UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE ESPECIALIZAÇÃO EM TECNOLOGIAS, GERÊNCIA E SEGURANÇA DE REDES DE COMPUTADORES

ADMILSON GONÇALVES JÚNIOR

Metodologias de Gerenciamento de Riscos em Sistemas de Tecnologia da Informação e Comunicação – abordagem prática para conscientização e implantação nas organizações

Trabalho de Conclusão apresentado como requisito parcial para a obtenção do grau de Especialista

Prof. Dr. Raul Fernando Weber
Orientador

Prof. Dr. Sérgio Luis Cechin
Prof. Dr. Luciano Paschoal Gaspary
Coordenadores do Curso

Porto Alegre, dezembro de 2008.

AGRADECIMENTOS

Agradeço acima de tudo a Deus que, com sua infinita misericórdia, permitiu a realização desta obra. Agradeço, com carinho, a minha esposa Eloisa Cláudia por ter permanecido sempre ao meu lado e por suas orações, e aos meus filhos, Isaías e Isadora, que, com sabedoria e paciência, souberam esperar o papai. Por fim, agradeço à empresa TMSA - Tecnologia em Movimentação, em especial aos seus diretores e colaboradores, cuja oportunidade e crédito foram fundamentais para a conclusão deste trabalho.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

BCM	Business Continuity Management
BIA	Business Impact Analysis
COBIT	Control Objectives for Information and Related Technology
IBGC	Instituto Brasileiro de Governança Corporativa
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ITC	Information Technology and Communication
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
MOF	Microsoft Operations Framework
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
OGC	Office of Government Commerce
TIC	Tecnologia da Informação e Comunicação

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Este artigo tem o objetivo de demonstrar de forma prática e aplicável metodologias de gerenciamento de riscos e como seus processos são úteis para que uma organização tenha condições de estimar, tratar e avaliar os riscos que porventura possam afetar seus negócios. Este documento visa organizar, de maneira objetiva, boas práticas de gerenciamento de riscos, normas, padrões, exemplos de controles, vulnerabilidades, ameaças e referências que podem ser utilizadas na condução do processo de gerenciamento de risco.

As organizações têm demonstrado maior conscientização em relação ao importante papel que a tecnologia da informação e comunicação (TIC) desempenha para o cumprimento dos objetivos do negócio. Além disso, as leis de proteção de privacidade, obrigações financeiras e a Governança Corporativa têm exigido que as organizações gerenciem suas infra-estruturas de TIC com a cautela e a eficácia nunca antes vistas, de forma a não colocar em risco a si próprias, seus sócios, colaboradores, clientes, fornecedores e sociedade, através do não cumprimento de responsabilidades legais e contratuais.

Gerenciar a segurança de suas infra-estruturas, bem como o valor comercial que geram tem se mostrado o principal desafio dos departamentos de TIC. Entretanto, as atuais infra-estruturas de TIC apresentam altos níveis de integração e compartilham ambientes cada vez mais hostis, que exigem respostas rápidas e precisas diante de incidentes que podem importar risco de danos às empresas. Na maioria das vezes, as organizações não estão preparadas o suficiente para reagir com efetividade às ameaças, em outras palavras, no tempo hábil para evitar que seus negócios sejam prejudicados.

Caracterizada pela preservação da confidencialidade, integridade e disponibilidade da informação, a segurança da informação protege os principais ativos de uma organização visando à continuidade, a minimização dos danos e maximização das oportunidades e investimentos do negócio.

A principal fonte que uma organização tem para identificar seus requisitos de segurança é derivada da avaliação de riscos, que é parte do processo geral e contínuo de gerenciamento de riscos, cuja finalidade é reduzir riscos a níveis aceitáveis pela organização.

Palavras-Chave: gerenciamento de risco, segurança da informação, governança corporativa, governança de tecnologia da informação e comunicação.

Risks Management Methodologies for Information Technology and Communication Systems - practical approach for awareness and implementation in the organizations

ABSTRACT

This article has the purpose to evidence of practical and applicable way a risks management methodologies and how its processes are useful to an organization to assess, to mitigate and to evaluate the risks that can affect your businesses. This document intent organize best practices of risks management, including norms, patterns examples of controls, vulnerabilities, threats and references that can be used in the implementation of management of risk process.

The organizations have been concerned about important role of the information technology and communication (ITC) to accomplish the business-oriented objectives. Moreover, the privacy protection laws, financial obligations and the Corporative Governance have demanded that the organizations manage its ITC infrastructures with the caution and the effectiveness never before seen, in order to not place at risk itself, partners, collaborators, customers, suppliers and society, through not accomplishment of legal and contractual responsibilities.

Manage infrastructures security and the associated commercial values have become the main challenge of the ITC departments. However, the high levels of integration and the sharing of aggressive environments of current ITC infrastructures require fast and necessary incidents response that can import risk of damages to the companies. Most of the time, the organizations are not sufficiently prepared to react with effectiveness against the threats, in other words, in the skillful time to prevent that its businesses are injured.

Characterized for the preservation of information confidentiality, integrity and availability, the information security protects the organization assets aiming at to the continuity, reducing damages and increasing the business investments and opportunities.

The main source that an organization has to identify security requirements is derived from the risks assessment, which is part of general and continuous risks management process, whose purpose is to reduce risks the acceptable levels for the organization.

Keywords: risk management, information security, corporative governance, information technology and communication governance.

1 INTRODUÇÃO

1.1 Segurança da Informação

A informação é um ativo que, como qualquer outro relevante para o negócio, tem um valor para a organização e necessita ser adequadamente protegido. Além disso, as dependências dos sistemas de informação e serviços, as tendências e evoluções tecnológicas da computação distribuída, as interconexões de redes públicas e privadas e o compartilhamento de recursos expõem as organizações às mais variadas fontes de ameaças: fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo, inundação, *blackouts*, códigos maliciosos, *hackers*, ataques de DDoS, entre outras (ABNT, 2005)

A segurança da informação protege a informação contra ameaças no intuito de garantir a continuidade, minimizar os danos e maximizar os investimentos e oportunidades do negócio. A segurança da informação é obtida pela utilização de controles: políticas, práticas, procedimento, estruturas organizacionais e infra-estruturas de hardware e software. É caracterizada pela preservação da confidencialidade, integridade e disponibilidade da informação, e visa preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização (ABNT, 2005).

Existem três fontes principais para que uma organização identifique seus requisitos de segurança. A primeira é o conjunto de princípios, objetivos e necessidades para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações. A segunda é a legislação vigente, os estatutos, as regulamentações e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender. As duas anteriores são utilizadas como referências para desenvolver a principal fonte de requisitos de segurança, que é derivada da avaliação de riscos, processo responsável por identificar as ameaças aos ativos, as vulnerabilidades com suas respectivas probabilidades de ocorrência e os impactos ao negócio (ABNT, 2005).

1.2 Gestão de Riscos e Governança de TIC

A governança de TIC, responsabilidade da alta direção, é parte integrante da governança corporativa. Consiste de estruturas organizacionais e de lideranças e de processos que asseguram a sustentação das estratégias e objetivos da empresa através da infra-estrutura tecnológica (GULDENTOPS, 2003).

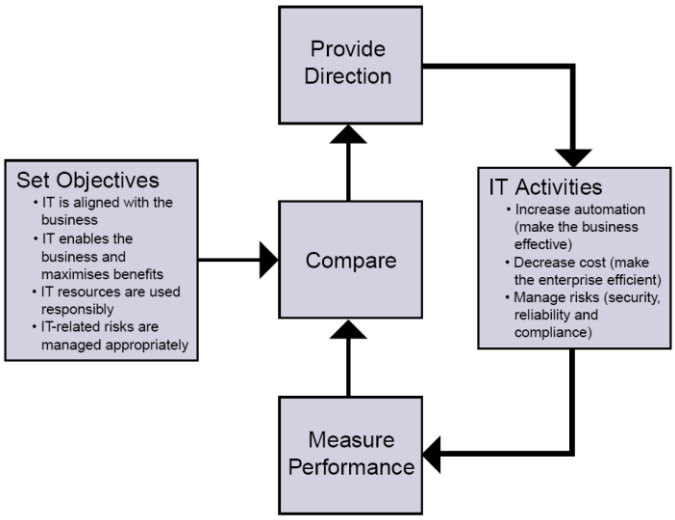


Figura 1.1: Estrutura da governança de TIC (GULDENTOPS, 2003).

Para grande parte das organizações, a informação e a tecnologia associada representam ativos valiosos. As organizações bem sucedidas utilizam a tecnologia da informação para dirigem e agregarem valores aos seus negócios. Estas empresas, em virtude de atenderem regulamentações e da dependência de seus processos com a da tecnologia da informação, reconhecem a necessidade de gerir os riscos associados. Valor, risco e controle fazem parte do núcleo da governança de TIC (ADLER, 2007).

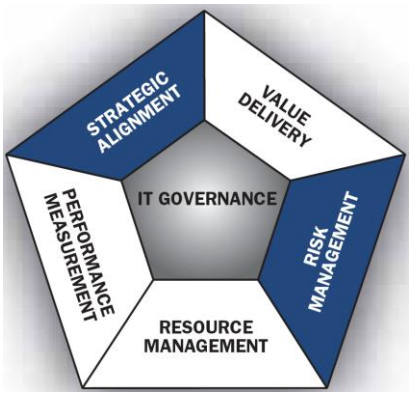


Figura 1.2: Áreas de foco da governança de TIC (ADLER, 2007).

A governança de TIC, cujo objetivo é o efetivo retorno dos investimentos realizados no aprimoramento da infra-estrutura e dos sistemas de informação e comunicação, é constituída por uma estrutura de relações e processos com o objetivo de aditar valor ao negócio através de um gerenciamento balanceado de riscos. (FAGUNDES, 2004).

O COBIT, *framework* referência para prover Governança de TIC, é formado por uma estrutura de domínios, processos e atividades. O domínio de Planejamento e Organização é constituído, entre outros, pelo processo de estimativa e controle de riscos. A Figura 1.3 mostra o alinhamento do processo de estimativa e controle de riscos do COBIT 4.1 com o ITIL V3 e ISO/EIC 27002.

CobiT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
P09.1 IT risk management framework	• Alignment to enterprise risk framework	• *SS 9.5 Risks* • *SD 4.5.5.1 Stage 1—Initiation*	• **14.1.1 Including information security in the business continuity management process** • **14.1.2 Business continuity and risk assessment**
P09.2 Establishment of risk context	• Internal and external context and goals of each assessment	• *SS 9.5 Risks* • *SD 4.5.5.1 Stage 1—Initiation* • *SD 4.5.5.2 Stage 2—Requirements and strategy*	• **14.1.1 Including information security in the business continuity management process** • **14.1.2 Business continuity and risk assessment**
P09.3 Event identification	• Important threats exploiting vulnerabilities having negative business impact • Risk registry	• *SS 9.5 Risks* • *SD 4.5.5.2 Stage 2—Requirements and strategy* • *ST 9 Challenges, critical success factors and risks* • *CSI 5.6.3 IT service continuity management*	• **13.1.1 Reporting information security events** • **13.1.2 Reporting**
P09.4 Risk assessment	• Likelihood and impact of all identified risks • Qualitative and quantitative assessment • Inherent and residual risk	• *SS 9.5 Risks* • *SD 4.5.5.2 Stage 2—Requirements and strategy* • *SD 8.1 Business impact analysis (not in detail)* • *ST 4.6 Evaluation*	• **5.1.2 Review of the information security policy** • **14.1.2 Business continuity and risk assessment**
P09.5 Risk response	• Cost-effective controls mitigating exposure • Risk avoidance strategies in terms of avoidance, mitigation or acceptance	• *SS 9.5 Risks* • *SD 4.5.5.3 Stage 3—Implementation* • *ST 4.6 Evaluation*	
P09.6 Maintenance and monitoring of a risk action plan	• Prioritising and planning risk responses • Costs, benefits and responsibilities • Monitoring deviations	• *SS 9.5 Risks* • *SD 4.5.5.4 Stage 4—Ongoing operation*	

Figura 1.3: Alinhamento do processo de estimativa e controle de riscos (P09) do domínio Planejamento e Organização do COBIT 4.1 com o ITIL V3 e ISO/EIC 27002 (HARDY, 2008)

Não é possível implantar o Gerenciamento de Continuidade de Serviços de TIC, um de processos das boas práticas de gerenciamento de serviços do ITIL, sem uma concisa definição dos requisitos do negócio. O ciclo de vida continuidade de negócio, tendo em vista os aspectos de tecnologia, depende de um bom entendimento do processo de Gerenciamento de Continuidade do Negócio (abreviado em inglês como BCM). O estágio de "análise de requisitos e definição de estratégias", o segundo estágio do BCM e fundamento para o processo de Gerenciamento de Continuidade de Serviços de TIC do ITIL, é responsável por definir como a organização reagirá a uma interrupção do negócio ou desastre e os custos associados. Esse estágio possui processos de avaliação de risco e análise de impacto no negócio, comuns do ciclo contínuo de gerenciamento de riscos (BARTLETT, 2003).

