**UNIVERSIDADE FEDERAL DE SANTA MARIA**
**CENTRO DE TECNOLOGIA**
**PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO**

# GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO BASEADA NA NORMA NBR ISO/IEC 27005 USANDO PADRÕES DE SEGURANÇA

**DISSERTAÇÃO DE MESTRADO**

**Marcos Paulo Konzen**

**Santa Maria, RS, Brasil**
**2013**

# GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO BASEADA NA NORMA NBR ISO/IEC 27005 USANDO PADRÕES DE SEGURANÇA

**Marcos Paulo Konzen**

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-Graduação em Engenharia de Produção, Área de concentração em Gerência de Produção, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Mestre em Engenharia de Produção**.

Orientador: Prof. Dr. Raul Ceretta Nunes

Santa Maria, RS, Brasil
2013

Ficha catalográfica elaborada através do Programa de Geração Automática
da Biblioteca Central da UFSM, com os dados fornecidos pelo(a) autor(a).

Konzen, Marcos Paulo
Gestão de Riscos de Segurança da Informação Baseada na Norma NBR ISO/IEC 27005 Usando Padrões de Segurança / Marcos Paulo Konzen.-2013.
119 p.; 30cm

Orientador: Raul Ceretta Nunes
Dissertação (mestrado) - Universidade Federal de Santa Maria, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia de Produção, RS, 2013

1. Gestão de Riscos 2. Padrões de Segurança 3. Normas de Segurança I. Nunes, Raul Ceretta II. Título.

**Universidade Federal de Santa Maria**
**Centro de Tecnologia**
**Programa de Pós-Graduação em Engenharia de Produção**

A Comissão Examinadora, abaixo assinada,
aprova a Dissertação de Mestrado

# GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO BASEADA NA NORMA NBR ISO/IEC 27005 USANDO PADRÕES DE SEGURANÇA

elaborada por
**Marcos Paulo Konzen**

como requisito parcial para obtenção do grau de
**Mestre em Engenharia de Produção**

## COMISSÃO EXAMINADORA:

**Raul Ceretta Nunes, Dr.**
(Presidente/Orientador)

**Lisandra Manzoni Fontoura, Dra.** (UFSM)

**Marco Antônio Sandini Trentin, Dr.** (UPF)

**Ana Trindade Winck, Dra.** (UFSM)

Santa Maria, 26 de Fevereiro de 2013.

# AGRADECIMENTOS

Agradeço, primeiramente, a Deus, pela saúde, sabedoria, força e determinação para enfrentar mais este desafio. Agradeço, também, por estar ao meu lado nos momentos difíceis e por proporcionar momentos de experiências e amizades adquiridas durante o curso.

Ao professor Raul Ceretta Nunes, um agradecimento especial pela acolhida e disposição em orientar este trabalho, pelo incentivo e pelas inestimáveis considerações.

Aos colegas do PPGEP, pela troca de experiências e saberes e pela amizade conquistada. Aos professores, em especial à professora Lisandra Manzoni Fontoura, que de forma direta contribuiu com suas considerações para o desenvolvimento deste trabalho.

À Universidade Federal de Santa Maria, por proporcionar uma estrutura de qualidade que contribuiu muito para mais uma etapa de aprendizado.

Aos meus pais, Egon e Nelsi, que me ensinaram os valores da vida, que sempre me apoiam e me incentivam em todas as caminhadas, sem vocês a realização desta etapa não seria possível. Aos meus irmãos, Fernando e Ângela, e aos meus amigos e familiares que sempre me incentivaram e me apoiaram nesta caminhada.

À minha noiva, Julice, pelo apoio incondicional em todas as horas, pela compreensão, pelo amor e por não me deixar desanimar nas horas mais difíceis.

Agradeço, também, aos professores da banca examinadora, pelo aceite do convite e pelas contribuições para o aprimoramento do trabalho.

# RESUMO

Dissertação de Mestrado
Programa de Pós-Graduação em Engenharia de Produção
Universidade Federal de Santa Maria

## GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO BASEADA NA NORMA NBR ISO/IEC 27005 USANDO PADRÕES DE SEGURANÇA

AUTOR: Marcos Paulo Konzen
ORIENTADOR: Prof. Dr. Raul Ceretta Nunes
Data e local da Defesa: Santa Maria, 26 de Fevereiro de 2013.

Nos últimos anos, cada vez mais novas ameaças e vulnerabilidades surgem comprometendo a segurança das informações em sistemas de Tecnologia da Informação e Comunicações (TIC), e muitas organizações encontram-se despreparadas para lidar com os riscos de segurança da informação, tornando-as mais vulneráveis às ameaças, e os impactos negativos causados pelos incidentes de segurança tendem a ser mais frequentes. A implantação de uma gestão de riscos de segurança da informação baseada no conjunto das melhores práticas é fundamental, porém ainda um desafio para a maioria das empresas. **Este trabalho** propõe uma metodologia de gestão de riscos baseada na norma NBR ISO/IEC 27005:2008, que apresenta uma sequência de atividades e uma série de diretrizes e objetivos que devem ser alcançados para que o gerenciamento dos riscos seja efetivo. Como na maioria das normas e modelos de referência, elas não descrevem como as atividades devem ser implementadas, o que acaba dificultando a sua adoção por organizações menos experientes em processos de segurança. A reutilização de soluções já testadas e consolidadas para resolver problemas recorrentes de segurança pode auxiliar na garantia de utilização de melhores práticas. Estas soluções podem ser encontradas em padrões de segurança que capturam e documentam o conhecimento de especialistas em segurança, mas se desconhece a sua aplicação para desenvolver atividades das normas de gestão de riscos. Desta forma, **este trabalho** faz uma revisão das diretrizes da norma NBR ISO/IEC 27005:2008 e de catálogos de padrões, a fim de identificar padrões de segurança para desenvolver as atividades de acordo com as diretrizes descritas pela norma. Portanto, **a principal contribuição deste trabalho** é o desenvolvimento de uma metodologia de gestão de riscos centrada em soluções, tarefas e técnicas descritas por 22 padrões de segurança. Uma análise e avaliação de riscos utilizando padrões de segurança foi aplicada em um CPD de uma instituição privada de ensino superior, cujo resultado mostra o risco final de cada ativo, atendendo as diretrizes da norma NBR ISO/IEC 27005:2008.

**Palavras-chave:** Gestão de riscos; Padrões de segurança; Normas de segurança.

# ABSTRACT

Master's Degree Dissertation
Graduate Program in Production Engineering
Federal University of Santa Maria

## RISK MANAGEMENT OF INFORMATION SECURITY BASED ON STANDARD NBR ISO/IEC 27005 USING SECURITY PATTERNS

AUTHOR: Marcos Paulo Konzen
ADVISER: Raul Ceretta Nunes
Date and place of defense: Santa Maria, February 26th, 2013.

In the last years more vulnerabilities and threats have emerged, compromising information security in Information and Communication Technology (ICT) systems. In addition, many organizations are unprepared to deal with the risks of information security, making them the most vulnerable to such threats. Thus the negative impact caused by security incidents tends to be more frequent. The implementation of information security risk management based on a set of best practices is critical, but still a challenge for most companies. This work proposes a methodology for managing risks based on NBR ISO/IEC 27005:2008. The methodology presents a sequence of activities and a series of guidelines and goals that must be achieved to make the risk management effective. As with most standards and reference models, the methodology does not describe how activities should be implemented, which makes it difficult to implement for organizations less experienced in security procedures. The reuse of solutions already tested and consolidated to recurring security problems it can assist in ensuring the use of best practices. These solutions can be found in security standards that capture and document the knowledge of security experts, but its application to develop standards for risk management activities is unknown. Thus, this work reviews the guidelines of NBR ISO/IEC 27005:2008 standards and pattern catalogs in order to identify security patterns to develop activities in accordance with the guidelines described by the standard. Therefore, the main contribution of this work is to develop a methodology for risk management centered in solutions, tasks and techniques described by 22 security standards. An analysis and risk assessment using security standards was applied to a DC (Data Center) of a private university, whose result shows the final risk for each asset, meeting the guidelines of NBR ISO/IEC 27005:2008.

**Keywords:** risk management; security patterns; security standards.

# LISTA DE FIGURAS

Figura 1- Gestão de Riscos segundo as Normas AS/NZ 4360 e NBR ISO 31000.....31

Figura 2 - Processo de gestão de riscos de segurança da informação. .....32

Figura 3- Alinhamento do ciclo PDCA com o processo de Gestão de Riscos.....33

Figura 4- A atividade de tratamento do risco. .....39

Figura 5 - *Security Needs Identification for Enterprise Assets*. .....50

Figura 6 - Processo de identificação de padrões de segurança.....57

Figura 7 – Diagrama de desenvolvimento das atividades. .....61

Figura 8 – Diagrama de implementação da análise e avaliação de riscos.....77

Figura 9 – Gráfico da pontuação do risco final de cada ativo. .....101

Figura 10 – Pontuação do risco de cada serviço.....104

# LISTA DE QUADROS

Quadro 1- Grupos de controles e objetivos de controle. ..... 30
Quadro 2 - Padrões de segurança relacionados com a gestão de riscos. ..... 60
Quadro 3 – Escala de avaliação e valores qualitativos. ..... 66
Quadro 4 – Lista e descrição dos ativos do DTI. ..... 82
Quadro 5 – Lista dos serviços e relação com os ativos. ..... 82
Quadro 6 – Necessidades de segurança dos ativos. ..... 86
Quadro 7 – Escala utilizada para o valor de segurança. ..... 88
Quadro 8 – Escala utilizada para o valor financeiro. ..... 88
Quadro 9 – Escala utilizada para o valor de impacto. ..... 89
Quadro 10 – Resultado do valor global dos ativos. ..... 90
Quadro 11 – Escala de probabilidade das ameaças. ..... 91
Quadro 12 – Lista de ameaças e suas consequências. ..... 92
Quadro 13 – Escala de gravidade das vulnerabilidades. ..... 94
Quadro 14 – Associação dos ativos, ameaças e vulnerabilidades. ..... 97
Quadro 15 – Pontuação do risco de cada ativo. ..... 99
Quadro 16 – Tradução qualitativa do risco ..... 102
Quadro 17 – Valor qualitativo dos riscos. ..... 102
Quadro 18 – Lista de ameaças identificadas. ..... 105
Quadro 19 – Lista de vulnerabilidades identificadas. ..... 108

# SUMÁRIO


**1 INTRODUÇÃO ..... 11**

**1.1 Motivação ..... 12**

**1.2 Definição do problema de pesquisa ..... 13**

**1.3 Objetivo geral ..... 14**

**1.4 Objetivos específicos ..... 14**

**1.5 Escopo e contribuições da pesquisa ..... 14**

**1.6 Estrutura da dissertação ..... 15**

**2 SEGURANÇA DA INFORMAÇÃO ..... 16**

**2.1 Conceitos básicos ..... 16**

2.1.1 Ativos da Informação ..... 19

2.1.2 Vulnerabilidades ..... 20

2.1.3 Ameaças ..... 20

2.1.4 Incidentes de Segurança ..... 21

2.1.5 Probabilidade ..... 22

2.1.6 Impacto ..... 22

2.1.7 Riscos ..... 23

**2.2 Gestão de Riscos em Segurança da Informação ..... 24**

**2.3 Normas para Gestão da Segurança e Riscos ..... 27**

2.3.1 Norma NBR ISO/IEC 27001:2006 ..... 27

2.3.2 Norma NBR ISO/IEC 27002:2005 ..... 28

2.3.3 Norma NBR ISO/IEC 27005:2008 ..... 29

2.3.3.1 Definição do contexto ..... 33

2.3.3.2 Identificação de riscos ..... 34

2.3.3.3 Estimativa de riscos ..... 36

2.3.3.4 Avaliação de riscos ..... 37

2.3.3.5 Tratamento do risco ..... 38

2.3.3.6 Aceitação do risco ..... 39

2.3.3.7 Comunicação do risco ..... 39

2.3.3.8 Monitoramento e análise crítica de riscos ..... 40

**2.4 Metodologias para Gestão de Riscos ..... 41**

**2.5 Conclusões parciais ..... 44**
**3 PADRÕES DE SEGURANÇA ..... 46**
**3.1 Visão geral ..... 46**
**3.2 Catálogos de padrões de segurança ..... 47**
**3.3 Conclusões parciais ..... 51**
**4 MÉTODO DA PESQUISA ..... 52**
**5 PROPOSTA DE UTILIZAÇÃO DE PADRÕES DE SEGURANÇA PARA DESENVOLVER ATIVIDADES DO PROCESSO DE GESTÃO DE RISCOS ..... 55**
**5.1 Fundamentação da proposta ..... 55**
**5.2 Processo de identificação de padrões de segurança ..... 56**
**5.3 Associando padrões de segurança com as atividades da norma NBR ISO/IEC 27005:2008 ..... 60**
5.3.1 Definição do contexto ..... 62
5.3.2 Identificação de riscos ..... 64
5.3.3 Estimativa de riscos ..... 66
5.3.4 Avaliação de riscos ..... 67
5.3.5 Tratamento do risco ..... 68
5.3.6 Aceitação do risco ..... 69
5.3.7 Comunicação do risco ..... 69
5.3.8 Monitoramento e análise crítica de riscos ..... 70
**5.4 Conclusões parciais ..... 73**
**6 IMPLANTAÇÃO DA ANÁLISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO USANDO PADRÕES DE SEGURANÇA ..... 75**
**6.1 Contextualização da organização ..... 75**
**6.2 Desenvolvimento das atividades ..... 76**
6.2.1 Definição do contexto ..... 78
6.2.2 Identificação de riscos ..... 87
6.2.3 Estimativa de riscos ..... 98
6.2.4 Avaliação de riscos ..... 100

**6.3 Conclusões parciais ..... 110**

**7. CONCLUSÕES ..... 112**

**7.1 Trabalhos futuros ..... 114**

**REFERÊNCIAS ..... 115**

# 1 INTRODUÇÃO

Na economia atual, a informação é um dos principais ativos das organizações. É através dela que as empresas gerenciam seus produtos ou serviços e traçam suas estratégias, tornando os sistemas de informações ativos críticos que necessitam serem protegidos contra ameaças que podem explorar as vulnerabilidades do sistema. Estas violações na segurança podem causar a perda da confidencialidade, integridade e disponibilidade das informações, gerando perdas financeiras e competitivas por parte das empresas afetadas (MARTINS; SANTOS, 2005).

Muitas organizações, sejam elas públicas ou privadas, ainda se mostram despreparadas para lidar com a segurança da informação. Isso decorre do fato dessas empresas possuírem poucos instrumentos de proteção, agravados pelo despreparo gerencial, tornando-as mais vulneráveis às ameaças e, com isso, os impactos causados pelos eventos negativos tendem a ser mais fortes (LUNARDI; DOLCI, 2006).

O gerenciamento dos riscos é um dos principais processos da gestão da segurança da informação, pois visa identificar, analisar, avaliar e controlar os riscos inerentes à segurança da informação. Porém, gerenciar os riscos pode ser um processo complexo e oneroso, o que contribui para que muitas empresas não priorizem esse processo em projetos de segurança da informação (OLIVEIRA et al., 2009).

Existem normas e metodologias que guiam o desenvolvimento de uma gestão de riscos, onde cada uma fornece um conjunto de diretrizes distintas para o gerenciamento dos riscos. Dentre os modelos de referência para gestão dos riscos que visam nortear as implementações necessárias está a norma NBR ISO/IEC 27005:2008. O conjunto de processos descritos nesta norma forma um embasamento para a construção de metodologias para gestão de riscos, que aponta o que a organização deve fazer, mas não detalha suficientemente como executar as atividades, dificultando a sua implementação por partes das organizações.

Padrões de segurança descrevem boas soluções para problemas recorrentes de segurança da informação e são propostos como um meio de capturar o conhecimento de especialistas em segurança sob a forma soluções consolidadas (KIENZLE et al., 2002). Estas soluções, descritas como padrões, vêm sendo utilizadas para propor segurança em processos de desenvolvimento e implementação de sistemas, pois incluem informações suficientemente

detalhadas no nível de implementação, o que automatiza a fase da execução das atividades, economizando tempo e custo de implantação (ROSADO et al., 2006).

Considerando que, padrões de segurança descrevem boas soluções para problemas recorrentes de segurança da informação, este trabalho contribui para a elaboração de metodologias de gestão de riscos apontando associações de padrões às atividades indicadas na norma NBR ISO/IEC 27005:2008. Organizações que desejam elaborar processos consistentes alinhados a esta norma poderão assim usar os padrões sugeridos para agilizar o processo de implantação da gestão de riscos.

Este trabalho explora normas e modelos para gestão de riscos à segurança da informação, a partir de soluções provenientes dos catálogos de padrões de segurança. Considerando a definição, em normas e modelos, de atividades a serem desenvolvidas, faz-se o delineamento de uma proposta de metodologia baseada em padrões de segurança que pode ser usada por pessoas não especialistas na área, facilitando a implementação da gestão de risco de segurança da informação.

## 1.1 Motivação

Conforme o *International ISMS Register* (2008), em 2007 o Brasil ocupava a 18ª posição dentre os países que possuem organizações certificadas na norma ISO/IEC 27001:2006, com 15 organizações. Em 2011, o Brasil passou a ocupar a 26ª posição, com 23 organizações certificadas, demonstrando que as organizações brasileiras ainda não têm uma cultura de segurança da informação estabelecida.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) registrou um aumento de 152% no número total de notificações de incidentes de segurança na internet no terceiro trimestre de 2011 em relação ao mesmo período de 2010. Dentre os principais incidentes registrados no período estão tentativas de fraudes (aumento de 35%), páginas falsas de bancos e de sites de comércio eletrônico (aumento de 16% e 45%, respectivamente) e ataques a servidores (aumento de 85%) (CERT.BR, 2011). Em parte, este aumento está associado aos ambientes cada vez mais heterogêneos e dinâmicos, onde os riscos variam conforme a estrutura organizacional e tecnológica, as ameaças e as vulnerabilidades que fazem parte do contexto.

No intuito de fazer com que as organizações desenvolvam mecanismos para lidar com os riscos de segurança da informação, algumas normas foram criadas para orientar no desenvolvimento dos processos de segurança, dentre elas a norma NBR ISO/IEC 27005:2008, que trata sobre gestão de riscos de segurança da informação. Porém a definição das atividades, de forma geral, para o desenvolvimento das normas ainda é um desafio para as organizações, já que a própria norma deixa esta questão em aberto, pois informa “o que fazer” e não “como fazer”. Outra questão que vale destacar é a falta de preparo por parte das organizações em executar uma gestão de riscos, pois não conseguem compreender e desenvolver de forma satisfatória o que é proposto nas normas, ocasionando o fracasso em muitos projetos de gestão da segurança da informação (LUNARDI, 2006).

## 1.2 Definição do problema de pesquisa

Devido ao cenário em que cada vez mais as organizações estão expostas a eventos que colocam em risco as suas informações e, consequentemente, os seus processos de negócio, as empresas estão sendo obrigadas a adotar procedimentos que garantam a segurança de suas informações. Entretanto, implementar uma gestão de segurança da informação baseado em normas de segurança pode ser um processo complexo e oneroso, principalmente pelo fato de as normas descreverem as atividades em uma forma bastante abstrata, não detalhando suficientemente como elas devem ser desenvolvidas.

Na literatura, encontram-se algumas metodologias propostas para identificar e analisar riscos de segurança da informação, contudo a maioria delas não relaciona suas atividades com a norma NBR ISO/IEC 27005:2008 ou como a norma pode ser atendida. Isso faz com que as organizações não saibam qual metodologia utilizar ou acabam escolhendo uma que não é adequada com o seu contexto, acarretando em um processo ineficiente.

Neste sentido, o problema definido para esta pesquisa é: como desenvolver as atividades de gestão de riscos de segurança da informação da norma NBR ISO/IEC 27005:2008?

Como hipótese para resolver este problema vislumbra-se a reutilização das soluções e do conhecimento de especialistas descritos em padrões de segurança.

## 1.3 Objetivo geral

O objetivo principal deste trabalho é propor uma metodologia de gestão de riscos de segurança da informação baseada na norma NBR ISO/IEC 27005:2008 centrada na utilização de padrões de segurança. Para tal, o estudo objetiva analisar catálogos de padrões a fim de propor padrões de segurança que possuam soluções para serem utilizados no desenvolvimento das atividades da norma.

## 1.4 Objetivos específicos

Para alcançar o objetivo geral deste trabalho, serão desenvolvidas as seguintes tarefas:

- Estudo e compreensão dos processos e diretrizes das normas de segurança da informação, em especial a norma NBR ISO/IEC 27005:2008 para gestão de riscos em segurança da informação;
- Pesquisa e identificação de catálogos e padrões de segurança relacionados com gestão de riscos;
- Planejamento/descoberta da associação dos padrões de segurança de acordo com as diretrizes da norma NBR ISO/IEC 27005:2008; e
- Analise da aplicação e viabilidade de se usar padrões de segurança para desenvolver as atividades da norma NBR ISO/IEC 27005:2008.

## 1.5 Escopo e contribuições da pesquisa

O foco desta pesquisa são os processos de gestão de riscos de segurança da informação de acordo com as recomendações da norma NBR ISO/IEC 27005:2008, mais precisamente como que estes processos podem ser implementados. Outro foco desta dissertação está centrado no estudo de padrões de segurança, já que eles descrevem soluções que podem ser aplicadas para resolver problemas recorrentes de segurança. Com base nisso, a limitação deste

trabalho está em utilizar padrões de segurança para desenvolver as atividades da norma NBR ISO/IEC 27005:2008. No entanto, é necessário identificar os catálogos e padrões de segurança mais adequados e relacioná-los com as atividades da norma.

A principal contribuição deste trabalho é experimentar o uso de padrões de segurança para desenvolver as atividades de gestão de riscos da norma NBR ISO/IEC 27005:2008. Com isso, espera-se contribuir com uma metodologia que utiliza soluções que reconhecidamente deram certo, aumentando as garantias de uso de boas práticas.

Consequentemente, outras contribuições podem ser observadas como uma melhor compreensão dos objetivos da norma, um melhor conhecimento sobre o potencial dos padrões de segurança e suas aplicabilidades.

Parte dos resultados obtidos neste trabalho estão presentes em Konzen, Nunes e Fontoura (2012).

## 1.6 Estrutura da dissertação

Este trabalho está organizado como segue. O capítulo 2 faz uma revisão de literatura sobre os principais conceitos de Segurança da Informação, Gestão de Riscos e principais Normas de Segurança. O capítulo 3 faz uma revisão de literatura sobre Padrões de Segurança. No capítulo 4 é apresentada a metodologia utilizada neste trabalho. No capítulo 5 é discutida a principal contribuição deste trabalho, a proposta de utilização de padrões de segurança para desenvolver as atividades do processo de gestão de riscos estabelecido na norma NBR ISO/IEC 27005:2008. No capítulo 6 é discutido um estudo de caso que demonstra a aplicabilidade do uso de padrões de segurança nas atividades de análise e avaliação dos riscos. Por fim, no capítulo 7, são apresentadas as considerações finais.

# 2 SEGURANÇA DA INFORMAÇÃO

Neste capítulo será feita uma revisão bibliográfica dos principais conceitos aplicados em segurança da informação, gestão de riscos e normas sobre segurança da informação. A seção 2.1 trata dos conceitos básicos sobre segurança da informação. A seção 2.2 fala sobre gestão de riscos em segurança da informação. A seção 2.3 faz uma revisão das principais normas de segurança da informação. Na seção 2.4 é feita uma breve revisão sobre algumas metodologias para gestão de riscos existentes na literatura. Por fim, na seção 2.5 são feitas as conclusões parciais deste capítulo.

## 2.1 Conceitos básicos

Nos últimos anos as organizações têm enfrentado um mercado cada vez mais competitivo, onde a informação é o principal elemento para geração de conhecimento e formulação de novas estratégias para o negócio. Os sistemas de informação surgiram como ferramentas para apoiar a gerência e processamento das informações, e os avanços tecnológicos têm proporcionado às empresas maior eficiência e rapidez na troca de informações e tomadas de decisões.

Com o advento da internet, estes sistemas estão cada vez mais interconectados, fato que aumenta a exposição dos dados a um crescente número e grande variedade de ameaças e vulnerabilidades, que podem afetar negativamente os negócios (NETTO; SILVEIRA, 2007).

Como consequência, grande parte dos dados importantes ao negócio está armazenada em computadores, tornando as empresas cada vez mais dependentes dos sistemas de informação, os quais assumem um papel estratégico e vital. Hoje os sistemas de informação ajudam a melhorar a produtividade e a obter vantagem competitiva (GAMBÔA; CAPUTO; FILHO, 2004).

É inegável que a informação passou a ser um dos principais bens que as empresas possuem. Porém, tão importante quanto a própria informação está a infraestrutura tecnológica que oferece suporte para seu processamento e manuseio. Falhas nos sistemas de informação

podem causar a perda, roubo ou indisponibilidade dos dados, causando impactos negativos para a organização e, por isso, necessitam de um grau de proteção adequado.

Muitos sistemas de informação não foram projetados para serem seguros, dessa forma, as organizações precisam adotar medidas de proteção que sejam capazes de proteger adequadamente os dados das ameaças a que estão sujeitos (BEAL, 2005).

Conforme Beal (2005), Sêmola (2003) e Campos (2007), segurança da informação é o processo que visa proteger a informação das ameaças que podem violar a sua integridade, disponibilidade e confidencialidade. A NBR ISO/IEC 27001:2006 define segurança da informação como sendo a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Para Zapater e Suzuki (2005), o conceito de segurança da informação pressupõe a identificação das diversas vulnerabilidades e a gestão de riscos associados aos diversos ativos da informação de uma corporação, independentemente de sua forma ou meio em que são compartilhados ou armazenados (digital ou impresso).

A segurança da informação não é definida somente sob a ótica tecnológica, mas também sob o ponto de vista humano e gerencial. Por exemplo, Caruso e Steffen (1999) definem segurança da informação como sendo mais que uma estrutura hierárquica envolvendo pessoas e equipamentos, mas uma postura gerencial, ultrapassando a abordagem tradicional que é vista na maioria das empresas. Ainda sob a ótica social, Marciano e Marques (2006) defendem que o conceito de segurança da informação precisa ser visto também a partir do comportamento humano, além dos tecnológicos para sua correta cobertura.

Kiely e Benzel (2005) defendem que o aspecto humano, tecnológico e gerencial são os elementos chaves para uma organização que busca uma segurança da informação mais efetiva.

Assegurar a proteção da informação é um princípio base para que a organização forneça um serviço de qualidade, organizado e controlado, independentemente do meio de armazenamento, seja ela eletrônica ou em papel.

Observa-se que independentemente do ponto de vista em que a segurança da informação é abordada, o principal objetivo é garantir a Confidencialidade, a Integridade e a Disponibilidade dos ativos de informação, princípios básicos da segurança da informação.

- Confidencialidade requer que a informação deve ser acessada apenas por pessoas explicitamente autorizadas. Está associada ao conceito de privacidade e implica em proteger as informações contra o acesso de qualquer pessoa não autorizada, isto é, as

informações e processos devem ser liberados apenas a pessoas que possuem autorização explícita. Casos típicos de quebra de confidencialidade ocorrem quando, intencionalmente ou não, uma senha é descoberta e o sistema computacional é invadido (CAMPOS, 2007).

- Integridade requer que a informação deve ser encontrada em sua forma original, sendo mantida a proteção dos dados ou informações contra modificações intencionais ou acidentais não autorizadas. É a garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida (BEAL, 2005). Falsificação de um documento, alteração de registros de um banco de dados não autorizado, não validação da consistência de migração de um sistema para outro, são exemplos que configuram um incidente de segurança da informação por quebra de integridade (CAMPOS, 2007).
- Disponibilidade requer que toda informação deve estar disponível a qualquer momento que for necessário para os usuários autorizados. Pode ainda ser definida como a garantia de que os serviços de um sistema são acessíveis, sob demanda, aos usuários ou processos autorizados (BEAL, 2005). Quando a informação não é acessível às pessoas autorizadas, seja pela perda de documentos, sistemas "fora do ar" (intencionalmente ou não), servidores inoperantes por ataques de negação de serviço (*Deny of Service* - DoS), pane elétrica ou incêndios, tem-se um incidente de segurança da informação por quebra da disponibilidade.

Alguns autores ainda atribuem outros princípios básicos que a segurança da informação objetiva preservar:

- Autenticidade: o objetivo da autenticidade da informação é englobado pelo de integridade quando se assume que este visa a garantir não só que as informações permaneçam completas e precisas, mas também que a informação tenha sua fidedignidade verificada e que seja produzida apenas por pessoas autorizadas e atribuída ao seu autor legítimo (BEAL, 2005).
- Legalidade: garantia de que a informação foi produzida em conformidade com a lei. O acesso à informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos para o negócio, bem como os princípios éticos que deve ser seguidos pela organização (FONTES, 2000).

Além dos princípios básicos, para melhor compreender e implementar um Sistema de Gestão da Segurança da Informação é necessário conhecer a definição dos principais conceitos básicos da área, os quais compreendem: ativos da informação, vulnerabilidades, ameaças, incidentes de segurança, probabilidade, impacto e riscos. A seguir cada um deles é detalhado.

### 2.1.1 Ativos da Informação

Segundo Ferreira e Araújo (2006), ativos da informação podem ser compreendidos como o conjunto que envolve as pessoas, tecnologia e processos, sendo estes responsáveis por alguma etapa do ciclo de vida da informação. Já Sêmola (2003) conceitua ativo como todo elemento que faz parte do processo de manipulação e processamento da informação, os meios em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

A maioria das organizações costuma dar mais atenção aos ativos de maior valor monetário ou os menos comuns. Entretanto é importante identificar a participação do ativo no ciclo de vida da informação, ou seja, quanto maior for essa participação, maior também será a prioridade com que ele deve ser considerado no que tange à segurança da informação (MARCIANO; MARQUES, 2006).

Para assegurar que a informação receba um nível adequado de proteção, os ativos precisam ser mapeados durante o planejamento da segurança da informação, sendo de extrema relevância a realização da sua classificação a qual irá determinar o grau de sigilo às informações neles contidas. A classificação dos ativos está relacionada ao seu grau de importância, sendo possível classificá-las como “muito importante”, “pouco importante”, etc. Também é muito comum a classificação pelo grau de sigilo que podem ser “pública” - informação que pode vir a público sem maiores consequências; “interna” - informação que diz respeito a determinados setores ou unidades; e, “confidencial” - informação restrita, onde somente pessoas autorizadas possam acessar (CAMPOS, 2007).

Entretanto, os ativos, independente do grau de importância, estão sujeitos a vulnerabilidades que podem comprometer a segurança da informação.

### 2.1.2 Vulnerabilidades

Segundo a NBR ISO/IEC 27002:2005, vulnerabilidade é uma fragilidade de um ativo ou um grupo de ativos que pode ser explorada por uma ou mais ameaças, incidindo na quebra de um ou mais princípios de segurança. As vulnerabilidades estão presentes nos próprios ativos, ou seja, são inerentes a eles, e podem ser de ordem tecnológica, humana, processos e ambientes (CAMPOS, 2007). Já Sêmola (2003) exemplifica vulnerabilidades do tipo físicas, naturais, hardware, software, mídias, comunicação e humanas.

As vulnerabilidades por si só não provocam incidentes, porém estas falhas podem ser exploradas por um agente causador ou condição favorável para um evento negativo, que são as ameaças.

### 2.1.3 Ameaças

As ameaças podem advir de diferentes formas, sejam elas naturais ou tecnológicas. A NBR ISO/IEC 27002:2005 define ameaça à segurança da informação como sendo uma causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. Ameaças são agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades (SÊMOLA, 2003).

