é uma estimativa de incerteza[1] e consequências relacionadas à ocorrência de um evento desejável ou indesejável. Segundo a *Society for Risk Analysis*[2], o risco tem sido usado desde antes da Grécia antiga como fundamento para a tomada de decisões.

Por exemplo, suponha que tenho que decidir entre fumar ou não fumar. Há um risco de que, se eu adotar o hábito de fumar, desenvolva câncer de pulmão antes dos 50 anos. Também há um risco de que, se não fumar, desenvolva câncer de pulmão antes dos cinquenta anos! Qual dos riscos é maior? Diz a ciência[3] que se eu fumar terei um maior risco. Vários fatores podem estar envolvidos da determinação do risco acerca dessa questão específica sobre fumo e câncer, como idade, sexo, hábitos alimentares, profissão, condição familiar etc. Embora o exemplo acima seja aplicável à tomada de decisões individuais, os mesmos princípios podem ser transpostos para a tomada de decisões acerca de segurança nas organizações.

Vários modelos e métodos da gestão de riscos contemporânea foram desenvolvidos na última década, como STONEBURNER, GOGUEN, FERINGA (2002), PELTIER (2001), Standards Australia and Standards New Zealand (2004), ISO/IEC (2007), ISO/IEC (2009), COSO (2004), ALBERTS, DOROFEE (2002), MEULBROEK (2002), ASIS (2007), HHS (2005), BSI (2005), BS (2006) e CNSS (2005). Tais métodos baseiam-se na construção de uma argumentação racional, que emprega fundamentos do método científico para produzir medições quantitativas ou qualitativas acerca do risco organizacional ou relacionado a projetos. Tais medições permitem a tomada de decisões acerca da implementação de controles e outras ações de segurança. Por meio da gestão de riscos os fatores do risco são decompostos, recompostos e recalculados de forma iterativa, produzindo continuamente subsídios a decisões satisfatórias para melhoria da segurança de uma organização. O plano de gerenciamento de riscos é o principal direcionador de um plano de segurança.

Este texto apresenta uma introdução conceitual à gestão de riscos de segurança da informação. O modelo de gestão de riscos de segurança é baseado na abordagem descrita na versão *International Draft* da ISO/IEC 27005 (ISO/IEC, 2007), bem como na sua congênere nacional, a ABNT NBR ISO/IEC 27005:2008 (ABNT, 2008). A monografia contém uma compilação de vários elementos descritos na referida norma, mas não a substitui.

O restante do texto está dividido em mais 11 seções. Na Seção 2 são apresentados fundamentos gerais das organizações e gestão da segurança. Na Seção 3 são apresentados conceitos básicos da gestão de riscos. Nas seções 4 a 10 são apresentados os elementos do processo de gestão de riscos de segurança da informação da ISO/IEC (2007). Na seção 11 são apresentadas recomendações para a introdução da gestão de riscos em organizações, baseadas na norma Neozelandesa-Australiana de Gestão de Riscos (Standards Australia and Standards New Zealand, 2004).

1 De acordo com o site http://www.businessdictionary.com, incerteza é "uma situação na qual o estado corrente de conhecimento é tal que (1) a ordem ou natureza das coisas é desconhecida, (2) as consequências, extensão ou magnitude das circunstâncias, condições ou eventos é imprevisível e (3) probabilidades críveis relacionadas aos resultados possíveis não podem ser atribuídas. Embora um excesso de incerteza seja indesejável, incerteza gerenciável provê liberdade para tomada de criativa de decisões."

2 Kimberly M. Thompson, Paul F. Deisler, Jr., and Richard C. Schwing. Interdisciplinary Vision: The First 25 Years of the Society for Risk Analysis (SRA), 1980–2005. Risk Analysis, Vol. 25, No. 6, 2005.

3 http://www.cancer.gov/cancertopics/smoking

2 Fundamentos Gerais da Gestão e da Segurança

2.1. Organizações

A humanidade vem aperfeiçoando ao longo da sua história um tipo de empreendimento de duração indeterminada denominado organização ou empresa. Uma organização é um sistema autorregulado, cujo ambiente interno é composto por vários agentes que executam processos organizacionais em um espaço social segregado, buscando o alcance de objetivos de negócio ou metas coletivas.

Toda organização – assim como todo sistema – relaciona-se com o ambiente externo. Esse relacionamento é estabelecido por meio de uma interface com clientes, fornecedores, governo etc. São exemplos de interfaces de uma organização com o meio externo as áreas de recepção, *call center*, os vendedores, os compradores, os atendentes e demais agentes que interagem com clientes, fornecedores, governo e cidadão.

2.2 Ordem e Caos

Nenhuma organização consegue viver em isolamento. Vários eventos ocorrem no entorno de qualquer organização, tanto em seu ambiente externo quanto no interno, e não é possível adquirir-se o controle pleno sobre todos esses eventos. Um evento é uma dinâmica indivisível do ponto de vista prático, que ocorre em um lugar no espaço e num instante do tempo. Tais eventos podem ser regulares ou caóticos. Um evento regular ou ordenado é um evento para o qual é possível alguma previsão de ocorrência. Um evento caótico é um evento que tem ocorrência tão irregular e imprevisível que se torna difícil ou impossível prever quando e onde ele acontecerá. Há, portanto, um elevado grau de incerteza acerca de quando e onde um evento caótico ocorrerá. Muitos eventos são regulares, como a nossa respiração, e uma quantidade infinita de eventos é caótica, como a queda de uma estrela cadente. Situada entre a estrita ordem dos eventos completamente regulares e o completo caos dos eventos completamente incertos e imprevisíveis reside uma infinitude de eventos para os quais é possível fazer-se uma estimativa de frequência e consequências, embora seja praticamente impossível afirmar exatamente quando e quais serão as consequências de um evento futuro. A gestão de riscos compartilha características com a futurologia[4], ao buscar antever a ocorrência desses eventos a fim de controlar suas consequências e impactos sobre uma organização.

2.3 Sistema Seguro

A gestão de riscos tem o efeito de tornar um sistema mais seguro. Um sistema seguro é um sistema que possui um grau de garantia de que continuará a funcionar adequadamente conforme suas características estabelecidas, mesmo na presença de eventos negativos decorrentes da interação com agentes maliciosos ou na ocorrência de eventos decorrentes de acidentes ou desastres de origem natural ou ambiental. Para uma organização, segurança significa continuar a cumprir seus objetivos de negócio, mesmo em face do sinistro.

4 http://en.wikipedia.org/wiki/Futurology

2.4 Gestão e Gestores

O controle ou regulação sistematicamente efetuada nas organizações é realizado por um subsistema dentro da própria organização, denominado *sistema de gestão* ou simplesmente gestão.

Um dos efeitos que a gestão produz sobre uma organização é a atuação na redução dos eventos que contribuem para produzir efeitos negativos, bem como a atuação para aumentar eventos que contribuem para produzir efeitos positivos. A forma sistemática como a gestão atua surge por meio do uso de controles.

A gestão mobiliza as pessoas e outros agentes que atuam na organização, especialmente por meio de controles de gestão, com vistas a reduzir efeitos negativos e produzir efeitos positivos que garantam o alcance das metas coletivas dessa organização diante da ocorrência de eventos incertos.

2.5 Controles

Depreende-se da discussão anterior que os controles aumentam a previsibilidade do funcionamento da organização e, dessa forma, são vistos como estabilizadores dos processos e sistemas nas organizações.

De forma geral, controle pode ser referir ao ato ou processo de controlar, como:

a. [Controle] é intervir numa situação, pessoa (ou grupo de pessoas) e fazer com ela(s) realize(m) o que você quer (LOGMAN, 1993);

b. [Controle] é intervir sobre um processo, sistema etc, de modo que ele funcione adequadamente e não cause problemas (LOGMAN, 1993);

c. [Controle] é intervir sobre máquinas, equipamentos ou veículos usando suas mãos, pés, ferramentas etc (LOGMAN, 1993);

d. [Controle] é o poder de direção e comando (PEARSALL; THUMBLE, 1996);

e. [Controle] é ter responsabilidade sobre uma atividade ou grupo de pessoas (LOGMAN, 1993).

Controle também pode ser referir aos objetos que controlam, especialmente quando usado no plural, como:

a. [Controles] são métodos, leis etc que são usados para controlar uma situação (LOGMAN, 1993);

b. [Controles] são chaves e outros dispositivos por meio dos quais uma máquina ou um veículo é controlado (PEARSALL; THUMBLE, 1996);

c. [Controle] é uma pessoa ou grupo que controla algo (PEARSALL; THUMBLE, 1996).

Em auditoria, o termo controle é mais empregado no sentido de exame e verificação, conforme as seguintes definições:

a. [Controle] é examinar ou verificar algo (LOGMAN, 1993);

b. [Controle] "é uma das funções gerenciais, da mesma forma que planejamento, organização, recursos humanos e direção. Compreende a definição de padrões, medição do desempenho real e tomada de ações corretivas" (WIKIPEDIA, 2009);

c. [Controle] "significa conhecer a realidade, compará-la com o que deveria ser, tomar conhecimento rápido das divergências e suas origens e tomar medidas para sua correção" (ELISEU, 1995 apud PAULA, 1999, p. 21);

d. [Controle] "abrange os vários processos nos quais a administração determina seus objetivos, delineia os planos para alcançar esses objetivos, organiza e supervisiona as operações necessárias para a implementação dos planos e desempenhos esperados" (ELISEU, 1995 apud PAULA, 1999, p. 21);

e. [Controle] Controle é um processo que compara a realidade com o planejado e toma medidas para correção dos desvios encontrados;

f. [Controle] é um processo que possui um papel ativo na estabilização de outro processo.

Todo controle é um estabilizador e, dessa forma, possui todas as características gerais de um estabilizador, como redução de caos (e aumento de estabilidade) em face da ocorrência de eventos se aplicam a um controle.

2.6 Controles de Segurança

Controles em funcionamento que tenham por objetivo neutralizar eventos potencialmente negativos que venham a ocorrer numa organização são chamados de controles de segurança.

A adoção de controles de segurança depende de ações de planejamento (quais os riscos da organização? quais controles devem ser implementados?), monitoramento (como os controles estão funcionando?) e controle (os controles estão funcionando a contento? que ações corretivas ou aperfeiçoadoras devem ser tomadas?). Em suma, a adoção de controles, tanto de gestão como de segurança, é parte essencial da autorregulação realizada pela gestão da organização.

O NIST (NIST, 2006; NIST, 2009) oferece a seguinte definição para controle de segurança:

> *Um controle de segurança é uma salvaguarda ou contramedida de natureza gerencial, operacional ou técnica, prescrita para um sistema de informações, de modo a proteger a confidencialidade, integridade e disponibilidade do sistema de sua informação.*

Os controles de segurança podem se dividir entre gerenciais, operacionais ou técnicos, com as seguintes definições (NIST, 2006):

2.6.1 Controle de Segurança Operacional

Conforme NIST (2006), um controle de segurança operacional é um controle de segurança (salvaguarda ou contramedida) para um sistema de informação que é primariamente implementado e executado por pessoas (em oposição a sistemas).

2.6.2 Controle de Segurança Gerencial

Conforme NIST (2006), um controle de segurança gerencial é um controle de segurança (salvaguarda ou contramedida) para um sistema de informação que foca a gestão do risco e a gestão da segurança do sistema de informação.

2.6.3 Controle de Segurança Técnico

Conforme NIST (2006), um controle de segurança técnico é um controle de segurança (salvaguarda ou contramedida) para um sistema de informação que é primariamente executado e implementado pelo sistema de informação, através de mecanismos contidos nos componentes de *hardware*, *software* ou *firmware* presentes no sistema.

2.6.4 Salvaguardas, Contramedidas ou Medidas de Segurança

O termo "salvaguarda" também é empregado como um sinônimo de controle, contramedida ou medida de segurança. Conforme NIST (2006),

> *Salvaguardas são medidas de proteção prescritas para alcançar requisitos de segurança (confidencialidade, integridade e disponibilidade) que foram especificadas para um sistema de informação. Salvaguardas podem incluir características de segurança, restrições gerenciais, segurança de pessoal e segurança de estruturas físicas, áreas e dispositivos. Salvaguardas são sinônimos de controles e contramedidas de segurança.*

Controles de natureza operacional ou técnica, como criptografia, são difíceis de caracterização como processos. O termo "medida de segurança" se aplica melhor aos casos em que controles não são facilmente caracterizados como processos, isto é, quando são objetos ou artefatos quaisquer.

2.6.5 Implementação de Controles

A norma ABNT NBR ISO/IEC 27002:2005 (ABNT, 2005) contém um guia de implementação de 133 controles de segurança tipicamente usados nas organizações. A norma ABNT NBR ISO/IEC 27001:2006 (ABNT, 2006) descreve um processo sistemático de introdução de controles de segurança em organizações. No cerne do processo, proposto pela ABNT (2006), reside a gestão de riscos. A Seção 8 deste texto apresenta um pouco mais de detalhes sobre a norma ISO/IEC 27002 (ABNT, 2005).

2.7 Eventos e Incidentes de Segurança

Eventos negativos para a segurança da informação são mais comumente chamados de incidentes de segurança da informação. Há, no entanto, diferenças entre os conceitos de eventos e incidentes, e a ABNT (2005) oferece definições para eventos e incidentes de segurança.

2.7.1 Evento de Segurança da Informação

Um evento de segurança da informação, segundo a ABNT (2005), é uma ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida que possa ser relevante para a segurança da informação.

2.7.2 Incidente de Segurança da Informação

Um Incidente de Segurança da Informação, segundo a ABNT (2005), é indicado por um simples evento ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Incidentes de segurança da organização:

a. provocam obstrução ou erro na execução de um ou mais processos organizacionais;

b. a obstrução ou erro decorre de dificuldades na ação dos agentes organizacionais humanos ou computacionais, no desempenho de suas atividades;

c. provocam queda no desempenho de uma ou mais funções organizacionais;

d. impactam o alcance de metas organizacionais;

Dado que alguns eventos de segurança são classificados como incidentes, quanto mais eventos ocorrerem, maior a chance de incidentes serem provocados. A gestão de riscos de segurança da informação busca mapear o risco de ocorrência dos incidentes de segurança da informação.

2.8 Risco e Risco de Segurança

Risco é um evento hipotético, cuja ocorrência pode afetar de forma positiva ou negativa uma organização. Ele possui chance de ocorrência futura que não é nula e apresenta impacto ou oportunidade significante.

2.8.1 Risco de Segurança

Um risco de segurança é um evento possível e potencialmente danoso a uma organização, isto é, um evento hipotético, que possui chance de ocorrência futura que não é nula e que apresenta impacto negativo significante.

Sem chance de ocorrência futura, um evento hipotético não se configura como risco. Sem impacto negativo significante, um evento hipotético não se configura como risco. É também importante destacar que, mesmo que um evento futuro negativo tenha 50% de chance de ocorrer e impacto negativo valorado, haverá sempre uma incerteza associada a tal estimativa. Isto é, podemos ter baixa, média ou alta confiança de que o evento tem 50% de chance de ocorrer, bem como podemos ter baixa, média ou alta confiança de que o impacto negativo real será do valor que estimamos.

Dessa forma, um risco poderia, de modo abstrato, ser obtido pela fórmula abaixo:

Risco de Segurança = Chance de ocorrência * Impacto negativo estimado * Incerteza relacionada com as medidas.

2.8.2 Perfil do Risco de Segurança

Ao conjunto de riscos de segurança aos quais está sujeito uma organização dá-se o nome de perfil do risco de segurança.

Perfil do Risco de Segurança = {Risco de segurança 1 + Risco de segurança 2 + ... + Risco de segurança n}

2.8.3 Cenário de Incidentes de Segurança

A descrição fictícia e textualmente enriquecida de um conjunto de incidentes que podem potencialmente ocorrer com uma organização é chamada de "cenário de incidentes". O conjunto de cenários de incidentes é uma forma empregada para facilitar a compreensão do perfil de riscos de uma organização. A partir do cenário de incidentes podem ser construídos vários riscos.

2.8.4 Redução do Risco

A redução gerenciada de um risco é obtida por meio da introdução de controles, produzindo um novo tipo de risco, chamado de "risco residual". De forma abstrata, poderíamos expressar a redução do risco, ou risco residual, por meio de uma fórmula como a seguir:

Risco residual = Risco original / Controles de Segurança

2.8.5 Iteratividade na Gestão do Risco

Cada controle de segurança implementado para reduzir um ou mais riscos incorre em um custo, bem como aumenta a chance de que outros eventos, de natureza positiva, também sejam reduzidos e que, com isto, a organização perca alguma flexibilidade e deixe de inovar. Dessa forma, o gestor de segurança precisa encontrar um ponto de equilíbrio entre o ganho no aumento da segurança em comparação com as perdas decorrentes de investimentos em controles e aquelas relacionadas à perda de flexibilidade organizacional.