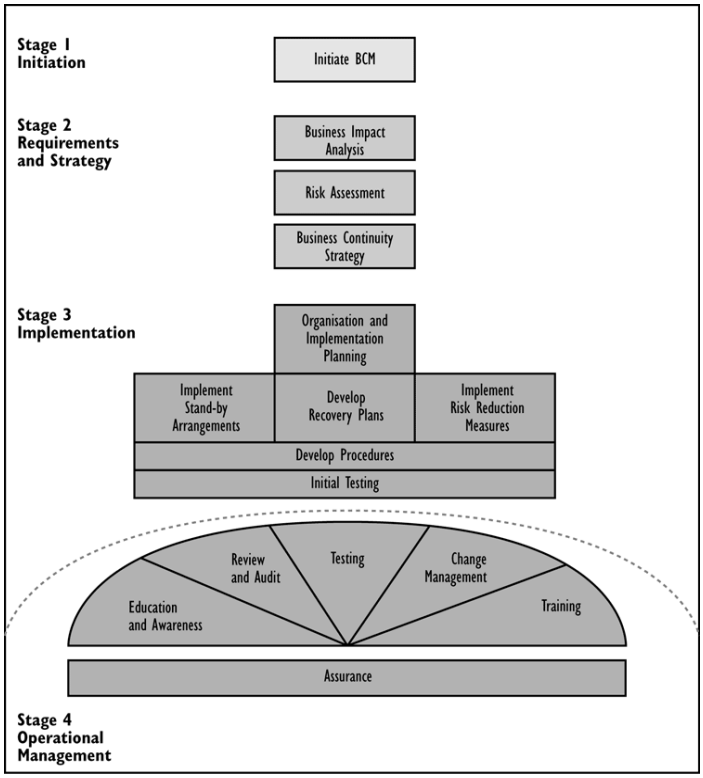


Figura 1.4: Modelo do processo do BCM (BARTLETT, 2003).

Como alternativa para as boas práticas do ITIL, o *Microsoft Operations Framework* (MOF) consiste de atividades, princípios e boas práticas para o alcance da confiabilidade nas soluções e serviços de TIC. O MOF tem o objetivo de criar um ambiente onde negócio e tecnologia da informação e comunicação possam trabalhar juntos em direção a maturidade operacional (BROEKARTS, 2008).

A camada de Gestão do ciclo de vida do MOF possui uma função de gestão de serviço denominada Governança, Risco e Conformidade. Esta função possui, entre outros, o processo de avaliação, monitoramento e controle de riscos.

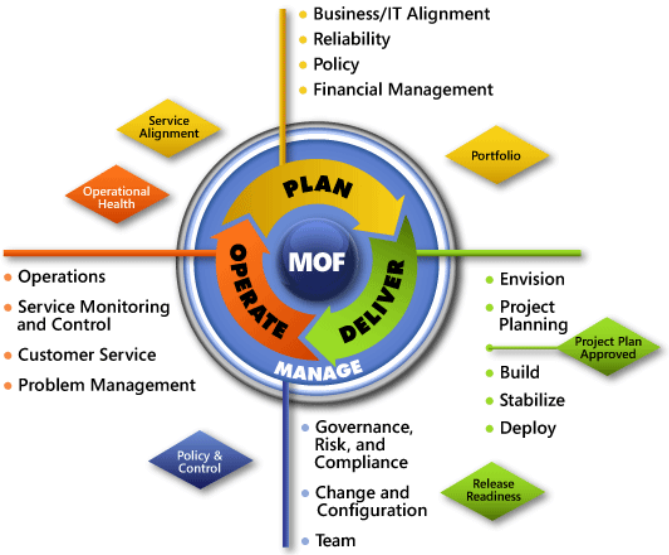


Figura 1.5: Fases do ciclo de vida dos serviços de TIC e funções de gestão de serviço (BROEKARTS, 2008).

1.3 Definição de risco

Segundo o Guia de Orientação para Gerenciamento de Riscos Corporativos:

> O termo risco é proveniente da palavra *risicu* ou *riscu*, em latim, que significa ousar (*to dare*, em inglês). Costuma-se entender risco como a possibilidade de "algo não dar certo", mas seu conceito atual envolve a quantificação e qualificação da incerteza, tanto no que diz respeito às "perdas" como aos "ganhos", com relação ao rumo dos acontecimentos planejados, seja por indivíduos, seja por organizações (LA ROCQUE, 2007, p. 11) [grifo do autor].
>
> Quando investidores compram ações, cirurgiões realizam operações, engenheiros projetam pontes, empresários abrem seus negócios e políticos concorrem a cargos eletivos, o risco é um parceiro inevitável. Contudo, suas ações revelam que o risco não precisa ser hoje tão temido: administrá-lo tornou-se sinônimo de desafio e oportunidade (BEMSTEIN aput LA ROCQUE, 2007, p. 11).
>
> O risco é inerente a qualquer atividade na vida pessoal, profissional ou nas organizações, e pode envolver perdas, bem como oportunidades (LA ROCQUE, 2007, p. 11).

A estrutura lingüística Semântica proporciona ao termo *risco* outros significados:

> **ris.co** *sm* (*ital rischio*) Possibilidade de perigo, incerto mas previsível, que ameaça de dano a pessoa ou a coisa. *R. bancário, Com*: o que decorre do negócio entre banqueiros ou entre o banco e os correntistas. *R. profissional, Dir*: perigo inerente ao exercício de certas profissões, o qual é compensado pela taxa adicional de periculosidade. *A risco de, com risco de*: em perigo de. *A todo o risco*: exposto a todos os perigos. *Correr risco*: estar exposto a. (MELHORAMENTOS, 1998, dicionário eletrônico Babylon 6.0) [grifo do autor]

Na área de tecnologia da informação e comunicação, risco é considerado como o impacto negativo motivado pela exploração de uma vulnerabilidade, considerando a possibilidade e o impacto da sua ocorrência. O processo para identificar, mensurar e planejar passos para reduzir um determinado risco a níveis aceitáveis pela organização é definido como Gerenciamento de Riscos (STONEBURNER, 2002).

2 GERENCIAMENTO DE RISCOS

2.1 Visão Geral

O gerenciamento de riscos é um processo que tem como objetivo dar subsídios à organização realizar sua missão institucional: possibilita segurança efetiva dos sistemas de TIC, responsáveis pelo processamento, armazenagem e transmissão de informações; cria uma base sólida para as tomadas de decisão, principalmente no que se relaciona com execução coerente do orçamento e no investimento em tecnologias necessárias para mitigar riscos de impacto ou potencial impacto para o negócio; e permite que gestores de equilibrem seus custos de proteção e desempenho dos sistemas de informação vitais para o negócio (STONEBURNER, 2002).

Um fato importante é que processo de gerenciamento de risco não deve ser considerado apenas na área de tecnologia da informação e comunicação, mas sim em todas as outras unidades de negócio (STONEBURNER, 2002).

2.1.1 Fundamentos de sucesso

Elementos fundamentais devem estar presentes para garantir o sucesso de qualquer iniciativa realizada por uma organização. Para a implementação de um processo de gerenciamento de riscos, é essencial a presença de determinados componentes (DILLARD, 2004):

- **Patrocínio executivo:** total apoio da alta direção ao processo de gerenciamento de riscos, de modo a reduzir a resistência à mudanças ou incredulidades em relação aos possíveis riscos;
- **Lista de interessados**: membros da organização diretamente interessados com o sucesso do processo de gerenciamento de riscos, identificados de forma que possam participar de cada etapa;
- **Maturidade corporativa**: a maturidade corporativa relaciona-se com o processo de gerenciamento de riscos, em outras palavras, quanto menor a experiência de uma empresa em relação ao processo, mais radicais e rápidas poderão ser as mudanças;
- **Ambiente de comunicação**: o processo de gerenciamento de riscos exige uma abordagem de comunicações abertas e honestas, tanto no âmbito da equipe como dos interessados. O ambiente de comunicação é importante para que se evitem mal-entendidos, resultando em desperdício de tempo, recursos e até em soluções erradas;

- **Espírito de equipe:** é necessário que a equipe de gerenciamento de riscos seja colaborativa, tanto internamente quanto com cada um dos representantes das diversas unidades de negócio envolvidas no processo;
- **Visão holística:** o escopo do gerenciamento de risco deve levar em conta a organização como um todo. O que é bom para um setor, pode não ser bom para outro. Isto não deve impactar no sucesso do processo;
- **Autoridade:** além da responsabilidade de identificar e controlar os riscos mais graves para o negócio, a equipe de gerenciamento de riscos precisam de autoridade suficiente para realizar as mudanças necessárias e cumprir metas.

2.1.2 Abordagem reativa e proativa

Quando ocorre determinado incidente de segurança, muitos profissionais de informática tendem a agir para conter a situação, descobrir as causas e reparar os danos no menor tempo possível. Tal abordagem é dita reativa, depende de um estímulo causado por um incidente para que ações sejam tomadas (DILLARD, 2004).

As respostas a incidentes são taticamente eficazes, principalmente se executada com rigor para se descobrir as causas raiz. Como resultado, incidentes de segurança recentes podem auxiliar na prevenção de incidentes futuros (DILLARD, 2004).

A abordagem proativa de gerenciamento de riscos de segurança almeja a redução da probabilidade de um incidente com a utilização de planos de controles. Ao contrário da abordagem reativa, a abordagem proativa não espera pelo surgimento de um incidente (DILLARD, 2004).

Em hipótese alguma, as organizações devem abandonar seus processos de respostas a incidentes, pois a abordagem proativa diminui a chance, mas não evitam que determinados incidentes possam ocorrer. Recomenda-se que as organizações utilizem as duas abordagens, aprimorando-as ao longo do tempo (DILLARD, 2004).

2.1.3 Papéis principais

Os principais atores num processo de gerenciamento de riscos podem ser assim definidos (STONEBURNER, 2002):

- **Patrocinador executivo:** a alta direção, sob a qual está a responsabilidade final de execução da missão da empresa, deve garantir que os recursos necessários são efetivamente aplicados para atender os requisitos de negócio. Além disso, devem avaliar e integrar os resultados das atividades na avaliação de risco no processo de decisão. Um programa de gestão de risco eficaz, que avalia e atenua riscos potenciais ao negócio, exige o apoio e a participação da alta direção.
- **Diretor de TIC:** responsável pela tecnologia de informação interna de uma organização.
- **Gerentes de Sistemas e Tecnologia**: responsáveis pela gestão do departamento de tecnologia da informação e comunicação e por garantir os controles adequados à segurança dos sistemas que estão sob suas responsabilidades. Estes gerentes são responsáveis também por garantir o processo de mudança nos sistemas e infra-estrutura tecnológica, compreendendo tais mudanças dentro do processo de gerenciamento de riscos.

- **Gerentes Funcionais:** são os responsáveis pela execução do negócio e, por possuírem poder de decisão, tendem a contribuir diretamente no processo de gerenciamento de riscos.
- **Gerentes de Segurança da Informação:** são os responsáveis pela gestão da segurança da informação em suas organizações, incluindo o gerenciamento de risco. Atuam como apoio a alta direção na garantia de execução das atividades de segurança da informação.
- **Administradores de Sistemas e Infra-Estrutura**: responsáveis por atuar diretamente nos sistemas e infra-estrutura de TIC das organizações. Quando uma mudança ocorre no ambiente de um sistema de TIC, os administradores devem apoiar-se no processo de gerenciamento de risco para identificar potenciais riscos e programar novos controles de segurança para salvaguardar seus sistemas.
- **Instrutores de Noções de Segurança:** responsáveis por disseminar a cultura de segurança da informação, regras de utilização dos recursos e política de segurança aos usuários de recursos de TIC. Este papel é essencial para minimizar riscos na infra-estrutura, já que a má utilização do recurso pelo usuário pode ser considerada como um risco em potencial.

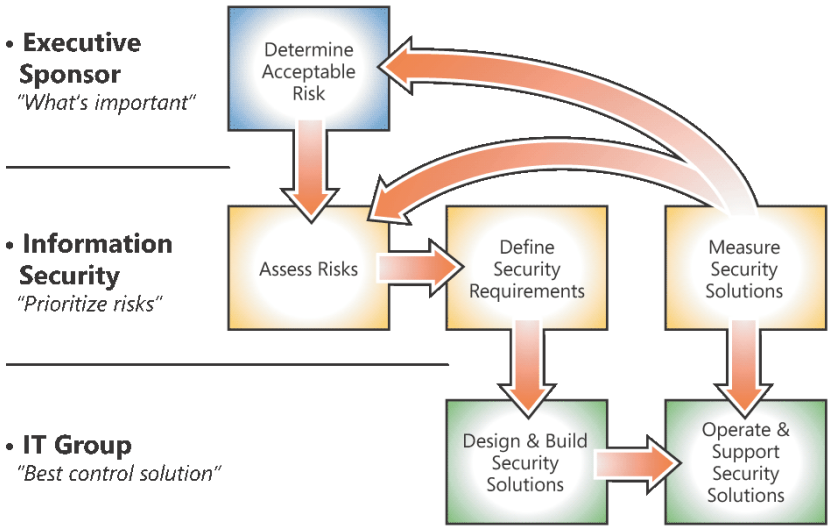


Figura 2.1: Visão geral das funções e responsabilidades no processo de gerenciamento de riscos de segurança (DILLARD, 2004).