No início dos anos 2000 as principais ameaças eram os vírus de computador. Nos últimos anos, as ameaças mais comuns são as advindas do recurso humano ou a chamada Engenharia Social, que é um método de ataque onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações sigilosas (PEIXOTO, 2006).

Como podemos ver as ameaças sempre existiram e têm as mais diversas origens e à medida que a tecnologia avança surgem novas formas através das quais as informações podem ficar expostas. Entretanto, muitas organizações não dão o devido reconhecimento de que a segurança da informação é importante e acabam deixando os ativos de informação sem as proteções adequadas, contribuindo para a ocorrência de incidentes de segurança.

### 2.1.4 Incidentes de Segurança

De acordo com a NBR ISO/IEC 27001:2005, um incidente de segurança da informação é reconhecido como sendo um ou mais eventos indesejados ou inesperados, que tenham alguma probabilidade de comprometer as operações ou os processos do negócio e ameaçar a segurança da informação. Incidentes são conceituados como sendo um evento que ocorre em decorrência da ação de uma ameaça que explora uma ou mais vulnerabilidades (BEAL, 2005).

Um incidente de segurança da informação pode ser entendido ainda como a ocorrência de um evento que possa causar interrupções nos serviços oferecidos pelos sistemas de informação, causando prejuízos aos processos do negócio (CAMPOS, 2007).

Dentre uma série de tipos de incidentes presentes em grande parte das organizações, Ferreira e Araújo (2006) citam:

- Roubo e extravio de informações;
- Perda de informações ou equipamento que armazenam dados críticos;
- Propagação de vírus ou outros códigos maliciosos;
- Ataques de negação de serviço e engenharia social;
- Uso ou acesso não autorizado a um sistema, sem o conhecimento, instruções ou consentimento prévio de seu proprietário; e
- Desrespeito a Política de Segurança da Informação.

Por exemplo, se um vírus explora a vulnerabilidade de um servidor de serviços *Web*, deixando-o inoperante ou indisponível, isto pode gerar um prejuízo ou um impacto para a organização. O mesmo se dá no caso de pessoa mal intencionada (ameaça) conseguir convencer um colaborador (ativo) a passar informações confidenciais.

Somente no primeiro semestre de 2012, o CERT.br[2] recebeu mais de 201 mil reportes de incidentes de segurança. O reporte de incidentes de segurança da informação é visto como uma das questões centrais para que haja a sua redução, pois possibilita a análise de tendências e uma melhor resposta a incidentes (CERT.br, 2012) . Rich, Sveen e Jager (2006) destacam que incentivar os usuários a reportarem todo e qualquer incidente que seja identificado é uma forma de alcançar o sucesso nas respostas a eventos negativos.

[2] www.cert.br

Um incidente gera impactos aos processos de negócio da empresa, podendo ser de maior ou menor gravidade e deve ser analisada para que as medidas mais adequadas possam ser implementadas.

### 2.1.5 Probabilidade

Campos (2007) define que em segurança da informação a probabilidade é a chance de um incidente ocorrer. Beal (2005) associa uma escala de 0 a 1 a um evento que pode estar relacionado a uma frequência de ocorrência ou a um grau de confiança de que um evento irá ocorrer.

Vários fatores contribuem para a probabilidade da ocorrência de um incidente de segurança, porém a principal relação está com a probabilidade das ameaças e a gravidade das vulnerabilidades. Podemos citar como ameaças mais prováveis os vírus de computador, e ameaças menos prováveis os meteoros que podem cair na superfície da terra. Como vulnerabilidades de maior gravidade podemos citar computadores sem antivírus conectados à internet, e de menor gravidade prédios sem proteção contra queda de meteoros.

Como se pode perceber, quanto maior for a probabilidade das ameaças e a gravidade das vulnerabilidades, maior será a probabilidade de um incidente de segurança se concretizar. Além da probabilidade, deve-se levar em consideração o impacto que um incidente de segurança possa causar se ocorrer.

### 2.1.6 Impacto

Sêmola (2003) descreve o impacto como sendo a abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio. O impacto refere-se aos potenciais prejuízos causados ao negócio por um incidente de segurança da informação. Esses prejuízos podem significar perdas financeiras, desgaste da imagem, perda na qualidade dos serviços prestados, insatisfação dos colaboradores e clientes, perda de recursos entre outros.

Cada organização possui estratégias de negócios, processos e capacidade de resposta a incidentes diferentes uma das outras, portanto o impacto de um mesmo incidente pode não ser

igual para diferentes organizações (CAMPOS, 2007). Por exemplo, a paralização de um *site* da internet de uma instituição financeira que realiza operações pela internet provocará um impacto negativo muito maior do que a paralização de um *site* de uma empresa que não efetua negócios pela internet.

Podemos observar que um mesmo ativo pode ter valor diferente dependendo da organização. Quanto maior for a relevância do ativo, maior será o impacto caso ele sofra um incidente de segurança. Por isso, é preciso conhecer os riscos que cada eventual incidente de segurança da informação representa para as organizações.

### 2.1.7 Riscos

A NBR ISO/IEC 27001:2006, define o risco como sendo a combinação da probabilidade de um evento e de suas consequências. Já Oliveira (2006) classifica os riscos como sendo uma oportunidade, uma incerteza ou uma ameaça. Esta última como sendo de maior preocupação, pois está atrelada à ocorrências de efeitos negativos como, por exemplo, perda financeira, fraude, roubo, comprometimento da imagem, infração legal, indisponibilidade de serviços, dentre outros (VASILE; STUPARU; DANIASA, 2010).

O nível do risco, independentemente do tipo de organização ou do seu segmento, está relacionado direta ou indiretamente a diversas variáveis. Segundo Sêmola (2003), a relação destas variáveis pode ser resumida pela seguinte equação:

$$R = \frac{V \; x \; A \; x \; I}{M}$$

onde *R* é o nível de risco, *V* são as vulnerabilidades, *A* são as ameaças, *I* é o impacto e *M* são as medidas de segurança.

Observe que o nível do risco é inversamente proporcional às medidas de segurança, ou seja, quanto mais controles de segurança forem implantados menor será o nível de risco em que a organização estará sujeita. Porém, as ameaças, segundo Peixoto (2006), são agentes externos aos ativos e sempre existirão, logo a organização não tem domínio sobre elas. O impacto vai depender do tipo de negócio da organização e, muitas vezes, depende diretamente da exposição às ameaças. Já as vulnerabilidades são fraquezas presentes nos ativos de

informação da empresa e estão sob domínio da organização. Pode-se dizer que a melhor forma de otimizar os esforços para diminuir o nível dos riscos é investir em medidas de segurança para minimizar ao máximo as vulnerabilidades presentes nos ativos de informação.

Desta formulação, pode-se perceber que é necessário avaliar e tratar os riscos para que ocorra sua mitigação, e isto somente será possível se a organização adotar a gestão de riscos, prática preconizada pela NBR ISO/IEC 27001:2005.

## 2.2 Gestão de Riscos em Segurança da Informação

As atividades das organizações estão frequentemente sob riscos. A presença destes riscos implica que tais organizações devem gerenciar os mesmos, identificando-os, analisando-os e, posteriormente avaliando se estes devem ser tratados ou não. Este processo de identificação, análise e avaliação resulta em tomadas de decisões estratégicas por parte da organização que, ao detectar um risco, avalia a dimensão do impacto deste risco e com que frequência este ocorre.

Em um processo de implantação de Gestão de Segurança da Informação a gestão de riscos é fundamental para o processo de decisão, pois visa à identificação, avaliação e priorização de riscos. Nesta fase são definidas ações para a aplicação coordenada e econômica dos recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos, possibilitando a redução do risco a um nível aceitável (VASILE; STUPARU; DANIASA, 2010).

De acordo com Baccarini, Geoff e Love (2004) muitos projetos da área de Tecnologia da Informação e Comunicação pecam pela ineficácia e acabam falhando por não priorizarem a etapa de gerenciamento dos riscos, fazendo com que o fracasso de muitos projetos de Gestão de Segurança da Informação esteja fortemente relacionado ao gerenciamento de riscos.

Segundo Gerber e Solms (2005), o processo de gerenciamento de riscos se refere ao planejamento, monitoramento e controle, baseado nas informações produzidas pela atividade de análise de riscos, que é parte integrante do processo de gerenciamento de risco.

Para Scudere (2006) a condução de uma análise de riscos pode ser dividida em seis etapas distintas:

a) *Planejamento e estratégia*: caracteriza-se pelo planejamento de ações e criações de estratégias de avaliação;

b) *Identificação*: criação de procedimentos que vise uma correta identificação dos riscos;
c) *Qualificação*: qualificação das ameaças e vulnerabilidades;
d) *Quantificação*: pontuação do nível de risco;
e) *Impactos e respostas*: criação de procedimentos que determine o impacto de um determinado risco e a resposta que deverá ser utilizada; e
f) *Monitoramento e Controle*: definição de procedimentos para um constante acompanhamento dos riscos e ações realizadas para minimizá-los.

Diferentemente, Sêmola (2003) propõe que a análise de riscos comece pelo mapeamento das funcionalidades dos processos de negócio e o relacionamento deles com os diversos ativos físicos, tecnológicos e humanos. Após, inicia-se a identificação de ameaças e vulnerabilidades potencialmente presentes nos ativos; a probabilidade da ameaça explorar uma vulnerabilidade; e a projeção do impacto resultante da concretização da ação de uma ameaça. Além disso, o autor ainda destaca que a análise de riscos pode ser de forma qualitativa e/ou quantitativa, onde ele observa que a metodologia qualitativa tem demonstrado eficiência superior.

As abordagens podem ser consideradas na maior parte semelhantes, principalmente nos pontos básicos que são a identificação, estimação (qualificação e quantificação) e controle dos riscos. No entanto, as abordagens diferem em como estes pontos básicos são estabelecidos. Por exemplo, Scudere (2006) define o planejamento como sendo a primeira ação no processo de análise de riscos. Já Sêmola (2003) defende que primeiramente deve ser realizado o mapeamento dos processos de negócio e o relacionamento com os ativos, etapa fundamental para os próximos passos da análise de riscos. Ainda, Gerber e Solms (2005) estabelecem o planejamento após o resultado da análise de riscos. Eloff e Eloff (2005) defendem que muitas vezes a abordagem escolhida por uma organização pode sofrer algumas modificações para estar em sincronia e adaptada ao cenário de aplicação, sendo estes ajustes responsáveis para a obtenção de bons resultados. Disto, pode-se perceber que não existe definição consensual de metodologia ou abordagem ideal. O processo depende muito do contexto da organização, da natureza do problema, do custo e do tempo.

Porém, de acordo com Lichtenstein (1996), um dos fatores que são decisivos na escolha de uma abordagem ou metodologia para o gerenciamento de riscos é o conceito de usabilidade, que está ligado exatamente à facilidade de uso com que a metodologia proporciona em todo processo de realização do gerenciamento de riscos, sendo que quanto

mais usual e fácil ela for menos tempo se gasta e, consequentemente, menos custo se despende para sua aprendizagem.

Compreendido os riscos que envolvem os ativos de informação é possível, então, decidir o que fazer em relação aos riscos identificados. As estratégias ou respostas que podem ser dadas aos riscos identificados, segundo Steinberg et al. (2004) e Campos (2007), podem ser definidas em 4 categorias de respostas aos riscos:

- Evitar: não se adota tecnologia ou processos que ofereçam riscos ao negócio. A forma de tratar estes riscos pode gerar um novo risco maior do que o benefício que ele pode vir a trazer, desta forma opta-se por evitar;
- Transferir: é transferido o tratamento desses riscos a terceiros ou a outro setor sendo uma alternativa viável quando o seu tratamento onera o custo de implantação do projeto;
- Reduzir: são adotados mecanismos ou controles que tenham a ação de mitigar o risco encontrado;
- Aceitar: consiste em não se tomar nenhuma ação para reduzir probabilidade de ocorrência ou impacto.

Dentre estas estratégias, a opção por redução do risco implicará na determinação de um conjunto de medidas a serem implantadas a partir de um nível de prioridade que é definido pela própria organização. Este nível de prioridade pode variar, como por exemplo, riscos que possuem um maior impacto serão tratados primeiro. As ações ou conjunto de ações que serão escolhidos em resposta ao risco irá depender da natureza do negócio e os seus objetivos (CAMPOS, 2007).

Observa-se que a definição de medidas precisa ser compreendida como um processo dinâmico, adaptando-se as mudanças geradas na organização, sendo concretizável seja pelo lado financeiro ou temporal.

Esta discussão a cerca dos aspectos norteadores para atuação da segurança da informação são fortemente destacados nas normas de gestão de segurança da informação que promove amplamente os seus conceitos dentro da organização através da implementação de controles, processos, políticas e procedimentos, que juntos fortalecem os objetivos do negócio com a minimização dos seus riscos.

## 2.3 Normas para Gestão da Segurança e Riscos

Devido à importância de se proteger as informações e sistemas de eventos que possam colocar em riscos os negócios da empresa, diversas normas que guiam a implantação de processos de gestão de segurança da informação foram criadas, a fim de garantir as melhores práticas. A *International Organization for Standartization* (ISO) e a *International Electrotechnical Commission* (IEC) padronizaram internacionalmente este conjunto de normas e criaram a série ISO/IEC 27000, a qual é aceita em todo o mundo. No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) foi responsável pela tradução e adaptação desta série no país, nomeada série NBR ISO/IEC 27000.

As normas NBR ISO/IEC 27001:2006, NBR ISO/IEC 27002:2005 e NBR ISO/IEC 27005:2008 são as principais normas desta série, pois descrevem os processos bases para a implantação de um sistema de gestão de segurança da informação. Estas três normas são descritas nas seções seguintes.

### 2.3.1 Norma NBR ISO/IEC 27001:2006

Conforme Dey (2007), as normas de segurança fornecem uma abordagem de gerenciamento para a implementação e melhoria das práticas de segurança, através do estabelecimento de um Sistema de Gestão da Segurança da Informação (SGSI), permitindo a organização identificar os pontos vulneráveis e as falhas nos sistemas, que deverão ser corrigidos.

A norma NBR ISO/IEC 27001:2006 tem como objetivo especificar os requisitos para o estabelecimento, implementação, funcionamento, acompanhamento, revisão, manutenção e melhoria de um SGSI, dentro do contexto de gerenciamento dos riscos (DEY, 2007). Ela pode ser aplicada em qualquer tipo de organização, dentro do contexto dos riscos que cada negócio enfrenta (KROLL; D'ORNELLAS; FONTOURA, 2010).

Esta norma recomenda estratégias para a especificação e implementação de segurança da informação, e estabelece que estas devam ser influenciadas estrategicamente pelas necessidades e objetivos da organização, podendo ser usada para avaliar a conformidade pelas partes interessadas.

Além disso, a norma incorpora um processo de categorização dos riscos e valorização de ativos, orientando quanto à análise e identificação de riscos e a implantação de controles para minimizá-los. Essa abordagem de processos enfatiza a importância dos seguintes aspectos (KROLL; D'ORNELLAS; FONTOURA, 2010):

- Entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação;
- Implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;
- Monitoração e análise crítica do desempenho e eficácia do SGSI; e
- Melhoria contínua baseada em medições objetivas.

O modelo de gestão de um SGSI preconizado pela NBR ISO/IEC 27001:2006 está baseado no ciclo de melhoria contínua, conhecido como PDCA (*Plan-Do-Check-Act*) (MARTINS; SANTOS, 2005). Este ciclo é aplicado na estruturação de todos os processos do SGSI. Na fase *Plan* (planejar) é estabelecido os objetivos, requisitos e processos para a gestão dos riscos; na fase *Do* (fazer) são implementados e operados as políticas, processos e procedimentos; a fase *Check* (verificar) avalia e mede o desempenho dos processos para uma análise crítica pela direção; e a fase *Act* (agir) executa as ações corretivas e preventivas para alcançar a melhoria contínua.

A norma assegura, também, a seleção adequada de controles para proteger os ativos de informação. Estes controles de segurança recomendados pela norma NBR ISO/IEC 27001:2006 são apoiados pelas recomendações e um guia de implementação das melhores práticas da norma NBR ISO/IEC 27002:2005.

### 2.3.2 Norma NBR ISO/IEC 27002:2005

De fato, existem inúmeras normas que auxiliam as organizações a prover a segurança da informação. Reconhecidamente a NBR ISO/IEC 17799:2005 é referência quando se fala em melhores práticas para segurança da informação (SOLMS; SOLMS, 2004). Segundo Duarte (2006) o Brasil foi o primeiro país do mundo a traduzir a ISO/IEC 17799, sendo adotada como norma nacional em setembro de 2005 denominada na versão brasileira como

NBR/ISO IEC 17799:2005. A partir do ano de 2007 a NBR/ISO IEC 17799:2005 passou a ser chamada de NBR ISO/IEC 27002:2005, fazendo parte da série de normas ISO/IEC 27000.

A norma aborda que a garantia da segurança da informação significa proteger a informação de vários tipos de ameaças, possibilitando minimizar os riscos, maximizar o retorno sobre os investimentos e a continuidade do negócio. Além disso, ela recomenda que as ações sejam tomadas baseadas na análise de riscos da organização, onde cada ativo da informação deverá ser analisado, valorado e classificado conforme sua importância.

A norma NBR ISO/IEC 27002:2005 é um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Ela apresenta um guia prático para implementação de cada um dos 133 controles apresentados no apêndice A da NBR ISO/IEC 27001:2006, que estão divididos em 11 grupos de controles. No Quadro 1 são listados os 11 grupos de controles e seus respectivos objetivos.

De acordo com a norma NBR ISO/IEC 27001:2006, os controles citados acima não são exaustivos e conforme o contexto dos riscos de cada organização pode ser considerado controles adicionais, assim como parte dos controles podem ser irrelevantes para as necessidades individuais da organização.

Segundo Moura e Gaspary (2008), para atender aos objetivos de controle de segurança da informação relacionados às estes grupos de controle a segurança da informação passa por identificar quais controles são necessários para mitigar os riscos associados aos ativos da organização.

### 2.3.3 Norma NBR ISO/IEC 27005:2008

Devido à importância do processo de gestão de riscos para as organizações, algumas normas foram criadas com o intuito de nortear os conceitos e práticas de gestão de riscos. Dentre estas normas, a NBR ISO/IEC 27005:2008, que discute - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação, é reconhecida por fornecer recomendações para condução de uma gestão de riscos. A utilização de normas de segurança da informação garante que a organização está seguindo as diretrizes dos processos de gestão da segurança da informação e possibilita com que a organização seja reconhecida pela utilização de boas práticas em gestão da segurança da informação.

| Grupo de Controle | Objetivos de controle |
|---|---|
| Política de segurança | Prover uma orientação e apoio da direção para a segurança da informação de acordo com o contexto do negócio. |
| Organizando a segurança | Gerenciar a segurança da informação dentro e fora da organização. |
| Gestão de ativos | Determinar a responsabilidade pelos ativos e classificar a informação. |
| Segurança em recursos humanos | Diminuir os riscos decorrentes de atos advindos de ações das pessoas. |
| Segurança física e do ambiente | Proteger as áreas restritas, equipamentos e infraestrutura. |
| Gerenciamento das operações e comunicações | Tratar falhas em procedimentos operacionais, homologação e implantação de sistemas, gerenciamento de serviços terceirizados, proteção contra códigos maliciosos e móveis, manuseio de médias e cópias de segurança, segurança em redes, troca de informações e monitoramento. |
| Controle de acessos | Proteger e controlar o acesso à informação e sistemas, definindo competências e responsabilidades. |
| Aquisição, desenvolvimento e manutenção de sistemas de informação | Tratar dos requisitos de sistemas, criptografia, controlar o processamento de aplicações, segurança dos arquivos, segurança no desenvolvimento e suporte e gestão de vulnerabilidades técnicas. |
| Gestão de incidentes de segurança | Notificar vulnerabilidades, ocorrências de segurança e gestão de incidentes. |
| Gestão da continuidade do negócio | Manter um plano de continuidade e contingência para recuperação de desastres. |
| Conformidade | Cuidar da conformidade com requisitos legais, normas, políticas e auditorias. |

Quadro 1- Grupos de controles e objetivos de controle.
Fonte: ABNT NBR ISO/IEC 27001 (2006).

A norma NBR ISO/IEC 27005:2005 é parte da série de normas da ISO/IEC 27000, e o âmbito de aplicação destas normas pode ser na organização como um todo, ou em partes, como os processos de um departamento, uma aplicação de TI ou uma infraestrutura de TI (BECKERS et al., 2011). Esta norma fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI) proposta na norma NBR ISO/IEC 27001:2006.

A norma AS/NZ 4360:2004 – *Risk Management* – serviu de referência para o desenvolvimento da maioria das demais normas que a sucederam, incluindo as atuais normas NBR ISO/IEC 31000:2009 e NBR ISO/IEC 27005:2008, sendo esta última voltada para segurança de sistemas de informação e comunicação ou tecnologia da informação (BRANDÃO; FRAGA, 2008).

As normas AS/NZ 4360 e NBR ISO 31000 definem o processo de gestão de riscos por meio de 7 atividades principais, conforme ilustrado na Figura 1: estabelecer o contexto; identificar os riscos; analisar os riscos; avaliar os riscos; tratar os riscos; monitorar e rever; e comunicar e consultar.

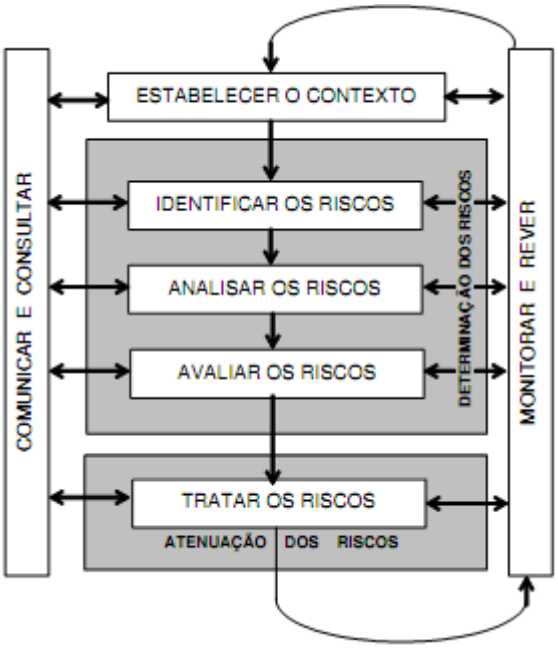


Figura 1- Gestão de Riscos segundo as Normas AS/NZ 4360 e NBR ISO 31000.
Fonte: Brandão e Fraga (2008, p. 11).

Já a norma NBR ISO/IEC 27005:2008 define o processo de gestão de risco como atividades coordenadas para dirigir e controlar o risco de uma organização (LUND; SOLHAUG; STØLEN, 2010). Neste contexto, o processo de gestão de riscos é definido por oito atividades, como pode ser observado na Figura 2.

Como pode ser observado nas Figuras 1 e 2, o processo da norma NBR ISO/IEC 27005:2008 traz uma pequena variação dos termos. Além disso, na norma NBR ISO/IEC 27005:2008 são indicados dois pontos de decisão nos quais o processo pode ser revisto, além de uma nova atividade “aceitação do risco”.

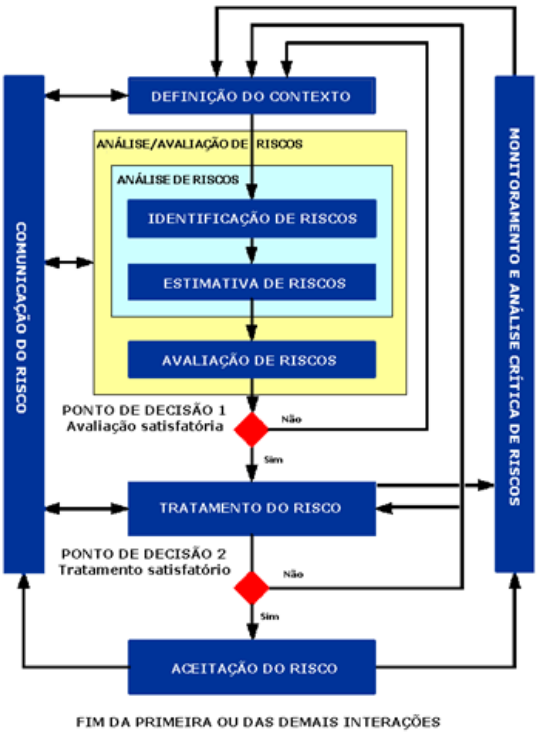


Figura 2 - Processo de gestão de riscos de segurança da informação.
Fonte: ABNT NBR ISO/IEC 27005 (2008, p. 5).

Outro ponto que vale destacar, segundo Brandão e Fraga (2008), é o alinhamento com a norma NBR ISO/IEC 27001:2006, principalmente em relação ao ciclo PDCA. De acordo com o ciclo PDCA, as etapas da gestão de riscos são divididas nas quatro fases, conforme ilustrado na Figura 3. Na fase de planejamento (*Plan*) são agrupadas as etapas: de Definição do Contexto, de Análise/Avaliação de Riscos, de Definição do Plano de Tratamento do Risco e de Aceitação do Risco. Na fase de Execução (*Do*) é realizada a implantação do Plano de Tratamento do Risco. Na verificação (*Check*) é feito o Monitoramento Contínuo e Análise Crítica do Risco. Finalmente, a fase Ação (*Act*) envolve manter e melhorar o processo de Gestão de Riscos de Segurança da Informação.

Para cada etapa do processo a norma propõe diretrizes para implementação, as quais serão brevemente descritas a seguir.

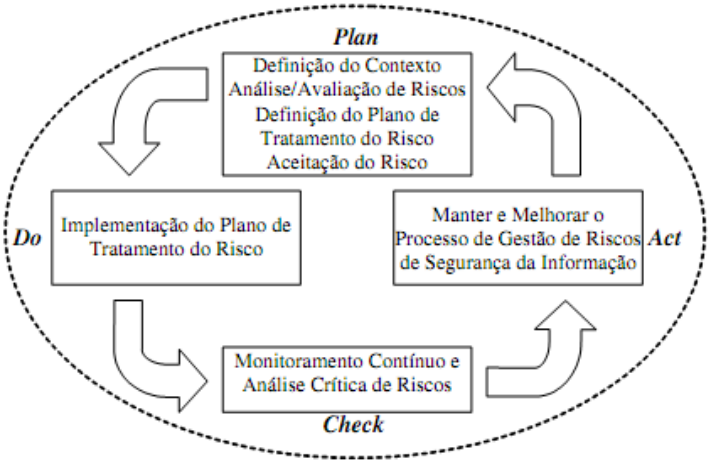


Figura 3- Alinhamento do ciclo PDCA com o processo de Gestão de Riscos.
Fonte: Brandão e Fraga (2008, p. 12).

### 2.3.3.1 Definição do contexto

É essencial determinar o contexto para gestão de riscos. Para isso, convêm que sejam definidos os critérios básicos para a gestão de riscos, a definição do escopo e limites e o estabelecimento das responsabilidades para a gestão de riscos. Para que esta atividade seja desenvolvida são necessárias todas as informações possíveis e relevantes para a definição do contexto da gestão de riscos.

A definição do propósito da gestão de riscos também é importante, pois afeta diretamente a definição do contexto. O propósito para uma gestão de riscos pode ser servir de suporte para um SGSI, preparação de um plano de continuidade de negócios, preparação de um plano de respostas a incidentes, descrição dos requisitos de segurança para um produto ou um serviço ou conformidade com a realização dos procedimentos corretos.

Os critérios básicos definem: os critérios para a avaliação de riscos baseados na importância dos processos para a organização; critérios de impacto especificados em função do montante dos danos ou custos à organização causados por um incidente de segurança; e critérios para a aceitação do risco tendo como base as políticas, metas e objetivos da organização, assim como os interesses das partes interessadas.

A definição do escopo e limites da gestão de risco assegura que todos os ativos relevantes sejam considerados na análise/avaliação de riscos. Informações sobre os objetivos estratégicos da organização, os processos de negócio, requisitos legais, a estrutura da

organização, os ativos de informação, entre outros, são fundamentais para a definição do escopo. Exemplos do escopo de uma gestão de riscos podem ser: uma aplicação de TI, a infraestrutura de TI, um processo de negócios ou uma parte da organização. O estabelecimento da organização e as responsabilidades definem os principais papéis envolvidos no processo de gestão de riscos.

Como visto na seção 2.1.7, risco é a combinação da probabilidade de um evento negativo ocorrer e seu impacto sobre os processos de negócios. A análise/avaliação de riscos capacita os gestores a priorizar os riscos de acordo com o valor dos ativos de informação e com os critérios de avaliação de riscos estabelecidos na definição de contexto.

A análise de risco pode ser uma forma eficiente de mostrar à alta administração a real necessidade de investimentos em medidas de segurança, pois permite detectar falhas que podem acarretar em prejuízos para a organização (AMARAL, 2011). Desta forma, é possível investir em medidas de segurança nos pontos mais críticos da organização.

A atividade de Análise/Avaliação de Riscos é subdividida em três atividades: Identificação de riscos; Estimativa de riscos; e Avaliação de riscos.

#### 2.3.3.2 Identificação de riscos

O objetivo da identificação dos riscos é determinar os eventos que possam ter impacto negativo nos negócios da organização. Devem ser identificados os ativos, as ameaças que podem causar danos a estes ativos, suas vulnerabilidades e os controles já existentes. Além disso, devem ser identificadas também as consequências que as perdas de confidencialidade, de integridade e de disponibilidade podem ter sobre os ativos identificados.

Um ativo é algo que tem valor para a organização e requer proteção. Portanto, para identificar os riscos aos ativos mais importantes da organização, primeiramente estes ativos devem ser identificados em um nível de detalhamento adequado. Eles podem ser de dois tipos:

a) Ativos primários:
   - Processos e atividades do negócio
   - Informação
b) Ativos de suporte e infraestrutura
   - Hardware

- Software
- Rede
- Recursos humanos
- Instalações físicas
- A estrutura da organização

Uma ameaça tem o potencial de comprometer os ativos e, consequentemente, os processos que eles suportam, e precisam ser identificadas. Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais e podem afetar mais de um ativo. Informações sobre as ameaças podem ser obtidas a partir da análise crítica do histórico de incidentes, pela experiência dos responsáveis pelos ativos ou dos usuários, ou também através de catálogos externos. Como resultado, deve-se ter uma lista de ameaças com a identificação do tipo e da fonte das ameaças.

A NBR ISO/IEC 27005:2008 recomenda que a identificação de controles existentes seja realizada para evitar custos e retrabalho desnecessários, pois medidas de segurança já implementadas podem ter um impacto direto nos riscos identificados. Além disso, podem ser identificados controles ineficazes ou insuficientes que podem ser removidos ou substituídos.

As vulnerabilidades que podem ser exploradas por ameaças para comprometer os ativos ou a organização necessitam ser identificadas. Muitas vulnerabilidades podem não ter uma ameaça correspondente no presente momento e podem não requerer a implementação de controles de forma imediata. As vulnerabilidades podem ser identificadas nas seguintes áreas:

- Organização
- Processos e procedimentos
- Rotinas de gestão
- Recursos humanos
- Ambiente físico
- Configuração dos sistemas de informação
- Hardware, software ou equipamentos de comunicação

As consequências que a perda de confidencialidade, de integridade e de disponibilidade podem ter sobre os ativos devem finalmente ser identificadas. Um cenário de incidente de segurança pode ser descrito como uma ameaça explorando certa vulnerabilidade ou um conjunto delas. O impacto de um incidente de segurança pode ser, por exemplo, a perda da eficácia devido à investigação e tempo de reparo de um dano, tempo de trabalho

perdido, oportunidade de negócio perdida, custo financeiro para reparar o prejuízo, danos à imagem, reputação e valor de mercado.