É preciso também compreender que cada novo controle introduzido para tratar um risco específico produz um risco residual e pode introduzir surgimento ou desaparecimento de novos riscos. Diante desse cenário mutável e complexo para a segurança, mais especificamente, a gestão da segurança organizacional contém pelo menos três atividades, executadas nesta ordem:

a. levantamento do perfil de riscos de segurança da organização;

b. adoção de controles de segurança compatíveis com o perfil de riscos da organização;

c. reavaliação.

A ordem na qual essas atividades devem ser realizadas é a apresentada acima. É um desperdício de recursos a adoção de controles de segurança sem que haja compreensão do perfil de riscos ao qual a organização está sujeita. As atividades de levantamento do perfil de riscos e de adoção de controles são realizadas no âmbito da Gestão de Riscos de Segurança, que vem a ser o cerne da Gestão da Segurança.

A implementação da segurança em uma organização, fundamentalmente baseada em controles, depende da compreensão da natureza do conjunto de eventos potencialmente negativos a essa organização, os quais podem não possuir relação direta com a natureza do processo em si que está sendo executado.

A falta de energia, por exemplo, é um evento que não possui relação direta com o processo de ensino de uma universidade. O uso de senhas não é uma característica inerente a um sistema de controle de rendimento escolar. No entanto, um conjunto genérico de eventos pode impactar um grande número de processos de uma organização, e é essencial saber quais são eles e do que eles dependem para funcionar.

Como há uma quantidade finita de recursos para implementação de controles de segurança, para o alcance de uma situação de equilíbrio é necessário estabelecer prioridades, identificando quais atividades são essenciais à atuação da organização e até que ponto elas são influenciadas por riscos de segurança. Todas as ações de segurança devem ser prioritariamente guiadas para a preservação da continuidade do desempenho dessas atividades e alcance das metas a elas associadas.

2.9 Paradoxo da Segurança

A segurança é um processo que envolve o emprego de uma quantidade considerável de recursos não diretamente relacionados à satisfação das necessidades de uma organização. Tais recursos são empregados para analisar eventos, processos e sistemas, bem como para conceber, implementar, operar e aprimorar controles.

Por ser uma consumidora de recursos não relacionada à realização das atividades fim de uma organização, a segurança cria um aparente paradoxo.

Por um lado, existe uma quantidade infinita de eventos negativos que podem ocorrer, e a adoção de controles de segurança para neutralizar cada um destes eventos levaria uma organização a comprometer todos os seus recursos, levando-a à morte por esgotamento de recursos.

A segurança excessiva não garante a continuidade da vida.

Por outro lado, a inexistência de quaisquer controles de segurança, onde a organização observa e aproveita apenas os eventos positivos para a realização de negócios, conduz tal organização à exposição a situações que a levarão à morte prematura.

A falta de segurança garante que a vida será descontinuada. A preocupação com segurança aumenta na medida em que uma organização vive mais.

Na prática, maior investimento de recursos em segurança garante a sobrevivência em situações difíceis (eventos danosos), enquanto investimentos de recursos na busca ou aproveitamento de eventos para a satisfação de necessidades básicas estão relacionados ao próprio desfrute da existência ou à realização de objetivos de negócio.

O alcance da segurança efetiva exige uma situação de equilíbrio na aplicação de recursos, em ambas as situações.

O processo de encontro do ponto de equilíbrio entre a segurança e a realização de objetivos de negocio é iterativo, reflexivo e virtualmente infinito.

O processo é iterativo porque são necessários vários ciclos para o alcance de uma situação adequadamente equilibrada. Ora os controles de segurança são excessivos e a organização perde oportunidade para realização de negócios; ora os controles de segurança são insuficientes, e a sobrevivência da organização é ameaçada.

O processo de segurança é reflexivo porque a adoção de controles de segurança diante dos eventos negativos possíveis influencia a futura ocorrência desses e de outros eventos, fazendo com que os próprios ambientes externo e interno se ajustem à medida que os controles são adotados.

Por fim, o alcance do ponto de equilíbrio é um processo virtualmente infinito, com duração para toda a vida. As organizações que atuam em um espaço modificam-se contínua e imprevisivelmente conforme a ação das demais. Quando combinada com a caoticidade da natureza e dos sistemas artificiais, inclusive de natureza tecnológica, essa situação conduz a uma contínua busca e coevolução, sendo parcialmente encerrada quando a organização morre, mas continuada pelos descendentes possivelmente gerados.

O alcance do ponto de equilíbrio entre a aplicação de controles de segurança e a realização de negócios é encontrado apenas por meio de um processo iterativo, reflexivo e virtualmente infinito.

A segurança, embora consistindo na adoção planejada de controles, necessita ponderar a necessidade e suficiência dos controles de segurança, em face do conjunto de eventos potenciais negativos que possam ocorrer no futuro.

2.10 Conclusão

Esta seção compôs um arcabouço conceitual geral sobre segurança, por meio do qual será efetuada uma apresentação do processo de gestão de riscos. Eis uma súmula dos conceitos discutidos na seção:

a. organizações estão sujeitas à ocorrência de eventos incertos que podem desestabilizar suas atividades e processos. Tais eventos são denominados riscos;

b. gestores precisam controlar as atividades e processos organizacionais, isto é, controlar riscos. Para tal, despendem recursos organizacionais na implementação de controles;

c. controles de segurança são aqueles voltados à redução de potenciais eventos de impacto negativo (riscos de segurança), e são usualmente enquadrados em classes de controle operacional, gerencial ou técnico;

d. a redução do risco de segurança é um processo iterativo, que depende do levantamento do perfil de riscos de segurança que afetam uma organização, da implementação de controles de segurança para mitigar esses riscos e da reavaliação do perfil de riscos diante das mudanças inevitáveis provocadas pelos controles.

O próximo capítulo introduz a abordagem da ABNT NBR ISO/IEC 27005:2008 à gestão de riscos.

3 Conceitos de Gestão de Riscos

A gestão de riscos de segurança é um processo sistemático da gestão organizacional que determina a aplicação equilibrada de controles de segurança nessa organização, diante do seu perfil de riscos de segurança.

A ISO/IEC 27005, norma base usada para apresentação de um modelo de gestão de riscos, tem as finalidades de ser (ISO/IEC, 2007):

a. uma descrição de um processo genérico para a gestão do risco de segurança da informação;

b. um guia para gestão do risco que pode ser usado em empresas, projetos, ciclos de melhoria contínua etc;

c. um guia para desenvolvimento de métodos e metodologias que atendam às necessidades de gestão de riscos apontadas na norma ABNT NBR ISO/IEC 27001:2006;

d. uma norma de consenso entre diversas outras normas e metodologias de gestão de riscos em nível mundial.

Segundo (FERNANDEZ; SCHAUER, 2007), a ISO/IEC (2007) deriva de várias outras normas como:

a. A norma inglesa BS-7799-3 (BS, 2006), que é funcionalmente similar à 27005;

b. AS/NZS 4360 (Standards Australia and Standards New Zealand, 2004), que possui um modelo de processo de grande similaridade com o da 27005;

c. ISO/IEC 27001 - Sistemas de gestão de segurança da informação – requisitos (ABNT, 2006), que pertence à mesma família da 27005 e articula-se explicitamente com essa norma.

d. ISO 31000:2009 - *Risk management -- Principles and guidelines* (ISO/IEC, 2009) apresenta um arcabouço conceitual similar ao da norma AS/NZS 4360.

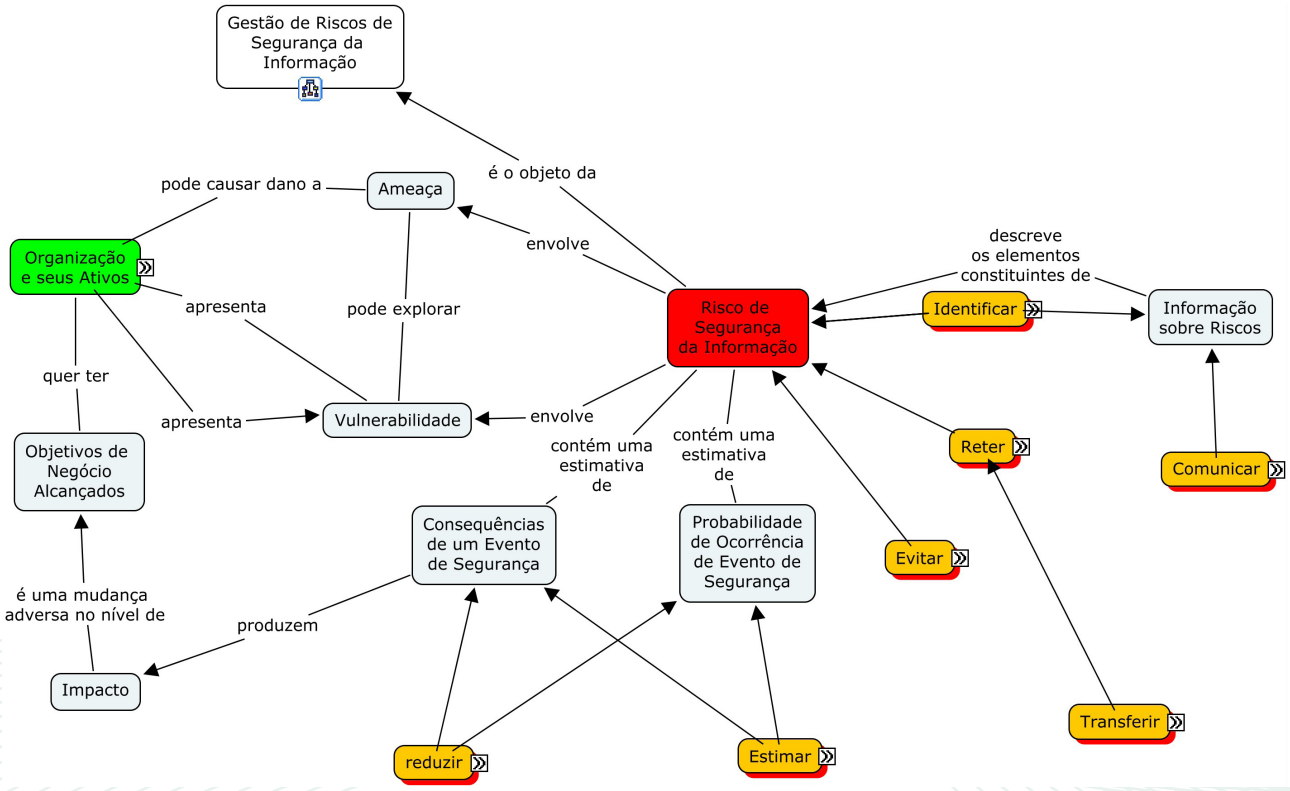

Figura 1 – Mapa Conceitual sobre Gestão de Riscos de Segurança.

O mapa da Figura 2 apresenta o arcabouço conceitual geral sobre o qual se apoia a 27005, e alguns de seus elementos são definidos na lista a seguir.

a. [Organização] é "uma entidade que possui um conjunto de ativos (de informação)" (ISO/IEC, 2007);

b. [Ativo] é "Qualquer coisa que tenha valor para a organização" (ISO/IEC, 2007). Um ativo é uma parte da organização, podendo ser um elemento tangível como um de seus subsistemas, ou intangível como uma marca comercial ou segredo industrial;

c. [Evento de Segurança da Informação] é "uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação" (ISO/IEC, 2007);

d. [Consequência de um Evento de Segurança] "É uma variação negativa no nível de um objetivo de segurança devido a um evento" (ISO/IEC, 2007). São os principais objetivos de segurança a confidencialidade, integridade, disponibilidade e autenticidade;

e. [Impacto] é uma "mudança adversa no nível de objetivos de negócios alcançados." (ISO/IEC, 2007);

f. [Ameaça] é a "causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização" (ISO/IEC, 2004).

g. [Vulnerabilidade] é uma "fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças" (ISO/IEC, 2004);

h. [Risco de Segurança da Informação] é o "Potencial que uma ameaça explore vulnerabilidades de um ativo ou conjunto de ativos e desta forma prejudique uma organização. Um risco é mensurado em termos de probabilidade de materialização do risco e seus impactos" (ISO/IEC, 2007);

i. [Evitar o Risco] é a "Decisão de não se envolver ou de sair de uma situação de risco" (ISO/IEC, 2007);

j. [Comunicar o Risco] é a "Troca ou compartilhamento de informação sobre risco entre um tomador de decisão e outros interessados" (ISO/IEC, 2007);

k. [Estimar o Risco] é o "Processo de atribuir valores às probabilidades e consequências de um risco" (ISO/IEC, 2007);

l. [Identificar o Risco] é o "Processo de encontrar, listar e caracterizar elementos do risco" (ISO/IEC, 2007);

m. [Reduzir o Risco] é um conjunto de "ações adotadas para reduzir a probabilidade de ocorrência ou as consequências negativas, ou ambas, associadas a um risco" (ISO/IEC, 2007);

n. [Reter o Risco] é a "aceitação do encargo da perda ou benefício do ganho advindos de um risco em particular" (ISO/IEC, 2007);

o. [Transferir o Risco] é "compartilhar com outro parceiro o encargo da perda ou o benefício do ganho, associado a um risco" (ISO/IEC, 2007).

A partir das definições acima, pode-se inferir, entre outras coisas, que o conceito de ativo é fundamental para a gestão de riscos de segurança da informação, embora seja digno de nota que a norma AS/NZS 4360 (Standards Australia and Standards New Zealand, 2004), norma geral de gestão de riscos, não se fundamenta na existência de ativos para a gestão do risco.

Note-se ainda que a determinação de um risco de segurança da informação envolve a coleta de dados sobre vários elementos ou fatores de risco: ativos, ameaças, vulnerabilidades, probabilidades, consequências e impactos.

A próxima seção aprofunda o entendimento do conceito de ativo de informação e as formas de levantamento de inventários de ativos.

3.1 Ativos de Informação

Devido à natureza intangível de muitos ativos de informação, a ABNT (2008) é bastante genérica no que se refere a quais seriam estes ativos. Em seu Anexo B, a ABNT (2008) faz uma classificação primária dos ativos entre primários e de suporte. Os ativos primários apoiam-se nos ativos de suporte.

3.1.1 Classificação de Ativos

São ativos primários de uma organização (ISO/IEC, 2007):

a. [Processos e Atividades do Negócio] são executados visando o desempenho das funções da organização. Processos são os elementos que mais agregam valor à organização;

b. [Informações] são usadas no apoio à execução desses processos, além das de caráter pessoal, estratégicas ou com alto custo de aquisição.

Além dos ativos primários, o Anexo B da 27005 (ISO/IEC, 2007) sugere uma classificação de ativos de suporte, composta por seis classes:

a. [Hardware] Constituída todos os elementos físicos que suportam a execução automática de processos;

b. [Software] Constituída pelos programas de computador de sistema operacional, de suporte, software empacotado e aplicativos de negócio padronizados ou específicos da organização;

c. [Rede de Computadores] Constituída por todos os dispositivos de redes e telecomunicações que interconectam os dispositivos e elementos dos sistemas de informação, como redes telefônicas, redes de computadores de longa distância, metropolitanas, locais e *ad hoc*, roteadores, *bridges*, *hubs* e outras interfaces de comunicação;

d. [Pessoal] Constituída por grupos enquadrados entre: tomadores de decisão, usuários, pessoal de manutenção e operação e desenvolvedores de software;

e. [Sítio] Constituída por todos os lugares que agregam os demais ativos sob escopo, bem como os meios para operar este sítio, como: (i) espaços exteriores, (ii) perímetros defensivos, (iii) zonas dentro do perímetro (escritórios, zonas seguras), (iv) serviços essenciais para operação de equipamentos, (v) serviços de comunicação, e (vi) utilidades para suprimento de energia elétrica, água, esgoto, condicionamento do ar etc;

f. [Estrutura Organizacional] Constituída por (i) autoridades (conselhos e comitês), (ii) subunidades da organização (departamentos, divisões, seções), (iii) projetos e (iv) subcontratados e fornecedores.

3.1.2 Levantamento de Ativos

O levantamento dos ativos baseado na ABNT (2008) compreende a catalogação dos ativos nas categorias descritas.