2.1.4 Etapas do processo

O gerenciamento de riscos é composto basicamente por três macro-processos: a *avaliação*, a *mitigação* e o *monitoramento, análise e melhoria contínua*. A avaliação de riscos inclui a identificação dos ativos e dos riscos associados, os impactos e medidas preventivas. A mitigação de riscos refere-se à priorização, implantação e manutenção das medidas preventivas para redução de riscos, recomendadas pelo processo de avaliação de riscos. E o processo de monitoramento, análise e melhoria contínua é constituído de um acompanhamento do ambiente para garantir a efetividade do programa, propondo alterações quando necessário (STONEBURNER, 2002).

Dependendo da metodologia, o gerenciamento de riscos poderá ter variações nas fases de seu processo, com maior ou menor detalhamento em cada subfase, mas todas têm como objetivo a redução do risco a um nível aceitável para o negócio.

A norma NBR ISO/EIC 27005:2008 prescreve que o gerenciamento de riscos pode ser realizado iniciando-se com uma *definição de contexto*: determina os critérios básicos para a condução do processo, o escopo, limites e a equipe de gestão de riscos de segurança da informação; seguido por uma *análise/avaliação de riscos*: etapa que identifica, qualifica, quantifica e prioriza os riscos em função dos critérios de avaliação da organização; *tratamento de riscos*: seleciona controles para reduzir, reter evitar ou transferir os riscos priorizados na etapa anterior; *aceitação de riscos*: é a decisão formal de aceitar o risco; *comunicação do riscos*: comunicação das informações de riscos entre o tomador de decisão e os interessado; e *monitoramento e análise crítica dos riscos*: processo contínuo para identificar rapidamente mudanças contextuais na organização que possam afetá-la futuramente (ABNT, 2008).

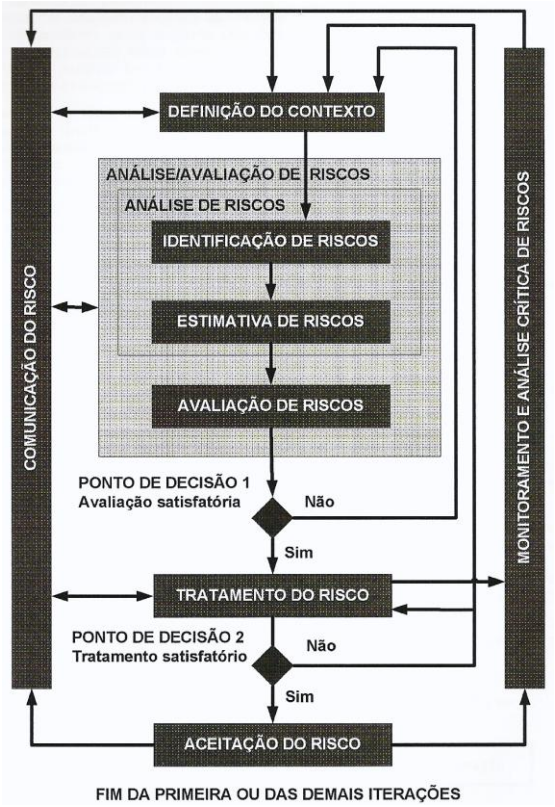


Figura 2.2: Processo de gestão de riscos de segurança da informação (ABNT, 2008).

O *Security Risk Management Guide* contextualiza um processo contínuo de quatro fases (DILLARD, 2004):

- Avaliação de riscos: planejamento da coleta de dados sobre riscos, ação de coleta de dados e priorização dos riscos;
- Oferecendo suporte a decisão: definição dos requisitos funcionais; seleção de soluções de controle; revisão de soluções existentes, estimativa de a redução de riscos, estimativa de o custo de soluções e seleção das estratégias de mitigação;
- Implantando controles: busca de soluções completas e organização da defesa em profundidade.

- Medindo a efetividade do programa: desenvolvimento de um indicador de riscos e análise da eficácia do programa

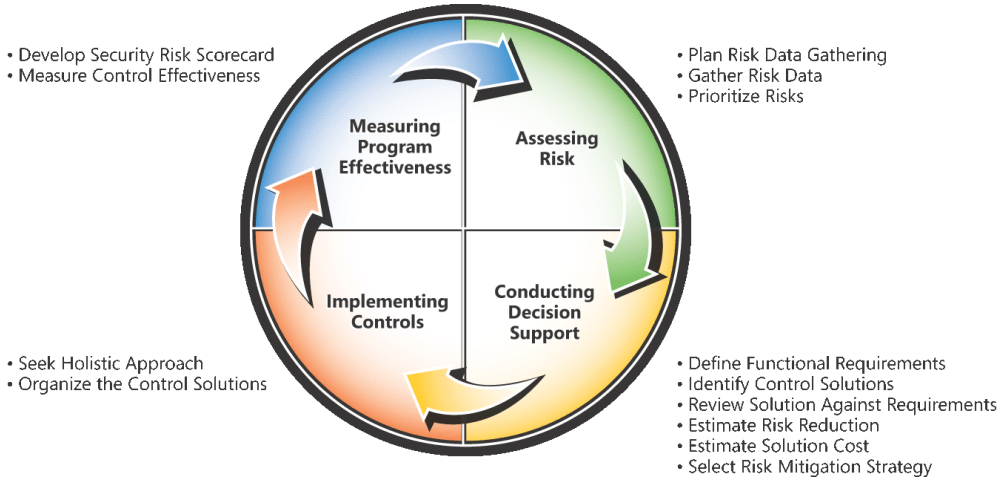


Figura 2.3: As quatro fases do processo de gerenciamento de riscos de segurança (DILLARD, 2004).

A abordagem do OCTAVE, técnica de planejamento e estimativa estratégica de segurança baseada em risco, tem como alvo o risco organizacional e concentra-se na estratégia e em questões práticas, e não somente em riscos tecnológicos e questões táticas. Quanto aplicado, o OCTAVE proporciona o nivelamento de três pontos chave: risco operacional, práticas de segurança e tecnologia (ALBERTS, 2003).

Os aspectos organizacionais, tecnológicos e operacionais da avaliação de riscos de segurança da informação são realizados pelo OCTAVE em três fases: *construção de perfis de ameaças baseados em ativos*: visão organizacional para definição dos ativos críticos ao negócio e quais seus requisitos de segurança; *identificação de vulnerabilidades na infra-estrutura*: avaliação da infra-estrutura de TIC e quais suas condições em relação aos requisitos de segurança definidos; e *desenvolvimento de planos e estratégias de segurança*: identificação de riscos aos ativos críticos e a criação de estratégias de proteção e planos de mitigação de riscos (ALBERTS, 2003).

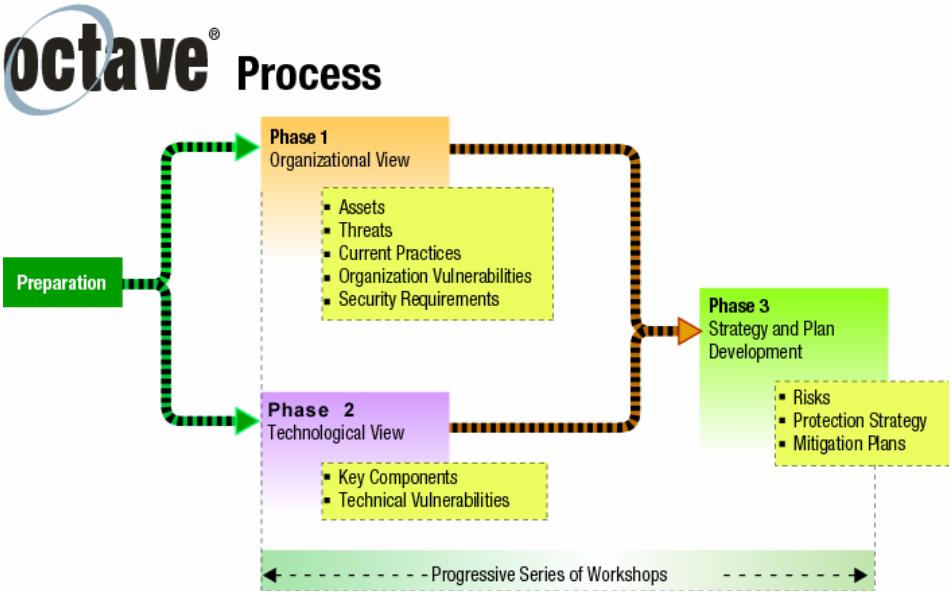


Figura 2.4: Fases do OCTAVE (ALBERTS, 2003).

2.2 Avaliação de Riscos

O processo de avaliação de riscos, o primeiro macro-processo do gerenciamento de riscos de segurança da informação, é utilizado para determinar a extensão das potenciais ameaças e os riscos associados à infra-estrutura de TIC. O produto deste processo será utilizado no processo seguinte, o de mitigação de riscos, na identificação de controles para reduzir ou eliminar os riscos (STONEBURNER, 2002).

Uma avaliação de riscos pode ser realizada, em geral, por uma seqüência de nove passos: caracterização do ambiente, identificação de ameaças, identificação de vulnerabilidades, análise de controles, determinação de probabilidades, análise de impacto, definição dos riscos, recomendações de controle e documentação dos resultados. (STONEBURNER, 2002).

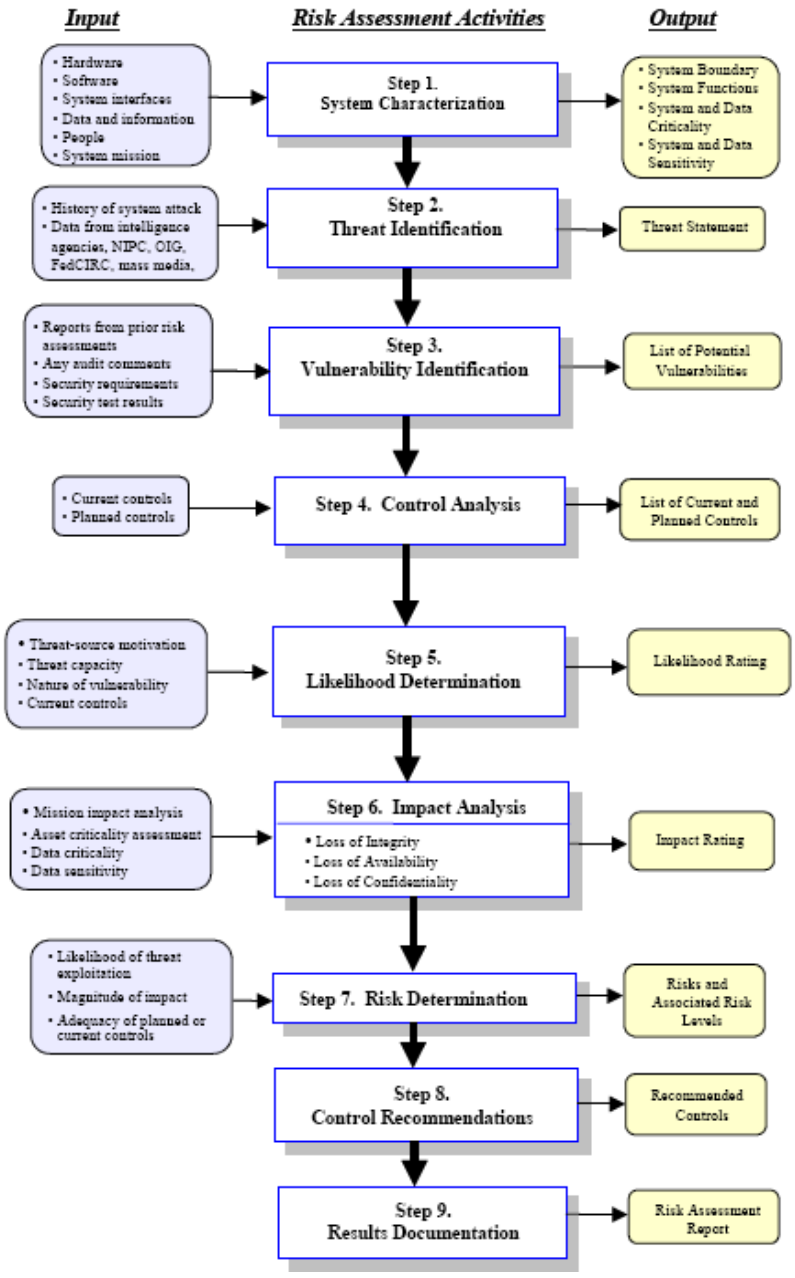


Figura 2.5: Processo de avaliação de risco (STONEBURNER, 2002).

O gerenciamento de riscos é subordinado a um adequado planejamento de avaliação de riscos. Falhas no alinhamento, escopo ou na obtenção da aceitação da avaliação reduz a eficácia das próximas fases. Por ser onerosa, a fase de avaliação de riscos reclama por investimentos significativos de recursos e tempo, e depende da participação ativa do interessado (DILLARD, 2004).