#### 2.3.3.3 Estimativa de riscos

Esta atividade tem como objetivo atribuir valor ao impacto que um risco pode ter e a probabilidade de sua ocorrência. A estimativa do risco então é calculada através da combinação entre a probabilidade de um cenário de incidente e suas consequências. Nesta atividade são produzidos dados que irão auxiliar na decisão sobre quais riscos serão tratados (BRANDÃO; FRAGA, 2008).

De uma forma geral, a estimativa de riscos pode ser de forma qualitativa ou quantitativa ou uma combinação das duas, dependendo do grau de detalhamento necessário conforme os critérios básicos estabelecidos na definição do contexto. A metodologia qualitativa utiliza cálculos mais simples com resultados mais subjetivos, já a quantitativa utiliza formas mais complexas para o cálculo, porém pode apresentar resultados em valores financeiros (CAMPOS, 2007).

Conforme a NBR ISO/IEC 27005:2008, as metodologias qualitativa e quantitativa possuem as seguintes definições:

- **Estimativa qualitativa**: utiliza uma escala com atributos qualificadores que descrevem a magnitude das consequências potenciais (por exemplo: Pequena, Média e Grande) e a probabilidade dessas consequências ocorrerem. A estimativa qualitativa tem como vantagem a facilidade de compreensão por todas as pessoas envolvidas. Porém, sua desvantagem é a dependência à escolha subjetiva da escala. As escalas podem ser adaptadas ou ajustadas, de acordo com a necessidade. Na prática, a estimativa qualitativa é frequentemente utilizada em primeiro lugar para obter uma indicação geral do nível de risco e para revelar os grandes riscos.
- **Estimativa quantitativa**: a estimativa quantitativa utiliza uma escala com valores numéricos tanto para consequências quanto para a probabilidade, usando dados de diversas fontes. A estimativa quantitativa, na maioria dos casos, utiliza dados históricos dos incidentes, proporcionando a vantagem de poder ser relacionada diretamente aos objetivos da segurança da informação e interesses da organização. Sua desvantagem é a falta de tais dados sobre novos riscos ou sobre fragilidades da

segurança da informação. Nesse caso, a exatidão da análise/avaliação de riscos e os valores associados tornam-se não precisos.

De acordo com Campos (2007), avaliar as consequências de um cenário de incidente de segurança é determinar o grau do impacto deste incidente, ou seja, estimar o prejuízo envolvendo um determinado ativo de um determinado processo de negócio. O grau do impacto está ligado diretamente com a relevância do processo analisado e seus ativos e pode ser ainda avaliado de acordo com o valor de reposição do ativo e as consequências ao negócio relacionadas à perda ou ao comprometimento do ativo.

Outro fator importante para a estimativa de riscos é a probabilidade de um incidente ocorrer. Convém levar em conta o grau das ameaças, ou seja, a frequência da ocorrência das ameaças e a facilidade com que as vulnerabilidades podem ser exploradas. De acordo com a NBR ISO/IEC 27005:2008, convém que seja considerado: as estatísticas referentes à probabilidade das ameaças, caso estejam disponíveis; as fontes de ameaças intencionais; as fontes de ameaças acidentais; e os controles existentes e a eficácia com que eles reduzem as vulnerabilidades.

Por fim, a estimativa do nível do risco é baseada no grau de impacto e na probabilidade estimados, ou seja, o risco estimado é uma combinação entre a probabilidade de um cenário de incidente e suas consequências.

#### 2.3.3.4 Avaliação de riscos

A atividade de avaliação de riscos é responsável pela classificação dos riscos de acordo com sua criticidade, em função da importância dos ativos para a realização dos objetivos de negócios da organização. O processo de avaliação de riscos tem como entrada a lista de riscos com níveis de valores designados e como saída uma lista de riscos ordenados por prioridades (NBR ISO/IEC 27005:2008).

Esta atividade tem como objetivo determinar a prioridade de cada risco através de uma comparação entre o nível estimado do risco e o nível aceitável estabelecido pela organização, a fim de auxiliar na tomada de decisão sobre quais riscos devem ser priorizados e tratados.

O ponto de decisão 1 (vide Figura 2) verifica se a avaliação dos riscos foi satisfatória, conforme os critérios estabelecidos pela organização. Caso não seja satisfatória, a atividade

pode ser reiniciada de forma que se possa revisar, aprofundar e detalhar ainda mais a avaliação, assegurando que os riscos possam ser adequadamente avaliados.

#### 2.3.3.5 Tratamento do risco

Com a lista de riscos ordenados por prioridade, esta atividade tem como objetivo planejar a implementação de controles para reduzir, reter, evitar ou transferir os riscos identificados. Se o tratamento do risco não for satisfatório, ou seja, não resultar em um nível de risco residual que seja aceitável, deve-se iniciar novamente a atividade ou o processo até que os riscos residuais sejam explicitamente aceitos pelos gestores da organização. Esta iteração se dá no ponto de decisão 2, como visto na Figura 2.

A Figura 3 ilustra a atividade de tratamento de risco dentro do processo de gestão de riscos de segurança da informação da norma NBR ISO/IEC 27005:2008.

As opções de tratamento do risco devem ser selecionadas com base no resultado da análise e avaliação de riscos, no custo esperado para a implementação dessas opções e nos benefícios esperados. As opções de tratamento dos riscos são descritas resumidamente a seguir, conforme a norma NBR ISO/IEC 27005:2008:

- **Redução do risco**: seleção de controles apropriados para mitigar os riscos de segurança da informação.
- **Retenção do risco**: refere-se à opção de não implementar controles para tratamento do risco, diante do fato de o nível desse risco atender aos critérios para a aceitação do risco, ou pelo fato de o custo para implementar uma medida de segurança foi inaceitável.
- **Evitar o risco**: eliminação das atividades/processos que causam o risco ou alteração nas condições de operação de tais.
- **Transferência do risco**: compartilhar determinados riscos com entidades externas, para que o mesmo seja tratado de forma mais eficaz.

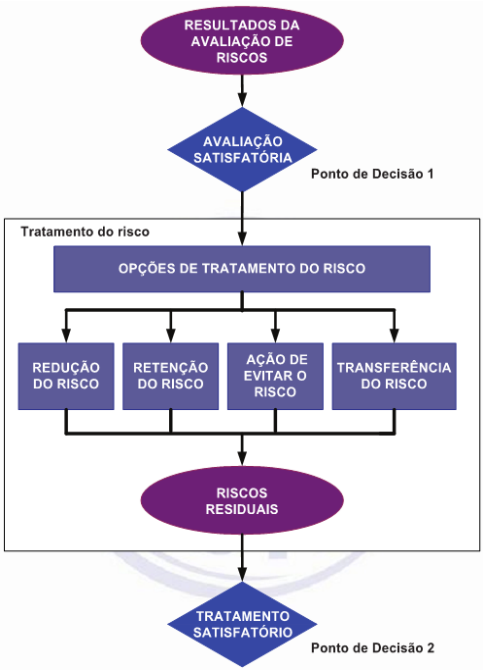


Figura 4- A atividade de tratamento do risco.
Fonte: ABNT NBR ISO/IEC 27005 (2008, p.18).

### 2.3.3.6 Aceitação do risco

É importante que gestores responsáveis façam uma análise crítica e aprovem, se assim entenderem, formalmente os planos de tratamento do risco, os riscos residuais resultantes, juntamente com a responsabilidade pela decisão.

Como resultado desta atividade tem-se uma lista de riscos aceitos, incluindo uma justificativa para aqueles que não satisfaçam os critérios normais para aceitação do risco.

### 2.3.3.7 Comunicação do risco

A comunicação do risco é uma atividade que objetiva alcançar um consenso sobre como os riscos devem ser gerenciados, trocando ou compartilhando informações entre os tomadores de decisão e as partes interessadas. A comunicação eficaz é importante, uma vez

que assegurará que os responsáveis pela implementação da gestão de riscos, e aqueles com interesses reais, tenham um bom entendimento do por que as decisões são tomadas.

Ainda de acordo com a norma NBR ISO/IEC 27005:2008, a comunicação do risco tem como finalidade também:

- Fornecer garantia do resultado da gestão de riscos;
- Coletar informações sobre os riscos;
- Compartilhar resultados da análise/avaliação de riscos;
- Apresentar o plano de tratamento do risco;
- Evitar a falta de entendimento mútuo entre os tomadores de decisão e as partes interessadas;
- Dar suporte ao processo decisório;
- Coordenar com outras partes e planejar respostas para reduzir as consequências de um incidente;
- Dar aos tomadores de decisão e as partes interessadas um senso de responsabilidade sobre os riscos; e
- Melhorar a conscientização.

Portanto, a atividade tem como principal meta desenvolver planos de comunicação dos riscos para assegurar que todos tenham consciência sobre os riscos e controles a serem adotados.

#### 2.3.3.8 Monitoramento e análise crítica de riscos

A atividade de monitoramento e análise crítica de riscos tem como objetivo monitorar e analisar criticamente os fatores de risco e melhoria do processo de gestão de riscos.

A norma NBR ISO/IEC 27005:2008 recomenda que os riscos e seus fatores sejam monitorados continuamente a fim de identificar eventuais mudanças no contexto. O monitoramento constante é necessário para que sejam detectadas mudanças nas ameaças, nas vulnerabilidades, na probabilidade e nas consequências. Novas ameaças, novas vulnerabilidades, assim como fatores que provocam mudanças na probabilidade ou nas consequências podem vir a ampliar os riscos anteriormente avaliados. O resultado da

atividade de monitoramento de riscos pode fornecer um alinhamento contínuo da gestão de riscos.

O monitoramento, análise e melhoria do processo de gestão de riscos são necessários para assegurar que o contexto, o resultado da análise e avaliação de riscos e do tratamento do risco permaneçam relevantes e adequados com a realidade da organização. Além disso, assegura que as atividades planejadas estejam sendo acompanhadas, e quaisquer mudanças na gestão de riscos devem ser comunicadas aos gestores e partes interessadas.

O monitoramento e a análise crítica podem identificar mudanças em fatores que afetam a gestão de riscos e, consequentemente, que ela seja revista. É necessário, portanto, monitorar e analisar:

- Contexto legal e do ambiente;
- Método de análise/avaliação de riscos;
- Valor e as categorias dos ativos;
- Critérios de impacto;
- Critérios para avaliação de riscos;
- Critérios para a aceitação do risco;
- Custo total da segurança;
- Recursos necessários.

Como resultado desta atividade é possível certificar que o processo de gestão de riscos de segurança da informação e as atividades relacionadas permaneçam apropriados nas circunstâncias presentes.

A norma NBR ISO/IEC 27005:2008 não determina uma metodologia específica para a gestão de riscos de segurança da informação, cabendo a cada organização definir a melhor abordagem conforme o contexto na qual está inserida. Na seção 2.4 são apresentadas algumas metodologias presentes na literatura que são utilizadas para desenvolver atividades de gestão de riscos.

## 2.4 Metodologias para Gestão de Riscos

Podemos encontrar na literatura algumas metodologias que são propostas para desenvolver atividades do gerenciamento de riscos, onde cada metodologia fornece um

conjunto de práticas para o gerenciamento do risco. Segundo Oliveira (2006), dentre as mais utilizadas estão as metodologias OCTAVE – *Operationally Critical Threat, Asset, and Vulnerability Evaluation* – (ALBERTS e DOROFEE, 2004) e NIST SP 800-30: *Risk Management* (NIST, 2002).

A metodologia OCTAVE foi desenvolvida pelo SEI (*Software Engineering Institute*) e é indicada para uso em organizações que possuam mais de duzentos colaboradores. As atividades desta metodologia são divididas em três fases:

- Fase 1 - Construção do perfil das ameaças baseado em ativos: Esta fase dá o conhecimento necessário sobre os ativos, ameaças e estratégias de proteção;
- Fase 2 - Identificação da infraestrutura das vulnerabilidades: Nesta fase a equipe de análise examina os principais componentes para deficiências operacionais (tecnologia e vulnerabilidades) que podem conduzir a uma ação não autorizada contra os ativos;
- Fase 3 - Desenvolvimento de planos e estratégias de segurança: Durante esta fase são identificados os riscos para os ativos da organização e são decididas as medidas de proteção.

A abordagem OCTAVE é estruturada em dezoito volumes, sendo que cada volume detalha os processos e as atividades da metodologia, podendo ser entendida por organizações com qualquer nível de maturidade em gestão de riscos. Como característica, a metodologia OCTAVE utiliza a análise qualitativa do risco e tem como principais processos a identificação dos ativos críticos de informação, identificação das ameaças que afetam os ativos críticos, identificação das vulnerabilidades associadas com tais ativos e a determinação dos níveis atuais de riscos referentes aos ativos críticos.

O NIST SP 800-30 é um conjunto de diretrizes para gerenciamento de riscos publicado pelo *National Institute of Standards and Technology*. Essa metodologia também utiliza uma abordagem qualitativa para analisar e avaliar os riscos e fornece uma visão geral dos seguintes processos:

- Caracterização do sistema: reúne informações sobre a criticidade e sensibilidade dos ativos (definidos no escopo da avaliação), que são mapeados por meio de diversas técnicas de obtenção de informações;
- Identificação das ameaças: as ameaças são identificadas e agrupadas de acordo com a motivação de cada uma e suas respectivas ações;

- Identificação das vulnerabilidades: identifica as possíveis vulnerabilidades do sistema através de uma análise das políticas de segurança adotadas pela organização e que se aplicam ao sistema;
- Análise dos controles: visa avaliar a efetividade dos controles empregados atualmente, ou que se planeja implementar, para minimizar ou eliminar a probabilidade de uma ameaça explorar uma vulnerabilidade;
- Determinação das probabilidades: determinação da probabilidade de uma ameaça explorar uma vulnerabilidade. No final desta avaliação obtém-se uma lista com os índices de probabilidades;
- Análise do impacto: consiste na mensuração do impacto causado pela exploração de uma vulnerabilidade por uma ameaça;
- Determinação dos riscos: são relacionadas às probabilidades e o impacto para a construção da matriz de risco;
- Recomendações de controles: define quais controles devem ser empregados para mitigar ou eliminar os riscos identificados nas etapas anteriores;
- Documentação dos resultados: elaboração de documentos com os resultados da avaliação de risco para o escopo avaliado.

A metodologia NIST SP 800-30 é mais voltada para a gestão de riscos no ciclo de vida de desenvolvimento de software e, por apresentar uma visão superficial de todo o processo, é recomendada para organizações que já tenham um nível médio de maturidade e que estejam buscando aprimorar os seus processos de gestão de riscos de segurança no desenvolvimento de sistemas.

Além das metodologias citadas, pode-se destacar ainda a CRAMM (*CCTA RISK Analisys and Management Method*) (MARQUIS, 2006). Desenvolvida pelo governo britânico, a metodologia CRAMM é utilizada por muitas organizações do Reino Unido e oferece suporte a implementação da ISO 17799. Esta metodologia apresenta uma abordagem de informações em alto nível e dá suporte a decisões para o desenvolvimento do gerenciamento de riscos. A metodologia CRAMM utiliza como principais ferramentas reuniões, entrevista e questionários para a coleta de dados, e é desenvolvida através de três processos:

- Identificação e avaliação dos ativos: o objetivo é identificar e valorizar ativos;
- Avaliação das ameaças e vulnerabilidades: o objetivo é avaliar os riscos sobre os ativos;

- Seleção de contramedidas e recomendações: o objetivo é identificar as mudanças necessárias para gerir os riscos identificados.

Oliveira et al. (2009) propõem um *framework* para gerenciamento de riscos utilizando o modelo DMAIC. Este modelo compreende o desenvolvimento de 5 fases para implementar um processo de gestão de riscos: Definir, Medir, Analisar, Implementar ou Melhorar e Controlar. Para cada fase é sugerida ferramentas que podem ser utilizadas para uma melhor condução das atividades de gestão de riscos.

Onwubiko e Lenaghan (2007) propõem um processo de identificação dos riscos em ambientes de rede, onde a classificação dos ativos é baseada em seu valor e a classificação das ameaças é baseada em cronograma de ataque. O modelo de classificação para os ativos é proposto como "crítico", "importante" e insignificante". A classificação das ameaças tem como base um cronograma de ataque, sendo os seguintes estágios: sondagem, penetração e perpetuação. O risco é então calculado de acordo com a classificação da importância do ativo e com relação a classificação da ameaça baseada na facilidade de concretização do ataque.

## 2.5 Conclusões parciais

A segurança das informações está diretamente atrelada à segurança dos bens que a suportam, portanto, para garantir a sua segurança devemos garantir a segurança destes bens. Para isso, deve-se, primeiramente, conhecer os riscos que estes bens correm. Os riscos estão relacionados com o impacto que um ativo representa para a empresa, a probabilidade de as ameaças gerarem um incidente de segurança e a gravidade das falhas que podem ser exploradas pelas ameaças.

A gestão da segurança das informações basicamente compreende em gerenciar os riscos que podem atingir os ativos, em que controles de segurança deverão ser implementados para prevenir ou corrigir falhas que possam comprometer os ativos. Com o conhecimento dos riscos que atingem os ativos é possível estabelecer planos para desenvolver, manter e operar um sistema de gestão de segurança da informação.

Normas de segurança foram criadas para garantir a utilização de boas práticas no desenvolvimento de processos de segurança da informação. Dentre as principais normas estão a NBR ISO/IEC 27001:2006, NBR ISO/IEC 27002:2005 e a NBR ISO/IEC 27005:2008. Esta última, define um processo com 8 atividades que servem de referência para implementar um

processo de gerenciamento dos riscos. Apesar disso, a utilização efetiva das normas ainda é um desafio por parte das organizações, pois elas descrevem as diretrizes de forma abstrata, não detalhando suficientemente como desenvolver cada atividade.

# 3 PADRÕES DE SEGURANÇA

Este capítulo apresenta uma breve revisão de literatura sobre padrões de segurança e suas principais características. A seção 3.1 apresenta uma visão geral sobre padrões de segurança. A seção 3.2 fala sobre catálogos de padrões, citando alguns dos principais autores de catálogos. Na seção 3.3 são feitas as conclusões parciais sobre este capítulo.

## 3.1 Visão geral

Apesar de existirem preocupações com a segurança das informações, muitas falhas ocorrem porque poucos engenheiros de software e gestores de TI são especialistas em segurança. Assim como os padrões de software capturam as melhores práticas de especialistas para serem reaproveitadas no desenvolvimento de software, padrões de segurança capturam as melhores práticas de especialistas no contexto da segurança, visando o desenvolvimento de sistemas seguros (YOSHIOKA; WASHIZAKI; MARUYAMA, 2008).

O conhecimento especializado retratado nos padrões de segurança fornece soluções a problemas recorrentes de segurança, podendo servir de referência para os requisitos de segurança (WAGNER; FONTOURA; FONTOURA, 2011) e para soluções dentro de diversos contextos (SUPAPORN; PROMPOON; ROJKANGSADAN, 2007). Os padrões de segurança também ajudam na identificação e formulação das práticas e procedimentos de segurança recomendados pelas normas de segurança da informação (ROMANOSKY, 2002).

Para Heyman et al. (2007), reutilizar o conhecimento que já foi utilizado e testado é melhor do que implementar soluções do zero. Por exemplo, é melhor utilizar protocolos de criptografia já conhecidos e testados do que criar um novo protocolo, o que certamente seria arriscado devido à probabilidade de falhas de projeto. Neste sentido, apontam algumas vantagens proporcionadas pelos padrões:

- as soluções propostas pelos padrões de segurança são reconhecidas e testadas ao longo do tempo;
- as vantagens e desvantagens de um padrão são conhecidas com antecedência e podem servir para a tomada de decisão ao se desenhar uma metodologia; e

- os padrões estabelecem um vocabulário comum que pode facilitar a comunicação entre os diferentes papéis.

Além disso, pode-se acrescentar que padrões de segurança incluem informações suficientemente detalhadas no nível de implementação, o que automatiza a fase da execução das atividades, economizando tempo e custo de implantação.

O termo "padrão de segurança" começou a ganhar uma atenção significativa na comunidade acadêmica nos meados dos anos 90, quando Yoder e Barcalow (1997) examinaram a literatura resumindo algumas recomendações de segurança publicadas por especialistas da área e, inicialmente, padrões de segurança foram concebidos para serem usados em projetos de software.

## 3.2 Catálogos de padrões de segurança

Nos últimos anos, vários autores publicaram diversos padrões de segurança em seus catálogos. Catálogos de padrões são repositórios que contém a documentação com a descrição e os passos necessários para implementar as soluções propostas pelos padrões (HAFIZ; ADAMCZYK; JOHNSON, 2007). Devido ao aumento de números de padrões de segurança documentados, alguns autores como Bunke, Koschke e Sohr (2012), Heyman et al. (2007) e Hafiz, Adamczyk e Johnson (2007) publicaram alguns estudos no sentido de organizar os padrões de acordo com seus domínios de aplicação. Em seu estudo, Bunke, Koschke e Sohr (2012) propõem uma classificação que resume ao todo 415 padrões de segurança. Neste estudo, os padrões são classificados conforme o seu domínio de aplicação, sendo de nível organizacional, usuário, criptografia, rede e software.

Yoder e Barcalow (1997) introduziram pela primeira vez o conceito de arquitetura de segurança como padrão, fornecendo uma descrição de sete padrões de segurança: *Single Access Point, Check Point, Roles, Session, Full View with Errors, Limited View,* e *Secure Access Layer Patterns*. A publicação de Steel et al. (2005) contém uma coleção de 23 padrões de arquitetura de segurança que abrange os fundamentos de segurança em aplicações Java.

Kienzle et. al. (2006) publicaram o catálogo *Security Patterns Repository Version 1.0,* composto por 29 padrões de segurança focados no domínio de segurança para aplicações *web*. Os padrões são divididos entre padrões estruturais e padrões processuais. Padrões estruturais são padrões que podem ser incorporados na arquitetura e implementação de software. Padrões

processuais podem ser usados para melhorar o processo de desenvolvimento e segurança crítica de software.

Em seu catálogo, Blakley e Heath (2004) fornecem um conjunto de 13 padrões de desenvolvimento, definidos para fornecerem uma estrutura para a construção de sistemas seguros. Os padrões se dividem em padrões para disponibilidade de sistemas e padrões para proteção de sistemas. Padrões para disponibilidade de sistemas oferecem soluções para facilitar a construção de sistemas que ofereçam acesso ininterrupto de recursos e serviços para os usuários. Padrões para proteção de sistemas oferecem soluções que facilitam a construção de sistemas que protegem os recursos contra o uso, divulgação ou modificações não autorizadas.

Dougherty et al. (2009) descreve em seu catálogo um conjunto de padrões de segurança que fornecem orientações gerais para eliminar vulnerabilidades em códigos de software. Os 15 padrões deste catálogo são divididos em três classes: (a) Padrões de nível de arquitetura, focam na alocação de alto nível de responsabilidades entre os diferentes componentes de um sistema e definem como deve ser a interação entre estes componentes; (b) Padrões de nível de projeto, descrevem como projetar e implementar partes de um componente do sistema; e (c) Padrões de nível de implementação, abordam questões de segurança em baixo nível e são geralmente aplicados na execução de funções específicas no sistema.

Cerca de 50 padrões de segurança são apresentados por Schumacher et al. (2006) em seu catálogo. O catálogo aborda o uso de padrões em vários níveis de abstração, não limitados a padrões de arquitetura e desenvolvimento. Os padrões propostos por Schumacher et al. (2006) abordam desde processos a nível de organização, nível de sistemas e nível operacional, possibilitando qualquer organização projetar uma arquitetura de segurança. Os padrões são organizados nos domínios de segurança empresarial, gestão de riscos, identificação e autenticação, controle de acesso, contabilidade, arquitetura de *firewall* e segurança para aplicações de Internet.

Além destes autores, podemos destacar ainda os trabalhos de Rosado et al. (2006), Romanosky (2002, 2003). Rosado et al. (2006) publicou em seu trabalho um estudo de um conjunto de padrões de segurança que ajudam a implementar requisitos de segurança em projetos de software com o objetivo de torná-los mais seguros, de forma mais prática e eficiente. Romanosky (2002, 2003) publicou alguns trabalhos com padrões voltados para a aplicação de segurança operacional, segurança em linguagem de programação, padrões de segurança empresarias e padrões de segurança integrados a engenharia de software.

Beckers et al. (2011) observam que os padrões de segurança satisfazem os requisitos de segurança em diversos domínios, através da reutilização de práticas bem sucedidas para a segurança da informação. Neste sentido, padrões de segurança possuem potencial para serem associados a modelos de referência e podem ser utilizados para implementar um processo de gestão de riscos de segurança da informação.

De acordo com Hafiz, Adamczyk e Johnson (2007) e Bunke, Koschke e Sohr (2012), os catálogos de padrões incluem uma descrição do padrão, uma identificação do problema a qual ele propõe resolver e a solução para o problema. A solução descreve as tarefas, a sequência de execução, papéis, relacionamento entre padrões, detalhados suficientemente para facilitar sua implementação.

Os padrões de segurança, para serem considerados como tal, devem ser descritos de forma clara e adequada, contendo informações suficientes para implementar atividades que sejam aplicáveis para resolver os problemas aos quais se propõe (HEYMAN et al., 2007; HAFIZ; ADAMCZYK; JOHNSON, 2007). De acordo com estes autores, uma boa descrição de um padrão de segurança deve, pelo menos, conter os seguintes elementos:

- Nome e descrição: Identifica e descreve os objetivos do padrão;
- Contexto: Descreve as situações em que o padrão pode ser aplicado;
- Problema: Problema endereçado ao padrão, incluindo uma discussão de suas forças associadas;
- Solução: Compreende nos passos indicados e nas suas relações para resolver o problema;
- Dinâmica: Descreve uma sequência típica de execução da solução;
- Implementação: Fornece as diretrizes para a implementação do padrão. É descrito em nível suficientemente detalhado para que seja possível sua implementação, inclusive com exemplos;
- Consequências: Descreve os benefícios que são esperados ao se aplicar o padrão.

Os elementos acima mostram uma forma geral de descrever os padrões, embora não seja a única forma de descrevê-los.

A seguir, um exemplo de padrão de segurança, em que são descritos, de forma resumida, os elementos para a sua implementação:

**Nome:** *Security Needs Identification for Enterprise Assets*

**Descrição:** Identifica as reais necessidades de segurança e quais propriedades de segurança devem ser aplicadas para um determinado contexto. Propriedades de segurança consideradas pelo padrão incluem a confidencialidade, integridade, disponibilidade e responsabilidade.

**Contexto:** A empresa necessita considerar a segurança como um importante requisito não-funcional. Para isso, os fatores críticos de negócio e seus ativos devem ser compreendidos.

**Problema:** A empresa deve considerar e planejar a segurança de forma adequada e em conformidade com os processos de negócios globais dela. Para os sistemas de TI, a empresa precisa adotar medidas de segurança de acordo com as suas necessidades. Como identificar as reais necessidades de segurança da empresa?

**Solução:** Identificar formalmente e de forma sistemática os tipos de ativos de negócio que necessitam de proteção e determinar os tipos de proteção que eles precisam. Esta atividade é geralmente desenvolvida por gestores e analistas, e inclui cinco etapas:

a. Identificar os ativos de negócios da empresa.
b. Identificar os fatores de negócio que influenciam as necessidades de segurança e proteção dos ativos.
c. Determinar a relação dos ativos com os fatores de negócio
d. Identificar as propriedades de segurança (confidencialidade, integridade e disponibilidade) que podem ser necessárias.
e. Com base nos fatores de negócio, determinar para cada tipo de ativo quais as propriedades de segurança são necessárias.

**Dinâmica:** Uma sequencia recomendável para a realização das etapas da solução é apresentada na Figura 5.

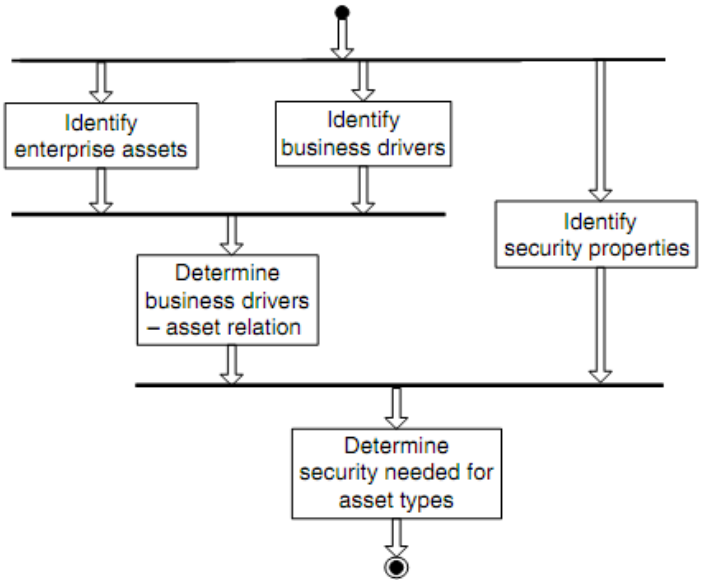


Figura 5 - *Security Needs Identification for Enterprise Assets*.

**Implementação:** Detalhes da implementação deste padrão são descritos da seção 4.2.1.

**Consequências:** A aplicação deste padrão pode trazer os seguintes benefícios:

- Facilita a tomada de decisões sobre as necessidades de segurança para os ativos da empresa, possibilitando uma distinção entre os ativos mais críticos e a garantia de que estes receberão a segurança necessária;
- Possibilita uma rastreabilidade dos ativos da empresa com os fatores relevantes do negócio. Estas informações oferecem uma base para a escolha das melhores abordagens para as medidas de segurança.

  Responsabilidades na execução do padrão:
- Requer que os gestores e analistas tenham um bom conhecimento dos ativos e dos fatores de negócio, além de tempo necessário para a execução das atividades;
- É necessário dar sequencia as atividades fazendo uso da aplicação dos padrões seguintes.

## 3.3 Conclusões parciais

Neste capítulo pode-se observar que existe um esforço de diversos autores em capturar as melhores práticas para o desenvolvimento de atividades e processos relacionados com a segurança das informações. Estas práticas são então documentadas e formam o que a literatura chama de catálogo de padrões, onde cada autor descreve o contexto de aplicação das soluções descritas por cada padrão e como elas devem ser implementadas e integradas com outras atividades.

Pode-se perceber que padrões de segurança foram concebidos, principalmente, para incorporar segurança em processos de desenvolvimento de software. Porém, alguns catálogos trazem padrões que descrevem atividades de segurança que podem ser usadas em nível organizacional, como é o caso dos catálogos de Schumacher et al. (2006), Kienzle et al. (2006) e Scarfone et al, (2008). Estes catálogos contém a descrição de soluções que podem servir para implementar as recomendações descritas na norma NBR ISO/IEC 27005:2008.

No capítulo 5 deste trabalho é descrito o processo de análise das soluções dos padrões de segurança, a fim de verificar o atendimento, ou não, das diretrizes propostas por cada atividade da norma NBR ISO/IEC 27005:2008.

# 4 MÉTODO DA PESQUISA

A pesquisa é um procedimento formal que tem como principal característica ser um procedimento reflexivo e sistemático, que permite descobrir novos fatos ou dados, ou as relações entre eles, em qualquer campo do conhecimento, que requer um tratamento científico e se constitui no caminho para conhecer a realidade ou para descobrir verdades, mesmo que parcialmente (MARCONI; LAKATOS, 2010).