A catalogação fragmentada de ativos enquadrados nas categorias propostas pela 27005, embora seja uma forma prática de tratamento do grande volume de informações necessárias ao inventário de ativos de uma organização, propõe a separação dos ativos em hardware,

software, rede, pessoal, sítio e estrutura organizacional. É opinião do autor que tal separação torna difícil a identificação precisa da interdependência entre as partes que constituem a execução dos processos e sistemas de informação.

Como não há consenso entre as metodologias de gestão de riscos sobre qual a melhor forma de proceder ao inventário de ativos, que constitui o conjunto de elementos delimitados pelo escopo de GRSI, bem como não é papel de uma norma internacional como a 27005 apresentar uma metodologia específica para levantamento de ativos, outras abordagens devem vir em auxílio, como a metodologia Octave (ALBERTS; DOROFEE, 2002), por exemplo, que aborda de forma mais precisa a gestão de riscos em ativos de Tecnologia da Informação, e apresenta um modelo propositivo para levantamento dos ativos de TI. O levantamento é feito por meio da realização de workshops de elicitação de conhecimento, empregando-se técnicas como entrevistas e *brainstorm*, onde os participantes selecionados das áreas de negócios da organização focam os seus trabalhos e identificam os ativos relacionados ao desempenho de suas atividades.

3.2 Análises de Eventos

Para que se possa ter eficácia na descoberta das consequências para os ativos e dos possíveis impactos sobre os negócios da organização, faz-se necessário identificar mais precisamente quais os eventos poderiam levar a essas perdas. Tal análise evita esforço desnecessário na análise de consequências e impactos, uma vez que, se não forem encontrados quaisquer eventos que poderiam afetar um ativo, não há necessidade de empregar muitos recursos na identificação de consequências e impactos.

São exemplos de eventos de segurança da informação:

a. o funcionário X não está usando crachá;
b. o *firewall* X não está bloqueando a porta 1521 na máquina Y;
c. a senha do usuário X é fraca;
d. um curto-circuito ocorreu no estabilizador na tarde de hoje;
e. faz 2 meses que o *backup* do banco de dados Z não é realizado;
f. a chave da sala de servidores sumiu;
g. faltou energia no bloco C hoje à tarde;
h. a cerca foi rompida na noite de ontem;
i. o alarme de detecção de intrusos disparou três vezes seguidas;
j. o alarme de detecção de intrusos está quebrado.

A compreensão dos eventos que ocorrem no ambiente de uma organização é essencial para que os riscos sejam avaliados com maior precisão. No caso específico da GRSI, os eventos estão relacionados aos ativos. Dessa forma, após o levantamento de ativos, é possível uma melhor estimativa dos eventos possíveis que poderão estar associados a cada ativo crítico.

3.2.1 Critérios ou Objetivos de Segurança da Informação

Disponibilidade, integridade e confidencialidade são os três principais critérios de segurança da informação para uso nas organizações em geral, sendo também utilizados outros como a autenticidade, o não repúdio, a contabilização, a confiança e a conformidade. Além dos critérios ou objetivos citados, a informação também apresenta como critérios de mensuração de consequências a efetividade e a eficiência, entre outros:

a. [Confidencialidade] "propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados" (ABNT, 2006);

b. [Integridade] "propriedade de salvaguarda da exatidão e completeza de ativos" (ABNT, 2006);

c. [Disponibilidade] "propriedade de que (um sistema de) informação esteja acessível e utilizável sob demanda por uma entidade autorizada" (ABNT, 2006);

d. [Autenticidade] Garantia da identidade ou veracidade do emissor de uma mensagem, como sendo genuíno e que possa ser verificado quanto à sua confiança (ITGI, 2007);

e. [Não repúdio] Mecanismo para garantia à autoria de determinadas ações, impedindo o repúdio (negação) da mesma (ITGI, 2007);

f. [Contabilização (*accountability*)] Habilidade de um sistema em determinar as ações e comportamentos de um único indivíduo dentro de um sistema, e identificar aquele indivíduo em particular (ITGI, 2007);

g. [Confiança (*reliability*)] É a segurança de que um sistema pode ser usado para o cumprimento de uma determinada atividade demandada por um usuário (ITGI, 2007);

h. [Conformidade] É a garantia de que a informação é gerida conforme os regulamentos e leis aplicáveis (ITGI, 2007);

i. [Efetividade] É a garantia de que a informação é relevante e pertinente aos processos de negócio e é entregue ao usuário de forma correta, tempestiva, consistente e usável (ITGI, 2007);

j. [Eficiência] É a garantia de que a informação é produzida com o uso otimizado de recursos, isto é, da forma mais produtiva e econômica (ITGI, 2007).

Esses critérios de segurança são a base para as análises dos fatores de risco, conforme aprofunda o restante desta seção.

3.2.2 Causalidade e Cadeias de Eventos

Não há uma forma simples de análise de eventos, pois os mesmos usualmente ocorrem em cadeias complexas. Um evento de segurança de grande severidade é usualmente decorrência de vários eventos de menor severidade que formam uma cadeia.

A eficácia de sistemas automatizados de monitoramento da segurança depende fortemente da análise de correlações entre eventos.

Os eventos que se situam entre a pura regularidade (inevitabilidade) e entre o caos (imprevisibilidade) estão correlacionados a um ou mais eventos passados bem como tem elevada chance de provocar um ou mais eventos futuros. O estudo das relações entre os eventos, chamado de "causalidade", é feito no domínio da filosofia há pelo menos 3.000 anos[5]. É importante para um gestor de segurança desenvolver a habilidade de analisar a causalidade entre eventos, porque é por meio dessa habilidade que se desenvolve melhor capacidade de prever os eventos e modelá-los na forma de riscos.

5 http://en.wikipedia.org/wiki/Causality

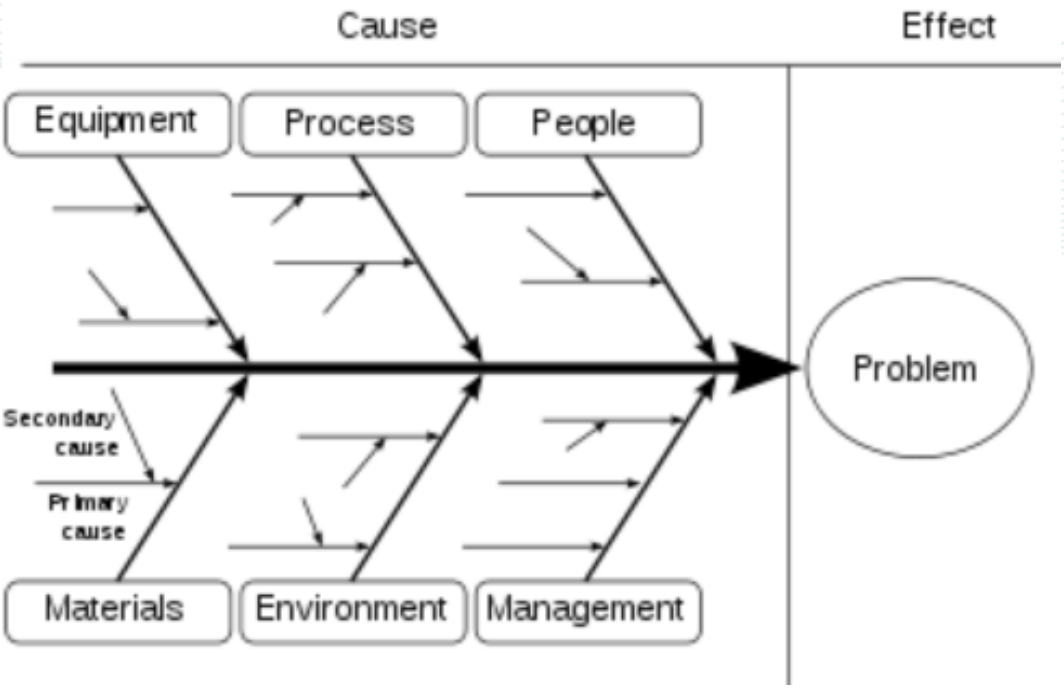

Figura 2 – Diagrama espinha de peixe.
Fonte: http://en.wikipedia.org/wiki/Causality.

Várias são as teorias e modelos desenvolvidos para explicar como um evento produz outro, e na área da gestão da qualidade foi desenvolvido o diagrama de causa-efeito, conhecido como diagrama de Ishikawa ou de "espinha de peixe". Um exemplo é ilustrado na Figura 2, onde a ocorrência de um problema ou do efeito de um problema é descrita por meio da análise de suas causas-raiz, que são falhas relacionadas a equipamentos, processos, pessoas, materiais, ambiente e gestão.

A Figura 2 ilustra como um evento de segurança hipotético pode ser resultante de uma série de outros eventos de menor severidade.

3.2.3 Análise de ameaças e vulnerabilidades

A análise de eventos de segurança da informação pode ser dividida em várias etapas que compreendem análise de fatores de risco como ameaças, vulnerabilidades, controles, consequências operacionais e impactos sobre negócios.

As principais análises que são reconhecidas como tal são a análise de ameaças e a análise de vulnerabilidades.

Uma ameaça "é uma causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização" (ISO/IEC, 2004).

Uma vulnerabilidade "é uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças" (ISO/IEC, 2004).

Em ambos os casos, ameaças e vulnerabilidades podem ser representações de eventos passíveis de ocorrência em um ambiente de uma organização.

Para fins de racionalização de esforços na busca por ameaças e vulnerabilidades, os métodos de GRSI propõem que a identificação de ameaças seja feita antes da identificação de vulnerabilidades, porque seria proibitivo o custo para identificação de vulnerabilidades em todos os ativos existentes, independentemente da existência de ameaças correspondentes.

3.2.4 Análise de Ameaças

Conforme a 27005, uma fonte de ameaças é um agente ou condição que exercita ameaças. Ameaças podem ter como fonte seres humanos e o ambiente, sendo que seres humanos podem agir deliberadamente ou acidentalmente. Desta forma, quanto à origem, as ameaças podem ser classificada em:

a. humanas deliberadas (D);

b. humanas acidentais (A); e

c. ambientais (E - *Environmental*)

Conforme a 27005, as ameaças também podem ser organizadas quanto ao tipo:

a. [Dano físico] Incidente com equipamento, instalação, mídia ou substância que foi comprometido;

b. [Eventos naturais] Incidentes com fontes de água, do solo e subsolo ou do ar;

c. [Paralisação de serviços essenciais] Incidentes em serviço de energia elétrica, água encanada, esgoto, condicionamento de ar etc;

d. [Distúrbio causado por radiação] Incidentes causados por radiação térmica ou eletromagnética;

e. [Comprometimento da informação] Interceptação, destruição, furto, cópia indevida, adulteração de hardware ou software;

f. [Falhas técnicas] Falha, defeito, saturação ou violação das condições de uso de equipamento de informática;

g. [Ações não autorizadas] Uso, cópia ou processamento ilegal de dados;

h. [Comprometimento de funções] Erro em uso, abuso de direitos, forjamento de direitos, repúdio de ações, indisponibilidade de pessoas.

O Anexo C da 27005 apresenta um catálogo de ameaças típicas, classificadas quanto ao tipo e à origem.

A 27005 indica que atenção especial deve ser dada às fontes de ameaças intencionais e humanas, com suas correspondentes motivações. Para tanto a norma também apresenta uma tabela de fontes de ameaças humanas intencionais, associadas às possíveis motivações dessas fontes.

O uso das informações do Anexo C provê auxílio à identificação de eventos possíveis que se constituam em ameaças aos ativos catalogados durante a GRSI.

3.2.5 Análise de Controles

Na 27005 é proposta uma etapa de identificação de controles existentes e planejados} efetuada possivelmente antes da identificação de vulnerabilidades, mas após a identificação de ameaças. Ao se detectar os controles atualmente existentes na organização, bem como aqueles planejados, pode-se descobrir uma série de vulnerabilidades potenciais, já que cada vulnerabilidade pode ser descrita por uma correspondente ausência de controles, bem como cada controle usualmente corresponde à redução de uma vulnerabilidade.

3.2.6 Análise de Vulnerabilidades e Controles

Uma vulnerabilidade "é uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças" (ISO/IEC, 2004).

Vulnerabilidades têm origem no ambiente interno dos ativos, sejam eles processos, documentos, pessoas, software, hardware, redes, instalações e estruturas organizacionais.

A 27005 apresenta um catálogo de vulnerabilidades classificadas quanto ao tipo de ativo secundário à qual se aplicam:

a. vulnerabilidades de hardware;

b. vulnerabilidades de software;

c. vulnerabilidades de rede;

d. vulnerabilidades de pessoal;

e. vulnerabilidades de instalações e

f. vulnerabilidades da estrutura organizacional.

Essas vulnerabilidades estão ainda associadas a possíveis ameaças, possibilitando a construção de cenários de incidentes sobre os ativos inventariados.

O catálogo de vulnerabilidades da 27005 possui uma natureza genérica e pouca aplicabilidade sobre vulnerabilidades específicas de ativos tecnológicos, como computadores e software.

Dessa forma, para o caso de análise de vulnerabilidades de ativos tecnológicos, bem como de sistemas específicos, a 27005 (ISO/IEC, 2007) recomenda o uso de métodos, técnicas e ferramentas específicas, algumas das quais são:

a. [Ferramenta automatizada de análise de vulnerabilidade] Aplica-se à análise de redes de computadores e busca identificar portas abertas em *hosts* e vulnerabilidades associadas a essas portas. Nessus é uma das ferramentas mais comumente utilizadas para análise de vulnerabilidades em redes;

b. [Teste e avaliação de segurança] Baseada na elaboração e execução de *scripts* de teste;

c. [Teste de penetração] Técnica amplamente variável e aplicável a vários canais, como artefatos tecnológicos (ex: sítios *web*, redes de telecomunicação, redes sem fio, prédios, perímetros e áreas militares) e pessoas (tentativas de fraude, engenharia social, áreas vigiadas por humanos). Um exemplo de metodologia aplicável é a ISECOM (2008);

d. [Revisão de Código] Técnica aplicável a software, onde o código-fonte de um programa é inspecionado visualmente por programadores (ou por meio de softwares parcialmente eficientes) a fim de se identificar vulnerabilidades a ataques como *SQL injection*, *buffer overflow*, *stack overflow*, *cross site-script* etc. A revisão de código é parte de abordagens como as descritas em Howard e Lipner (2006);

e. [Entrevistas] Aplicáveis a colaboradores e usuários;

f. [Questionários] Para coleta de grandes volumes de dados;

g. [Inspeção física] Visitas ao sítio;

h. [Análise de documentos], por exemplo: análise de registros de incidentes.

3.2.7 Análise de Consequências e Impactos

Uma vez levantados ou elicitados os ativos de informação de uma organização, estes precisam ser valorados, isto é, ordenados dos mais críticos ao menos críticos, segundo o julgamento dos analistas, que deve ser o menos subjetivo possível.

Na GRSI, essa valoração é inicialmente estabelecida em dois passos:

a. levantamento de consequências operacionais da perda de segurança em ativos;

b. estimativa de impacto sobre negócios relacionados à perda de proteção para cada ativo.

3.2.8 Análise de Consequências Operacionais da Perda de Segurança

Um levantamento preliminar de ativos deve considerar quais são os ativos e quais as consequências operacionais relativas a perdas de proteção sobre estes ativos.

Um levantamento pode ser guiado por respostas a perguntas como:

a. quais são os ativos que você quer proteger, por exemplo, devido a leis e regulamentos?

b. quais são os ativos mais importantes e de quais outros ativos eles dependem?

c. qual é a justificativa para que X seja um ativo?

d. você ampliou o seu escopo de análise para o nível da organização inteira?

A perda de segurança em um ativo decorre de eventos de segurança relacionados ao ativo. Tal perda é tecnicamente chamada de {bf brecha de segurança}, e apresenta consequências operacionais para a organização. Os eventos possíveis são descritos em cenários de incidentes, resultantes da combinação entre ameaças e vulnerabilidades. Sem entrar no mérito de quais seriam os eventos de segurança que podem afetar um ativo, as consequências operacionais devem ser estimadas em termos de queda na disponibilidade, integridade e confidencialidade da informação relacionadas a um ou mais ativos impactados pelo evento.

Uma vez que são conhecidos como os incidentes reduzem o alcance dos objetivos de segurança relacionados aos ativos, é possível estimar as consequências operacionais dessas reduções. Em outras palavras, deve-se traduzir perda de confidencialidade, integridade e disponibilidade em termos como perda de serviços, pagamento de multas e infrações contratuais.

A 27005 apresenta, no seu Anexo B, um conjunto de critérios que podem ser empregados para atribuição de valores de criticidade aos ativos na ocorrência de eventos em geral. A recomendação é que se defina uma base comum de análise, e duas formas são indicadas:

a. pela análise das consequências operacionais resultantes da perda de confidencialidade, integridade, disponibilidade, não repúdio, contabilização, autenticidade ou confiabilidade dos ativos ;e

b. de forma mais simples, pela avaliação direta dos impactos sobre os negócios da organização (ver Seção Impactos), em decorrência do comprometimento dos ativos.

Acerca da primeira abordagem, algumas consequências operacionais a considerar são (ISO/IEC, 2007):

a. violação da legislação, regulamentos ou contratos;

b. redução no desempenho de negócios;

c. perda de confiança e reputação de clientes e sociedade;

d. vazamento de informação pessoal;

e. aumento de perigos para os colaboradores;

f. efeitos adversos no cumprimento da lei;

g. brechas de confidencialidade;

h. brechas na ordem pública;

i. perdas ou custos financeiros;

j. riscos e crises ambientais;

k. crise governamental;

l. interrupção de serviços;

m. perda de vantagem competitiva.

Abordagens qualitativas são usualmente adotadas para avaliar as consequências de comprometimento dos ativos, uma vez que a atribuição de valores financeiros a ativos nem sempre é possível. Uma escala de pelo menos três valores pode ser usada: alta, média e baixa.

O estabelecimento das dependências entre os ativos é importante para uma correta valoração de consequências aos mesmos. Quanto mais processos de negócio dependerem de um certo ativo, mais crítico é o ativo. Por exemplo, se três grandes sistemas de comércio eletrônico dependem de um servidor de banco de dados e de uma conexão de rede, esses dois ativos devem também ser críticos.

Conforme a 27005, o resultado do levantamento de ativos deve conter uma lista dos ativos, com a correspondente valoração das consequências relativas para:

a. perda de confidencialidade (divulgação indevida);

b. perda de integridade, autenticidade, não repúdio e contabilização (modificação indevida);

c. perda de disponibilidade e confiabilidade (indisponibilidade e destruição); e

d. custos de substituição.

3.2.9 Análise de Impactos sobre Negócios

A estimativa das consequências da perda de segurança para um ativo na eventualidade de incidentes permite apenas a descoberta dos valores operacionais dos ativos para a organização, mas não indica precisamente como essas perdas poderão impactar os negócios da organização em si.

Conforme a 27005, impacto é "uma mudança adversa no nível de objetivos de negócios alcançados". Há que se considerar que um único incidente pode afetar vários ativos simultaneamente. Em vez de estar diretamente relacionado ao ativo, o impacto decorre dos efeitos de um incidente que pode afetar vários ativos de forma agregada e da mudança adversa sobre os negócios da organização. Essa mudança adversa pode se dar imediatamente (operacionalmente) bem como no futuro, por meio de perdas financeiras e de mercado.

A 27005 propõe, para a avaliação do impacto operacional direto e indireto, a consideração dos seguintes efeitos:

a. custo financeiro de substituição de um ativo;

b. custo de aquisição, configuração e instalação de um novo ativo ou de seu {\it backup};

c. custo de operações suspensas devido ao acidente, até que o serviço seja restaurado;

d. resultados devido a brechas na segurança da informação;

e. violação de obrigações;

f. violação de códigos de conduta, entre outros.

Uma vez feita uma valoração do impacto sobre negócios, um nível de impacto ou criticidade deve estar relacionado a cada ativo, e pode empregar escalas qualitativas, usando valores como "muito alto", "alto", "médio", "baixo" e "muito baixo".

4 O Processo de Gestão de Riscos

A seção anterior apresentou os principais elementos conceituais que são articulados no processo da 27005. A Figura 4 apresenta o fluxograma geral do processo de gestão de riscos de segurança da informação, GRSI, adotado pela 27005.

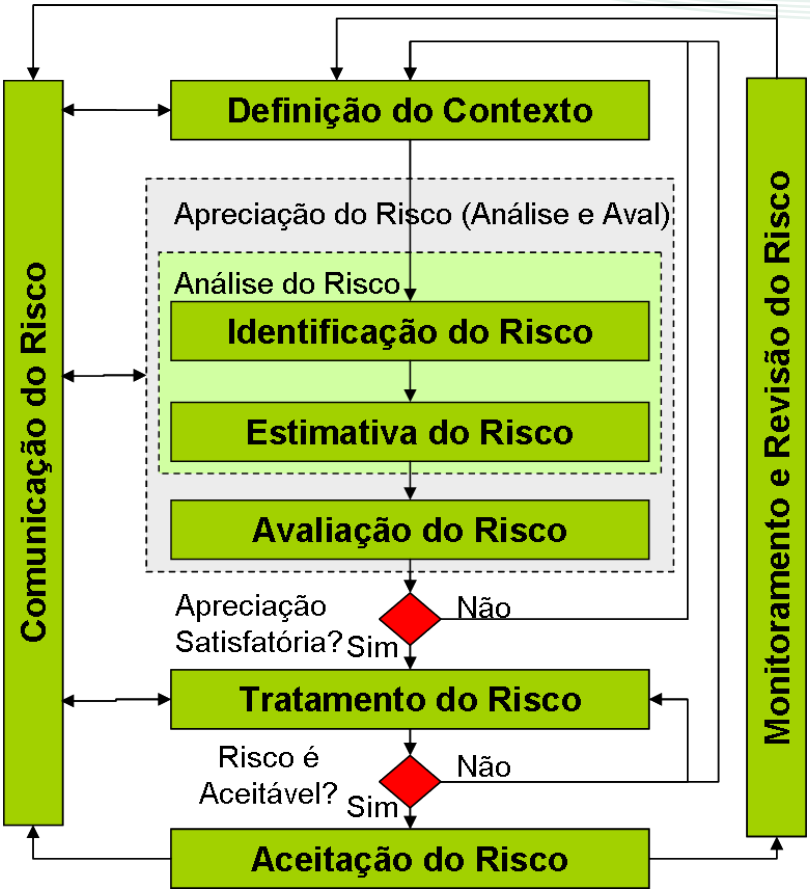

Figura 4. O processo de gestão do risco da ISO 27005:2008.
Fonte: Adaptado de ISO/IEC (2007).

O Processo de gestão dos riscos é um processo contínuo e iterativo e suas atividades e fases são apresentadas nas cláusulas 7 a 12 da norma, compreendendo as seguintes (ISO/IEC, 2007):

a. [Definição do contexto] Fase de preparação para implementação da gestão de riscos, que envolve principalmente a definição de três aspectos: (i) critérios básicos para GRSI, (ii) escopo e limites do SGRSI; e (iii) organização que vai operar a GRSI;

b. [Apreciação do Risco] A Apreciação do Risco é a fase mais intensa do processo de GRSI no que concerne à coleta e tratamento de informações. Envolve a Análise do Risco e a Avaliação do Risco. A Análise do Risco compreende a Identificação do Risco e a Estimativa do Risco. A Identificação do Risco é o processo de encontrar, listar e caracterizar os elementos ou fatores dos riscos. Durante a identificação, várias análises são efetuadas, e pode ser empregado um amplo arcabouço de técnicas. A Estimativa do Risco determina a magnitude ou nível de cada risco individual, e pode empregar métodos qualitativos e (ou) quantitativos. Atribui níveis para as probabilidades e consequências de cada risco. A Avaliação do Risco compreende a priorização de cada risco dentro do conjunto dos riscos estimados, conforme os critérios de avaliação e os objetivos de segurança relevantes para a organização;

c. [Tratamento do risco] Fase que envolve a decisão entre reter, evitar, transferir (compartilhar) ou reduzir os riscos;

d. [Aceitação do risco] fase que compreende o registro formal da decisão pelo aceite dos riscos residuais existentes na organização;

e. [Comunicação do risco] conjunto de atividades continuamente executadas e que envolve a troca de informações sobre riscos entre os tomadores de decisão e todos os envolvidos na organização (*stakeholders*);

f. [Monitoramento e revisão do risco] conjunto de atividades continuamente executadas e que envolve o monitoramento dos diversos fatores de caracterização do risco, a fim de identificar quaisquer mudanças no contexto da organização, atualizar o panorama de riscos da organização e aprimorar o processo de gestão de riscos da organização.

Uma característica geral da 27005 é que todas as suas fases e atividades são organizadas na forma de processos, que contém entradas, ações, guias para implementação e saídas bem caracterizadas, mas de forma genérica.

Conforme a 27005, os benefícios decorrentes da adoção de uma abordagem de gestão de riscos aderente à norma compreendem:

a. riscos são identificados;

b. riscos são apreciados em termos de consequências e chances de ocorrência;

c. as chances e consequências de riscos são comunicadas e compreendidas;

d. uma ordem de prioridade para tratamento de riscos é estabelecida;

e. uma ordem de prioridade para redução dos riscos é estabelecida;

f. os intervenientes são envolvidos em decisões sobre riscos e mantidos informados sobre o *status* da gestão de riscos;

g. o monitoramento dos riscos é efetivo;

h. os riscos e o processo de gerência de riscos são monitorados e revistos regularmente;

i. captura-se informação que permite a melhoria da abordagem de gestão de riscos;

j. os gerentes e o *staff* são educados sobre riscos e ações tomadas para mitigá-los.

A Figura 5 apresenta numa visão esquemática de como ocorre o fluxo da informação num processo organizado segundo o modelo da 27005.

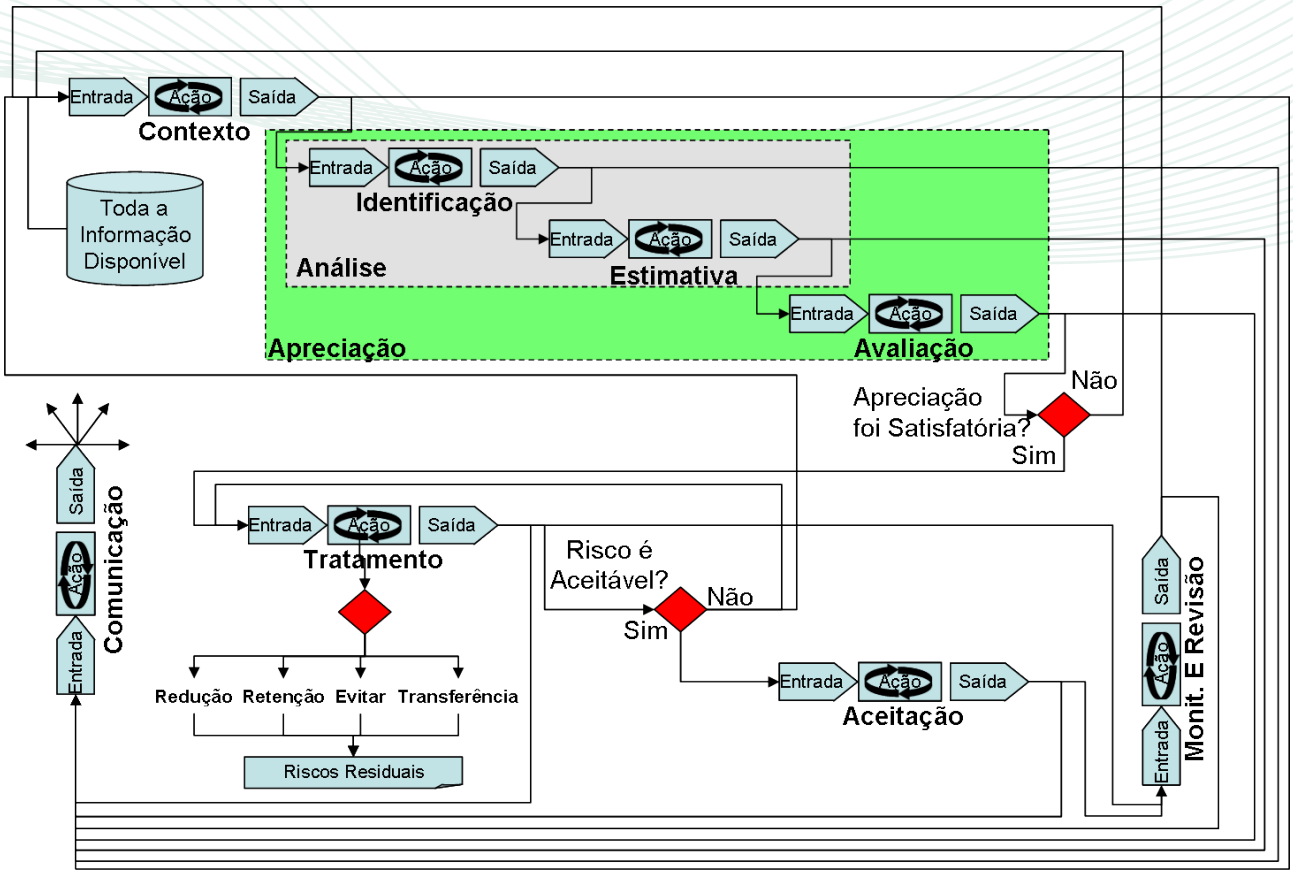

Figura 5. Fluxo de informações na Gestão de Riscos aderente à ISO/IEC (2007).
Fonte: Autor.

Conforme ilustra o fluxo de dados da Figura 5, para a Definição do Contexto é necessária toda a informação disponível, inclusive as produzidas por execuções anteriores de qualquer fase, os resultados das apreciações insatisfatórias e os planos de tratamento do risco que não foram aceitos, bem como dados do monitoramento e revisão da GRSI. A Apreciação do Risco é composta pelas fases de Identificação, Estimativa e Avaliação. A Identificação e a Estimativa compreendem a Análise.

Existem dois *pontos de controle* importantes em um processo de gestão de riscos aderente à 27005, que atuam imediatamente após a Apreciação e após o Tratamento do Risco. No caso dos resultados da Apreciação ou do Tratamento serem insatisfatórios, faz-se necessário repetir a execução de passos anteriores do processo. O Tratamento produz um plano que contém uma estimativa de riscos residuais, que devem ser aceitos pela alta gestão. O processo é completado pela fase de Aceitação, que compreende a aceitação do plano de tratamento de riscos, que por sua vez indica os riscos residuais da organização.

As seções seguintes descrevem em mais detalhes os aspectos de cada fase.

5 Definição do Contexto da GRSI

A fase de Definição do Contexto cria ou ajusta o contexto para execução da GRSI. Recebe como entrada todas as informações sobre a organização relevantes para a definição do contexto, e produz como saída: (i) a especificação dos critérios básicos para GR; (ii) a especificação do escopo e limites cujos riscos serão geridos e (iii) uma organização preparada para operar a gestão de riscos. As ações realizadas na fase são as capazes de produzir os resultados esperados, e são detalhadas a seguir.

5.1 Descrição de Critérios Básicos para GR

Os Critérios Básicos para GR são estabelecidos preferencialmente sob supervisão direta da alta gestão e subdividem-se em:

a. [Critérios para Avaliação de RSI] Que considerações devem ser usadas para avaliar os riscos?

b. [Critérios para Determinação do Impacto de Incidentes] Que considerações devem ser usadas para determinar o impacto de incidentes de segurança para o alcance dos objetivos de negócio da organização?

c. [Critérios para Aceitação de RSI] Que considerações serão usadas pela alta gestão para aceitar os riscos residuais da organização?

Abordagens para a descrição de cada um desses critérios são definidas a seguir.

5.1.1 Critérios para Avaliação de Riscos de Segurança da Informação

Os critérios para avaliação de RSI são usados na fase de Avaliação, que compreende a ordenação dos riscos quanto à prioridade para tratamento. O estabelecimento de critérios deve considerar (ISO/IEC, 2007):

a. [Valor Estratégico] Qual o valor Estratégico para a organização dos processos de negócio que tratam com informação? Qual o valor dos processos responsáveis pelo tratamento da informação em sua organização?

b. [Criticalidade dos ativos de informação] Quão crítico para o alcance dos objetivos de negócio da organização são os ativos de informação envolvidos?

c. [Requisitos legais, regulatórios e contratuais] A quais aspectos legais, regulatórios e contratuais está sujeito o tratamento da informação na sua organização?

d. [Importância da disponibilidade, confidencialidade e integridade] Qual a importância da disponibilidade, confidencialidade e integridade para a operação e para os negócios? Qual a importância absoluta e relativa destes critérios?

e. [Expectativas e percepções] Quais as expectativas e percepções dos envolvidos, além de consequências negativas para a boa fé e reputação destes e da organização? Todos os envolvidos manifestaram suas percepções?

f. [Prioridades] Quais as prioridades para tratamento de riscos? Quais as ações prioritárias de tratamento?