O risco é calculado em função da probabilidade de uma vulnerabilidade ser explorada por uma ameaça e o resultado do impacto na organização caso este evento ocorra. Para que se possam determinar as possibilidades de ocorrência de um evento adverso no ambiente de TIC, as ameaças devem ser analisadas em conjunto com as potenciais vulnerabilidades e os controles já existentes. O nível do impacto é definido pela sua influência no negócio e por sua vez no valor do bem ou recurso de TIC atingido (STONEBURNER, 2002).

2.2.1 Caracterização do ambiente

A caracterização do ambiente é responsável por definir o escopo da avaliação de riscos, assim como os limites operacionais, os recursos computacionais e as informações que constituem as fronteiras dos sistemas que serão contemplados no processo de gerenciamento de riscos (STONEBURNER, 2002).

Nesta etapa, convêm que sejam levantadas todas as informações da organização relevantes ao estabelecimento do contexto, em especial, os critérios para a avaliação dos riscos. Estes critérios devem considerar o valor estratégico do processo que trata as informações; a criticidade dos ativos; os requisitos legais, contratuais e regulatórios; as exigências de disponibilidade, confidencialidade e integridade da informação; as expectativas dos interessados; e as conseqüências negativas para o mercado, para a imagem e reputação da organização (ABNT, 2008)

Inventariar os ativos, conhecer seus respectivos valores e importância ao negócio assegura proteção de forma efetiva, pois os níveis de cuidado serão proporcionais a estes parâmetros, além de serem pré-requisitos fundamentais para o gerenciamento de risco. Exemplos de ativos associados a sistemas são (ABNT, 2005):

- Informação: bancos dados, arquivos, documentação de sistemas, manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de contingência, procedimentos de recuperação, informações armazenadas;
- *Softwares:* aplicativos, sistemas, ferramentas de desenvolvimento, e utilitários;
- *Hardwares*: equipamentos computacionais (processadores, monitores, *laptops*, discos rígidos, impressoras, *storages*, *autoloaders*, *nobreaks*), ativos de rede (roteadores, *switches*), equipamentos de apoio (geradores, condicionadores de ar, iluminação);
- Serviços: contratos de apoio ou suporte, contratos de níveis de serviço, fornecimento de energia elétrica.

É conveniente a identificação de um responsável para cada ativo. Mesmo que o não tenha direitos de propriedade sobre o ativo, o responsável responderá pela sua produção, desenvolvimento, manutenção utilização e segurança. Normalmente é o responsável a pessoa mais adequada para definir o valor do ativo para a organização (ABNT, 2008).

Para sistemas em fase de desenvolvimento, as informações necessárias para o processo caracterização devem derivar das documentações de requisitos (STONEBURNER, 2002).

A coleta das informações relacionadas com o ambiente de TIC pode ser realizada por meio de questionários específicos, entrevistas com pessoas chaves, revisão das documentações, uso de aplicação para rastrear o ambiente ou uma combinação de todas elas (STONEBURNER, 2002).

Data Gathering Template

Identify assets that your group is responsible for developing, managing, supporting, or maintaining.

Asset Name	Asset Classification (High, Medium, or Low Business Impact)
1.	

For each asset, complete the following:

Defense-in-Depth Layer	What You Are Afraid of or Are Trying to Avoid: (Threats)	How It May Happen: (Vulnerabilities)	Exposure Level (H,M,L)	**Current Controls Descriptions**	Probability (H,M,L)	**Control Concerns, Potential New Controls**
Physical						
Application						
Host						
Network						
Data						

Figura 2.6: Modelo de formulário para coleta de dados (DILLARD, 2004).

Como produtos, a caracterização do ambiente terá um inventário de ativos, classificados conforme sua importância aos negócios da organização e seus responsáveis, os sistemas e dados sensíveis e quais serão as fronteiras do processo de gerenciamento de riscos.

2.2.2 Identificação das Ameaças

Define-se ameaça como o potencial de uma fonte de ameaças explorar uma vulnerabilidade (fraqueza) específica. As fontes de ameaça podem ser criadas intencionalmente ou são eventos aleatórios que desencadeiam acidentalmente uma vulnerabilidade, e podem ter origem **natural** (enchentes, terremotos, tornados, deslizamento de terra, tempestades de raios, etc.), **humana** (atos dolosos, negligentes, imperitos ou imprudentes de uso de programas maliciosos, de acesso a dados sigilosos, de mau uso dos sistemas, etc.) ou **ambiental** (falta de energia, poluição, substâncias químicas, etc.). Quando não há vulnerabilidades associadas, a fonte de ameaça não apresenta riscos (STONEBURNER, 2002).

O ANEXO A contém exemplos de ameaças típicas que podem ser utilizados no processo de identificação de ameaças, e uma visão geral de algumas ameaças causadas especificamente por pessoas, suas possíveis motivações e ações que podem ocasionar um ataque.

É considerável que se analise o histórico de eventos que causaram incidentes de segurança na organização. Tais históricos podem ser adquiridos por intermédio de entrevistas com os responsáveis dos ativos, entrevistas com os usuários, análise de chamados de *help-desk*, experiências internas de incidentes e identificação de ameaças anteriores (STONEBURNER, 2002).

Outras referências para identificação de ameaças podem ser especialistas em segurança da informação, peritos em segurança física, a mídia, acontecimentos históricos, departamentos jurídicos, outras organizações, organismos legais, autoridades climáticas, companhias de seguro e agências ou instituições governamentais. O que é

ameaça para uma organização pode não ser para outra, desta forma, aspectos culturais e relacionados ao ambiente precisam ser considerados (ABNT, 2008)

Uma lista de possíveis fontes de ameaças que podem explorar vulnerabilidades na infra-estrutura e nos sistemas é o produto deste processo.

2.2.3 Identificação de Vulnerabilidades

O inventário de ativos críticos ao negócio e uma lista de possíveis fontes de ameaças são parâmetros para a identificação das vulnerabilidades associadas ao ambiente de tecnologia da informação.

Vulnerabilidades são falhas ou fraquezas nos processos de segurança, nos projetos, no desenvolvimento ou nos controles internos de um sistema, os quais, se explorados, podem resultar em eventos não desejados (STONEBURNER, 2002).

O ANEXO B fornece exemplos de vulnerabilidades em diversas áreas de segurança e ameaças que poderiam explorar tais vulnerabilidades.

Métodos proativos de testes podem ser utilizados para identificar vulnerabilidades nos ambientes de tecnologia da informação e comunicação, pode-se citar (ABNT, 2008):

- Sistemas de varredura e análise de vulnerabilidades;
- Testes e simulações;
- Testes de invasão de sistemas;
- Auditorias em códigos-fonte;
- Listas de verificação e análise crítica de segurança.

As listas de verificação de segurança podem conter padrões básicos de segurança de um sistema ou infra-estrutura e podem ser utilizadas para identificar vulnerabilidades nos ativos, procedimentos não automatizados, nos processos de transferências de informações, nos processamentos e armazenamentos de dados nos ambientes de tecnologia da informação. Estas listas normalmente contêm critérios distribuídos em três áreas distintas de segurança: *gerencial*, *operacional* e *técnica*. A definição de uma lista de verificação pode ser feita norteada pelas boas práticas da indústria, por padrões conhecidos, pela necessidade de atendimento de legislações ou contratos de negócio, pela cultura e necessidades específicas de uma organização (STONEBURNER, 2002).

Tabela 2.1: Exemplos de critérios de segurança

Áreas de Segurança	Critérios de Segurança
Segurança Gerencial	Capacidade de resposta a incidentes; Análise crítica dos controles e indicadores; Avaliação de riscos; Treinamentos técnicos em segurança; Definição e segregação de responsabilidades; Planos de segurança de sistemas ou recursos;

	Treinamento dos usuários; Contratos de nível de serviço.
Segurança Operacional	Controle de contaminação do ar; Garantia da qualidade do fornecimento de energia; Metodologia de acesso e descarte de dados; Identificação e distribuição externa de dados; Medidas de proteção das instalações; Controle de umidade e temperatura.
Segurança Técnica	Comunicações e ativos relacionados; Criptografia dos dados e entre comunicações; Controle de acesso arbitrário; Sistemas de autenticação e identificação; IDS's; Auditoria de sistemas; Monitoramento do ambiente de rede; Sistema de antivírus; Atualização de sistemas.

Fonte: STONEBURNER, 2002, p. 18.

Os APÊNDICES A e B apresentam respectivamente exemplos de organizações responsáveis por responder a incidentes de segurança e de ferramentas de auditoria de segurança em sistemas.

O resultado deste processo de identificação é uma relação de vulnerabilidades que podem ser exploradas por fontes de ameaças.

2.2.4 Análise de Controles

Este passo tem como objetivo avaliar os controles existentes ou planejados para minimizar ou eliminar chances de uma ameaça explorar determinada vulnerabilidade.

Para que se evitem custos e retrabalhos, é conveniente que os controles existentes sejam identificados e avaliados quanto sua a eficácia. Controles existentes podem ser considerados ineficazes, insuficientes ou não-justificáveis, devendo estes ser avaliados quanto a sua substituição ou manutenção no ambiente (ABNT, 2008).

Informações de controles podem ser obtidas: pela análise de documentos dos processos de gestão de segurança da informação; juntamente com responsáveis pela segurança da informação, responsáveis pelas instalações, segurança predial ou usuários; e pela averiguação da efetividade de funcionamento dos controles utilizados (ABNT, 2008).

O produto da análise de controle é uma lista de controles utilizados para reduzir a probabilidade de uma ameaça explorar uma vulnerabilidade ou de reduzir o dano causado por um evento não desejado.

2.2.5 Definição de Probabilidades

A produção de um índice que indique as chances de uma vulnerabilidade ser explorada deriva da capacidade e do estímulo das fontes de ameaças, da natureza da vulnerabilidade e da existência e da efetividade de controles existentes (STONEBURNER, 2002).

Probabilidades são ditas altas quando a fonte de ameaça está altamente estimulada, é capaz de exercer a ameaça e não existem controles preventivos, ou se existem não são efetivos. Probabilidades são ditas médias quando a fonte de ameaça está motivada, é capaz de exercer a ameaça, mas os controles utilizados são efetivos, ou seja, não permitem o sucesso da fonte de ameaça. E por fim, probabilidades são ditas baixas quando as fontes de ameaças carecem de motivação e os controles são efetivos na prevenção da exploração da vulnerabilidade (STONEBURNER, 2002).

É notório afirmar que a definição de probabilidades é um tanto subjetiva, pois depende de fatores variados. Uma vulnerabilidade pode ser mais ou menos provável de ser explorada dependendo do ambiente, do tipo do ativo, da localização geográfica, dos controles existentes, dos estímulos das fontes das ameaças.

Para uma definição refinada de probabilidade é conveniente considerar: experiências passadas e estatísticas de ocorrência de ameaças; as motivações, competências e ferramentas disponíveis para a realização de atos intencionais, bem como a percepção de vulnerabilidade em ativos valiosos; os fatores geográficos e os eventos climáticos; as situações que poderiam produzir erros humanos; e a análise de efetividade dos controles atuais (ABNT, 2008).

Da definição de probabilidades resulta uma lista de classificação das vulnerabilidades quanto às suas chances de exploração.

2.2.6 Análise de Impacto

A análise de impacto é o passo principal do processo de avaliação de riscos e tem como objetivo determinar o resultado do impacto no negócio no caso de uma ameaça ter sucesso na exploração de uma determinada vulnerabilidade (STONEBURNER, 2002).

Como pré-requisito, é necessário conhecer o objetivo, a criticidade, e sensibilidade dos sistemas e dos dados. Estas informações podem ser obtidas em relatórios existentes na organização como, por exemplo, no relatório de avaliação de ativos críticos ou no relatório de Análise de Impacto no Negócio (abreviado na língua inglesa como BIA). O BIA tem como objetivo dar uma visão, qualitativa e/ou quantitativa, de quão crítico sensível é um ativo para a organização (STONEBURNER, 2002).

No ITIL, o propósito do BIA é identificar os processos críticos do negócio e os potencias danos ou perdas que uma organização pode ter se houver interrupções destes processos. O BIA também procura identificar: a forma do dano ou perda considerando redução de rendimentos, custos adicionais, influências negativas na reputação e perda de vantagens competitivas; os serviços, incluindo os serviços de TIC, vitais para que o negócio possa continuar num nível mínimo aceitável; o tempo de recuperação dos níveis mínimos dos serviços vitais; e o tempo que todos os processos de negócio devem ser restabelecidos no caso de uma falha (BARTLETT, 2003).

Na ausência informações detalhas a respeito da criticidade dos ativos, a avaliação do impacto nos negócios pode ser realizada tendo como fundamento os requisitos de segurança atuais e as definições de nível de impacto dos responsáveis pelos ativos.