Este trabalho utiliza como método a Pesquisa Indutiva, já que utiliza argumentos que se apoiam fundamentalmente em premissas. Este trabalho fundamenta-se na premissa de que se padrões de segurança são descritos como práticas recomendadas para resolver problemas recorrentes de segurança da informação, podem servir para implementar atividades descritas em normas de segurança. Na pesquisa Indutiva, pode-se afirmar que as premissas de um argumento indutivo correto sustentam, com certa verossimilhança, uma conclusão verdadeira (MARCONI; LAKATOS, 2010).

Do ponto de vista de sua natureza, esta pesquisa classifica-se como sendo Aplicada, pois objetiva gerar conhecimentos para a aplicação prática dirigida à implementação da gestão de riscos em segurança da informação baseada em normas de segurança. Quanto à forma de abordagem, esta pesquisa é de cunho Qualitativo. De abordagem Qualitativa, pois parte da interpretação de contextos para a atribuição de significados. Este trabalho faz uma leitura da estrutura do processo da norma NBR ISO/IEC 27005:2008, identificando as diretrizes de cada atividade e apresenta padrões de segurança que descrevem soluções de gestão de riscos que satisfazem as diretrizes da norma, implicando em melhor compreensão no desenvolvimento das atividades de gerenciamento dos riscos. A abordagem Quantitativa se justifica por traduzir em números opiniões e informações sobre os fatores de riscos, coletados no ambiente de estudo, em que estes números são utilizados para calcular o risco final de cada ativo e, posteriormente, são classificados e analisados.

De acordo com Richardson (1999) a pesquisa Exploratória é realizada em área na qual há pouco conhecimento acumulado e sistematizado, e visa aprofundar questões a serem estudadas e ganhar maior conhecimento sobre o tema. O estudo Exploratório tem como objetivo encontrar ideias e novas relações para elaborar explicações prováveis. Portanto, uma vez que existem poucos estudos acadêmicos e científicos acerca dos aspectos de gerenciamento de risco em segurança da informação com base na norma NBR ISO/IEC

27005:2008 e se desconhece a utilização de padrões de segurança para implementar as atividades da norma, esta pesquisa se caracteriza como Exploratória.

Quanto aos fins, esta pesquisa pode ser classificada, também, como Descritiva, já que expõe características de determinado fenômeno, em que o pesquisador tende a analisar seus dados indutivamente, em que o processo e seu significado são os focos principais de abordagens. Ainda quanto aos fins, a pesquisa ainda caracteriza-se como Estudo de Caso, já que é uma investigação empírica que investiga um fenômeno dento do contexto da vida real, principalmente quando os limites entre o fenômeno e o contexto não estão claramente definidos. A gestão de riscos de segurança da informação com base na norma NBR ISO/IEC 27005:2008 usando as soluções propostas pelos padrões de segurança é um fenômeno na realidade das organizações que ainda não está claramente definido.

Segundo Marconi e Lakatos (2010) a pesquisa Bibliográfica é o estudo sistematizado desenvolvido com base em material publicado em livros, revistas, jornais, anais de eventos ou repositórios eletrônicos. A revisão bibliográfica supre as deficiências de conhecimento que o pesquisador tem acerca de uma determinada área de conhecimento. O levantamento bibliográfico deste trabalho se concentrou em publicações sobre segurança da informação, gerenciamento de riscos, normas de segurança da informação e padrões de segurança. Os temas segurança das informações, gerenciamento de riscos e normas de segurança possuem um bom acervo bibliográfico de livros e trabalhos publicados e são facilmente encontrados. Quanto à norma NBR ISO/IEC 27005:2008, por ser uma norma um tanto quanto recente ainda não existem muitos trabalhos que abordam o seu uso em organizações, fornecendo poucas evidências sobre a sua aplicação prática. Neste caso, a própria norma foi usada para estudo e compreensão de seus processos. Além disso, uma das principais fontes de pesquisa utilizada foi o portal *IEEE Xplore*[3], que reúne as principais publicações internacionais de trabalhos na área de computação, e foi a principal fonte de consulta sobre padrões de segurança, já que no Brasil ainda existem poucos trabalhos que fazem referência a este assunto. Os capítulos 2 e 3 deste trabalho fazem referência ao estudo bibliográfico realizado neste trabalho.

Padrões de segurança formam o ponto central da proposta, pois descrevem pequenos processos, ou partes de processo, que podem ser reusados para compor diferentes processos. Deste modo, a principal contribuição está na proposição de utilizar padrões de segurança para garantir o uso de práticas recomendadas na implementação de soluções de gestão de risco

[3] http://ieeexplore.ieee.org

segundo as diretrizes da norma NBR ISO/IEC 27005:2008. Porém, para se chegar à proposta de quais padrões serão utilizados para implementar as atividades da norma foi necessário, através da revisão de literatura, identificar, classificar e selecionar os catálogos de padrões de acordo com seu contexto de aplicação. Após, nestes catálogos, são identificados e selecionados padrões de segurança que descrevem soluções que podem ser aplicadas no contexto da gestão de riscos. Em seguida, estas soluções são analisadas de acordo com os objetivos das atividades da norma NBR ISO/IEC 27005:2008. Caso a solução proposta pelo padrão atenda a algum objetivo proposto pela norma, ele é então associado com a atividade atendida. Este processo de identificação, classificação e associação dos padrões de segurança com as atividades da norma NBR ISO/IEC 27005:2008 é detalhado na seção 5.2 e 5.3 deste trabalho.

Finalmente, a fim de verificar a aplicabilidade e os resultados da utilização das soluções propostas pelos padrões de segurança, foi realizado um estudo de caso, em que o resultado da análise e avaliação dos riscos dos ativos foi centrado na aplicação das tarefas e ferramentas propostas pelos padrões de segurança, associados a estas atividades. O estudo de caso é detalhado no capítulo 6 deste trabalho.

# 5 PROPOSTA DE UTILIZAÇÃO DE PADRÕES DE SEGURANÇA PARA DESENVOLVER ATIVIDADES DO PROCESSO DE GESTÃO DE RISCOS

Este capítulo descreve uma proposta de se utilizar padrões de segurança para implementar uma gestão de riscos baseada na norma NBR ISO/IEC 27005:2008, em que são utilizados padrões de segurança que atendam as diretrizes das atividades da norma. A seção 5.1 apresenta a fundamentação da proposta, a seção 5.2 descreve o processo de identificação e escolha dos padrões de segurança, na seção 5.3 é descrito como que os padrões podem implementar as atividades da norma NBR ISO/IEC 27005:2008. Na seção 5.4 são apresentadas as conclusões parciais do capítulo.

## 5.1 Fundamentação da proposta

Baseado no que foi exposto através da revisão de literatura, percebe-se que a gestão da segurança da informação tem como base a gestão de riscos. Para a organização poder priorizar e tomar medidas de segurança atendendo as áreas mais críticas para o negócio é necessário aplicar uma metodologia que identifique os riscos que podem comprometer os ativos e causar danos aos processos.

A maioria das organizações de pequeno e médio porte possuem poucos conhecimentos sobre normas e metodologias para gestão de riscos de segurança da informação, ou simplesmente não as seguem. Isto pode ser percebido porque muitos profissionais da área de Tecnologia da Informação e Comunicação (TIC) não possuem formação ou conhecimentos suficientes em segurança da informação, o que acaba contribuindo para que as organizações não tenham uma forma sistemática de analisar e avaliar os riscos.

Apesar de existir diferentes metodologias para gestão de riscos, observa-se que praticamente nenhuma delas diz como as diretrizes da norma NBR ISO/IEC 27005:2008 podem ser implementadas. Apenas a metodologia CRAMM (MARQUIS, 2006) cita a norma ISO/IEC 17799 como modelo de referência a qual ela pode atender. Além disso, outro fator a

destacar é que grande parte das metodologias tratam apenas de uma parte das atividades do processo de gestão do risco, não contemplando o processo como um todo.

As metodologias OCTAVE (ALBERTS e DOROFEE, 2004) e NIST SP 800-30 (NIST, 2002), apesar de descreverem atividades de forma detalhada para gerenciar os riscos, possuem uma documentação muito extensa e seus processos exigem um bom nível de experiência da organização para serem implementados. Isto acaba fazendo com que as organizações não saibam qual metodologia usar ou acabam escolhendo uma metodologia que não é adequada para o seu contexto, o que pode acarretar em um processo ineficaz.

Para garantir o alinhamento com as melhores práticas é necessário seguir procedimentos que estão descritos em normas. Deste modo, a proposta descrita nesta dissertação é utilizar como referência a norma NBR ISO/IEC 27005:2008, que normaliza os processos para a gestão de riscos de segurança da informação. Porém, a norma NBR ISO/IEC 27005:2008 diz "o que" deve ser feito para que os objetivos de cada atividade sejam atingidos, mas não detalha "como fazer". Para tentar resolver o problema do "como fazer", é proposta a utilização de padrões de segurança para desenvolver as atividades da norma, já que os padrões de segurança apresentam soluções objetivas para problemas de segurança através de tarefas detalhadas que capturam práticas descritas por especialistas.

O problema é que a maioria dos padrões de segurança está espalhada em diversos catálogos, o que acaba dificultando a identificação de padrões que podem ser aplicados no contexto da gestão de riscos. Na seção 5.2 é discutido como que os padrões de segurança podem ser identificados e selecionados.

## 5.2 Processo de identificação de padrões de segurança

Como visto no capítulo 3 desta dissertação, existem diversos padrões de segurança que estão esparsos em vários catálogos, e estes catálogos muitas vezes não são organizados por contexto de aplicação. Isto quer dizer que um catálogo pode ter padrões que servem para diversas aplicações, o que acaba dificultando a identificação dos padrões. Uma forma de facilitar a identificação dos padrões e verificar se eles podem ser aplicados para atender aos objetivos da norma NBR ISO/IEC 27005:2008 é ilustrada na Figura 6.

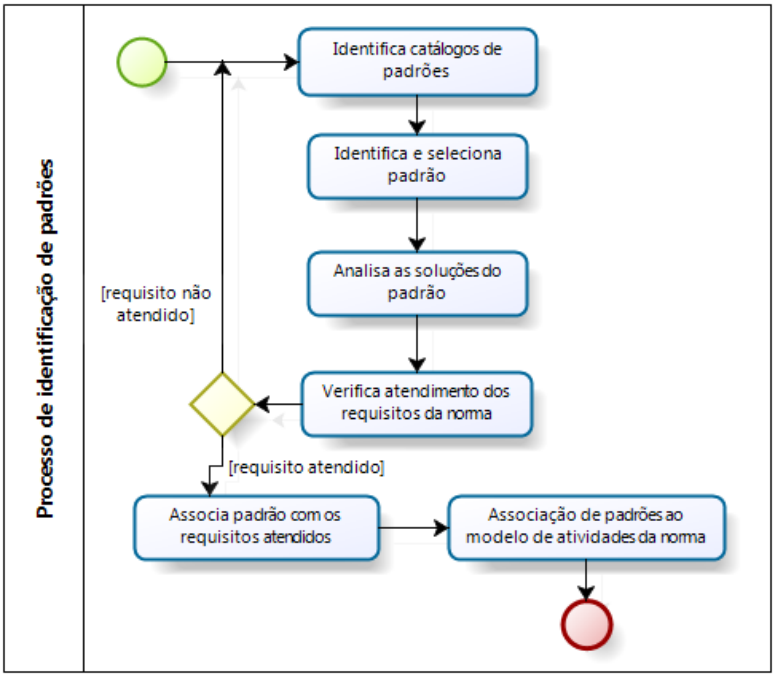


Figura 6 - Processo de identificação de padrões de segurança.

Para facilitar a identificação dos padrões de segurança, primeiramente, é necessário identificar os catálogos de padrões de acordo com os domínios em que as soluções podem ser aplicadas. Esta etapa foi auxiliada com o trabalho de Bunke, Koschke e Sohr (2012), que classifica os catálogos em cinco domínios de aplicação: organizacional, rede, usuário, software e criptografia. Este trabalho foca nos catálogos que descrevem padrões de domínio organizacional, rede e software, o que possibilitou reduzir o esforço para selecionar quais são realmente os catálogos que devem ser pesquisados. Apesar de a maioria dos catálogos tratarem de vários domínios de aplicação, internamente eles são organizados por contextos de aplicação, fazendo com que a procura dentro destes catálogos também seja otimizada. Um dos únicos catálogos onde foi encontrada uma seção exclusiva com padrões para gestão de riscos foi o de Schumacher et al. (2006), fazendo com que este catálogo apresente um número maior de padrões sobre gerenciamento de riscos. Porém, outros catálogos como o de Kienzle et al. (2006) e Scarfone et al. (2008) não possuem padrões exclusivos sobre riscos, mas possuem padrões que podem atender a objetivos específicos do processo de gerenciamento de riscos.

Após os catálogos terem sido identificados, é feito a identificação dos padrões dentre destes catálogos. Como a descrição da maioria dos padrões segue uma forma padronizada, a identificação preliminar dos padrões pode ser feita através do nome. Por exemplo, os padrões *Asset Valuation*, *Threat Assessment*, *Vulnerability Assessment* e *Risk Determination* possuem

nomes ligados diretamente com atividades de gestão de riscos, o que facilita a sua seleção. Para os outros padrões é necessário verificar, além do nome, a descrição do seu contexto de aplicação, para poder saber se ele pode atender algum requisito da norma. Por exemplo, o padrão *Share Responsibility for Security* não possui um nome ligado diretamente com alguma atividade da norma, mas analisando o seu contexto de aplicação podemos identificar ações que podem atender ao requisito "determinar as responsabilidades para gestão de riscos" da atividade de Definição do Contexto da norma NBR ISO/IEC 27005:2008.

Somente a identificação do nome e do contexto de aplicação não é suficiente para garantir que o padrão atenda as diretrizes da norma. Deste modo, após a identificação preliminar dos padrões, é feito uma análise mais criteriosa das soluções propostas por estes padrões. Nesta etapa, o resultado das soluções propostas pelos padrões é comparado com os requisitos e diretrizes da norma NBR ISO/IEC 27005:2008, a fim de se verificar o nível de atendimento dos requisitos. Se a solução atende de forma satisfatória algum requisito da norma, ele é associado com aquela atividade da norma cujo requisito é atendido. Caso contrário, o padrão é descartado e uma nova iteração de identificação de catálogos e padrões pode ser feita, a fim de identificar outros padrões que possam satisfazer os requisitos da norma ainda não atendidos.

Por exemplo, o padrão *Security Needs Identification for Enterprise Assets* implementa soluções que atendem apenas parte dos requisitos da atividade de Definição do Contexto da norma NBR ISO/IEC 27005:2008. Para que os outros requisitos da atividade de Definição do Contexto possam ser atendidos é necessário identificar e selecionar outro padrão de segurança, neste caso o padrão *Share Responsibility for Security*.

Outra característica que é importante destacar é o fato de que na descrição dos padrões são mostrados exemplos de aplicação, o que dá uma visão mais detalhada dos resultados que podem se atingidos, possibilitando inclusive se ter uma noção do grau de dificuldade na hora da implementação do padrão de segurança.

Desta forma, salienta-se que uma das características desta metodologia é que ela permite uma flexibilidade na escolha dos padrões, já que não é necessário que um único padrão atenda a todos os requisitos de uma atividade da norma, podendo ser complementado com a utilização de outros padrões ou partes de padrões. Isto reforça também a possibilidade de se utilizar novos catálogos e padrões que podem surgir com o passar do tempo, possibilitando manter a metodologia sempre atualizada.

Após os padrões serem associados com os requisitos atendidos, de cada atividade, forma-se a associação destes padrões com o modelo de atividades proposto pela norma, em

que a implementação dos padrões segue o fluxo de implementação das atividades de gestão de riscos proposto pela norma NBR ISO/IEC 27005:2008 (vide Figura 2).

Como resultado deste processo, foram identificados 22 padrões de segurança que possuem soluções que podem ser aplicadas no âmbito da gestão de riscos. Vale ressaltar que estes podem não ser os únicos padrões que podem ser aplicados na gestão de riscos e, dependendo do contexto da análise de riscos, outros padrões podem ser selecionados. O Quadro 2 lista os padrões identificados e uma breve descrição de cada um deles.

| **Padrão de Segurança** | **Descrição** |
|---|---|
| *Security needs Identification for Enterprise Assets* (SCHUMACHER et al., 2006) | Identificar as necessidades de segurança e quais propriedades de segurança que devem ser aplicadas para cada ativo. |
| *Asset Valuation* (SCHUMACHER et al., 2006) | Determinar a importância de cada ativo para os negócios da empresa. |
| *Threat Assessment* (SCHUMACHER et al., 2006) | Identificar as ameaças aos ativos; determinar a probabilidade e o potencial de prejuízo de cada ameaça. |
| *Vulnerability Assessment* (SCHUMACHER et al., 2006) | Identificar as vulnerabilidades dos ativos da empresa e a gravidade caso sejam exploradas. |
| *Risk Determination* (SCHUMACHER et al., 2006) | Analisar, avaliar e priorizar os riscos para os ativos. |
| *Enterprise Security Approaches* (SCHUMACHER et al., 2006) | Selecionar a abordagem de segurança para fornecer uma base de decisão sobre quais controles aplicar. As abordagens são prevenir, detectar ou responder. |
| *Enterprise Security Services* (SCHUMACHER et al., 2006) | Orienta na seleção de controles de segurança para proteger os ativos da empresa. |
| *Enterprise Partner Communication* (SCHUMACHER et al., 2006) | Assegurar que as partes envolvidas com atividades de segurança tenham uma coordenação aberta da comunicação entre grupos de segurança, com outros grupos de parceiros e grupos externos. |
| *Share Responsibility for Security* (KIENZLE et al., 2006) | Definir os papéis e as responsabilidades de cada participante do processo de segurança. |
| *Document the Security Goals* (KIENZLE et al., 2006) | Documentar as metas de segurança baseadas nos objetivos gerais da organização e seus negócios. |
| *Security Accounting Requirements* (SCHUMACHER et al., 2006) | Definir um conjunto de requisitos de responsabilidades sobre as atividades de segurança. Resolver os conflitos entre os requisitos de segurança e processos de negócio. |
| *Security Accounting Design* (SCHUMACHER et al., 2006) | Desenvolver um plano de revisão das responsabilidades sobre a segurança. |
| *Audit Requirements* (SCHUMACHER et al., 2006) | Definir um conjunto de requisitos para auditoria nos processos de gestão de riscos. |
| *Audit Design* (SCHUMACHER et al., 2006) | Criar mecanismos de auditoria que satisfaçam os seus requisitos. |
| *Audit Trails & Logging Requirements* (SCHUMACHER et al., 2006) | Definir um conjunto de requisitos de trilhas de auditoria e registros de logs para permitir a reconstrução e análise de eventos. |

(conclusão)

| Padrão de Segurança | Descrição |
|---|---|
| *Audit Trails & Logging Design* (SCHUMACHER et al., 2006) | Fornecer orientações para criar trilhas de auditoria e mecanismos de registros de logs. |
| *Non-Repudiation Requirements* (SCHUMACHER et al., 2006) | Definir um conjunto de requisitos para manter as evidências em que os usuários não podem negar que participaram de determinadas atividades. |
| *Non- Repudiation Design* (SCHUMACHER et al., 2006) | Fornecer orientações para criar mecanismos de não-repúdio. |
| *Documentation Review* (SCARFONE et al., 2008) | Revisar todos os documentos (políticas de segurança, requisitos, procedimentos, memorandos etc.), provenientes das atividades de segurança a fim de localizar lacunas e deficiência nos processos. |
| *Log Review* (SCARFONE et al., 2008) | Analisar os logs para verificar a eficácia dos controles implementados e possíveis falhas nos processos. |
| *Log for Audit* (KIENZLE et al., 2006) | Garantir que os registros de *log* fazem parte dos processos de auditoria. |
| *System Configuration Review* (SCARFONE et al., 2008) | Identificar as deficiências nos controles de configuração de segurança. |

Quadro 2 - Padrões de segurança relacionados com a gestão de riscos.

Na seção seguinte é detalhado como que os padrões identificados no Quadro 2 podem atender aos objetivos das atividades da norma NBR ISO/IEC 27005:2008 através de suas técnicas, ferramentas e tarefas.

## 5.3 Associando padrões de segurança com as atividades da norma NBR ISO/IEC 27005:2008

A associação dos padrões de segurança com as atividades da norma aqui apresentado mostra como que os padrões de segurança são utilizados para implementar as atividades da norma NBR ISO/IEC 27005:2008. Toda a concepção de implantação das atividades da norma é centrada nas soluções dos padrões. A Figura 7 ilustra o diagrama de desenvolvimento das atividades da norma, salientando o uso dos padrões de segurança em uma sequência de tarefas.

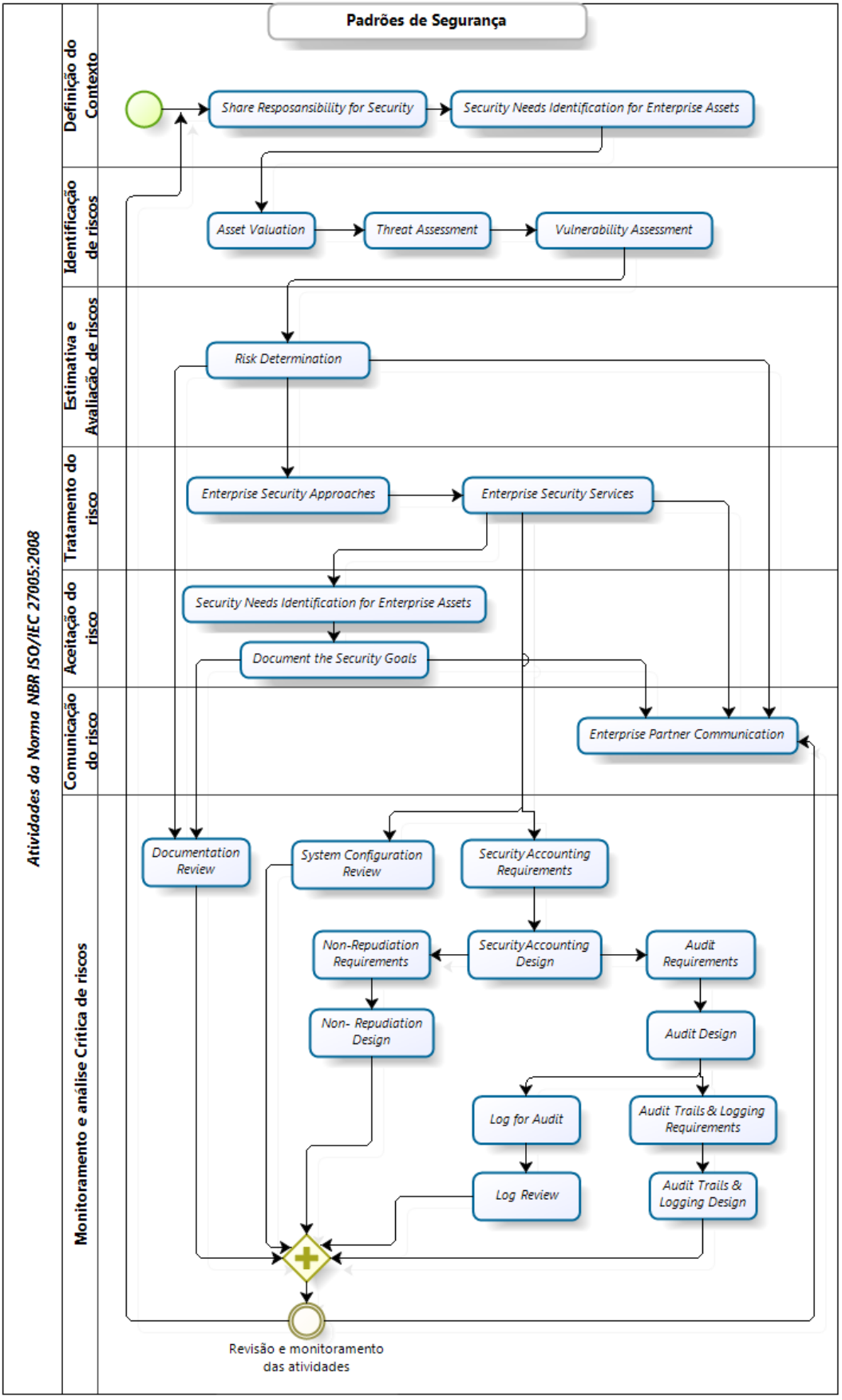


Figura 7 – Diagrama de desenvolvimento das atividades.

O processo de gestão de riscos ilustrado na Figura 7 mostra o desenvolvimento das atividades através da implementação de uma sequencia de padrões. O fluxo de execução dos padrões é organizado de forma que as informações e os resultados de cada padrão sejam utilizados para desenvolver as atividades seguintes. Alguns padrões fornecem informações que são utilizados em mais de uma atividade como, por exemplo, os resultados do padrão *Risk Determination* podem ser reutilizados pelos padrões *Enterprise Security Approaches, Enterprise Partner Communication* e *Documentation Review*. Já, por exemplo, o padrão *Enterprise Partner Communication* recebe as informações provenientes de mais de um padrão. Alguns padrões são implementados paralelamente, não necessariamente em uma sequencia, como é o caso dos padrões que implementam a atividade de Monitoramento e análise crítica de riscos. Os resultados destes padrões servirão para analisar o desempenho e a eficácia do processo de gestão de riscos, possibilitando que as partes interessadas possam reavaliar as ações desenvolvidas e reiniciar o processo novamente, formando um ciclo de melhoria. As seções 5.3.1 até 5.3.8 detalham o uso dos padrões em cada atividade.

### 5.3.1 Definição do contexto

Um processo de gestão de riscos pode ser aplicado em uma organização inteira, o que nem sempre é possível, ou pode ser dividido em áreas ou domínios menores como, por exemplo, a área de TI de uma empresa. Quando a gestão de riscos estiver implementada satisfatoriamente em setores menores, então o escopo pode ser ampliado gradativamente e incluir outras áreas. Desta forma, o processo pode se tornar mais simples. Por isso, a primeira etapa da gestão de riscos é delimitar qual será o escopo ou área que será analisada.

É recomendado pela atividade de Definição do Contexto que se leve em consideração o valor estratégico do setor ou do processo que trata as informações do negócio, a criticidade dos ativos daquele setor envolvido, a importância do ponto de vista operacional para o negócio, da disponibilidade, da confidencialidade e da integridade. É importante que se leve em consideração, também, as expectativas das partes interessadas (internas e externas) e os fatores de imagem e reputação.

Durante o planejamento e o levantamento preliminar do contexto a ser analisado é importante definir as responsabilidades e os papéis que irão colaborar com a condução do processo de análise a avaliação dos riscos. Para ajudar nesta tarefa propõe-se a utilização do

padrão *Share Responsibility for Security*, em que as responsabilidades sobre o processo de gestão de riscos devem ser divididas com os colaboradores ou funcionários chaves do contexto analisado, possibilitando que todos entendam as implicações de segurança e seus componentes, a fim de que possam contribuir em todo o ciclo do processo de análise dos riscos. Porém, é necessário que um especialista em segurança faça parte da equipe para que o processo possa ser coordenado e orientado de forma correta, mas é fundamental que as responsabilidades não recaiam somente em uma única pessoa.

Após ser mapeado quem são as pessoas que irão participar do processo é necessário fazer um levantamento do ambiente que será analisado. Este levantamento tem por objetivo identificar primeiramente os ativos, quais os processos que estes ativos suportam e qual a importância destes processos para o negócio, já que a importância do processo irá impactar na importância dos ativos.

Para executar este levantamento, propomos a utilização do padrão *Security Needs Identification for Enterprise Assets* que ao fazer o mapeamento dos ativos com os processos de negócio facilita a tomada de decisão, pois utiliza os fatores de negócio para fazer a distinção entre ativos críticos e os não críticos. O resultado será uma maior probabilidade de que as necessidades de segurança serão priorizadas para os ativos mais críticos.

Outro benefício de se aplicar o padrão *Security Needs Identification for Enterprise Assets* é que ele mantém uma rastreabilidade das necessidades de proteção dos ativos de acordo com os fatores relevantes do negócio documentada. Esta informação é útil para revisar e aperfeiçoar as necessidades de segurança ao longo do tempo. Além disso, este documento pode ser utilizado como apoio no planejamento dos controles de segurança para os ativos.

Nesta etapa é necessário um bom nível de envolvimento das pessoas que possuem conhecimento dos ativos e dos fatores de negócio envolvidos para que a obtenção dos resultados seja precisa.

Como principal resultado desta etapa será construído uma tabela com os ativos críticos que deverão ser analisados e as propriedades de segurança que deverão ser preservadas. O próximo passo será identificar os fatores que podem impactar na segurança dos ativos, portanto na seção seguinte será descrita a atividade de Identificação de Riscos.

### 5.3.2 Identificação de riscos

A atividade de Identificação de riscos tem o objetivo de identificar os principais fatores associados aos ativos que podem impactar negativamente na segurança das informações, os riscos. Para isso, devemos identificar quais são as ameaças que podem comprometer os ativos e quais são as vulnerabilidades que estes ativos possuem e que podem ser exploradas pelas ameaças identificadas.

São as ameaças e as vulnerabilidades identificadas que irão determinar o nível de riscos de um ativo. Por exemplo, se for identificado ameaças a um ativo, mas não for identificado vulnerabilidades, podemos dizer que o risco será quase nulo. Em contrapartida, caso seja identificado um grande número de ameaças e o ativo possuir várias vulnerabilidades, o risco será bastante elevado. Portando, para que possamos calcular o nível do riscos de cada ativo devemos medir a probabilidade de as ameaças ocorrerem, o nível de gravidade das vulnerabilidades encontradas, assim como determinar o valor do ativo para a organização.

O padrão *Asset Valuation* pode ser utilizado na atividade de Identificação de riscos para identificar de forma sistemática o valor global dos ativos. Para definição do valor global é necessário identificar o valor de segurança, o valor financeiro e o valor para o negócio de cada ativo. O valor de segurança mede o valor do ativo baseado nas necessidades de garantia das propriedades de segurança. Por exemplo, se for necessário garantir a confidencialidade, a integridade e a disponibilidade ao mesmo tempo, dizemos que o ativo possui um alto valor de segurança. O valor financeiro dá a possibilidade de valorar o ativo conforme o seu custo em termos monetários. Já o valor para o negócio determina a importância do ativo para que se atinja os objetivos de negócio.

O valor global atribuído ao ativo é definido pelo maior valor atribuído aos critérios de segurança, financeiro e importância. Por exemplo, um ativo pode ter um baixo valor financeiro, porém é muito importante para o desempenho dos processos de negócio e ainda necessita estar sempre disponível (disponibilidade). Portanto, o valor global deste ativo será medido pela importância que representa para os processos de negócio.

Com a aplicação do padrão *Asset Valuation* é possível a empresa obter uma visão mais completa de quais ativos são mais críticos. O resultado da avaliação dos ativos pode ser usado também para desenvolver ou atualizar o plano de recuperação de desastres e continuidade dos negócios da empresa, caso ela possua.

Com os ativos identificados e valorados, a próxima tarefa será identificar as ameaças aos ativos e determinar a probabilidade ou a frequência de sua ocorrência. Para executar a tarefa de identificar e definir o grau das ameaças propõe-se a utilização do padrão *Threat Assessment*. Para cada ativo é feito um levantamento das possíveis ameaças e construída uma tabela onde serão associados os ativos com as suas respectivas ameaças. O agrupamento das ameaças por ativo facilita o processo da determinação do risco final mais adiante. Após ter sido construída a tabela das ameaças, cada relação "ativo x ameaça" é avaliada a probabilidade da ameaça ocorrer. A fim de otimizar esta tarefa é importante que seja identificada somente as ameaças que realmente tem potencial de ocorrem.

