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

UM MODELO CONCEITUAL PARA ESPECIFICAÇÃO DA GESTÃO DE RISCOS DE SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

DISSERTAÇÃO DE MESTRADO

Josiane Kroll

Santa Maria, RS, Brasil

2010

UM MODELO CONCEITUAL PARA ESPECIFICAÇÃO DA GESTÃO DE RISCOS DE SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

por

Josiane Kroll

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia da Produção da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para a obtenção do grau de
Mestre em Engenharia da Produção

Orientador: Prof. Dr. Marcos Cordeiro d'Ornellas (UFSM)

Santa Maria, RS, Brasil

2010

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

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

UM MODELO CONCEITUAL PARA ESPECIFICAÇÃO DA GESTÃO DE RISCOS DE SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

elaborada por
Josiane Kroll

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

COMISSÃO EXAMINADORA:

Prof. Dr. Marcos Cordeiro d'Ornellas (UFSM)
(Presidente/Orientador)

Prof. Dr. Raul Ceretta Nunes (UFSM)

Prof. Dr. Lisandra Manzoni Fontoura (UFSM)

Santa Maria, 12 de março de 2010.

Você vê as coisas como elas são e pergunta: por quê? Mas eu sonho com coisas que nunca foram e pergunto: por que não? — BERNARD SHAW

RESUMO

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

UM MODELO CONCEITUAL PARA ESPECIFICAÇÃO DA GESTÃO DE RISCOS DE SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

Autor: Josiane Kroll
Orientador: Prof. Dr. Marcos Cordeiro d'Ornellas (UFSM)
Local e data da defesa: Santa Maria, 12 de março de 2010.

A falta de alinhamento entre os conceitos que envolvem a gestão de riscos de segurança tem causado um impasse na adoção de modelos de gestão de riscos de segurança pelas organizações. Há diversas normas e metodologias de gestão de riscos e de segurança que possuem uma série de conceitos e são definidos de várias maneiras. Para obter o alinhamento desses conceitos e estabelecer um vocabulário próprio para a gestão de riscos, este trabalho utilizou a modelagem conceitual para o domínio da gestão de riscos de segurança. Com a modelagem conceitual foi possível abstrair esses conceitos e obter um modelo conceitual para a especificação da gestão de riscos de segurança, chamado GRiSSI (Gestão de Riscos de Segurança de Sistemas de Informação). Algumas métricas também foram propostas para os conceitos identificados no modelo conceitual, com o intuito de contribuir para promover melhorias e efetuar correções em processos de segurança. O modelo conceitual proposto foi validado por meio da verificação feita como a aplicação de auditorias e métricas para modelos UML.

Palavras-chave: Gestão de Riscos de Segurança, Métricas de Segurança, Sistemas de Informação, Modelagem Conceitual.

ABSTRACT

Master's Dissertation
Programa de Pós-Graduação em Engenharia da Produção
Universidade Federal de Santa Maria

A CONCEITUAL MODEL FOR ESPECIFICATION FOR SECURITY RISK MANAGEMENT OF INFORMATION SYSTEMS

Author: Josiane Kroll
Advisor: Prof. Dr. Marcos Cordeiro d'Ornellas (UFSM)

The lack of an alignment among concepts that involve security risk management has caused the stalemate in the adoption of security risks management models for organizations. There are several standards and risk management methodologies, having a large set of concepts, defined in many ways. In order to get an alignment of concepts and establish a suitable vocabulary for risk management, the conceptual modeling was used within the realm of security risks management. By using the conceptual modeling it was possible to abstract concepts and obtain a conceitual model for the specification of security risks management, called GRiSSI - *Gestão de Riscos de Segurança de Sistemas de Informação* (Information Systems Security Risk Management). Some metrics were also proposed for the identified concepts in the conceitual model, to make further improvements and corrections in security processes. The proposed conceitual model was validated through the application audits and metrics for UML models.

Keywords: Security Risk Management, Security Metrics, Information Systems, Conceitual Modeling.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CVSS	Common Vulnerability Scoring System
GQM	Goal Question Metric
GRiSSI	Gestão de Riscos de Segurança de Sistemas de Informação
GSI	Gestão de Segurança da Informação
IDEAL	Initiating, Diagnosing, Establishing, Acting and Learning
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NBR	Norma Brasileira Reguladora
NIST	The National Institute of Standards and Technology
PDCA	Plan-Do-Check-Act
SEI	Software Engineering Institute
SGSI	Sistema de Gestão da Segurança da Informação
SI	Sistemas de Informação
SSE-CMM	Systems Security Engineering Capability Maturity Model
TI	Tecnologia da Informação
UFSM	Universidade Federal de Santa Maria
UML	Unified Modeling Language

SUMÁRIO

AGRADECIMENTOS

Agradecimento ao Laboratório de Computacão Aplicada (LaCA) do Centro de Tecnologia (CT) da Universidade Federal de Santa Maria (UFSM), aos colegas que estão vinculados a ele, pelo apoio em todos os sentidos e também pela infraestrutura disponibilizada para a elaboração deste trabalho.

Agradecimento a Profa. Lisandra M. Fontoura, pela amizade, pelo constante incentivo e pela contribuição dada a este trabalho.

1 INTRODUÇÃO

Muitas organizações têm sofrido frequentes ataques contra a segurança dos Sistemas de Informação (SI), o que tem causado a preocupação constante de muitos gestores. Esses ataques resultam em consideráveis perdas financeiras e morais que levam as organizações a adotar medidas rigorosas de segurança. Nesse contexto, as organizações buscam aliar medidas e procedimentos de segurança ao processo de gestão de riscos.

A gestão de riscos é tida como uma forma de priorizar e controlar os riscos de segurança que tem maior potencial de dano. É por meio da gestão de riscos que são identificados os principais impactos, ameaças e vulnerabilidades que cercam um SI. Além disso, a gestão de riscos de segurança é necessária para assegurar a proteção dos SI e para diminuir a incidência de falhas de segurança.

A utilização das normas e metodologias de segurança aliadas ao desenvolvimento da gestão de riscos podem trazer maior confiabilidade ao processo e assegurar que as organizações mantenham-se atreladas as leis e regulamentações governamentais. Com a gestão de riscos é possível estruturar a política de segurança organizacional de acordo com o ambiente de exposição ao risco. A gestão de riscos também é um requisito de qualquer política de segurança e deve estar associada a uma ou mais normas que possam embasar um processo de proteção e guiar a formulação estratégias de segurança.

1.1 Definição do Problema

As organizações estão tornando-se cada vez mais expostas aos riscos de segurança, devido principalmente ao aumento da dependência tecnológica que incide sob a utilização constante de informações sigilosas. O aumento de ameaças que ocasionam ataques, quebras de segurança que provocam a perda da confidencialidade, integridade e disponibilidade das informações, tem chamado a atenção dos órgãos governamentais.

A Instrução Normativa GSI Nº1 publicada em 13 de junho de 2008, que trata da disciplina da gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, demonstra essa preocupação. Ela objetiva orientar as organizações no desenvolvimento de medidas e procedimentos de segurança necessários para manter os SI protegidos.

Com isso muitas organizações tem buscado manter-se atreladas as normas e metodologias para desenvolver seus programas de segurança. No entanto, as organizações não dispõem de um modelo de gestão de riscos específico que possa atender as recomendações da Instrução Normativa GSI Nº1 e que possa ser aplicado por todas as organizações. Também é possível verificar que os modelos de gestão de riscos encontrados na literatura possuem características distintas, alguns considerados mais completos que outros ou ainda mais eficientes.

No entanto, cada modelo de gestão de riscos é desenvolvido com propósito de atender uma necessidade específica, não podendo dessa forma ser aplicado para todas as organizações. Isso tem dificultado a sua adesão pelas organizações, onde podem ser encontrados muitos modelos de gestão de riscos na literatura, mas nenhum deles tem se consagrado e tornado-se referência para as organizações.

O modelo conceitual de gestão de riscos proposto nesta dissertação, busca solucionar os problemas como a definição de conceitos relacionados ao processo de gestão de riscos de segurança. Há vários elementos dentro da gestão de riscos que são tratados de maneira distinta por normas de segurança e de gestão de riscos. Isso causa um impasse

na definição dos conceitos que estão relacionados ao risco.

1.2 Domínio da Pesquisa

O foco dessa pesquisa é a gestão de riscos de segurança de SI. Para o seu desenvolvimento são abordados outros temas relacionados que são as normas de segurança, normas e metodologias de gestão de riscos, a integração de normas de segurança, a modelagem conceitual e as métricas de segurança, úteis na construção do modelo conceitual de gestão de riscos. Na Figura 1.1 podem ser observadas as áreas de domínio da pesquisa que resultam no modelo conceitual de gestão de riscos de segurança proposto.

Figura 1.1: Áreas de domínio da pesquisa

As normas de segurança são tratadas buscando-se verificar as recomendações de segurança que são oferecidas. Também é verificado como cada norma trata da gestão de riscos e fornece subsídios para a mitigação e para a avaliação do risco. Já nas normas e metodologias de gestão de riscos são identificados os métodos e técnicas que envolvem o desenvolvimento do processo de avaliação de riscos e seus objetivos.

A integração de normas segurança, é discutida para cumprir com as orientações da Instrução Normativa GSI N^{o}1 e assegurar que o modelo conceitual proposto esteja alinhado a metodologia imposta pelo governo federal.

Com uma série de normas de segurança e de gestão de riscos é necessário conceituar os elementos que compõem todo o processo de gestão de riscos. Dessa forma, a modelagem conceitual é utilizada como uma ferramenta que auxília na definição do escopo da gestão de riscos de segurança de SI.

Dessa forma, a pesquisa agrupa as recomendações feitas pelas normas, fornece o mapeamento dos conceitos que envolvem a gestão de riscos, servindo para a elaboração de um modelo conceitual de gestão de riscos que será denominado GRiSSI (Gestão de Riscos de Segurança de Sistemas de Informação).

1.3 Escopo da Pesquisa e suas Limitações

O escopo da pesquisa abrange o gerenciamento de riscos de segurança em SI e a utilização de normas de segurança. As recomendações feitas pela Instrução Normativa GSI Nº1 ocasionaram a adesão à norma ISO/IEC 27005, já que a mesma faz parte da família ISO/IEC 27000, a qual é sugerida pela Instrução Normativa GSI Nº1. Entretanto, mudanças em leis ou regulamentações podem provocar a substituição da norma.

1.4 Contribuições da Pesquisa

Com o desenvolvimento do modelo conceitual GRiSSI baseado nas metodologias e normas de segurança e de gestão de riscos, espera-se contribuir no contexto organizacional para o aumento das garantias de proteção dos SI, por meio do controle de riscos, para a diminuição das perdas e danos provenientes de falhas de segurança e para o cumprimento das leis e regulamentações governamentais.

No contexto científico e para a comunidade acadêmica, os resultados deram origem a um modelo conceitual de gerenciamento de riscos de segurança com a elaboração da modelagem conceitual. O atrelamento de normas e metodologias de gestão de riscos pode também servir de referência para a padronização dos processos segurança. As métricas construídas para o modelo conceitual também estimularão novas fontes de

pesquisa além de contribuir para o gerenciamento dos riscos de segurança.

1.5 Estrutura da Dissertação

Esta dissertação está organizada em sete partes, como apresentada na Figura 1.2.

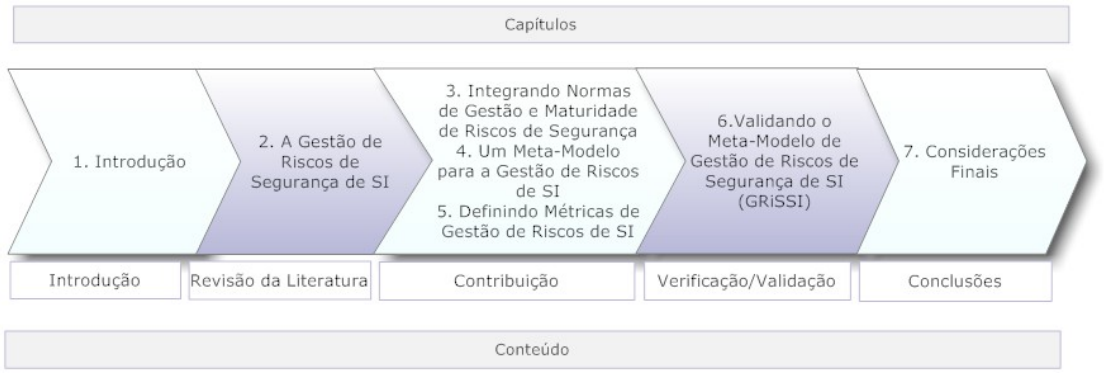

Figura 1.2: Estrutura da dissertação

O capítulo 1 apresenta a introdução, onde são tratados os aspectos que envolvem o desenvolvimento da pesquisa.

No capítulo 2 é realizada a revisão da literatura com o objetivo de entender a abrangência da gestão de riscos, normas e metodologias no contexto da segurança organizacional.

Nos capítulos 3, 4 e 5 são apresentadas as principais contribuições dessa dissertação. O capítulo 3 aborda a integração das normas de gestão e maturidade de riscos de segurança, de modo a apresentar como essas normas estão relacionadas e podem ser integradas para assegurar maiores garantias de segurança. No capítulo 4 é abordado o desenvolvimento de um modelo conceitual para a gestão de riscos de segurança de SI, que será denominado GRiSSI. O capítulo 5 apresenta a definição de métricas para o modelo conceitual.

No capítulo 6 é apresentada a validação/verificação do modelo conceitual GRiSSI por meio da utilização de auditorias e métricas para modelos UML. O modelo conceitual é verificado para que o mesmo e as normas possam ser validadas para o tratamento de

riscos de segurança.

Por fim, o capítulo 7 traz as considerações finais e as conclusões obtidas com o desenvolvimento da pesquisa.

2 A GESTÃO DE RISCOS DE SISTEMAS DE INFORMAÇÃO

Nesta seção é realizada uma análise da gestão de riscos para o gerenciamento estratégico da segurança da informação, buscando indícios de melhorias nas medidas de segurança tomadas pelas organizações. São apresentadas as normas e metodologias de gestão de riscos de SI que favorecem a implementação da segurança pelas organizações.

Parte dos resultados obtidos neste capítulo estão presentes no artigo "Aplicação da Metodologia de Avaliação de Riscos para o Gerenciamento Estratégico da Segurança da Informação", publicado nos anais XLI SPBO (Simpósio Brasileiro de Pesquisa Operacional)[1] e no artigo "Uma Análise Comparativa das Abordagens de Gerenciamento de Riscos OCTAVE, NIST SP 800-30, CRAMM, FRAP, COBRA e Risk Watch", publicado no XVI SIMPEP[2].

2.1 O Papel Estratégico da Gestão de Riscos

Estabelecer o gerenciamento da segurança das informações é um grande desafio para as organizações que crescem em complexidade de mecanismos de segurança e em

[1] O XLI Simpósio Brasileiro de Pesquisa Operacional foi realizado no período de 1º a 4 de setembro de 2009, em Porto Seguro-BA. Teve como tema "A Pesquisa Operacional na Gestão do Conhecimento". Os trabalhos aceitos foram publicados no Livro de Resumos do Simpósio.

[2] O XVI SIMPEP (Simpósio de Engenharia da Produção) foi realizado no período de 09 a 11 de novembro de 2009 na cidade de Bauru -SP, com o intuito de discutir e apresentar as pesquisas desenvolvidas voltadas para Engenharia de Produção e suas ênfases. Informações sobre o evento podem ser obtidas em http://www.simpep.feb.unesp.br/

incertezas de proteção (CARALLI e WILSON, 2004). Desenvolver além de um plano de segurança pode ser muito difícil para as organizações que procuram um modelo de gestão de segurança.

A gestão de riscos aplicada ao gerenciamento estratégico da segurança contribui para aumentar as garantias de proteção das informações das organizações. Isso pode ser observado pelos seguintes fatores:

- A tomada de decisões reflete no conhecimento prévio dos riscos de segurança: com os dados obtidos pela gestão de riscos é possível verificar quais são as ameaças e as vulnerabilidades que podem resultar riscos para a organização. A tomada de decisões então, é realizada baseada em fatores de segurança. Isso pode trazer mais confiança as organizações e reduzir erros de planejamento.

- A política de segurança é bem estruturada: ao estabelecer uma política de segurança é necessário ter conhecimento das necessidades de proteção da organização. A gestão de riscos fornece um panorama da segurança que contribui para o estabelecimento de procedimentos e métodos adequados.

- O plano de segurança focaliza ações futuras: planejar a segurança envolve estabelecer ações de curto e longo prazo que garantam a progressão gradual da segurança. O plano de segurança pode ser mais bem estruturado e direcionado aos objetivos da organização.

- Os investimentos em segurança são devidamente planejados: os investimentos em segurança podem ser reduzidos quando bem planejados. Uma melhor distribuição dos recursos financeiros destinados à segurança pode ser realizada através da definição das urgências e prioridades.

- São tomadas ações preventivas e não corretivas: gasta-se muito tempo tentando reparar danos ocorridos pela falta de segurança que poderiam ser evitados com

simples medidas de proteção. A gestão de riscos fornece informações necessárias para que sejam tomadas ações de prevenção a ataques.

- Os recursos de segurança são gerenciados: com a avaliação de riscos é verificada a necessidade de proteção de cada recurso e então são implementados mecanismos de segurança com uma finalidade específica. O gerenciamento dos recursos de segurança é realizado através do planejamento e da correta distribuição da segurança. Assim, não há uma sobrecarga de processos de segurança e nem de mecanismos de segurança desnecessarios. Com isso, ganha-se mais desempenho e se reduz custos.

- A sensibilização da segurança está focada na realidade da organização: conscientizar os funcionários e os clientes baseando-se em dados obtidos pela avaliação de riscos é expor fatos reais da organização que realmente necessitam de medidas de proteção. Dessa forma a organização pode melhor elaborar a documentação de normas e regulamentações de segurança para os usuários.

- A organização tem mais credibilidade dos clientes: uma organização que possui uma boa reputação e fornece garantias de segurança das informações dos seus clientes, consegue ampliar seus negócios.

- O custo-benefício da implementação da segurança é relatado: a gestão de riscos fornece evidências dos benefícios que a organização pode ter se protegendo e dos custos decorrentes de não se prevenir. A gestão de riscos fornece uma perspectiva futura de possíveis danos e cabe a cada organização decidir que medidas devem ser tomadas.

A gestão de riscos influência diretamente no estabelecimento de estratégias de segurança. A identificação das ameaças, vulnerabilidades e dos riscos fornece indícios para implementação de estratégias. O planejamento financeiro destinado à segurança deve estar alinhado aos objetivos de proteção da organização. Com a definição de prioridades

de proteção a organização pode gerenciar a estrutura de segurança e garantir que a segurança acompanhe o crescimento da organização.

2.2 Normas e Metodologias de Gestão de Riscos de Sistemas de Informação

O desenvolvimento da gestão de riscos de SI é realizado por meio de normas e metodologias que dão suporte as organizações na definição dos processos de mitigação, avaliação e gerenciamento de riscos. Nesta seção, são apresentadas as principais normas e metodologias de gestão de riscos utilizadas pelas organizações e citadas na literatura.

2.2.1 Normas de gestão de riscos

Com o objetivo de guiar o desenvolvimento da gestão de riscos, foram elaboradas as normas que definem elementos para a organização do processo de gestão de riscos. Entre essas normas podem ser citadas a norma PD ISO/IEC *Guide* 73:2002 (ISO/IEC Guide 73,2002), a AS/NZS 4360 (AS/NZS 4360, 1999) e a ISO/IEC 31000:2008 (ISO/DIS 31000, 2008). Atualmente essas normas têm uma grande aceitação pelas organizações e estabelecem um modelo clássico para o gerenciamento de riscos (BEZERRA, NAKAMURA e RIBEIRO, 2006).

2.2.1.1 PD ISO/IEC Guide 73:2002

A PD ISO/IEC *Guide* 73:2002 é um guia para escritores de normas, que fornece definições genéricas de termos de gestão de riscos (AIRMIC, ALARM e IRM, 2002). Este guia é entendido como um documento genérico de alto nível para a preparação ou revisão de padrões, que incluem o gerenciamento de riscos. Seu objetivo é contribuir para a compreensão mútua entre os membros da ISO e IEC no fornecimento de orientações sobre a prática da gestão dos riscos.

As definições do PD ISO/IEC *Guide* 73:2002 são mais amplas que as contidas na ISO/IEC *Guide* 51 que trata dos aspectos de segurança (AIRMIC, ALARM e IRM, 2002).

As questões relacionadas com a segurança nas definições dadas na norma ISO/IEC *Guide* 51 são indicadas no Anexo A da norma ISO/IEC *Guide* 73.

A estrutura da PD ISO/IEC *Guide* 73:2002 conciste de três seções: escopo, visão geral dos termos e definições de gestão de riscos e termos e definições. Os termos e definições são agrupados em 4 subseções: termos básicos, termos relacionados com pessoas ou organizações afetadas pelo risco, termos associados com a avaliação de riscos e termos relacionados ao controle e tratamento de riscos (BORNMAN, 2004). Na Figura 2.1 é mostrada a representação gráfica da estrutura da PD ISO/IEC *Guide* 73:2002.

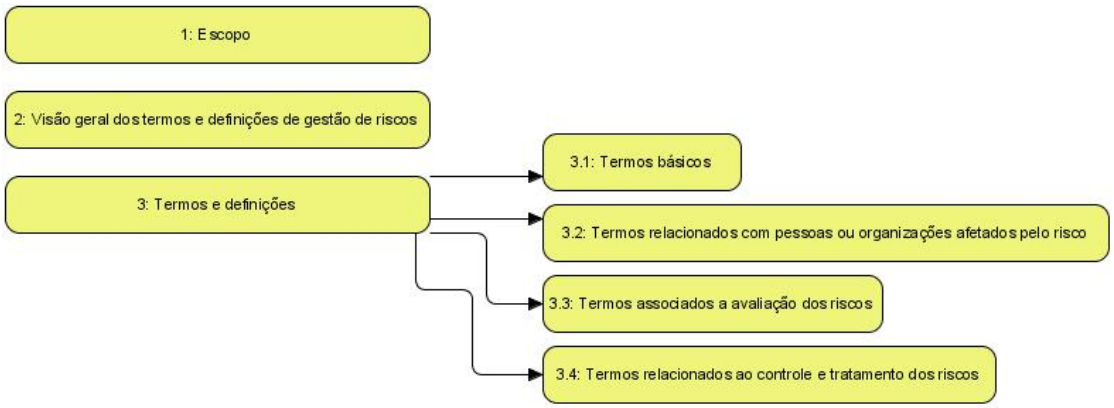

Figura 2.1: Representação gráfica da PD ISO/IEC *Guide* 73:2002

2.2.1.2 AS/NZS 4360

A norma AS/NZS 4360 foi elaborada em 1999 pelo Comitê OB/7, com o objetivo de fornecer uma estrutura genérica para o estabelecimento dos contextos para a identificação, avaliação, tratamento, monitoramento e comunicação de riscos (BORNMAN, 2004*apud* AS/NZS 4360, 1999). A AS/NZS 4360 pode ser aplicada em todos os níveis estratégicos e operacionais da organização e em conjunto com outras normas de segurança já existentes.

Visando atender diferentes setores de atividades, a AS/NZS 4360 se tornou a principal referência para a ISO 31000 - *General guidelines for principles and implementation of risk management*.

2.2.1.3 A norma ISO/IEC 31000:2009

A ISO/IEC 31000:2009 - *General guidelines for principles and implementation of risk management* é uma norma de gerenciamento de riscos genérica que estabelece um padrão globalmente válido para a gestão de riscos (ERBEN, 2008). A norma ISO/IEC 31000 começou a ser desenvolvida em 2005 e é baseada na norma AS/NZS 4360.

O objetivo de desenvolvimento da ISO/IEC 31000 é fornecer um documento para estabelecer princípios e orientações práticas para o processo de gestão de riscos. Esse documento poderá ser aplicável em todas as organizações e para todos os tipos de riscos. A ISO/IEC 31000 também fornece um entendimento comum da gestão de riscos, com o propósito de orientar e recomendar requisitos de segurança.

O princípio básico da gestão de riscos da ISO/IEC 31000 está alinhado com o ciclo de melhoria PDCA (*Plan, Do, Check, Act*), reformulado como "concepção do quadro, execução, acompanhamento e revisão e melhoria contínua" (ISO/DIS 31000, 2008).

2.2.2 Normas de segurança

Além das normas que são especificamente desenvolvidas para a gestão de riscos, há outras normas como a ISO/IEC 13335 (GMITS) e a ISO/IEC 15408 (*Common Criteria*) que são direcionadas ao gerenciamento de segurança de TI. Por apresentarem estruturas que são aplicadas em conjunto com outras normas de gestão de riscos, estas normas são descritas nesta subseção a fim de evidenciar a gestão da segurança no qual o controle dos riscos é altamente necessário.

2.2.2.1 ISO/IEC 13335

A norma ISO/IEC 13335 ou GMITS (*Guidelines for the Management of IT Security*) é um guia padrão para o gerenciamento de segurança de TI. Sua estrutura está concentrada em cinco estágios (RÖHRIG, 2003):

- Estágio 1: Conceitos e modelos para a segurança de TI - contém uma visão geral

dos conceitos básicos que são utilizados pela ISO/IEC 13335;

- Estágio 2: Gerenciamento e planejamento de segurança de TI - descreve os aspectos de gerenciamento e planejamento da segurança, incluindo a determinação dos objetivos, estratégias, políticas e requisitos organizacionais de segurança de TI;

- Estágio 3: Técnicas para o gerenciamento de segurança de TI - descreve técnicas para o gerenciamento de riscos e para o desenvolvimento de um plano de segurança de TI;

- Estágio 4: Seleção de medidas de segurança - explica o processo de seleção das medidas de segurança de acordo com as necessidades específicas do ambiente da organização usando medidas de garantia de segurança de outras normas;

- Estágio 5: Guia de gerenciamento de segurança de rede - descreve um processo para a seleção de medidas de segurança, para conexões de sistemas de TI de redes externas, diferenciado pelos tipos de conexão.

2.2.2.2 ISO/IEC 15408 (Common Criteria)

A ISO/IEC 15408 (*Common Criteria*) é um conjunto de critérios que permite a especificação da segurança de uma aplicação, baseado nas características do ambiente de desenvolvimento (COELHO, 2007). Dessa forma, o *Common Criteria* fornece um *framework* padronizado de critérios para especificação, implementação e avaliação de requisitos e propriedades de segurança em SI e produtos de TI.

O propósito do *Common Criteria* é permitir que os usuários especifiquem suas exigências de segurança, para permitir aos desenvolvedores especificar os atributos de segurança de seus produtos e para permitir aos avaliadores determinar se os produtos realmente satisfazem suas reivindicações (MELLADO et al., 2007).

A aplicação do *Common Criteria* destina-se a proteção dos aspectos de segurança de TI que são a confidencialidade, integridade e disponibilidade (COMMON CRITERIA,

2003). Assim, o *Common Criteria* é aplicável aos riscos decorrentes das atividades humanas (maliciosas ou não) e para os riscos decorrentes de atividades não-humanas.

2.2.3 Normas de gestão e maturidade de riscos de segurança

Nesta subseção serão apresentadas as normas ISO/IEC 27005, ISO/IEC 21827:2008 (SSE-CMM) e NIST SP 800-30, a fim de descrever como cada norma é desenvolvida e como a gestão de riscos é tratada.