A Figura 2.1 mostra uma representação gráfica de uma análise de impacto, que varia conforme aplicação de planos de contingência no decorrer do tempo:

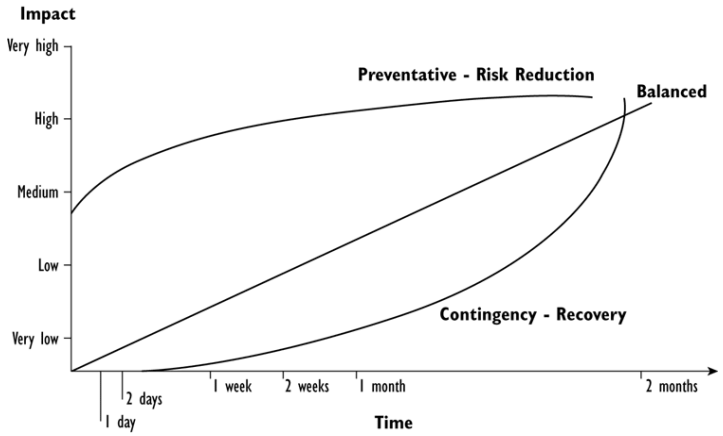


Figura 2.7: Representação gráfica dos impactos nos negócios (BARTLETT, 2003).

O impacto adverso de um evento pode ser descrito como a perda e/ou degradação da integridade, disponibilidade ou confidencialidade da informação. Impactos tangíveis podem ser mensurados **quantitativamente** utilizando-se uma unidade de medida conhecida, como: perda de desempenhos, custos de manutenção ou tempo gasto para corrigir problema. Outros, de difícil mensuração, podem ser definidos **qualitativamente** como alto, médio ou baixo impacto, classificados conforme grandeza dos custos pela perda dos ativos ou recursos, significância do dano em relação à missão ou reputação da empresa, ou prejuízos a vida humana (STONEBURNER, 2002).

As abordagens quantitativa e qualitativa apresentam benefícios e inconveniências que precisam ser consideradas na avaliação de riscos. A organização deve optar pelo uso individual ou por combinação de ambas, conforme seus requisitos e níveis de exigência.

Tabela 2.2: Vantagens e desvantagens das abordagens quantitativa e qualitativa

	Quantitativa	Qualitativa
Vantagens	Os riscos e os ativos são avaliados de acordo com o impacto financeiro; Os resultados facilitam o gerenciamento de riscos graças ao retorno do investimento em segurança; Os resultados podem ser expressos usando uma terminologia de gerenciamento por valores ou percentuais; A precisão tende a aumentar com o passar do tempo, à medida que a organização coleta registros históricos	Permite a visibilidade e a compreensão da classificação de riscos; Maior facilidade de chegar a um consenso; Não é necessário quantificar a freqüência da ameaça; Não é necessário determinar os valores financeiros dos ativos; Maior facilidade de envolver pessoas que não sejam especialistas em segurança ou

	dos dados e ganha experiência.	computadores.
Desvantagens	Os valores do impacto atribuído ao risco podem ser baseados na opinião subjetiva dos participantes; O processo para atingir resultados confiáveis e um consenso pode ser demorado; Os cálculos podem ser complexos e demorados; Os resultados são apresentados em termos monetários e podem ser difíceis de serem interpretados por pessoas sem conhecimento técnico; O processo exige experiência e conhecimento, portanto pode ser difícil explicá-lo aos participantes.	Riscos graves podem não ser diferenciados o suficiente; Dificuldade de justificar o investimento na implementação de controles, pois não há valores básicos para realizar a análise de custo/benefício; Os resultados dependem da qualidade da equipe de gerenciamento de riscos formada.

Fonte: DILLARD, 2004, p. 3.

A extensão dos impactos de incidentes adversos ao negócio é o resultado do processo de análise de impacto.

2.2.7 Definição dos Riscos

A definição dos riscos pode ser expressa por uma combinação de três argumentos: a possibilidade de exploração de uma vulnerabilidade; o impacto ao negócio devido à ocorrência de um evento adverso; e pela efetividade do controles de segurança utilizados para reduzir ou eliminar riscos (STONEBURNER, 2002).

O nível e a escala do risco podem ser demonstrados a partir de uma matriz, onde os argumentos supracitados são cruzados de modo a mensurar um determinado risco. A Figura 2.8 mostra um exemplo básico de uma classificação de risco levando em conta a abordagem qualitativa do impacto ao negócio e da probabilidade de ocorrência de um evento indesejado.

		Summary Level Risk Rating		
Impact (from Impact Table above)	**High**	Moderate	High	High
	Med	Low	Moderate	High
	Low	Low	Low	Moderate
		Low	**Medium**	**High**
		Probability Value		

Figura 2.8: Planilha de análise de risco: Impacto/Probabilidade (DILLARD, 2004).

Dependendo da necessidade de maior granularidade, as classificações podem ser mais detalhadas, adaptando-se à necessidade da organização.

A Figura 2.9 mostra um exemplo de tabela com maior nível de detalhamento na qualificação dos parâmetros de probabilidade de incidente e no impacto ao negócio. Levando em consideração uma escala de 0 a 8, os riscos podem variar de uma classificação de "muito baixo" a "muito alto", respectivamente.

	Probabilidade do cenário de incidente	Muito baixa (Muito improvável)	Baixa (Improvável)	Média (Possível)	Alta (Provável)	Muito alta (Freqüente)
Impacto ao negócio	Muito baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito alto	4	5	6	7	8

Figura 2.9: Classificação de riscos (ABNT, 2008).

Após a definição dos riscos é possível obter-se a classificação dos riscos conforme seu nível de relevância para a continuidade dos negócios.

2.2.8 Recomendações de Controle

A fase de recomendações de controle tem como objetivo identificar os controles de segurança ou soluções alternativas que podem ser utilizados pela organização para reduzir ou eliminar riscos. Devem ser consideradas as opções recomendadas ou compatíveis, questões culturais da organização, dificuldades operacionais de implantação, as que fornecem confiabilidade e segurança e, principalmente, as que têm melhor relação custo x benefício para o negócio (STONEBURNER, 2002).

O processo de identificação de controles pode ser desafiador, especialmente se os envolvidos possuírem vivência limitada no assunto. Duas abordagens podem ser empregadas: a primeira consiste em um debate informal, enquanto a segunda fundamenta-se na organização e classificação de controles. A equipe de gerenciamento de riscos de segurança deve usar uma combinação dessas duas abordagens (DILLARD, 2004).

Na abordagem através de debate informal, os controles podem ser identificados depois de respondidas perguntas como (DILLARD, 2004):

- Que medidas a organização poderia tomar para resistir ou prevenir a ocorrência de riscos?
- O que a organização poderia fazer para recuperar-se de um evento adverso?
- Que medidas a organização pode tomar para detectar a ocorrência de riscos?
- Como o controle pode ser auditado e monitorado para garantir sua efetividade?
- Existem outras ações que podem ser tomadas para gerenciar o risco?

O segundo método de recomendação de controles sustenta-se na classificação do controle em organizacional, operacional e tecnológico, e ainda em subdivisões como prevenção, detecção/recuperação e gerenciamento de riscos. Os controles

organizacionais definem como os colaboradores de uma organização devem executar suas tarefas. Os controles operacionais normatizam a utilização dos recursos de tecnologia da informação e comunicação, e incluem também as proteções ambientais e físicas. Enquanto que controles tecnológicos compreendem o planejamento arquitetônico, engenharia, *hardwares*, *softwares* e *firmware*s, ou seja, os componentes tecnológicos usados para construir os sistemas de informação da organização (DILLARD, 2004).

A Tabela 2.3 apresenta uma relação de controle classificados conforme classificação acima explicada. O ANEXO C apresenta uma relação não exaustiva de controles e objetivos de controles que podem ser utilizados nos sistemas de gerenciamento de segurança da informação de uma organização de forma a prevenir-se de riscos.

Tabela 2.3: Organização e classificações de controles

	Organizacional	Operacional	Tecnológico
Prevenção de riscos	Definição de funções e responsabilidades; Separação de tarefas e restrições de privilégios; Documentação de planos e procedimentos de segurança; Treinamentos de segurança e campanhas de conscientização de usuários; Sistemas e processos para fornecimento e cancelamento de usuários; Processos para conceder acessos a contratados, fornecedores, parceiros e clientes.	Proteção das instalações computacionais através de meios físicos; Proteção física dos sistemas de usuários finais; Sistemas de fornecimento de energia redundantes; Sistemas de proteção contra incêndio; Sistemas de controle de temperatura e umidade; Controle de acesso à mídia e procedimentos de descarte; Sistemas de *backup* e com opção de armazenamento externo.	Autenticação: processo de validação de credenciais; Autorização: processo de concessão de acesso a determinadas informações, serviços ou funcionalidades; Não-repúdio: técnica usada para impedir negação de autoria; Controle de acesso: mecanismo para limitar o acesso com base na identidade ou na participação em grupos predefinidos; Comunicações protegidas por sessões criptografadas.

Detecção/Recuperação de riscos	Aplicação contínua do processo gestão de riscos; Análises contínuas de verificação dos controles; Auditorias periódicas de configuração e integridade dos sistemas; Investigação de histórico pessoal e profissional dos futuros funcionários; Estabelecimento de rodízio de tarefas para identificar ações mal-intencionadas.	Segurança física, defendendo a organização contra invasores que tentam acessar suas instalações; Segurança ambiental, protegendo a organização contra ameaças ambientais como inundações e incêndios.	Sistemas de auditoria e monitoração de sistemas; Programas antivírus; Ferramentas de verificação de integridade de sistemas.
Gerenciamento de riscos	Planejamento de resposta a incidentes, possibilitando rápida reação e recuperação de violações de segurança, minimizando o impacto e impedindo o alastramento a outros sistemas; Planejamento de continuidade dos negócios, permitindo que a organização se recupere de eventos catastróficos que afetam uma grande parte da infra-estrutura de TIC.		Ferramentas de administração de segurança de sistemas operacionais e aplicativos comerciais; Criptografia; Identificação de usuários e processos exclusivos; Proteções inerentes ao sistema, desenvolvidas dentro dos sistemas para proteger as informações nele processadas ou armazenadas.

Fonte: DILLARD, 2004, p. 6.

O resultado desta fase será entrada para o processo de mitigação de risco, onde os controles aqui recomendados serão avaliados, priorizados e executados.

2.2.9 Documentação dos Resultados

Convém que os resultados até então encontrados sejam formalmente documentados. Os dados coletados em todas as etapas do processo de avaliação de riscos servirão de apoio nas decisões gerenciais do negócio, na elaboração de políticas, procedimentos, orçamentos e mudanças operacionais e gerenciais dos sistemas.

O relatório de avaliação de riscos não possui a características de apontar erros e sim de sistematizar de maneira analítica os riscos inerentes ao negócio, justificando investimentos e reduzindo potenciais perdas ou danos. Seu conteúdo demonstra as ameaças e vulnerabilidades, a medida dos riscos identificados, e fornece recomendações

de controle que podem ser implantados pelo processo de mitigação de riscos. (STONEBURNER, 2002).

2.3 Mitigação de Riscos

A mitigação de riscos, sustentada por uma análise de custo-benefício, tem o encargo de analisar e priorizar os controles recomendados pelo processo de avaliação de riscos, além de planejá-los e pô-los em prática com o objetivo de eliminar ou reduzir eventos que possam causar impacto adverso aos negócios da organização (STONEBURNER, 2002).

2.3.1 Opções de Mitigação de Riscos

Os riscos podem ser tratados conforme as seguintes opções (ABNT, 2008):

- Ação de evitar risco: evitar o risco eliminando suas causas ou conseqüências;
- Redução do risco: limitar o risco através de controles que reduzam ou eliminam o impacto gerado pela exploração de uma vulnerabilidade;
- Retenção do risco: aplicar controles de correções tendo como base o conhecimento da vulnerabilidade, falha ou defeito;
- Transferência do risco: transferir o risco pelo uso de outras opções que compensam a perda. A transferência pode ser feita por um seguro que cubra as conseqüências do risco ou através da subcontratação de um parceiro cujo papel seria o de monitorar o ambiente de TIC e tomas medidas imediatas que impeçam dano ou prejuízo. Transfere-se a responsabilidade pelo gerenciamento do risco, mas não a responsabilidade legal pelas conseqüências.

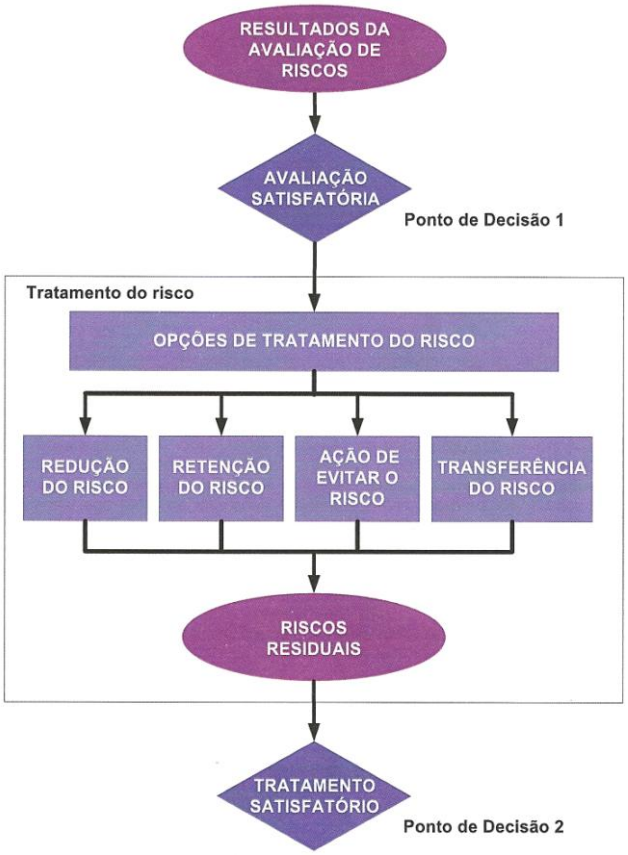


Figura 2.10: Atividade de tratamento de riscos (ABNT, 2008).