Durante o estabelecimento de critérios para avaliação de riscos de segurança da informação, uma descrição formal que responda às questões acima precisa ser formalizada. Tal descrição será usada como base para várias etapas do processo de GRSI.

5.1.2 Critérios para Determinação do Impacto de Incidentes

A quais eventos de segurança está sujeita a organização? Que impactos esses eventos podem causar? O desenvolvimento e a especificação de critérios de determinação de impacto devem descrever o grau de danos ou custos para a organização, causado por eventos de segurança, e deve considerar os seguintes aspectos (ISO/IEC, 2007):

a. [Níveis de classificação] Quais os níveis de classificação de segurança dos ativos de informação impactados? Como os eventos impactam ativos de informação de diversos níveis?

b. [Brechas de segurança da informação] Brechas de segurança da informação envolvem perda de confidencialidade, integridade e disponibilidade. Quais são as brechas que podem ocorrer?

c. [Operações obstruídas] Quais podem ser as operações obstruídas, sejam elas internas ou com terceiras partes? Que operações podem ser interrompidas por eventos?

d. [Perda de negócios e valores financeiros] Como a organização pode perder negócios e valor financeiro com os eventos?

e. [Rompimento de planos e prazos] Como os planos da organização podem ser afetados ou completamente obstruídos? Como os prazos de sua organização podem ser afetados por eventos?

f. [Danos à reputação] Quais os danos que podem ocorrer à reputação da organização?

g. [Infração de requisitos] Que infrações de requisitos legais, regulatórios ou contratuais podem ocorrer? Como a sua organização pode infringir leis, normas, regulamentos ou contratos em decorrência de eventos de segurança?

Durante o estabelecimento de critérios para determinação do impacto de incidentes, uma descrição formal que responda às questões acima precisa ser elaborada, e será usada como base para várias etapas do processo de GRSI.

5.1.3 Critérios para Aceitação de RSI

Que considerações serão usadas pela alta gestão para aceitar os riscos da organização na fase de Aceitação? Essas considerações devem ser definidas na forma de critérios para aceitação de riscos de segurança da informação. Tais critérios guiarão os analistas de risco na preparação de análises e avaliações preliminares de riscos, de modo que o trabalho do analista de riscos possa ser aceito pela gestão da organização. Uma organização deve desenvolver escalas próprias para níveis de aceitação de riscos, considerando os seguintes aspectos (ISO/IEC, 2007):

a. [Múltiplos níveis de disparo] como são alcançados os níveis de risco alvo que são desejados pelos gestores? Quais os níveis e gatilhos de risco de sua organização?

b. [Provisão para aceitação] Como a alta gestão poderá aceitar riscos acima dos níveis estabelecidos? Sob quais circunstâncias definidas? Que condições especiais possibilitam a aceitação de riscos que, em condições normais, seriam inaceitáveis?

c. [Custos e benefícios] Qual a relação entre o benefício estimado (ex: financeiro) e risco de dano estimado?

d. [Diferentes níveis de risco] Quais são os diferentes níveis de risco aceitáveis conforme as classes de risco? Qual a tolerância a riscos de não conformidade com legislação comparativamente à tolerância a riscos de quebra de contrato?

e. [Aceitação condicionada] Como aceitar condicionalmente o risco, sujeito à aprovação de tratamentos futuros dentro de um determinado período? Quais os riscos que você aceita hoje, condicionados à tomada de ações de controle futuras?

f. [Tempo para existência do risco] O risco aceito está relacionado a uma atividade de curto prazo ou de longo prazo?

g. [Critérios de negócio] Como o seu negócio é diferente dos demais?

h. [Aspectos legais e regulatórios] Como os aspectos legais e regulatórios se aplicam ao negócio da organização?

i. [Operações] Em que tipos de operações a organização está envolvida?

j. [Tecnologias] Quais as tecnologias empregadas pela organização?

k. [Finanças] Quais os impactos financeiros dos riscos à organização?

l. [Fatores sociais e humanitários] Fatores sociais e humanitários se aplicam à sua organização e podem influenciar a aceitação dos riscos?

A Tabela 1 apresenta um exemplo de escala de mensuração de riscos. Um exemplo de critério a ser referendado pela alta gestão de um órgão seria aceitar, sem justificativas, apenas os riscos cujo valor seja baixo (entre 0 e 2).

Tabela 1. Uma escala para mensuração do risco. Fonte: (ISO/IEC, 2007)

- Low risk: 0-2
- Medium Risk: 3-5
- High Risk:6-8

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

5.2 Especificação do Escopo e Limites da Gestão de Riscos

Todo sistema possui um escopo e limites que demarcam esse escopo; tal escopo precisa dessa delimitação para que tenha convergência a gestão de riscos. Segundo a ISO/IEC (2007) é preciso, com a especificação do escopo e limites, produzir um documento que responda às seguintes questões:

a. qual o escopo da GRSI a ser adotado?

b. quais os ativos relevantes que serão considerados, e que formarão o escopo?

c. quais ativos são pouco relevantes?

d. como você delimita os elementos do escopo? Por meio de limites físicos? Limites legais? Limites tecnológicos? Limites contratuais? Limites organizacionais?

e. em que ambiente a organização opera? Qual a relevância do ambiente para a GRSI? A sua organização opera em um ambiente controlado? Em um ambiente hostil? Com muitas ameaças?

Além desses aspectos, deve-se considerar, também segundo ISO/IEC (2007), que a delimitação do escopo pode ser influenciada pelos:

a. objetivos estratégicos, estratégias e políticas de negócios e serviços da organização;

b. processos de negócios;

c. funções e estruturas organizacionais;

d. requisitos legais, regulatórios e contratuais aplicáveis;

e. política de segurança da informação da organização;

f. abordagem geral de gestão de riscos da organização;

g. ativos de informação;

h. quantidade de sítios físicos da organização e suas características geográficas;

i. restrições afetando a organização;

j. expectativas dos intervenientes e outras partes interessadas;

k. ambiente sociocultural;

l. interfaces (ex: de troca de informação com o meio ambiente).

Devem ser providas justificativas para quaisquer exclusões de ativos do escopo indicado.

O resultado da atividade é uma *declaração preliminar de escopo de gestão de riscos*, um documento formal.

5.3 Definição da Organização para Operar a Gestão de Riscos

A definição da organização para operar a gestão de riscos (GR) é o ultimo aspecto na fase de Definição do Contexto. Uma organização com responsabilidades pela GRSI deve ser criada e mantida. Essa organização forma um subsistema, que poderia ser chamado de Sistema de Gestão de Riscos de Segurança da Informação. A Figura 5 apresenta o escopo desse sistema de forma abstrata e suas relações com o restante da organização.

Figura 5 – Arcabouço de um SGRSI - Sistema de Gestão de Riscos de Segurança da Informação.

Fonte: o autor.

Segundo a (ISO/IEC, 2007), são papéis e responsabilidades dessa organização:

a. desenvolvimento de um processo de GRSI adequado para a organização;

b. identificação e análise dos intervenientes e partes interessadas;

c. definições de papéis e responsabilidades por todos os parceiros na GRSI, tanto internos quanto externos à organização;

d. estabelecimento dos relacionamentos requeridos entre o SGRSI e os intervenientes, bem como das interfaces com as funções de gerenciamento de riscos de alto nível da organização (ex: gestão de riscos operacional), bem como com outros projetos e atividades relevantes;

e. definição dos caminhos de escalação de decisão;

f. especificação dos registros a serem mantidos;

O SGRSI deve ser aprovado pelos gestores de níveis adequados na organização, e é um importantes recursos que atendem aos requisitos da 27001 (ISO/IEC, 2006).

6 Apreciação do Risco

A Apreciação do Risco é o processo responsável por identificar, estimar e avaliar o risco. Envolve várias análises e avaliações que são agrupadas sobre os processos de Análise do Risco e de Avaliação do Risco. A apreciação do risco é um processo iterativo que, segundo a ABNT (2008), deve ser executada em pelo menos duas iterações. Tal abordagem é devida à inter-dependência entre os vários elementos levantados durante a identificação (ativos, ameaças, controles, vulnerabilidades, probabilidades, consequências, impactos e magnitude de riscos).

A Apreciação recebe como entradas os critérios básicos, escopo e limites, bem como a organização responsável pelo processo de GRSI, definidos na fase de definição dos conceitos.

A saída da apreciação é uma lista de riscos avaliados e priorizados conforme os critérios estabelecidos na fase anterior.

A seguir são detalhadas a análise e a avaliação dos riscos.

6.1 Análise do Risco

A Análise do Risco é a composição dos processos de Identificação do Risco e de Estimativa do Risco. A identificação do risco é o processo de encontrar, listar e caracterizar os elementos ou fatores do risco. O propósito da Avaliação do Risco é priorizar os riscos contra critérios de avaliação (estabelecidos na Definição do Contexto) e objetivos relevantes para a organização.

6.1.1 Identificação do Risco

O propósito da identificação do risco é, segundo ISO/IEC (2007), determinar o que pode acontecer para causar uma perda potencial, ou ganhar percepção sobre como, onde e porque a perda pode acontecer. A identificação do risco decompõe o risco em cinco fatores e os analisa individualmente. As atividades são:

a. identificação de ativos;

b. identificação de ameaças;

c. identificação de controles;

d. identificação de vulnerabilidades;

e. identificação de consequências,

Essas atividades são detalhadas a seguir.

6.1.1.1 Identificação de Ativos

A atividade de Identificação de Ativos recebe como entradas: (i) a declaração do escopo e limites da GR; e (ii) uma lista preliminar de ativos da organização, com indicação do responsável por cada um, além das localizações, funções e outras características dos ativos. O objetivo da atividade é identificar quais dos ativos estão no escopo a ser gerenciado, produzindo como saída uma lista de ativos cujos riscos devem ser gerenciados, associado a uma lista de processos de negócio relacionados com os ativos e a relevância desses relacionamentos.

Alguns aspectos importantes devem ser considerados na identificação de ativos são (ISO/IEC, 2007):

a. sistemas de informação são mais que hardware e software;

b. o nível de detalhamento dos ativos deve ser suficiente para permitir as fases subsequentes, especialmente a avaliação;

c. deve-se ter em mente que o nível de detalhamento das descrições dos ativos será refinado em iterações posteriores;

d. para cada ativo identificado, um responsável ou proprietário também deve ser identificado. Esse pessoal deve ser responsável pela produção, desenvolvimento, manutenção, uso e segurança do ativo. Ela é a principal fonte de informações sobre o ativo;

e. o responsável pelo ativo é a pessoa mais indicada para determinar o valor do ativo para a organização;

f. a coleta de dados não deve ultrapassar o escopo da gestão de riscos.

Tabela 2 – Exemplo de lista de ativos e suas relações com processos de negócio.

Ativo			Processos de Negócio						
#	Nome	Responsável	Venda	Atendimento	Compras	Finanças	Contabilidade	Gestão RH	Marketing
1	Sítio Web	João	ALTA	ALTA	BAIXA	BAIXA	BAIXA	MÉDIA	ALTA
2	Prédio Rua X	José		ALTA	BAIXA	BAIXA	BAIXA	ALTA	
3	Cadastro de Clientes	José	ALTA	ALTA	BAIXA	BAIXA	BAIXA	MÉDIA	ALTA
4	Aplicativo Web	João	ALTA	ALTA	BAIXA	BAIXA	BAIXA	MÉDIA	ALTA
5	Presidência	Pedro	BAIXA	BAIXA	ALTA	ALTA	MÉDIA	ALTA	MÉDIA

A Tabela 2 apresenta um esboço do que seria uma lista de ativos identificados, produzida ao final dessa atividade.

6.1.1.2. Identificação de Ameaças

A atividade de Identificação de Ameaças recebe como entradas informações sobre ameaças, obtidas por meio: (i) da revisão dos registros de incidentes e eventos de segurança; (ii) dos responsáveis pelos ativos, dos usuários; e (iii) de outras fontes, incluindo catálogos externos de ameaças. O objetivo é que ameaças e suas fontes sejam identificadas. A atividade produz como saída uma lista de ameaças, com a identificação do tipo e fonte da ameaça, como a Tabela 3.

Tabela 3. Exemplo de tabela de identificação de ameaças.

Ameaças	Tipo	Origem	Fonte
Incêndio	Dano Físico	Ambiental	Raios
		Acidental	Empregado negligente
			Curto-Circuito
		Intencional	Sabotador
			Ex-empregado
Dano por água		Ambiental	Chuva
			Inudação
		Acidental	Empregado negligente
			Empregado mal-treinado
		Intencional	Sabotador
			Ex-empregado
Falha no condicionamento de ar	Perda de serviços essenciais	Acidental	Falha técnica
			Empregado mal-treinado
Falha no suprimento de energia		Ambiental	Falha do fornecedor
			Tempestade
		Acidental	Empregado mal-treinado
			Sobrecarga de circuitos
		Deliberada	Sabotador
			Ladrão

Alguns aspectos importantes devem ser considerados na identificação de ativos, conforme a 27005:

a. uma ameaça pode afetar mais de um ativo e os impactos de uma mesma ameaça podem ser diferentes, conforme o ativo;

b. fontes de ameaça acidental e deliberada devem ser identificadas;

c. ameaças podem ter origem fora e dentro da organização;

d. a fim de tornar o trabalho limitado, ameaças devem ser identificadas genericamente e por tipo. Posteriormente, onde apropriado, ameaças individuais dentro das classes genéricas devem ser identificadas;

e. considerar que as ameaças estão em constante modificação, especialmente quando negócios e sistemas de informação se modificam;

Por fim, devem-se empregar, para a análise de ameaças, várias fontes de informação, como: (i) responsáveis pelos ativos; (ii) usuários dos ativos; (iii) {\it staff} da organização; (iv) gestores de instalações; (v) especialistas de segurança da informação; (vi) especialistas em segurança física; (vii) pessoal da área jurídica; (viii) agências de regulação e outras organizações civis; (ix) meteorologistas; (x) seguradoras; (xi) autoridades do governo; e (xii) catálogos e estatísticas obtidas em Normas; sociedades de indústria, comércio e serviços; governo; organizações jurídicas e seguradoras.

6.1.1.3 Identificação de Controles

A atividade de Identificação de Controles recebe como entradas a documentação dos controles e planos de implementação de tratamento de risco, se existentes. O objetivo da identificação de controles é que os controles existentes e planejados sejam identificados. A atividade produz como saída uma lista de todos os controles existentes e planejados, com seu *status* de implementação e uso.

São aspectos importantes que devem ser considerados na identificação dos controles, conforme a 27005 (ISO/IEC, 2007):

a. a identificação dos controles existentes evita trabalhos e custos desnecessários, com possível duplicação de controles;

b. controles que não funcionam adequadamente podem causar vulnerabilidades;

c. ao se identificar um controle, deve-se medir a efetividade do mesmo. A consulta a resultados de auditorias porventura existentes reduz o esforço na medição dessa eficácia (este é um dos principais trabalhos dos auditores);

d. como os controles existentes reduzem as vulnerabilidades de forma efetiva? A efetividade de um controle pode ser estimada através da estimativa do quanto ele reduz: (i) a chance de a ameaça ocorrer (ii) facilidade de exploração de uma vulnerabilidade por uma ameaça; ou (iii) impacto do evento de segurança;

e. controles com implementação planejada devem ser tratados da mesma forma que controles existentes;

f. a estimativa de eficácia dos controles é uma boa oportunidade para ajustes nos mesmos;

g. Um controle pode ser identificado como: (i) efetivo, (i) não efetivo, (iii) não suficiente ou (iv) não justificado. Nos casos (iii) controle não suficiente e (iv) controle não justificado, devem ser adotadas medidas para: (a) remoção; (b) substituição; ou (c) manutenção do controle (devido a razões como custo). Às vezes é mais econômico manter um controle implementado, mesmo que ele seja ineficaz.

São atividades recomendadas pela ISO/IEC (2007), quando da identificação de controles:

a. a revisão de documentos contendo informações sobre controles, por exemplo, planos de tratamento de riscos;

b. a revisão do *status* de implementação dos controles, no caso de um sistema de gestão de segurança da informação já implementado;

c. a verificação, junto a responsáveis pela segurança da informação e usuários dos controles, acerca do *status* real de implementação dos controles relativos ao escopo sob análise;

d. a condução de revisão de controles físicos nas instalações da organização em escopo, comparando com a lista dos controles que deveriam estar presentes e verificação de que os implementados estão funcionando corretamente e efetivamente.

6.1.1.4 Identificação de Vulnerabilidades

A Identificação de Vulnerabilidades recebe como entradas a lista de ameaças conhecidas, a lista de ativos e a lista de controles existentes e planejados. O objetivo é identificar as vulnerabilidades que podem ser exploradas pelas ameaças e, dessa forma, causar danos a ativos e à organização.

A identificação de vulnerabilidades produz:

a. uma lista de vulnerabilidades em relação a ativos, ameaças e controles; e

b. uma lista de vulnerabilidades não relacionadas a quaisquer ameaças, para revisão e monitoramento.

Uma lista das áreas e aspectos que devem ser observados é conforme a ISO/IEC (2007):

a. organização;

a. processos e procedimentos;

b. rotinas gerenciais;

c. pessoal;

d. ambiente físico;

e. configurações de sistemas de informação;

f. hardware, software e equipamentos de comunicação;

g. dependências de parceiros externos.

Alguns aspectos importantes devem ser considerados na identificação das vulnerabilidades, conforme a ISO/IEC (2007):

a. vulnerabilidades não são intrinsecamente ruins, pois é preciso uma ameaça estar presente para explorá-las;

b. vulnerabilidades sem ameaças correspondentes devem ser reconhecidas e monitoradas continuamente quanto a mudanças;

c. quaisquer controles ineficazes podem ser considerados vulnerabilidades;

d. a efetividade de um controle depende do ambiente onde ele está funcionando. Dessa forma, mudanças ambientais podem modificar bastante o grau e a extensão das vulnerabilidades;

e. ameaças sem vulnerabilidades correspondentes não constituem riscos;

f. vulnerabilidades podem estar intrinsecamente relacionadas às propriedades funcionais de um ativo (estarão sempre presentes);

g. muitas vulnerabilidades podem estar relacionadas a características de uso não previstas para um ativo quando de sua aquisição ou construção. Por exemplo, softwares, dispositivos e sistemas cujo uso atual não corresponde ao planejado;

h. vulnerabilidades dos ativos ocorre tanto de forma individual como agregada a outros ativos;

6.1.1.5 Identificação de Consequências e Cenários de Incidentes

A atividade de Identificação de Consequências recebe como entradas: (i) a lista de ativos; (ii) uma lista de processos de negócios da organização; (iii) uma lista de ameaças e vulnerabilidades correlacionadas com ativos e suas relevâncias. O objetivo da atividade é identificar as consequências de eventuais perdas de confidencialidade, integridade e disponibilidade sobre os ativos. A atividade produz como saída uma lista de {\bf cenários de incidentes} com suas consequências relacionadas aos ativos e processos de negócio. Esses cenários de incidente são base para a identificação dos riscos de segurança.

Conforme a ISO/IEC (2007), um cenário de incidente é a descrição de uma ameaça explorando uma vulnerabilidade ou conjunto de vulnerabilidades dentro de um incidente de segurança da informação. São consequências típicas da perda de confidencialidade, integridade e (ou) disponibilidade descritas num cenário de incidentes:

a. perda de efetividade do ativo;

b. condições operacionais adversas;

c. perda de negócios;

d. perda de reputação;

e. danos etc.

Alguns aspectos importantes devem ser considerados na identificação de consequências, conforme a 27005:

a. as consequências e o impactos de um cenário de incidente devem ser determinados por meio dos critérios definidos durante a Definição do Contexto;

b. um cenário de incidente pode afetar um ou mais ativos, ou parte de um ativo;

c. ativos devem ser valorados quanto ao valor financeiro ou consequências para o negócio no caso de dano ou comprometimento;

d. são aspectos que auxiliam na identificação de consequências operacionais em cenários de incidente: (i) o tempo de reparo e investigação; (ii) perda de tempo em trabalho; (iii) oportunidades perdidas para realização de outras atividades; (iv) impactos sobre a saúde e segurança humana; (v) o custo financeiro no emprego de habilidades específicas para reparar o dano; e (vi) a perda de imagem, reputação ou boa fé.

Mais detalhes sobre a identificação de consequências foram abordados na seção 2 deste texto.

6.1.2 Estimativa do Risco

A Estimativa do Risco é a última etapa da fase de análise do risco, e seu objetivo é atribuir valores para as probabilidades e consequências de cada risco, usando escalas qualitativas e (ou) quantitativas. O grau de detalhamento da estimativa pode ser amplamente variável, dependendo de:

a. quão críticos os ativos são para a organização;

b. qual a extensão de vulnerabilidades conhecidas;

c. o registro de incidentes prévios aos quais se tem acesso.

Segundo a ISO/IEC (2007), no início da gestão de riscos, a estimativa do risco deve ser de alto nível, para evitar demora excessiva na apreciação, que inicialmente compreende pelo menos duas iterações para obter resultados satisfatórios. A norma apresenta algumas estratégias sobre como começar a realizar abordagem de alto nível na estimativa dos riscos.

As atividades realizadas na estimativa envolvem:

a. estimativa das consequências;

b. avaliação da probabilidade de incidente;

c. estimativa do nível do risco.

Essas atividades são detalhadas a seguir.

6.1.2.1 Avaliação do Impacto de Incidentes (Estimativa das Consequências)

A Avaliação do Impacto de Incidentes (estimativa das consequências) recebe como entrada uma lista de cenários de incidente identificados como relevantes, incluindo identificação de ameaças, vulnerabilidades, ativos afetados, consequências para ativos e processos de negócio. O objetivo é avaliar o impacto sobre os negócios da organização que resultaria da ocorrência desses cenários de incidentes. Devem ser levadas em consideração as brechas de segurança, como perda de confidencialidade, integridade e disponibilidade. A saída do processo é uma lista de avaliações de impacto (consequências) apreciadas, decorrentes de um cenário de incidente, expressas com respeito a ativos e critérios de impacto.

São aspectos importantes que devem ser considerados na estimativa de consequências, conforme a 27005:

a. valorar todos os ativos no escopo e considerar o valor desses ativos quando estimando as consequências;

b. valorar impactos sobre os negócios de forma quantitativa ou qualitativa (valores monetários facilitam tomada de decisão);

c. ordenar os ativos quanto à criticidade, isto é, a importância dos ativos para alcance dos objetivos de negócios da organização;

d. analisar na ordem dos mais críticos para os menos críticos;

e. adotar algumas formas de valoração indicadas, dentre as quais são indicadas: (i) estimar qual o valor para substituir o ativo; (ii) estimar qual o custo de recuperação, depuração e substituição da informação perdida; (iii) estimar as consequências para o negócio devido à perda ou compromisso do ativo, devido à divulgação indevida, devido à modificação não autorizada, à indisponibilidade e à destruição;

f. realizar uma análise de impacto sobre negócios - BIA ({\it Business Impact Analysis});

g. considerar que incidentes podem afetar mais de um ativo;

h. modelar as consequências de um evento ou de uma série de eventos usando dados experimentais;

i. expressar consequências usando critérios de impacto em termos monetários, técnicos ou humanos, ou outros.

6.1.2.2 Estimativa da Probabilidade de Incidente

A Estimativa da Probabilidade de Incidentes, segundo a ISO 27705, recebe como entradas: (i) uma lista de cenários de incidente identificados como relevantes, incluindo identificação de ameaças, vulnerabilidades, ativos afetados, consequências para ativos e processos de negócio; e (ii) uma lista de todos os controles existentes e planejados, suas efetividades e *status* de implementação e uso.

O objetivo da atividade é avaliar a probabilidade de realização de cenários de incidentes. A saída dessa atividade é a lista das probabilidades de cenários de incidentes.

Alguns aspectos importantes devem ser considerados na estimativa de probabilidades, conforme a 27005:

a. a frequência com a qual as ameaças ocorrem;

b. quão fácil é, para as ameaças, explorarem as vulnerabilidades;

c. a experiência e estatísticas sobre probabilidade de ameaças;

Para ameaças de origem deliberadas, a norma recomenda observar:

a. motivações e capacidades;

b. mudanças ao longo do tempo;

c. recursos disponíveis aos atacantes;

d. percepção da atratividade e vulnerabilidade dos ativos para um atacante possível.

Para ameaças acidentais, a norma recomenda observar:

a. fatores geográficos;

b. proximidade a outras instalações;

c. condições meteorológicas extremas;

d. fatores que influenciam erro humano;

e. mau funcionamento de equipamentos;

6.1.2.3 Estimativa do Nível do Risco

A Estimativa do Nível do Risco recebe como entrada a lista de cenários de incidentes, com suas consequências relacionadas a ativos e processos de negócios, associados às probabilidades (qualitativas ou quantitativas). O objetivo da atividade é estimar o nível de risco para todos os cenários de incidentes relevantes. A saída da atividade é a lista de riscos com níveis de valoração atribuídos.

Durante a Estimativa do Nível do Risco, deve-se considerar antecipadamente os custos e benefícios do tratamento dos riscos e as preocupações dos intervenientes.

Para a realização da estimativa das consequências, probabilidades e nível do risco, podem ser usadas abordagens qualitativas, quantitativas ou mistas. A abordagem qualitativa é usualmente realizada, em primeiro lugar, para indicação geral do nível de risco e para revelar os maiores riscos. A abordagem quantitativa é mais complexa e custosa, e demora a produzir resultados satisfatoriamente precisos. Apenas os riscos de maior impacto podem ser estimados com maior detalhamento por meio de abordagem quantitativa. Independentemente da abordagem, as estimativas devem ser baseadas em informação factual e todos os dados disponíveis.

Detalhes sobre os métodos qualitativo e quantitativo são apresentados a seguir.

6.1.2.4 Métodos de Estimativa de Risco Qualitativos

Os métodos de estimativa qualitativos usam escalas nominais (qualificadoras) para descrever as magnitudes de consequências potenciais de um risco, bem como a probabilidade de materialização do risco. Há também, para métodos mais avançados, informação sobre o grau de incerteza ou de confiança relativamente às medições. Uma escala qualitativa ou nominal usa valores como: alta, média e baixa. Métodos qualitativos são fáceis de entender e empregar, mas são sujeitos à maior subjetividade quando comparados ao quantitativo.

Métodos qualitativos são recomendados, segundo a ISO/IEC (2007), para uso em atividades: (i) de varredura inicial para identificar necessidades de análise detalhada em casos específicos; (ii) quando apropriados, à tomada de decisão; (iii) quando dados numéricos ou recursos são inadequados para estimativa quantitativa, por exemplo, quando o valor dos ativos é intangível.

6.1.2.5 Métodos de Estimativa Quantitativa

Os métodos de estimativa quantitativa usam uma escala numérica tanto para estimar consequências quanto para estimar probabilidades, empregando dados de fontes diversas. A qualidade da análise quantitativa é dependente da validade dos modelos numéricos usados. Estimativas quantitativas dependem fortemente de dados históricos de incidentes e, dessa forma, podem ser relacionados diretamente aos objetivos e preocupações de segurança da organização.

Novos tipos de risco são difíceis de estimar pelo método quantitativo devido à falta de informações históricas. Na ausência de dados factuais ou auditáveis, os métodos quantitativos são frágeis, pois a precisão é ilusória. A incerteza e variabilidade das consequências e probabilidades estimadas numericamente devem ser consideradas e comunicadas efetivamente, pois os números facilitam a tomada de decisão; porém, se forem ilusoriamente precisos, podem causar mais problemas que soluções.

Os parágrafos seguintes demonstram um pequeno exemplo de emprego de método quantitativo, baseado no exposto em Harris (2005).

Estimativa Quantitativa das Consequências

Em métodos quantitativos, as consequências podem ser determinadas pelo fator de exposição ao risco (RE). RE (*Risk Exposure*) é a percentagem de perda que uma ameaça realizada incorre sobre um ativo específico.

Por exemplo, uma série de estudos efetuados por seguradoras americanas indicam que um incêndio típico em um *datacenter* provoca 25% de perda do valor do ativo, devido à indisponibilidade e perda de integridade.

Estimativa Quantitativa da Probabilidade de Incidente

Em métodos quantitativos, as probabilidades de ocorrência do incidente podem ser determinadas pelo índice de ocorrência anualizado - ARO (*Anualized Rate of Occurrence*). ARO é igual à frequência estimada da ameaça sendo realizada em um horizonte de um ano.

Por exemplo, suponha que dados históricos do Governo Inglês indicam que um incêndio ocorra a cada 10 anos num *datacenter*. Nesse caso, o ARO seria igual a 1 incidente a cada 10 anos = 0,1 = 10%.

Estimativa Quantitativa do Nível do Risco

Para estimativa quantitativa do nível do risco, é preciso determinar um valor monetário

para o ativo (AV - *asset value*). Como o *datacenter* aqui no Brasil custou R$ 5.000.000,00 para ser implantado, então AV = R$ 5.000.000,00.

Baseado nos números obtidos, se a estimativa de perda anual é dada pela determinação do fator SLE - *Single Loss Expectancy*[6], quanto haverá de perda, caso a ameaça seja realizada sobre o ativo vulnerável? A resposta é dada pela fórmula abaixo.

SLE = AV x RE = R$ 5.000.000,00 x 25% = R$ 1.250.000,00.

Recomendações para Tratamento

Conforme o exemplo de abordagem quantitativa apresentado, a organização em pauta deverá investir, no máximo, R$ 1.250.000,00, anualmente, para o combate a incêndio no *datacenter*. Perceba que a afirmação é válida se o incêndio afeta o *datacenter* apenas na forma identificada. As recomendações para tratamento são empregadas na fase de tratamento do risco.

6.2 Avaliação do Risco

Segundo a ISO/IEC (2007), o propósito da Avaliação do Risco é priorizar os riscos contra critérios de avaliação (definidos na Definição do Contexto) e objetivos relevantes para a organização. São entradas para a Avaliação do Risco:

a. lista de riscos com valorações de níveis;

b. critérios de avaliação de riscos (declarados na Definição do Contexto);

c. critérios de aceitação do risco (declarados na Definição do Contexto).

Uma vez que as entradas são recebidas, os níveis dos riscos valorados são comparados com os critérios de avaliação estabelecidos e os critérios de aceitação de riscos. A saída da atividade é uma lista de riscos priorizados, conforme critérios de avaliação, em relação aos cenários de incidente que levam a esses riscos.

São aspectos importantes que devem ser considerados na avaliação do risco, conforme a 27005:

a. as decisões serão apoiadas nos critérios estabelecidos durante a Definição do Contexto;

b. as decisões e o contexto devem ser revisitados com maior detalhamento, uma vez que mais informações são conhecidas sobre os riscos;

c. critérios de avaliação devem ser consistentes com os cenários de segurança da informação interno e externo;

d. critérios de avaliação devem considerar os objetivos da organização e as percepções dos intervenientes;

e. decisões são principalmente baseadas no nível de risco aceitável (tolerável);

f. agregações de múltiplos riscos de menor escala podem resultar em riscos mais elevados do que o real;

g. deve-se observar atentamente a relevância dos critérios, pois: (i) alguns objetivos de segurança da informação podem ser irrelevantes para uma organização. Ex: confidencialidade; (ii) Processos de pouca importância para a organização terão seus riscos associados avaliados com menor consideração; (iii) Observar aspectos legais, regulatórios e contratuais, em adição aos riscos estimados.

A Avaliação do Risco conclui a fase de Apreciação. Ao final da Avaliação, os riscos foram identificados, estimados e avaliados, e produziu-se uma lista de riscos priorizados conforme critérios previamente estabelecidos.

Se a Apreciação do Risco não produz resultados satisfatórios, deve-se retornar à fase de Definição do Contexto, para refinamentos e nova análise e avaliação. Caso a Apreciação produza resultados satisfatórios, deve-se passar à fase de Tratamento do Risco.

6 Expectativa de perda em um evento isolado.

7 Tratamento dos Riscos

O Tratamento do Risco é a fase da gestão de riscos que envolve a decisão entre reter, evitar, transferir (compartilhar) ou reduzir os riscos. A entrada para o Tratamento dos Riscos é uma lista de riscos priorizados conforme critérios de avaliação em relação aos cenários de incidente que levaram a tais riscos. Os objetivos a serem alcançados com o tratamento dos riscos são:

a. a definição de quais controles serão empregados para reduzir alguns destes riscos;

b. a retenção ou aceitação de outros riscos;

c. a ação de evitar outros riscos;

d. a transferência de alguns desses riscos a outros agentes; e

e. a definição de um *plano de tratamento do risco*.