2.2.3.1 ISO/IEC 27005

A ISO/IEC 27005 é integrante da família da norma ISO/IEC 27000 (CAMPOS, 2007). Esta norma fornece diretrizes para a segurança da informação da gestão de riscos, que suporta os conceitos gerais especificados na norma ISO/IEC 27001. Seu objetivo é fornecer um guia para a implementação da abordagem de gerenciamento de riscos orientada ao processo, para auxiliar na execução e no cumprimento satisfatório da implementação da gestão de riscos da informação, baseado nos requisitos da norma ISO/IEC 27001.

Nesta norma é encontrado um conjunto de técnicas que são empregadas para guiar o gerenciamento dos riscos de segurança, incluindo recomendações sobre a avaliação de riscos, tratamento, aceitação, comunicação, monitoramento e revisão dos riscos.

2.2.3.2 NIST SP 800-30

O NIST *(National Institute of Standards & Technology)* SP *(Special Publication)* 800-30 é uma abordagem destinada para avaliação qualitativa dos riscos, que foi baseada em trabalhos já realizados por analistas de segurança com sistemas proprietários. Essa abordagem trabalha para identificar, avaliar e gerenciar os riscos em sistemas de TI. A metodologia de desenvolvimento da abordagem NIST SP 800-30 consiste de nove processos (STONEBURNER, GOGUEN e FERINGA, 2002):

- Processo 1 - Caracterização do sistema;
- Processo 2 - Identificação das ameaças;
- Processo 3 - Identificação das vulnerabilidades;
- Processo 4 - Análise dos controles;
- Processo 5 - Determinação das probabilidades;
- Processo 6 - Análise do impacto;
- Processo 7 - Determinação dos riscos;
- Processo 8 - Recomendações de controles; e
- Processo 9 - Documentação dos resultados.

2.2.3.3 ISO/IEC 21827:2008 (SSE-CMM)

A norma ISO/IEC 21827:2008 ou modelo SSE-CMM *(Systems Security Engineering Capability Maturity Model)* foi desenvolvido pelo ISSEA *(International Systems Security Engineering Association)* em 1999. Esta norma descreve as características essenciais que um processo de engenharia da segurança da informação deve possuir para assegurar a boa segurança (SSE-CMM, 2003).

A norma ISO/IEC 21827:2008 examina a maturidade dos processos de engenharia da segurança de TI executados por uma organização (HOPKINSON, 1999). Esta norma baseia-se na implementação de processos de segurança (*Process Areas*) destinados a atender áreas específicas de segurança. O processo dado pela ISO/IEC 21827:2008 inclui um conjunto de *Process Areas* que são avaliadas para determinar o nível de maturidade. A maturidade dos processos que são atribuídos por cinco níveis, dando a organização os resultados dos processos implementados.

O desenvolvimento da ISO/IEC 21827:2008 pode ser realizado pelas organizações de acordo os seu objetivos organizacionais. Assim cada organização pode definir quais *Process Areas* implementar e quais níveis de maturidade se deseja alcançar. As *Process Areas* podem alcançar diferentes níveis de maturidade, estabelecidos de forma a facilitar o desenvolvimento da norma (HOPKINSON, 1999). Maiores detalhes sobre a estrutura da norma ISO/IEC 21827:2008 são descritos no capítulo 3.

2.2.4 Metodologias de gestão de riscos

Nesta subseção serão apresentadas as metodologias COSO, OCTAVE, CRAMM, CORAS, FRAP, COBRA e *Risk Watch* por apresentarem uma alta taxa de aceitação nas organizações e por estarem baseadas nas práticas, normas e padrões nacionais e internacionais de gerenciamento de riscos.

2.2.4.1 COSO

O COSO *(Comittee of Sponsoring Organizations of the Treadway Commission)* é um controle interno que foi criado em 1992. Ele tem por objetivo definir um processo para garantir que os objetivos da organização sejam atingidos (CARVALHO, 2009).

O controle interno definido pelo COSO compreende de um plano para a organização e um conjunto coordenado de métodos e medidas para proteger o patrimônio, verificar a exatidão dos dados contábeis, promover a eficiência operacional e encorajar a adesão da política estipulada pela administração.

Em 2004, o COSO passou a integrar a avaliação global do sistema de gestão de riscos chamado COSO *Enterprise Risk Management - Integrated Framework* (ERBEN, 2008). Os processos definidos pelo controle interno do COSO são constituídos por cinco elementos que estão inter-relacionados (CARVALHO, 2009):

- Ambiente de controle;
- Avaliação e gerenciamento de riscos;

- Atividade de controle;
- Informação e comunicação;
- Monitoramento.

2.2.4.2 OCTAVE

A abordagem OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) foi desenvolvida pela equipe do SEI (*Software Engineering Institute*), responsável pelo desenvolvimento do CMM/CMMI (*Capability Maturity Model / Capability Maturity Model Integration*). É uma metodologia que recomenda um processo de sessões nas quais os colaboradores que trabalham na área analisada da organização definem os riscos e as medidas de proteção (STONEBURNER; GOGUEN e FERINGA, 2002).

A abordagem OCTAVE está focada na identificação dos ativos críticos e das ameaças sobre esses ativos, das vulnerabilidades organizacionais e tecnológicas, que expõem essas ameaças e criam um risco para a organização (WOODY, 2006).

A OCTAVE usa uma metodologia com três fases para examinar a organização e os recursos tecnológicos, fornecendo um gráfico de informações das necessidades de segurança da organização.

O principal objetivo da metodologia OCTAVE é ajudar as organizações a melhorar a habilidade de gerenciar e proteger os riscos de segurança da informação (OLIVEIRA, 2006).

2.2.4.3 CRAMM

O CRAMM (*CCTA RISK Analisys and Management Method*) é uma abordagem que foi desenvolvida pelo governo britânico da organização CCTA (*Central Communication and Telecom Agency*), agora denominado OGC (*Office of Government Commerce*). Essa metodologia é utilizada por muitas organizações em torno do mundo por oferecer suporte a implementação da ISO/IEC 17799 (MARQUIS, 2006).

O CRAMM é uma abordagem para o desenvolvimento do processo de gerenciamento de riscos que identifica as ameaças face aos ativos e vulnerabilidades para gerir o risco e propor contramedidas. Essa abordagem fornece uma ferramenta para calcular o risco sobre a exploração de uma vulnerabilidade sobre um ativo, ajudando a evitar, reduzir ou estabelecer riscos aceitáveis (YAZAR, 2002).

A avaliação de um ativo é realizada para identificar o potencial de dano que pode ser causado por uma falha na confidencialidade, integridade ou disponibilidade (MARQUIS, 2006). O CRAMM supõe que o custo para eliminar o risco restringe o seu uso pelas organizações, mas quando adotado pode reduzir efetivamente o risco (JONES e ASHENDEN, 2005).

2.2.4.4 CORAS

O CORAS é um método para conduzir a análise da segurança baseado em técnicas tradicionais de análise de segurança como a técnica *brainstorming*, análise de árvore de falhas (FTA - *Fault Tree Analysis*) e análise de modo e efeito de falha (FEMEA - *Failure Mode and Effect Analysis*), combinado com o desenvolvimento UML (*Unified Modeling Language*) (AAGEDAL et al., 2002).

O modelo CORAS para a avaliação de riscos de segurança é separado em três diferentes componentes:

1. O CORAS linguagem de modelagem de riscos: inclui a sintaxe gráfica dos diagramas do CORAS e a sintaxe textual e semântica;

2. O método CORAS: descreve o passo-a-passo do processo de análise de segurança com um guia para a construção de diagramas;

3. A ferramenta CORAS: uma ferramenta para documentar, manter e relatar resultados de analises de riscos.

O CORAS está baseado nas normas AS/NZS 4360, ISO/IEC 17799, ISO/IEC 13335 e

em um sistema de documentação em forma de modelo de referência para processamento distribuído aberto (AAGEDAL et al., 2002).

2.2.4.5 FRAP

A abordagem FRAP *(Facilitated Risk Assessment Process)* foi desenvolvida por Thomas Peltier e está baseada na aplicação de técnicas de gestão de riscos de uma forma altamente eficáz em termos de custos (OLIVEIRA, 2006). Ela foi designada como uma abordagem que pode ser usada pelos próprios gerentes com a assistência de um facilitador.

O FRAP consiste de um processo que deve ser completado em um período de dez dias de avaliação (LANDOLL, 2006). Essa abordagem utiliza métodos quantitativos para mitigar o risco e fornecer *templates* e *checklists*. Os processos que envolvem o desenvolvimento da abordagem FRAP são:

- Sessão de *brainstorming* para identificar as ameaças;
- Atribuição de níveis de impacto e de probabilidade de cada ameaça;
- Identificação e atribuição de controles;
- Relatório de gerenciamento.

2.2.4.6 COBRA

A abordagem COBRA *(Consultative, Objective and Bi-functional Risk Analysis)* consiste de um conjunto de ferramentas e aplicativos que são utilizados para realizar auto-avaliações do risco. Essas ferramentas foram desenvolvidas para o reconhecimento da natureza mutável da segurança de TI e das exigências colocadas pelas organizações em suas áreas (ELKY, 2006).

Existem dois produtos primários do COBRA: o Consultor de Riscos e a Conformidade ISO. O consultor de riscos é uma ferramenta com o conhecimento construído em bases

e modelos que permitem o usuário criar questionários para recolher informações sobre tipos de bens, vulnerabilidades, ameaças e controles. A partir destas informações, o consultor de riscos cria relatórios e faz recomendações de forma personalizada. A conformidade ISO é uma ferramenta semelhante, porém sua avaliação está centrada no cumprimento da norma ISO/IEC 17799.

A metodologia COBRA fornece um serviço de avaliação de riscos quantitativo e qualitativo, com o uso de questionários baseados em sistemas PC usando sistemas peritos e uma extensiva base de conhecimento (ELKY, 2006).

O COBRA avalia a importância relativa de todas as ameaças e vulnerabilidades gerando recomendações e soluções. Ele possui relatórios que fornecem a avaliação dos riscos relativos com a pontuação ou o nível, para cada categoria de riscos. Os riscos identificados são automaticamente relacionados com as implicações potenciais (financeiros, perda cliente, etc.) para a organização ou departamento.

2.2.4.7 Risk Watch

A abordagem *Risk Watch* é uma metodologia que utiliza uma base de dados de conhecimento especializada para encaminhar o usuário ao gerenciamento de riscos. O *Risk Watch* fornece relatórios sobre o cumprimento das atividades e instruções para a gestão dos riscos (ELKY, 2006).

A base de dados de conhecimento que é fornecida pela abordagem é totalmente personalizável pelo seu utilizador, incluindo a habilidade de criar novas categorias de ativos, ameaças, vulnerabilidades, salvaguardas e categorias de perguntas em um conjunto questões. A ferramenta inclui controles da norma ISO/IEC 17799 e US-NIST 800-26 além de outros produtos, cada um deles centrado ao longo do cumprimento de diferentes necessidades (OLIVEIRA, 2006).

Essa abordagem de gerenciamento de riscos inclui informações estatísticas para apoiar a avaliação quantitativa dos riscos, permitindo ao usuário apresentar o ROI

(*Return On Investment*) para várias estratégias de segurança.

2.3 Conclusões Parciais

A gestão de riscos associada ao gerenciamento estratégico da segurança da informação, pode ser utilizada para estabelecer medidas preventivas de segurança que podem tanto tratar de riscos emergenciais como prevenir futuros riscos. A segurança pode ser planejada para garantir que não ocorram incidentes de segurança e ainda para definir prioridades de proteção.

O gerenciamento estratégico da segurança pode trazer maiores garantias de proteção para organização através da implementação de métodos e de procedimentos apropriados ao ambiente de exposição das informações. Além da redução dos custos relacionados aos investimentos em segurança e reparos ocasionados por falhas ou ausência de procedimentos de segurança. Com o conhecimento das ameaças, vulnerabilidades e riscos, as organizações podem estabelecer estratégias que acompanham a evolução das mudanças e as alterações das características dos riscos. O entendimento da segurança pode apoiar as decisões relacionadas ao desenvolvimento, manutenção ou operação dos procedimentos de segurança.

O desenvolvimento da gestão de riscos é realizado por meio de normas de segurança e normas específicas de gestão de riscos. Também existem metodologias de gestão de riscos que apóiam a mitigação, avaliação e gestão dos riscos. O uso dessas soluções fornecem maiores garantias de segurança a organização.

Além dos fatores que contribuem para o aumento da segurança das informações, a gestão de riscos pode revelar fatos ainda desconhecidos pelas organizações. Essa premissa determina que não é possível estabelecer uma boa estratégia de segurança sem conhecer os riscos. Dessa forma a gestão de riscos influência diretamente no planejamento estratégico da segurança.

3 INTEGRANDO NORMAS DE GESTÃO E MATURIDADE DE RISCOS DE SEGURANÇA

Neste capítulo serão descritas e analisadas as normas ISO/IEC 27001:2006 e ISO/IEC 21827:2008(SSE-CMM) buscando relacioná-las de forma que se possa compreender o processo de implantação e estabelecimento de cada uma. O objetivo é verificar como essas normas podem ser integradas para o desenvolvimento de um SGSI (Sistema de Gestão da Segurança da Informação) que forneça maiores garantias de proteção. Também é realizada a análise da abordagem e da estrutura de desenvolvimento que cada uma fornece.

Partes deste capítulo e os resultados obtidos estão presentes no artigo "Desenvolvimento de Sistemas de Gestão da Segurança da Informação através da Integração das Normas ISO/IEC 27001:2006 e ISO/IEC 21827:2008 (SSE-CMM)", publicado nos anais do V CONeGOV (Conferência Sul-Americana em Ciência e Tecnologia aplicada ao Governo Eletrônico)[1][2].

[1] O V CONeGOV (Conferência Sul-Americana em Ciência e Tecnologia aplicada ao Governo Eletrônico) foi realizado nos dias 17, 18 e 19 de novembro de 2009 na cidade de Florianópolis - Santa Catarina, Brasil. Ressaltando a importância da publicação dos resultados de pesquisa e se consolidando como importante canal de comunicação científica. Detalhes do evento podem ser encontrados em http://www.i3g.org.br/conegov.

[2] Este artigo foi premiado como o melhor artigo da conferência.

3.1 O Desenvolvimento de Sistemas de Gestão da Segurança da Informação

A necessidade de garantir a confidencialidade, integridade e disponibilidade das informações faz com que as organizações estabeleçam um SGSI (HERRERA, 2005). Um SGSI é uma maneira de proteger e de gerenciar as informações sobre uma abordagem de riscos do negócio, que estabelece, implementa, monitora, revisa, mantém e melhora a segurança da informação (HANASHIRO, 2007). A coleção de componentes de segurança requeridos para um sistema ser implementado cuidadosamente, evitando o ataque de ameaças e a exposição a riscos, é chamado de SGSI (DEY, 2007).

No desenvolvimento de um projeto de SGSI é aplicado um conjunto adequado de controles tais como políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware* (HANASHIRO, 2007). Esse conjunto de controles de segurança é dado por normas e guias de segurança.

A efetividade de um SGSI desenvolvido por uma organização está condicionada à efetividade dos controles de segurança da informação disponíveis (HERRERA, 2007). Sem a implementação adequada dos controles ou sem o apoio das normas de segurança, um SGSI pode não atender às necessidades de segurança organizacionais.

3.2 Normas de Segurança

Nesta seção serão apresentadas duas normas de segurança, a ISO/IEC 27001:2006 recomendada pela Instrução Normativa GSI Nº 1[3] e a ISO/IEC 21827:2008 indicada para a melhoria dos processos de segurança organizacionais. Essas normas serão descritas e comparadas, a fim de identificar características específicas de segurança.

[3] A Instrução Normativa GSI Nº 1, de 13 de junho de 2008, recomenda e orienta a condução de políticas de segurança da informação e comunicações já existentes ou a serem implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta (FELIX, 2008).

3.2.1 A estrutura de desenvolvimento da norma ISO/IEC 27001:2006

A norma ISO/IEC 27001:2006 foi construída baseada na norma britânica BS7799 e na ISO/IEC 17799 (ABNT NBR ISO/IEC 27001, 2006). Seu objetivo é proporcionar um modelo para o estabelecimento, implementação, funcionamento, acompanhamento, revisão, manutenção e melhoria do SGSI, dentro do contexto dos riscos globais do negócio da organização (FENZ et al., 2007). Esta norma pode ser aplicada em todos os tipos de organizações, como por exemplo, empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos, etc. Esta norma é principalmente adotada para o estabelecimento de estratégias de segurança pela organização e pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas (ABNT NBR ISO/IEC 27001, 2006).

O SGSI projetado pela norma assegura a seleção de controles de segurança adequados e proporcionados para proteger os ativos da informação propiciando confiança às partes interessadas.

Todos os controles de segurança recomendados pela norma ISO/IEC 27001:2006 são encontrados na norma ISO/IEC 17799:2005. A norma ISO/IEC 17799:2005 está contida na ISO/IEC 27001:2006, ou seja, a norma ISO/IEC 27001:2006 fornece um processo definido de implantação dos controles da norma ISO/IEC 17799:2005.

A norma ISO/IEC 27001:2006 aplica um sistema de processos dentro da organização, junto com a identificação e interações destes processos. Essa abordagem de processos enfatiza a importância dos seguintes aspectos:

- Entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança da informação;

- Implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos globais do negócio;

- Monitoração e análise crítica do desempenho e eficácia do SGSI; e
- Melhoria contínua baseada em medições objetivas.

A norma ISO/IEC 27001:2006 incorpora o ciclo *Plan-Do-Check-Act* (PDCA), que é adotado em toda a estrutura dos processos do SGSI. O ciclo PDCA baseia-se no ciclo de melhoria continua que consiste em planejar (*Plan - P*), fazer (*Do - D*), verificar (*Check - C*) e agir (*Act - A*). O ciclo PDCA é uma ferramenta importante para a análise e melhoria dos processos organizacionais contribuindo para a tomada de decisões gerenciais e para o alcance das metas e objetivos da organização (KAJAVA et al., 2006).

3.2.2 A estrutura de desenvolvimento da norma ISO/IEC 21827:2008 (SSE-CMM)

A norma ISO/IEC 21827:2008 não prescreve uma sequência ou um processo particular, mas captura as práticas que são geralmente observadas na indústria. Esta norma é designada para todos os tipos de organizações, sendo usada para a melhoria e avaliação da capacidade de maturidade dos processos de segurança (SG-SBP, 2008).

A estrutura de desenvolvimento da norma ISO/IEC 21827:2008 é dada por 22 PAs (*Process Areas*), divididas em dois grupos, Práticas Base de Segurança e Práticas Base Organizacionais e do Projeto. A estrutura de distribuição das PAs em seus grupos correspondentes pode ser vista na tabela 3.1.

Tabela 3.1: Estrutura de distribuição das PAs da norma ISO/IEC 21827:2008 (SSE-CMM)

Categorias	PAs *(Process Areas)*
Práticas Base de Segurança	PA01 - Administrar os Controles de Segurança PA02 - Avaliar o Impacto PA03 - Avaliar os Riscos de Segurança PA04 - Avaliar as Ameaças PA05 - Avaliar as Vulnerabilidades PA06 - Construir Argumentos de Segurança PA07 - Coordenar a Segurança PA08 - Monitorar a Postura da Segurança PA09 - Estabelecer a Entrada de Segurança

continua na próxima página

Tabela 3.1: Estrutura de distribuição das PAs da norma ISO/IEC 21827:2008 (SSE-CMM)(continuação)

Categorias	PAs *(Process Areas)*
	PA10 - Especificar as necessidades de segurança PA11 - Verificar e Validar a Segurança
Práticas Base Organizacionais e do Projeto	PA12 - Assegurar a Qualidade PA13 - Gerenciar a Configuração PA14 - Gerenciar o Risco do Projeto PA15 - Monitorar e Controlar o Esforço Técnico PA16 - Planejar o Esforço Técnico PA17 - Definir o Processo de Engenharia de Sistemas da Organização PA18 - Melhorar o Processo de Engenharia de Sistemas da Organização PA19 - Gerenciar a Evolução da Linha do Produto PA20 - Gerenciar o Ambiente de Suporte a Engenharia de Sistemas PA21 - Promover a Habilidade e Conhecimento Progressivo PA22 - Coordenar com os Fornecedores

A norma ISO/IEC 21827:2008 também define níveis de maturidade dos processos de segurança da organização que são ampliados após o estabelecimento e cumprimento das práticas da segurança (BATISTA, 2007). O processo mais "maduro" define uma organização cujos processos são melhores definidos e conduzidos. São seis níveis de maturidade definidos, onde cada um desses níveis consiste de um número de Práticas Genéricas (*GP - Generic Practices*) que suportam o desempenho das PAs. Os níveis de maturidade atribuídos pela norma ISO/IEC 21827:2008 são:

- Nível 0 - Práticas base não são realizadas;
- Nível 1 - Práticas base são realizadas informalmente;
- Nível 2 - Práticas base são planejadas e monitoradas;
- Nível 3 - Práticas base estão bem definidas;

- Nível 4 - Práticas base são controladas quantitativamente;
- Nível 5 - Práticas base estão em contínua melhoria.

Uma característica marcante da ISO/IEC 21827:2008 é a utilização de métricas de segurança para avaliar os processos. As métricas de segurança são abordadas nos níveis mais altos de maturidade para um processo bem definido ou em contínua melhoria (SSE-CMM, 2003). Kormos et al.(1999) cita que a ISO/IEC 21827:2008 fornece para a organização um conjunto de métricas para avaliar a segurança dos produtos, serviços ou operacões.

O processo de melhoria e maturidade organizacional da norma ISO/IEC 21827:2008 é realizado por meio do modelo IDEAL e é usado para definir ações que capacitem as organizações a melhorar seus processos. O modelo IDEAL serve como um guia para iniciar, planejar e implementar ações de melhoria. A palavra IDEAL é um acrônimo do inglês para Iniciar (*initiating*), Diagnosticar (*diagnosing*), Estabelecer (*establishing*), Agir (*acting*) e Aprender (*learning*). O modelo IDEAL forma uma infra-estrutura de cinco fases para guiar organizações no planejamento e na implementação de um efetivo programa de melhoria de processos (ISO/IEC 21827, 2008).

3.2.3 Análise comparativa das normas ISO/IEC 27001:2006 e ISO/IEC 21827:2008

Para que se possa compreender a relação entre as normas ISO/IEC 27001:2006 e ISO/IEC 21827:2008 foram realizadas duas comparações. Na primeira comparação, as características da norma ISO/IEC 27001:2006 são comparadas com as da norma ISO/IEC 21827:2008. Na segunda comparação, são identificados os controles da norma ISO/IEC 17799:2005 que correspondem as PAs da norma ISO/IEC 21827:2008. As informações para critério de comparação foram obtidas dos documentos ABNT NBR ISO/IEC 27001:2006 (ABNT NBR 27001, 2006), ABNT NBR ISO/IEC 17799 (NBR ISO/IEC 17799, 2005) e SSE-CMM *Systems Security Engineering Capability Maturity Model Model Description Document vesion 3.0* (SSE-CMM, 2003).

Como resuldado da primeira comparacão (ver Tabela 3.2, foi observado que as normas apresentam duas visões que estão permanentemente presentes antes e depois do SGSI ser implementado: a visão funcional e a visão de processos. A visão funcional é representada pela norma ISO/IEC 27001:2006 que fornece uma estrutura de recomendações que deve ser seguida para o desenvolvimento de um SGSI. Já a norma ISO/IEC 21827:2008 representa uma visão de processos, que fornece as práticas que devem ser implementadas para a construção de um SGSI.

Com relação ao ciclo de melhoria, que indica uma ferramenta de qualidade para o desenvolvimento da norma, verifica-se que a ISO/IEC 27001:2006 utiliza o ciclo de melhoria PDCA para a análise e melhoria dos processos organizacionais, enquanto a ISO/IEC 21827:2008 utiliza o modelo IDEAL. Ambos os modelos consistem em um ciclo de atividades modelado para guiar a melhoria contínua e para desenvolvimento adequado de cada norma.

Tanto a norma ISO/IEC 27001:2006 como a norma ISO/IEC 21827:2008 podem ser adotadas por qualquer tipo de organização, seja ela de pequeno ou grande porte. Isso indica que não há restrições quanto ao uso das normas e a escolha de aderir a uma ou a outra norma de segurança, que deve ser direcionada ao atendimento dos objetivos de segurança organizacionais.

O desenvolvimento da norma ISO/IEC 27001:2006 está baseada na implementação dos controles de segurança contidos na ISO/IEC 17799:2005. Dessa forma, a ISO/IEC 27001:2006 implementa a ISO/IEC 17799:2005. Na ISO/IEC 21827:2008 não há um documento de segurança complementar para o seu desenvolvimento. Ela é implantada por meio da implementação das PAs e é avaliada pelo método SSAM (*SSE-CMM Appraisal Method*).

Uma característica importante da ISO/IEC 21827:2008 é o uso das métricas para avaliar os processos de segurança e estabelecer níveis de maturidade. Essa característica está voltada ao gerenciamento da segurança. Já a norma ISO/IEC 27001:2006 foi

projetada para permitir a uma organização alinhar ou integrar seu SGSI com requisitos de sistemas de gestão relacionados.

As características da norma ISO/IEC 27001:2006 e da norma ISO/IEC 21827:2008 mencionadas anteriormente podem ser vistas no quadro comparativo da Tabela 3.2:

Tabela 3.2: Quadro comparativo de características das normas ISO/IEC 27001:2006 e ISO/IEC 21827:2008

Principais características	**ISO/IEC 27001:2006**	**ISO/IEC 21827:2008**
Propósito da norma	Estabelecer, revisar, implementar, acompanhar, manter e melhorar um SGSI	Descrever características de segurança de um processo
Ferramenta de qualidade	PDCA	IDEAL
Organizações que podem fazer uso	Todas	Todas
Norma de complemento	ISO/IEC 17799:2005	Não apresenta
Recursos de gerenciamento	Controles da ISO/IEC 17799:2005	Métricas
Visão de implementação	Controles de segurança	Processos de segurança
Base de implementação	Controles da ISO/IEC 17799:2005	Áreas do Processo (PAs)
Pré-condição de implementação	Não apresenta	Não apresenta
Principal característica	Fornecimento de um conjunto de recomendações de segurança	Melhoria dos processos de segurança

A segunda comparação foi realizada entre as normas ISO/IEC 21827:2008 e ISO/IEC 17799:2005. A norma ISO/IEC 17799:2005 está contida na norma ISO/IEC 27001:2006, sendo que as recomendações de segurança da norma ISO/IEC 27001:2006 implicam na implementação dos controles da ISO/IEC 17799:2005.

Para essa comparação foram selecionadas 11 PAs referentes as Práticas Base de Segurança da norma ISO/IEC 21827:2008 e foram selecionados controles da norma ISO/IEC 17799:2005. O critério adotado para identificar os controles relacionados com

as PAs foi baseado no atendimento dos objetivos e requisitos (*Base Practices* - BP) de cada PA. Também foi usado como critério de comparação a literatura relacionada as normas e as publicações oficiais da ABNT e do SEI (*Software Engineering Institute*). Na Tabela 3.3 são apresentados os controles da ISO/IEC 17799:2005 que estão relacionados com as PAs da ISO/IEC 21827:2008:

Tabela 3.3: Quadro comparativo das PAs da norma ISO/IEC 21827:2008 (SSE-CMM) com os controles da norma ISO/IEC 27001:2006.