2.3.2 Fluxo para execução de Controles

As estratégias para tratar os riscos definem em quais as circunstâncias e quais controles devem ser utilizados para proteger a organização dos riscos. Prioriza-se a utilizando de controles sempre focando aqueles que deverão mitigar os riscos prioritários - de maior impacto e probabilidade – e com melhor relação custo-benefício.

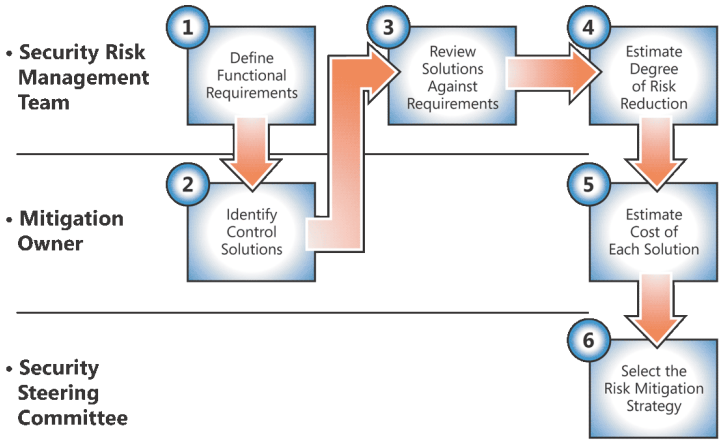


Figura 2.11: Visão geral da fase de suporte às decisões do *Security Risk Management Guide* (DILLARD, 2004).

A metodologia de mitigação de risco abaixo descreve uma abordagem de como uma organização pode proceder para escolher e utilizar controles (STONEBURNER, 2002):

2.3.2.1Priorização de Ações

Entrada: os níveis dos riscos definidos na etapa de avaliação de riscos.

Ação: organizar as ações, dando prioridade aos riscos cuja relação impacto/probabilidade seja significativa.

Saída: ações priorizadas, da maior para a menor prioridade.

2.3.2.2Validação das Opções de Controle Recomendadas

Entrada: os controles recomendados no processo de avaliação de riscos.

Ação: analisar a aplicabilidade e a efetividade dos controles recomendados e selecionar os que são mais apropriados para tratar os riscos.

Saída: lista dos controles aplicáveis.

2.3.2.3Realização de uma Análise de Custo-Benefício

Entrada: Lista de controles aplicáveis

Ação: realizar um estudo de viabilidade técnica e financeira para demonstrar o custo de desenvolvimento e utilização de controles, novos ou aprimorados, em quais circunstâncias eles poderiam ser utilizados e quais os impactos ao negócio caso se opte ou não por sua utilização.

Saída: relatório de viabilidade técnico-financeira dos controles aplicáveis.

2.3.2.4Seleção de Controles

Entrada: relatório de viabilidade financeira dos controles aplicáveis.

Ação: seleção dos controles que combinam elementos técnicos, operacionais e gerenciais, dentre os que possuem uma relação custo-benefício aceitáveis, e que garante a adequada segurança do ambiente de TIC.

Saída: controles selecionados.

2.3.2.5Delegação de Responsabilidades

Entrada: controles selecionados.

Ação: definir pessoas, internas ou externas a organização, conformes suas experiências e conhecimentos, para implantar e gerenciar os controles selecionados.

Saída: lista de responsáveis e seus respectivos controles.

2.3.2.6Desenvolvimento de um Plano de Ação

Entrada: riscos e seus respectivos níveis de risco, ações e suas respectivas priorizações, controles recomendados e selecionados, lista de responsáveis, data de início, previsão de conclusão, e condições de manutenção.

Ação: criar um plano de ação.

Saída: plano de ação de proteção.

2.3.2.7Implantar controles selecionados

Entrada: plano de ação de proteção.

Ação: implantar os controles selecionados conforme definido no planto de ação de proteção.

Saída: riscos residuais.

Os riscos residuais, resultantes da ação de controles aprimorados ou novos (redução de falhas ou defeitos, inclusão de dispositivos pontuais, redução da grandeza do impacto), devem ser analisados pela organização, nos termos de redução da probabilidade de ocorrência ou impacto da ação de ameaças, para serem aceitos (STONEBURNER, 2002)

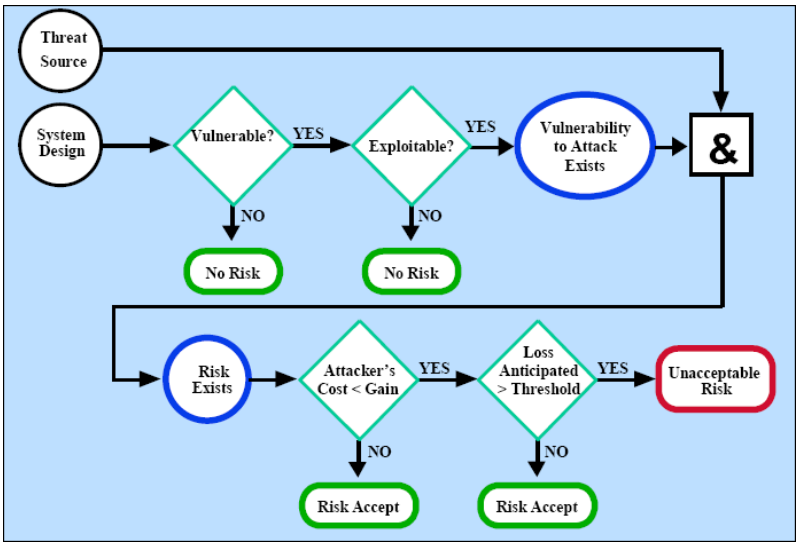


Figura 2.12: Exemplo de fluxo de aceitação de riscos (STONEBURNER, 2002).

Aceitar um risco, conforme critérios pré-definidos, pode ser mais complexo que uma mera indicação se ele está, ou não, dentro dos limites determinados. Em alguns casos, o risco residual pode não atender aos critérios de aceitação, mas a decisão de conformá-lo, ou não, pode ser influenciada por situações momentâneas, como por exemplo, a inviabilidade técnico-financeira da implantação de um controle. Diante de tais circunstâncias, cabem duas decisões: revisar os critérios de aceitação ou justificar de forma explícita a decisão de sobrepô-los (ABNT, 2008).

Convém que a decisão de aceite dos riscos seja realizada e formalmente registrada, constando os responsáveis e as justificativas de anuência de cada risco residual, em especial daqueles que não satisfaçam os critérios normais de aceitação (ABNT, 2008).

2.4 Análise e Melhoria Contínua

Em geral, o ambiente de tecnologia da informação e comunicação está em constante evolução dentro das empresas e isto significa que novos riscos, ou aqueles anteriormente tratados, podem afetar os negócios. Deste modo, gerenciamento de risco é um processo evolutivo, que requer melhorias contínuas durante o clico de vida de uma organização. Deve ter uma agenda específica, o qual deve ser preventivamente repetido, mas deve ser flexível o suficiente para ser executado sempre que grandes mudanças forem realizadas, as quais resultarão em novas políticas, novas tecnologias e por conseqüência novas vulnerabilidades (STONEBURNER, 2002).

A reavaliação periódica do ambiente através dos processos avaliação de riscos é o primeiro passo para se começar um novo ciclo. A equipe de gestão de riscos de segurança deve reutilizar e atualizar as listas de ativos, vulnerabilidades, controles e outras propriedades intelectuais desenvolvidas durante o projeto inicial de gerenciamento de riscos (DILLARD, 2004).

A equipe pode determinar onde se concentrar, reunindo informações atuais, precisas e relevantes sobre as alterações que afetam os sistemas de informações da organização. Os eventos internos que exigem uma apuração mais cuidadosa incluem a instalação de novos *hardwares* e *softwares* nos computadores; novos aplicativos desenvolvidos internamente; reorganizações corporativas; aquisições e fusões corporativas; bem como liquidações de partes da organização. Também é recomendável revisar a lista de riscos existente para determinar se houve alterações. Além disso, examinar os registros de auditoria de segurança pode trazer idéias sobre outras áreas a investigar (DILLARD, 2004).

Além disso, é necessário que se verifique se os critérios utilizados para medir o risco ainda são coerentes com os objetivos do negócio, estratégias e políticas da organização (ABNT, 2008).

O sucesso do gerenciamento de riscos irá depender do compromisso da alta direção, de total apoio e participação da equipe de tecnologia da informação e comunicação, da competência e da experiência do time de gestão de riscos em aplicar com efetividade a metodologia, da consciência e cooperação dos usuários em cumprir os procedimentos e da melhoria contínua na validação e estimativa dos riscos.

3 CONCLUSÃO

A dependência tecnológica das organizações nos tempos atuais fez com que um ramo da Governança Corporativa migrasse para dentro dos departamentos de informática. A sustentabilidade dos negócios através dos pilares da infra-estrutura tecnológica é incumbência da Governança de TIC, que tem no Gerenciamento de Riscos em Segurança em Segurança da Informação seu balizador de decisões e guia de ações de segurança.

O processo de gerenciamento de riscos em sistemas de tecnologia de informação e comunicação é responsabilidade direta da alta direção, que tem a missão de fazer com que organização atenda às expectativas da sociedade que dela depende.

O sucesso do ciclo de gerenciamento de riscos é subordinado intrínseco à cultura organizacional. São papeis dos acionistas o apoio e o fomento ao programa de gestão de riscos de segurança. Cada unidade de negócio, departamento e usuário é peça fundamental de um processo que necessita ser continuamente multiplicado e melhorado.

Este artigo focou-se em destacar, senão indicar, as boas práticas de gerenciamento de riscos disponíveis, e organizá-las de tal forma que possibilite sua aplicação dentro das organizações. Foram disponibilizadas, também, farta documentação de apoio nos ANEXOS e APÊNDICES, visando auxiliar às equipes de gestão de riscos.

REFERÊNCIAS

ABNT. **ABNT NBR ISO/EIC 27005:2008** : Tecnologia da Informação : Técnicas de Segurança : Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2008.

ABNT. **ABNT NBR ISO/IEC 27002:2005** : Tecnologia da Informação : Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005.

ABNT. **ABNT NBR ISO/IEC 27001:2006** : Tecnologia da Informação : Técnicas de Segurança da Informação : Sistemas de Gestão de Segurança da Informação : Requisitos. Rio de Janeiro, 2006.

ADLER, M. et al. **COBIT® 4.1**. Rolling Meadows: IT Governance Institute, 2007. 213 p. Disponível em: <http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=39279>. Acesso em: nov. 2008.

ALBERTS, C. et al. **Introduction to the OCTAVE® Approach**. Pittsburgh: Carnegie Mellon University, 2003. 37 p. Disponível em: <www.cert.org/octave/approach_intro.pdf>. Acesso em: nov. 2008.

BARTLETT, J. et. al. **ITIL® Service Delivery v.2.0**. Norwich: TSO - The Stationery Office, 2003.

BROEKARTS, A. et al. **Microsoft Operations Framework (MOF) 4.0**. [S.l.]: Microsoft Corporation, 2008. Disponível em: <http://technet.microsoft.com/en-us/library/cc506049.aspx>. Acesso em: nov. 2008.

CERT.BR. **Cartilha de Segurança para Internet, versão 3.1**. São Paulo, 2006. 117 f. Disponível em: <http://cartilha.cert.br/download/ cartilha-seguranca-internet.pdf>. Acesso em: nov. 2008.

DILLARD, K.; PFOST, J.; RYAN, S. **Security Risk Management Guide**. [S.l.]: Microsoft Corporation, Oct. 2004. Disponível em: <http://technet.microsoft.com/en-us/library/cc163143.aspx>. Acesso em: out. 2008.

FAGUNDES, E. **COBIT® Um kit de ferramentas para a excelência na gestão de TI**. [S.l.: s.n.], 2004. 6 f. Disponível em: <http://www.efagundes.com/Artigos/Arquivos_pdf/ cobit.pdf>. Acesso em: out. 2008.

GULDENTOPS, E. et al. **Board Briefing on IT Governance**. 2nd ed. Rolling Meadows: ITGI - IT Governance Institute, 2003. 66 p. Disponível em: <http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=39649>. Acesso em: nov. 2008.

HARDY, G. et al. **Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit**. Rolling Meadows: ITGI - IT Governance Institute, 2008. 131 p. Disponível em: <

http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=46288 >. Acesso em: nov. 2008.

LA ROCQUE, E. et al. **Guia de Orientação para o Gerenciamento de Riscos Corporativos**. São Paulo: IBGC – Instituto Brasileiro de Governança Corporativa, 2007. 48 f. (Série de Cadernos de Governança Corporativa 3). Disponível em: <http://www.audicaixa.org.br/arquivos_auditoria/GerenciamentoRiscosCorporativos-IBGC.pdf >. Acesso em: nov. 2008.