As saídas da fase de tratamento são (i) o plano de tratamento do risco e (ii) a lista de riscos residuais, ambos sujeitos à decisão de aceitação pelos altos gestores da organização.

A Figura 6 apresenta um fluxograma básico da atividade de tratamento do risco.

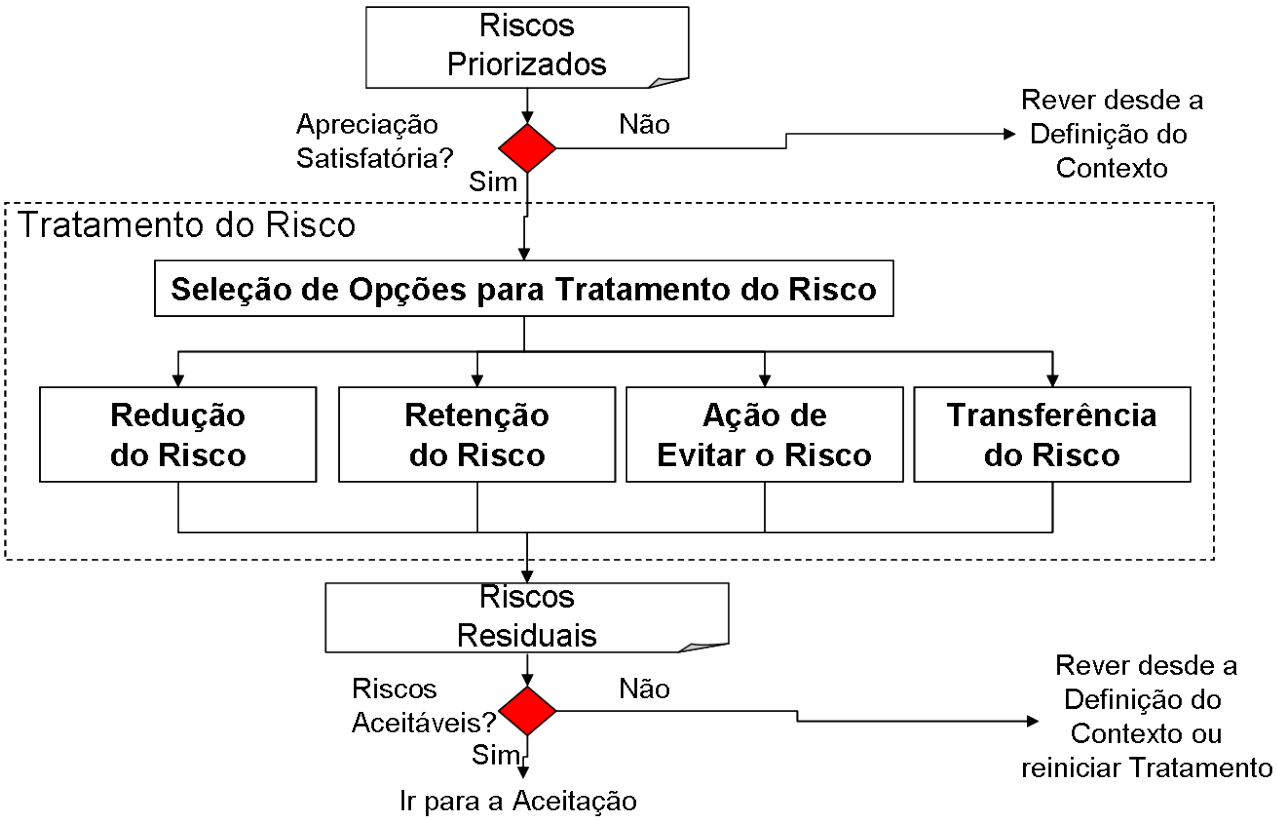

Figura 6 – Fluxograma do tratamento do risco. Fonte: Adaptado de ISO/IEC (2007).

São aspectos gerais que devem ser considerados no tratamento do risco, conforme a ISO/IEC (2007):

a. as opções devem ser selecionadas baseadas em três aspectos: (i) nos resultados da apreciação do risco; (ii) no custo esperado para implementar as opções; e (iii) nos benefícios esperados com as opções;

b. quando largas reduções de risco podem ser obtidas com poucas despesas, essas opções devem ser implementadas. Outras opções de tratamento dependem de julgamento melhor exercitado;

c. as consequências adversas de riscos devem ser reduzidas a níveis mínimos, até quando isso for prático;

d. os riscos raros e severos devem ser cuidadosamente considerados pelos gestores. Nesses casos, podem ser necessários controles custosos, que não são economicamente justificados (ex: relativos à continuidade de negócios);

e. as opções para tratamento não são mutuamente exclusivas. Uma combinação de opções pode ser praticável;

f. alguns tratamentos reduzem mais de um risco (ex: treinamentos).

Guias de implementação para cada uma das opções são apresentados a seguir.

7.1 Um Guia Rápido para Redução do Risco

A Redução do Risco consiste em tomar ações "para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco" (ABNT, 2005). A redução envolve a adoção de controles. É também chamada de mitigação.

7.1.1 Um catálogo de controles

A ISO/IEC 27002:2005, também conhecida como ISO/IEC 17799:2005, apresenta um guia para implementação de controles de segurança da informação, agrupados por objetivo de controle, num total de 39 objetivos. Estes objetivos de controle e controles são enunciados no Anexo A na ISO/IEC 27001:2006. As seções da norma 27002:2005 e a quantidade de objetivos de controle e controles (133 controles ao total), cuja implementação é descrita em cada seção, são enumerados a seguir:

a. seção 5 - Política de Segurança da Informação (1 objetivo de controle - 2 controles)

b. seção 6 - Organizando a Segurança da Informação (2 objetivos de controle - 11 controles)

c. seção 7 - Gestão de Ativos (2 objetivos de controle - 5 controles)

d. seção 8 - Segurança em Recursos Humanos (3 objetivos de controle - 9 controles)

e. seção 9 - Segurança Física e do Ambiente (2 objetivos de controle - 13 controles)

f. seção 10 - Gestão das Operações e Comunicações (10 objetivos de controle - 32 controles)

g. seção 11 - Controle de Acesso (7 objetivos de controle - 25 controles)

h. seção 12 - Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (6 objetivos de controle - 16 controles)

i. seção 13 - Gestão de Incidentes de Segurança da Informação (2 objetivos de controle - 5 controles)

j. seção 14 - Gestão da Continuidade do Negócio (1 objetivo de controle - 5 controles)

k. seção 15 - Conformidade (3 objetivos de controle - 10 controles)

A publicação inicial desses controles pelo órgão de padronização britânico, em meados da década de 1990, é reconhecida como uma grande contribuição à uniformização das práticas de gestão da segurança da informação em todo o mundo.

7.1.2 Seleção de controles

São aspectos que devem ser considerados para redução do risco, conforme a 27005:

a. controles apropriados e justificados devem ser selecionados;

b. aspectos normativos e contratuais devem ser considerados quando da aceitação dos riscos;

c. o custo, o tempo e os aspectos técnicos, ambientais e culturais relacionados à seleção do controle devem ser considerados;

d. usualmente, o TCO (custo total de apropriação ou *total cost of ownership*) de um sistema é reduzido por meio da adoção de controles propriamente selecionados;

7.1.3 Efeitos de controles

Os efeitos de um controle podem ser (ISO/IEC, 2007):

e. prevenção;

f. conscientização;

g. monitoramento;

h. detecção;

i. detenção;

j. eliminação;

k. correção;

l. minimização de impacto e

m. recuperação.

Um controle pode exercer um ou mais desses efeitos.

7.1.4 Investimentos, oportunidades e controles

Controles necessitam de investimentos da capital e custeio para:

a. aquisição;

b. implementação (colocar em funcionamento);

c. planejamento;

d. operação;

e. monitoramento; e

f. manutenção;

Uma vez que algumas habilidades especiais podem ser necessárias para definir e implementar os controles ou modificar os existentes, antes de se decidir pela adoção de controles deve-se comparar os custos dos controles em função dos custos dos ativos protegidos, bem como se deve realizar estimativa de oportunidades de investimentos, isto é, quais investimentos em controles permitem reduzir o risco e que novas oportunidades de negócios podem ser possíveis com esses investimentos.

7.1.5 Restrições na seleção de controles

Deve-se considerar que existem restrições durante a seleção de controles, relacionadas ao:

a. tempo para implementar *versus* a janela de oportunidade ou necessidade;
b. custo financeiro para implementar;
c. técnicas necessárias para implementar;
d. aspectos operacionais do controle no interior da organização;
e. aspectos culturais vinculados à adoção do controle;
f. aspectos éticos vinculados à adoção do controle;
g. aspectos ambientais vinculados à adoção do controle;
h. aspectos jurídico-legais vinculados à adoção do controle;
i. facilidade de uso do controle;
j. restrições de pessoal no uso do controle; e
k. restrições de integração com controles novos e existentes.

Em suma, a elaboração de um plano de redução de riscos é uma atividade que articula diversos elementos do nível humano, operacional, tático e estratégico organizacional.

7.2 Guia Rápido de Retenção do Risco

A Retenção do Risco é a decisão de reter ou aceitar o risco sem ações subsequentes. Deve-se, no entanto, evitar uso da palavra aceitar o risco, para evitar confusão com a fase de Aceitação do Risco, que envolve aceitar o plano de tratamento do risco.

Para retenção do risco, deve-se considerar que, se os níveis de risco são compatíveis com os critérios de aceitação do risco, não há necessidade de implementar mais controles. Nesse caso, o risco deve ser retido. O registro do risco retido permite o seu monitoramento futuro, uma vez que mudanças no ambiente organizacional podem modificar o perfil do risco.

O fluxograma da Figura 7 apresenta um critério para retenção de riscos provocados por agentes de ameaça intencional. Este modelo é proposto pela Norma NIST 800-100.

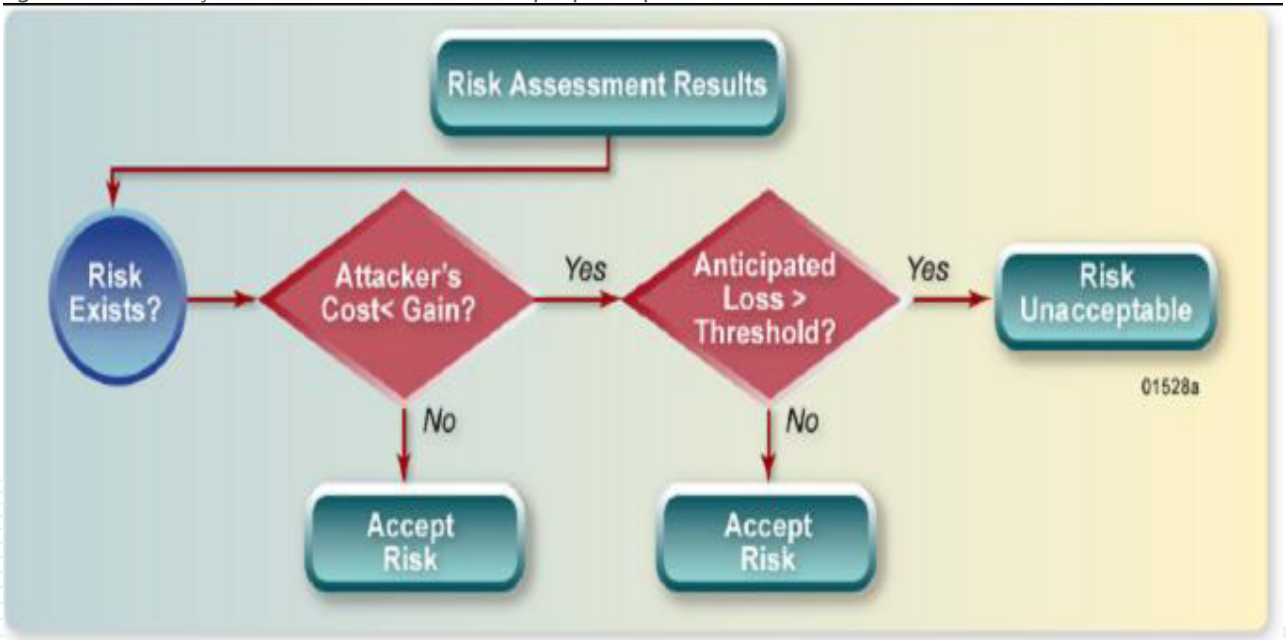

Figura 7. Critério para retenção do risco com agentes de ameaça intencionais.
Fonte: (NIST).

Conforme o fluxograma da Figura 7, se o custo do atacante é menor que o ganho que ele pode ter, e, adicionalmente, se a perda estimada é maior que um limite de tolerância indicado, então o risco é inaceitável. Caso contrário, o risco é retido (aceito). O fluxograma descreve um critério para aceitação do risco que tem como um de seus fatores um agente de ameaça intencional.

7.3 Ação de Evitar o Risco

Na ação de evitar o risco, a atividade, condição, ação ou processo que permite a existência do risco deve ser evitada. A organização abstém-se de realizá-la.

Uma decisão de evitar o risco completamente pode ser tomada quando os riscos são excessivamente elevados ou os custos de implementação de outras opções excedem os benefícios. Nesse caso, a organização se recusa a executar atividades planejadas ou existentes, ou muda as condições sobre as quais a atividade é executada.

Por exemplo, para riscos de causas naturais, o mais efetivo pode ser mudar-se para um local onde o risco não existe ou está sob controle.

7.4 Transferência do Risco

A "transferência do risco é o compartilhamento com uma outra entidade do ônus da perda ou do benefício do ganho associado a um risco" (ABNT, 2004).

Na transferência do risco, os riscos são transferidos para outro parceiro, que é mais efetivo em controlar esse tipo particular de risco. A transferência de riscos envolve a decisão de compartilhar certos riscos com parceiros externos. A transferência pode introduzir novos riscos ou modificar os riscos existentes e (ou) identificados e, dessa forma, pode ser necessário tratar riscos adicionais.

Transferência pode ser feita por meio da contratação de seguros ou subcontratação de um parceiro especializado em monitorar o sistema e adotar ações para parar um ataque antes que ele alcance níveis de dano elevados.

A transferência usualmente transfere a responsabilidade gerencial pelo risco, mas não a responsabilidade jurídica ou contratual pelos impactos. O cliente possivelmente continuará a atribuir à organização a culpa pelas falhas e impactos adversos.

8 Aceitação do Risco

A Aceitação do Risco é a fase da gestão de riscos que compreende o registro formal da decisão pelo aceite dos riscos residuais existentes na organização. Essa decisão é tomada pelo gestor responsável pelo escopo de risco.

As entradas para a aceitação do risco são: (i) o *plano de tratamento de riscos*, sujeito à aprovação; e (ii) a *avaliação de riscos residuais*, sujeitos à aprovação.

O objetivo da aceitação do risco é efetuar a decisão e formalmente registrar a aceitação dos riscos e responsabilidades pela decisão. A saída da atividade é a *lista de riscos aceitos*, à qual estão associadas justificativas para aceitação daqueles que não se coadunam com os critérios normais de aceitação de risco da organização.

São aspectos que devem ser considerados para a aceitação do risco, conforme ISO/IEC (2007):

a. planos de tratamento de risco devem descrever como riscos apreciados devem ser tratados. É importante que os gestores responsáveis revisem e aprovem os planos propostos e riscos residuais resultantes;

b. é importante que as decisões e condições de aprovação sejam formalmente registradas;

c. Em alguns casos, os riscos residuais não atendem a critérios que foram parcialmente estabelecidos, bem como não atendem às condições de contorno do problema. No último caso, o gestor pode incluir uma justificativa da decisão de sobrepor critérios.

Por fim, deve-se ter claro que os critérios de aceitação do risco podem ser bem mais complexos que a simples comparação entre níveis de gatilho estabelecidos. Dessa forma, a aceitação pode depender de julgamento subjetivo e tornar-se algo demorado.

9 Comunicação do Risco

A Comunicação do Risco é um conjunto de atividades continuamente executadas e que envolve a troca de informações sobre riscos entre os tomadores de decisão e todos os envolvidos na organização. O objetivo da comunicação é fazer com que as informações sejam trocadas ou compartilhadas entre tomadores de decisão e outros intervenientes.

As entradas para a Comunicação do Risco são todas as informações sobre riscos obtidas a partir das atividades de GRSI. O resultado da atividade é a compreensão mútua e contínua do processo de GRSI e seus resultados, com o alcance de acordos sobre como gerenciar riscos.

As principais informações compartilhadas acerca do risco envolvem:

a. existência do risco;

b. natureza do risco;

c. forma do risco;

d. probabilidade do risco;

e. severidade do risco;

f. tratamento do risco; e

g. critérios para aceitação do risco.

Segundo ISO/IEC (2007), as percepções de risco variam muito de pessoa para pessoa, pois suposições, formação, conceitos, necessidades e preocupações variam de pessoa para pessoa, e é necessário identificar, documentar e considerar *claramente* tais percepções e raciocínios. Desse modo, a comunicação do risco é bidirecional e mantê-la dessa forma é importante, pois pode impactar severamente a tomada de decisões e contribuir para que as corretas sejam tomadas. Pode-se formar comitês de debate durante a priorização e tratamento apropriado dos riscos.

Segundo ISO/IEC (2007), a comunicação de riscos facilita:

a. a garantia dos resultados da GRSI;

b. a coleta de informações sobre riscos;

c. o compartilhamento de resultados da avaliação de riscos e do plano de tratamento de riscos;

d. a compreensão mútua que elimina ou reduz a ocorrência e consequências de brechas de segurança;

e. o processo de tomada de decisões;

f. o fluxo de conhecimentos sobre segurança da informação;

g. a coordenação com outros parceiros e o desenvolvimento de respostas aos planos quando da ocorrência de incidentes;

h. a formação de senso de responsabilidade acerca de riscos entre tomadores de decisão e intervenientes;

i. a melhor conscientização.

Diferentes planos de comunicação do risco devem ser desenvolvidos para os casos de operação da organização sob condições normais e quando a mesma está operando em modo de emergência ou crise. É importante, sobretudo, estabelecer um canal de informações sobre riscos com a área de relações públicas da organização, especialmente durante emergências ou crises.

Por fim, na opinião do autor, negligenciar a correta comunicação dos riscos reduz sensivelmente a eficácia da gestão de riscos. Um plano de gestão de riscos guardado a "sete chaves", cujos elementos são conhecidos exclusivamente pela gestão da segurança, não conduz à melhoria da segurança.

10 Monitoramento e Revisão do Risco

Monitoramento e Revisão do Risco é o nome dado a um conjunto de atividades continuamente executadas e que envolve o monitoramento dos diversos fatores de caracterização do risco, a fim de identificar quaisquer mudanças no contexto da organização, atualizar o panorama de riscos da organização e aprimorar o processo de gestão de riscos da organização.

O Monitoramento e Revisão do Risco, segundo a ISO/IEC (2007), é dividido em dois subprocessos:

a. monitoramento e Revisão dos Fatores de Risco;

b. monitoramento, Revisão e Melhoria da Gestão de Riscos.

Esses subprocessos são detalhados a seguir.

10.1 Monitoramento e Revisão dos Fatores de Risco

O Monitoramento e Revisão dos Fatores de Risco recebe como entradas todas as informações originadas das atividades de GRSI. O objetivo é o monitoramento e revisão dos riscos e seus fatores (valoração dos ativos, impactos, ameaças, vulnerabilidades e probabilidades), a fim de identificar qualquer início de *mudanças significativas* no contexto organizacional.

Durante o monitoramento e revisão dos fatores de risco deve-se observar que:

a. riscos não estáticos;

b. mudanças abruptas podem ocorrer sem indicação aparente e exigem contínuo monitoramento;

c. a contratação de serviços externos pode auxiliar no monitoramento desses fatores;

d. a organização deve rever todos os riscos regularmente, especialmente quando grandes mudanças ocorrem nos ambientes interno e (ou) externo.

Destacam-se entre os principais aspectos a serem monitorados, segundo ISO/IEC (2007):

a. novos ativos que foram incluídos no escopo;

b. modificações nos valores dos ativos devido a, por exemplo, mudanças em negócios;

c. novas ameaças que passaram a existir interna e (ou) externamente;

d. possibilidade de novas ameaças explorarem vulnerabilidades novas ou que aumentaram;

e. aumento do impacto ou de consequências em ameaças, vulnerabilidades e riscos, quando apreciados de forma agregada;

f. incidentes de segurança da informação.

O resultado do monitoramento e revisão dos fatores de risco é o alinhamento contínuo entre a gestão de riscos e os objetivos de negócios, dentro dos critérios de risco estabelecidos (ISO/IEC, 2007).

10.2 Monitoramento, Revisão e Melhoria da Gestão de Riscos

O Monitoramento, revisão e melhoria da gestão de riscos recebe como entradas todas as informações originadas das atividades de GRSI. O objetivo é fazer com que o *processo* de GRSI,

cujo modelo é descrito nas seções 5 a 10 dessa monografia, seja continuamente monitorado, revisto e melhorado, quando necessário e apropriado.

O monitoramento, revisão e melhoria da gestão de riscos deve-se garantir que:

a. o processo de GRSI é apropriado e seguido;

b. os riscos são realistas;

c. a gestão de riscos tem capacidade de responder aos riscos;

d. os critérios de medição de riscos aderem aos objetivos de negócios, estratégias e políticas.

São aspectos específicos a serem monitorados e revisados de forma contínua e periódica, para a melhoria do processo de gestão de riscos de segurança da informação, segundo a ISO/IEC (2007):

a. contexto jurídico e ambiental;

b. contexto da competição;

c. abordagem de avaliação de risco;

d. valores e categorias de ativos;

e. critérios de impacto;

f. critérios de avaliação de riscos;

g. critérios de aceitação de riscos;

h. TCO - custo total de apropriação ou propriedade;

i. recursos necessários à GRSI.

Conforme a 27005, as modificações da abordagem, metodologia e ferramentas usadas na GRSI dependem principalmente das:

a. necessidades de mudança identificadas durante a prática efetiva;

b. de qual é a iteração para apreciação do risco que está sendo realizada;

c. das mudanças nas motivações para estabelecimento da GRSI

d. de mudanças no escopo ou objeto da GRSI.

Dentre as distintas motivações para estabelecer GRSI numa organização, destacam-se demandas para:

a. continuidade de negócios;

b. conformidade; ou

c. resiliência da organização a incidentes;

Acerca de mudanças no escopo ou objeto da GRSI, estas podem se referir a mudanças:

a. na organização;

b. numa unidade de negócios dentro da organização;

c. no processo de tratamento da informação;

d. na implementação técnica do processo;

e. de aplicativo; e

f. de conexão à Internet.

O resultado do emprego do monitoramento é que o processo de GRSI se mantém atualizado e continuamente relevante para o cumprimento dos objetivos de negócio da organização. De outra forma, sem o monitoramento, o processo de GRSI tornar-se-á fatalmente obsoleto e de pouca utilidade.

11 Introduzindo a Gestão de Riscos em Organizações

Como já discutido anteriormente, o processo da ISO 27005 já descrito anteriormente apresenta grande similaridade com a norma AS/NZS 4360. As principais diferenças entre as normas residem no fato de que a AS/NZS 4360:

a. aborda a gestão de riscos positivos e negativos, simultaneamente;

b. é uma norma mais antiga, curta, simplificada e abstrata que a ISO/IEC 27005:2008;

c. enfatiza a importância da comunicação e da consulta junto aos vários intervenientes no início do processo de gestão de riscos; e

d. subdivide a análise do contexto organizacional em externo e interno.

Além das diferenças de processo acima sumarizadas, a AS/NZS 4360 apresenta uma breve descrição de um processo para estabelecer a gerência de riscos efetiva numa organização, o qual é baseado: (i) na avaliação de práticas de gestão de riscos existentes e necessárias e (ii) no planejamento da gestão de riscos. A norma também propõe o estabelecimento de sistemas de informação para a gestão de riscos.

Um modelo de planejamento da gestão de riscos e os elementos presentes em sistemas de informação para a gestão de riscos são brevemente sumarizados a seguir, com a intenção de apresentá-los e apontar oportunidades para desenvolvimento de trabalhos de ordem prática relacionados à gestão de riscos.

11.1 O Planejamento da Gestão de Riscos

Segundo a Standards Australia and Standards New Zealand (2004), o planejamento da gestão de riscos deve observar o cumprimento dos seguintes aspectos:

a. [Desenvolvimento de planos de gestão de riscos] que definem como a gestão de riscos deve ser conduzida por meio da organização. É importante destacar que todas as práticas e processos importantes na organização devem ser incorporados à gestão de riscos, especialmente durante: (i) o desenvolvimento de políticas; (ii) o planejamento estratégico e de negócios e (iii) a gestão de mudanças, (iv) a gestão de ativos; (v) a auditoria; (vi) a continuidade de negócios; (v) a gestão ambiental; (vi) o controle de fraudes; (vii) os recursos humanos; (viii) os investimentos e (ix) a gestão de projetos. Planos para tais incorporações devem ser elaborados e organizados;

b. [Garantia de suporte da alta gestão] por meio de um compromisso para com a gestão de riscos que deve ser alcançado por meio de: (i) obtenção de suporte ativo e contínuo por parte de diretores e executivos seniores, para desenvolvimento e implementação de políticas e planos de gestão de riscos; (ii) indicação de um indivíduo ou grupo de alto respaldo organizacional para conduzir o processo; além de (iii) obtenção de suporte por parte de toda a alta gestão, para execução dos planos;

c. [Desenvolvimento e comunicação de uma política de gestão de riscos], onde os executivos devem definir, documentar e se comprometer com uma política para gestão de riscos, que: (i) seja satisfatoriamente justificada; (ii) esteja relacionada com a política e planos estratégicos da organização; (iii) descreva a extensão e os tipos de riscos que a organização assumirá, com o alcance de equilíbrio entre ameaças e oportunidades; (iv) descreva o processo a ser usado para gerenciar os riscos; (v) indique como será contabilizada a gestão de alguns riscos específicos; (vi) detalhe o suporte e os conhecimentos disponíveis para apoiar aqueles responsáveis pela gestão de riscos; (vii) declare como o desempenho da gestão de riscos será medido e relatado; (viii) apresentação de um compromisso para a

revisão periódica do sistema de gestão de riscos; e (ix) declare o compromisso dos diretores e executivos;

d. [Estabelecimento de contabilização e autoridade], onde a gestão de riscos é responsabilidade, em última instância, da alta gestão. O pessoal responsável por cada área de controle tem responsabilidades pelos riscos a ela pertinentes. Devem ser especificados os responsáveis pela gestão, implementação e manutenção dos controles em cada área. Indicadores de desempenho e mecanismos de relato da gestão de riscos precisam ser criados. Níveis de reconhecimento, recompensa, aprovação e sanção devem ser estabelecidos.

e. [Customização do processo de gestão de riscos], onde o processo deve ser alinhado às características da organização, às suas políticas e à sua cultura, em contínua mudança.

f. [Garantia de recursos adequados], que envolve a identificação dos recursos necessários e suficientes para a gestão de riscos, abrangendo: pessoal e habilidades; processos e procedimentos documentados; sistemas de informação e bancos de dados; dinheiro e outros recursos para desempenho de atividades.

11.2 Sistemas de Informação para a Gestão de Riscos

A Gestão de Riscos é uma atividade que manipula um imenso volume de informação. Faz-se necessário empregar sistemas de informação, especialmente os automatizados por software, para oferecer suporte à atividade. Conforme a norma AS/NZS 4630, sistemas de informação para gestão de riscos devem possuir capacidade para:

a. registrar detalhes de riscos, controles e prioridades, bem como as mudanças nesses elementos;

b. registrar tratamentos de risco e necessidades de recursos associadas;

c. registrar detalhes de incidentes, eventos de perda e lições aprendidas;

d. rastrear a contabilização dos riscos, controles e tratamentos;

e. rastrear o progresso e registrar o cumprimento das ações de tratamento;

f. medir o progresso dos planos de gestão de risco;

g. monitorar o disparo de gatilhos; e

h. realizar auditorias.

12 Conclusões

Este texto apresentou uma introdução à gênese, conceitos e processos de gestão de riscos de segurança, com foco na perspectiva da norma ISO/IEC 27005:2008. O processo de gestão de riscos de segurança da informação é o cerne de qualquer ação bem-sucedida de Gestão da Segurança da Informação, e sua adoção, conforme o modelo da 27005, permite a construção de uma abordagem eficaz na organização, onde a comunicação, monitoramento e melhoria contínua garantem que a GRSI continuará a atender às necessidades da organização no curto, médio e longo prazo.

A 27005 não é uma metodologia, mas sua descrição apresenta uma quantidade suficiente de detalhes para permitir a construção de metodologias e ferramentas adequadas à gestão de riscos em organizações de pequeno, médio e grande porte.

Por fim, é importante destacar princípios para uso da gestão de riscos na gestão da segurança da informação, que são os seguintes:

a. o alcance da segurança da informação em uma organização compreende, de forma geral, a implementação de controles de segurança;

b. qualquer controle custa caro para ser implementado, de modo que não há como implementar todos os controles possíveis, sob pena de conduzir uma organização à falência e à inoperância;

c. é necessário tomar uma decisão racional sobre quais controles de segurança serão implementados. Tal decisão deve ser baseada em métodos qualitativos ou quantitativos que, a partir do traçado do perfil de riscos de uma organização, orientam a implementação de um conjunto de controles em detrimento de outros.

d. a eventual implementação dos controles de segurança planejados modifica o próprio perfil de riscos da organização, fazendo com que seja necessário reavaliar periodicamente os riscos que levaram à atual configuração de controles de segurança. O desafio para a organização é gerenciar seus riscos de forma contínua, custo-efetiva e sustentável.

O conhecimento produzido durante a gestão de riscos aumenta a consciência situacional e o *sense-making*[7] organizacional.

7 De acordo com o link http://en.wikipedia.org/wiki/Sensemaking, sense-making é um processo através do qual as pessoas dão significado às suas experiências. Conforme Karl E. Weick, em *Sensemaking in Organizations*, Sage Publications: USA. 1995, "Sense-making é testado ao extremo quando pessoas encontram um evento cuja ocorrência é tão implausível que elas hesitam em relatá-las por medo de não serem acreditadas."

Referências

ASIS. *General Security Risk Assessment guideline*. Disponível em: <http://www.asisonline.org/guidelines/guidelinesgsra.pdf>. Acesso em: julho de 2008.

ABNT. *ABNT ISO/IEC GUIA 73:2005*. [S.l.], 2005.

ABNT. *Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 27002:2005*. 2a. ed. Rio de Janeiro, 2005.

ABNT. *Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos: ABNT NBR ISO/IEC 27001:2006*. 1a. ed. Rio de Janeiro, 2006.

BOWEN, P.; HASH, J.; WILSON, M. *NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers*. [S.l.], October 2006. Disponível em: <http://csrc.nist.gov/publications/PubsSPs% -.html>. Acesso em: agosto de 2010.

BS. *B. S. Information Security Management Systems (BS 7799-3-2006): Part 3: guidelines for information security risk management*. 2006.

COSO: Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management Framework: Exposure Draft for Public Comment*. [S.l.], 2004. 152 p. Disponível em: <http://www.erm.coso.org>. Acesso em: fevereiro de 2009.

CNSS, C. on N. S. S. *National Information Assurance Training Standard For Risk Analysts*. [S.l.], November 2005. 38 p. Disponível em: <http://www.cnss.gov/instructions.html>. Acesso em: Agosto de 2008.

FERNANDEZ, A.; SCHAUER, H. ISO27005 Gestion de risque. [S.l.], 2007. Disponível em: <http://www.hsc.fr/index.html.en>. Acesso em: fevereiro de 2009.

ISO/IEC. *ISO/IEC 13335-1:2004 - Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*. [S.l.], 2004.

ISO/IEC. *ISO/IEC FDIS 27005 - Information technology - Security Techniques - Information security risk management*. [S.l.], 2007.

ISO/IEC. *ISO/IEC 31000:2009 - Risk management – Principles and guidelines*. [S.l.], 2009.

MEULBROEK, L. K. *Integrated Risk Management for the Firm: A Senior Manager's Guide*. Soldiers Field Road. Boston, MA 02163, 2002.

NIST. FIPS PUB 200: *Minimum Security Requirements for Federal Information and Information Systems*. [S.l.], March 2006. 17 p. Disponível em: <"http://csrc.nist.gov/">. Acesso em: fevereiro de 2009.

PELTIER, T. R. *Information security risk analysis*. Boca Raton: Auerbach Publications, 2001.

Standards Australia and Standards New Zealand. *AS/NZS 4360:2004 - Australia/New Zealand Standard for Risk Management*. [S.l.], 2004.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. *NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems*. [S.l.], July 2002. 55 p. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. Acesso em: julho de 2009.