O resultado da aplicação do padrão *Threat Assessment* será uma lista de ameaças agrupadas por ativos e classificadas conforme a sua probabilidade de se concretizar. Isto possibilita a empresa compreender melhor os fatores que podem causar algum evento danoso.

Após a identificação e classificação das ameaças faz-se a identificação das vulnerabilidades que estão associadas a estas ameaças. Com a aplicação do padrão *Vulnerability Assessment* é possível construir uma tabela que relaciona cada ameaça com as vulnerabilidades que podem estar presentes e que podem ser exploradas. Uma vulnerabilidade pode ser explorada por várias ameaças, mas dependendo da ameaça e do ativo, uma vulnerabilidade poderá ser mais grave ou menos grave. Para ajudar a determinar a gravidade de uma vulnerabilidade utilizamos a escala de gravidade do padrão *Vulnerability Assessment*, que possibilita atribuir um valor para cada vulnerabilidade identificada.

Como resultado da aplicação do padrão *Vulnerability Assessment* a empresa obtém uma visão mais detalhada das vulnerabilidades que podem afetar os seus ativos ou sistemas. Estas informações são importantes e podem ser usadas para o planejamento de ações para corrigir as falhas encontradas.

A utilização de uma escala qualitativa para atribuir o valor global dos ativos, a probabilidade das ameaças e a gravidade das vulnerabilidades, ao invés de escalas quantitativas, pode agilizar o processo de análise e avaliação do risco. Portanto, para manter a coerência entre os valores em todo o processo de análise e avaliação dos riscos será utilizada uma escala de avaliação qualitativa padrão definida em cinco valores, conforme o Quadro 3.

Os resultados da atividade de Identificação de riscos serão utilizados para calcular o risco de cada ativo. A atividade de Estimativa dos riscos está detalhada na seção seguinte.

| Escala | Valor qualitativo |
|---|---|
| 5 | Muito alto |
| 4 | Alto |
| 3 | Médio |
| 2 | Baixo |
| 1 | Muito baixo |

Quadro 3 – Escala de avaliação e valores qualitativos.

### 5.3.3 Estimativa de riscos

Uma organização deve direcionar os seus esforços para proteger aqueles ativos mais sensíveis contra os incidentes de segurança, e para isso ela deve conhecer o nível de risco dos seus ativos. A atividade de Estimativa de riscos consiste justamente em atribuir valor ao risco final de cada ativo identificado.

A combinação de uma ameaça com uma vulnerabilidade pode afetar várias ativos ao mesmo tempo, porém poderão ter o grau de probabilidade e impacto diferente para diferentes ativos. Portanto, deve-se considerar o risco individual para cada ativo. Para tornar o cálculo do risco o mais preciso possível cada ativo deve ser associado com os seus pares de ameaças e vulnerabilidades correspondentes, com seus respectivos valores de probabilidade e impacto.

Para calcular o risco devem ser utilizadas as informações obtidas na atividade anterior de Identificação de riscos. Os resultados dos três fatores avaliação global dos ativos, avaliação das ameaças e avaliação das vulnerabilidades serão usados para calcular o valor final do risco. Propõe-se para esta atividade a utilização do padrão *Risk Determination*, pois este padrão utiliza uma equação para o cálculo do risco que leva em consideração estes três fatores. A equação (1) demonstra este cálculo.

$$\textbf{Risco(A) = SOMA[Ameaça * Vulnerabilidade](A) * Valor do ativo(A)} \quad (1)$$

O risco para o ativo “A” é a soma de todas as combinações “probabilidade da ameaça *versus* gravidade da vulnerabilidade”, multiplicado pelo valor global do ativo “A”. Uma das vantagens em se utilizar esta equação é que ela leva em consideração o valor do ativo, ou seja, quanto mais importante o ativo for para a organização maior será o valor do risco. Outra

questão, também, é que quanto mais ameaças e vulnerabilidades o ativo tiver, maior será o seu risco.

Após a conclusão desta atividade, os resultados, ou seja, os riscos de cada ativo, geralmente são apresentados para as pessoas interessadas como gestores e participantes do processo de gestão de riscos. Para isso, os resultados devem ser organizados de forma que todos possam compreendê-los, e é detalhado na atividade seguinte de Avaliação de riscos.

### 5.3.4 Avaliação de riscos

Após calcular o risco de cada ativo, as informações obtidas na atividade de Estimativa de riscos devem ser disponibilizadas de tal forma que os gestores da organização possam interpretar e compreender o nível do risco que a organização se encontra e os fatores que contribuem para o cenário de risco.

Nesta atividade, utiliza-se ainda as orientações e tarefas do padrão *Risk Determination*, em que os maiores valores representarão os ativos com maiores riscos de segurança, consequentemente, os com valores menores os riscos menores. Para um melhor entendimento e visualização dos resultados, principalmente se estes resultados forem apresentados à alta direção da empresa, os valores podem ser convertidos em termos qualitativos, consistentes com os usados durante todo o conjunto de padrões para análise de risco. A geração de gráficos, tabelas resumidas e relatórios de avaliação são recursos e ferramentas que podem ser utilizadas para apresentar as informações de forma mais objetiva.

O resultado desta atividade possibilita a organização avaliar quais são os ativos que estão mais suscetíveis a eventos negativos de segurança. Além disso, a organização pode comparar estes resultados com novas iterações de análise de risco. Por exemplo, após a aplicação de medidas de segurança, novos valores poderão ser comparados com valores antigos possibilitando uma análise da efetividade das medidas de segurança, formando um ciclo de gestão de riscos.

### 5.3.5 Tratamento do risco

Com os riscos calculados e classificados a organização poderá aplicar controles de segurança para que estes riscos sejam tratados e minimizados a um nível aceitável. Todavia, antes de aplicar qualquer medida de segurança é necessário avaliar qual a melhor abordagem para lidar com os riscos identificados, ou seja, se será melhor reduzir, reter, evitar ou transferir.

Para auxiliar na definição da melhor abordagem a ser considerada, propõe-se a utilização do padrão *Enterprise Security Approaches* que orienta a empresa na seleção da melhor abordagem de tratamento dos riscos, pois leva em consideração não somente o risco que a organização corre por estar exposta, mas também o valor de cada ativo, o custo e viabilidade de resolução das falhas e as metas de segurança a qual a organização planeja. Esta tarefa deverá ser executada em conjunto da equipe responsável pelo processo de gestão da segurança com os gestores da organização, já que a escolha das abordagens envolve considerar a necessidade de alocação de recursos financeiros para implementar medidas de segurança.

Nem sempre os riscos identificados poderão ser aceitos, evitados ou transferidos, o que implica na aplicação de medidas de segurança para diminuir o risco a um nível previamente aceito pela organização. O padrão *Enterprise Security Service* poderá ser utilizado como guia na construção de um plano de implementação de controles de segurança.

A seleção das medidas de segurança deverá estar em conformidade com as necessidades de segurança do ativo identificadas na atividade de Definição do contexto (seção 5.3.1). A prioridade de quais controles de segurança devem ser implantados primeiro será determinada pela classificação do risco definida na atividade de Avaliação dos riscos (seção 5.3.4), entretanto controles que são fáceis e rápidos de serem implementados podem ser aplicados antes.

Um dos resultados desta atividade, através da utilização dos padrões *Enterprise Security Approaches* e *Enterprise Security Service,* é a documentação das decisões sobre as estratégias de segurança acordadas, possibilitando uma maior garantia na alocação de recursos para proteger os ativos. As medidas de segurança devem ser constantemente revisadas para

garantir que elas ainda possuem o efeito esperado, por isso a documentação é um importante *feedback*[4] para o processo de decisão e melhoria dos serviços de segurança.

### 5.3.6 Aceitação do risco

Com a aplicação de medidas de segurança espera-se reduzir o risco ao menor nível possível. Porém é praticamente impossível reduzir o risco a zero e, em alguns casos, o custo de implantação de uma medida de segurança pode se tornar inviável. Deste modo, o objetivo desta atividade é assegurar que os riscos residuais sejam explicitamente aceito pelos gestores.

A Aceitação do risco pode tomar como referência os resultados do padrão *Security Needs Identification for Enterprise Assets*, que produz informações sobre as necessidades de segurança da organização que tem como base os fatores críticos de negócio, os ativos críticos e os processos que são afetados pelos riscos. As decisões sobre quais riscos serão toleráveis ou não devem assim ser fundamentadas de acordo com as metas e necessidades de segurança. Por exemplo, a organização pode estar submetida a leis e regulamentações onde os riscos relacionados devem estar obrigatoriamente dentro dos níveis aceitáveis, não podendo ser aceitos caso estejam fora do nível recomendado.

Decisões sobre aceitação de riscos devem ser documentadas de forma legível e consistente para que todos possam compreender tais decisões. Para isso, pode-se utilizar o padrão *Document Security Goals* para guiar a organização na documentação das decisões de segurança de acordo com as metas e objetivos gerais de negócio. A documentação torna possível o rastreamento das decisões e o porquê de terem sido tomadas, e é através dela que as decisões são comunicadas para as partes interessadas.

### 5.3.7 Comunicação do risco

Durante todo o processo de gestão de riscos é importante que o andamento e o resultado das atividades sejam comunicados às partes interessadas, possibilitando aos gestores lidar com os possíveis incidentes e eventos não previstos de maneira mais efetiva.

[4] Palavra em inglês que no português significa retorno, resposta, crítica, análise crítica.

Esta atividade pode ser desenvolvida utilizando-se o padrão *Enterprise Partner Communication*, que tem como objetivo definir os mecanismos de comunicação mais adequados de acordo com as diversas partes interessadas. Pode ser utilizado como canal de comunicação o e-mail, páginas de *intranet* com acesso restrito para centralização das informações ou reuniões de acompanhamento e divulgação dos resultados. Além disso, o padrão *Enterprise Partner Communication* corrobora na definição de quais informações deverão ser comunicadas e qual a melhor forma de estruturá-las.

A definição das responsabilidades no processo de gestão de riscos pelo padrão *Share Responsibility for Security* ajuda a identificar as partes que deverão ser comunicadas, já que elas foram identificadas na atividade de Definição do contexto (seção 5.3.1). A seleção das informações que serão comunicadas deverá estar de acordo com a responsabilidade de cada parte envolvida no processo.

As decisões sobre as ações recomendadas para os riscos e as metas de segurança da organização também devem ser comunicadas, a fim de conscientizar a todas as pessoas envolvidas, direta ou indiretamente, sobre as necessidades de segurança da empresa. Por isso, podemos utilizar os resultados das tarefas do padrão *Document the Security Goals* que foram desenvolvidas na atividade de Aceitação do risco (seção 5.3.6).

O uso do padrão *Enterprise Partner Communication* para desenvolver a atividade de Comunicação do risco tem como principal resultado um plano para gerenciar as expectativas das partes interessadas com relação às ações e procedimentos para gerenciar os riscos.

### 5.3.8 Monitoramento e análise crítica de riscos

De acordo com a norma NBR ISO/IEC 27005:2008 a atividade de Monitoramento e análise crítica de riscos tem como principais objetivos monitorar e analisar os fatores de riscos, e monitorar e analisar criticamente o processo de gestão de riscos para que possa ser melhorado, quando necessário e apropriado.

As constantes mudanças nos fatores de riscos, isto é, valores dos ativos, das ameaças, vulnerabilidades, impactos e probabilidade de ocorrência requerem que o processo de gestão de riscos seja frequentemente monitorado e analisado criticamente para que se detectem essas mudanças. De modo geral, a atividade de Monitoramento e análise crítica de riscos envolve a revisão periódica da documentação gerada pelo processo de gestão de riscos, que contém

informações provenientes de atividades como análise e avaliação dos riscos e das decisões de tratamento e aceitação dos riscos. Para implementar a tarefa de revisão do processo de gestão dos riscos foi selecionado o padrão *Documentation Review*.

O padrão *Documentation Review* fornece a base que determina se os aspectos técnicos e procedimentos são atuais e abrangentes. Este padrão determina que para garantir uma revisão abrangente, além dos documentos provenientes das atividades de gestão de riscos, devem ser revisados documentos que incluem políticas de segurança, requisitos de segurança, procedimentos operacionais padrão, planos de segurança, memorandos de acordo e entendimento e planos de resposta a incidentes. Desta forma, a revisão deve verificar se a documentação da organização é compatível com as normas e regulamentações como a NBR ISO/IEC 27001:2006, por exemplo. O padrão *Documentation Review* recomenda que esta tarefa seja acompanhada por uma assessoria especializada em gerenciamento de riscos ou segurança da informação, e o resultado da análise da documentação deve ser usado para definir quais melhorias devem ser feitas no processo de gestão de riscos.

Em ambientes de TIC a maioria dos riscos está associada a *hardware* e *software*, portanto, as medidas de segurança selecionadas para o tratamento do risco são aplicadas nestes tipos de ativos. Assim sendo, na atividade de Monitoramento e análise crítica de riscos convém que não só as atividades de monitoramento de riscos sejam repetidas regularmente, mas também se as ações tomadas na atividade de Tratamento dos riscos (seção 5.3.5) estão surtindo o efeito esperado.

Primeiramente, deve-se identificar quais são os controles que se quer monitorar e analisar. O padrão *Security Accounting Requirements* pode ser utilizado para auxiliar na identificação do conjunto de requisitos para avaliar a qualidade das ações de segurança. Os requisitos podem ser identificados a partir das medidas de segurança selecionadas para reduzir o risco. Por exemplo, o requisito “quantidade de infecções por vírus” pode ser utilizado para medir a eficácia de um sistema antivírus, ou o requisito “tentativas de acesso não autorizado ao banco de dados” para medir a eficácia de um sistema de detecção de intrusão. Após, o padrão *Security Accounting Design* ajuda a escolher a melhor abordagem para capturar e analisar os dados relacionados com os requisitos de contabilidade da segurança.

Uma das abordagens mais utilizadas para verificar os eventos que ocorrem em sistemas de informação é a auditoria. A realização frequente de auditorias pode identificar possíveis falhas e desvios no processo de gestão de riscos e é uma estratégia a ser considerada para monitorar e analisar criticamente os riscos. Uma forma de realizar auditoria é examinar,

por exemplo, os *logs*[5] dos sistemas. Os *logs* fornecem informações valiosas sobre eventos que ocorrem nos sistemas e sobre o funcionamento dos dispositivos de segurança. O planejamento, a implementação e o processo de gerenciamento dos *logs* para trilhas de auditorias podem ser desenvolvidos com o auxílio dos padrões *Audit Requirements, Audit Design, Log for Audit, Log Rewiew, Audit Trails & Logging Requirements* e *Audit Trails & Logging Design*.

Os padrões *Audit Requirements* e *Audit Design* fornecem um conjunto comum de requisitos genéricos de auditoria e ajuda a priorizá-los com orientações para criar mecanismos de auditoria que satisfaça as necessidades da organização, identificando quais registros devem ser capturados. O padrão *Log for Audit* auxilia na implementação dos sistemas de *logs* definindo que os registros devem ser armazenados num local central, de modo que o espaço em disco possa ser gerenciado e protegido contra ataques, assim como impedir que o espaço em disco ocupado pelos *logs* interfira no funcionamento dos demais sistemas. Periodicamente, os registros mais antigos devem ser movidos para armazenamentos *off-line*, a fim de liberar espaço em disco para novos registros. O padrão *Log for Audit* também ajuda a definir quem são as pessoas mais indicadas para analisar os *logs*, de acordo as capacidades da equipe. Por exemplo, os administradores de banco de dados devem examinar registros de banco de dados, enquanto administradores de rede examinam registros de atividades da rede. O padrão *Log Review* é usado para ajudar a validar se os *logs* estão sendo registrados de acordo com as políticas estabelecidas. Por exemplo, se foi estabelecida a política de registrar as tentativas de autenticação nos servidores críticos, a revisão de registro irá determinar se esta informação está sendo coletada no nível de detalhe apropriado. Isto ajuda a revelar problemas, tanto nos serviços de proteção dos sistemas e ativos quanto nos registros de *logs*.

Com base nos registros de *logs*, as trilhas de auditorias capturam as informações registradas e permitem a reconstrução e análise de eventos e atividades que ocorrem dentro de um sistema. Os padrões *Audit Trails & Logging Requirements* e *Audit Trails & Logging Design* fornecem um conjunto genérico de trilhas de auditoria que são usados para reconstruir os eventos, determinar quem é responsável pelos eventos, quais atividades ocorreram e formas de analisar os problemas. Além do registro das atividades, é importante a utilização de mecanismos que evidenciem a relação entre as pessoas e as atividades, de modo que a participação de uma pessoa em uma atividade não possa ser negada. Estes mecanismos podem ser criados com o auxílio das tarefas dos padrões *Non-Repudiation Requirements* e

[5] Em computação, *log* é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional.

*Non-Repudiation Design*, contribuindo para que as ações e as tomadas de decisões durante o processo de gestão dos riscos sejam negadas pelos participantes do processo. Além disso, ajuda a rastrear as responsabilidades pelas ações de segurança, correspondendo a uma abordagem de prevenção à segurança, em que é possível evitar a violação das responsabilidades pela segurança.

Já o padrão *System Configuration Review* pode ser aplicado com o objetivo de se identificar deficiências nas configurações dos controles de segurança. Este padrão utiliza técnicas de revisão de configurações que contam com guias de configuração de segurança, listas de verificação e ferramentas automatizadas para verificar se as configurações dos sistemas estão adequadas para minimizar os riscos de segurança. Pontos fracos nas configurações devem ser sinalizados e relatados para as equipes responsáveis. Esta tarefa é importante pois é uma forma de monitorar e analisar a eficiência dos controles de segurança, além de dar maiores garantias de que as configurações de segurança estão atualizadas perante os cenários de riscos.

O resultado final da atividade de Monitoramento e análise crítica dos riscos será uma série de registros, revisão de documentos e de sistemas de segurança que devem ser comunicadas às partes interessadas, permitindo que se possa avaliar o desempenho das atividades e, se for o caso, sugerir mudanças e correções, o que é fundamental para a continuidade e melhorias do processo de gestão dos riscos. Novas iterações no processo de gestão de riscos ou a identificação de novos padrões de segurança são importantes para formar um ciclo de melhoria contínua do processo.

## 5.4 Conclusões parciais

Apesar de existirem diferentes metodologias para gestão de riscos, observa-se que praticamente nenhuma delas diz como as diretrizes da norma NBR ISO/IEC 27005:2008 podem ser atendidas. Além disso, outro fator a destacar é que se desconhece o potencial de se utilizar padrões de segurança para implementar atividades das normas. Deste modo, a proposta apresentada neste capítulo traz como contribuição o alinhamento das tarefas com os objetivos e diretrizes da norma NBR ISO/IEC 27005:2008 e utiliza as soluções propostas por padrões de segurança para atingir os objetivos da norma. Portanto, o desenvolvimento desta metodologia está centrado nas tarefas descritas pelos padrões de segurança selecionados.

A seleção de padrões de segurança que podem ser utilizados para atender aos objetivos da norma é um desafio devido aos padrões estarem espalhados em diversos catálogos, o que acaba dificultando a localização dos padrões. Porém, este trabalho utilizou uma sequência de passos que auxiliou na identificação e escolha de padrões de segurança para as atividades de gestão de riscos.

Uma das vantagens de se utilizar padrões de segurança é o foco no desenvolvimento de pequenas tarefas de maneira modular. Com isto, a metodologia proposta pode se tornar mais dinâmica, em que novos padrões podem ser selecionados de acordo com as necessidades da organização, possibilitando um processo de adaptação e melhoria contínua do processo.

# 6 IMPLANTAÇÃO DA ANÁLISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO USANDO PADRÕES DE SEGURANÇA

Este capítulo descreve a implantação de uma análise e avaliação de riscos de acordo com a norma NBR ISO/IEC 27005:2008 usando os padrões de segurança propostos no capítulo anterior. O objetivo é implementar as atividades da norma utilizando as tarefas, técnicas e ferramentas propostas pelos padrões, a fim de avaliar e validar a utilização de padrões na implantação de normas de segurança.

As atividades de análise e avaliação de riscos podem ser consideradas as atividades mais importantes do processo de gestão de riscos, pois fornecem as informações sobre o nível de riscos a qual os ativos estão sujeitos. Com estas informações a organização terá uma base para desenvolver as melhores estratégias para proteção de seus ativos.

Neste trabalho o ambiente de aplicação desta análise e avaliação de riscos é o Departamento de Tecnologia da Informação (DTI) de uma instituição privada de ensino superior. No DTI é onde fica concentrada toda a infraestrutura lógica e física responsável pelo funcionamento dos sistemas de informação da instituição, motivo pelo qual foi escolhido para a realização do estudo de caso.

A seção 6.1 faz um breve contexto da organização e a seção 6.2 descreve o desenvolvimento e o resultado das atividades através de padrões de segurança. Ao final, na seção 6.3, são apresentadas a conclusões parciais deste capítulo.

## 6.1 Contextualização da organização

A organização objeto deste estudo de caso é uma instituição privada de ensino superior da cidade de Santa Maria/RS. Devido este trabalho tratar de informações sensíveis no ponto de vista da segurança da informação, optou-se por manter o nome da instituição em sigilo, sendo referida apenas pelo nome Faculdade.

A Faculdade tem aproximadamente 900 alunos divididos em 6 cursos de graduação e conta com um quadro docente de cerca de 50 professores. Além disso, conta com um quadro administrativo em torno de 120 funcionários, alocados em diversos setores como Central de Atendimento Integrado (CAI), financeiro, registro acadêmico, biblioteca, comunicação, marketing e vestibular, suprimentos, coordenações de cursos, Departamento de Tecnologia da Informação (DTI) e direção de unidade. A Faculdade faz parte de uma Rede de instituições de ensino e a direção geral está sediada em outra cidade.

O DTI é responsável pela implementação e manutenção da infraestrutura lógica e física para o funcionamento dos sistemas de informação da instituição. Esta infraestrutura compreende em redes de computadores, servidores, estações de trabalho, acesso à internet e *softwares*. O DTI conta com dois analistas de suporte, porém a gerência central do departamento fica na cidade sede, onde todas as decisões gerenciais são tomadas.

Apesar da importância do departamento para o funcionamento dos sistemas que dão suporte aos processos da instituição, não há um plano de gestão de riscos e a maioria das ações de segurança é executada de forma intuitiva, sem que haja um planejamento e sem o conhecimento de quais riscos são prioritários. Isto demonstra a fragilidade do setor perante as diversas ameaças, tendo registrado, inclusive, alguns incidentes de segurança nos últimos anos.

Diante deste cenário, este trabalho realiza uma análise e avaliação de riscos no DTI da Faculdade utilizando os padrões propostos no capítulo anterior, em que os resultados podem ser utilizados pela instituição para elaborar um plano de segurança que reflita as reais necessidades da instituição. A seção seguinte descreve o desenvolvimento das atividades de análise e avaliação dos riscos usando padrões de segurança.

## 6.2 Desenvolvimento das atividades

Para realizar a análise e avaliação de riscos de acordo com a norma NBR ISO/IEC 27005:2008 é necessário implementar as atividades de Definição de contexto, Identificação de riscos, Estimativa de riscos e Avaliação de riscos. Conforme a metodologia proposta no capítulo anterior, para o desenvolvimento destas atividades pode ser utilizado os seguintes padrões de segurança: *Security Needs Identification for Enterprise Assets* e *Share Responsibility for Security* (Definição do contexto), *Asset Valuation*, *Threat Assessment* e

*Vulnerability Assessment* (Identificação de riscos) e *Risk Determination* (Estimativa de riscos e Avaliação de riscos).

A Figura 8 ilustra, de forma esquemática, o diagrama de implementação das atividades de acordo com a norma NBR ISO/IEC 27005:2008, salientando o uso dos padrões de segurança em uma sequência de tarefas. O detalhamento de cada uma das atividades será descrito nas seções a seguir.

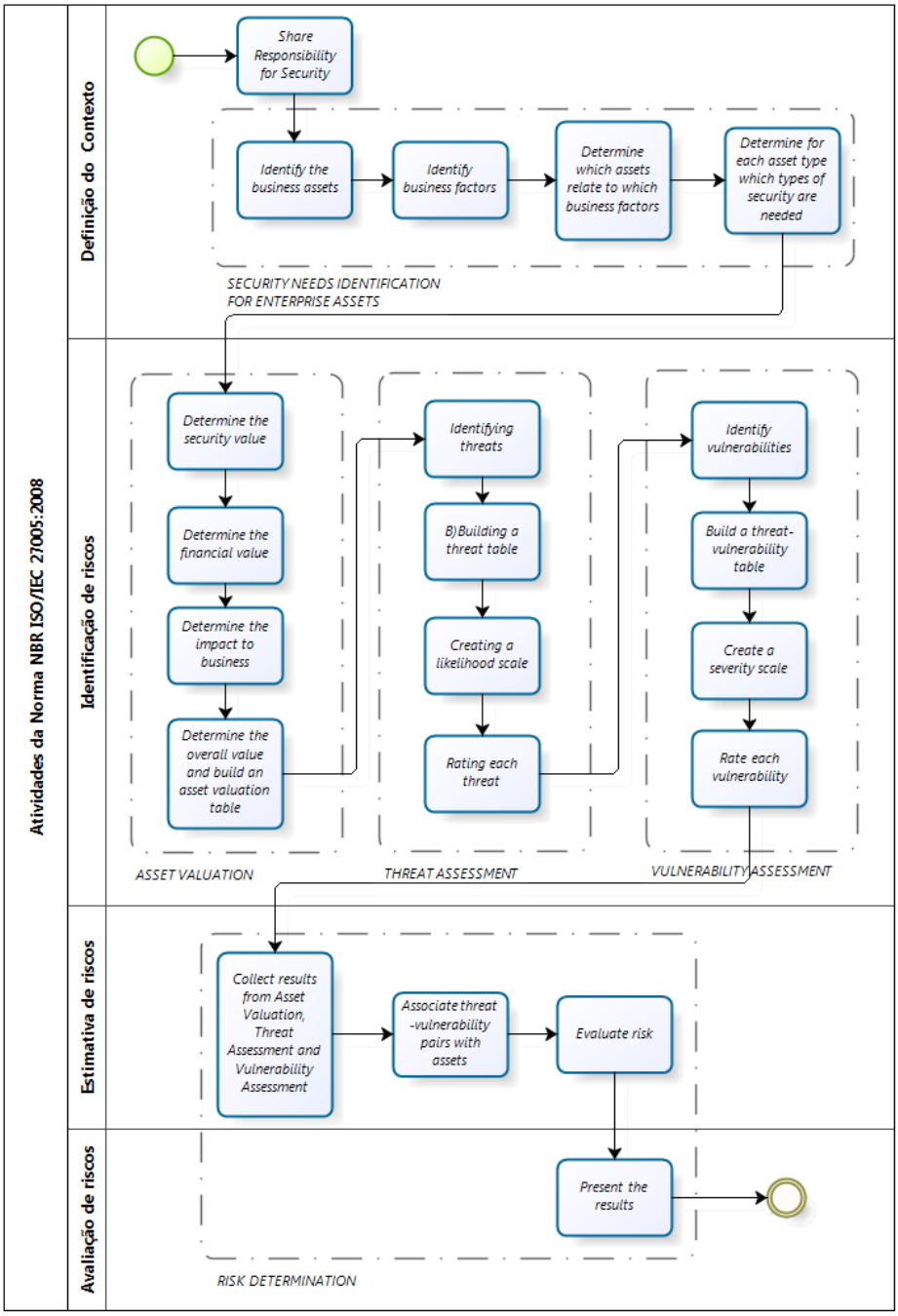


Figura 8 – Diagrama de implementação da análise e avaliação de riscos.

### 6.2.1 Definição do contexto

Nesta atividade de Definição do contexto inicia-se um mapeamento do ambiente que será analisado. O propósito é identificar as pessoas que farão parte do processo e suas responsabilidades, os ativos que farão parte da análise, os processos que estes ativos suportam e quais são as necessidades de segurança.

Neste trabalho, o escopo é o Departamento de Tecnologia da Informação (DTI) da instituição alvo deste estudo e as atividades se concentram em identificar, analisar e avaliar os riscos dos ativos tecnológicos do DTI.

A seguir, são detalhadas as tarefas desenvolvidas na atividade de Definição do contexto utilizando os padrões *Share Responsibility for Security* e *Security Needs Identification for Enterprise Assets*, conforme proposto na seção 5.3.1 deste trabalho.

#### 6.2.1.1 *Share Responsibility for Security*

Os processos de segurança da informação, assim como a gestão de riscos, não devem ser responsabilidade de um único grupo de pessoas ou setor de uma empresa. Para haver segurança, todos devem assumir responsabilidades relacionadas à segurança. O padrão *Share Responsibility for Security* procura corrigir o que muitos fazem ao atribuir a responsabilidade sobre segurança a um especialista ou grupo de especialistas. Com o auxílio do padrão *Share Responsibility for Security* são identificados os principais grupos de pessoas da instituição e suas responsabilidades quanto a segurança das informações, assim como a equipe que irá conduzir e auxiliar no processo de gestão de riscos. A composição da equipe leva em consideração a recomendação da inclusão de um especialista em segurança e é fundamental que os membros da equipe tenham uma boa compreensão sobre os fatores de risco e das soluções para diminuir os riscos. Com isso, foram identificadas as seguintes pessoas e suas responsabilidades:

- **Analistas de suporte do DTI**: Auxiliarão em todas as atividades fornecendo e revisando todas as informações necessárias para o processo de análise de riscos. Além disso, atuarão como interface de comunicação e suporte permanente nos processos de segurança para os demais setores.

- **Lideranças dos setores**: Atuam como gestores de seus setores e, quando necessário, serão responsáveis por fornecerem requisitos e informações sobre os processos de negócio.
- **Direção:** Deve atuar como o principal "patrocinador" dos processos de segurança da informação dentro da instituição. É a parte que tem o poder de aprovar as mudanças e recomendações e discuti-las juntamente com a equipe de segurança.
- **Funcionários:** Devem seguir as recomendações e políticas de segurança e, quando necessário, informar sobre possíveis eventos que possam causar riscos à instituição.
- **Especialista**: Responsável por coordenar e orientar todo o processo de análise e avaliação de riscos, aplicando as técnicas e ferramentas descritas nos padrões de segurança. Neste caso, o papel do especialista será desempenhado pelo autor deste trabalho.

O especialista é responsável por fazer uma descrição dos objetivos e da importância do processo de análise dos riscos a todos os envolvidos, ou seja, uma capacitação inicial para que as pessoas tenham uma melhor noção das atividades envolvidas e possam contribuir de forma mais efetiva, e juntamente com os analistas de suporte forma a equipe de segurança.

O envolvimento da Direção é fundamental, pois dá sustentabilidade e mostra que a segurança da informação é um assunto que deve ser tratado por todos. Sem o apoio da Direção se conseguirá realizar apenas algumas ações isoladas. Portanto, reuniões entre a equipe de segurança e a Direção devem ser realizadas periodicamente, ou quando necessário, a fim de esclarecer os impactos e clarificar os objetivos e as ações necessárias para diminuir os riscos.

Com o apoio da Direção, é possível envolver as Lideranças de cada setor e os Funcionários. Os gestores são importantes no processo de gestão de riscos, pois são responsáveis por fornecerem *feedback*[6] dos processos de negócio, e que devem ser levados em consideração para resolver os conflitos com os requisitos de segurança.

Os Funcionários geralmente são o elo mais fraco da segurança, por isso devem entender as implicações da segurança dos dados e dos processos que manipulam diariamente. Para isso, deve-se incluir no calendário funcional palestras sobre segurança da informação, confecção de cartilhas, assim como a reestruturação e divulgação das políticas de segurança. Desta forma, a meta é que os Funcionários passam também a ter responsabilidades quanto à segurança das informações, e a médio e longo prazo este compartilhamento de

[6] Palavra em inglês que no português significa provimento ou retorno de informação.

responsabilidades entre um número maior de pessoas deve melhorar, de modo geral, as ações de segurança dentro da instituição.

Como resultado desta tarefa é possível ter a identificação das pessoas e grupos de pessoas e suas responsabilidades. Isto facilita o mapeamento das informações, a definição das estratégias e as expectativas de cada um destes grupos.

#### 6.2.1.2 *Security Needs Identification for Enterprise Assets*

Após a identificação da equipe e das responsabilidades pela segurança, as próximas tarefas a serem executadas são a identificação dos ativos, a identificação dos serviços afetados pelos ativos, a relação dos ativos com estes serviços e a definição das necessidades de segurança para cada ativo.

A NBR ISO/IEC 27005:2008 recomenda que os ativos sejam identificados em um nível de detalhamento adequado (seção 2.3.3.1). Portanto, para uma identificação mais detalhada dos ativos foi utilizada a técnica *brainstorming*[7], possibilitando que a equipe (especialista em conjunto com os dois analistas de suporte do DTI) fizesse um levantamento de todos os ativos que fazem parte do suporte e infraestrutura do DTI. Nesta etapa, com a utilização do *brainstorming*, foi possível obter um melhor conhecimento da organização e consequentemente dos equipamentos e particularidades do setor. A tarefa de levantamento dos ativos foi feito *in loco*[8], já que o setor não possui uma documentação atualizada com o inventário dos bens. O foco principal da análise são os ativos de suporte e infraestrutura, portanto os ativos identificados são do tipo *hardware*, *software*, rede, recursos humanos e instalações físicas. O resultado do levantamento dos ativos e suas descrições é mostrado no Quadro 4.

O DTI é considerado um setor estratégico dentro da instituição, pois presta serviços de tecnologia essenciais para o desenvolvimento das atividades de todos os setores. Acesso à internet, acesso aos sistemas gerenciais, armazenamento de dados e sistemas de impressão são exemplos de alguns serviços prestados pelo DTI. Estes serviços geralmente necessitam de um conjunto de ativos para funcionar, e se algum destes ativos falhar ou ficar comprometido o serviço como um todo também ficará comprometido. O comprometimento dos serviços

[7] Técnica utilizada para reunir ou coletar informações em um grupo de pessoas.
[8] Expressão em inglês que no português significa “no local”.

impacta negativamente nos processos de negócio podendo, inclusive, gerar insatisfação por parte dos alunos e funcionários, ou até mesmo violações de contratos, leis e regulamentações. Portanto, é importante que se faça a identificação dos serviços que são oferecidos e a relação dos ativos que os suportam. Desta forma, é possível criar um mapeamento de quais serviços podem ser afetados caso algum ativo fique indisponível ou sofra algum tipo de dano. Com a ajuda dos analistas de suporte foi possível elencar os serviços suportados pelo DTI e quais os ativos envolvidos. O Quadro 5 lista os principais serviços relacionados com os ativos.

| **Ativo** | **Descrição** |
|---|---|
| Servidor vmware01 | Servidor responsável pela virtualização dos sistemas de armazenamento e compartilhamento dos arquivos e das contas de usuários de toda a instituição. |
| Servidor vmware02 | Servidor responsável pela virtualização dos sistemas de gerenciamento da VPN[9] e do serviço de terminal de acesso remoto. |
| Servidor LABS | Servidor responsável pelo gerenciamento dos arquivos e das contas de usuários dos laboratórios de informática. |
| *Firewall* | Servidor responsável pelo gerenciamento e controle de acesso à internet de toda a instituição. |
| Servidor Impressão | Servidor responsável pelo controle das impressões dos setores administrativos. |
| Servidor Backup | Servidor responsável por gerenciar os *backups* das configurações dos demais servidores e dos arquivos. |
| Estação Telefonia | Estação utilizada para o gerenciamento das ligações telefônicas. |
| Estações de trabalho/suporte | Estação de trabalho da equipe de analistas de suporte do DTI. |
| Sistema *Papercut* | Sistema responsável pelo gerenciamento de cotas e relatórios das impressões. |
| Sistema *TGCO* | Sistema responsável pelo gerenciamento e configuração da central telefônica. |
| Sistema *LOGOS* | Sistema que gerencia todas as informações acadêmicas da instituição (alunos, professores, cursos, disciplinas), além do controle financeiro das mensalidades. |
| Sistema *SOPHIA* | Sistema utilizado para controle do acervo da biblioteca e empréstimos de livros. |
| Banco de dados | Banco de dados de armazenamento das contas de usuários, configurações dos sistemas de informação, regras de navegação na internet e *logs*. |
| *Swicth*/roteador | Equipamento responsável pela interligação da rede de dados da sala do DTI com os demais setores. |
| *Link* de dados e telefonia | Serviço de conexão com a internet e troncos de telefonia fornecida por empresa terceirizada. |
| Central Telefônica | Equipamento responsável pelas ligações telefônicas. |
| Rede de dados | Rede de dados composta pelo cabeamento que liga os pontos de rede e telefonia ao *rack* de comunicação. |
| *Nobreak* | Equipamento responsável por manter os servidores em funcionamento em caso de falta de energia elétrica. |

[9] *Virtual Private Network* – Rede Privada Virtual.

(conclusão)

| Ativo | Descrição |
|---|---|
| Analistas de suporte | Equipe responsável por planejar, implementar e manter a infraestrutura física e lógica do DTI. |
| Sala DTI | Local onde estão instalados todos os ativos do DTI. Funciona como o Centro de Processamento de Dados (CPD) da instituição. |

Quadro 4 – Lista e descrição dos ativos do DTI.

| Serviços | Ativos de suporte |
|---|---|
| Controle de usuários | Servidor vmware01<br>Banco de dados<br>*Nobreak* |
| Acesso à internet | Servidor vmware01<br>*Firewall*<br>*Switch*/roteador<br>*Link* de dados<br>Rede de dados<br>*Nobreak* |
| Acesso a e-mail | Servidor vmware01<br>*Firewall*<br>*Switch*/roteador<br>*Link* de dados<br>Rede de dados<br>*Nobreak* |
| Impressão | Servidor vmware01<br>Servidor Impressão<br>Sistema *Papercut*<br>*Switch*/roteador<br>Rede de dados<br>*Nobreak* |
| Compartilhamento de arquivos | Servidor vmware01<br>*Switch*/roteador<br>Rede de dados<br>*Nobreak* |
| Telefonia | Estação Telefonia<br>Sistema *TGCO*<br>*Link* de telefonia<br>Central Telefônica |
| Suporte técnico | Analistas de suporte<br>Estações de trabalho/suporte<br>Servidor *Backup* |
| Acesso aos sistemas *LOGOS* e *SOPHIA* | Servidor vmware02<br>Serviço de Acesso à internet |

Quadro 5 – Lista dos serviços e relação com os ativos.

Apesar de cada setor desempenhar funções específicas, a maioria dos recursos e serviços de tecnologia da instituição é compartilhada e são essenciais para o bom desempenho das funções. É importante salientar que os sistemas *LOGOS* e *SOPHIA* não ficam

armazenados localmente no DTI, mas sim em um *data center* localizado em outra cidade e é acessado via internet através de uma rede VPN criptografada. Os serviços de e-mail e hospedagem dos *sites* da instituição também estão armazenados externamente e são compartilhados com outras instituições que fazem parte da rede da Faculdade.

Uma das únicas informações que são mantidas localmente são documentos e planilhas geradas pelos setores, e que são armazenadas no servidor de arquivos local. Além disso, são mantidas localmente as contas de usuário de todos os funcionários da instituição que permitem ter acesso aos computadores e serviços da rede de dados.

Ao analisar o cenário tecnológico da instituição, percebe-se que a maioria dos sistemas de informação está armazenada em servidores fora da instituição, necessitando do acesso à internet para poder acessá-los. Isto demonstra que o acesso à internet é um dos serviços mais críticos para todos os setores da instituição.

Após identificar os ativos e os serviços, a próxima tarefa indicada no padrão *Security Needs Identification for Enterprise Assets* é identificar as necessidades de segurança para cada ativo. As necessidades de segurança são descritas em termos das propriedades de segurança Confidencialidade, Integridade, Disponibilidade e Responsabilidade. Dependo de quais informações e quais serviços um ativo suporta, ele pode requerer uma combinação de necessidades de segurança. Por exemplo, os documentos armazenados no servidor de arquivos devem ser acessados e alterados somente por pessoas autorizadas e devem estar disponíveis no momento que for necessário. Por isso, o servidor de arquivos necessita assegurar a Confidencialidade, a Integridade, a Disponibilidade e a Responsabilidade de suas informações.

A tarefa de identificar as necessidades de segurança foi executada em conjunto com o especialista e os dois analistas de suporte. Para ajudar na definição das necessidades de segurança o padrão *Security Needs Identification for Enterprise Assets* sugere que se façam as seguintes perguntas para cada ativo:

- Necessita de proteção contra divulgação involuntária ou não autorizada? Confidencialidade.
- Necessita de proteção contra modificações involuntárias ou não autorizadas? Integridade.
- O ativo deve estar sempre disponível para uso autorizado? Disponibilidade.
- Necessita de atribuição de responsabilidade pelas ações? Responsabilidade.

Se a resposta para a pergunta for “sim”, então o ativo necessita de controles de segurança que garantam a propriedade em questão.

A partir disto, a equipe definiu as necessidades de segurança para cada ativo e o resultado desta tarefa é ilustrado no Quadro 6.

| **Ativo** | **Necessidades de segurança** **Confidencialidade (C) – Integridade (I) – Disponibilidade (D) – Responsabilidade (R)** | **Discussão** |
|---|---|---|
| Servidor vmware01 | C I D R | Os dados armazenados contêm documentos e informações estratégicas da instituição e devem ser acessados e modificados somente pessoas autorizadas. Os dados precisam estar disponíveis a todos os setores e cada setor é responsável pelos seus documentos. |
| Servidor vmware02 | I D | Serviços que rodam neste servidor são essenciais para o funcionamento de alguns sistemas, por isso devem estar sempre disponível e os sistemas e configurações só podem ser alterados pela equipe de suporte. |
| Servidor LABS | C I D | Este servidor armazena as contas de usuários dos alunos, que possibilita o acesso aos laboratórios de informática e a rede sem fio. Portanto, necessita que as informações das contas estejam sempre disponíveis e que os dados não possam ser acessados e nem modificados por pessoas não autorizadas. |
| *Firewall* | I D | Equipamento responsável pelo acesso à internet e rede de dados, portanto suas configurações não podem ser alteradas por pessoas não autorizadas e sua indisponibilidade deixará o acesso aos sistemas fora do ar. |
| Servidor Impressão | I D | É o dispositivo que gerencia todas as impressoras, portanto a sua indisponibilidade impossibilita os setores imprimirem seus documentos. Alterações nas configurações só podem ser efetuadas pela equipe de suporte. |
| Servidor Backup | C I R | Cópias de segurança, inclusive dados confidenciais dos setores, não podem ser divulgados ou modificados por pessoas não autorizadas. A equipe de suporte é responsável pela proteção e armazenamento seguro das informações. |

(continuação)

| Ativo | Necessidades de segurança<br>Confidencialidade (C) – Integridade (I) – Disponibilidade (D) – Responsabilidade (R) | Discussão |
|---|---|---|
| Estação Telefonia | I D | Equipamento que é conectado a central telefônica e é utilizado pela telefonista para realizar as ligações solicitas pelos setores. Nele é instalado o sistema *TGCO* e as configurações só podem ser alteradas pela equipe de suporte. |
| Estações de trabalho/suporte | D | A estação de trabalho deve estar disponível para que os analistas de suporte possam ter acesso aos sistemas e configurações para o suporte aos usuários. |
| Sistema *Papercut* | I D R | Cada usuário possui sua cota de impressões no mês e estas não podem ser modificadas sem autorização e cada usuário é responsável por gerenciar sua cota. O sistema deve estar disponível para que as impressoras funcionem. |
| Sistema *TGCO* | I | Alterações não autorizadas neste sistema podem implicar em mau funcionamento do sistema de telefonia da instituição. |
| Sistema *LOGOS* | C I D R | Dados dos alunos, notas e dados financeiros devem estar protegidos e não podem ser divulgados sem autorização. Os professores de cada disciplina são responsáveis pelo lançamento das notas e faltas e o registro acadêmico e o setor financeiro pela manutenção de todas as informações. O sistema deve estar sempre disponível para acesso dos setores autorizados, professores e alunos. |
| Sistema *SOPHIA* | C I D R | As informações sobre o empréstimos de livros e dados dos alunos devem ser confidenciais e as alterações dos dados e manutenção do registro do acervo é de responsabilidade da biblioteca. O sistema deve estar disponível durante o horário de funcionamento da biblioteca. |
| Banco de dados | C I D R | Informações como dados de usuário, senhas de acesso e permissões de acesso não podem ser divulgadas e acessadas sem autorização e por pessoas não autorizadas e devem estar disponíveis para o acesso às estações de trabalho e sistemas. A equipe de suporte é responsável pela manutenção e armazenamento das informações. |

(conclusão)

| Ativo | Necessidades de segurança<br>Confidencialidade (C) – Integridade (I) – Disponibilidade (D) – Responsabilidade (R) | Discussão |
|---|---|---|
| *Swicth*/roteador | I D | Para a disponibilidade da rede de dados os equipamentos de rede também devem estar sempre em funcionamento e qualquer modificação nas configurações e na instalação só pode ser efetuada pela equipe de suporte. |
| *Link* de dados e telefonia | I D | Como a maioria dos sistemas necessitam do acesso à internet para serem acessados, é necessário que os *links* de dados estejam sempre disponíveis e não podem ser modificados sem autorização. |
| Central Telefônica | I D | A indisponibilidade do equipamento impossibilita a instituição de realizar ou receber ligações telefônicas. Modificações nas configurações só podem ser efetuadas pela equipe de suporte. |
| Rede de dados | I D | Sem a disponibilidade da rede de dados não é possível acessar as informações e os sistemas da instituição. Modificações na rede de dados devem ser feitas somente pela equipe de suporte. |
| *Nobreak* | D | Equipamento deve estar sempre disponível para o funcionamento dos servidores. |
| Analistas de suporte | D R | A instituição precisa oferecer condições de trabalho seguros e favoráveis para assegurar a disponibilidade do pessoal. A instituição é responsável pela correta atribuição das atividades aos analistas. |
| Sala DTI | C I D R | A instituição é responsável por manter e preservar as instalações físicas da sala de forma a oferecer um ambiente favorável para a instalação dos equipamentos e de trabalho, garantindo a disponibilidade das instalações. O acesso à sala deve ser controlado e permitido somente a pessoas autorizadas, a fim de garantir a integridade e a confidencialidade dos equipamentos. |

Quadro 6 – Necessidades de segurança dos ativos.

As necessidades de segurança podem refletir o nível de criticidade dos ativos para a organização. Os ativos que necessitam garantir ao mesmo tempo a Confidencialidade, a Integridade e a Disponibilidade requerem uma segurança maior e podem provocar um

impacto negativo maior na organização do que aqueles que necessitam garantir somente uma das propriedades de segurança. Além disso, o mapeamento das necessidades de segurança irá ajudar na definição das medidas de segurança mais adequadas.

Com a definição da equipe e suas responsabilidades, identificação dos ativos e sua relação com os serviços e a identificação das necessidades de segurança já é possível estabelecer um contexto para que seja feita a análise de risco no DTI. Portanto, as próximas atividades visam identificar as ameaças e as vulnerabilidades dos ativos do contexto do DTI.

### 6.2.2 Identificação de riscos

A atividade de Identificação de riscos tem por objetivo identificar os principais fatores associados aos ativos que podem impactar na segurança das informações, os riscos. Será definido também um valor global para os ativos, já que este valor do ativo para a organização influencia diretamente no nível do risco.

Para desenvolver a atividade de Identificação de riscos as tarefas foram desenvolvidas conforme propõe os padrões *Asset Valuation*, *Threat Assessment* e *Vulnerability Assessment*. O detalhamento de cada uma das tarefas será descrita a seguir.

#### 6.2.2.1 *Asset Valuation*

Com a aplicação do padrão *Asset Valuation* é possível atribuir de forma simplificada e sistemática o valor global para os ativos. A proposta de se utilizar o padrão *Asset Valuation* é atribuir um valor global para o ativo baseado no seu valor de segurança, valor financeiro e no impacto para o negócio. Conforme exposto na seção 5.3.2, foi utilizada uma escala padrão de 1 a 5 para a atribuição de valores qualitativos.

Para que se possa utilizar uma mesma linha de raciocínio entre a equipe foram utilizados os Quadros 7, 8 e 9 como referência para atribuir os valores de segurança, financeiro e de impacto para cada ativo, respectivamente.

O valor financeiro dos ativos leva em consideração a importância das propriedades de segurança para garantir cumprimento dos objetivos e as obrigações legais da instituição. O

valor financeiro tem como base o custo do ativo, o tempo de reparo, manutenção, operação, substituição ou multas e sanções legais por violação da segurança. Já o valor do impacto foi baseado nas implicações para a instituição, caso os ativos sejam comprometidos, como perda de alunos ou sua confiança, perda de vantagem competitiva, perda da qualidade dos serviços internos e externos e violação de legislação.

| Escala | Valor qualitativo | Descrição |
|---|---|---|
| 5 | Muito alto | O ativo requer um grau muito alto de confidencialidade, integridade ou disponibilidade. O comprometimento de uma das propriedades pode afetar as informações e colocar em perigo as operações da empresa. |
| 4 | Alto | O ativo requer um alto grau de confidencialidade, integridade ou disponibilidade. O comprometimento de uma das propriedades pode afetar as informações, violando legislações internas ou externas, afetando os negócios da empresa. |
| 3 | Médio | Exigência moderada para controles de segurança sobre o ativo. O comprometimento das propriedades de segurança pode violar as políticas internas e afetar a produtividade dos processos da empresa. |
| 2 | Baixo | Baixa exigência para controles de segurança sobre o ativo. O comprometimento do ativo pode afetar apenas informações não críticas. |
| 1 | Muito baixo | O ativo não tem valor significativo para a empresa e a informação é de caráter público. |

Quadro 7 – Escala utilizada para o valor de segurança.

| Escala | Valor qualitativo | Descrição |
|---|---|---|
| 5 | Muito alto | O ativo possui um grande valor monetário. A perda ou dano pode acarretar um custo financeiro substancial para a empresa. |
| 4 | Alto | O ativo tem um valor monetário significativo. A reparação ou substituição pode exigir recursos financeiros significativos. |
| 3 | Médio | O ativo tem valor monetário moderado. A perda ou dano acarreta custos financeiros moderados. |
| 2 | Baixo | O ativo tem baixo valor monetário para a empresa. A perda ou dano acarreta custos financeiros baixos. |
| 1 | Muito baixo | A perda ou dano do ativo não representa custos extras. |

Quadro 8 – Escala utilizada para o valor financeiro.

Para determinar o valor global do ativo são combinados os valores de segurança, financeiro e de impacto, em que o valor global é definido como sendo o maior valor atribuído entre os três valores. Isto é, se um ativo tem um valor muito alto de segurança, mas um valor

financeiro baixo, o seu valor global deve corresponder ao valor de segurança. Isto possibilita com que a ativo seja avaliado de acordo com a criticidade de cada um destes fatores.

| Escala | Valor qualitativo | Descrição |
|---|---|---|
| 5 | Muito alto | O ativo representa um serviço crítico para a empresa. Sua perda ou dano pode acarretar no cancelamento de um serviço ou grave perda da qualidade de muitos serviços críticos. |
| 4 | Alto | O ativo suporta muitos serviços para ou da empresa. Sua perda ou dano pode acarretar a interrupção ou perda da qualidade de um ou mais serviços importantes. |
| 3 | Médio | O ativo suporta um bom número de clientes ou suporta um serviço importante para a empresa. Sua perda ou dano pode resultar numa perda de qualidade nos serviços mais importantes. |
| 2 | Baixo | O ativo suporta serviços secundários. Seu comprometimento pode ter um impacto pequeno nos processos de negócio. |
| 1 | Muito baixo | A perda ou dano no ativo não tem nenhum impacto para o negócio. |

Quadro 9 – Escala utilizada para o valor de impacto.

O resultado da avaliação global dos ativos é mostrado no Quadro 10. O valor global dos ativos será utilizado no cálculo do risco, a ser desenvolvido na atividade de Estimativa do risco.

| Ativo | Valor de segurança | Valor financeiro | Valor de impacto | Valor global |
|---|---|---|---|---|
| Servidor vmware01 | 5 | 3 | 5 | **5** |
| Sistema *LOGOS* | 5 | 2 | 5 | **5** |
| Sala DTI | 5 | 5 | 5 | **5** |
| Banco de dados | 5 | 2 | 5 | **5** |
| *Firewall* | 4 | 3 | 5 | **5** |
| Rede de dados | 4 | 2 | 5 | **5** |
| *Swicth*/roteador | 3 | 3 | 5 | **5** |
| *Link* de dados e telefonia | 3 | 2 | 5 | **5** |
| Analistas de suporte | 2 | 3 | 5 | **5** |
| *Nobreak* | 1 | 3 | 5 | **5** |
| Servidor Backup | 4 | 3 | 2 | **4** |
| Servidor vmware02 | 2 | 3 | 4 | **4** |
| Servidor Impressão | 2 | 3 | 3 | **4** |

(conclusão)

| Ativo | Valor de segurança | Valor financeiro | Valor de impacto | Valor global |
|---|---|---|---|---|
| Central Telefônica | 1 | 4 | 3 | **4** |
| Estações de trabalho/suporte | 3 | 3 | 3 | **3** |
| Sistema *SOPHIA* | 3 | 2 | 3 | **3** |
| Estação Telefonia | 2 | 3 | 3 | **3** |
| Sistema *Papercut* | 2 | 1 | 3 | **3** |
| Servidor LABS | 2 | 3 | 2 | **3** |
| Sistema *TGCO* | 1 | 1 | 2 | **2** |

Quadro 10 – Resultado do valor global dos ativos.

#### 6.2.2.2 *Threat Assessment*

Após definido o valor global dos ativos a próxima tarefa foi identificar as ameaças que podem colocar os ativos em risco. Para isso, o padrão *Threat Assessment* ajudou na identificação e na classificação das ameaças de acordo com a probabilidade de ocorrerem.

A quantidade de ameaças que circunda um ativo pode ser bastante grande e é difícil listar todas elas. Por isso, é indicado trabalhar com ameaças mais genéricas ao invés de criar uma lista específica de ameaças, procurando-se identificar somente as ameaças que realmente possuem uma probabilidade de afetar os ativos identificados. Por exemplo, ameaças do tipo "queda de meteoro", "terremoto" ou "ataque terrorista", apesar de existirem, são praticamente nulas no contexto do DTI e não é necessário lista-las.

Para padronizar a identificação das ameaças foi usado como referência o Anexo C da norma NBR ISO/IEC 27005:2008, que contém uma lista das ameaças mais comuns. Com esta lista foi organizado uma *checklist*[10] que serviu como ferramenta para apontar as potenciais ameaças aos ativos.

Cada ameaça apontada deve ser avaliada de acordo com a frequência ou a probabilidade de ocorrerem. Para atribuir o valor de cada ameaça foi utilizado a escala proposta pelo padrão *Threat Assessment*, como descrito no Quadro 11.

[10] Expressão em inglês que no português significa "lista de checagem" ou "lista de tarefas".

A definição do valor de probabilidade para cada ameaça leva em consideração alguns fatores como a proximidade de áreas de risco, estado das instalações físicas, histórico de incidentes e as características organizacionais em que o DTI se encontra.

| Escala | Valor qualitativo | Descrição |
|---|---|---|
| 5 | Muito alto | A ameaça é contínua ou pode ocorrer a qualquer momento. |
| 4 | Alto | A ameaça ocorre muito frequentemente ou existe grande chance de se manifestar. |
| 3 | Médio | A ameaça ocorre regularmente ou pode se manifestar ocasionalmente. |
| 2 | Baixo | A ameaça raramente ocorre ou as chances de se manifestar são baixas. |
| 1 | Muito baixo | A ocorrência da ameaça é extremamente improvável ou remota de se manifestar. |

Quadro 11 – Escala de probabilidade das ameaças.

O resultado desta tarefa é uma lista de ameaças classificadas conforme a sua probabilidade, possibilitando a instituição compreender melhor os fatores que contribuem para os riscos. O Quadro 12 lista as ameaças identificadas no contexto do DTI e seus respectivos valores de probabilidade de ocorrência e quais as possíveis consequências que podem vir acontecer em decorrência de sua manifestação.

Concluído a etapa de identificação e classificação das ameaças, a próxima tarefa foi identificar e avaliar as vulnerabilidades que podem estar presentes nos ativos e que podem ser exploradas pelas ameaças.

| Ameaças | Probabilidade ou frequência | Consequências |
|---|---|---|
| Fogo | **2** | Destruição de informações e ativos físicos. |
| Dano irreparável na mídia ou equipamento | **3** | Perda e corrupção de informações ou inutilização do equipamento ou mídia. |
| Poeira, corrosão, umidade | **4** | Inutilização e danos em ativos físicos |
| Inundação | **4** | Inutilização ou destruição de ativos físicos e corrupção de informações. |
| Falha do ar-condicionado | **4** | Incapacitação de ativos físicos |
| Interrupção do suprimento de energia | **3** | Incapacitação e corrupção de ativos de informação. |
| Falha no equipamento de telecomunicação | **3** | Indisponibilidade das informações. |
| Furto de mídia ou equipamento | **3** | Indisponibilidade, exposição e divulgação de informações. |
| Divulgação indevida | **3** | Exposição e divulgação de informações |

(conclusão)

| Ameaças | Probabilidade ou frequência | Consequências |
|---|---|---|
| Alteração do *software* | **2** | Indisponibilidade, exposição e divulgação de informações. |
| Falha de equipamento | **4** | Corrupção de informações e indisponibilidade de ativos físicos. |
| Saturação do sistema de informação | **4** | Incapacitação dos ativos físicos, corrupção ou indisponibilidade das informações. |
| Comprometimento dos dados | **3** | Corrupção de informações. |
| Erro durante o uso | **3** | Incapacitação dos ativos físicos. |
| Abuso de direitos | **4** | Roubo, exposição e divulgação de informações. |
| Repúdio de ações | **3** | Roubo de ativos físicos e informações. |
| Indisponibilidade de recursos humanos | **2** | Má prestação dos serviços de suporte. |
| Ataque de vírus e *trojans* | **5** | Indisponibilidade de sistemas e roubo de informações. |
| Acesso indevido | **4** | Roubo, exposição e divulgação de informações. |
| Falha da comunicação de dados | **3** | Indisponibilidade das informações. |
| Indisponibilidade da informação | **4** | Má prestação de serviço. |
| Defeito de equipamento | **3** | Corrupção e indisponibilidade das informações. |
| Falha na mídia de armazenamento | **4** | Corrupção, indisponibilidade e perda das informações. |
| Indisponibilidade do sistema | **4** | Indisponibilidade das informações e serviços. |
| Acidente grave | **2** | Comprometimento dos recursos humanos. |
| Problemas na rede pública | **3** | Indisponibilidade de serviços de telecomunicações. |
| Radiação eletromagnética | **3** | Interferência na comunicação de dados e corrupção das informações. |
| Rompimento do cabeamento | **2** | Indisponibilidade das informações. |
| Violação dos acordos de prestação de serviços | **3** | Indisponibilidade das informações e comprometimento na prestação dos serviços. |

Quadro 12 – Lista de ameaças e suas consequências.

#### 6.2.2.3 *Vulnerability Assessment*

Baseado na tabela das ameaças esta tarefa teve como objetivo identificar as vulnerabilidades que possam estar presentes nos ativos. O padrão *Vulnerability Assessment* foi utilizado para guiar a identificação das vulnerabilidades e na classificação das vulnerabilidades de acordo com sua gravidade.

Listar detalhadamente todas as vulnerabilidades de cada ativo ou sistema pode ser uma tarefa bastante dispendiosa, portanto, recomenda-se utilizar catálogos que fornecem uma lista comum de vulnerabilidades de acordo com o tipo de ativo. Para facilitar a identificação das vulnerabilidades foi utilizado como referência o Anexo D da norma NBR ISO/IEC 27005:2008, que fornece uma lista das vulnerabilidades mais comuns encontradas em ativos de tecnologia. No entanto, a equipe considerou outras vulnerabilidades que julgaram estarem presentes, além daqueles listadas na norma.

Desta forma foram identificadas apenas as vulnerabilidades que possuem ameaças relacionadas. Uma forma de identificar se uma vulnerabilidade tem uma ameaça associada foi perguntar se há alguma maneira de a confidencialidade, integridade ou disponibilidade serem comprometidas pela exploração de uma falha. Diferentemente das ameaças, que são agentes externos aos ativos e que a organização não tem controle sobre elas, é difícil atribuir um nível de gravidade geral para as vulnerabilidades, pois apesar de uma vulnerabilidade poder afetar mais de um bem ela está relacionada com as características específicas de cada ativo, que pode torná-lo mais ou menos vulnerável a determinadas falhas. Além disso, ao se avaliar uma vulnerabilidade deve-se levar em consideração a existência de condições específicas que precisam existir para a vulnerabilidade ser explorada e a existência (ou não) de controles que atenuam a gravidade da vulnerabilidade.

Da mesma forma que as ameaças, as vulnerabilidades são classificadas utilizando-se uma escala de avaliação da gravidade, que é proposta pelo padrão *Vulnerability Assessment*. Esta escala representa o grau de gravidade da vulnerabilidade presente em cada ativo e é descrita no Quadro 13.

Para fazer a avaliação das vulnerabilidades foi necessário associá-las com os ativos e com a as ameaças. Isto se deve ao fato de que uma vulnerabilidade pode afetar vários ativos e ser explorada por diversas ameaças em graus diferentes, pois cada ativo possui características específicas que podem torná-lo mais ou menos vulnerável a determinadas falhas. Na hora de se classificar as vulnerabilidades foi levado em consideração, também, fatores como a existência de condições específicas para a vulnerabilidade ser explorada e a existência de controles que atenuam a gravidade de uma vulnerabilidade. O resultado da associação dos ativos com as suas ameaças e vulnerabilidades que irão impactar no risco é apresentado no Quadro 14.

| Escala | Valor qualitativo | Descrição |
|---|---|---|
| 5 | Muito alto | A vulnerabilidade pode ser facilmente explorável e pode comprometer a maioria dos ativos, ou sua exploração por ameaças pode acarretar na perda ou destruição da informação ou na paralização total dos serviços. |
| 4 | Alto | A exploração da vulnerabilidade requer um pequeno esforço e pode expor vários ativos, ou sua exploração pode comprometer seriamente algumas informações ou serviços. |
| 3 | Médio | A vulnerabilidade é difícil de ser explorada e expõe alguns ativos, ou sua exploração pode comprometer alguns serviços. |
| 2 | Baixo | A vulnerabilidade é muito difícil de ser explorada, ou sua exploração não acarreta maiores problemas para a segurança. |
| 1 | Muito baixo | A vulnerabilidade é extremamente difícil de ser explorada, ou sua exploração não acarreta danos para a empresa. |

Quadro 13 – Escala de gravidade das vulnerabilidades.

| Ativo | VG[1] | Ameaças | P[2] | Vulnerabilidades | G[3] |
|---|---|---|---|---|---|
| Servidor vmware01 | 5 | Dano irreparável na mídia ou equipamento | 3 | Falta de rotina de manutenção periódica | 3 |
| | | | | Local de instalação inapropriado | 3 |
| | | Poeira, corrosão, umidade | 4 | Sensibilidade à umidade, poeira, sujeira | 3 |
| | | Furto de mídia ou equipamento | 3 | Ineficácia dos mecanismos de proteção física | 4 |
| | | | | Inexistência de auditorias periódicas | 4 |
| | | Defeito de equipamento | 3 | Falta de rotina de atualização de hardware | 3 |
| | | Falha de equipamento | 4 | Configuração de parâmetros incorretos | 3 |
| | | | | Sistema operacional desatualizado | 3 |
| | | Comprometimento dos dados | 3 | Rotina de backup ineficiente | 5 |
| | | | | Sensibilidade a variações de voltagem | 3 |
| | | Indisponibilidade da informação | 4 | Inexistência de plano de continuidade | 3 |
| Servidor vmware02 | 4 | Dano irreparável na mídia ou equipamento | 3 | Falta de rotina de manutenção periódica | 3 |
| | | | | Local de instalação inapropriado | 3 |
| | | Poeira, corrosão, umidade | 4 | Sensibilidade à umidade, poeira, sujeira | 3 |
| | | Furto de mídia ou equipamento | 3 | Ineficácia dos mecanismos de proteção física | 4 |
| | | | | Inexistência de auditorias periódicas | 4 |
| | | Defeito de equipamento | 3 | Falta de rotina de atualização de hardware | 3 |
| | | Falha de equipamento | 4 | Configuração de parâmetros incorretos | 3 |
| | | | | Sistema operacional desatualizado | 3 |
| Servidor LABS | 3 | Dano irreparável na mídia ou equipamento | 3 | Falta de rotina de manutenção periódica | 3 |
| | | | | Local de instalação inapropriado | 3 |
| | | Poeira, corrosão, umidade | 4 | Sensibilidade à umidade, poeira, sujeira | 3 |
| | | Furto de mídia ou equipamento | 3 | Ineficácia dos mecanismos de proteção física | 4 |
| | | | | Inexistência de auditorias periódicas | 4 |
| | | Falha de equipamento | 4 | Configuração de parâmetros incorretos | 3 |
| | | | | Sistema operacional desatualizado | 3 |
| | | | | Equipamento defasado | 3 |

(continuação)

| Ativo | VG[1] | Ameaças | P[2] | Vulnerabilidades | G[3] |
|---|---|---|---|---|---|
| Firewall | 5 | Dano irreparável na mídia ou equipamento | 3 | Falta de rotina de manutenção periódica | 4 |
| | | | | Local de instalação inapropriado | 3 |
| | | Poeira, corrosão, umidade | 4 | Sensibilidade à umidade, poeira, sujeira | 3 |
| | | Furto de mídia ou equipamento | 3 | Ineficácia dos mecanismos de proteção física | 4 |
| | | | | Inexistência de auditorias periódicas | 4 |
| | | Falha de equipamento | 4 | Configuração de parâmetros incorretos | 4 |
| | | Saturação do sistema de informação | 4 | *Hardware* defasado | 4 |
| Servidor Impressão | 4 | Dano irreparável na mídia ou equipamento | 3 | Falta de rotina de manutenção periódica | 3 |
| | | | | Local de instalação inapropriado | 3 |
| | | Poeira, corrosão, umidade | 4 | Sensibilidade à umidade, poeira, sujeira | 3 |
| | | Furto de mídia ou equipamento | 3 | Ineficácia dos mecanismos de proteção física | 4 |
| | | | | Inexistência de auditorias periódicas | 4 |
| | | Ataque de vírus e *trojans* | 5 | Antivírus inexistente ou desatualizado | 4 |
| | | | | Sistema operacional desatualizado | 3 |
| Servidor *Backup* | 4 | Dano irreparável na mídia ou equipamento | 3 | Falta de rotina de manutenção periódica | 3 |
| | | Poeira, corrosão, umidade | 4 | Sensibilidade à umidade, poeira, sujeira | 3 |
| | | Furto de mídia ou equipamento | 3 | Ineficácia dos mecanismos de proteção física | 4 |
| | | | | Inexistência de auditorias periódicas | 4 |
| | | Comprometimento dos dados | 3 | Sensibilidade a variações de voltagem | 4 |
| | | Falha na mídia de armazenamento | 4 | Inexistência de rotina de substituição periódica | 5 |
| Estação Telefonia | 3 | Poeira, corrosão, umidade | 4 | Sensibilidade à umidade, poeira, sujeira | 3 |
| | | Furto de mídia ou equipamento | 3 | Ineficácia dos mecanismos de proteção física | 4 |
| | | | | Inexistência de auditorias periódicas | 4 |
| | | Ataque de vírus e *trojans* | 5 | Antivírus inexistente ou desatualizado | 4 |
| | | | | Sistema operacional desatualizado | 3 |
| Estações de trabalho/suporte | 3 | Poeira, corrosão, umidade | 4 | Sensibilidade à umidade, poeira, sujeira | 3 |
| | | Furto de mídia ou equipamento | 3 | Ineficácia dos mecanismos de proteção física | 4 |
| | | | | Inexistência de auditorias periódicas | 4 |
| | | Comprometimento dos dados | 3 | Rotina de backup ineficiente | 3 |
| | | Ataque de vírus e *trojans* | 5 | Antivírus inexistente ou desatualizado | 4 |
| Sistema *Papercut* | 3 | Comprometimento dos dados | 3 | Rotina de backup ineficiente | 2 |
| | | Falha de *software* | 3 | Configuração de parâmetros incorretos | 3 |
| Sistema *TGCO* | 2 | Comprometimento dos dados | 3 | Rotina de backup ineficiente | 2 |
| | | Indisponibilidade do sistema | 4 | Inexistência de plano de continuidade | 3 |
| Sistema *LOGOS* | 5 | Abuso de direitos | 4 | Inexistência de trilhas de auditoria | 4 |
| | | Acesso indevido | 4 | Compartilhamento de senhas | 4 |
| | | Erro durante o uso | 3 | Interface de usuário complicada | 2 |
| | | | | Configuração de parâmetros incorretos | 3 |
| | | | | Treinamento insuficiente | 2 |
| | | Indisponibilidade da informação | 4 | Inexistência de rotas alternativas | 3 |
| | | | | Acordo de nível de serviço (SLA) inexistente ou insuficiente | 3 |
| | | | | Resposta inadequada do serviço de manutenção | 3 |

(continuação)

| Ativo | VG[1] | Ameaças | P[2] | Vulnerabilidades | G[3] |
|---|---|---|---|---|---|
| Sistema *SOPHIA* | 3 | Abuso de direitos | 4 | Inexistência de trilhas de auditoria | 3 |
| | | Acesso indevido | 4 | Compartilhamento de senhas | 3 |
| | | Erro durante o uso | 3 | Treinamento insuficiente | 2 |
| | | Indisponibilidade da informação | 4 | Inexistência de rotas alternativas | 3 |
| | | | | Acordo de nível de serviço (SLA) inexistente ou insuficiente | 3 |
| | | | | Resposta inadequada do serviço de manutenção | 3 |
| Banco de dados | 5 | Comprometimento dos dados | 3 | Rotina de backup ineficiente | 4 |
| | | Alteração de *software* | 2 | Falhas conhecidas no *software* | 2 |
| | | Divulgação indevida | 3 | Compartilhamento de senhas | 4 |
| *Swicth*/roteador | *5* | Poeira, corrosão, umidade | 4 | Sensibilidade à umidade, poeira, sujeira | 3 |
| | | Falha de equipamento | 4 | Inexistência de plano de continuidade | 4 |
| | | | | Ponto único de falha | 4 |
| | | Dano irreparável na mídia ou equipamento | 3 | Falta de proteção contra descargas elétricas | 4 |
| | | Saturação do sistema de informação | 4 | Configuração de parâmetros incorretos | 4 |
| *Link* de dados e telefonia | *5* | Violação dos acordos de prestação de serviços | 3 | Acordo de nível de serviço (SLA) inexistente ou insuficiente | 3 |
| | | Problemas na rede pública | 3 | Inexistência de rotas alternativas | 4 |
| | | Falha no equipamento de telecomunicações | 3 | Ponto único de falha | 4 |
| Central Telefônica | 4 | Poeira, corrosão, umidade | 4 | Sensibilidade à umidade, poeira, sujeira | 3 |
| | | Falha de equipamento | 3 | Sensibilidade a variações de voltagem | 3 |
| | | Dano irreparável na mídia ou equipamento | 3 | Falta de proteção contra descargas elétricas | 4 |
| Rede de dados | 5 | Falhas na comunicação de dados | 3 | Cabeamento desprotegido ou mal feito | 4 |
| | | Rompimento do cabeamento | 2 | Cabeamento desprotegido ou mal feito | 3 |
| | | Radiação eletromagnética | 3 | Sensibilidade à radiação eletromagnética | 4 |
| | | Saturação do sistema de informação | 4 | Gerenciamento de rede inadequado | 3 |
| *Nobreak* | *5* | Falha de equipamento | 4 | Equipamento defasado | 5 |
| | | | | Falta de rotina de manutenção periódica | 4 |
| | | Dano irreparável na mídia ou equipamento | 3 | Sobrecarga de trabalho | 5 |
| | | | | Ausência de proteção contra descargas elétricas | 4 |
| Analistas de suporte | 5 | Erro durante o uso | 3 | Treinamento insuficiente | 3 |
| | | | | Documentação inexistente | 3 |
| | | Acidente grave | 2 | Falta de política de execução das tarefas | 3 |
| | | Abuso de direitos | 4 | Falta de conscientização em segurança | 4 |
| | | Repúdio de ações | 3 | Atribuição inadequada de funções | 4 |
| | | Indisponibilidade de recursos humanos | 2 | Ausência de recursos humanos | 2 |

(conclusão)

| Ativo | VG[1] | Ameaças | P[2] | Vulnerabilidades | G[3] |
|---|---|---|---|---|---|
| Sala DTI | 5 | Fogo | 5 | Ausência de extintores adequados | 5 |
| | | | | Instalação predial antiga | 4 |
| | | | | Ausência de detectores e alarmes de fumaça | 5 |
| | | Inundação | 4 | Local suscetível a inundações | 3 |
| | | Furto de mídia ou equipamento | 3 | Ineficácia dos mecanismos de proteção física | 4 |
| | | Falha do ar condicionado | 4 | Equipamento defasado | 5 |
| | | | | Falta de rotina de manutenção periódica | 4 |
| | | Interrupção do suprimento de energia | 3 | Fornecimento de energia instável | 3 |
| | | Acesso indevido | 4 | Ineficácia dos mecanismos de proteção física | 4 |

Quadro 14 – Associação dos ativos, ameaças e vulnerabilidades.
[1] Valor Global.
[2] Probabilidade.
[3] Gravidade.

O Quadro 14 faz um mapeamento da relação entre as vulnerabilidades e ameaças, que possibilita a organização rastrear quais são as principais falhas que podem comprometer os ativos e assim forçar, primeiramente, em um plano emergencial para minimizar as vulnerabilidades mais graves. Em um segundo momento a organização pode revisar novamente as vulnerabilidades e propor um plano contínuo de mecanismos visando diminuir as falhas e, consequentemente, os riscos.

A elaboração do quadro com a associação dos ativos com seus respectivos pares de ameaças e vulnerabilidades foi uma das tarefas mais demoradas, levando em torno de uma semana para ser finalizada. Isto se deve ao fato de que cada associação de ameaça e vulnerabilidade teve de ser discutida pela equipe de análise, em que cada membro da equipe atribuiu um valor que julgou ser correspondente com a realidade do ambiente analisado. Depois de criada a primeira versão da planilha ela teve de ser revisada em pelo menos três vezes devido a divergências entre os valores atribuídos pelos diferentes membros da equipe. Estas revisões são importantes para que os valores atribuídos estejam o mais próximo possível da realidade do contexto analisado, já que estes valores influenciarão diretamente no valor do risco.

Finalizada esta etapa de Identificação dos riscos, teve-se como principal resultado uma planilha com o valor global dos ativos, as principais ameaças e a probabilidade de ocorrerem

e as vulnerabilidades associadas. Estas informações servirão de entrada para a próxima etapa do processo de gestão de riscos, a Estimativa dos riscos.

### 6.2.3 Estimativa de riscos

A atividade de Estimativa de riscos visa calcular os riscos presentes nos ativos de acordo com o contexto em que estão inseridos. O objetivo principal desta atividade é fornecer uma estimativa para os riscos de segurança da informação. Com isso, a organização poderá direcionar os seus esforços para proteger aqueles ativos mais sensíveis contra incidentes de segurança.

Para o desenvolvimento desta etapa foi utilizado as tarefas propostas pelo padrão *AVA*, que utiliza os dados do valor global dos ativos, as ameaças e as vulnerabilidades identificadas para calcular o risco de cada ativo.

Cada tipo de ativo possui diferentes vulnerabilidades que podem ser exploradas por diferentes ameaças. Portanto, para calcular o risco efetivo de cada ativo foi necessário associá-los em uma tabela com seus respectivos pares de ameaças e vulnerabilidades (Quadro 14). Desta forma, foram consideradas somente as combinações de ameaças e vulnerabilidades que realmente representam um risco direto para o ativo.

Após cada ativo ter sido associado com seus pares de ameaças e um valor ter sido atribuído para cada vulnerabilidade, a equação proposta pelo padrão *Risk Determination* (vide seção 5.3.3) foi usada para calcular o risco utilizando o valor global do ativo, o valor de probabilidade das ameaças e o valor de gravidade das vulnerabilidades, e o resultado deste cálculo representa a pontuação do risco de cada ativo.

Por exemplo, a equação a seguir mostra o cálculo do risco do ativo "*Firewall*" de acordo com os valores atribuídos no Quadro 14:

$$\mathbf{Risco}_{Firewall} = \mathbf{SOMA[Ameaça * Vulnerabilidade]}_{Firewall} \mathbf{* Valor\ Global}_{Firewall} \quad (2)$$

$$\mathbf{Risco}_{Firewall} = \mathbf{[(3*4)+(3*3)+(4*3)+(3*4)+(3*4)+(4*4)+(4*4)]*5} \quad (3)$$

$$\mathbf{Risco}_{Firewall} = \mathbf{[12+9+12+12+12+16+16]*5} \quad (4)$$

$$\mathbf{Risco}_{Firewall} = \mathbf{89*5} \quad (5)$$

$$\mathbf{Risco}_{Firewall} = \mathbf{445} \quad (6)$$

Similarmente, foi calculo o valor final do risco de cada ativo identificado e o resultado é apresentado, resumidamente, no Quadro 15.

| Ativo | Pontuação do Risco |
|---|---|
| Sala DTI | **775** |
| Servidor vmware01 | **615** |
| Firewall | **445** |
| Sistema *LOGOS* | **445** |
| *Swicth*/roteador | **360** |
| Servidor Impressão | **356** |
| Servidor vmware02 | **348** |
| *Nobreak* | **340** |
| Servidor *Backup* | **308** |
| Analistas de suporte | **280** |
| Servidor LABS | **270** |
| Estação Telefonia | **213** |
| Rede de dados | **210** |
| Sistema *SOPHIA* | **198** |
| Estações de trabalho/suporte | **195** |
| *Link* de dados e telefonia | **165** |
| Banco de dados | **140** |
| Central Telefônica | **132** |
| Sistema *Papercut* | **45** |
| Sistema *TGCO* | **36** |

Quadro 15 – Pontuação do risco de cada ativo.

Os resultados desta etapa identificam o nível dos riscos de acordo com o valor dos ativos, as ameaças e vulnerabilidades. A análise dos dados tabelados possibilita a organização avaliar quais são os ativos que estão mais suscetíveis a eventos negativos de segurança. Além disso, a organização pode comparar estes resultados com novas iterações de análise de risco. Por exemplo, após a aplicação de medidas de segurança, novos valores poderão ser comparados com valores antigos possibilitando uma análise da efetividade das medidas de segurança, formando um ciclo de melhoria da gestão de riscos.

Independentemente do método utilizado para avaliar o risco, podemos inferir que quanto mais vulnerabilidades um ativo possuir e mais grave forem, maior o risco. Quanto maior o número de ameaças que podem explorar uma vulnerabilidade e maior for a sua probabilidade de se manifestar também irão contribuir para que o risco aumente. Além disso,

o risco está diretamente relacionado ao valor do ativo para a organização, ou seja, quanto maior a importância do ativo maior será o impacto que um incidente de segurança pode causar para a instituição.

Uma melhor discussão dos resultados da análise de risco será feita na atividade de Avaliação de riscos, detalhada na seção a seguir.

### 6.2.4 Avaliação de riscos

Os resultados da análise de riscos servem de guia para a instituição planejar as melhores ações visando diminuir os maiores riscos encontrados e também para melhor compreender os fatores que estão relacionados aos riscos que influenciam na segurança de suas informações e dos seus serviços.

Esta etapa de Avaliação dos riscos é importante na medida em que os resultados da análise de risco são traduzidos em informações objetivas que contribuem para a tomada de decisões dos gestores. A geração de gráficos, planilhas resumidas e avaliações qualitativas são exemplos de técnicas que podem ser utilizadas para apresentar os resultados de uma análise de riscos.

Com a ajuda, ainda, do padrão *Risk Determination*, formatamos algumas informações que podem ser úteis para que os gestores da organização possam interpretar e compreender melhor cenário de risco que o DTI se encontra. Essas informações compreendem em uma avaliação geral do risco final dos ativos, uma avaliação do risco dos principais serviços que são suportados pelo DTI, uma avaliação das principais ameaças e das principais vulnerabilidades.

Com base nos resultados do Quadro 15, foi elaborado o gráfico da Figura 9 que apresenta a pontuação final do risco de cada ativo.

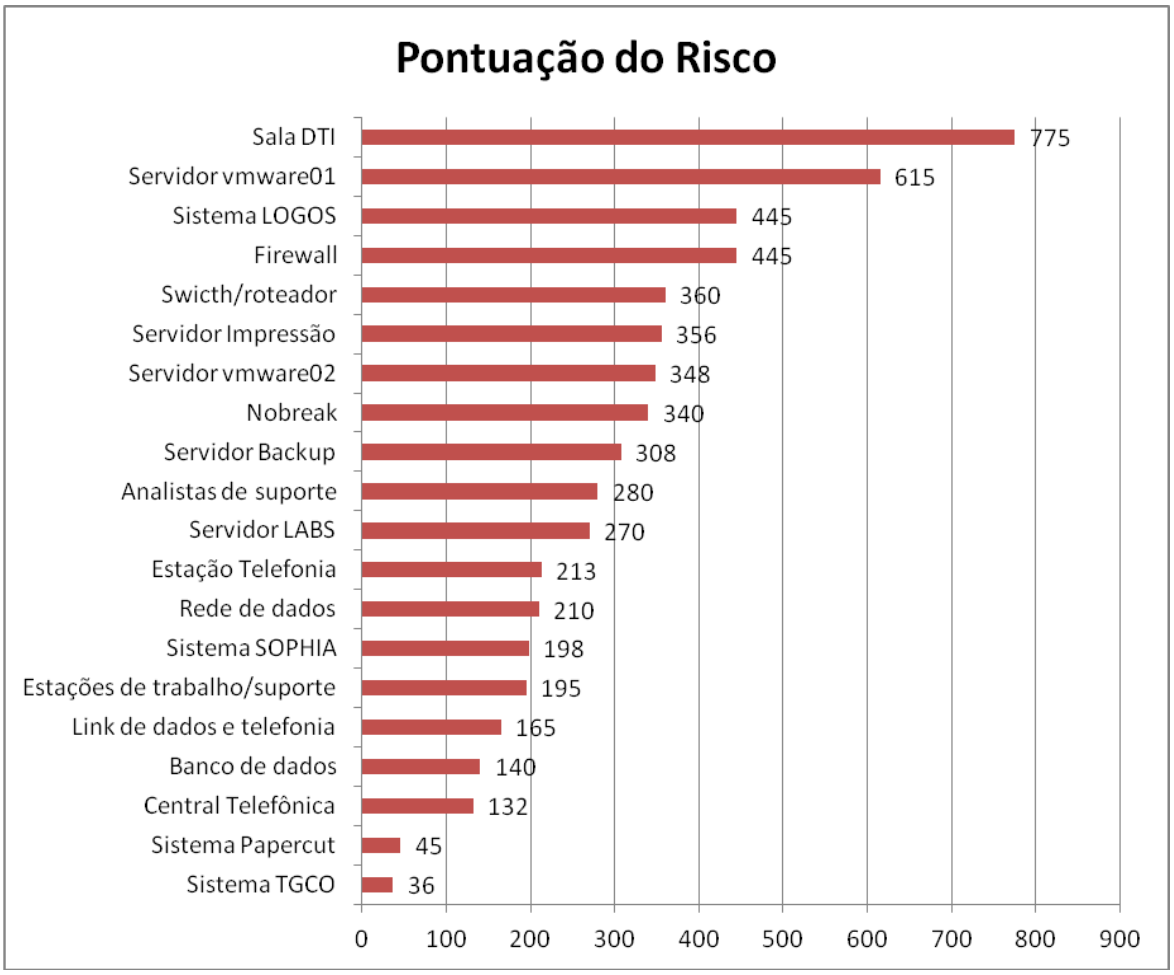


Figura 9 – Gráfico da pontuação do risco final de cada ativo.

Porém, na maioria das vezes, os gestores não estão muito interessados nos valores em si dos riscos, mas sim no que eles representam dentro do contexto da organização. Uma forma de tornar a avaliação dos riscos mais objetiva é transformar os valores quantitativos em termos qualitativos, consistentes com os usados no processo de análise de riscos. Para isso, o padrão *Risk Determination* sugere criar um intervalo que vai de 1 (representando o valor de risco mais baixo possível) até o maior valor de risco encontrado na análise (neste caso, representado pelo valor 775) e dividi-lo em 5 faixas iguais que serão rotuladas como Muito Alto, Alto, Médio, Baixo e Muito Baixo. Em seguida, os valores da tabela de risco são substituídos pelos valores qualitativos de acordo com as faixas. O Quadro 16 representa as 5 faixas criadas (1 – 775), e no Quadro 17 a tabela com a classificação qualitativa dos riscos.

| Valor qualitativo | Intervalo |
|---|---|
| Muito Alto | 621 - 775 |
| Alto | 466 - 620 |
| Médio | 311 - 465 |
| Baixo | 156 - 310 |
| Muito Baixo | 1 - 155 |

Quadro 16 – Tradução qualitativa do risco

| Ativo | Risco |
|---|---|
| Sala DTI | **Muito Alto** |
| Servidor vmware01 | **Alto** |
| Firewall | **Médio** |
| Sistema *LOGOS* | **Médio** |
| *Swicth*/roteador | **Médio** |
| Servidor Impressão | **Médio** |
| Servidor vmware02 | **Médio** |
| *Nobreak* | **Médio** |
| Servidor *Backup* | **Baixo** |
| Analistas de suporte | **Baixo** |
| Servidor LABS | **Baixo** |
| Estação Telefonia | **Baixo** |
| Rede de dados | **Baixo** |
| Sistema *SOPHIA* | **Baixo** |
| Estações de trabalho/suporte | **Baixo** |
| *Link* de dados e telefonia | **Baixo** |
| Banco de dados | **Muito Baixo** |
| Central Telefônica | **Muito Baixo** |
| Sistema *Papercut* | **Muito Baixo** |
| Sistema *TGCO* | **Muito Baixo** |

Quadro 17 – Valor qualitativo dos riscos.

Pela classificação qualitativa mostrada no Quadro 17 é possível perceber que os ativos que possuem maiores riscos são “Sala DTI” (Muito Alto) e “Servidor vmware01” (Alto). A alta relevância desses ativos para a instituição certamente contribuiu para esse resultado. Além disso, esse resultado é o reflexo da quantidade de ameaças e da probabilidade delas ocorrerem e afetarem seriamente estes ativos. Por exemplo, ameaças como “Fogo”, “Inundação”, “Furto de equipamentos”, “Dano irreparável no equipamento” e

“Comprometimento dos dados” são ameaças que possuem um grande potencial de dano, elevando o risco destes ativos.

Aliado a isso, muitas das vulnerabilidades identificadas nestes ativos foram consideradas graves, aumentando a chance de as ameaças se concretizarem. Por exemplo, a sala do DTI não possui nenhum sistema de prevenção contra incêndios e um sistema de alarmes contra roubo pouco eficiente. Apesar de haver uma rotina de *backup* periódica, as cópias de segurança são armazenadas dentro da própria sala do DTI, o que as torna inúteis em caso de roubo ou incêndio, por exemplo.

Em seguida, na faixa de riscos considerados Médios, mas ainda assim podendo ser considerados riscos relevantes, estão classificados os ativos “*Firewall*”, “Sistema *LOGOS*”, “*Switch*/roteador”, “Servidor Impressão”, “Servidor vmware02” e “*Nobreak*”. A maioria desses ativos foi considerada importante para a instituição e também estão expostos a ameaças com uma boa probabilidade de se manifestarem. A maioria das vulnerabilidades encontrada nesses ativos também possui uma gravidade que vai de média a alta. O comprometimento destes ativos pode provocar a parada de alguns serviços essenciais, mas não chega a colocar em risco os objetivos e as informações da instituição.

Na faixa de riscos considerados Baixos, estão os ativos “Servidor *Backup*”, “Analistas de suporte”, “Servidor LABS”, “Estação Telefonia”, “Rede de dados”, “Sistema *SOPHIA*”, “Estações de trabalho/suporte” e “*Link* de dados e telefonia”. Esses ativos apresentam algumas ameaças com probabilidade de ocorrerem, assim como ameaças menos potenciais. Uma característica desses ativos é que em sua maioria foi detectada a presença de algumas medidas de segurança, que fazem com que algumas vulnerabilidades sejam menos graves, contribuindo para que eles estejam menos expostos aos riscos.

Na faixa de riscos considerados Muito Baixos temos os ativos “Banco de dados”, “Central Telefônica”, “Sistema *Papercut*” e “Sistema TGCO”. Apesar da importância desses ativos para as atividades de rotina da instituição, são ativos que não armazenam ou tratam de informações críticas para a instituição e estão expostas a um número mais limitado de ameaças e, consequentemente, possuem menos vulnerabilidades para serem exploradas. Estes ativos são de fácil reposição e não apresentam custos extras em caso de necessidade de serem repostos ou recuperados, influenciando para uma pontuação de risco mais baixa.

Em outra forma de se avaliar os riscos, é possível somar a pontuação de cada ativo que está associado aos serviços identificados de acordo com o Quadro 5. Desta maneira, podemos identificar os serviços que correm mais riscos de serem afetados. O gráfico da Figura 10 ilustra o resultado da soma da pontuação dos riscos para cada serviço.

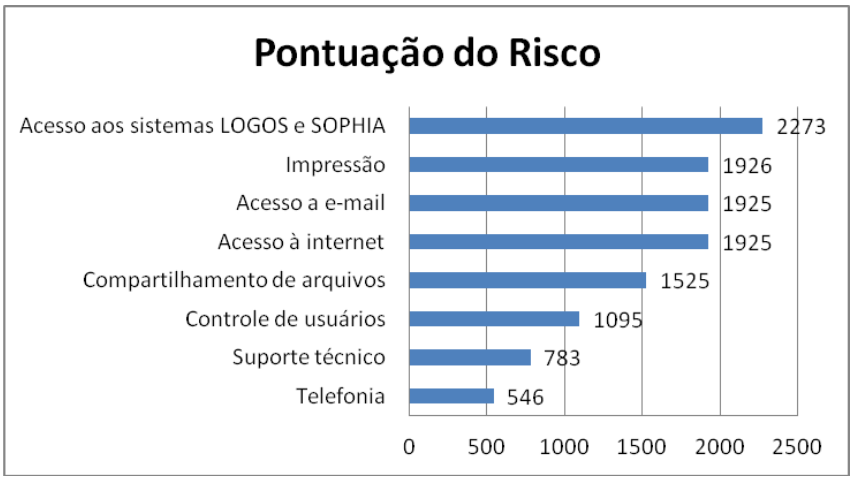


Figura 10 – Pontuação do risco de cada serviço.

O risco de cada serviço vai depender de quais ativos são necessários para o seu funcionamento e da pontuação do risco desses ativos. Podemos observar que o serviço "Acesso aos sistemas *LOGOS* e *SOPHIA*" é o que resultou em uma maior pontuação, ou seja, é o que corre mais risco de ser afetado. Em seguida, os serviços de "Impressão", "Acesso à internet" e "Acesso a e-mail" possuem praticamente a mesma pontuação, pois dependem dos mesmos ativos para funcionarem. Logo mais abaixo, numa faixa intermediária, temos os serviços de "Compartilhamento de arquivos" e "Controle de usuários". Com uma pontuação mais baixa, temos os serviços "Suporte técnico" e "Telefonia".

Desta forma, a instituição pode, por exemplo, traçar estratégias para priorizar o tratamento dos riscos daqueles serviços que estão mais expostos ou daqueles que são mais importantes para o desenvolvimento das atividades organizacionais.

Outra informação que pode ser útil para a definição das estratégias de tratamento dos riscos é identificar quais são as ameaças às quais os ativos estão mais expostos. O Quadro 18 lista as ameaças identificadas e a quantidade de ativos que elas podem afetar.

Uma das características das ameaças é que elas podem afetar mais de um ativo ao mesmo tempo. Foram identificadas 29 potenciais ameaças que oferecem riscos aos ativos do DTI, e as ameaças que mais representam riscos são "Dano irreparável na mídia ou equipamento" e "Poeira, corrosão e umidade" (10 ativos), seguido pela ameaça "Furto de mídia ou equipamento" (9 ativos). As ameaças "Falha de equipamento" e "Comprometimento dos dados" também podem afetar um número razoável de ativos, oferecendo perigo para 6 ativos cada uma. A maior probabilidade destas ameaças se manifestarem pode ser justificada

pelo fato de que muitos ativos possuem semelhanças de *hardware* e por estarem instalados no mesmo local físico, fazendo com que uma única ameaça possa colocar em risco vários ativos ao mesmo tempo. Analisando as cinco primeiras ameaças listadas no Quadro 18, podemos dizer que elas representam cerca da metade da quantidade de ameaças registradas, 41 vezes do total de 80 registros.

| **Ameaças** | **Quantidade de ativos expostos** |
|---|---|
| Dano irreparável na mídia ou equipamento | 10 |
| Poeira, corrosão e umidade | 10 |
| Furto de mídia ou equipamento | 9 |
| Falha de equipamento | 6 |
| Comprometimento dos dados | 6 |
| Erro durante o uso | 4 |
| Ataque de vírus e *trojans* | 3 |
| Indisponibilidade da informação | 3 |
| Saturação do sistema de informação | 3 |
| Abuso de direitos | 3 |
| Acesso indevido | 3 |
| Defeito de equipamento | 2 |
| Interrupção do suprimento de energia | 2 |
| Falha na mídia de armazenamento | 1 |
| Indisponibilidade do sistema | 1 |
| Acidente grave | 1 |
| Alteração de *software* | 1 |
| Divulgação indevida | 1 |
| Falha do ar condicionado | 1 |
| Falha no equipamento de telecomunicações | 1 |
| Falhas na comunicação de dados | 1 |
| Fogo | 1 |
| Indisponibilidade de recursos humanos | 1 |
| Inundação | 1 |
| Problemas na rede pública | 1 |
| Radiação eletromagnética | 1 |
| Repúdio de ações | 1 |
| Rompimento do cabeamento | 1 |
| Violação dos acordos de prestação de serviços | 1 |

Quadro 18 – Lista de ameaças identificadas.

Uma das estratégias que pode ser utilizada para diminuir os riscos mais críticos é focar primeiramente na proteção contra as ameaças que tem probabilidade de atingir um número maior de ativos. Desta forma, as ações de segurança podem atingir um número maior de ativos, tornando-as mais eficaz.

Porém, é importante salientar que uma ameaça é um agente externo ao ativo, em que não é possível se ter total controle sobre como e quando podem acontecer. Por exemplo, é impossível eliminar todos os vírus da Internet, mas é possível prevenir um ataque de códigos maliciosos mantendo um antivírus instalado e atualizado nos computadores da organização. Portanto, deve-se focar na prevenção ou correção das falhas, do que simplesmente querer eliminar todas as ameaças.

Por isto, é importante fazer uma avaliação das vulnerabilidades e quais são os ativos mais afetados. No Quadro 19 resumem-se as vulnerabilidades identificadas e com quais ativos elas estão relacionadas, possibilitando avaliar as vulnerabilidades mais críticas.

| **Vulnerabilidades** | **Ativos** |
|---|---|
| Sensibilidade à umidade, poeira, sujeira | Servidor vmware01<br>Servidor vmware02<br>Servidor LABS<br>*Firewall*<br>Servidor Impressão<br>Servidor *Backup*<br>Estação Telefonia<br>Estação de trabalho/suporte<br>*Switch*/roteador<br>Central Telefônica |
| Ineficácia dos mecanismos de proteção física | Servidor vmware01<br>Servidor vmware02<br>Servidor LABS<br>*Firewall*<br>Servidor Impressão<br>Servidor *Backup*<br>Estação Telefonia<br>Estação de trabalho/suporte<br>Sala DTI |
| Falta de rotina de manutenção periódica | Servidor vmware01<br>Servidor vmware02<br>Servidor LABS<br>*Firewall*<br>Servidor Impressão<br>Servidor *Backup*<br>*Nobreak*<br>Sala DTI |

(continua)

| Vulnerabilidades | Ativos |
|---|---|
| Inexistência de auditorias periódicas | Servidor vmware01<br>Servidor vmware02<br>Servidor LABS<br>*Firewall*<br>Servidor Impressão<br>Servidor *Backup*<br>Estação Telefonia<br>Estação de trabalho/suporte |
| Configuração de parâmetros incorretos | Servidor vmware01<br>Servidor vmware02<br>Servidor LABS<br>*Firewall*<br>Sistema *Papercut*<br>Sistema *LOGOS*<br>*Switch*/roteador |
| Local de instalação inapropriado | Servidor vmware01<br>Servidor vmware02<br>Servidor LABS<br>*Firewall*<br>Servidor Impressão |
| Sistema operacional desatualizado | Servidor vmware01<br>Servidor vmware02<br>Servidor LABS<br>*Firewall*<br>Servidor Impressão<br>Estação Telefonia<br>Estação de trabalho/suporte |
| Rotina de backup ineficiente | Servidor vmware01<br>Estação de trabalho/suporte<br>Sistema *Papercut*<br>Sistema TGCO<br>Banco de dados |
| Inexistência de plano de continuidade | Servidor vmware01<br>Sistema TGCO<br>*Switch*/roteador |
| Antivírus inexistente ou desatualizado | Servidor Impressão<br>Estação Telefonia<br>Estação de trabalho/suporte |
| Compartilhamento de senhas | Sistema *LOGOS*<br>Sistema *SOPHIA*<br>Banco de dados |
| Treinamento insuficiente | Analistas de suporte<br>Sistema *LOGOS*<br>Sistema *SOPHIA* |
| Inexistência de rotas alternativas | Sistema *LOGOS*<br>Sistema *SOPHIA*<br>*Link* de dados e telefonia |
| Acordo de nível de serviço (SLA) inexistente ou insuficiente | Sistema *LOGOS*<br>Sistema *SOPHIA*<br>*Link* de dados e telefonia |

(conclusão)

| Vulnerabilidades | Ativos |
|---|---|
| Falta de rotina de atualização de hardware | Servidor vmware01<br>Servidor vmware02 |
| Sensibilidade a variações de voltagem | Servidor vmware01<br>Servidor *Backup*<br>Central Telefônica |
| Inexistência de trilhas de auditoria | Sistema *LOGOS*<br>Sistema *SOPHIA* |
| Resposta inadequada do serviço de manutenção | Sistema *LOGOS*<br>Sistema *SOPHIA* |
| Ponto único de falha | *Switch*/roteador<br>*Link* de dados e telefonia |
| Falta de proteção contra descargas elétricas | *Switch/*roteador<br>Central Telefônica |
| Cabeamento desprotegido ou mal feito | Rede de dados |
| Equipamento defasado | Servidor LABS<br>*Nobreak*<br>Sala DTI |
| Inexistência de rotina de substituição periódica | Servidor Backup |
| Documentação inexistente | Analistas de suporte |
| Interface de usuário complicada | Sistema LOGOS |
| Falhas conhecidas no software | Banco de dados |
| Sensibilidade à radiação eletromagnética | Rede de dados |
| Gerenciamento de rede inadequado | Rede de dados |
| Sobrecarga de trabalho | *Nobreak* |
| Ausência de proteção contra descargas elétricas | *Nobreak* |
| Falta de política de execução das tarefas | Analistas de suporte |
| Falta de conscientização em segurança | Analistas de suporte |
| Atribuição inadequada de funções | Analistas de suporte |
| Ausência de recursos humanos | Analistas de suporte |
| Ausência de extintores adequados | Sala DTI |
| Instalação predial antiga | Sala DTI |
| Ausência de detectores e alarmes de fumaça | Sala DTI |
| Local suscetível a inundações | Sala DTI |
| Fornecimento de energia instável | Sala DTI |

Quadro 19 – Lista de vulnerabilidades identificadas.

Assim como uma ameaça pode colocar em risco mais de um ativo, uma mesma vulnerabilidade também pode afetar mais de um ativo. Na análise de risco realizada neste trabalho foram identificadas 42 diferentes vulnerabilidades e que podem ser exploradas pelas 29 diferentes ameaças identificadas. Destas vulnerabilidades, as que mais comprometem os

ativos são “Sensibilidade à umidade, poeira, sujeira” (10 ativos), “Ineficácia dos mecanismos de proteção física” (9 ativos), “Falta de rotina de manutenção periódica” (8 ativos), “Inexistência de auditorias periódicas” (8 ativos), “Configuração de parâmetros incorretos” (7 ativos), “Local de instalação inapropriado” (5 ativos), “Sistema operacional desatualizado” (5 ativos) e “Rotina de backup ineficiente” (5 ativos). Essas vulnerabilidades representam cerca de 50% da quantidade total de falhas identificadas nos ativos do DTI, e estão diretamente relacionadas com as principais ameaças. A seguir, é mostrada a relação entre as principais vulnerabilidades e ameaças:

- a vulnerabilidade “Sensibilidade à umidade, poeira, sujeira” está associada com a ameaça “Poeira, corrosão, umidade”;
- as vulnerabilidades “Ineficácia dos mecanismos de proteção física” e “Inexistência de auditorias periódicas” estão associadas com a ameaça “Furto de mídia ou equipamento”;
- as vulnerabilidades “Falta de rotina de manutenção periódica” e “Local de instalação inapropriado” estão associadas com a ameaça “Dano irreparável na mídia ou equipamento”;
- as vulnerabilidades “Configuração de parâmetros incorretos” e “Sistema operacional desatualizado” estão associadas com a ameaça “Falha de equipamento”; e
- a vulnerabilidade “Rotina de backup ineficiente” está associada com a ameaça “Comprometimento dos dados”.

O tratamento destas principais vulnerabilidades poderá reduzir consideravelmente os riscos, já que irá diminuir a probabilidade de exploração das principais ameaças, ou seja, a instituição poderá em primeiro momento focar nas vulnerabilidades mais críticas, para depois tentar tratar todas as falhas. Isto poderá otimizar o tempo e custo de implementação das medidas de segurança.

Porém, vale ressaltar que algumas vulnerabilidades identificadas em poucos, ou em um único ativo, podem ser tão críticas quanto as que afetam vários ativos ao mesmo tempo. Por exemplo, a vulnerabilidade “Ausência de detectores e alarmes de fumaça” ou “Ausência de extintores adequados”, se exploradas pela ameaça “Fogo”, podem comprometer seriamente o ativo “Sala do DTI” e, consequentemente, os demais ativos. Portanto, deve-se levar em consideração também o impacto e a importância do ativo no contexto como um todo.

A partir das informações sobre os riscos, as ameaças e as vulnerabilidades identificadas e classificadas, a instituição possui subsídios para discutir e traçar a melhor

abordagem visando diminuir os riscos identificados através do correto Tratamento dos riscos, etapa não explorada neste trabalho.

## 6.3 Conclusões parciais

Este capítulo teve como principal objetivo descrever a aplicação prática das tarefas recomendadas pelos padrões de segurança para desenvolver as atividades de gestão de riscos. Para isso, foi escolhido o Departamento de Tecnologia da Informação (DTI) de uma instituição privada de ensino superior, considerado um setor importante para a instituição, mas ao mesmo tempo vulnerável por não conhecer seus riscos de segurança.

Na atividade de Definição do contexto um dos resultados alcançados foi a definição da equipe que fará a análise e avaliação dos riscos. Esta tarefa utilizou como referência as orientações do padrão *Share Responsibility for Security.* Apesar de os padrões de segurança descrever as tarefas com certo grau de detalhamento, a participação de um especialista em segurança da informação foi fundamental para conduzir e orientar as tarefas. Mas, o envolvimento dos analistas de suporte que trabalham no setor também foi essencial por conhecerem os fluxos dos processos organizacionais e, principalmente, o ambiente analisado. Isso possibilitou otimizar o tempo que se perderia para conhecer os processos da instituição e o mapeamento dos ativos. Por outro lado, o envolvimento dos analistas que não possuíam conhecimento em gestão de risco fez com que aparecessem algumas divergências, principalmente na atribuição de valores para os fatores de riscos, fazendo com que fosse necessário discutir e revisar mais de uma vez estes valores.

O padrão *Security Needs Identification for Enterprise Assets* possibilitou, na atividade de Definição do contexto, o mapeamento dos ativos do DTI e a identificação dos serviços que eles suportam, além das necessidades de segurança que eles requerem. Foram identificados 20 ativos críticos que suportam 8 serviços essenciais para a instituição.

Na atividade de Identificação de riscos os padrões utilizados foram *Asset Valuation*, *Threat Assessment* e *Vulnerability Assessment* e os resultados obtidos foram a atribuição de um valor global para os ativos, a lista das ameaças e a probabilidade de ocorrerem e a lista das principais vulnerabilidades e sua gravidade. Um *checklist* com as ameaças e as vulnerabilidades mais comuns foi criado para ajudar na padronização da coleta das informações. Esta atividade foi a mais demorada, pois cada membro da equipe atribuiu um

valor para as ameaças e vulnerabilidades, e depois os resultados foram revisados e discutidos em equipe para que fosse possível chegar a consenso entre os valores. Foram identificadas 29 ameaças que podem explorar 42 vulnerabilidades diferentes dos ativos identificados.

Na atividade de Estimativa dos riscos, o principal resultado foi a obtenção da pontuação do risco de cada ativo. Para cálculo do risco foi utilizado uma fórmula proposta pelo padrão de segurança *Risk Determination*, que se diferencia de outros métodos de cálculo do risco por levar em consideração o valor global do ativo, ou seja, a importância do ativo tem impacto direto no valor do risco.

Na atividade de Avaliação de riscos foi feita uma análise um pouco mais detalhada dos resultados obtidos, em que uma das recomendações do padrão *Risk Determination* era de apresentar as informações de forma que os gestores da instituição pudessem compreender de forma mais clara e objetiva os riscos. A tabela com a pontuação dos riscos foi ordenada do maior para o menor risco, possibilitando uma visão mais objetiva sobre quais ativos estão mais sujeitos a eventos negativos. Foi possível verificar que cerca de 25% das ameaças representam 50% dos eventos identificados que podem causar danos aos ativos, e que 20% das vulnerabilidades representam cerca de 50% do total de falhas identificadas nos ativos.

Apesar de alguns resultados serem demonstrados em termos numéricos, esta análise e avaliação de riscos possui como principal característica a análise qualitativa, já que a atribuição de valores para os ativos, ameaças e vulnerabilidades refletem valores numéricos relativos, atribuídos de acordo com a percepção da equipe. O método qualitativo pode não obter resultados tão precisos quanto o método quantitativo, mas é mais fácil de ser compreendido e executado. Esta etapa de análise e avaliação dos riscos levou aproximadamente duas semanas para ser desenvolvida, demonstrando que a utilização dos padrões de segurança para desenvolver as atividades de gestão de riscos se mostrou satisfatória. O resultado final apontou informações suficientes e de forma organizada para que a instituição possa discutir e planejar estratégias para diminuir os riscos.

# 7. CONCLUSÕES

O cenário atual, em que as empresas estão cada vez mais dependentes das tecnologias da informação e comunicações, indica que é necessário se preocupar cada vez mais com a segurança das informações e com a qualidade dos serviços prestados através do uso da tecnologia informacional. O gerenciamento efetivo da segurança das informações só é possível se os riscos forem identificados, avaliados e controlados, ou seja, de nada adianta implementar controles de segurança sem antes conhecer as ameaças e as falhas presentes nos ativos. Porém, a maioria das organizações se mostra despreparada ou não sabem identificar e avaliar os riscos as quais suas informações e ativos tecnológicos estão expostos.

Neste trabalho foi observado que o embasamento em diretrizes de modelos de referência é fundamental para as organizações programarem processos bem definidos e com resultados satisfatórios. No entanto, a maioria das normas para gestão da segurança da informação diz o que tem que ser feito, mas não detalha como deve ser feito.

A norma NBR ISO/IEC 27005:2008 define uma estrutura de oito atividades que devem ser implementadas para formar um ciclo completo de gestão de riscos. Cada uma das diferentes atividades possui diretrizes e objetivos que servem de guia para o que deve ser alcançado ao final de cada iteração, sendo que as atividades de Definição do contexto, Identificação de riscos, Estimativa de riscos e Avaliação de riscos são as atividades chaves do processo de gestão dos riscos.

O estudo de padrões de segurança possibilitou identificar que eles capturam o conhecimento de especialistas em segurança e fornecem soluções para problemas de segurança em diversos contextos, sendo que algumas soluções encontradas podem ser utilizadas no processo de gestão de riscos. Porém a identificação e seleção de catálogos de padrões e padrões de segurança se mostraram como um dos principais desafios, pois a maioria dos 415 padrões de segurança existentes na literatura está espalhada em diversos catálogos e não possuem uma organização clara por contexto de aplicação. Este trabalho identificou, através de uma metodologia que pode ser reutilizada, 22 padrões de segurança que podem ser aplicados no âmbito da gestão de riscos. Para facilitar a identificação dos padrões os catálogos de padrões foram primeiramente classificados em contextos de aplicação, o que possibilita limitar o campo de pesquisa dos padrões. Considerando o contexto de aplicação, os padrões foram identificados através do nome, e aqueles que possuíam alguma relação com os

processos de gestão de riscos foram pré-selecionados para uma análise mais criteriosa de suas soluções. Num processo de gestão que considera ciclo de melhoria contínua, tal como o proposto na norma NBR ISO/IEC 27001:2006, esta metodologia permite a atualização contínua dos catálogos, contextos e padrões.

A associação dos padrões de segurança com as atividades da norma NBR ISO/IEC 27005:2008 mostrou que para algumas atividades da norma serem totalmente atendidas é necessário mais de um padrão para implementar as tarefas. Entretanto, alguns padrões podem atender as diretrizes de mais de uma atividade da norma, o que possibilita reduzir o tempo de desenvolvimento das atividades.

Uma das vantagens observadas na utilização de padrões de segurança é o foco no desenvolvimento de pequenas tarefas, como se fosse em módulos. Isto possibilita tornar o processo mais dinâmico, na medida em que novos padrões podem ser incorporados de acordo com as necessidades da organização, possibilitando um processo de adaptação e melhoria contínua.

O estudo de caso possibilitou avaliar a aplicabilidade do uso de padrões no desenvolvimento das atividades da norma, mesmo não sendo possível desenvolver todo o processo de gerenciamento de riscos, devido a limitações de tempo e dos processos organizacionais da instituição analisada. O uso dos padrões de segurança selecionados para desenvolver as atividades de Definição do contexto, Identificação de riscos, Estimativa de riscos e Avaliação de riscos se mostrou satisfatório, já que as tarefas implementadas resultaram em informações relevantes e condizentes com as metas estabelecidas pela norma NBR ISO/IEC 27005:2008. Pode-se destacar também o fato de que apesar da equipe que participou desta análise de riscos não ter experiência em análise de riscos, o que é bastante comum em pequenas e médias empresas, o levantamento dos dados e o desenvolvimento da análise e avaliação dos riscos levaram aproximadamente duas semanas para serem executadas. Este resultado também pode ser considerado satisfatório, uma vez que permite manter o custo destas etapas num nível aceitável.

Finalmente, pode-se concluir que é possível e viável desenvolver atividades de gestão segundo a norma NBR ISO/IEC 27005:2008 utilizando-se das experiências já consolidadas nos padrões de segurança, possibilitando assim que pessoas não especialistas na área realizem gestão de risco de segurança da informação com mais facilidade e eficácia.

## 7.1 Trabalhos futuros

Outros vieses que se pode avaliar em trabalhos futuros seria explorar a utilização de ferramentas de qualidade na gestão de riscos e incorporá-las aos padrões de segurança. Identificar o custo de implantação das atividades desta abordagem frente outras abordagens como, por exemplo, a de Oliveira et al. (2009), verificando formas de identificar o custo financeiro e de tempo para a implementação das atividades de gestão de riscos.

Outra possibilidade de desdobramento deste trabalho é estudar qual a melhor forma de ligar a gestão de riscos com o Plano Diretor de Tecnologia da Informação (PDTI), já que as ações de segurança da informação devem estar alinhadas e integradas com o planejamento estratégico da instituição.

# REFERÊNCIAS


ABNT NBR ISO/IEC 27001:2006. **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos**. Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2006.

ABNT NBR ISO/IEC 27002:2005. **Tecnologia da informação - Técnicas de segurança - Código de pratica para a gestão da segurança da informação**. Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2005.

ABNT NBR ISO/IEC 27005:2008**. Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação.** Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2008.

ALBERTS, C; DOROFEE, A. **Managing Information Security Risks: the OCTAVE approach**, 2º ed: Pearson Educations, Inc, 2004.

ALVES, A. A. **Segurança da Informação** - Uma Visão Inovadora de Gestão. Editora Ciência Modera, Rio de Janeiro, 2006.

AMARAL, E. H.; AMARAL, M. M.; NUNES, R. C**. Metodologia para Cálculo do Risco por Composição de Métodos**. X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2010, p. 461-473.

BACCARINI, D.; GEOFF. S.; LOVE, P. E.D. **Management of risks in information technology projects**. Industrial Management & Data Systems. Volume 104, Number 4, pp. 286, 2004.

BALDISSERA, T. A. **Gestão da segurança da informação em colégios**: uma análise da utilização da Norma NBR ISO/EIC 17799. 119f. Dissertação de Mestrado - UFSM, Santa Maria. 2007.

BEAL, A. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações –. São Paulo: Atlas, 2005.

BECKERS, K.; SCHMIDT, H.; KÜSTER, J. C.; FAßBENDER, S**. Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing**. Sixth International Conference on Availability, Reliability and Security, 2011, p.327-333.

BLAKLEY, B.; HEATH, C. **Security Design Patterns**: Technical Guide. U.K.: The Open Group, 2004.

BRANDÃO, J. E. ; FRAGA, J. S. **Gestão de Riscos de Segurança**. In: Carlos Alberto Maziero. (Org.). Livro texto dos Minicursos do SBSeg 2008. 89ed.: SBC, 2008, v. 1, p. -68.

BUNKE, M.; KOSCHKE, R.; SOHR, K. **Organizing Security Patterns Related to Security and Pattern Recognition Requirements**. In: *International Journal On Advances in Security*, 2012, vol. 5,1 e 2 ed., p. 46–67.

CAMPOS, A. **Sistema de Segurança da informação:** Controlando os Riscos. 2.ed. Florianópolis: Visual Books, 2007.

CARUSO, C. A. A.; STEFFEN, F. D. **Segurança em Informática e de Informações**. São Paulo: Editora SENAC São Paulo, 1999.

CERT.br. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em: < http://www.cert.br/stats/incidentes/#2012 http://www.cert.br/stats/incidentes/> Acesso em: 20 Out. 2012.

DIAS, C. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2000.

DOUGHERTY, C.; SAYRE, K.; SEACORD, R. C.; SVOBODA, D.; TOGASHI, K. **Secure Design Patterns.** TECHNICAL REPORT CMU/SEI-2009-TR-010, ESC-TR-2009-010. Software Engineering Institute, 2009.

DUARTE, C. **Normas Internacionais em Segurança da Informação:** Grandes mudanças na versão 2005 da ISO/IEC 17799. 10 Jan 2006. Modulo Security Magazine. Disponível em: <http://www.modulo.com.br>. Acesso em: 20 Set 2011.

ELOFF , J. H. P. ; ELOFF, M. M. **Information security architecture**. Computer Fraud & Security, vol. 2005, pp. 10-16, 2005.

FERNANDEZ, E. B.; YOSHIOKA, N.; WASHIZAKI, H.; JURJENS, J**. Using security patterns to build secure systems**. Workshop on Software Patterns and Quality (SPAQu'07), 2007, Nagoya, Japan, with the 14th Asia-Pacific Software Engineering Conference (APSEC).

FERREIRA, F. N. F.; ARAÚJO, M. T. **Política de Segurança da Informação:** Guia Prático para Implementação e Elaboração. Rio de Janeiro: Editora Ciência Moderna Ltda., 2006.

FONTES, E. L. G. **Vivendo a segurança da informação:** orientações práticas para as organizações. In: 1. ed. São Paulo: Sicurezza: Brasiliano e Associados, 2000, p. 21-39.

GAMBÔA, F. A. R.; CAPUTO, M. S.; FILHO, E. B. **Método para Gestão de Riscos em Implementações de Sistemas ERP Baseado em Fatores Críticos de Sucesso.** In: Revista de Gestão da Tecnologia e Sistemas de Informação, Vol. 1, No. 1, 2004, pp. 45-62.

GERBER, M ; SOLMS, R. V.; **Management of risk in the information age**. Computers & Security, vol. 24, pp. 16-30, 2005.

HAFIZ, M.; ADAMCZYK, P.; JOHNSON, R. E**. Organizing Security Patterns**. In: IEEE Software, vol. 24, 4 ed., 2007, p. 52-60.

HEYMAN, T.; YSKOUT, K.; SCANDARIATO, R. ; JOOSEN, W. **An Analysis of the Security Patterns Landscape**. In: Proceedings of the Third International Workshop on Software Engineering for Secure Systems (SESS '07), 2007, p. 3.

ISMS. **Information Security Management System (ISMS) International User Group Ltd**. Disponível em: <http://www.iso27001certificades.com>. Acesso em: outubro/Out. 2011.

JACOBSON, R. V. **Risk Assessment and Risk Management in Computer Security**. Handbook, S. Bosworth and M. E. Kabay, Eds., 4º ed: John Wiley & Sons, INC, 2002.

KIELY, L.; BENZEL, T. V. **Systemic Security Management**. IEEE Security & Privacy, pp. 74-77, 2005.

KIENZLE, D. M.; ELDER, M. C.; TYREE, D.; EDWARDS-HEWITT, J. **Security patterns repository**, version 1.0, 2006.

KONZEN, M. P.; NUNES, R. C.; FONTOURA, L. M. **Gestão de Riscos de Segurança da Informação Baseada na Norma NBR ISO/IEC 27005 Usando Padrões de Segurança.** Anais do IX Simpósio de Excelência em Gestão de Tecnologia (IX SEGeT). Resende/RJ, 2012.

KROLL, J.; FONTOURA, L. M.; WAGNER, R.; DORNELLAS, M. C. **Usando Padrões para o Desenvolvimento da Gestão da Segurança de Sistemas de Informação baseado na Norma ISO/IEC 21827:2008**. Simpósio Brasileiro de Sistemas de Informação (SBSI), 2010, Marabá. Anais do Simpósio Brasileiro de Sistemas de Informação (SBSI), 2010.

LICHTENSTEIN, S. **Factors in the selection of a risk assessment method**. Information Mamagement & Security, 1996. Disponível em: <http://www.emeraldinsight.com.>. Acesso em: 10 Fev. 2011.

LUNARDI, G. L. &; DOLCI, P. C. **Adoção de Tecnologia da Informação e seu Impacto no Desempenho Organizacional:** um estudo realizado com micro e pequenas empresas. 30º Encontro da ANPAD, Salvador: ENANPAD, 2006.

LUND, M. S.; SOLHAUG, B. &; STØLEN, K. **Evolution in relation to risk and trust management**. IEEE Computer Society, 2010, p. 49-55.

MARCIANO, J. L. P.;, MARQUES, M. L. **O Enfoque Social da Segurança da Informação**. Ciência da Informação, V.35, n.3, p.89-98, set/dez 2006. Disponível em: <http://www.ibict.br>. Acesso em: 10 Fev. 2012.

MARQUIS, H. **10 steps to do it yourself CRAMM**. itSM Solutions LLC, Vol. 2.8, 2006. Disponível em: <http://www.itsmsolutions.com/newsletters/DITYvol2iss8.htm> Acesso em: 24 Nov. 2012.

MARTINS, A. B. M; SANTOS, C. A. S. **Uma Metodologia para Implantação de um Sistema de Gestão de Segurança da Informação.** In: Revista de Gestão da Tecnologia e Sistemas de Informação, Vol. 2, No. 2, 2005, pp. 121-136.

MARTINS, J. C. **Gestão de projetos de segurança da informação**. Rio de Janeiro: Editora Brasport, 2003.

MAY, L; LANE, T. **A Model for Improving e-Security in Autralian Universities**. In: Journal of Theoretical and Applied Eletronic Commerce Research. v 1, p. 90-96, 2006.

MOURA, G. C. M.; GASPARY, L. P. **Uma Proposta para Medição de Complexidade de Segurança em Procedimentos de Tecnologia da Informação**. In: VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais – SBSEG, 2008, Gramado. Anais... Gramado: SBC, set.2008, p.129-142.

NETTO, A.S; SILVEIRA. M. A. P. **Gestão da Segurança da Informação:** Fatores que influenciam sua adoção em pequenas e médias empresas. In: Revista de Gestão da Tecnologia e Sistemas de Informação, Vol. 4, No. 3, 2007, p. 375-397.

NIST SP 800-30. **Risk Management Guide for Information Technology Systems**. National Institute for Standards and Technology. Gaithersburg/USA: NIST, July, 2002, pp.56.

OLIVEIRA, M. A. F.; ELLWANGER, C.; VOGT, F. C.; R. C. NUNES**. Framework para gerenciamento de riscos em processos de gestão de segurança da informação baseado no modelo DMAIC**. In: XXIX Encontro Nacional de Engenharia de Produção (ENEGEP), 2009, Salvador, XXIX Encontro Nacional de Engenharia de Produção. Rio de Janeiro: Abepro, 2009. v. 1. p. 11-20.

OLIVEIRA, V. L**. Uma análise comparativa das metodologias de gerenciamento de risco FIRM, NIST SP 800-30 e OCTAVE**. Dissertação de Mestrado, UNICAMP, Campinas, Brasil, 2006.

ONWUBIKO, C; LENAGHAN, A. P. **Managing Security Threats and Vulnerabilities for Small to Medium Enterprises**. In: IEEE International Conference on Intelligence and Security Informatics, 2007, p. 244 – 249.

PEIXOTO, M. C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

RICH, E.; SVEEN, F.O.; JAGER, M. **Overcoming Organizational Challenges to Secure Knowledge Management**. Proceedings of the Second Secure Knowledge Management Workshop, 2006, Brooklyn, NY 2006.

ROMANOSKY, S. **Operational security patterns.** In: EuroPLoP. 2003. Disponível em: <http://hillside.net/europlop/europlop2003/papers/WritingGroup/WG4_RomanoskyS. doc>. Acesso em: 20 Out. 2012.

ROMANOSKY, S. **Security design patterns**. In: SecurityFocus., 2002. Disponível em: <http://www.securityfocus.com/guest/9793>. Acesso em: 20 Out. 2012.

ROSADO, D. G.; MEDINA, E. F.; PIATTINI, M. ; GUTIERREZ, C. **A Study of Security Architectural Patterns**. In: Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), 2006, p. 358-365.

SCARFONE, K.; SOUPPAYA, M.; CODY, A.; OREBAUGH, A. **Technical Guide to Information Security Testing and Assessment:** Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology (NIST) Special Publication 800-115. 2008. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>. Acesso em: 20 Out. 2012.

SCHNEIDER, B. **Segredos e mentiras sobre a proteção na vida digital**. Rio de Janeiro: Campus, 2001.

SCHUMACHER, M.; FERNANDEZ, E. B.; HYBERTSON, D.; BUSCHMANN, F.; SOMMERLAD, P. **Security Patterns: integrating security and systems engineering**, Series in Software Designs Patterns, USA: J.Wiley & Sons, 2006.

SCUDERE, L. **Risco Digital**. Rio de Janeiro: Elsivier, 2006.

SÊMOLA, M. **Gestão da Segurança da Informação**: Uma visão executiva. Editora Campus, 2003.

SOLMS, R. V.; SOLMS, B.V. **From policies to culture**. In: Computers and Security, 23(4): 275–9, 2004.

SOLMS, R.V. **Information security management (2):** guidelines to the management of information technology security (GMITS). Information Management & Computer Security, 6(5): 221-223. MCB, University Press.1998

STEEL, C.; NAGAPPAN, R.; LAI, R. **Core Security Patterns:** Best Practices and Strategies for J2EE, Web Services, and Identity Management, Prentice Hall, 2005.

STEINBERG, R. M.; EVERSON, M.E.A.; MARTENS, F.J.; NOTTINGHAM, L.E. **Enterprise Risk Management Framework (DRAFT).** Comittee of Sponsoring Organizations of the Tradeway Commission (COSO). Disponível em: <http://www.erm.coso.org>. Acesso em: jJulho. 2011.

SUPAPORN, K.; PROMPOON, N.; ROJKANGSADAN, T. **An approach: Constructing the grammar from security pattern.** Proc.In: 4th International Joint Conference on Computer Science and Software Engineering (JC-SSE2007), 2007.

SUPAPORN, K.; PROMPOON, N ; ROJKANGSADAN, T. **Enterprise Assets Security Requirements Construction from ESRMG Grammar based on Security Patterns**. In: Proceedings of the 14th Asia-Pacific Software Engineering Conference (APSEC '07), 2007, p. 112-119.

VASILE, T; STUPARU, D.;DANIASA, C. **The relative risk weighting process**. In: Annals Economic Science Series, vol. XVI, p. 540-544, 2010.

ZAPATER, M.; SUZUKI, R. **Segurança da Informação:** Um diferencial determinante na competividade das corporações. Rio de Janeiro: Promon Businnes & Tecnology Review, 2005.

WAGNER, R.; FONTOURA, L. M.; FONTOURA, A. B. **Using Security Patterns to Tailor Software Process**. In: Proceedings of the 23rd International Conference on Software Engineering Knowledge Engineering (SEKE'2011), 2011, Eden Roc Renaissance, Miami Beach, USA, July 7-9, p. 672-677.

YODER, J.; BARCALOW, J. **Architectural patterns for enabling application security.** In: *Proceedings of the Conference on Pattern Languages of Programs*, Monticello/IL, 1997, p. 1–31.

YOSHIOKA, N.; WASHIZAKI, H.; MARUYAMA, K. **A survey on security patterns**. In: Progress in Informatics, 2008, No. 5, p.35–47.