MICHAELIS: moderno dicionário da Língua Portuguesa. São Paulo: Melhoramentos, 1998. Dicionário eletrônico Babylon 6.0.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. **Risk Management Guide for Information Technology Systems.** Gaithersburg: NIST - National Institute of Standards and Technology**,** July 2002. 54 p. (Special Publication 800-30). Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. Acesso em: out. 2008.

GLOSSÁRIO

Ação de evitar risco: decisão de não se envolver ou agir de forma a se retirar de uma situação de risco.

Aceitação do risco: decisão de aceitar o risco residual.

Análise de risco: uso sistemático de informações para autenticar fontes e estimar o risco.

Antivírus: programa ou software especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.o sigilo de comunicações pessoais e comerciais

Ataque: tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques as tentativas de negação de serviço.

Ativo: qualquer coisa que tenha valor par a organização.

***Blackouts*:** falha na geração de energia elétrica.

Boato: e-mail que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente ou aponta como autora da mensagem alguma instituição, empresa importante ou órgão governamental. Através de uma leitura minuciosa deste tipo de e-mail, normalmente, é possível identificar em seu conteúdo mensagens absurdas e muitas vezes sem sentido.

***Bot*:** programa que, além de incluir funcionalidades de worms, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o bot, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar spam, etc.

***Botnets*:** redes formadas por diversos computadores infectados com bots. Podem ser usadas em atividades de negação de serviço, esquemas de fraude, envio de spam, etc.

Cavalo de tróia: programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Código malicioso: termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms*, *bots*, cavalos de tróia, *rootkits*, etc.

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

Criptografia: ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais

DDoS: do inglês *Distributed Denial of Service*. Ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.

Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

Engenharia social: método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Estimativa de riscos: processo utilizado para atribuir valores à probabilidades e conseqüências de um risco.

***Exploit*:** programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um software de computador.

Identificação de riscos: processo para localizar, listar e caracterizar elementos do risco.

IDS: do inglês *Intrusion Detection System*. Programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

Impacto: mudança adversa no nível obtido dos objetivos de negócio

Incidente de segurança: um único ou uma série de eventos indesejados ou inesperados que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Integridade: propriedade de salvaguarda da exatidão e completeza de ativos.

Invasão: ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

IP *spoofing*: técnica que consiste em mascarar (spoof) pacotes IP utilizando endereços de remetentes falsificados.

ITIL – Information Technology Infrastructure Library: conjunto de melhores práticas para o Gerenciamento de Serviços de TIC. O ITIL foi desenvolvido no final dos anos 80 pela Central Computer and Telecommunications Agency (CCTA, hoje OGC), órgão do Governo Britânico. A criação foi motivada pela insatisfação com o custo e a qualidade dos serviços de TI fornecidos ao Governo Britânico, pela dependência crítica dos serviços de TI e pela necessidade de independência de fornecedores.

***Malware*:** do inglês *malicious software*, veja código malicioso.

Negação de serviço: atividade maliciosa onde o atacante utiliza um computador para tirar de operação um serviço ou computador conectado à Internet.

NIST – National Institute of Standards and Technology: fundada em 1901, NIST é uma agência federal não-reguladora ligada ao Departamento de Comércio Norte

Americano que tem como missão promover a competitividade e a inovação industrial americana através de avanços científicos, padrões e tecnologias para melhorar a economia e qualidade de vida.

***Phishing*:** também conhecido como *phishing scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros ou à instalação de códigos maliciosos.

Redução do risco: ações tomadas para reduzir a probabilidade, as conseqüência negativas, ou ambas, associadas a um risco.

Retenção do risco: aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco. No contexto dos riscos da segurança da informação, somente as conseqüência negativas são consideradas.

Risco residual: riscos remanescentes após o tratamento de riscos.

Riscos de segurança da informação: a possibilidade de uma ameaça explorar vulnerabilidades de recursos num ambiente de TIC de forma que venha a prejudicar a organização.

***Rootkit*:** conjunto de programas que tem como finalidade esconder e assegurar a presença de um invasor em um computador comprometido.

Segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade.

Transferência do risco: compartilhamento com outra entidade do ônus da perda ou benéfico do ganho associado a um risco. No contexto dos riscos da segurança da informação, somente as conseqüência negativas são consideradas.

Tratamento do risco: processo de seleção e implementação de medidas para modificar um risco.

Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

Vulnerabilidade: falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

***Worm*:** programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

ANEXO A EXEMPLOS DE AMEAÇAS COMUNS

A Tabela A.1 contém exemplos de ameaças típicas que pode ser utilizada no processo de avaliação de ameaças. Ameaças podem ser: (I) intencionais, que indica as ações intencionais direcionadas contra os ativos da informação; (A) acidentais, que indica as ações de origem humana que podem comprometer acidentalmente e os ativos da organização; ou de origem (N) natural ou ambiental, que indica incidentes que não são provocados pela ação dos seres humanos (ABNT, 2008):

Tabela A.1: Exemplos de ameaças comuns

Tipo	Ameaça	Origem
Dano Físico	Fogo	A, I, N
	Água	A, I, N
	Poluição	A, I, N
	Acidente grave	A, I, N
	Destruição de equipamento ou mídia	A, I, N
	Poeira, corrosão ou congelamento	A, I, N
Eventos naturais	Fenômeno climático	N
	Fenômeno sísmico	N
	Fenômeno vulcânico	N
	Fenômeno meteorológico	N
	Inundação	N
Paralisação de serviços essenciais	Falha do condicionador de ar	A, I
	Interrupção no suprimento de energia	A, I, N
	Falha do equipamento de telecomunicações	A, I
Distúrbio causado por radiação	Radiação eletromagnética	A, I, N
	Radiação térmica	A, I, N
	Pulsos eletromagnéticos	A, I, N
Comprometimento da informação	Interceptação de sinais	I
	Espionagem à distância	I
	Escuta não autorizada	I
	Furto de mídia ou documentos	I
	Furto de equipamentos	I
	Recuperação de mídia reciclada ou descartada	I
	Divulgação indevida	A, I
	Dados de fones não confiáveis	A, I
	Alteração do *hardware*	I
	Alteração do *software*	A, I
	Determinação da localização	I

Falhas técnicas	Falha de equipamento	A
	Defeito de equipamento	A
	Saturação do sistema de informação	A, I
	Defeito de *software*	A
	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	A, I
Ações não autorizadas	Uso não autorizado de equipamento	I
	Cópia ilegal de *software*	I
	Uso de cópias de *software* falsificadas ou ilegais	A, I
	Comprometimento dos dados	I
	Processamento ilegal dos dados	I
Comprometimento de funções	Erro durante o uso	A
	Forjamento de direitos	A, I
	Abuso de diretos	I
	Repúdio de ações	I
	Indisponibilidade de recursos humanos	A, I, N

Fonte: ABNT, 2008, p. 39-40.

A Tabela A.2 representa fontes de ameaças representadas por seres humanos, motivações e suas possíveis conseqüências (ABNT, 2008):

Tabela A.2: Exemplos de ameaças causadas por seres humanos

Fontes de ameaça	**Motivação**	**Possíveis Conseqüências**
Hacher, cracker	Desafio Egocentrismo Protesto Rebeldia *Status* Dinheiro	• *Hacking*; • Engenharia social; • Negação de serviço; • Pichação de *sites*; • Invasão de sistemas, infiltrações; • Acesso não autorizado.
Criminosos digitais	Destruição de informações Acesso a dados sigilosos Divulgação ilegal de informações Ganho monetário Alterações não autorizadas de dados	• Atos virtuais fraudulentos (interceptação de dados, ataque homem-no-meio, IP *spoofing*, etc.); • Intrusão de sistemas. • Suborno por informação; • Ataques a sistemas (negação de serviço);
Terroristas	Chantagem Destruição Vingança Exploração Ganho político	• Ataques com bombas; • Guerra de informação; • Ataques a sistemas (negação de serviço distribuído);

	Cobertura da mídia	• Invasão e dominação de sistemas; • Alteração de sistemas.
Espiões	Vantagem competitiva Espionagem econômica	• Garantir vantagem de um posicionamento defensivo; • Garantir uma vantagem política; • Exploração econômica; • Furto de informações; • Violação da privacidade das pessoas; • Engenharia social; • Invasão de sistemas; • Invasão de privacidade; • Acessos não autorizados em sistemas (acesso a informação restrita, de propriedade exclusiva, e/ou relativa à tecnologia).
Pessoas: mal treinadas, insatisfeitas, mal-intencionadas, negligentes, imprudentes, desonestas, demitidas.	Curiosidade Egocentrismo Informações para serviço de Inteligência Ganhos financeiros Vingança Ações não intencionais ou omissões (erro na entrada de dados, erro na programação).	• Agressão a funcionário; • Chantagem; • Busca de informação sensível; • Abuso dos recursos computacionais; • Fraudes; • Furto de ativos; • Suborno de informação; • Inclusão de dados falsos; • Corrupção de dados; • Interceptação de informação; • Desvio de informação; • Uso de programas ou códigos maliciosos; • Sabotagens; • Invasão de sistemas; • Acessos não autorizados a sistemas.

Fonte: ABNT, 2008, p. 40-41.

ANEXO B EXEMPLOS DE VULNERABILIDADES

A Tabela B.1 fornece exemplos de vulnerabilidades e possíveis ameaças em diversas áreas de segurança e pode servir de auxílio durante o processo de avaliação das ameaças e vulnerabilidades do ambiente de TIC (ABNT, 2008).

Tabela B.1: Exemplos vulnerabilidades

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Hardware	Manutenção insuficiente ou instalação defeituosa de mídia de armazenamento	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia
	Sensibilidade à umidade, poeira ou sujeira	Poeira, corrosão, congelamento.
	Sensibilidade à radiação eletromagnética	Radiação eletromagnética
	Inexistência de um controle de mudanças de configuração	Erro durante o uso
	Sensibilidade a variações de voltagem	Interrupção do suprimento de energia
	Sensibilidade a variações de temperatura	Fenômeno meteorológico
	Armazenamento não protegido	Furto de mídia ou documentos
	Descuidado durante o descarte	Furto de mídia ou documentos
	Utilização de cópias não controladas	Furto de mídias ou documentos
Software	Inexistência de procedimentos de teste de *softwares*.	Abuso de direitos
	Falhas conhecidas no *software*	Abuso de diretos
	Não execução do "*logout*" ao se deixar uma estação de trabalho	Abuso de direitos
	Descarte ou reutilização de mídia de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados	Abuso de direitos

	Inexistência de uma trilha de auditoria	Abuso de direitos
	Atribuição errônea de direitos de acesso	Abuso de diretos
	Software amplamente distribuído	Comprometimento dos dados
	Utilizar programas aplicativos com um conjunto errado de dados	Comprometimento dos dados
	Interface de usuário complexa	Erro durante uso
	Inexistência de documentação	Erro durante uso
	Parâmetros Incorretos	Erro durante uso
	Datas incorretas	Erro durante uso
Rede	Inexistência de mecanismos de autenticação e identificação	Forjamento de direitos
	Tabelas de senhas desprotegidas	Forjamento de diretos
	Gerenciamento mal feito de senhas	Forjamento de direitos
	Serviços desnecessários habilitados	Processamento ilegal de dados
	Software novo ou imaturo	Defeito de *software*
	Especificações confusas o incompletas para os desenvolvedores	Defeito de *software*
	Inexistência de um controle eficaz de mudança	Defeito de *software*
	Download e uso não controlado de *software*	Alteração do *software*
	Inexistência de cópias de segurança	Alteração do *software*
	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de mídia ou documentos
	Inexistência de relatórios de gerenciamento	Uso não autorizado de equipamento
	Inexistência de evidências que comprovem o envio ou recebimento de mensagens	Repúdio de ações
	Linhas de Comunicação desprotegidas	Escuta não autorizada
	Tráfego sensível desprotegido	Escuta não autorizada
	Junções de cabeamento mal feitas	Falha do equipamento de telecomunicação
	Ponto único de falha	Falha do equipamento de telecomunicação
	Não identificação e não autenticação do emissor ou receptor	Forjamento de diretos
	Arquitetura insegura da rede	Espionagem à distância
	Transferências de senhas em claro	Espionagem a distância
	Gerenciamento de rede inadequado, quanto à configuração de roteamentos	Saturação do sistema de informação
	Conexões de redes públicas desprotegidas	Uso não autorizado de equipamento
Recursos humanos	Ausência de recursos humanos	Indisponibilidade de recursos humanos