ISO/IEC 21827:2008	**ISO/IEC 17799:2005**
Descrição das PAs	**Controles relacionados**
PA01 - Administração dos controles de segurança	Documento da política de segurança da informação; Atribuição de responsabilidades para a segurança da informação; Processo de autorização para os recursos de processamento da informação; Recomendações para classificação; Rótulos e tratamento da informação; Papéis e responsabilidades; Responsabilidades da direção; Conscientização, educação e treinamento em segurança da informação; Documentação dos procedimentos de operação; Gestão de mudanças; Gerenciamento de mudanças para serviços terceirizados; Procedimentos para tratamento de informação; Gerenciamento de privilégios; Gerenciamento de senha do usuário; Sistema de gerenciamento de senha; Prevenção de mau uso de recursos de processamento da informação;
PA02 - Avaliação do impacto	Apresentado no item 4 referente à Introdução da norma ISO/IEC 17799:2005;
PA03 - Avaliação dos Riscos de segurança	Identificação dos riscos relacionados com partes externas; Inventário dos ativos; Proprietário dos ativos;

continua na próxima página

Tabela 3.3: Quadro comparativo das PAs da norma ISO/IEC 21827:2008 (SSE-CMM) com os controles da norma ISO/IEC 27001:2006 (continuação).

Descrição das PAs	**Controles relacionados**
	Uso aceitável dos ativos; Apresentado no item 4 referente à Introdução da norma ISO/IEC 17799:2005;
PA04 - Avaliação de ameaças	Apresentado no item 4 referente à Introdução da norma ISO/IEC 17799:2005;
PA05 - Avaliação de Vulnerabilidades	Apresentado no item 4 referente à Introdução da norma ISO/IEC 17799:2005;
PA06 - Construção de argumentos de garantia	Identificando a segurança da informação, quando tratando com os clientes;
PA07 - Coordenação da segurança	Acordos de confidencialidade; Identificando segurança da informação nos acordos com terceiros; Segregação de funções; Acordos para a troca de informações; Procedimentos para controle de mudanças; Conformidade com as políticas e normas de segurança da informação;
PA08 - Monitoração da postura da segurança	Comprometimento da direção com a segurança da informação; Coordenação da segurança da informação; Contato com autoridades; Análise crítica independente de segurança da informação; Gestão de capacidade; Controles contra códigos maliciosos; Controles contra códigos móveis; Registros de auditoria; Monitoramento do uso do sistema; Proteção das informações dos registros (log); Registros *(log)* de administrador e operador; Registros *(log)* de falhas; Vazamento de informações; Controle de vulnerabilidades técnicas; Controles de auditoria de SI;

continua na próxima página

Tabela 3.3: Quadro comparativo das PAs da norma ISO/IEC 21827:2008 (SSE-CMM) com os controles da norma ISO/IEC 27001:2006 (continuação).

Descrição das PAs	**Controles relacionados**
PA09- Fornecer a entrada segurança	Documento da política de segurança da informação; Análise crítica da política de segurança da informação; Processo disciplinar; Políticas e procedimentos para troca de informações; Política de controle de acesso; Registro de usuário; Restrição de acesso à informação; Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação;
PA10 - Especificar as necessidades de segurança	Segurança da documentação dos sistemas; Uso de senhas; Autenticação para conexão externa do usuário; Procedimentos seguros de entrada no sistema *(log-on)*; Identificação e autenticação de usuário; Análise e especificação dos requisitos de segurança; Integridade de mensagens; Incluindo segurança da informação no processo de gestão da continuidade de negócio; Continuidade de negócios e análise/avaliação de riscos; Estrutura do plano de continuidade do negócio; Identificação da legislação vigente; Direitos de propriedade intelectual; Vazamento de informações; Proteção de ferramentas de auditoria de SI;
PA11 - Verificação e validação da segurança	Entrega de serviços; Monitoramento e análise crítica de serviços terceirizados; Cópias de segurança das informações; Análise crítica dos direitos de acesso de usuário; Validação dos dados de entrada; Controle do processamento interno; Validação de dados de saída;

continua na próxima página

Tabela 3.3: Quadro comparativo das PAs da norma ISO/IEC 21827:2008 (SSE-CMM) com os controles da norma ISO/IEC 27001:2006 (continuação).

Descrição das PAs	Controles relacionados
	Testes, manutenção e reavaliação dos planos de continuidade do negócio; Verificação da conformidade técnica.

Foi observado que nem todos os controles da ISO/IEC 17799:2005 possuem uma relação direta com as PAs da ISO/IEC 21827:2008. Os controles manuseio de mídias, serviço de comércio eletrônico, controles criptográficos, computação móvel e de trabalho remoto e alguns outros, não estão contidos na tabela 3.3 por não terem ligação aparentemente direta com o objetivos da PAs.

No entanto, a implementação de um projeto de SGSI recomendado pela norma ISO/IEC 27001:2006 está condicionado as necessidades de segurança organizacionais e portanto, nem todos os controles de segurança têm obrigatoriedade de implementação. Na norma ISO/IEC 21827:2008, as PAs também são selecionadas objetivando atender às necessidades de segurança organizacionais e podem ser selecionadas PAs tanto da categoria de práticas base de segurança como do grupo práticas base organizacionais e do projeto.

3.3 Integrando as Normas de Segurança ISO/IEC 27001:2006 e ISO/IEC 21827:2008

A relação da norma ISO/IEC 27001:2006 com a ISO/IEC 21827:2008 está baseada no estabelecimento de maiores garantias de proteção. Cada norma fornece meios para assegurar o desenvolvimento da segurança de forma sistemática e contínua.

A norma ISO/IEC 17799:2005 que fornece os controles recomendados pela norma ISO/IEC 27001:2006 foi comparada com as PAs da ISO/IEC 21827:2008 para se verificar a similaridade de processos. A partir dessa comparação nota-se que alguns controles não estão diretamente ligados com a ISO/IEC 21827:2008. Com isso, pode ser observado que

a ISO/IEC 21827:2008 é mais indicada para o gerenciamento de processos de segurança e não para a sua definição dos processos (controles) que serão implementados.

A definição dos controles de segurança que serão implementados pelo SGSI seguem a estrutura de segurança organizacional, podendo alguns controles serem selecionados e outros não. O mesmo acontece com as PAs da ISO/IEC 21827:2008, onde nem todas as PAs são selecionadas e procura-se fazer a seleção de acordo com a necessidade de segurança organizacional. Dessa maneira, os controles que são selecionados da ISO/IEC 17799:2005 recomendados pela ISO/IEC 27001:2006 podem ganhar níveis de maturidade por meio da implementação da ISO/IEC 21827:2008.

A integração das normas está no desenvolvimento em conjunto das normas. Ganhando níveis de maturidade, os controles da ISO/IEC 17799:2005 podem ser gerenciados e monitorados assegurando o aprimoramento da segurança organizacional. Cada organização pode definir seus objetivos de segurança selecionando controles e determinando níveis de maturidade que atendam suas necessidades de segurança.

A integração das normas ISO/IEC 27001:2006 e ISO/IEC 21827:2008 pode trazer benefícios para as organizações onde se pode observar:

- Melhoria nos aspectos de definição da segurança fundamental: em uma organização que não tenha definido o processo global de segurança, a primeira etapa deveria ser definí-lo, levando em consideração os sub-processos de segurança e controles que são propostos no modelo de referência;

- Desenvolvimento de projetos SGSI específicos: em organizações científicas como laboratórios ou empresas de desenvolvimento de *software* com processos de negócio especializado os projetos de SGSI poderiam ser desenvolvidos com o objetivo de aprofundar as relações com a norma ISO/IEC 21827:2008. Este conhecimento é importante tanto para conhecer melhor as necessidades de segurança requisitadas por estes setores da economia, como também, as dificuldades inerentes aos setores

facilitando a criação de padrões para o desenvolvimento de soluções de segurança setoriais;

- Determinação de níveis de maturidade para os processos de segurança: em um projeto de SGSI, deve-se exigir que o processo global de segurança projetado e implementado possa ser avaliado como nível maior de maturidade. Um SGSI de nível 1 teria deficiências. Com a utilização da ISO/IEC 21827:2008 é possível estipular o nível de capacidade que se deseja alcançar;

- Atendimento dos requisitos legislativos: uma vez que tanto as leis quanto seus regulamentos levam em consideração os processos de segurança da informação, os projetos poderiam revisar as próprias leis conforme a visão de processos de segurança assim como identificar as falhas que a norma pode apresentar para compreendê-las, melhorá-las e aplicá-las;

- Redução de custos: com a implementação de controles monitorados pela ISO/IEC 21827:2008, pode-se assegurar a redução de falhas de segurança e consequentemente a diminuição de recursos financeiros aplicados para reparação de danos;

- Definição de estratégias de segurança: o gerenciamento dos processos de segurança fornece uma visão do quadro de segurança atual da organização, fornecendo subsídios para a implementação de medidas preventivas que assegurem o bem estar organizacional;

- Reconhecimento organizacional: a certificação por normas reconhecidas no ambiente de segurança garante maior confiabilidade por parte de clientes, colaboradores e terceiros.

3.4 Um Modelo de Referência para o Desenvolvimento de SGSI

A Figura 3.1 mostra a integração da norma ISO/IEC 27001:2006 e a norma ISO/IEC 21827:2008 no modelo de referência, onde se pode observar:

- **Visão orientada por disciplinas funcionais:** no modelo diferenciam-se seis disciplinas funcionais incluindo a segurança fundamental, segurança ambiental e de infra-estrutura, segurança dos sistemas, segurança em comunicações e redes, segurança física e segurança pessoal;

- **Visão orientada por processos:** no modelo estão identificados oito sub-processos de segurança incluindo a gestão estratégica da segurança, cumprimento legal e padrões aplicáveis, identificação, classificação e avaliação de ativos, análise e avaliação de riscos de segurança, tratamento e gestão de riscos de segurança, gestão da segurança operacional, segurança das operações - condições normais e segurança das operações - condições anormais;

- **Segurança Fundamental:** na tabela 3.4, pode-se observar que a mesma contém um conjunto de controles e sub-processos definidos em ambas as normas ISO/IEC 21827:2008 e ISO/IEC 27001:2006 que são imprescindíveis para que o processo de segurança exista não só na melhoria da sua capacidade, mas também das necessidades específicas de segurança em áreas concretas do negócio. Os controles e sub-processos indicados neste nível são comuns para o resto das áreas funcionais.

Este modelo, em que se integram ambas as visões de segurança, deriva-se da base de conhecimentos TPKB[4] *Theoretical and Practical Knowledge Base* produzida pelo ISSPCS *International Systems Security Professional Certification Scheme*, o qual colabora com o ISSEA *International Systems Security Engineering Association*.

[4]http://www.isspcs.org/tpkb

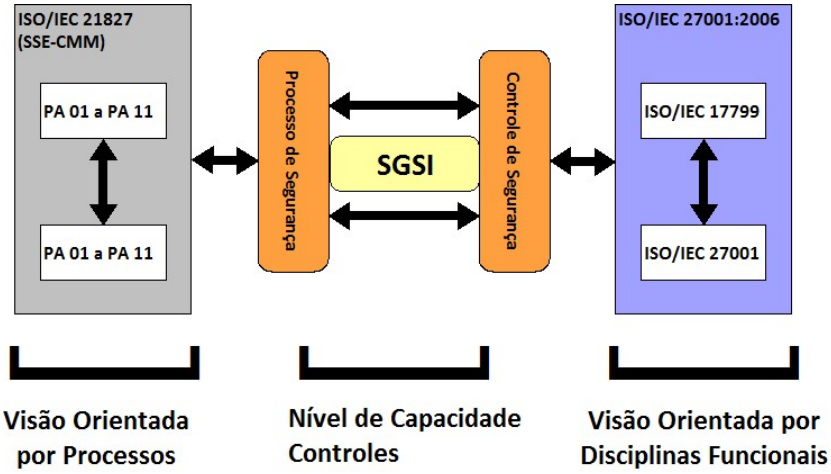

Figura 3.1: Integração da norma ISO/IEC 27001:2006 com a norma ISO/IEC 21827:2008 no modelo de referência
Fonte: HUMPHREYS, 2007.

Tabela 3.4: Distribuição dos controles da ISO/IEC 27001:2006 nas PAs da ISO/IEC 21827:2008 no modelo de referência do SGSI

Processo de Segurança nas Organizações	**1.Gestão Estratégica da Segurança**	**2.Concordância e Normas Aplicáveis**	**3.Identificação, Classificação e Avaliação de Ativos**	**4.Análise e Avaliação de Riscos de Segurança**	**5.Tratamento e Gestão de Riscos de Segurança**	**6.Gestão da Segurança Operacional**	**7.Segurança em Operações - Normais**	**8.Segurança em Operações - Anormais**
Segurança Fundamental	A5 (completo) A6.1 (1,2,3,7) PA06 PA07 PA09 PA10 PA11	A15.1 A5.1.5 A6.2.3 A8.1.1.3 A10.8.2 PA10 PA11	A7 (completo) PA02 PA10	A6.2.1 A14.1.2 PA02 PA03 PA04 PA05	A6.1.8 A6.2.2 PA03	A9.1 A10 (1,2,3) A11.2 A11.6 PA01 PA07 PA08 PA11	A6.1 (4,6,7) A10 (4,5,6) A10 (7,8,9) PA07 PA09 PA10	A13 (completo) A14 (completo) PA06 PA10

continua na próxima página

Tabela 3.4: Distribuição dos controles da ISO/IEC 27001:2006 nas PAs da ISO/IEC 21827:2008 no modelo de referência do SGSI (continuação).

Processo de Segurança nas Organizações	**1.Gestão Estratégica da Segurança**	**2.Concordância e Normas Aplicáveis**	**3.Identificação, Classificação e Avaliação de Ativos**	**4.Análise e Avaliação de Riscos de Segurança**	**5.Tratamento e Gestão de Riscos de Segurança**	**6.Gestão da Segurança Operacional**	**7.Segurança em Operações - Normais**	**8.Segurança em Operações - Anormais**
Ambiental e Infraestrutura	PA06 PA07 PA09 PA10 PA11 PA02	PA10 PA11 PA02	PA02 PA10 PA09	PA02 PA03 PA04 PA05 PA09	PA03 PA09 PA10	A9.2 PA01 PA07 PA08 PA11	PA07 PA09 PA10	PA06 PA10 PA07 PA09
Segurança dos Sistemas	A12.1 PA06 PA07 PA09 PA10 PA11	A15.2 A15.3 PA10 PA11	PA02 PA10	PA02 PA03 PA04 PA05	A12.2 A12.3 PA03	A11.5 A11.7 A12.4 A12.5 PA01 PA07 PA08 PA11	A12.6 PA07 PA09 PA10	PA06 PA10
Segurança em Comunicações e Redes	PA06 PA07 PA09 PA10 PA11 PA01 PA08	PA10 PA11 PA02	PA02 PA10	PA02 PA03 PA04 PA05	PA03	A11.4 PA01 PA07 PA08 PA11 PA09 PA10	A10.10 PA07 PA09 PA10	PA06 PA07 PA10
Segurança Física	PA06 PA07 PA09 PA10 PA11	PA10 PA11	A9 (completo) PA02 PA10	PA02 PA03 PA04 PA05	PA03	PA01 PA07 PA08 PA11	A6.2 (1,2) PA07 PA09 PA10	PA06 PA10

continua na próxima página

Tabela 3.4: Distribuição dos controles da ISO/IEC 27001:2006 nas PAs da ISO/IEC 21827:2008 no modelo de referência do SGSI (continuação).

Processo de Segurança nas Organizações	**1.Gestão Estratégica da Segurança**	**2.Concordância e Normas Aplicáveis**	**3.Identificação, Classificação e Avaliação de Ativos**	**4.Análise e Avaliação de Riscos de Segurança**	**5.Tratamento e Gestão de Riscos de Segurança**	**6.Gestão da Segurança Operacional**	**7.Segurança em Operações - Normais**	**8.Segurança em Operações - Anormais**
Segurança Pessoal	PA06 PA07 PA09 PA10 PA11	PA10 PA11	PA02 PA10	A8.1 PA02 PA03 PA04 PA05	A8.2 PA03	A11.3 PA01 PA07 PA08 PA11	A8.3 PA07 PA09 PA10	PA06 PA10

3.5 A Abrangência das Normas de Segurança no Contexto Organizacional

Desenvolver um SGSI que forneça garantias de segurança não está atrelado apenas ao uso de uma norma. Uma norma de segurança pode satisfazer inúmeros requisitos de segurança, mas não pode abranger todos os aspectos que asseguram proteção.

A Instrução Normativa GSI Nº 1, de 13 de junho de 2008 que trata disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, têm o propósito de manter seguras as informações e orientar a condução de políticas de segurança da informação e comunicações pelos órgãos da Administração Pública Federal, direta e indireta. Cumprindo o art. 3 da Instrução Normativa GSI Nº 1, o Gabinete de Segurança Institucional da Presidência da República - GSI, ficou responsável por orientar a condução da Política de Segurança da Informação e Comunicações. Ficou então definido pelo GSI, que a metodologia de gestão de segurança da informação e comunicações deve basear-se no processo de melhoria contínua, denominado ciclo PDCA (*Plan-Do-Check-Act*), estabelecido pela norma ISO/IEC 27001:2006 e todos os órgãos

da Administração Pública Federal, direta e indireta, devem adotá-la. A escolha realizada pelo GSI levou em consideração três critérios:

- Simplicidade do modelo;
- Compatibilidade com a cultura de gestão de segurança da informação em uso nas organizações públicas e privadas brasileiras; e
- Coerência com as práticas de qualidade e gestão adotadas em órgãos públicos brasileiros.

No entanto, o GSI não leva em consideração que as organizações possuem necessidades de segurança diferentes. O que pode ser adaptado consideravelmente bem para uma organização, pode não ser tão bem adaptado para outra.

Definir uma metodologia para a gestão da segurança da informação baseada na aplicação de apenas uma norma pode deixar lacunas na segurança, resultando em futuras falhas de segurança, danos financeiros e sociais.

Além disso, uma norma não pode ser recomendada para todo e qualquer tipo de organização. As organizações são diferentes, possuem necessidades de segurança específicas e estão em outro contexto cultural. Em muitos casos, a relação de uma organização com uma norma de segurança não se completa. Isso ocorre não pela inconsistência da segurança fornecida por uma norma, mas pelo fato da organização possuir objetivos vinculados as necessidades de segurança próprias.

A utilização de uma única norma de segurança pode trazer benefícios agregando mais proteção a organização, mas de fato, ela não preenche e nem se enquadra a todos os aspectos de segurança necessários para fornecer controle sobre todos os aspectos de segurança organizacional.

As normas de segurança se complementam, de forma a fornecer maiores garantias de segurança. Com a integração das normas de segurança as organizações podem focar seus objetivos de proteção, prevenindo que incidentes de segurança ocorram. A integração

das normas que se dá pela combinação da segurança pode adequar-se a maioria das organizações e se enquadrar em um contexto específico.

3.6 Conclusões Parciais

Pode-se observar que a norma ISO/IEC 27001:2006 fornece uma estrutura bem definida para a implementação de um SGSI, enquanto a norma ISO/IEC 21827:2008 pode ser usada para assegurar que os processos de segurança sejam desenvolvidos e mantidos em conformidade com a segurança, adquirindo níveis de maturidade. Neste sentido, a integração das normas ISO/IEC 27001:2006 e ISO/IEC 21827:2008 pode ser utilizada como um modelo de referência para o desenvolvimento de processos de SGSI.

Com a existência de vários documentos de segurança, destes incluem o NIST, BS7799, ISO/IEC 13335 entre outros, a ISO/IEC 21827:2008 pode ser entendida como um sistema para a descrição das características essenciais do processo de engenharia de segurança da organização, que sempre deve existir para assegurar a boa engenharia de segurança. As organizações que buscam segurança podem usar a ISO/IEC 21827:2008 para avaliar e refinar as práticas de engenharia de segurança; os clientes podem usá-la para avaliar o recurso de engenharia de segurança de um dado sistema; e as organizações para estabelecer valores organizacionais com base nos recursos.

4 UM MODELO CONCEITUAL PARA A GESTÃO DE RISCOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

Um modelo de gestão de riscos pode ser descrito como uma metodologia de análise que consiste na seleção de um conjunto de conceitos chaves e termos associados, os quais formam um vocabulário para a descrição do risco (OLIVEIRA, 2006). Dessa forma, a fim de obter um maior entendimento sobre a gestão de riscos, este capítulo aborda as teorias e conceitos que dão suporte a modelagem conceitual.

Também neste capítulo, será apresentado o modelo conceitual GRiSSI que oferece suporte a gestão da segurança. A proposta do modelo conceitual contribuirá para ampliar a documentação disponível na literatura, auxiliando também no entendimento de conceitos relacionados ao risco.

4.1 A Abordagem Utilizada

A abordagem utilizada para a construção do modelo conceitual GRiSSI é apresentada na Figura 4.1.

A abordagem consiste de dois passos:

1. Alinhamento de conceitos: o objetivo é identificar os conceitos relevantes para o domínio do risco e integrá-los a terminologia. Os principais resultados deste passo são:

- *Tabela de alinhamento de conceitos:* identifica e destaca os conceitos de várias

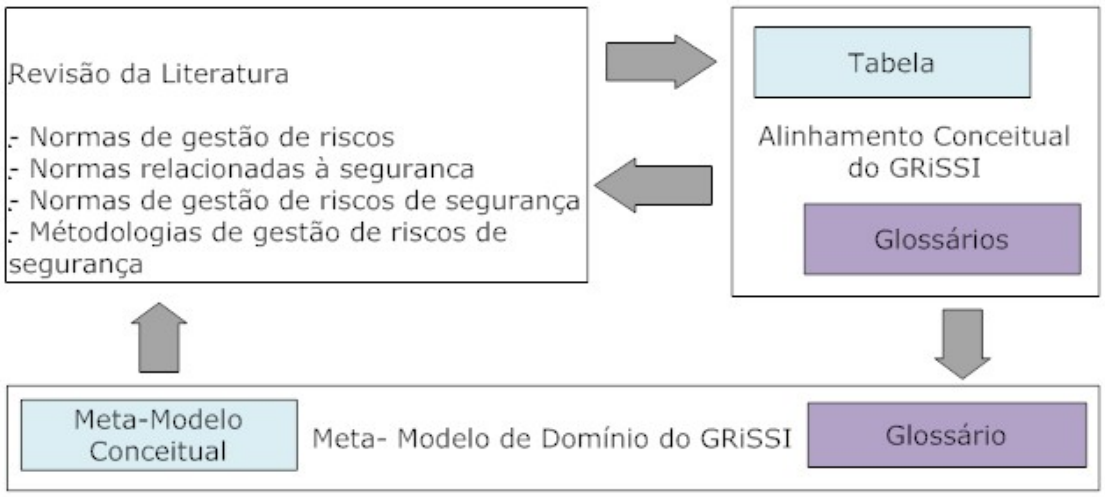

Figura 4.1: Abordagem utilizada para a definição do modelo conceitual GRiSSI

normas e metodologias de gestão de riscos e indica a existência de um sinônimo ou de uma relação de similaridade semântica, quando as normas ou metodologias utilizam termos distintos;

- *Glossários de termos:* possui termos disponíveis na literatura classificados conforme a fonte analisada. Este passo está baseado na revisão de literatura presente no capítulo 2, a qual inclui as normas de gestão de riscos, normas de segurança, normas de gestão e maturidade de riscos de segurança e metodologias de gestão de riscos de segurança.

Em cada referência utilizada, somente partes das sentenças são selecionadas levando em consideração a seleção do aspecto semântico e/ou não-redundante dos elementos. Posteriormente, as relações entre os conceitos são identificadas.

2. Construção do modelo conceitual GRiSSI: baseado nos resultados obtidos no passo 1, é construído o modelo conceitual GRiSSI. Sua representação é dada em um diagrama de classes UML que será apresentado na seção 4.3.5.

Para a construção do modelo conceitual, será primeiramente definida uma denominação para o conceito identificado. Após, uma definição é dada para cada conceito no glossário em paralelo. A última etapa é a definição das relações entre os conceitos derivados a partir da literatura. Caso ocorra a necessidade de inserção de um novo

conceito, o processo é reiniciado a partir da revisão da literatura.

4.2 A Importância da Modelagem Conceitual

Os modelos de informação expressam soluções dadas pelos especialistas para problemas de negócios. Da mesma forma, estes modelos servem de referência para que indivíduos não especialistas no domínio do problema agreguem conhecimento sobre as diferentes interpretações do mesmo problema. O conjunto de modelos de informação disponível pelos especialistas, está representado na Figura 4.2, e pode ser:

- Transformado em linguagens que podem ser compreendidas pelo conjunto de usuários em potencial (estes usuários são membros da organização, os quais agem como participantes no processo interno do negócio ou desenvolvedores de tecnologia da informação que atuam como provedores de SI);
- Mantido, pela redução da complexidade dos modelos; ou
- Mantido, através da manutenção da complexidade original.

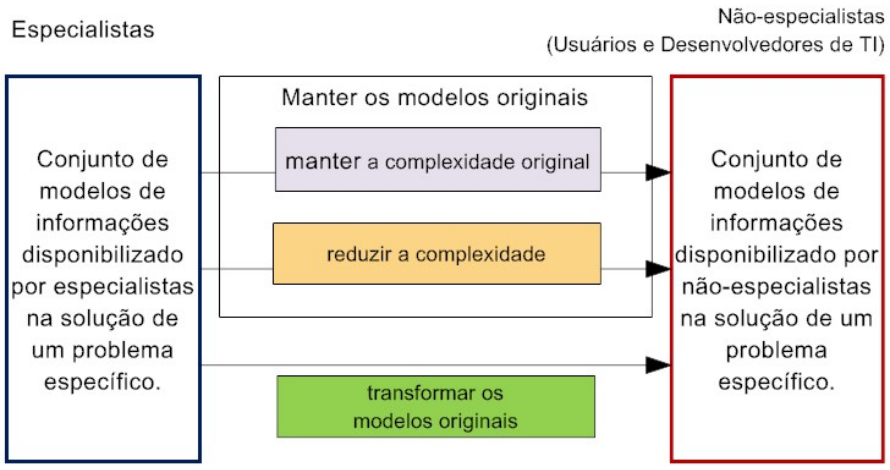

Figura 4.2: Modelo de informação para os negócios e para usuários de tecnologias da informação

Na Figura 4.2 podem ser observadas algumas implicações, as quais permanecem na utilização ou na criação de novos modelos:

- Para cada vocabulário especializado dentro da organização, um conjunto de modelos de informação necessita ser definido. Para realizar esta definição, um especialista ou membro da organização deve realizar as definições e conversões manualmente ou definir regras de forma que as definições possam ser executadas automaticamente. Considerando que existe grande quantidade de papéis e linguagens que fazem uso de vocabulários especializados dentro das organizações, pode haver um número grande de definições executadas de maneira inapropriada. Além disso, a definição só é efetiva se a linguagem de destino, na qual o conjunto de modelos de informação deve estar disponível, tem pelo menos o mesmo poder de expressão da linguagem origem. Caso contrário, algumas construções não podem ser realizadas;

- A complexidade do conjunto original dos modelos de informação deve representar todos os aspectos que o conjunto de usuários necessita para resolver um problema. Uma vez que os modelos de informação disponíveis aos usuários são os modelos originais de complexidade reduzida, as linguagens nas quais os modelos origem e destino são modelados compartilham da mesma complexidade;

- Considerando que os modelos originais permanecem inalterados, os usuários constituem uma comunidade a cerca da linguagem de modelagem. Os modelos usados nesta abordagem devem preservar detalhes técnicos e organizacionais. Os especialistas fornecem modelos de informação como uma solução para um problema de negócios particular que podem abstrair detalhes e focar no problema.

As vantagens como a redução de complexidade da modelagem para o especialista, facilidade de interpretação dos modelos ou a inclusão dos usuários na solução do problema acabam naturalmente tendo um custo adicional. Dependendo dos indivíduos envolvidos, a representação do problema de negócio pode ser mais ou menos apropriada e influenciar nas capacidades de interpretação e solução dos problemas pelos indivíduos. Porém, em

razão dos problemas potenciais no sentido de disponibilizar modelos de informação que contenham uma solução para o problema a partir da perspectiva do especialista para o usuário final, observa-se que a modelagem conceitual é a melhor escolha para reduzir a lacuna existente entre especialistas e não-especialistas.

Para modelar a solução do problema em um nível conceitual, de forma que o resultado possa ser usado por todos os membros da organização, a técnica de modelagem conceitual empregada deve possuir algumas características (BARBIERE, 1994):

- Deve abstrair os detalhes técnicos e organizacionais;
- A linguagem empregada pela modelagem conceitual deve ser facilmente compreendida;
- Deve ser formal o suficiente para evitar falsas interpretações quando os usuários aplicam modelos conceituais criados com esta técnica;
- Deve possuir mecanismos de transformação, os quais permitem a utilização de modelos conceituais consistentes.

4.3 O Alinhamento de Conceitos no Domínio da Gestão de Riscos de Segurança de Sistemas de Informação

4.3.1 Reduzindo o universo de conceitos

A primeira etapa do alinhamento de conceitos é a definição de um subconjunto de conceitos que devem levados em consideração. O principal conceito considerado é o risco, o qual será analisado em profundidade. Entretanto, deve-se considerar que os riscos dependem das necessidades de segurança associadas aos ativos e do tratamento de riscos selecionado. Desta maneira, estes conceitos são inseridos no subconjunto de conceitos em questão. O conjunto final de conceitos será tabelado ao término desta etapa. Entretanto, a quantidade de conceitos pode ser ampliada ou reduzida conforme as necessidades específicas para a elaboração do modelo conceitual GRiSSI.

4.3.2 A análise de conceitos em torno do risco

Esta seção considera a análise do conceito de risco conforme as fontes consultadas durante a revisão bibliográfica realizada no capítulo 2. O foco principal está na definição do risco e na identificação dos componentes a ele associados. Em termos da modelagem conceitual, representada sob a forma de diagramas de classes UML, o objetivo desta análise é identificar os objetos e classes do modelo conceitual GRiSSI. A identificação das métricas se tornarão propriedades ou atributos destes objetos, sendo estas apresentadas no capítulo 5.

4.3.2.1 O risco no contexto das normas de gestão

Além de algumas aplicações da gestão de riscos em alguns setores específicos, existe um guia de terminologia de gestão de riscos, adotado como guia brasileiro. Ele é chamado de ISO/IEC *Guide* 73 - Gestão de riscos - Vocabulário.

De acordo com a ISO/IEC *Guide* 73, reduzir um risco significa aplicar um controle de segurança para que a probabilidade e/ou a consequência do evento sejam reduzidas. Tanto na norma ISO 31000 quanto na ISO *Guide* 73:2009, tem-se as seguintes definições:

- **Gestão de riscos:** atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco;
- **Estrutura da gestão de riscos:** conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização.

A ISO/IEC *Guide* 73 define o risco como uma combinação da probabilidade[1] de um evento e sua consequência (ABNT ISO/IEC *Guide* 73, 2002).

[1]Tanto na ISO 31000:2009 como na ISO/IEC *Guide* 73, o termo probabilidade é definido da seguinte maneira: Uma probabilidade *(likelihood)* é a chance de algo acontecer. Na terminologia de gestão de riscos, a palavra probabilidade é utilizada para referir-se à chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita

O texto original da ISO 31000 fundamenta-se na norma AS/NZS 4360. Na norma AS/NZS 4360, riscos são definidos como a chance que algo aconteça e que promova um impacto nos objetivos do negócio. Assim, o risco é frequentemente especificado em termos de um evento ou circunstância e das consequências que podem surgir (BORNMAN (2004) *apud* AS/NZS 4360, 1999). Observa-se que tanto para a ISO 31000, ISO/IEC *Guide* 73 e para a AS/NZS 4360 o risco é composto de dois elementos relacionados: a causa, chamada de evento ou algo que poderá acontecer, e a consequência, chamada de impacto.

4.3.2.2 O risco no contexto das normas de segurança

A ISO/IEC 13335 define o risco no glossário de termos e envolve três conceitos. Dessa maneira, o risco é definido como o potencial que uma dada ameaça possui para explorar as vulnerabilidades de um ativo ou de um conjunto de ativos e, desta forma, causar um dano para a organização (ISO/IEC 13335-2, 1997). A análise desta definição mostra que a mesma está em acordo com as normas de gestão de riscos, uma vez que o risco é composto por uma causa e uma consequência. Independente da definição, apresentada, novos conceitos são empregados:

- Ativo: algo que tem valor para a organização (ISO/IEC 13335, 2004). O ativo pode ser representado por uma informação, processo, produto, base de dados, *software*, *hardware*, etc. Assim, a organização acredita que o seu valor justifica as medidas de segurança para a sua proteção, uma vez que a sua modificação, ausência ou revelação para terceiros podem gerar prejuízos, desde perdas financeiras ou de

utilizando-se termos gerais ou matemáticos (tal como uma probabilidade ou uma frequência durante um determinado período de tempo). O termo *likelihood*, em inglês, não têm um equivalente direto em algumas línguas, em vez disso, o equivalente do termo *probability* é frequentemente utilizado. Entretanto, *probability* é muitas vezes interpretado como uma expressão matemática. Portanto, na terminologia de gestão de riscos, *likelihood* é utilizado com a mesma ampla interpretação que o termo *probability*. Outra definição de probabilidade só aparece na ISO *Guide* 73:2009 como: Probabilidade *(probability)* é medida da chance de ocorrência expressa como um número entre 0 e 1, onde 0 é a impossibilidade e 1 é a certeza absoluta.

produtividade como também a respeito da reputação da organização, entre outras;

- Ameaça: é entendida como a causa potencial de um incidente que poderá resultar em danos para um sistema ou organização (ISO/IEC 13355, 2004). Uma ameaça jamais poderá ser completamente eliminada de um sistema ou organização, embora a mesma possa ter sua potencialidade e probabilidade de ocorrência reduzida com relação aos ataques e impactos (STONEBURNER, GOGUEN e FERINGA, 2002);
- Vulnerabilidade: interpretada como uma fraqueza de um ativo ou conjunto de ativos que poderá ser explorada por uma ou mais ameaças (ISO/IEC 13335,2004);
- Impacto: é o resultado de um incidente de segurança da informação (ISO/IEC 13335,2004).

A Figura 4.3 retrata um modelo de segurança da informação conforme os conceitos presentes na ISO/IEC 13335.

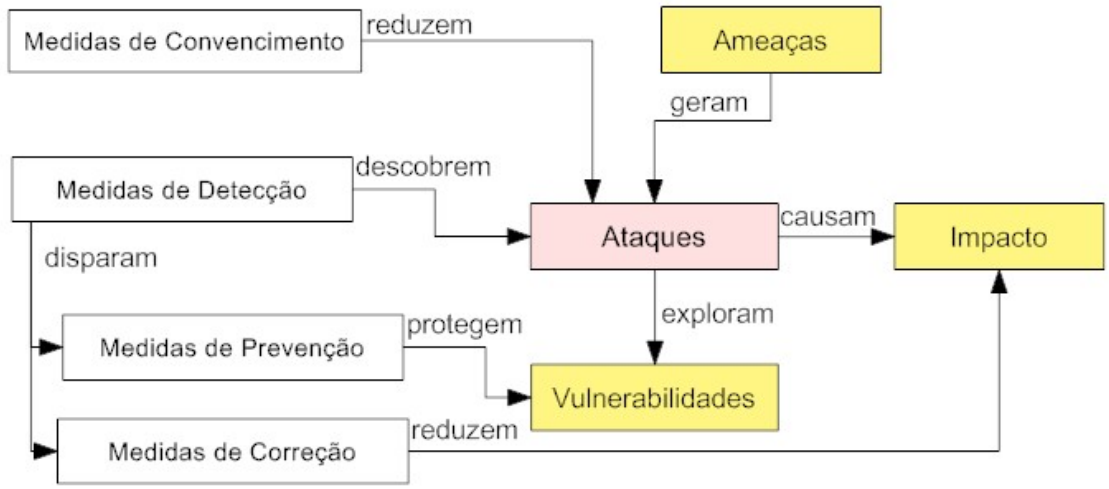

Figura 4.3: Modelo para a segurança da informação conforme os conceitos da norma ISO/IEC 13335

Neste modelo observa-se a importância dada as ameaças que geram ataques. O uso do conceito de risco no contexto das normas de segurança mostra que a sua definição é

mais precisa do que a proposta pelas normas de gestão. O risco conforme as normas de segurança é a especialização no contexto da segurança do risco.

4.3.2.3 O risco inserido nas normas de gestão e maturidade

Conforme a ISO/IEC 27001:2006, o conceito de risco não está presente no glossário. O conceito aparece em um extrato da norma onde se observa:

- Identificação dos ativos dentro do escopo de um sistema de gestão de segurança da informação e os proprietários destes ativos;
- Identificação dos tipos de ativos;
- Identificação dos tipos e das ameaças impostas sobre estes ativos;
- Identificação das vulnerabilidades sob os ativos que podem ser exploradas pelas ameaças;
- Identificação dos impactos que geram a perda de confiabilidade, integridade e disponibilidade sobre estes ativos.

A ISO/IEC 27005:2008 contém a definição de risco no glossário, a qual é dada pela capacidade que uma dada ameaça possui para explorar as vulnerabilidades de um ativo ou de um conjunto de ativos e, desta forma, provocar um dano para a organização. No Guia SOMAP[2] que contempla as definições da ISO/IEC 27001:2006 e ISO/IEC 27005 cada ativo ainda possui um tipo no qual são subdivididas as categorias dos ativos.

A NIST SP 800-30 propõe a definição para o risco como sendo o impacto do negócio na rede, considerando a semelhança que uma fonte de ameaça particular tem para explorar ou atingir uma vulnerabilidade do sistema e o impacto resultante de que isso venha a ocorrer (STONEBURNER, GOGUEN e FERINGA, 2002). Em termos dos conceitos

[2]O Guia SOMAP está disponível em http://www.somap.org/sobf/default.html e possui definições das ISO/IEC 27001:2006, ISO/IEC 27005 e ISO 7498-2.

envolvidos, o risco é novamente definido com a ajuda de três terminologias que são a ameaça, a vulnerabilidade e o impacto. O conceito de ameaça é definido como a combinação da ameaça, da sua motivação e das suas medidas de proteção.

A norma ISO/IEC 21827:2008 (SSE-CMM) considera que a engenharia de segurança envolve três pilares: Risco, Engenharia e Garantia. No nível mais simples, o processo de risco identifica e prioriza perigos inerentes ao sistema ou produto desenvolvido. O processo de engenharia de segurança trabalha com outras disciplinas de engenharia, para determinar e implementar soluções aos problemas apresentados (SSE-CMM, 2003). O processo de garantia estabelece confiança nas soluções de segurança e transmite essa confiança aos clientes. Esses três fatores trabalham juntos para assegurar que os resultados do processo da engenharia de segurança atinjam seus objetivos.

Riscos são reduzidos através do desenvolvimento de medidas de proteção que podem lidar com a ameaça, com a vulnerabilidade, com o impacto ou com o risco. Contudo, não é possível reduzir todos os riscos ou mitigar completamente qualquer risco em particular. Isto se deve principalmente ao custo da redução do risco e às incertezas associadas. Algum risco residual deve ser sempre aceito. Em situações de alta incerteza, a aceitação do risco torna-se muito problemática devido a essa incerteza. As áreas de processo do SSE-CMM incluem atividades que garantem que a organização analise ameaças, vulnerabilidades, impactos e os riscos associados (SSE-CMM, 2003).

Assim como as normas de segurança, as normas de gestão de segurança ampliam a precisão dos componentes do risco. A consequência disso, é que o risco somente se difere em termos dos nomes associados tais como impacto ou consequência, porém, a semântica permanece a mesma. Por outro lado a causa do risco é apresentada através de um conjunto de elementos, os quais diferem entre suas origens. O conceito de ativo é frequentemente mencionado na definição de riscos de normas de segurança. Porém, ele é também associado com a ameaça, com as vulnerabilidades e também com o impacto. O conceito de ativo é muito importante na definição dos riscos e, portanto, deve ser

relacionado a ele.

4.3.2.4 O risco através das metodologias de gestão de riscos de segurança

O COSO é formado por cinco componentes, sendo um deles a avaliação de riscos (COSO, 2004). Esta avaliação é realizada para a identificação e a análise de riscos relevantes para atingir os objetivos formais da entidade que são bases para a determinação das atividades de controle de segurança. A definição de riscos no contexto do COSO é dada como a probabilidade de perda ou incerteza associada ao cumprimento de um objetivo. Para cada objetivo proposto deve ser feito um processo de identificação dos riscos. Uma vez identificados, estes riscos devem ser avaliados conforme a probabilidade de ocorrência e de impacto nas atividades da organização.

A metodologia OCTAVE menciona que o risco é uma situação onde uma pessoa pode fazer algo indesejado ou uma ocorrência natural que pode causar um resultado improvável ou inesperado, resultando em um impacto ou em uma consequência negativa (ALBERTS e DOROFEE, 2001). No OCTAVE, o risco é novamente construído sobre os ativos, ameaças e vulnerabilidades.

No modelo CRAMM, o risco é dado pela semelhança que uma vulnerabilidade inerente do sistema é explorada pelas ameaças (INSIGHT CONSULTING, 2005). Na Figura 4.4 é apresentada a representação do risco no modelo CRAMM.

É importante mencionar que as metodologias de gestão de riscos de segurança como o COSO, OCTAVE e CRAMM utilizam três componentes para definir o risco. A metodologia CRAMM cita o conceito de ataque relacionado ao risco que por sua vez, não está inserido no contexto da gestão de riscos de maneira potencial.

Dentro das metodologias de gestão de riscos de segurança, o conceito de risco é novamente diverso. Os métodos destacam o que foi apresentado pelas normas de gestão de riscos que identificam a causa e a consequência do risco. Com os novos elementos obtidos a partir dos métodos de gestão de riscos e normas de segurança relacionadas,

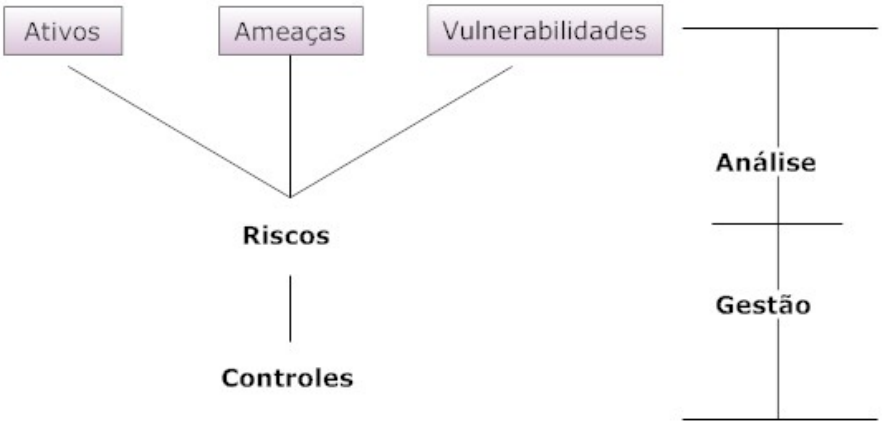

Figura 4.4: Representação do risco no modelo CRAMM.

pode-se observar que a causa do risco é formada por dois elementos que são a ameaça e a vulnerabilidade.

4.3.3 Tabelas de alinhamento de conceitos para o GRiSSI

Após a análise das definições para os conceitos relacionados à gestão de riscos de segurança de SI (GRiSSI), são construídas tabelas para o alinhamento de conceitos. Baseado na definição dos conceitos, os mesmos são analisados semanticamente e alinhados uns com os outros. Esta seção considera as tabelas de alinhamento para os conceitos distintos relacionados ao GRiSSI.

4.3.3.1 Tabela de alinhamento para as normas de gestão de riscos

As normas de gestão de riscos não inserem o conceito de ativo. Somente o critério do risco é introduzido para expressar como a importância do risco é avaliada. Conforme mencionado na seção anterior, o risco é formado por um evento (causa) e uma consequência. A causa do risco é também identificada por fonte ou perigo. Posteriormente, dois níveis para o tratamento de riscos são propostos: como tratar o risco e quais as medidas de controle que devem ser aplicadas. A tabela 4.1 apresenta o alinhamento de conceitos para as normas de gestão de riscos.

Tabela 4.1: Alinhamento para as normas de gestão de riscos

Tipo	**ISO/IEC *Guide* 73**	**AS/NZS 4360**
Conceitos Relacionados ao Risco	Critério de Risco	Critério de Risco
	Risco	Risco
	Evento	Evento
	Consequência	Consequência
		Perda
		Dano
	Fonte	Perigo
Conceitos Relacionados ao Tratamento dos Riscos	Medidas de Tratamento de Riscos Decisões sobre a Gestão de Riscos	Medidas de Tratamento de Riscos
	Controle de Riscos	Controle

4.3.3.2 Tabela de alinhamento para as normas de segurança

Primeiramente, o conceito de ativo é introduzido o contexto destas normas. Logo após, novos conceitos são introduzidos tais como vulnerabilidade ou agente da ameaça. Também surge o conceito valor de uma interpretação da ISO/IEC 13335 e da ISO/IEC 15408.

4.3.3.3 Tabela de alinhamento para as normas de gestão e maturidade de riscos de segurança

Os conceitos utilizados nas normas de gestão de riscos de segurança são mais bem definidos e mais completos quando baseados nas normas de segurança. Na norma ISO/IEC 27001:2006 e ISO/IEC 27005, o conceito geral de ativo é dividido em dois tipos: um relacionado ao negócio da organização e a informação ou processo e o outro relacionado com os componentes do SI que suportam a atividade dos negócios (SOMAP, 2008). Nota-se ainda a existência de uma causa e de uma consequência defindas por essas normas. Entretanto, a causa é composta pela ameaça e pela vulnerabilidade. Em alguns casos, a ameaça é definida pela diferenciação entre as fontes de ameaças e as

Tabela 4.2: Alinhamento para as normas de segurança

Tipo	**ISO/IEC 13335 (GMITS)**	**ISO/IEC 15408 (*Common Criteria*)**
Conceitos Baseados em Ativos	Ativo	Ativo
	Valor	Valor
Conceitos Relacionados ao Risco	Requisitos de Segurança	
	Risco	Risco
	Evento	
	Impacto	Impacto
	Efeito	Impacto
		Ameaça
	Objetivo Malicioso	
	Vulnerabilidade	Vulnerabilidade
	Agente da Ameaça	Agente da Ameaça
	Ataque	
	Método de Ataque	
	Ameaça	Ação Contrária
	Política de Segurança	Medidas Política de Segurança Requisitos da Segurança
	Salvaguardas Controles	

ações que devem ser tomadas. A tabela 4.3 representa o alinhamento de conceitos para as normas de gestão e maturidade de riscos de segurança.

4.3.3.4 Tabela de alinhamento para as metodologias de gestão de riscos de segurança

Há diversos conceitos entre as metodologias quando considerados os conceitos usados na modelagem conceitual. O conceito de ativo para o COSO, OCTAVE e CRAMM é mais focado no nível da segurança da informação. O conceito de risco está presente em todos os métodos, sendo que a causa do mesmo é chamada de impacto. Em cada método, a vulnerabilidade é um sub-componente da causa do risco. O conceito de ameaça é também identificado em todos os métodos. O conceito de controle, presente em várias normas, é mantido, mas seu nome é mudado para medidas de controle, soluções de segurança, prática estratégica de proteção, etc. A tabela 4.4 mostra o alinhamento para

Tabela 4.3: Alinhamento para as normas de gestão e maturidade de riscos de segurança

Tipo	**ISO/IEC 27001:2006 ISO/IEC 27005**	**NIST SP 800-30**	**ISO/IEC 21827:2008**
Conceitos Baseados em Ativos	Ativo		Ativo
	Tipo de Ativo		
	Ativo Principal		
	Critério de Propriedade	Objetivo da Segurança	
Conceitos Relacionados ao Risco	Risco	Risco	Risco
	Evento	Ameaça	Ameaça
	Impacto	Impacto	Impacto
	Consequência	Consequência	
	Tipo de Ameaça		
	Vulnerabilidade	Vulnerabilidade	Vulnerabilidade
	Fonte da Ameaça	Fonte da Ameaça	
	Origem da Ameaça		
	Método de Ataque	Ação da Ameaça	
Conceitos Relacionados ao Tratamento dos Riscos	Tratamento de Riscos	Mitigação de Riscos	Mitigação de Riscos
	Controle	Controle	Controle
	Objetivo	Controle	Controle

as metodologias de gestão de riscos de segurança.

O alinhamento de conceitos como parte da modelagem conceitual para a gestão de riscos de segurança de SI mostrou que o domínio não é unificado. Vários termos diferentes são usados para descrever o mesmo conceito. Uma grande quantidade de nomes diferentes foi encontrada para alguns conceitos, sendo que em alguns casos, o mesmo nome era usado para identificar conceitos distintos. As tabelas apresentadas nesta seção auxiliam a interligação das diferentes fontes de informação entre si.

Tabela 4.4: Alinhamento para as metodologias de gestão de riscos de segurança

Tipo	COSO	OCTAVE	CRAMM
Conceitos Baseados em Ativos	Ativo	Ativo	
	Ativo Principal		
		Componente Principal	Ativo
		Requisitos de Segurança	Propriedade
Conceitos Relacionados ao Risco	Risco	Risco	Risco
	Causa	Domínio	
	Consequência	Impacto	Impacto
		Ameaça	Ameaça
	Vulnerabilidade	Vulnerabilidade	Vulnerabilidade
		Ator	
Conceitos Relacionados ao Tratamento dos Riscos		Plano de Mitigação de Riscos	
	Serviço de Segurança Medidas de Segurança		Medidas de Controle Objetivos de Segurança
	Solução de Segurança		Medidas de Controle

4.3.4 Relacionando conceitos no contexto da gestão de riscos de segurança de SI

Após o alinhamento de conceitos é necessária a identificação das relações entre estes. O processo é similar ao utilizado para a redução do universo de conceitos. As relações entre os conceitos são fundamentadas no texto referente à identificação dos conceitos entre outros materiais presentes na literatura.

Para ilustrar a análise dos relacionamentos, foi mostrada a definição das relações entre a ameaça e a vulnerabilidade. Porém, após uma análise de definições para o alinhamento de conceitos, pode-se observar que ambos os conceitos estão relacionados.

Nas normas de gestão de riscos, o conceito de vulnerabilidade não está presente. Não há, portanto, relação entre os conceitos analisados. No contexto das normas de segurança, os conceitos de ameaça e vulnerabilidade estão relacionados na ISO/IEC

13334. Nesta norma, a vulnerabilidade é uma fraqueza de um ativo ou conjunto de ativos que pode ser explorada por uma ou mais ameaças. Entretanto, a ameaça nesta norma não é equivalente ao conceito empregado na ISO/IEC 15408. A ISO/IEC 15408 também menciona a vulnerabilidade, porém este conceito não é claramente associado ao conceito de ameaça. A relação entre os conceitos é clara no domínio das normas de gestão e maturidade de riscos de segurança. A norma ISO/IEC 27001:2006, ISO/IEC 27005 e a ISO/IEC 21827:2008 relacionam os conceitos entre si, onde:

- As vulnerabilidades que podem ser exploradas pelas ameaças devem ser identificadas (ISO/IEC 27001:2006);
- Vulnerabilidades que podem ser exploradas pelas ameaças e podem causar um dano aos ativos ou para a organização, devem ser identificadas (ISO/IEC 27005);
- A informação do risco produzido depende da informação da ameaça, da vulnerabilidade e do impacto (SSE-CMM, 2003).

O NIST SP 800-30 descreve o risco como sendo o impacto do negócio na rede, considerando a semelhança que uma fonte de ameaça particular irá explorar ou atingir uma vulnerabilidade do sistema e o impacto resultante de que isso venha a ocorrer.

A metodologia CRAMM induz que a ameaça e vulnerabilidade são relacionadas somente pela agregação no conceito de risco. A metodologia OCTAVE propõe a definição de vulnerabilidade como uma fraqueza no SI, práticas ou procedimentos de sistemas de segurança, controles administrativos, controles internos, implementação ou estrutura física que pode ser explorada por uma ameaça para obter acesso ou interromper um serviço.

Com isso, pode-se observar que a vulnerabilidade está relacionada com os conceitos de ameaça, fonte da ameaça e método de ataque conforme o alinhamento de conceitos. Estudos mais criteriosos mostram que os conceitos fonte de ameaça e método de ataque

estão agregados na ameaça. Isso explica a razão de que todos eles podem ser relacionados com a vulnerabilidade.

4.3.5 Apresentação do modelo conceitual para a específicação da gestão de riscos de segurança de SI (GRiSSI)

Conforme apresentado na seção 4.3.4, o resultado da primeira etapa produziu o alinhamento de conceitos para a gestão de riscos de segurança de sistemas de informação e suas respectivas relações. A segunda etapa pretende construir um modelo conceitual de especificação para a gestão de riscos de SI. Este modelo conceitual, representado sob a forma de um diagrama de classes em UML, é composto de conceitos identificados e apresentados pela tabela de alinhamento de conceitos resultante (ver tabela 4.5). Para cada conceito, um nome é escolhido em conformidade com a literatura utilizada nesta dissertação. Um glossário é disponibilizado com o modelo conceitual, permitindo a existência de uma definição para cada conceito presente na modelagem conceitual. Posteriormente, os conceitos são interligados conforme suas respectivas relações.

4.3.5.1 Nomenclatura utilizada

Os resultados obtidos no alinhamento de conceitos é a primeira fonte a ser utilizada. Logo após, o número de ocorrências do nome do conceito em diferentes fontes obtidas na literatura é levado em consideração. Posteriormente, a terminologia utilizada na família da norma ISO/IEC 27000 é considerada, uma vez que a mesma possui um vocabulário controlado. Nesta seção os conceitos são ordenados e relacionados uns aos outros na forma de um diagrama de classes em UML.

Tabela 4.5: Nome dos conceitos para o modelo conceitual GRiSSI

Tipo	**Nome**
Conceitos baseados em ativos	Ativo
	Tipo de Ativo
	Ativo de Negócio

continua na próxima página

Tabela 4.5: Nome dos conceitos para o modelo conceitual GRiSSI (continuação)

Tipo	Nome
	Ativo de Segurança da Informação Valor Critério de Segurança
Conceitos relacionados ao risco	Risco Evento Impacto Ameaça Tipo de Ameaça Vulnerabilidade Efeito Agente da Ameaça Objetivo malicioso Ataque Método de Ataque
Conceitos relacionados ao tratamento de riscos	Controle Tratamento de Riscos Requisitos de Segurança Política de Segurança

4.3.6 A definição dos conceitos

Para classificar esses conceitos foram feitas três divisões. A primeira divisão trata dos conceitos baseados em ativos, a segunda, dos conceitos relacionados ao risco e a terceira dos conceitos relacionados ao tratamento dos riscos. A Figura 4.5 apresenta a divisão de conceitos no contexto da gestão de riscos.

4.3.6.1 Conceitos baseados em ativos

Conceitos baseados em ativos descrevem quais os ativos que são importantes e merecem a proteção e quais os critérios que garantem a segurança do ativo.Ele é representado e referenciado pelas normas e metodologias de gestão de riscos de forma abrangente, dependendo do contexto organizacional onde está inserido.

Ativo

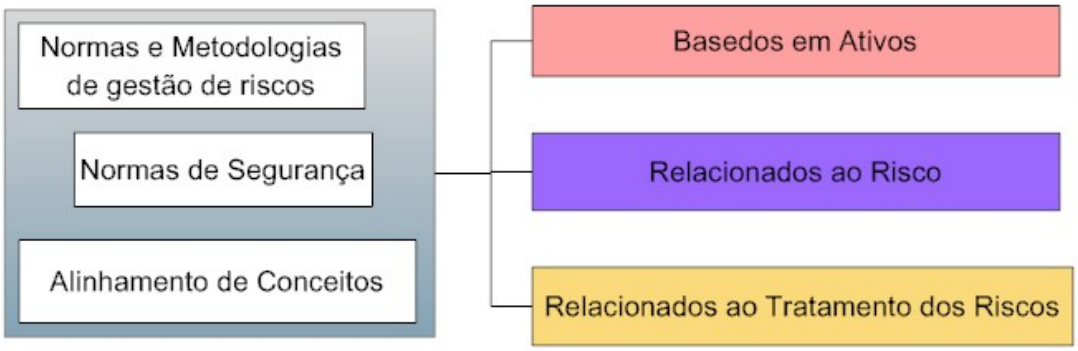

Figura 4.5: Organização dos conceitos no contexto da gestão de riscos

A literatura define ativo como:

- Qualquer coisa que tenha valor para a organização. ISO/IEC 13335-1:2004 e ISO/IEC 27001:2006 (ISO/IEC 27001, 2006);
- Um ativo pode ser definido como alguma coisa de valor para as organizações. OCTAVE (ALBERTS e DOROFFE, 2003);
- Entidade na qual o proprietário do objetivo da avaliação presume um valor sobre ele. *Common Criteria* citado em versão do *Common Criteria* para a avaliação da tecnologia da informação (COMMON CRITERIA, 2003);
- Alguma coisa que tem valor para a organização. ISO/IEC 27002:2009 (ISO/IEC 27002, 2009).

Algumas normas e metodologias de gestão de riscos não conceituam o termo ativo ou não definem a referência que é utilizada. Entre elas podem ser citadas: ISO/IEC 31000:2008, ISO/IEC *Guide* 73, ISO/IEC 21827:2008 (SSE-CMM), entre outras.

Tipo de Ativo

O tipo de ativo é usado para agrupar ativos em grupos lógicos de ativos similares (Guia SOMAP contemplando as normas ISO/IEC 27001:2006 e ISO/IEC 27005).

Ativo de Negócios

As referências sobre o ativo de negócios informam que o mesmo pode ser um processo ou habilidade inerente ao negócio da organização, o qual possui um valor para a organização em termos do modelo de negócios empregado e que é necessário para a obtenção dos objetivos. Exemplos de ativos de negócios podem ser plantas técnicas, processos de cálculos, *softwares* de planejamento, etc.

Ativo de Segurança da Informação

É considerado como um componente ou parte de um SI que possui valor para a organização e é necessário para a obtenção dos objetivos e recursos necessários da organização. Um ativo de segurança da informação pode ser um componente de um SI tal como um *software*, *hardware* ou uma infra-estrutura de rede como também recursos humanos. Exemplos deste ativo podem ser sistemas operacionais, redes de computadores, o administrador do sistema, etc.

Critério de Segurança

É uma propriedade ou restrição sobre os ativos do negócio, caracterizando suas necessidades de segurança. O critério de segurança atua como um indicador para avaliar a importância do risco. Critérios de segurança são, na maioria das vezes, descritos pela confidencialidade, integridade e disponibilidade. Porém, em alguns casos e dependendo do contexto, algum critério específico pode ser usado como a autenticidade.

Valor

Uma organização atribui valores aos ativos que requerem proteção. Um ativo tem um valor associado a cada parte interessada. O valor patrimonial é medido em termos de importância para o negócio. Os valores são normalmente expressados em termos de impactos potenciais ao negócio.

O diagrama de classes dos conceitos baseados em ativos é apresentado na Figura 4.6.

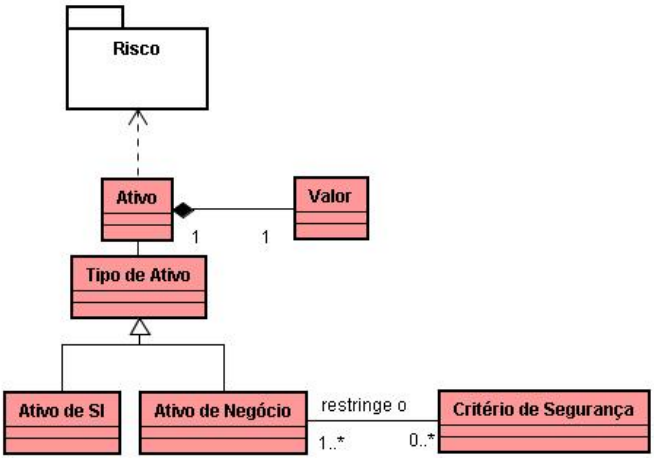

Figura 4.6: Diagrama de classes dos conceitos baseados em ativos

4.3.6.2 Conceitos relacionados ao risco

O risco tem várias definições dependendo do contexto onde está inserido (BORNMAN, 2004). A definição do risco e dos elementos que contribuem para a mitigação e gestão de riscos é dada de diversas maneiras.

Risco

Conforme a literatura, o risco pode ser definido por:

- Uma combinação da probabilidade de um acontecimento e das suas consequências. ISO/IEC *Guide* 73 (COELHO (2002) *apud* FREDRIKSEN, 2002);
- Risco é a mudança de algum fato que terá um impacto sobre os objetivos do negócio. AS/NZS 4360 (BORNMAN, 2004);
- Risco é o potencial de uma dada ameaça explorar vulnerabilidades de um ativo ou grupo de ativos para causar perdas ou danos a um ativo. ISO/IEC 13335 - GMITS (ISO/IEC TR 13335-2, 1998);
- Risco é o efeito da incerteza sobre os objetivos[3]. ISO 31000 *Risk Management*

[3]Um efeito é um desvio do esperado - positivo e/ou negativo. Objetivos podem ter diferentes aspectos

(ISO/TMB/WG *Risk management*, 2008) ISO/IEC *Guide* 73 e ISO 31000 *Risk Management* (ISO/TMB WG *on Risk management*, 2008).

Impacto

O impacto é o resultado ou efeito de um evento. Pode haver um intervalo de possíveis impactos associados a um evento. O impacto de um evento pode ser positivo ou negativo relativo aos objetivos relacionados às entidades. COSO (Risk Solutions, 2007).

Outra definição presente na literatura é uma alteração adversa do nível atingido dos objetivos do negócio (ISO/IEC 27001, 2006). Exemplos de impactos são vazamento de senhas, perda de confidencialidade sobre uma dado ou processo, etc.

Evento

A literatura descreve o evento como:

- Uma ocorrência ou mudança de um conjunto particular de circunstâncias. ISO/IEC *Guide* 73 , ISO 31000 Risk Management e ISO/IEC 27000:2009 (ISO/TMB/WG RISK MANAGEMENT(2008); ISO/IEC 27001 (2006));

- A ocorrência de um conjunto particular de circunstâncias[4]. ISO/IEC Guide 73:2002 (ISO/TMB/WG *Risk management*, 2008);

- Um incidente ou ocorrência de fonte interna ou externa que afeta a concretização dos objetivos[5](COSO (Risk Solutions, 2007)).

Vulnerabilidade

tais como financeiros, de saúde e segurança e objetivos do ambientes que podem ser aplicados a diferentes níveis tais como estratégico, toda a organização, projeto, produto e processos. O risco é frequentemente caracterizado por referência para eventos potenciais, consequências ou a combinação destes e como eles podem afetar a realização dos objetivos. Risco é frequentemente expressado em termos de uma combinação de consequências de um evento ou uma mudança nas circunstâncias, associadas à probabilidade de ocorrência.

[4]O evento pode ser certo ou incerto. O evento pode ser uma ocorrência única ou uma série de ocorrências. A probabilidade associada com um evento que pode ser estimado em um período de tempo (Risk Solutions, 2007)

[5]Eventos podem ter impactos negativos, positivos ou ambos. Eventos com impactos negativos representam riscos.

A vulnerabilidade é um conceito central, definido na literatura por:

- Uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. ISO/IEC 13335-1:2004 - GMITS (ISO/TMB/WG RISK MANAGEMENT, 2008);
- Uma fraqueza nos próprios procedimentos humanos. OCTAVE, AS/NZS 4360 (COELHO (2007) *apud* ALBERTS (2001));
- Uma propriedade intrínseca de alguma coisa que cria susceptibilidade para uma fonte de risco que pode levar a uma consequência. ISO 31000 (ISO/TMB/WG *Risk management*, 2008) ISO/IEC *Guide* 73 e ISO 31000 *Risk Management* (ISO/TMB/WG *Risk management*, 2008);
- Uma fraqueza de um ativo ou controle que pode ser explorada por uma ameaça. ISO/IEC 27000:2009 (ISO/IEC 27000, 2009).

Efeito

O efeito é caracterizado pelo atributo gravidade que especifíca a criticidade dos efeitos provocados por vulnerabilidades. Uma ação maliciosa pode explorar um número de vulnerabilidades as quais podem ter efeitos (negativos) sobre os elementos afetados.

Ameaça

A literatura define a ameaça por:

- Uma representação de uma causa potencial de perda de um ativo de valor. CORAS (BORNMAN, 2004);
- O potencial de causar um incidente indesejado que pode resultar em danos a um sistema ou a uma organização. ISO/IEC 27000:2009 (ISO/IEC 27000, 2009).

Uma ameaça é geralmente composta pelo binômio: agente da ameaça e método de ataque.

Tipo de Ameaça

Ameaças podem ser classificadas (acidental, intencional) e agrupadas (ativa, passiva).

Agente da Ameaça

É um agente que pode causar dano aos ativos de um SI. Um agente da ameaça dispara a ameaça e, desta forma, é considerado a fonte do risco. Exemplos de agentes são membros da organização com reduzida habilidade técnica, porém com uma motivação muito forte para executar o ataque.

Objetivo Malicioso

Os objetivos maliciosos são motivações dos atacantes, considerados necessários para os analistas avaliem o risco de um ataque.

Ataque

Um ataque é um conjunto de ações intencionais indevida (maliciosas) projetadas para comprometer a confidencialidade, integridade, disponibilidade ou qualquer outra característica desejada de um sistema de TI.

Método de Ataque

É o método padrão pelo qual o agente da ameaça executa a ameaça propriamente dita. Exemplos de métodos são intrusão, roubo de mídias ou documentos. O diagrama de classes dos conceitos relacionados ao risco é apresentado na Figura 4.7.

4.3.6.3 Conceitos relacionados ao tratamento dos riscos

Tratamento de Riscos

A definição de tratamento de riscos na literatura é dada por:

- Um processo de seleção e aplicação de medidas destinadas a modificar o risco[6]. AS/NZS 4360:1999 (Risk Solutions, 2007);

[6]O termo tratamento de risco é utilizado para medidas próprias. As medidas de tratamento de risco incluem evitar, modificar, dividir ou reter o risco.

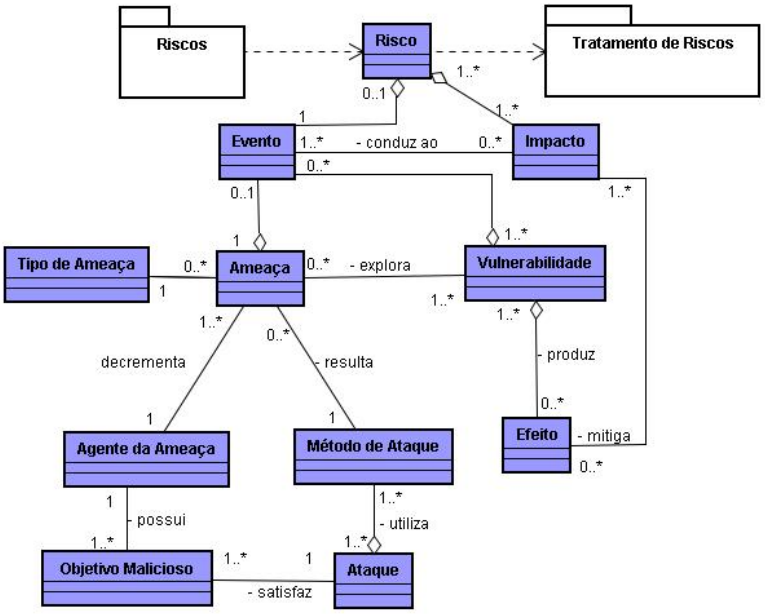

Figura 4.7: Diagrama de classes dos conceitos relacionados ao risco

- Um processo de seleção e implementação e medidas para modificar o risco[7]. ISO/IEC Guide 73:2002 (Risk Solutions, 2007);

- Um processo de desenvolvimento e implementação de medidas para modificar o risco[8]. ISO/IEC 13335-1:2004 - GMITS (ISO/TMB/WG *Risk management*, 2007);

- Uma seleção de uma ou mais opções para o endereçamento de riscos e implementação dessas opções. ISO 31000 *Risk Management* (ISO/TMB/WG *Risk management*, 2008).

Onde pode-se:

[7]O termo tratamento de risco é utilizado para medidas próprias. As medidas de tratamento de risco incluem evitar, otimizar, transferir e reter o risco.

[8]As medidas de tratamento do risco devem incluir: Evitar o risco pela decisão de não dar início ou prosseguir com a atividade que dá origem ao risco; Procurar uma oportunidade para tomar a decisão de iniciar ou prosseguir com uma atividade susceptível de criar ou manter o risco; Alterar a probabilidade do risco; Alterar as consequências; Dividir o risco com outra parte ou partes; e Manter o risco seja por opção ou por omissão.

- Evitar o risco: decidir não tratar o risco. Funcionalidades de um SI são modificadas ou descartadas;
- Reduzir o risco: ação para reduzir a probabilidade, consequências negativas ou ambas, as quais estão associadas ao risco. Requisitos de segurança devem ser selecionados para reduzir o risco;
- Transferir o risco: compartilhar o risco com outro parceiro;
- Reter o risco: aceitar a responsabilidade da perda a partir de um risco.

Requisitos de Segurança

É uma condição sobre um fenômeno do ambiente que queremos criar através de um SI, no sentido de mitigar os riscos. Exemplos são o uso de métodos apropriados de autenticação e identificação que devem ser usados para controlar o acesso de usuários remotos, etc.

Política de Segurança

Uma política de segurança descreve as regras, diretrizes e práticas que regem a forma como os ativos são gerenciados, protegidos e distribuídos dentro de uma organização e em seus SI. As políticas de segurança constituem requisitos de segurança em cima de um alvo de avaliação. Estes requisitos são projetados para proteger o valor dos ativos.

Controle

O controle pode ser entendido como um conjunto de medidas para modificar o risco. O controle do risco pode ser resultado do tratamento de risco, incluindo alguns processos, dispositivos, práticas ou outras ações destinadas a minimizar os riscos. ISO/IEC 13335-1:2004 - GMITS (ISO/TMB/WG *Risk management*, 2007).

O diagrama de classes dos conceitos relacionados ao tratamento dos riscos é apresentado na Figura 4.8.

O modelo conceitual de gestão de riscos de segurança de SI (GRiSSI) inicial é representado através da composição dos três diagramas de classes UML das figuras 4.6,

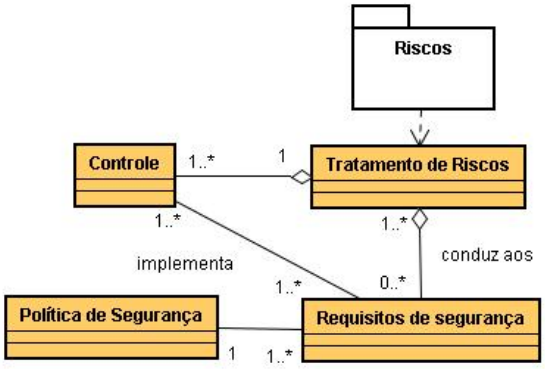

Figura 4.8: Diagrama de classes dos conceitos relacionados ao tratamento dos riscos.

4.7 e 4.8. O diagrama de classes UML da Figura 1 (ver Anexo 1) representa o modelo conceitual que mostra os conceitos e suas relações (com as propriedades) do modelo conceitual.

4.3.7 Relações do modelo conceitual para a gestão de riscos de segurança de Sistemas de Informação

Um risco pode ser causado por um evento e um ou mais impactos. O mesmo impacto pode ser proveniente de vários riscos, porém um evento identifica um risco particular conforme a Figura 1. Um dado evento conduz de zero (se nenhum impacto é identificado) a vários impactos, sendo que um impacto pode ser causado por vários eventos. Em alguns casos, um impacto relevante pode ser causado sem que ocorra um evento relevante. Um ou vários impactos podem provocar impactos indiretos. No contexto da segurança de SI, o evento é composto por uma ameaça e uma ou mais vulnerabilidades. Uma ameaça particular pode somente ser relacionada a um evento particular. Se a ameaça é identificada e não possui uma vulnerabilidade associada, a mesma não será parte do evento e nem do risco. As ameaças também são agrupadas em tipos onde um tipo pode possuir nenhuma ou várias ameaças. Uma vulnerabilidade pode ser explorada por várias ameaças o que dificulta a identificação da ameaça se relacionada com muitos eventos diferentes. As vulnerabilidades produzem nenhum ou vários efeitos (severidade) que

podem ser mitigados por meio da avaliação dos impactos.

Uma ameaça é definida em termos do agente da ameaça que possui um ou vários objetivos maliciosos para provocar um ataque conforme a Figura 1. Cada agente da ameaça pode envolver-se em várias ameaças ou em nenhuma delas, caso nenhum método de ataque relevante correspondente seja identificado. Um ataque pode satisfazer um ou vários objetivos maliciosos e pode utilizar um ou vários métodos de ataque.

Os ativos possuem um tipo e podem ser especializados de duas maneiras: ativos de negócio e ativos de segurança da informação. A vulnerabilidade é uma característica de um ativo de segurança da informação que pode possuir nenhuma ou várias vulnerabilidades. Um ativo possui um valor e uma vulnerabilidade pode afetar um ou vários valores. O impacto reduz o valor de um ativo, fornecendo a ele um novo valor.

Uma ameaça objetiva um ou mais ativos de segurança da informação, que pode ser atingido por várias ameaças. O ativo de segurança da informação, objetivado pela ameaça não é necessariamente o mesmo que o vinculado com a vulnerabilidade explorada por esta ameaça. Cada ativo de negócio pode ser restrito de zero até vários critérios de segurança. Um critério de segurança pode restringir vários ativos de negócios distintos ou nenhum deles. Os impactos podem danificar os ativos tanto no nível de ativos de segurança da informação quanto no nível do negócio. Um ativo pode ser danificado enquanto que um impacto prejudica pelo menos um ativo de segurança da informação e um ativo de negócio. Entretanto, mais de dois ativos são prejudicados por um impacto. No nível dos ativos de negócios, um impacto pode negar um ou mais critérios de segurança e um dado critério de segurança pode ser negado por nenhum ou até vários impactos. Nenhum ou muitos critérios de segurança avaliam a importância do risco. Porém um critério de segurança pode não ser afetado por nenhum risco quando não há impacto relevante para este critério.

O tratamento de riscos expressa a decisão em tratar um ou mais riscos. Cada risco identificado possui um dado tratamento e, em alguns casos, vários tratamentos podem

ser combinados. Os tratamentos de riscos levam a um ou mais requisitos de segurança. Um requisito de segurança, conforme a Figura 1, é dado por uma política de segurança. Por último, um controle implementa um ou mais requisitos de segurança e o mesmo requisito de segurança pode ser implementado por um ou mais controles.

4.4 Conclusões Parciais

O modelo conceitual GRiSSI contribui para o estabelecimento de uma terminologia padrão para o processo de gestão de riscos de segurança de SI. Como descrito no capítulo 2, há várias iniciativas dos órgãos vinculados às questões de segurança, porém este trabalho está em constante crescimento. O modelo conceitual proposto pode servir de referência para a formulação de novos modelos de segurança que estejam direcionados ao desenvolvimento dos controles da norma da família NBR ISO/IEC 27000.

Muito embora o modelo conceitual apresentado tenha sido fundamentado na literatura existente, o mesmo pode servir de base para a pesquisa de novas referências sobre a gestão de riscos. O domínio do modelo conceitual apresentado sugere a informação contextual, a qual pode ser sugerida em novas fontes. Além disso, o modelo conceitual pode evoluir quando novas fontes forem determinadas e levadas em consideração. Neste caso, as informações devem ser reorganizadas para a inserção da nova fonte.

O modelo conceitual apresentado tende a auxiliar a comunidade científica no âmbito da gestão de riscos de segurança de SI para que esta tenha um melhor entendimento do seu escopo, podendo atingir uma melhor integração com conceitos de gestão de riscos relacionados. No entanto, durante o desenvolvimento do modelo conceitual foram encontradas algumas limitações onde observou-se que:

- As fontes analisadas não são simples e não são suficientemente formalizadas, para que se faça um estudo semântico comparativo mais formal;
- Os conceitos fundamentais no âmbito da gestão de riscos podem ser formalizados através do modelo conceitual. Porém, um estudo mais aprofundado foi descartado,

pois estava além do escopo desta pesquisa.

Na construção do modelo conceitual várias técnicas estão presentes em linhas de desenvolvimento de *software*. Estas técnicas fazem parte da análise de domínio, a qual é ligada a engenharia de domínio. A análise de domínio deve especificar os elementos básicos deste domínio, organizar e compreender as relações entre seus elementos e representá-los de forma útil. Muito embora o presente trabalho não possua diretamente estas técnicas, a abordagem utilizada para a obtenção do modelo conceitual é compatível com estas técnicas. Este modelo conceitual será usado no capítulo 5 para a definição de métricas de segurança.

5 DEFININDO MÉTRICAS DE GESTÃO DE RISCOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

Grande parte das organizações vem reforçando suas políticas e procedimentos de segurança. Apesar dos vários métodos empregados, não se tem conhecimento de quão seguros os SI de uma organização podem estar. Para Aredo (2005) umas das formas de verificar o nível de segurança é por meio da utilização de métricas de segurança.

As métricas de segurança contribuem para promover melhorias e efetuar correções em processos de segurança (KOVACICH e HALIBOZEK, 2006). Com o uso das métricas de segurança as organizações podem verificar se os mecanismos de proteção estão sendo executados de forma apropriada.

Nesse sentido, este capítulo tem o objetivo de discutir a utilização de métricas de segurança aplicadas à gestão de riscos de segurança de SI e a definição de métricas de segurança para o modelo conceitual GRiSSI.

Partes deste capítulo constam no artigo "Avaliação das abordagens para a construção de métricas de segurança em sistemas de TI", publicado nos anais do XVI SIMPEP[1].

[1]O XVI SIMPEP (Simpósio de Engenharia da Produção) foi realizado no período de 09 a 11 de novembro de 2009 na cidade de Bauru -SP, com o intuito de discutir e apresentar as pesquisas desenvolvidas voltadas para Engenharia de Produção e suas ênfases. Informações sobre o evento podem ser obtidas em http://www.simpep.feb.unesp.br.

5.1 Métricas de Segurança

As métricas de segurança são aplicações de análises quantitativas, estatísticas ou matemáticas para mensuramento dos custos da segurança funcional, benefícios, sucessos, falhas, tendências e carga de trabalho (KOVACICH e HALIBOZEK, 2006).

As métricas de segurança também são diferentes formas de aferição que podem ser usadas para demonstrar o estado atual da segurança e para estabelecer quais recursos são necessários para incrementá-la (AREDO, 2005). Segundo Batista (2007) as métricas de segurança são ferramentas para que profissionais de segurança da informação avaliem os níveis de segurança de seus sistemas, produtos e processos, dando a possibilidade de tratar as questões de segurança que estão enfrentando.

Além disso, as métricas podem ser úteis para identificar vulnerabilidades em sistemas e avaliar os seus riscos, orientando para ações corretivas de maior prioridade, aumentando o nível de maturidade sobre a segurança na organização (BATISTA, 2007). As métricas podem também identificar riscos baseados em falhas ou sucessos de componentes de segurança e podem fornecer soluções para problemas de segurança (VELLANI, 2006).

5.2 Abordagens para a Definição de Métricas de Segurança

Há diferentes abordagens para a construção de métricas de segurança tais com as baseadas no modelo SSE-CMM (KORMOS et al., 1999), métricas baseadas no CVSS (PATRICIU, PRIESCU e NICOLAESCU, 2006), métricas baseadas em padrões (HEYMAN et al., 2008), métricas baseadas nas abordagens *Top-Down* e *Bottom-Up* (PAYNE, 2006) entre outras. Essas abordagens contribuem para a construção de programas de métricas de segurança e consequentemente para o aprimoramento da gestão da segurança.

5.2.1 Métricas baseadas na ISO/IEC 21827:2008 (SSE-CMM)

A construção das métricas de segurança a partir do modelo SSE-CMM estão baseadas nas PAs. As PAs estão divididas em quatro grupos:

- Design da Arquitetura (PA07, PA09, PA10);
- Avaliação da Segurança (PA02, PA03, PA04, PA05);
- Operação e manutenção (PA01, PA08);
- Convicção do cliente (PA06, PA11);

Para cada PA uma ou mais métricas podem ser definidas. A construção das métricas através do modelo SSE-CMM baseia-se em atividades e práticas de segurança que uma organização deve realizar durante o desenvolvimento de um projeto. Embora, a maioria dos projetos sejam diferentes e nem todas as PAs poderão ser aplicadas em todas as situações, essas PAs representam as melhores práticas de segurança que devem ser consideradas ao desenvolver requisitos de um sistema (PHILLIPS, 2003).

A construção das métricas baseadas no modelo SSE-CMM é indicado para programas de gerenciamento de segurança, onde os processos já estão implementados. Os processos de segurança são mensurados e avaliados resultando no diagnóstico do estado atual da segurança que pode ser aplicado por qualquer organização para a elaboração de um programa de segurança.

5.2.2 Métricas conforme o CVSS

O modelo CVSS (*Common Vulnerability Scoring System*) foi desenvolvido para proporcionar ao usuário final uma pontuação global, representando a severidade de um risco diante de uma vulnerabilidade (PATRICIU, PRIESCU e NICOLAESCU, 2006).

O CVSS é visto como um padrão de métricas para dimensionar vulnerabilidades e seus impactos em sistemas de forma mais precisa. É adotado pelo NIST (*The National Institute of Standards and Technology*) para a classificação das vulnerabilidades no NVD (*National Vulnerability Database*)[2].

[2] www.first.org/cvss/

O quadro de classificação das vulnerabilidades pode oferecer métricas operacionais utilizadas pelas grandes empresas na gestão do processo de segurança dos SI (PATRICIU, PRIESCU e NICOLAESCU, 2006). As métricas de segurança construídas através do CVSS indicam a gravidade dos riscos perante as vulnerabilidades. Com o uso das métricas e de algumas fórmulas pode-se ter um escopo total da segurança. O método para a utilização das métricas possui critérios para a caracterização das vulnerabilidades que está divido em 3 grupos de métricas:

- Métricas base;
- Métricas temporais;
- Métricas ambientais.

As métricas base possuem qualidades que são essenciais a qualquer vulnerabilidade, não se alterando ao longo do tempo ou em diferentes ambientes. As métricas temporais as aquelas que representam as características dependentes do tempo de uma vulnerabilidade e as métricas ambientais representam as características específicas da implementação e do ambiente de uma vulnerabilidade (PATRICIU, PRIESCU e NICOLAESCU, 2006).

As características de cada uma das métricas são valoradas e processadas para obter uma pontuação final ajustada que irá representar as ameaças que uma vulnerabilidade representa em um determinado instante de tempo para um ambiente específico (PATRICIU, PRIESCU e NICOLAESCU, 2006).

A contabilização é o processo de combinar todos os valores das métricas em uma função específica. A pontuação base tem o maior incidência sobre a pontuação final e representa a gravidade da vulnerabilidade. A pontuação temporal (TS) permite a introdução de fatores atenuantes para reduzir a pontuação da vulnerabilidade e está concebido para ser re-avaliado em intervalos específicos. A pontuação ambiental (ES) se ajusta combinada com a pontuação temporal e deverá ser considerada na pontuação

final para representar um ambiente específico. Organizações usuárias devem usar suas próprias respostas para priorizar ambientes.

As pontuações das métricas básicas e temporais são definidas pelos próprios fabricantes, enquanto que as métricas ambientais são definidas pelas empresas e organizações em função da sua realidade. Em função disso os dados obtidos se tornam mais consistentes e precisos.

O uso do CVSS para construção de métricas é indicado para mensurar o impacto das vulnerabilidades mediante os riscos de uma organização no processo de segurança. Essa abordagem foca em três métricas que podem ser facilmente obtidas através de fórmulas matemáticas que representam informações que contribuem para empresas como uma forma de priorizar ameaças, vulnerabilidades e riscos.

Com o crescente número de vulnerabilidades, as empresas podem usar o CVSS para classificar as vulnerabilidades de uma forma coerente e, ao mesmo tempo permitir uma personalização dentro do ambiente do usuário. O CVSS também pode auxiliar nas atividades de análise de riscos e definição do nível de urgência na tomada de decisões e ações. Além do mais, as métricas obtidas ajudam a dimensionar o impacto das vulnerabilidades na organização.

5.2.3 Métricas baseadas nas perspectivas *Top-Down* e *Bottom-up*

Payne (2006) propõe uma metodologia para a construção de um programa de métricas de segurança composto por sete passos:

1. Definir as metas e objetivos do programa de métricas;
2. Decidir quais métricas gerar;
3. Desenvolver estratégias para gerar as métricas;
4. Estabelecer padrões de referências e metas;
5. Determinar como as métricas serão reportadas;

6. Criar um plano de ação e agir sobre ele; e

7. Estabelecer um programa formal de revisão/ciclo de refinamento.

Essa metodologia objetiva produzir o entendimento da finalidade das métricas no programa de segurança, observando seus resultados, bem como, por quem e quando estas métricas serão fornecidas.

A construção de métricas de segurança proposta na metodologia de Payne (2006) é realizada através dos objetivos e metas definidas na primeira etapa da construção do programa de métricas de segurança e através das perspectivas *Top-down* e *Bottom-up*.

A perspectiva *Top-down* é usada na ausência de qualquer abordagem pré-existente para determinar quais são as métricas que devem ser utilizadas. A perspectiva *Top-Down* é descendente, começa com os objetivos do programa de segurança e em seguida, trabalha para identificar métricas específicas que poderiam ajudar a determinar se os objetivos do programa de segurança estão sendo cumpridos. O uso dessa perspectiva como abordagem estabelece as medições necessárias para gerar dados estatísticos. Essa abordagem é composta por 3 passos:

1. Definir os objetivos gerais do programa de segurança;

2. Identificar métricas que indicam o progresso para cada objetivo a ser cumprido;

3. Determinar as medições necessárias para cada métrica.

Já a perspectiva *Bottom-up* é ascendente e implica em uma pré-avaliação da segurança que envolve processos, produtos, serviços, etc. Em seguida, considerando que que as métricas significativas são derivadas a partir dessas medições, é avaliado como essas métricas contribuem para os objetivos do programa de segurança. Essa abordagem baseada na perspectiva *Bottom-up* compreende três passos:

1. Identificar medidas que são ou poderiam ser coletadas para cada processo;

2. Determinar as métricas que poderiam ser construídas a partir de tais medições;

3. Determinar a relação entre as métricas derivadas e os objetivos estabelecidos no programa de segurança.

A perspectiva *Top-down* facilita a identificação das métricas que atendem os objetivos do programa de segurança, enquanto que o uso da perspectiva *Bottom-up* facilita a obtenção das métricas. Ambas as abordagens assumem que os objetivos de um programa de segurança já foram estabelecidos.

A construção das métricas está baseada em itens que compõem a política de segurança e ficam restritas a essa condição. Esta abordagem é recomendada para suporte a decisão podendo estabelecer padrões de referência e metas.

Com a definição dos objetivos e metas a organização pode estabelecer o nível de segurança que deseja atingir tendo assim um entendimento da finalidade de cada métrica.

5.2.4 Métricas baseadas em padrões

A construção de métricas baseadas em padrões de segurança está focalizada no desenvolvimento da segurança do *software*. Na engenharia de *software*, padrões representam uma bem conhecida técnica para o acondicionamento de domínio independente de conhecimentos e especialização em uma forma reutilizável (HEYMAN et al., 2008).

A associação das métricas aos padrões de segurança permite que as métricas sejam facilmente instanciadas na aplicação, por dois motivos. Primeiro, as métricas são selecionadas implicitamente por padrões de segurança o que reduz o problema de seleção de métricas corretas para o problema da seleção correta de padrões. Esse processo se torna fácil porque busca padrões de segurança associados aos objetivos ao invés de padrões específicos para determinado escopo. Após os objetivos de segurança terem sido identificados entre os requisitos de segurança, um conjunto coerente de padrões é selecionado para permitir que os estes objetivos de segurança sejam atingidos. Com a implementação das métricas associadas padrões selecionados, as medições relevantes

para os objetivos de segurança exigidos são executadas. Em segundo lugar, quando os padrões são instanciados durante o projeto arquitetural ou detalhados na fase de projeto, é fornecida uma lista de métricas do tempo do projeto para medir se o padrão está sendo instanciado corretamente. Também é apresentada uma lista de métricas *run-time* que permitirá medir durante a operação se os padrões são apropriados. O desenvolvimento das métricas deve ser incorporado com a implementação da descrição do padrão, o que facilita a instanciação *run-time* das métricas. As medições de ambos os tipos de métricas fornecem garantias extras que o resultado esperado é seguro (HEYMAN et al., 2008).

A seleção da métrica é dada por um gráfico de dependência, que é construído durante o projeto do sistema. Para cada requisito de segurança que o sistema deve proteger, um gráfico de dependência é criado. Cada gráfico de dependência possui três camadas e um objetivo de segurança de alto nível, que corresponde à necessidade de segurança. Os objetivos de alto nível podem ser definidos dentro de um nível mais baixo, ou seja, nas funções de segurança usando um *AND-decomposition*. Esta decomposição captura inter-relações entre diferentes objetivos de segurança. A segunda camada do gráfico de dependência captura os padrões que colaboraram para alcançar os seus objetivos associados. Por fim, a primeira camada do gráfico mostra como as métricas são adicionadas a nós para os padrões que o processo mede. O mensuramento obtido por essas métricas instanciadas indicam o quão bem o processo é realizado.

No primeiro nível, quando um único padrão é considerado a combinação das métricas de um padrão depende da descrição mesmo. Baseado nesta descrição, as métricas são coletadas, normalizadas com uma porcentagem e combinadas em um único valor para cada padrão. Se várias métricas medirem o mesmo aspecto de um padrão, mas com métodos diferentes, uma média ponderada deve ser gerada. Com isso a média de erros dos dados obtidos com as métricas torna-se quase que inexistente (HEYMAN et al., 2008).

Os padrões de segurança usados para construir métricas de segurança são recomenda-

dos para o desenvolvimento de aplicações seguras, mas também podem ser empregados em outras situações (HEYMAN et al., 2008).

5.2.5 Análise comparativa das abordagens para a construção das métricas

Cada abordagem possui uma metodologia própria que considera aspectos diferentes para a construção das métricas. Todas as abordagens apresentadas são usadas como ferramentas que reforçam e contribuem para o aprimoramento dos processos de segurança.

A abordagem SSE-CMM e a CVSS estão baseadas em padrões, mas diferem-se por possuírem critérios diferentes para construção das métricas de segurança. A construção das métricas a partir das PAs do modelo SSE-CMM mensura e define o nível de maturidade dos processos de segurança. Já com o uso de um conjunto de padrões a construção das métricas está associada aos objetivos do programa de segurança.

A mensuração da gravidade das vulnerabilidades usando o CVSS possui dados já definidos pelos fabricantes. Enquanto as outras abordagens avaliam os processos, a abordagem CVSS determina urgências para a implementação de medidas de proteção. Isso contribui para dimensionar o impacto das vulnerabilidades e a padronização o processo de avaliação de riscos. A geração de dados estatísticos fica explícita já que a mesma trabalha com fórmulas matemáticas.

Os objetivos dos programas de segurança são utilizados na construção das métricas de segurança pelas abordagens baseadas em padrões e nas perspectivas *top-down* e *bottom-up*. A diferença entre tais abordagens está que a primeira, busca por padrões que possam estar adequados aos objetivos e na segunda, a construção das métricas é realizada diretamente dos objetivos do programa de segurança considerando as perspectivas *top-down* e *bottom-up*.

A tabela 5.1 resume o comparativo das características discutidas anteriormente referentes a cada abordagem utilizada para a construção de métricas de segurança.

Tabela 5.1: Quadro comparativo de características utilizadas para a construção de métricas de segurança.

Características	**SSE-CMM**	**CVSS**	**Associação de Padrões**	**Perspectivas *Top-down* e *Bottom-up***
Baseado em um padrão, norma ou metodologia.	*SSE-CMM*	*CVSS*	Associação de padrões	*Top-down e Bottom-up*
A segurança está centrada no(a):	Cliente	Usuário final	Objetivos da organização	Objetivos da organização
Tipo de métricas fornecidas	Qualitativas e quantitativas	Quantitativas e qualitativas	Quantitativas	Quantitativas
Objeto da mensuração da segurança:	Sistemas de Informação	Sistemas de Informação	Desenvolvimento seguro do *software*	Desenvolvimento de aplicações
A mensuração é aplicada sobre os (as):	Sistemas de Informação	Processos de segurança dos SI	Mecanismos de desenvolvimento *software*	Desenvolvimento de aplicações
Gerenciamento da segurança	Permite verificar níveis de progressão da segurança através da maturidade dos processos do SSE-CMM.	Realizado através da avaliação das ameaças, vulnerabilidades e riscos.	Realizado através da melhoria dos mecanismos da implementação do *software*.	Realizado através do cumprimento dos objetivos estabelecidos no programa de segurança.
Principal característica	Visualiza o avanço da segurança através dos níveis de maturidade do SSE-MM.	Determina a urgência e a prioridade de resposta às vulnerabilidades.	Fornece subsídios para a padronização dos processos de segurança de *software*.	Fornece uma metodologia para produzir o entendimento das métricas no programa de segurança.
Pré-condição				Existência de uma política de segurança já implantada.

As abordagens apresentadas também demonstram vantagens e desvantagens na sua adoção. A partir da análise das características pode-se observar os aspectos de segurança que cada abordagem pode atender. A tabela 5.2 mostra as principais vantagens e desvantagens de adoção de cada abordagem para a construção de métricas de segurança:

Tabela 5.2: Quadro das principais vantagens e desvantagens encontradas em abordagens de construção de métricas.

Abordagens	**Vantagens**	**Desvantagens**
SSE-CMM	- Permite verificar em qual nível de maturidade determinado processo de segurança se encontra; - Fornece uma abordagem flexível que pode se adaptar às necessidades de segurança de qualquer projeto; - Possui capacidades funcionais oferecidas pelo SSE-CMM para detectar, proteger e responder a inconsistências de segurança.	-O SSE-CMM deverá ser implementado e seguido rigorosamente para retornar bons resultados;
CVSS	- Proporciona uma pontuação global da severidade de um risco diante uma vulnerabilidade; - Auxilia na padronização das atividades de análise de riscos e definição do nível de urgência na tomada de decisões e ações; - Ajuda a dimensionar o impacto das vulnerabilidades dos sistemas de informações; - Prioriza as vulnerabilidades, ameaças e riscos da organização.	- Depende do fornecimento de métricas (métricas básicas e temporais) definidas pelos próprios fabricantes; - Não verifica a eficácia dos processos de segurança já implantados.
	- Os padrões utilizados para a construção de métricas estabelecem um vocabulário comum que facilita a comunicação entre as diferentes partes interessadas;	- Não indica qual padrão deve ser utilizado e qual se enquadra em determinada situação;

continua na próxima página

Tabela 5.2: Quadro das principais vantagens e desvantagens encontradas em abordagens de construção de métricas (continuação)

Abordagens	**Vantagens**	**Desvantagens**
Associação de Padrões	- A associação das métricas aos padrões de segurança permite que as métricas sejam facilmente instanciadas na aplicação; - Fornece garantias extras que o resultado esperado é seguro; - Pode ser empregada em outras situações além do desenvolvimento de aplicações.	- Várias métricas podem medir o mesmo aspecto de um padrão;
Perspectivas *Top-down* e *Bottom-up*	- Fornece o entendimento da finalidade das métricas no programa de segurança; - Fornece um passo-a-passo de como construir um programa de métricas de segurança; - Fornece suporte a decisão para estabelecer padrões e metas; - Gera dados estatísticos.	-A construção das métricas está baseada em itens que compõem a política de segurança e ficam restritas a essa condição.

Embora cada abordagem mencionada possua benefícios e dificuldades na sua construção, é visto que cada organização podem usufruir das abordagens de formas diferentes. Além do mais, uma tendência é usar abordagens de forma combinada para atender os objetivos da organização. Essa é uma idéia que começa a ser discutida pelas organizações que buscam maior eficiência nos programas de segurança. Acredita-se que com a elaboração de métricas em abordagens combinadas possam ser criadas abordagens futuras que indiquem mais benefícios aos programas de segurança.

Ainda não há uma abordagem que abranja todos os aspectos de segurança e que possa ser aplicado como um todo em uma organização. As abordagens citadas nesta seção possuem focos diferentes e cada abordagem é indicada para um determinado contexto.

5.3 A modelagem usando GQM

O GQM *(Goal Question Metric)* é uma abordagem orientada aos objetivos, usada para medição de produtos e processos de engenharia de *software* (FONTOURA e PRICE, 2004). A modelagem dada pelo GQM serve para a elaboração de um plano para monitorar os riscos definindo atividades de envolvem esse processo.

Os dados coletados são baseados em um objetivo ou em uma meta, onde o primeiro passo da abordagem é definir os objetivos a serem alcançadas no programa de medição. Após a identificação dos objetivos, um plano GQM é elaborado para cada objetivo selecionado. No plano GQM, para cada objetivo, são definidas métricas para monitorar cada risco priorizado. Com base no conjunto de métricas, é elaborado um plano de medição para o projeto, detalhando como as métricas devem ser coletadas e com qual periodicidade (FONTOURA, HARTMANN e PRICE, 2006). Na Figura 5.1 pode ser observada as etapas de desenvolvimento da abordagem GQM para a definição de métricas.

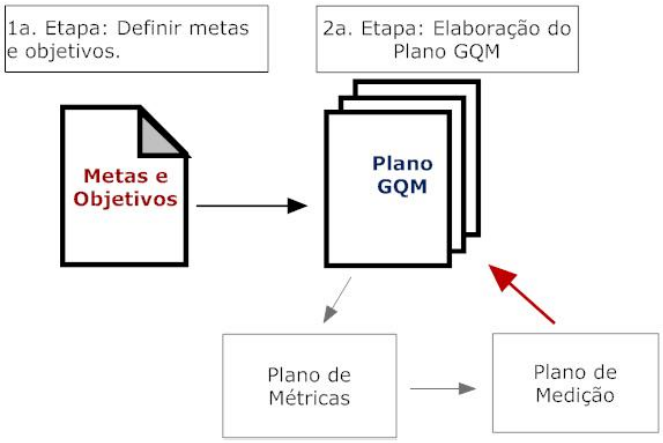

Figura 5.1: Etapas de desenvolvimento da abordagem GQM

Nesta abordagem, a medição é definida usando a perspectiva *top-down*. O GQM é baseado na premissa de que para a organização efetuar uma mensuração efetiva, a mesma deve especificar os seus objetivos e projetos antecipadamente e, posteriormente, analisar a trajetória para atingir estes objetivos. A abordagem também deve disponibilizar

uma estrutura para a interpretação dos dados com relação aos objetivos. O resultado da aplicação da abordagem GQM é a definição de um mecanismo de medição o qual é direcionado para um conjunto particular de elementos. O modelo GQM está dividido níveis:

1. Nível conceitual, chamado de *GOAL* (Objetivo): um objetivo é definido por um objeto podendo ele ser um produto, um processo ou um ativo;

2. Nível operacional, chamado de *QUESTION* (Questão): um conjunto de questões é usado para caracterizar a maneira com que a avaliação de um objetivo específico será realizada;

3. Nível quantitativo, chamado de *METRIC* (Métrica): um conjunto de dados é associado a cada questão, no sentido de respondê-la de maneira quantitativa.

O modelo GQM possui uma estrutura hierárquica conforme observa-se na Figura 5.2. O objetivo é refinado em várias questões. Cada questão é desta forma, refinada sob a forma de métricas. A mesma métrica pode ser usada no sentido de responder diferentes questões.

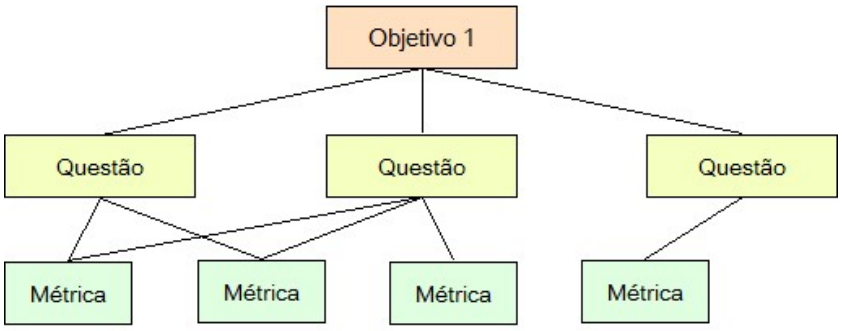

Figura 5.2: Estrutura do modelo GQM

No modelo conceitual GRiSSI, a diferença entre as expectativas de perda é relacionada à redução do risco enquanto que o custo do investimento é relacionado ao custo do

tratamento de risco. Essa premissa ainda indica dois objetivos do GQM, os quais são considerados a base de seus modelos:

- Maximizar a redução dos riscos;
- Minimizar o custo do tratamento dos riscos.

A Figura 5.3 apresenta o modelo GQM utilizado.

Figura 5.3: Modelo GQM - primeira etapa

Baseado nos conceitos do modelo conceitual GRiSSI, para maximizar a redução dos riscos é necessário envolver o conceito do que é um nível de risco, dependendo da frequência de ocorrência e de sua importância para o negócio. É necessário também conhecer qual é o nível de redução do risco. A partir destas questões e dos conceitos obtidos no modelo conceitual GRiSSI as métricas são desenvolvidas.

A primeira métrica é o nível de risco e o seu natural conceito de risco. A frequência de ocorrência do risco é obtida a partir da causa do risco no modelo conceitual GRiSSI. Ele é interpretado pela métrica potencialidade do conceito de evento, dependendo da semelhança da ameaça e do nível de vulnerabilidade. A importância do risco surge na consequência do risco, representada pelo conceito de impacto. O nível de impacto é uma métrica usada para medir a importância do impacto. A importância do risco é

também relacionada com o valor dos ativos do negócio. Para descrever corretamente a importância do risco, o objetivo da segurança é introduzido, expressando a aplicação de um critério de segurança sobre o ativo do negócio.

O objetivo de segurança é necessário uma vez que, para descrever a importância do risco, precisa-se estimar a necessidade da segurança associada para cada objetivo de segurança. Esta métrica é importante para estimar o impacto real sobre a organização e sobre a importância do risco em relação ao negócio. A respeito da redução de riscos, a mesma deve ser estimada para cada tratamento de riscos e cada requisito de segurança. O conceito de controle não pode ser estimado em termos de redução de riscos. A redução de riscos é somente viável sobre o tratamento de riscos e sobre os requisitos de segurança.

A minimização do custo de tratamento dos riscos envolve menos conceitos e também menos questões. Somente uma questão é necessária: “Qual é o custo do tratamento de risco?”. Em relação às métricas associadas, sabe-se que o GRiSSI contém três conceitos relacionados ao tratamento de riscos. A métrica custo é proposta para cada um deles (ver Figura 5.4).

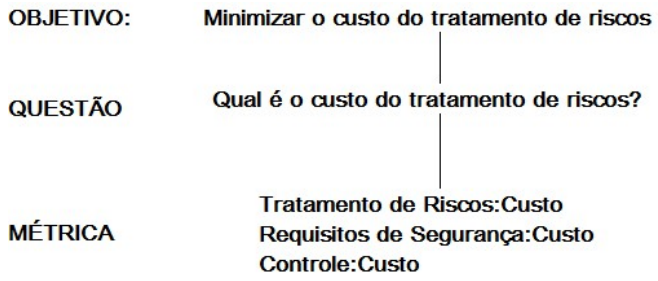

Figura 5.4: Modelo GQM - segunda etapa.

5.4 Normas e Métodos de Gestão de Riscos para a Validação das Métricas

Para a validação das métricas serão consultadas as fontes presentes na gestão de riscos de segurança de SI que contém a descrição do processo. Serão consideradas apenas

as normas de gestão e maturidade de riscos de segurança e as metodologias de gestão de riscos de segurança que não tratam apenas de aspectos terminológicos. A análise de cada fonte resultará nos elementos da métrica relacionada.

A combinação da tabela de análise de métricas, juntamente com o modelo conceitual GRiSSI ampliado e com a inserção das métricas são as contribuições obtidas para a melhoria dos processos de segurança.

5.4.1 Normas de gestão e maturidade de riscos de segurança

Nesta seção serão apresentadas as normas NBR ISO/IEC 27005, NIST SP 800-30 e a NBR ISO/IEC 21827:2008 (SSE-CMM) para a validação das métricas. Será considerado para estudo a ISO/IEC 27005 em primeira instância, passando para as duas restantes através de uma avaliação das tabelas de análise de métricas.

5.4.1.1 ISO/IEC 27005

As métricas e os seus conceitos associados a norma NBR ISO/IEC 27005 são descritos através da tabela 5.3:

Tabela 5.3: Relação entre métricas e seus conceitos associados

Métricas	Conceitos
Valores	para os ativos em estudo
Valor do impacto do negócio	para a consequência
Semelhança	de cenários do incidente ou um evento
Frequência	de ocorrência ameaças
Facilidade	com que as vulnerabilidades podem ser exploradas
Nível	do risco, o qual é uma combinação de um incidente e sua consequência.

As métricas utilizadas são analisadas na Tabela 5.4. As duas primeiras colunas são destinadas aos conceitos do modelo conceitual GRiSSI e aos conceitos da NBR ISO/IEC 27005. Os conceitos são organizados por categorias, as quais são delimitadas

na tabela. As duas colunas restantes apresentam as métricas associadas ao modelo conceitual GRiSSI e a NBR ISO/IEC 27005. Posteriormente, a coluna de definições indica como a métrica é definida ou calculada. Por último, a coluna unidade é usada para a representação de métricas quantitativas ou qualitativas, usando uma unidade ou uma escala.

O único conceito relacionado ao ativo mensurado na ISO/IEC 27005 é o conceito de ativo. A métrica relacionada é o valor do ativo. O ativo primário e o ativo de suporte são instâncias do ativo, sendo mensurados por esta métrica. O valor do impacto do negócio associado com cada ativo é estimado, baseado no valor do ativo. A estimação de riscos é fundamentada em avaliações sucessivas da ameaça e da vulnerabilidade, produzindo o evento semelhança. Combinando a semelhança com o valor do impacto do negócio é possível estimar o nível do risco. Os controles da NBR ISO/IEC 27005 que podem ser alinhados tanto com os requisitos de segurança quanto com os controles do GRiSSI, são estimados conforme a sua efetividade em reduzir as vulnerabilidades. A NBR ISO/IEC 27005 deixa o processo de estimativa (análise qualitativa e quantitativa) dos conceitos para o usuário.

Tabela 5.4: Tabela de análise de métricas a partir da NBR ISO/IEC 27005

Conceito GRiSSI	**Conceito NBR ISO/IEC 27005**	**Métrica NBR ISO/IEC 27005**	**Métrica GRiSSI**	**Definição**	**Unidade**
Ativo	Ativo	Valor		Definido pelo Usuário	Definido pelo Usuário
Ativo de Negócio	Ativo Primário	Valor	Valor	Definido pelo Usuário	Definido pelo Usuário
Ativo de Segurança da Informação	Ativo de Suporte	Valor		Definido pelo Usuário	Definido pelo Usuário

continua na próxima página

Tabela 5.4: Tabela de análise de métricas a partir da NBR ISO/IEC 27005 (continuação)

Conceito GRiSSI	**Conceito NBR ISO/IEC 27005**	**Métrica NBR ISO/IEC 27005**	**Métrica GRiSSI**	**Definição**	**Unidade**
Risco	Risco	Nível de Risco	Nível de Risco	F(evento, consequência)	Definido pelo Usuário
Evento	Evento	Semelhança	Potencialidade	F(ameaça, vulnerabilidade)	Definido pelo Usuário
Impacto	Consequência	Valor do Impacto do Negócio	Nível de Impacto	F(ativo)	Definido pelo Usuário
Ameaça	Ameaça	Frequência de Ocorrência	Semelhança	Definido pelo Usuário	Definido pelo Usuário
Vulnerabilidade	Vulnerabilidade	Facilidade de Exploração	Nível de Vulnerabilidade	Definido pelo Usuário	Definido pelo Usuário
Requisitos de Segurança Controle	Controle	Efetividade	Redução de Riscos	Definido pelo Usuário	Definido pelo Usuário

Na NBR ISO/IEC 27005 o valor do ativo é geralmente estimado em função de conceitos relacionados ao ativo. Usando GQM, o foco está mais nos ativos de negócio, o que aparentemente é considerado mais relevante.

Na segurança de SI, o valor dos ativos de segurança da informação é geralmente irrelevante se comparado com o valor da informação processada no nível de negócio. É necessário considerar o valor dos ativos de negócio para estimar os objetivos da segurança e avaliar a importância dos riscos conforme o modelo conceitual GRiSSI. O conceito de risco, evento, consequência, ameaça e vulnerabilidade presentes na NBR ISO/IEC 27005

possuem suas métricas associadas. Esta norma propõe características adicionais para a fonte de ameaça (equivalente ao agente no modelo conceitual GRiSSI). Para os conceitos relacionados ao tratamento de riscos, a efetividade dos controles deve ser estimada, tendo o mesmo objetivo da redução de riscos dos requisitos de segurança do modelo conceitual GRiSSI. O conceito de tratamento de riscos não é estimado em termos de efetividade. A Figura 2 (ver Anexo 2) apresenta as métricas no contexto da NBR ISO/IEC 27005 no âmbito do modelo conceitual GRiSSI.

5.4.1.2 NIST SP 800-30

As métricas para o contexto da norma NIST SP 800-30 concentra-se no risco. Primeiramente, a definição de semelhança da ameaça surge seguida da importância ou do grau do impacto. Desta forma, o nível de risco é definido com o auxílio de uma matriz (STONEBURNER, GOGUEN e FERINGA, 2002). A norma NIST SP 800-30 propõe três escalas qualitativas para cada métrica: alta, média e baixa. As métricas propostas pelo NIST 800-30 ou suas equivalentes, estão presentes na tabela 5.5:

Tabela 5.5: Tabela de análise de métricas para a norma NIST SP 800-30

Conceito GRiSSI	**Conceito NIST SP 800-30**	**Métrica NIST SP 800-30**	**Métrica GRiSSI**	**Definição**	**Unidade**
Risco	Risco	Nível de Risco	Nível de Risco	Definida por uma matriz de níveis de risco	Alta, Média ou Baixa
Evento	Ameaça (vulnerabilidade explorada por uma fonte de ameaça)	Semelhança	Potencialidade	Definido pelo Usuário	Alta, Média ou Baixa
Impacto	Impacto	Magnitude	Nível de Impacto	Definido pelo Usuário	Alta, Média ou Baixa

5.4.1.3 PA03 ISO/IEC 21827:2008 (SSE-CMM)

As métricas da PA03 concentram-se no 4 nível de capacidade onde todos os processos de segurança são quantitivamente controlados. Para a avaliação do risco proposta pela PA03 são combinadas a PA02 - Avaliação do Impacto, a PA04 - Avaliação das Ameaças e a PA05 - Avaliação das Vulnerabilidades. Juntas essas PAs fornecem dados para a estimativa do risco. As métricas obtidas pela PA03 estão presente na tabela 5.6:

Tabela 5.6: Tabela de análise de métricas para a PA03 da norma ISO/IEC 21827:2008

Conceito GRiSSI	**Conceito PA03**	**Métrica PA03**	**Métrica GRiSSI**	**Definição**	**Unidade**
Risco	Risco	Probabilidade de exposição ao Risco	Nível de Risco	Ordenação de riscos por prioridade	Escala de riscos
Evento	Ameaça	Identificação da exposição tripla	Potencialidade	Definido pelo Usuário	Alta, Média ou Baixa
	Vulnerabilidade	Identificação da exposição tripla	Potencialidade	Definido pelo Usuário	Alta, Média ou Baixa
Impacto	Impacto	Identificação da exposição tripla	Nível de Impacto	Definido pelo Usuário	Alta, Média ou Baixa

5.4.2 Metodologias de gestão de riscos

Nesta seção serão consideradas as metodologias OCTAVE e CRAMM para a validação das métricas. As tabelas de análise de métricas são apresentadas em conformidade com o modelo conceitual GRiSSI.

5.4.2.1 OCTAVE

Na abordagem OCTAVE foram encontradas poucas informações em termos de estimativa de riscos. O método procura estimar o impacto do risco em uma escala quantitativa. A estimativa produz informações que podem ser usadas para definir o nível de risco e as medidas de prevenção. A tabela 5.7 apresenta a análise de métricas para a metodologia OCTAVE.

Tabela 5.7: Tabela de análise de métricas para o OCTAVE

Conceito GRiSSI	**Conceito OCTAVE**	**Métrica OCTAVE**	**Métrica GRiSSI**	**Definição**	**Unidade**
Impacto	Impacto	Nível do Impacto	Nível do Impacto	Definido pelo Usuário	Alta, Média ou Baixa
Ameaça	Ameaça	Elaboração de perfis de ameaças	Semelhança	Definido pelo Usuário	Alta, Média ou Baixa

5.4.2.2 CRAMM

A metodologia CRAMM é um dos poucos métodos que sugere uma estimativa quantitativa. Por exemplo, a severidade/magnitude do impacto é estimada em uma escala de 1 a 10, porém seu custo é determinado em termos financeiros. Assim, o valor dos ativos é determinado baseado nestas métricas. Para ameaças e vulnerabilidades, o CRAMM propõe uma estimativa qualitativa baseada em escalas pré-definidas. A medida do risco é definida posteriormente com o auxílio de uma matriz que combina valor do ativo, nível de ameaça e nível de vulnerabilidade. Baseado nos diferentes níveis de risco, o método propõe medidas de prevenção apropriadas, cada uma das quais tendo o seu próprio nível de segurança. A prioridade é avaliada com a ajuda de alguns fatores, determinando o nível de implementação da medida de prevenção, podendo incluir o custo da medida e sua efetividade. Comparado com as métricas do GQM apresentadas na seção 5.3, as métricas do CRAMM são todas cobertas pelas métricas equivalentes, exceto

pelo nível de segurança, efetividade e prioridade, as quais são associadas ao conceito de requisito de segurança. A tabela 5.8 apresenta a análise de métricas para o CRAMM.

Tabela 5.8: Tabela de análise de métricas para o CRAMM

Conceito GRiSSI	**Conceito CRAMM**	**Métrica CRAMM**	**Métrica GRiSSI**	**Definição**	**Unidade**
Ativo de Segurança da Informação	Ativo	Valor	Valor	F(severidade, custo)	1-10, Unid. monetária (R$)
Risco	Risco	Medida do Risco			
Impacto	Impacto	Severidade	Nível de Impacto	Definido pelo Usuário	1-10
Impacto	Impacto	Custo	Nível de Impacto	Definido pelo Usuário	Unid. monetária (R$)
Ameaça	Ameaça	Nível da Ameaça	Semelhança	Definido pelo Usuário	Muito Alta, Alta, Média, Baixa ou Muito Baixa
Vulnerabilidade	Vulnerabilidade	Nível de Vulnerabilidade	Nível de Vulnerabilidade	Definido pelo Usuário	Alta, Média ou Baixa
Controle de Requisito de Segurança	Medidas de Prevenção	Nível de Segurança		Prioridadade = F(custo, efetividade, ...)	1-10
Controle de Requisito de Segurança	Medidas de Prevenção	Prioridade			Nível
Controle de Requisito de Segurança	Medidas de Prevenção	Custo	Custo	Funcionalidade da Ferramenta	Alta, Média ou Baixa

continua na próxima página

Tabela 5.8: Tabela de análise de métricas para o CRAMM (continuação)

Conceito GRiSSI	Conceito CRAMM	Métrica CRAMM	Métrica GRiSSI	Definição	Unidade
Controle de Requisito de Segurança	Medidas de Prevenção	Efetividade		Funcionalidade da Ferramenta	Alta, Média ou Baixa

A Figura 3 (ver Anexo 3) apresenta a contribuição do estudo das métricas no contexto das metodologias OCTAVE e CRAMM no âmbito do modelo conceitual GRiSSI.

5.5 Melhorando o Modelo Conceitual para a Gestão de Riscos de Segurança de Sistemas de Informação

As métricas no modelo conceitual GRiSSI são representadas sob a forma de atributos, como utilizado para as normas e metodologias envolvidas. O modelo conceitual resultante é dado pela Figura 4 (ver Anexo 4).

O modelo conceitual GRiSSI inclui a determinação do valor dos ativos de negócio. Somente os ativos de negócio são estimados em termos de um valor. Ativos de negócio são usados para definir uma estimativa dos objetivos de segurança e para avaliar a importância dos riscos. O valor do ativo de negócios é usado para estimar a necessidade da segurança para cada ativo de negócios, em termos da confidencialidade, integridade e disponibilidade. Um ativo com um valor elevado pode necessitar de mais segurança do que ativos de baixo valor.

Para os conceitos relacionados aos riscos, o risco é estimado pelo seu nível e depende da potencialidade e do nível de impacto. Um evento é formado pela ameaça e a vulnerabilidade. Os seus respectivos níveis são estimados através da semelhança e do nível de impacto, ou seja, a facilidade de exploração da vulnerabilidade. É importante ressaltar que o agente da ameaça e o método de ataque não possuem métricas. Somente a sua composição é estimada na ameaça.

No contexto dos conceitos relacionados ao tratamento de riscos, o tratamento de risco e os requisitos de segurança são estimados em termos da redução do risco e do custo. Controles somente podem ser estimados em termos de custo. Se um risco é propagado, o risco residual, que é o nível do risco após certa medida de controle, pode permanecer. Isto leva a um nível de redução de risco do tratamento de transferência de riscos. Para a aceitação do risco, a redução do risco é igual a zero.

5.6 Conclusões Parciais

Para alguns conceitos do GRiSSI não foram definidas métricas, o que não impossibilita a utilização da uma métrica subjacente ao conceito principal. Para todos os conceitos envolvidos observou-se que há uma relação da métrica do conceito principal como conceito subsequente.

O conceito Valor dado pelo CORAS, ISO *Guide* 73 e ISO/IEC 13335:2004 foi atribuído ao ativo e ao impacto como uma métrica. Com isso pode-se observar que embora o conceito Valor não esteja definido na ISO/IEC 27005 ele compõe uma das características do domínio da gestão de riscos. Da mesma forma, o Efeito é mensurado por sua severidade podendo se tornar uma métrica do impacto, mesmo que ainda não esteja definido pela ISO/IEC 27005.

Com a definição das métricas pode-se melhorar o modelo conceitual GRiSSI, contribuindo neste sentido para fortalecer o processo de identificação, avaliação e mitigação de riscos.

6 VALIDANDO O MODELO CONCEITUAL DE GESTÃO DE RISCOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÕES (GRiSSI)

O modelo conceitual GRiSSI possui características que podem revelar o seu potencial e a sua confiabilidade. A revisão e a melhoria da qualidade do modelo indicam uma maior adaptação no contexto das organizações e contribuem para a manutenção e redução dos custos associados a ineficiência da revisão humana (GRONBACK, 2004).

Nesse capítulo será abordada a validação[1] do modelo conceitual GRiSSI por meio da aplicação de auditorias e métricas para modelos UML. A utilização da análise estatística para modelos UML contribuirá para o aprimoramento do modelo conceitual, na ordem de obter uma modelagem mais rigorosa, inspecionando e detectando possíveis ineficiências.

6.1 A Abordagem Utilizada

A abordagem utilizada para a validação do modelo conceitual GRiSSI segue as seguintes etapas:

1. Identificação das auditorias e métricas para modelos UML: serão pesquisadas auditorias e métricas para modelos UML que podem ser aplicadas no modelo conceitual GRiSSI;

[1] A validação para esse contexto deve ser entendida como um método de verificação da conformidade do modelo conceitual com os princípios UML.

2. Seleção do conjunto de modelos: será estipulado um conjunto de 8 auditorias e 4 métricas para serem aplicadas no modelo conceitual GRiSSI. Esse conjunto de auditorias e métricas será selecionado conforme o melhor enquadramento com os objetivos do modelo conceitual GRiSSI;

3. Aplicação das auditorias e métricas: o conjunto selecionado será aplicado no modelo conceitual GRiSSI de forma a verificar a sua conformidade;

4. Avaliação dos resultados: construção de tabelas em forma de *cheklists*;

5. Definição de possíveis melhorias: os aspectos levantados na etapa de avaliação serão considerados para a melhoria do modelo conceitual caso se faça necessário;

Na Figura 6.1 pode-se observar o processo de validação dado pelas etapas descritas anteriormente:

Figura 6.1: Abordagem utilizada para o processo de validação do modelo conceitual GRiSSI

6.2 Modelos de Auditoria

A auditoria é realizada por meio da análise estática de um desvio normalmente aceito das melhores práticas para uma linguagem de programação (GRONBACK, 2004). A UML também é tida como uma linguagem de programação que utiliza a análise estática.

A auditoria que é utilizada para inspeção do código fonte é semelhante para inspeções de projetos, onde cada auditoria desempenha uma única inspeção para o propósito no qual foi criada (BORLAND, 2009).

Como a UML é uma linguagem visual, um outro nível de auditoria torna-se essencial para ajudar a aplicar as melhores práticas. A identificação de violações de auditoria para UML podem ser realizadas por meio do exame dos documentos XMI (*XMI Metamodel Interchange*) para UML e do seu arquivo correspondente de especificação (GRONBACK, 2004). O arquivo de especificação possui elementos do modelo que serão examinados no ambiente da ferramenta de modelagem através da API (*Application Programming Interface*) fornecida. Isto permitirá comentários adicionais para o usuário das violações encontradas e facilitará a refatoração do nível do modelo ou da remodelação de *software*.

Há muitas auditorias que podem ser aplicadas aos diagramas UML entre elas podem citadas as auditorias de diagramação geral, ou seja, aplicadas para todos os tipos de diagramas UML e as auditorias específicas do tipo de diagrama.

6.3 Modelos de Métricas

Os modelos de métricas são utilizados com um método de validar o modelo estático dos elementos dos diagramas UML (GRONBACK, 2004). A natureza visual da UML possibilita a utilização dessas métricas. Além disso os modelos de métricas são usados para determinar a qualidade dos modelos UML usados no códigos de geração do projeto (ENCKEVORT, 2009).

Um modelo pode ter vários elementos exibidos em um diagrama, o que pode apresentar algum tipo de violação. A utilização das métricas é necessária para detectar

essas violações quando a visualização do modelo excede a capacidade de compreensão humana.

Os modelos de métricas podem ser de diagramação geral (aplicados a todos os tipos de diagramas UML) e modelos de métricas específicos (específicos para o tipo de diagrama).

6.4 Aplicação das Auditorias e Métricas para o Modelo Conceitual GRiSSI

Para a validação do GRiSSI foram selecionadas 8 auditorias (4 auditorias de diagramação geral e 4 auditorias específicas para diagramas de classe) e 4 métricas (2 métricas de diagramação geral e 2 métricas específicas para diagramas de classe). A escolha das auditorias e das métricas foi realizada aleatoriamente, mas sem desconsiderar a possibilidade de melhoria do modelo conceitual GRiSSI. A seguir são apresentadas na tabela 6.1 as auditorias e na tabela 6.2 as métricas aplicadas ao modelo conceitual GRiSSI. Os nomes das auditorias e das métricas foram mantidos em inglês para assegurar a integridade da referência.

Tabela 6.1: Tabela de auditorias para modelos UML aplicadas ao GRiSSI

Auditorias de Diagramação Geral		
Auditoria	**Descrição**	**Referência**
Always Indicate Multiplicity (AIM)	Em muitos ambientes de modelagem, é possível criar uma associação sem especificar a multiplicidade sobre as associações finais. Isso é vantajoso durante os estágios iniciais de modelagem, mas pode confundir ou complicar a geração de instalações.	FRANKEL (2003), AMBLER (2003)
Always Indicate Navigability (AIN)	A falta de navegabilidade em UML indica a navegabilidade bidirecional ou não especificada. Isso é bom para interpretação humana com um entendimento comum, mas pode confundir ou complicar ferramentas de geração automática.	FRANKEL (2003)

continua na próxima página

Tabela 6.1: Tabela de auditorias para modelos UML aplicadas ao GRiSSI (continuação)

Auditoria	**Descrição**	**Referência**
Identifier Conflicts with Keyword (ICK)	Palavras-chaves utilizadas pela linguagem de programação devem ser evitadas para nomear elementos do modelo.	*Together Edition for Eclipse*
Avoid Using Dependencies (AUD)	Adicionar manualmente dependências semânticas em diagramas UML causa problemas aos desenvolvedores e resulta na não execução devido a significado insuficiente. As relações de dependências não existem no MOF (*Meta-Object Facility*) e devem ser desencorajadas em UML.	FRANKEL (2003)
Auditorias Específicas de Diagramas de Classe		
Use Singular Names for Classes (USNFC)	É prática comum para nomear uma classe usando um substantivo singular.	AMBLER (2003)
Avoid Qualifiers (AQ)	Associações qualificadas não são populares entre a maioria dos modeladores UML. Estas podem ser decompostas de uma classe que representa a associação com um atributo que representa o qualificador.	FRANKEL (2003)
Do not Name Associations that have Association Classes (DNATHAC)	Para o uso de classes de associação, não há necessidade de sobrecarregar a associação com um atributo de nome como deveria ser óbvio dado o nome da classe de associação.	AMBLER (2003)
Conflict With System Class (CWSC)	Classes devem dar nomes que não irão causar conflitos com o sistema de pacotes de uma determinada plataforma ou linguagem de programação da classe API.	*Together Edition for Eclipse*

Tabela 6.2: Tabela de métricas para modelos UML aplicadas ao GRiSSI

Métricas de Diagramação Geral				
Auditoria	**Descrição**	**Min.**	**Máx.**	**Referência**
Number of Colors on Diagram (NOCD)	Muitas cores em um diagrama pode causar problemas de legibilidade e deteriorar a finalidade do uso da cor. Recomenda-se a utilização de 2 ou 3 cores com o máximo de 4 cores.	0	4	COAD (1999).
Number of Elements on Diagram (NOED)	O excesso de elementos em um único diagrama torna difícil a legibilidade e a compreensão. Recomenda-se que grandes esquemas sejam divididos em vários outros menores, sem nenhum esquema com mais de 9 elementos.	1	9	AMBLER (2003).
Métricas Específicas de Diagramas de Classe				
Number of Classes (NOC)	Número de classes definidas.	0	5	*Together Edition for Eclipse*
Number of Operations (NOO)	Número de operações na classe.	0	50	*Together Edition for Eclipse*

6.4.1 Resultados obtidos com a aplicação das auditorias para modelos UML

Na avaliação por meio da aplicação das auditorias foi produzida a tabela 6.3, na qual podem ser observados os seguintes resultados:

Tabela 6.3: Tabela de resultados obtidos com aplicação das auditorias

Auditoria	**Atende**	**Não atende**	**Observações**
AIM	x		Todas as classes especificam a multiplicidade sobre as ações finais.
AIN		x	Não foi definida a navegabilidade no modelo conceitual GRiSSI por se tratar de um modelo conceitual, onde a navegabilidade não é obrigatória.

continua na próxima página

Tabela 6.3: Tabela de resultados obtidos com aplicação das auditorias(continuação)

Auditoria	**Atende**	**Não atende**	**Observações**
ICK	x		Não são utilizadas palavras reservadas de linguagem de programação nos elementos do modelo.
AUD	x		Foi evitado o uso de relações de dependência no modelo.
UFSNC	x		As classes são nomeadas somente no singular.
AQ	x		Foi evitado o uso de associações qualificadas no modelo.
DNATHAC	x		Grande parte das associações possuem um nome para facilitar o entendimento do modelo.
CWSC	x		Os nomes das classes não posuem nomeação correspondente com palavras-chaves relacionadas com plataformas ou linguagens de programação.

Das 8 auditorias aplicadas para a validação do GRiSSI, pode-se observar que somente a auditoria AIN (*DAlways Indicate Navigability*) não atendeu as recomendações de boas práticas para modelos UML proposto por AMBLER (2003). No entando, no modelo conceitual, uma entidade não representa uma classe de *software*, mas um conceito do domínio do problema. Portanto, a definição da navegabilidade não é obrigatória, devendo ser incluída apenas para melhorar o entendimento do modelo.

O GRiSSI é um modelo conceitual que utiliza a nomenclatura dos diagramas de classe para demonstrar todos os conceitos que estão inseridos no gerenciamento de riscos. Portanto, a utilização dos nomes nas associações tende a facilitar o seu entendimento e implementação.

6.4.2 Resultados obtidos com a aplicação das métricas para modelos UML

Com a aplicação das métricas foram verificadas importantes informações sobre o modelo conceitual GRiSSI. Uma das principais informações obtidas foi a dada pela métrica NOED, que restingue ao máximo de nove o número de elementos de um diagrama

de classes. O GRiSSI possui três pequenos diagramas de classes, um para cada conceito principal da gestão de riscos dado pelas normas e metodologias. Depois esses pequenos diagramas de classe são agrupados formando o modelo conceitual de gestão de riscos de SI (GRiSSI). Cada um desses pequenos diagramas não ultrapassa os nove elementos de classe principal, podendo ter subclasses agregadas que expandem o modelo conceitual.

Com a métrica NOO foi verificado que o modelo conceitual GRiSSI não possui operações definidas para suas classes. A não definição das operações foi adotada para reduzir a complexidade do modelo conceitual. No entanto, essa métrica considera de 0 a 50 operações por modelo, sendo que o GRiSSI não possui nenhuma operação atendendo dessa forma essa especificação UML.

O GRiSSI também atente a métrica NOCD satisfazendo o limite exigido de cores e a métrica NOC, com a definição de três classe principais. Dessa forma o GRiSSI atende a todas as métricas, como pode ser observado na tabela 6.4:

Tabela 6.4: Tabela de resultados obtidos com aplicação das métricas

Métrica	**Atende**	**Não atende**	**Observações**
NOCD	x		São utilizadas três cores no modelo conceitual GRiSSI.
NOED	x		O modelo conceitual GRiSSI foi formado por outros diagramas de classe não excendo o limite de nove elementos.
NOC	x		Foram definidas três classes principais.
NOO	x		Não foram definidas operações para o modelo conceitual GRiSSI, pois o mesmo se enquadra em um modelo de domínio.

Outras métricas podem ser úteis para o aperfeiçoamento de modelos. No entando, o modelo conceitual GRiSSI tem o propósito de ser simples e de fácil entendimento, restringindo dessa forma o emprego de todos os recursos da linguagem UML.

6.5 Conclusões Parciais

O modelo conceitual GRiSSI foi validado por meio da verificação feita pelas auditorias e métricas. Por ser um modelo conceitual de domínio, essa verificação se fez necessária já que o emprego desse modelo conceitual em uma organização deve ser o próximo passo.

Diante dos resultados encontrados observou-se que o modelo conceitual GRiSSI está consistente, mas a partir da inserção de novos conceitos será necessária a realização de uma nova validação.

Foram encontradas métricas e auditorias de diagramação geral e específicas para diagramas de classe, que não se enquadraram no modelo conceitual GRiSSI ocasionando a redução dos métodos de validação. Isso não impediu que o modelo conceitual pudesse ser validado, já que o mesmo representa uma forma de simplificar o universo de conceitos da gestão de riscos.

7 CONSIDERAÇÕES FINAIS

7.1 Conclusões

O aumento de ameaças que exploram vulnerabilidades gerando incidentes de segurança e colocado os sistemas de informação em risco, tem aumentado a necessidade da construção de novos modelos de gestão de riscos que vão de encontro com os objetivos organizacionais. O modelo conceitual para a especificação da gestão de riscos de segurança proposto, promoveu a modelagem conceitual da gestão de riscos, buscando nas normas e metodologias relacionar os conceitos que são comumente usados para identificar, avaliar e mitigar os riscos de segurança. O propósito do modelo conceitual é diminuir o impasse na escolha da metodologia ou norma a ser adotada pela organização, com também atender as orientações da Instrução Normativa GSI Nº 1.

Para a construção do modelo conceitual de gestão de riscos foi realizado um estudo das normas e metodologias de gestão de riscos e de segurança, onde pode-se observar que alguns conceitos são tratados de maneira distinta, causando um impasse para a definição do conceito. Alguns conceitos também presentes em algumas normas e metodologias não eram referenciados em outras. Para o modelo conceitual foi considerada a ISO/IEC 27005 em primeira instância para a definição dos conceitos, no entanto, nota-se que há a necessidade de um consenso sobre a definição dos conceitos essenciais para a identificação e avaliação dos riscos.

A modelagem conceitual proporcionou um modelo conceitual de gestão de riscos de

segurança que, conforme sua especificação, teve a integração de três conceitos principais: o ativo, o risco e o tratamento de riscos. Esses conceitos são comuns nas normas e metodologias apresentadas, podendo-se observar que estes fundamentam o processo de gestão de riscos, sendo úteis para o estabelecimento de estratégias de segurança.

As métricas definidas para o modelo conceitual servem de base para avaliar os elementos específicos da gestão de riscos. Esse conjunto de métricas pode ser considerado benéfico para mensurar qualquer processo de gestão de riscos. Na construção das métricas por meio da modelagem GQM foi possível fortalecer o modelo conceitual, podendo-se verificar que a elaboração dos objetivos como recomendado pelo GQM, está relacionado principalmente a redução de custos organizacionais.

A validação do modelo conceitual, realizado por meio da verificação com os princípios UML, proporcionou a correta estruturação do modelo conceitual. Das auditorias e métricas aplicadas somente foram observados requisitos mínimos, pois a proposta do modelo conceitual é facilitar a aplicação do processo de gestão de riscos pelas organizações mediante a estruturação dos conceitos realizada pela modelagem conceitual.

No contexto organizacional, o modelo conceitual GRiSSI pode ser considerado benéfico para o desenvolvimento de programas de gestão da segurança. As características do modelo conceitual indicam a sua ampla utilização. Ele está atrelado as principais normas e metodologias de segurança e de gestão de riscos, além de ser indicado para todos os tipos de organizações. O modelo conceitual atende principalmente as orientações da Instrução Normativa GSI Nº 1 e soluciona os problemas de definição de conceitos.

Para o contexto científico e acadêmico, dois itens devem ser principalmente observados a partir do modelo conceitual apresentado:

- O modelo conceitual se faz completo sendo indicado para a formulação de metodologias de gestão de riscos;
- Ele pode ser reformulado se surgirem novos conceitos, no entanto, isso não invalida o modelo conceitual já proposto.

Uma futura revisão do modelo conceitual pode agregar um conceito novo, mas muito embora seja indicado uma revisão geral dos conceitos do modelo conceitual observa-se que pode-se vincular o novo conceito a um dos três conceitos principais. Isso contribui para a redução do tempo de reformulação do modelo conceitual e de custos adicionais relacionados ao retrabalho.

7.2 Trabalhos Futuros

Para que o processo de gestão de riscos de segurança de sistemas de informação continue sendo aprimorado e estenda sua adesão e eficiência nas organizações se faz necessário dar continuidade aos estudos realizados acerca do modelo conceitual GRiSSI.

O modelo conceitual GRiSSI pode ser usado para a construção de novas metodologias de gestão de riscos de segurança de sistemas de informação, já que o mesmo define regras que devem ser respeitadas para a construção de novos modelos. Um trabalho mais intenso, no sentido de por em prática o que foi definido no modelo conceitual GRiSSI, é construir uma metodologia que faça uso dos conceitos e regras definidas pelo GRiSSI.

REFERÊNCIAS

AAGEDAL, Jan Oyving; BRABER, Den Folker; DIMITRAKOS, Theo; GRAN, Bjorn Axel; RAPTIS, Dimitris; STOLEN, Ketil. **Model-based risk assessment to improve enterprise security.** 6th International Enterprise Distributed Object Computing Conference, 2002.

_____. **NBR ISO/IEC 21827:2008.** Information technology. Security techniques. Systems Security Engineering. Capability Maturity Model (SSE-CMM).Published in Switzerland. 2nd edition, 2008.

_____. **NBR ISO/IEC 27001:2006.** Tecnologia da Informação. Sistema de Gestão da Segurança da Informação. Associação Brasileira de Normas. Rio de Janeiro, 2006.

_____. **NBR ISO/IEC 27002:2009.** Tecnologia da Informação. Sistema de Gestão da Segurança da Informação. Associação Brasileira de Normas. Rio de Janeiro, 2009.

_____. **ISO/IEC TR 13335-1.** Guidelines for the Management of IT Security(GMITS) - Techniques for the management of IT Security. 1st Edition. Switzerland, 2004.

_____. **ISO/IEC TR 13335-2.** Guidelines for the Management of IT Security (GMITS): Part 2— Managing and Planning IT Security. International Organisation for Standardisation, Switzerland, 1997.

_____. **ISO/DIS 31000.** Risk management — Principles and guidelines on implementation. International Organization for Standardization, 2008.

_____. **Risk Solutions.** Definitions. Risksol Consulting, 2007. Acesso em outubro de 2009. Disponível em: <www.risksol.co.uk/resources/print-definitions.php>.

_____. **ISO/IEC Guide 73:2002.** Risk management - Vocabulary - Guidelines for use in standards.ISO Technical Management Board, 2002.

AIRMIC, ALARM, IRM. **A Risk Management Standard.** ALARM The National Forum for Risk Management in the Public Sector, 2002. Disponível em: <www.airmic.com>. Acesso em: outubro de 2009.

ALBERTS, Christopher. J; DOROFEE, Audrey J. **OCTAVE Method Implementation.** Guide Version 2.0., Carnegie Mellon University, Pittsburgh, 2001.

AMBLER, Scott W. **An introduction to process patterns.** IGS Books/Cambridge University Press, 1998.

AREDO, Demissie B. **Metrics for quantifying the impacts of monitoring on security of adaptive distributed systems.** Master Thesis Proposal-II, 2005.

BARBIERE, Carlos. **Modelagem de Dados.** IBPI Press, 1994.

BATISTA, Carlos Freud Alves. **Métricas de Segurança de Software.** Dissertação do Programa de Pós-graduação em Informática do Departamento de Informática da PUC-Rio. Universidade Pontifícia Católica: Rio de Janeiro, 2007.

BEZERRA, Edson K.; NAKAMURA, Emílio T.; RIBEIRO, Sérgio L. **Maximizando Oportunidades com Gestão de Segurança e Gerenciamento de Riscos.** 2006. Disponível em: <www.cpqd.com.br/file.upload/6-sic-1-artigoforum-riscos.pdf> Acesso em: junho de 2009.

BORLAND. **Borland Together - Frequently Asked Questions.** Borland Software Corporation, 2009. Disponível em: <www.borland.com>. Acesso em: novembro de 2009.

BORNMAN, Werner George. **Information Security Risk Management:** A Holistic Framework. Dissertação de Mestrado em Ciência Econômica e de Gestão - Faculty of Economic and Management Sciences at the Rand Afrikaans University, 2004.

CAMPOS, André. **Sistema de Segurança da Informação:** Controlando Riscos. 2ed., Florianópolis: Visual Books, 2007.

CARALLI, Richard A.; WILSON, William R. **The Challenges of Security Management.** Networked Systems Survivability Program Software Engineering Institute, 2004.

CARVALHO, Fernando de Bonneval **COSO X ISO 31000.** Revista Gestão de Riscos, 44 ed., Campo Belo - SP, 2009.

COMMON CRITERIA. **Common Criteria for Information Technology Security Evaluation:** Part 1: Introduction and general model. Version 3.1, Setembro 2003.

COELHO, Paulo. **Security Certification for Organizations:** A Framework to Manage Information Securiy. Dissertação de Mestrado em Gerenciamento de Sistemas de Informação - Instituto Superior de Ciências do Trabalho e da Empresa, 2007.

COSO (Committee of Sponsoring Organizations of the Treadway Commission). **Enterprise Risk Management — Integrated Framework.** Executive Summary, 2004.

DEY, Manik. **Information Security Management - A Practical Approach.** AFRICON 2007, 1-6, 2007.

GOMES, Hermes Oliveira; CARDOSO, Antônio L. S. **Um olhar epistemológico sobre segurança digital nas organizações.** Universidade Federal da Bahia, Salvador-BA, 2008.

GRONBACK, Richard C. **Model Validation:** Applying Audits and Metrics to UML. Borland Software Corporation, BorCon, Embarcadero Technologies, 2004.

ELKY, Steve. **An Introduction to Information System Risk Management.** SANS Institute, 2006.

ERBEN, Roland Franz. **Risk Management Standards: role, benefits & applicability.** 2nd European Risk Conference Università Bocconi, 2008.

ENCKEVORT, Twan van. **Refactoring UML Models:** Using Open Architecture Ware to measure UML model quality and perform pattern matching on UML models with

OCL queries. OOPSLA 2009. Florida, USA, 2009.

FELIX, Jorge Armando. **Instrução Normativa GSI Nº 1, de 13 de junho de 2008**. Diário da União, seção 1, Nº 115, 2008.

FENZ, Stefan; GOLUCH, Gernot; EKELHART, Andreas; RIEDL, Bernhard; WEIPPL, Edgar. **Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard.** 13th IEEE International Symposium on Pacific Rim Dependable Computing, 2007.

FONTOURA, Lisandra M. e PRICE, Roberto T. **Usando GQM para Gerenciar Riscos em Projetos de Software**. 18º Simpósio Brasileiro de Engenharia de Software, 2004.

FONTOURA, L. M., HARTMANN, J e PRICE, T. **Metamodelo para Adaptação de Processos de Software com Base em Riscos do Projeto.** Workshop Iberoamericano de Engenharia de Requisitos e Ambientes de Software, 2006, La Plata. IX Workshop Iberoamericano de Engenharia de Requisitos e Ambientes de Software.

HANAHIRO, Maíra. **Metodologia para Desenvolvimento de Procedimentos e Planejamento de Auditorias de TI Aplicadas à Administração Pública Federal.** Dissertação de Mestrado em Engenharia Elétrica. Universidade de Brasília-UnB, 2007.

HERRERA, Sven S. **Information Security Management Metrics Development.** Security Technology, CCST '05. 39th Annual 2005 International Carnahan Conference , pages 51 - 56, 2005.

HEYMAN, Thomas; SCANDARIATO, Riccardo; HUYGENS, Christophe; JOOSEN, Wouter. **Using Security Patterns to combine Security Metrics.** Third International Conference on Availability, Reliability and Security, 2008.

HOPKINSON, John P. **The Relationship between the SSE-CMM and it Security Guidance Documentation.** EWA-Canada, 1999.

HOUMB, Siv Hilde; GEORG, Geri; FRANCE, Robert; BIEMAN, James; JURJENS, Jan. **Cost-Benefit Trade-Off Analysis Using BBN for Aspect-Oriented Risk-Driven Development.** ICECCS 2005.

HUMPHREYES, Edward. **Implementing the ISO/IEC 27001 Information Security Management System Standard.** Artech House, Inc. Norwood, MA, USA, 2007.

INSIGHT CONSULTING. **Integrating Security into IT Projects and Programmes - CRAMM v5.0**. Lithuania, 2005.

ISO/TMB/WG RISK MANAGEMENT. **Risk management — Guidelines on principles and implementation of risk management**. COMMITTEE DRAFT ISO/CD 31000, 2008.

JONES, Andy; ASHENDEN, Debi. **Risk Management for Computer Security:** Protecting your network and information assets. Revista Security Management, vol. 49, 2005.

LANDOLL, Douglas J. **The Security Risk Assessment Handbook:** a complete guide for performing security risk assessments. CRC Press, 2006.

KAJAVA, Jorma; ANTTILA, Juhani; VARONEN, Rauno; SAVOLA, Reijo; RONING, Juha. **Information Security Standards and Global Business.** ICIT 2006. IEEE International Conference. Industrial Technology, 2006.

KORMOS, Christina; GALLAGHER, Lisa A.; GIVANS, Natalie; BARTOL, Nadya. **Using security metrics to assess risk management capabilities.** 22nd National Information Systems Security Conference, Arlington -Virginia (USA), 1999.

KOVACICH, Gerald L.; HALIBOZEK, Edward P. **Security Metrics Management:** How to Manage the Costs of an Assets Protection Program. Elsevier Butterworth-Heinemann, 352p., 2006.

MARQUIS, Hank. **10 steps to do it yourself CRAMM.** Vol.2, itSM Solutions LL, 2006. Disponível em: <http://www.itsmsolutions.com/newsletters/DITYvol2iss8.htm>. Acesso em agosto de 2009.

MAYER, Janice; FAGUNDES, Leonardo Lemes. **Proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação.** VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, São Leopoldo-RS, 2008.

MELLADO, Daniel; FERNÁNDEZ-MEDINA Eduardo; PIATTINI, Mario. **A Common Criteria based Security Requirements Engineering Process for the Development of Secure Information Systems.** Computer Standards & Interfaces 29, 2007.

NICOLAU, Isabel. **O Conceito de Estratégia.** INDEG/ISCTE - Instituto para o desenvolvimento da Gestão Empresarial, Campo Grande, 2001.

OLIVEIRA, Viviane Luciana. **Uma Análise Comparativa das Metodologias de Gerenciamento de Risco FIRM, NIST SP 800-30 e OCTAVE.** Instituto de Computação - IC / UNICAMP, Campinas, 2006.

PAYNE, Shirley C. **A Guide to Security Metrics.** SANS InfoSec Reading Room, 2006.

PATRICIU, Victor-Valeriu; PRIESCU, Iustin; NICOLAESCU, Sebastian. **Security Metrics for Enterprise Information Systems.** Journal of applied quantitative methods, Vol.1, N. 2, 2006.

PHILLIPS, Mike. **Using a capability maturity model to derive security requirements.** SANS InfoSec Reading Room, 2003.

PINHEIRO, José Maurício dos Santos. **Os Benefícios da Política de Segurança baseada na Avaliação de Riscos e na Integração de Ferramentas.** Revista Científica do Centro Universitário de Volta Redonda, 2007.

RÖHRIG, Susanne. **Using Process Models to Analyse IT Security Requirements.** Tese de Doutorado em Ciência da Computação - Universidade de Zurique, 2003.

SCHUMACHER, Markus; FERNANDEZ-BUGLIONI, Eduardo; HYBERTSON, Duane; BUSCHMANN, Frank; SOMMERLAD, Peter. **Security Patterns.** J.Wiley & Sons, 2006.

SG-SBP. **Recommendation for Creating a Comprehensive Framework for Risk Management and Compliance in the Financial Services and Insurance Industries.** Information Technology Industry Council (ITI), 2008.

SOMAP (The Security Officers Management and Analysis Project). **Open Information Security Risk Assessment Guide.** Version 1.0, 2008. Disponível em:

<http://www.somap.org/sobf/default.html>. Acesso em outubro de 2009.

SSE-CMM Project. **Systems Security Engineering Capability Maturity Model SSE - CMM Model Description Document.** Version 3.0, 2003.

STONEBURNER, Gary; GOGUEN, Alice; FERINGA, Alexis.**Risk Management Guide for Information Technology Systems:** Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30, 2002.

VELLANI, Karim. H. **Strategic Security Management:** A Risk Assessment Guide for Decision Makers. USA: Elsevier, 2006. 416 p.

WOODY, Carol. **Applying OCTAVE:** Practitioners Report Contributors. Carnegie Mellon University. U.S. Department of Defense, 2006.

WRIGHT, Peter; KROLL, Mark J.; PARNELL, John. **Administração Estratégica:** Conceitos. São Paulo: Atlas, 2000. 433p.

YAZAR, Zeki. **A Qualitative Risk Analysis and Management Tool - CRAMM.** GSEC, Version 1.3, SANS Institute Reading Room, 2002.

YOSHIOKA, Nobukazu; HONIDEN, Shinichi; FINKELSTEIN, Anthony. **Security Patterns:** A Method for Constructing Secure and Efficient Inter-Company Coordination Systems. 8th IEEE Intl Enterprise Distributed Object Computing Conf (EDOC 2004), 2004.

ANEXO 1

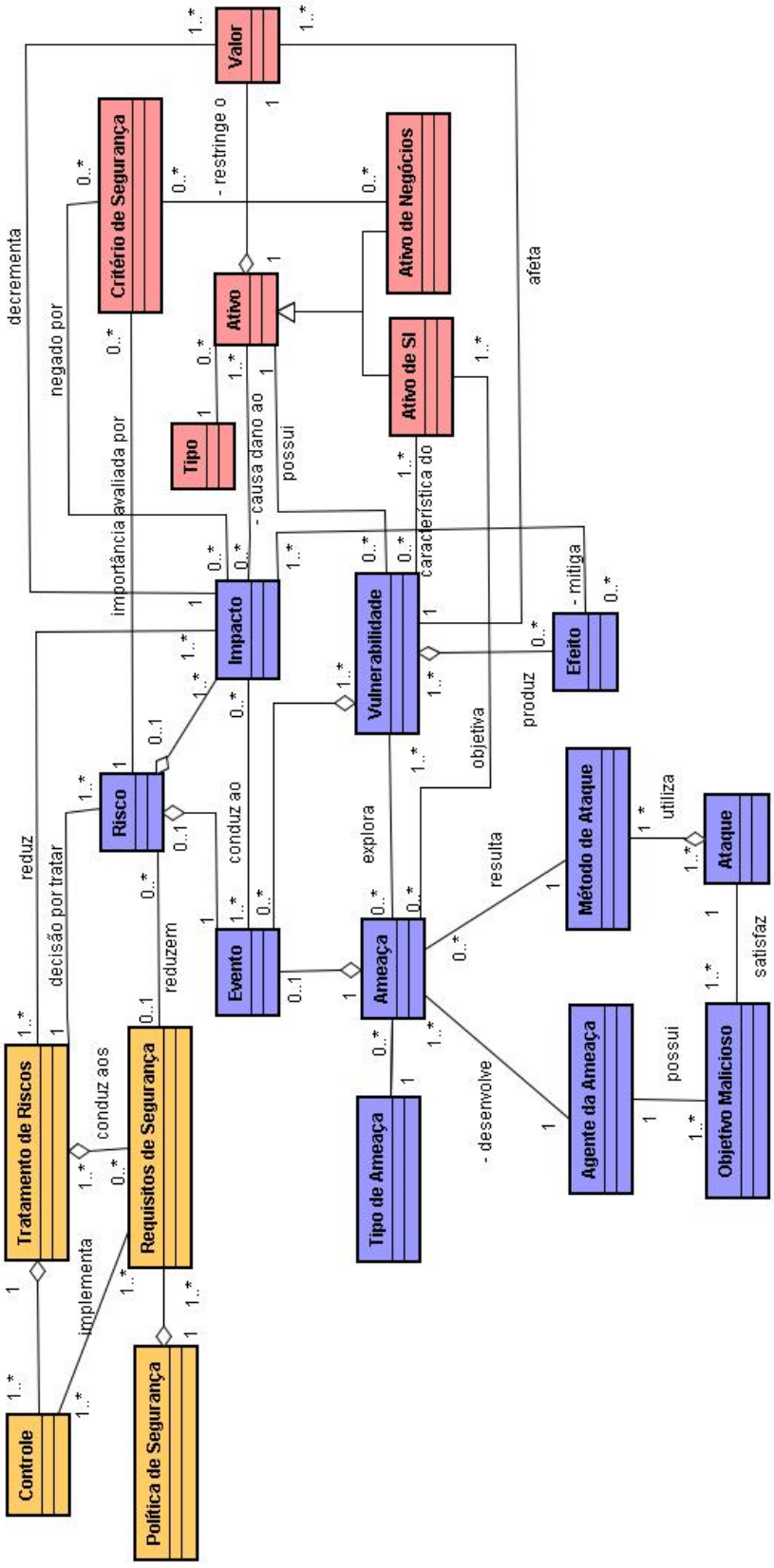

Figura 1: Modelo conceitual de gestão de riscos de segurança de sistemas de informação (GRiSSI)

ANEXO 2

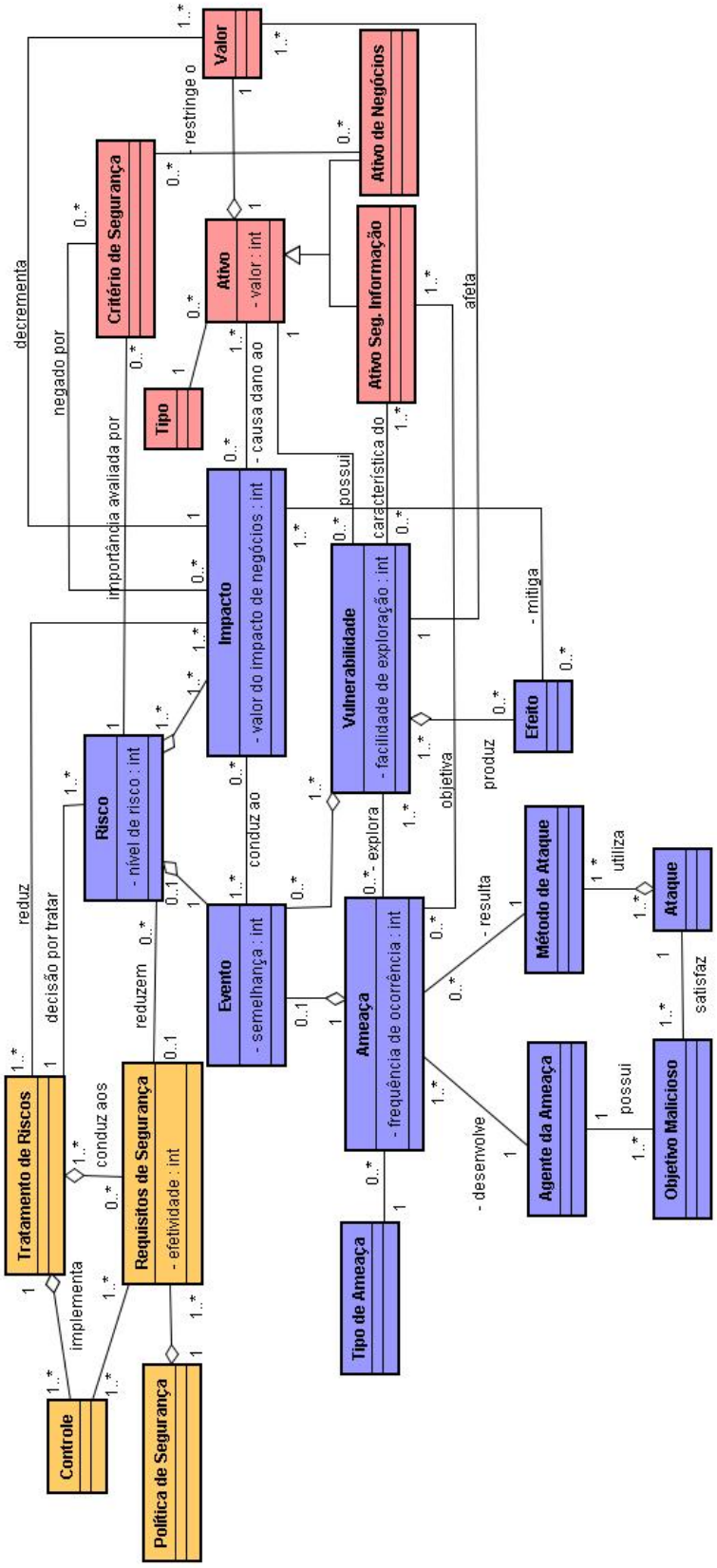

Figura 2: Modelo conceitual GRiSSI e as respectivas métricas associadas a NBR ISO/IEC 27005

ANEXO 3

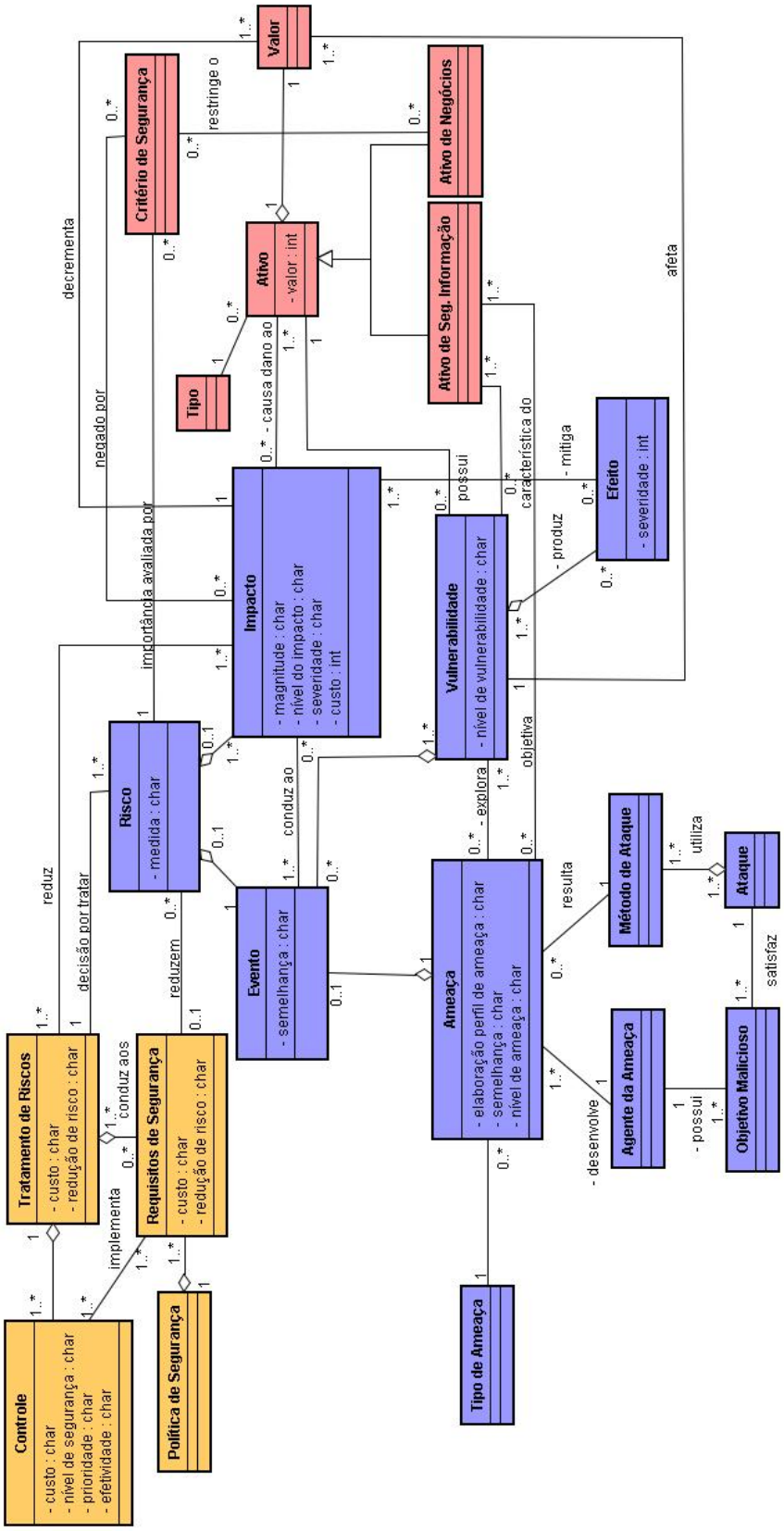

Figura 3: Modelo conceitual GRiSSI e as respectivas métricas associadas ao OCTAVE e ao CRAMM

ANEXO 4

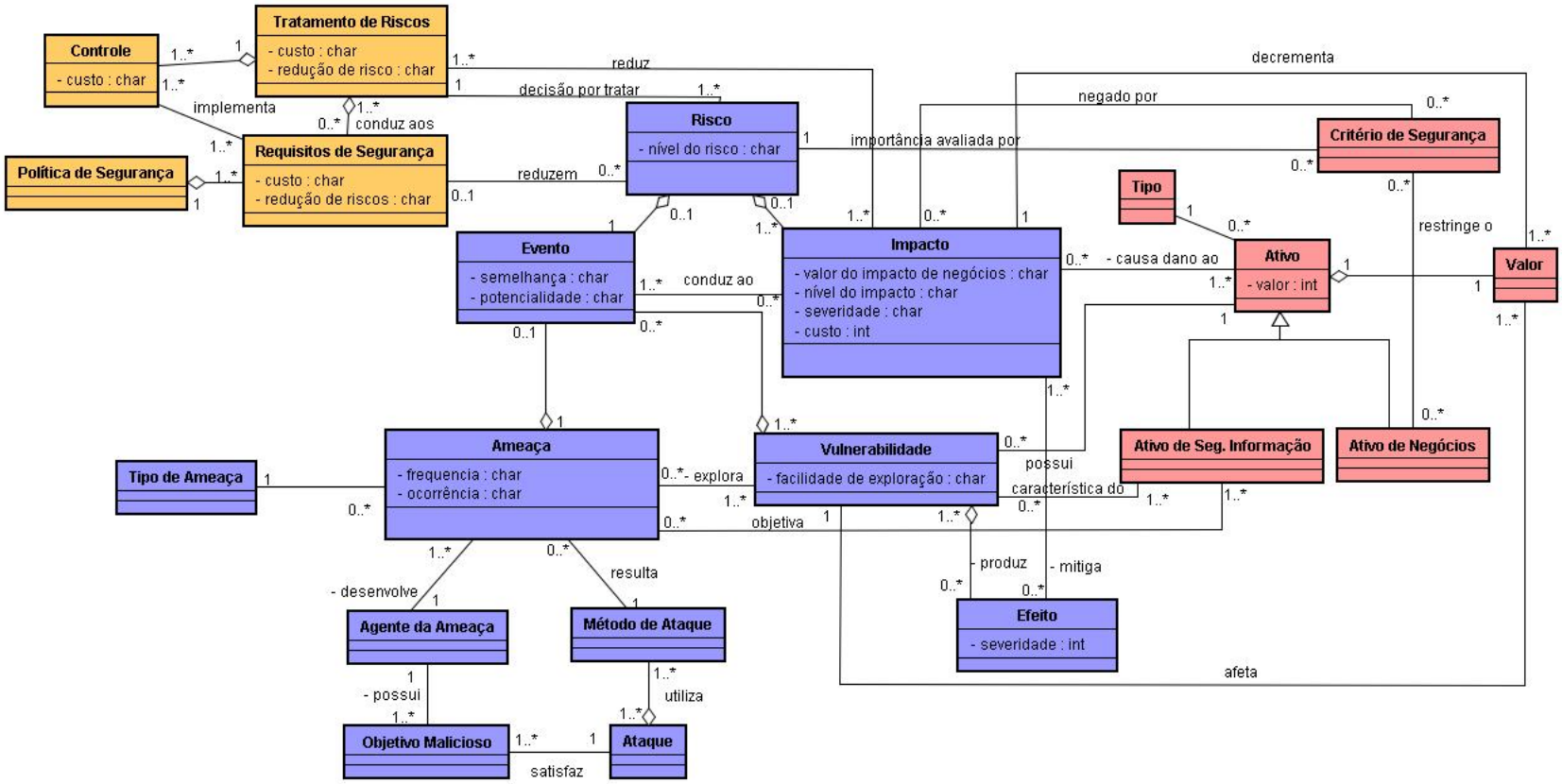

Figura 4: Modelo conceitual GRiSSI para a gestão de riscos de segurança de SI