	Procedimentos de recrutamento inadequados	Indisponibilidade de recursos humanos
	Treinamento insuficiente em segurança	Erro durante o uso
	Uso incorreto de *software* e *hardware*	Erro durante o uso
	Falta de conscientização em segurança	Erro durante o uso
	Inexistência de mecanismos de monitoramento	Processamento ilegal dos dados
	Trabalho não supervisionado de pessoal de limpeza ou de terceirizados	Furto de mídia ou documentos
	Inexistência de políticas pra o uso correto de meios de telecomunicação e de troca de mensagens	Uso não autorizado de recurso
Local ou instalações	Uso inadequado de mecanismos de controle de acesso físico a locais sensíveis	Destruição de equipamento ou mídia
	Localização em área suscetível a inundações	Inundação
	Fornecimento de energia instável	Interrupção de suprimento de energia
	Inexistência de mecanismos de proteção física no prédio portas e janelas	Furto de equipamentos
Organização	Inexistência de um procedimento formal para o registro de remoção de usuários	Abuso de direitos
	Inexistência de processo formal para a análise crítica dos direitos de acesso	Abuso de direitos
	Provisões de segurança insuficientes o inexistentes em contratos com clientes e/ou terceiros	Abuso de direitos
	Inexistência de procedimentos de monitoramento das instalações de processamento de informações	Abuso de direitos
	Inexistência de auditorias periódicas	Abuso de direitos
	Inexistência de procedimentos para a identificação e análise/avaliação de riscos	Abuso de direitos
	Inexistência de relatos de falha nos arquivos de auditoria das atividades de administradores e operações	Abuso de direitos
	Resposta inadequada do serviço de manutenção	Violação das condições de uso do sistema de informação
	Acordo de nível de serviço (SLA) inexistência ou ineficaz	Violação das condições de uso do sistema de informação
	Controle de mudanças inexistente ou ineficaz	Violação das condições de uso do sistema de informação

	Procedimento e controle de sistemas de gerenciamento de segurança inexistentes	Comprometimento dos dados
	Atribuição inadequada das responsabilidades pela segurança da informação	Repúdio de ações
	Plano de continuidade de serviços inexistente	Falha nos serviços
	Política de uso de e-mail inexistente	Erro durante o uso
	Ausência de registros de auditoria (logs)	Erro durante o uso
	Processo disciplinar no caso de incidentes de segurança inexistente	Furto de equipamentos ou dados
	Política de uso de recursos de informática inexistente	Furto de equipamentos ou dados
	Inexistência de controle de ativos fora da organização	Furto de equipamentos ou dados
	Inexistência de procedimentos de direitos de propriedade intelectual	Uso de cópias de aplicativos falsificadas ou ilegais.

Fonte: ABNT, 2008, p. 42-45.

ANEXO C CONTROLES E OBJETIVOS DE CONTROLES

Este anexo apresenta uma relação não exaustiva de controles e objetivos de controles que podem ser utilizados no gerenciamento de segurança da informação de uma organização de forma preventiva contra riscos aos negócios.

Tabela C.1: Controles e objetivos de controles

POLÍTICA DE SEGURANÇA	
Política de segurança da informação	
Objetivo: prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.	
Documento da política de segurança da informação	*Controle* Um documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunidades para todos os funcionários e partes externas relevantes. O documento dever ser analisado criticamente a intervalos planejados ou quando mudanças significativas ocorrerem.
ORGANIZANDO A SEGURANÇA DA INFORMAÇÃO	
Infra-estrutura da segurança da informação	
Objetivo: gerenciar a segurança da informação dentro da organização.	
Compromisso da direção com a segurança da informação	*Controle* A direção deve apoiar ativamente a segurança da informação dentro da organização, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação.
Acordos de confidencialidade	*Controle* Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação devem ser identificados e analisados criticamente, de forma regular.
GESTÃO DE ATIVOS	

Responsabilidades pelos ativos	
Objetivo: alcançar e manter a proteção adequada dos ativos da organização.	
Inventário dos ativos	*Controle* Todos os ativos devem ser claramente identificados e um inventário de todos os ativos importantes deve ser estruturado e mantido.
Classificação da informação	
Objetivo: assegurar que a informação receba um nível adequado de proteção.	
Recomendações de classificação	*Controle* A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.
SEGURANÇA EM RECURSOS HUMANOS	
Antes da contratação	
Objetivo: assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidade e estejam de acordo com os seus papéis para reduzir o risco de roubos, fraude ou mal uso de recursos.	
Papéis e responsabilidades	*Controle* Os papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros devem ser definidos e documentados de acordo com a política de segurança da informação da organização.
Termos e condições de contratação	*Controle* Como parte das suas obrigações contratuais, os funcionários, fornecedores e terceiros devem concordar e assinar os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidades e da organização para a segurança da informação.
Durante a contratação	
Objetivo: assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação durante seus trabalhos para reduzir riscos operacionais.	
Responsabilidades da direção	*Controle* A direção deve solicitar aos funcionários, fornecedores e terceiros que pratiquem a segurança da informação de acordo com o que foi definido nas políticas e procedimentos da organização.
Conscientização, educação e	*Controle* Todos os funcionários, e onde quando pertinente

treinamento	fornecedores e terceiros, devem receber treinamentos de conscientização das políticas e procedimentos organizacionais, inclusive quando estas são atualizadas.
Processo disciplinar	*Controle* Deve existir um processo disciplinar formal para os funcionários que tenham cometido uma violação de segurança da informação.

Encerramento ou mudança da contratação

Objetivo: assegurar que os funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.

Encerramento de atividades	*Controle* A responsabilidade para realizar o encerramento ou a mudança de um trabalho devem ser claramente definidas e atribuídas.
Devolução de ativos	*Controle* Todos os funcionários, fornecedores e terceiros devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.
Retirada de direitos de acesso	*Controle* O direto de acesso de todos os funcionários, fornecedores e terceiros às informações e recursos devem ser retirados após o encerramento das atividades, contratos ou acordos, ou devem ser ajustados conforme as novas atividades.

SEGURANÇA FÍSICA E DO AMBIENTE

Áreas seguras

Objetivo: prevenir acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

Controle de entrada física	*Controle* As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.
Proteção contra ameaças externas e do meio ambiente	*Controle* Devem ser projetadas e aplicadas proteções físicas contra incêndio, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.

Segurança de equipamentos

Objetivo: impedir perdas, danos, furto ou comprometimento de ativos e

interrupção das atividades da organização.

Utilidades	*Controle* Os equipamentos devem ser protegidos contra falta de energia e outras interrupções causadas por falhas das utilidades.
Segurança do cabeamento	*Controle* O cabeamento de energia e telecomunicações devem ser protegidos contra interrupções e danos.

Planejamento e aceitação dos sistemas

Objetivo: minimizar o risco de falhas nos sistemas.

Aceitação de sistemas	*Controle* Devem ser estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões, seguidos de testes antes da validação.

CONTROLES DE ACESSO

Computação móvel e trabalho remoto

Objetivo: garantir a segurança da informação quando utilizadas tecnologias de computação móvel e recursos de trabalho remoto.

Trabalho remoto	*Controle* Uma política, planos operacionais e procedimentos devem ser desenvolvidos para atividades de trabalho remoto.

Controle de acesso ao sistema operacional

Objetivo: prevenir acesso não autorizado aos sistemas operacionais.

Sistema de gerenciamento de senhas	*Controle* Sistemas de gerenciamento de senhas devem ser interativos e garantir senhas de qualidade.
Desconexão por inatividade	*Controle* Terminais inativos devem ser desconectados após período definido de inatividade.

Gerenciamento de acesso ao usuário

Objetivo: assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.

Análise crítica dos direitos de acesso	*Controle* O gestor deve conduzir a intervalos regulares a análise crítica dos direitos de acesso dos usuários por meio de um processo formal.

Fonte: ABNT, 2006, p. 14-30.

APÊNDICE A ORGANIZAÇÕES DE RESPOSTA A INCIDENTES DE SEGURANÇA

Este APÊNDICE fornece exemplos de organizações públicas e privadas que tem como objetivo receber, analisar, registrar e responder a incidentes de segurança envolvendo redes conectadas à Internet no mundo, e que poderão servir de referências para pesquisas de vulnerabilidades em sistemas.

Estas organizações exercem atividades como: atendimento a incidentes de segurança; coordenação de grupos de segurança novos ou já existentes; disseminação de informações na área de segurança em redes; divulgação de recomendações e alertas; testes e recomendação de ferramentas de segurança; estabelecimento de trabalho colaborativo com outras entidades, como as polícias, provedores de acesso e serviços de Internet e *backbones*; oferecimento treinamentos na área de resposta a incidentes de segurança; entre outros. Abaixo, segue uma lista não exaustiva contendo o nome e suas respectivas URL's, acessadas em novembro de 2008:

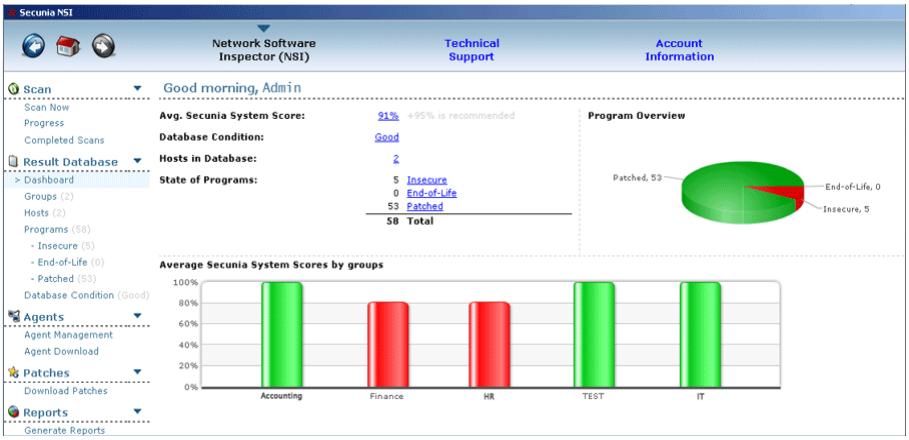
- CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil <www.cert.br>
- US-CERT - United States Computer Emergency Readiness Team <http://www.us-cert.gov>
- CAIS - Centro de Atendimento a Incidentes de Segurança <http://www.rnp.br/cais>
- SecurityFocus - The Largest Community of Security Professionals Available Anywhere <http://www.securityfocus.com>
- National Vulnerability Database <http://nvd.nist.gov>
- Common Vulnerabilities and Exposures <http://cve.mitre.org>
- Secunia <http://www.secunia.com>

APÊNDICE B FERRAMENTAS DE AUDITORIA DE SEGURANÇA EM SISTEMAS

As ferramentas de auditoria de segurança, ou simplesmente testes de segurança, são métodos proativos que podem identificar eficazmente vulnerabilidades conhecidas. Dentre as diversas soluções do mercado, são apresentadas a seguir duas opções deste tipo de ferramenta que podem ser úteis para detectar vulnerabilidade em ambientes de TIC:

Network Software Inspector - SNI, do Secunia, possibilita segurança completa do ambiente e visão geral das atualizações críticas dos sistemas da corporação. Localiza as vulnerabilidades que afetam a infra-estrutura, e fornece uma definição detalhada e concisa das vulnerabilidades e ameaças relacionadas <http://secunia.com/vulnerability_scanning/network>.

Program	Version	State	SA ID	Criticality	Issued	Vulnerabilities
Mozilla Thunderbird 1.5.x	1.5		SA28179	Highly critical	137 days ago	5
Skype for Windows 3.x	3.2.0.145		SA28791	Highly critical	89 days ago	0
Adobe Reader 8.x	8.1.0.137		SA28802	Highly critical	89 days ago	7
Opera 9.x	9.22		SA29662	Highly critical	32 days ago	2
ZoneAlarm 6.x	6.5.700.000		-	End-of-Life	-	0
Microsoft Windows Messenger 4.x	4.7.0.3001		-	-	-	0
Sun Java JRE 1.6.x / 6.x	6.0.50.13		-	-	-	0
Sun Java JRE 1.6.x / 6.x	6.0.50.13		-	-	-	0
Mozilla Firefox 2.0.x	2.0.0.14		-	-	-	0
Microsoft XML Core Services 3.x	8.90.1101.0		-	-	-	0
Yahoo! Messenger 8.x	8.1.0.421		-	-	-	0
Microsoft Windows Media Player 5.x	5.1.2600.2180		-	-	-	0
Adobe Flash Player 9.x	9.0.124.0		-	-	-	0
OpenOffice.org 2.x	2.3.9280.500		-	-	-	0
Microsoft Windows Media Player 6.x	6.4.9.1125		-	-	-	0
Microsoft Data Access Components (MDAC) 2.x	2.81.1128.0		-	-	-	0
ZoneAlarm Pro 6.x	6.5.700.0		-	-	-	0
Microsoft Internet Explorer 6.x	6.00.2900.2180		-	-	-	0
Adobe Help Viewer 1.x	1.0.0.185		-	-	-	0
Sysinternals Regmon 7.x	7.4.0.0		-	-	-	0
Microsoft Movie Maker 2.x	2.1.4026.0		-	-	-	0
7-Zip 4.x	4.57.0.0		-	-	-	0



Nessus®, da Tenable Network Security, é a ferramenta de detecção de vulnerabilidades caracterizada pela alta velocidade de detecção, auditorias na configuração de sistemas, perfis de ativos, descoberta de dados sensíveis e análise de vulnerabilidade do ambiente de TIC. Pode ser distribuído por toda a empresa, dentro de DMZ's e em redes fisicamente separadas < http://www.nessus.org/nessus>: