UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

ESCOLA POLITÉCNICA

DEPARTAMENTO DE ELETRÔNICA E DE COMPUTAÇÃO

IMPLEMENTAÇÃO DE UMA METODOLOGIA DE ANÁLISE DE RISCO BASEADA NA BS7799-3

Candidato:

Tulio Anselmo dos Santos Valentim

Orientador:

Prof. Sérgio Barbosa Villas-Boas

Examinador:

Prof. Aloysio de Castro Pinto Pedroza

Examinador:

Prof. Flávio Luis de Mello

DEL

Novembro de 2008

Dedicatória

A Deus, a meus pais e amados irmãos.

Agradecimentos

Especial agradecimento a Aldael Rizzo, Jonas de Oliveira , Rodrigo de Souza, Caio Louro, Guilherme Tomaz, Maria Elisa Miranda, amigos que em meus últimos anos de graduação foram fundamentais para que pudesse escrever essas linhas agora.

Aos amigos que pude fazer ao longo da graduação e ao longo da vida, com os quais aprendi e venho aprendendo muito.

A Lívia Cristina da Silva Santos, uma companheira muito especial.

A Tarso Valentim e Meive Valentim, irmãos maravilhosos que apesar da distância, nunca me deixaram só.

Aos professores do Departamento de Engenharia Eletrônica, que contribuíram para minha formação como Engenheiro Eletrônico e em especial a Sérgio Barbosa Villas-Boas que me orientou neste trabalho.

Aos meus pais, que sempre me deram amor, condições financeiras e força para que pudesse concluir esse curso de engenharia.

Ao povo brasileiro por pagar o meu curso superior.

Resumo

O padrão normativo BS7799 foi publicado em 1995 pela *British Standards Institute* e trata-se de um código da prática da segurança da informação que visa estabelecer práticas e procedimentos que garantam a segurança dos ativos de uma instituição. Essa mesma família de padrões, em especial as normas BS7799-1 e BS7799-2, foram formalizadas posteriormente como padrões internacionais da família ISO 27000, sendo uma norma certificável.

A BS7799-3 é um guia para o desenvolvimento de metodologias de análise de risco que pode ser utilizado por empresas que visem atender aos requisitos da BS7799-2 e, por conseqüência, da ISO 27001.

Uma instituição é composta por ativos que constituem os bens que possibilitam o funcionamento e a continuidade dos negócios. Os ativos possuem vulnerabilidades que podem vir a representar perdas em diferentes escalas, quantificar essas perdas permite medir quais ações são mais relevantes para solucionar os problemas de segurança e, portanto, priorizá-las. Baseado na BS7799-3, foi definido e implementado uma metodologia de análise de risco visando simplicidade e rapidez na análise.

O presente trabalho propõe a criação de uma estrutura de dados que permita mapear as principais ameaças e vulnerabilidades, propondo controles que resultem em um risco mitigado. O desenvolvimento da estrutura de dados foi feito em Java proporcionando rapidez e portabilidade no trabalho.

Palavras-chave

- ***Segurança da Informação***
- ***Análise de Risco***
- ***Desenvolvimento de Software***
- ***Java***
- ***GUI***

Glossário

IDE – Integrated Development Environment

SWT – Standard Widget Toolkit

JUDE – Java and UML Developer Environment

XML – Extensible Markup Language

GUI – Graphical User Interface

TEF – Transferência Eletrônica de Fundos

CRM - Customer Relationship Management

Índice

Índice de Figuras

1 Introdução

1.1 Motivação

Uma corporação possui um conjunto de ameaças e vulnerabilidades que precisam ser corrigidas com o intuito de evitar perdas em seus ativos. Essas perdas podem ocorrer devido aos mais variados motivos, como a indisponibilidades de sistemas, deixando de prestar serviços para seus clientes; ou no caso de vazamento de dados confidenciais da corporação.

A experiência mostra que nem sempre é economicamente viável ou eficiente corrigir todas as vulnerabilidades e ameaças. Existem casos em que o custo para correção de determinada vulnerabilidade é maior do que o custo dos prejuízos. Em outros é preciso avaliar quais riscos são mais críticos e emergenciais para a instituição.

Uma análise de risco permite identificar todas as vulnerabilidades e ameaças existentes nos ativos de determinada instituição e quantificar os riscos de cada ameaça, ajudando a definir prioridades. O balanceamento de todo os riscos associados a cada uma das ameaças é uma ferramenta fundamental dos programas ou políticas de segurança, que permite propor para as demais áreas qual o conjunto de metas a serem implementadas. Isto torna possível criar um cronograma para correções das vulnerabilidades, de curto a médio prazo.

Uma análise de risco é uma das ferramentas que compõem o gerenciamento do risco de determinada instituição, existem diversos métodos para realizar uma análise de risco e normalmente as mesmas são complexas e fechadas dificultando sua realização, seus métodos normalmente se baseiam em cálculos complexos e com várias entradas.

1.2 Objetivo

O objetivo do projeto é desenvolver uma metodologia para análise de risco baseada no padrão BS7799-3 da *British Standard*. Este padrão promove a análise de determinado ativo com a identificação das vulnerabilidades e ameaças para cálculo, controle e monitoramento do risco; permitindo mitigar o risco com implementação de controles.

Desenvolver uma GUI que funcione como ferramenta para gerenciamento do risco. Uma interface visual possibilitaria a usabilidade da estrutura de dados, possibilitando a fácil realização de uma análise de risco.

2 Fundamentos Teóricos

O capítulo mostra o conteúdo utilizado em cada divisão do projeto. Sendo esta coleta o estudo de técnicas, métodos e conceitos já existentes. Além das tecnologias cuja utilização se mostrou necessária ao andamento do projeto.

2.1 Norma BS 7799-3

A norma BS7799 é considerada um dos mais completos padrões para o gerenciamento da segurança da informação no mundo. Com ela é possível desenvolver um sistema de gestão de segurança baseado em controles e práticas definidos por normas e práticas internacionais.

Em 1995, o padrão BS 7799 foi publicado pelo *British Standard Institute* (BSI), tendo sido escrito pela *United Kingdom Government's Department of Trade and Industry* (DTI). Em 2000 a BS7799 foi adotada como a ISO/IEC 17799, "Information Technology - Code of practice for information security management." e em 2005 foi revisada novamente e renomeada para ISO/IEC 27002.

A BS7799 teve a segunda parte publicada em 1999, pela BSI. Com o título de "Information Security Management Systems - Specification with guidance for use", focando em como implementar um *Information Security Management System* (ISMS).

A BS 7799-3 [6] é um guia para gerenciamento da segurança da informação (*Guidelines for Information Security Risk Management*) definido dentro da ISO/IEC 27001:2005 pela *British Standard*. A terceira parte da BS7799 publicada em 2005 consiste num conjunto de boas práticas para realizar estimativas, monitoramento, reavaliação do risco.

2.2 Linguagem Java

A linguagem de programação Java [2] nasceu do esforço de cientistas da Sun Microsystem em obter uma nova linguagem que permitisse criar aplicativos em dispositivos eletrônicos dos mais variados tipos e fabricantes. Uma linguagem simples e neutra em relação à arquitetura, que inicialmente foi chamada de “Green”.

“Green” não foi muito utilizada para tal intento, mas evoluiu e hoje a conhecemos como Java. Java é uma linguagem orientada a objetos com um conjunto enorme de bibliotecas prontas para usar.

Java é portátil e permite utilizar o código compilado em vários sistemas operacionais. Tudo isso é possível devido à característica de Java, de não compilar o código, mas sim criar um código que será interpretado pela *Virtual Machine* instalada na máquina.

2.3 Segurança da Informação

Segurança da Informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade.

A segurança da informação não visa garantir segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de Segurança da Informática ou Segurança de Computadores está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

3 Definição da Metodologia da Análise de Risco

3.1 Introdução

Corporações, privadas ou públicas, possuem ativos que representam tudo àquilo que é utilizado para gerar recursos e garantir a manutenção dos mesmos. Os ativos podem ser sistemas computacionais, servidores ou até informações e processos contidos na cabeça dos funcionários. Garantir a manutenção desses ativos é fundamental para continuidade dos negócios a médio e longo prazo.

Os ativos podem possuir falhas em sua segurança que podem vir a proporcionar perdas em sua operabilidade por algumas horas ou até multas altíssimas. Ter em mente o conjunto de ativos e os riscos de cada um desses ativos possui é o que comumente se chama de gerenciamento de risco.

Um processo de gerenciamento de risco deve ser visto como um processo holístico que envolve todos os ambientes e processos que representem um ativo, permitindo uma instituição mapear todos os riscos que a cercam. A meta de um gerenciamento de risco é identificar tratamentos pra os riscos, permitindo alcançar os maiores níveis possíveis de sustentabilidade das atividades da organização.

Existem diversas metodologias de análise de risco disponíveis para uso em projetos de segurança da informação, cada uma com seu próprio conjunto de vantagens e desvantagens, e com maior ou menor grau de complexidade. Esses métodos são baseados em padrões de gerenciamento de risco, dentre os quais podemos citar:

- ISO/IEC 13335-2 (Information security risk management);
- BS7799-3 (Guidelines for Information Security Risk Management);
- AS/NZS 4360 (Australian Standard for Risk Management);
- ISO Guide 73 (Risk management - Vocabulary);
- ISO 27005 (Information security risk management);
- Risk Management Standard © AIRMIC, ALARM, IRM: 2002;

Procurando definir alternativas e benefícios para o escopo de projetos de gestão da segurança da informação e também em futuros esforços de manutenção e melhoria da gestão de risco, definindo uma metodologia de análise de risco baseada nos seguintes critérios-chave:

- Simplicidade, de forma a minimizar a necessidade de treinamento de colaboradores e clientes, ou manter e atualizar os produtos gerados;

- Baseada em padrões internacionais, de forma a garantir a corretude da metodologia e viabilizar sua utilização em projetos de certificação;
- Ser facilmente estendida para incorporar aspectos específicos de determinadas áreas de negócios ou outras normas.

Foi também decidido que deveria ser desenvolvida em concordância com a norma *BS7799-3 – Guidelines for Information Security Risk Management*. Esta norma define propriedades e características de metodologias de análise de risco usadas em Sistemas de Gestão de Segurança da Informação, e é referência para o atendimento aos requisitos de certificação para a ISO 27001:2005. Além deste padrão foram analisados e incorporados práticas de outros padrões:

Risk Management Standard © AIRMIC, ALARM, IRM: 2002;

O padrão BS-7799 [6] define um conjunto de processos que visam garantir a gerencia dos riscos do ativo e a manutenção de sua segurança. O processo inclui:

- Entender o processo de negócio do ativo analisado e necessidades associadas ao estabelecimento de uma política de segurança;
- Seleção, implementação e operação de controles no contexto dos riscos associado aos negócios;
- Monitoramento e revisão através de um sistema de gerenciamento de risco;
- Melhoramento continuado do gerenciamento do risco;

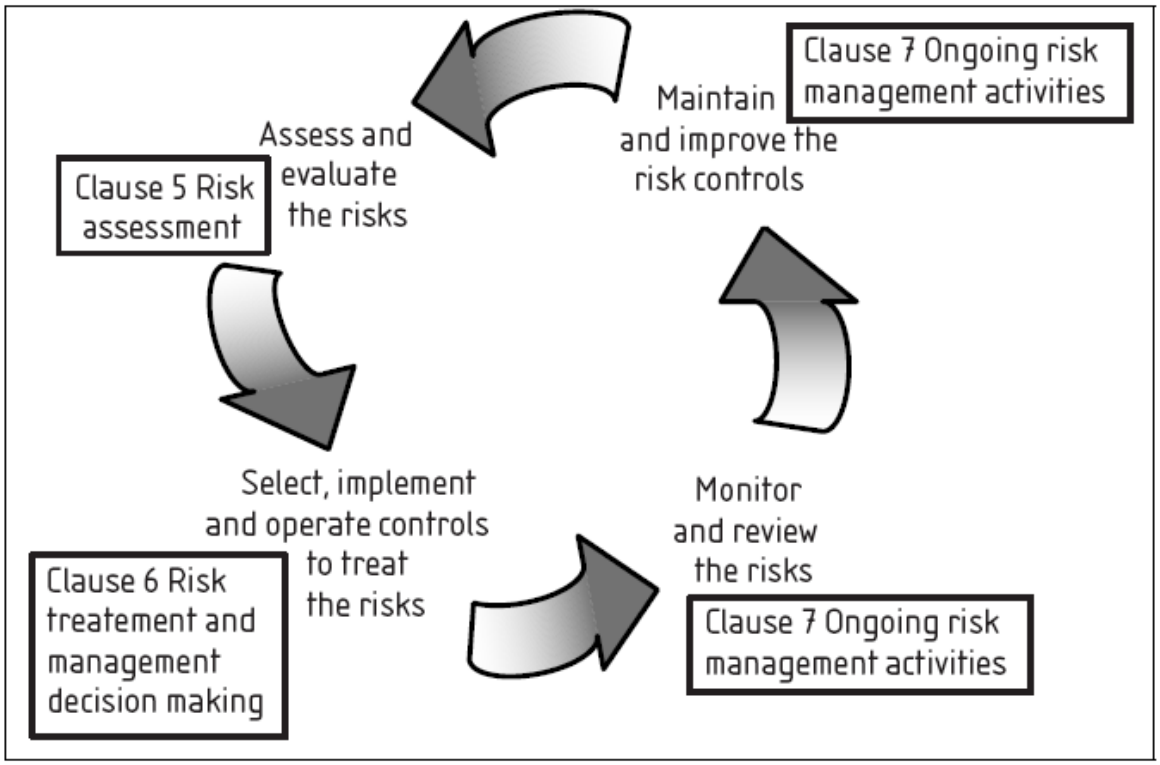

Figura 1 - Gestão de riscos de SGSIs baseados na ISO 27001:2005

Fonte: BS 7799 – 3 [6]

3.2 Termos e Definições

A fim de melhor entendermos o trabalho de análise de risco devemos entender o significado de termos específicos da área de segurança da informação e seu contexto no gerenciamento do risco.

3.2.1 Risco

O risco é a combinação das probabilidades de que determinado evento venha a ocorrer e suas possíveis conseqüências. É a probabilidade do agente de determinada ameaça venha explorar determinada vulnerabilidade causando danos aos ativos: computadores, processos ou dados armazenados em servidores.

3.2.2 Evento de Segurança da Informação

É a ocorrência de um evento nos sistemas, processos ou infra-estrutura de rede da corporação, indicando a probabilidade de uma brecha da política de segurança ou falha dos sistemas de proteção, como *firewall*, antivírus etc.

3.2.3 Redução de Risco

São ações que visam diminuir as conseqüências negativas, associadas à probabilidade de ocorrência de determinada ameaça. A redução do risco deve consistir de ações coordenadas, que atuem em conjunto no ativo, com a análise de todos os risco e ameaças existentes.

3.2.4 Gerenciamento de Risco

O gerenciamento de risco é o conjunto de atividades que visam controlar e manter o nível de segurança aceitável, através do mapeamento dos riscos existentes e aplicação dos respectivos controles. Uma gerencia de risco deve ser parte central das estratégias de gestão de uma organização.

Ela deve ser precedida por uma análise de risco, garantindo um estudo prévio dos riscos existentes e o planejamento de como saná-los.

3.2.5 Análise de Risco

Metodologia utilizada para identificar os riscos de um ativo, estimar esses riscos e propor controles para mitigá-los. Envolve a identificação das vulnerabilidades e ameaças que compõe um ativo e daí estimar o risco associado a cada ameaça.

Uma análise de risco é um processo metódico e necessita do conhecimento da dinâmica do ativo em questão e quais agentes são capazes de atingi-lo.

3.2.6 Ameaça

Potencial causa de um incidente de segurança, ocasionando danos para o ativo e resultando em impactos pra o Negócio. Uma ameaça é vista como a concretização de conjunto de vulnerabilidades.

Ameaças precisam ser concretizadas por um agente que se utiliza das brechas proporcionadas pela(s) vulnerabilidade(s). Existem diversos agentes de ameaças. Podem ser citados:

- Vírus de computador;
- Ações de Hackers;
- Usuário;
- Incêndio;

- Empregado;

3.2.7 Vulnerabilidade

Vulnerabilidades representam as falhas de segurança de um ativo ou conjunto de ativos, permitindo que esses sejam explorados por uma ou mais ameaças que causam incidentes indesejados, resultando em perdas e danos para esses ativos e para os negócios da organização.

Uma vulnerabilidade não causa danos, mas sim condições para que uma ameaça consiga explorar determinado conjunto de ameaças. As vulnerabilidades podem ser fraquezas relacionadas com os seguintes tipos de ativos:

- Hardware, Software e Equipamento de comunicação;
- Procedimentos e Controles para administração e gerenciamento das pessoas;
- Serviços e Operações dos negócios;
- Ambiente Físico;

3.2.8 Integridade

A integridade é obtida quando se garante a precisão das informações armazenadas pelas pessoas, sistemas e processos, prevenindo-se modificações indevidas. Integridade de um ativo pode ser afetada por ações intencionais como vírus, ou acesso indevido, ou ações não intencionais: por exemplo, como usuários inserindo informações inexatas nas entradas dos sistemas.

A perda da integridade compromete o funcionamento dos negócios devido à perda de informações essenciais para processos e/ou sistema.

3.2.9 Disponibilidade

A disponibilidade é obtida quando se garante o acesso ao sistema e a serviços para indivíduos autorizados com um nível de desempenho aceitável. A perda de disponibilidade implica em perdas de acesso ao dispositivo e pode representar falhas na prestação de serviços internos e/ou externos a organização, proporcionando perdas para esses parceiros.

3.2.10 Confidencialidade

A confidencialidade é obtida quando se garante que apenas indivíduos devidamente autorizados devem ter acesso as informações dos ativos de interesse. A confidencialidade deve garantir meios de segregar acessos indevidos a dados da organização.

3.3 Atividades da Análise de Risco

Uma análise de risco constitui uma parte fundamental do desenvolvimento de procedimentos de gerenciamento do risco, permitindo avaliar as falhas na segurança de determinados ativos.

A avaliação da segurança dos riscos inclui a análise de risco e a avaliação do risco. Nosso trabalho propõe uma metodologia que permita quantificar os principais riscos de determinado ativo, identificando suas vulnerabilidades e conseqüentes ameaças.

Uma análise de risco pode propor uma abordagem quantitativa ou qualitativa de acordo com as necessidades existentes, dos resultados que se deseja alcançar, ou mesmo da disponibilidade de recursos. Uma análise de risco quantitativa propõe avaliar um risco com dados reais e valores significativos, baseando-se nos custos das proteções e na freqüência de ocorrência das ameaças.

Uma análise qualitativa não propõe a utilização de valores reais, mas sim baseada na experiência do avaliador, estimando as possibilidades de perda com cada ameaça, sua freqüência de ocorrência etc. Baseando-se na BS7799-3 e numa análise de risco que possa ser feita isenta de valores reais, numa visão geral que tais ameaças representam para o ativo analisado, propõe-se uma análise de risco qualitativa.

- A análise de risco propõe as seguintes atividades básicas:
- Definição do Objeto e Escopo da Análise;
- Identificação dos requisitos de negócios e dos parceiros e áreas afetadas;
- Identificação dos Ativos e Grupo de Ativos;
- Classificação dos Ativos e Grupo de Ativos;
- Identificação e Classificação das Vulnerabilidades;
- Identificação e Classificação das Ameaças;
- Calculo do Risco Inicial;
- Definição de controles e suas ações;

- Cálculo do Risco Residual e Risco Atual

3.3.1 Definição do Objeto e Escopo da Análise

A análise de risco deve ser iniciada através da definição clara do objeto da análise, de forma a delimitar a aplicação da metodologia. O objeto da análise pode ser definido de diversas formas, abrangendo um ou mais processos de negócio, infra-estrutura de TI, sistemas corporativos ou qualquer combinação dos anteriores.

Alguns exemplos de definição de objeto de análise:

Aplicativo web da empresa XKB, abrangendo sua infra-estrutura de TI (ambiente de rede, servidores, software básico e software de aplicação), interfaces com usuários, com outros sistemas da empresa XKB e interfaces com empresas parceiras;

Infra-estrutura de rede de telecomunicações que suporta o serviço de Voz sobre IP da empresa XYZ na região Nordeste. Incluindo roteadores, servidores, software básico e software de aplicação do sistema de Voz sobre IP e de suporte, como DNS, necessários ao seu funcionamento;

Sistema de gestão acadêmica da Universidade FTX, incluindo os servidores de aplicação, banco de dados e localidade física;

Infra-estrutura para processamento de dados de cartão de crédito do Estabelecimento Comercial FCD, incluindo roteadores, modem com adquirentes, servidores de TEF, servidores de Banco de dados do CRM etc;

Sistema de vendas por mala-direta da empresa KEpsilon e o ambiente físico que armazena os servidores de Banco de Dados e os cupons que são enviados pelos clientes pelo correio;

Procedimentos para vendas por telefone da Empresas Móveis LTDA.

O objeto de análise terá impacto direto no esforço da análise de risco, através do aumento da lista de ativos envolvidos. Além do objeto de análise, é importante definir um escopo para o trabalho, restringindo os tipos de vulnerabilidades e ameaças que serão analisados.

A definição do escopo da análise afeta diretamente o esforço da análise de risco, permitindo definir de forma clara, quais processos e sistemas do ativo serão analisados. Restringindo a coleta de informação exclusivamente as vulnerabilidades e ameaças abordadas.

- As etapas da identificação do objeto de análise devem envolver:
- Entrevista com os gestores dos ativos e principais parceiros ou áreas correlatas;

- Escolha dos processos e sistemas que se devem ser incluídos na análise de risco;
- Definição do Escopo da análise de risco, contendo os seguintes atributos:
- Descrição dos sistemas e processos;
- Nome;
- Parceiros afetados pelo ativo;

3.3.2 Identificação dos Ativos e Grupo dos Ativos

Após definir a abrangência da análise de risco, deixando claro o escopo da análise, podem-se identificar os ativos envolvidos nesse escopo. Ativos podem ser pessoas, processos, infra-estrutura, incluindo todas as informações que tem valor ou utilidade para a organização, na operação de seus negócios e para continuidade dos negócios.

É importante manter a identificação dos ativos restrita ao escopo proposto. Uma análise pode definir mais de um ativo, agrupando aqueles que apresentarem similaridade, ou seja, o mesmo grupo de ameaças, sendo chamados de GRUPO DE ATIVOS.

Cada ativo ou grupo de ativos devem possuir um responsável por manter este ativo e implementar ou delegar os controles de segurança. Esse responsável pode ser um departamento dentro da organização ou mesmo um individuo que será identificado como OWNER.

O OWNER é responsável por definir os direitos de acesso e a segurança do ativo, podendo delegar a responsabilidade de manter e implementar os controles de segurança. A fim de manter um maior controle na análise de risco, o OWNER possui dois atributos definindo os responsáveis pela classificação de segurança e pelos direitos de acesso.

A seguir, deve-se identificar e listar os ativos relacionados com o objeto da análise, incluído a descrição e definição de responsáveis. As categorias de ativos que devem ser considerados são:

- Processos e serviços contidos no objeto da análise, incluindo:
    - Processos de negócios;
    - Serviço de ar-condicionado;
    - Processo de Backup;
    - Serviço de Comunicação;
    - Serviços específicos de uma aplicação;
- Pessoas envolvidas no objeto da análise, incluindo:
    - Responsáveis técnicos e/ou líderes de projeto;

    - Gestores das áreas usuárias e/ou responsáveis formais por ativos;
    - Usuários;
    - Terceiros;
- Infra-estrutura tecnológica contida no objeto da análise:
    - Software:
        - Sistemas operacionais;
        - Bancos de dados;
        - Sistemas de apoio;
        - Componentes da aplicação.
    - Hardware:
        - Servidores;
        - Elementos de rede (roteadores, *switches*, *firewalls*, IDS, IPS, etc);
        - Outros equipamentos como centrais telefônicas, POS de sistemas de pagamento por cartão, etc.
- Informação processada, armazenada e/ou transferida.

Os ativos identificados devem ser relacionados na documentação de análise de risco, incluindo a identificação, especificação e descrição. Cada ativo terá um tipo de descrição diferente, o mais importante é evitar ambigüidades e sempre que possível identificar unicamente os ativos envolvidos.

A metodologia define a necessidade de agrupar ativos com propriedades similares ou que compartilhem a mesma função. O agrupamento será então tratado como um único ativo, simplificando a realização e o entendimento da análise de risco. No limite, contudo, um grupo de ativos pode conter um único ativo caso isso seja necessário.

Alguns exemplos de grupos de ativos:

Na análise de risco de sistemas corporativos, normalmente é útil agrupar ativos por servidores, incluindo em cada grupo todo o software utilizado em um servidor (sistema operacional, sistema gerenciador de banco de dados, software de aplicação, sistema de acesso remoto) e as informações armazenadas ou processadas neste servidor;

Numa análise de infra-estrutura de rede altamente replicada, pode ser interessante agrupar os ativos por função, tais como: estações de trabalho, servidores da rede de serviços da localidade XYZ, etc.

Apesar do agrupamento de ativos se tornarem a unidade para realização da análise de risco, cada agrupamento deve conter a lista completa dos ativos que contém, conforme descrito anteriormente.

3.3.3 Classificação dos Ativos e Grupo de Ativos

Após a identificação dos ativos e de seus principais atores, torna-se necessário avaliá-los de acordo com os impactos que as falhas de segurança em determinado ativo podem representar para a instituição.

Cada ativo deve ser avaliado, de acordo com possíveis impactos que leve a perdas na confidencialidade, integridade e disponibilidade. A avaliação deve considerar a conseqüência de perdas em incidentes referentes à lucratividade, *market share*, imagem, reputação, etc. Um valor individual será definido para cada uma das propriedades do ativo, obedecendo a uma escala de 1 a 3, definida como impacto: baixo, médio, alto.

Os níveis de valor de confidencialidade (ATC) são:

Nível 3: ativos cuja divulgação indevida compromete ou impede a prestação de contas, ou atendimento aos requisitos oriundos de entidades externas à organização, tal como cumprimento de leis e regulamentos, prestação de contas e geração de resultados para acionistas, etc.

Nível 2: ativos cuja divulgação indevida compromete a capacidade da organização de tomar decisões operacionais, ou de funcionar de forma eficiente nos processos internos.

Nível 1: ativos cuja divulgação indevida traz impacto marginal à organização.

Os níveis de valor de integridade (ATI) são:

Nível 3: ativos cuja alteração indevida compromete ou impede a prestação de contas, ou atendimento aos requisitos oriundos de entidades externas à organização, tal como cumprimento de leis e regulamentos, prestação de contas, geração de resultados para acionistas, etc.

Nível 2: ativos cuja alteração indevida compromete a capacidade da organização de tomar decisões operacionais ou de funcionar de forma eficiente em seus processos internos.

Nível 1: ativos cuja alteração indevida traz impacto marginal à organização.

Os níveis de valor de disponibilidade (ATD) são:

Nível 3: ativos cuja não disponibilização compromete ou impede a prestação de contas ou atendimento aos requisitos oriundos de entidades externas à organização, tal como cumprimento de leis e regulamentos, prestação de contas e geração de resultados para acionistas, etc.

Nível 2: ativos cuja não disponibilização compromete a capacidade da organização de tomar decisões operacionais ou de funcionar de forma eficiente em seus processos internos.

Nível 1: ativos cuja não disponibilização traz impacto marginal à organização.

Idealmente, a classificação ou valoração dos ativos ou grupos de ativos deve ser obtida junto às áreas de negócio que são usuárias do mesmo ou aos gestores formais dos mesmos. Pode ser interessante reunir mais de um envolvido com cada ativo ou grupo de ativos para chegar a uma avaliação de consenso.

3.3.4 Identificação e Classificação das Vulnerabilidades

A segunda atividade tem como objetivo identificar e listar as vulnerabilidades associadas aos ativos do objeto de análise. Conforme a BS7799-3:2006 e a ISO 13335-1:2004, uma vulnerabilidade é "uma fraqueza em um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças".

De forma a diferenciar vulnerabilidades de ameaças é importante perceber que, uma vulnerabilidade é uma propriedade de um ativo ou grupo de ativos, e nunca uma ação ou evento.

As vulnerabilidades podem não ser de origem tecnológica, apesar da abordagem relacionada à tecnologia em segurança da informação. Contra-exemplos incluem a definição ou execução de processos (ausência de verificação de autorização de visitantes, ausência de processo formal de *patch management*) ou características intrínsecas do próprio ativo (credulidade de seres humanos, inflamabilidade de documentos e prédios, etc).

A identificação das vulnerabilidades será feita através de testes e interação direta com os ativos e grupos de ativos, com a execução de uma análise de vulnerabilidades ou *penetration testing*. Alternativamente, podem ser coletadas através de entrevistas com pessoas envolvidas com o objeto da análise.

As vulnerabilidades identificadas devem ser descritas detalhadamente na documentação da análise de risco. Todas as vulnerabilidades devem também ser classificadas conforme sua facilidade de exploração (VFE), em um dos seguintes três níveis, numa escala de 1 a 3:

Nível 1: exploração de grande complexidade: requer acesso especial ou restrito ao ativo, não automatizável. Vulnerabilidade com probabilidade de exploração baixa e com proteção adequada.

Nível 2: exploração complexa ou de difícil automatização; requer conhecimento avançado para exploração; *exploit* existe mas requer execução local. Vulnerabilidade com probabilidade média de exploração, mas é mantida uma proteção apropriada.

Nível 3: baixa complexidade de exploração; exploração facilmente automatizável; *exploit* remoto disponível na Internet. Vulnerabilidade com grande probabilidade de ser explorada, sem nenhuma ou pouca proteção.

3.3.5 Identificação e Classificação das Ameaças

A próxima etapa da análise de risco consiste na identificação das ameaças dos ativos ou grupos de ativos do escopo da análise, encontrando os incidentes indesejáveis que possam causar prejuízos para a organização.

Ameaças e vulnerabilidades devem ser analisadas em conjunto, evidenciado que ameaças são agentes ou eventos capazes de explorar uma vulnerabilidade. Uma ameaça sempre estará associada a uma vulnerabilidade. Alguns exemplos de ameaças incluem propagação de *worms* pela rede, a abertura de anexos de e-mail infectados por usuários crédulos, a ocorrência de desastres naturais como terremotos e enchentes, ou a falha de equipamentos por desgaste natural.

Uma ameaça pode ser ocasionada por fatores internos ou externos e deve ser identificada com base nas seguintes fontes:

Histórico de incidentes de segurança do objeto de análise. Esse histórico pode ser a lista genérica para determinado ativo ou um histórico interno na organização;

Análise a padrões de *hardening* ou de segurança para determinado ativo em conjunto com a configuração do ativo, determinando os itens de configuração do ativo que se encontra em discordância com as praticas seguras e, portanto, podem vir a ocasionar um incidente de segurança, uma ameaça;

- Normas de referência, tais como a ITU-T X.805 a ISO 13335.

Após a identificação, as ameaças devem ser classificadas conforme sua freqüência de ocorrência (AFO), em três níveis, numa escala de 1 a 3:

- Nível 1: A ameaça se concretiza apenas esporadicamente; freqüência muito baixa.

- Nível 2: A ameaça ocorre com uma freqüência perceptível; já ocorreu alguma vez relacionada ao ativo ou grupo de ativos.

- Nível 3: a ameaça ocorre com bastante freqüência; já foi detectada diversas vezes relacionada ao ativo ou grupo de ativos.

As ameaças devem ser listadas para cada ativo ou grupo de ativos relacionado à aplicação. Para cada ameaça identificada para um dado ativo, devem ser associadas às seguintes informações:

- Descrição da ameaça;

Natureza da ameaça, que pode ser de origem: estratégica, financeira, processos e serviços, hardware, software;

- Classificação da ameaça (AFO);

- Vulnerabilidades associadas à ameaça em questão; incluindo descrição e classificação (VFE);

- Probabilidade de Ocorrência (APO) da ameaça quantifica as chances de que determinado evento venha a ocorrer, esse valor é estimado com a facilidade de ocorrência da ameaça e das vulnerabilidades que a compõe. É um valor na faixa entre 1 (um) e 3 (três) que é calculado a partir da classificação da própria ameaça e das vulnerabilidades associadas, pela aplicação da seguinte fórmula:

$$APO = AFO + \max(VFE) - 1$$

- Identificação da possibilidade de comprometimento da Confidencialidade do ativo ou grupo de ativos pela concretização da ameaça (ACC), indicada pelos valores Sim ou Não;

- Identificação da possibilidade de comprometimento da Integridade do ativo ou grupo de ativos pela concretização da ameaça (ACI), indicada pelos valores Sim ou Não;

- Identificação da possibilidade de comprometimento da Disponibilidade do ativo ou grupo de ativos pela concretização da ameaça (ACD), indicada pelos valores Sim ou Não;

- Uma ameaça deve possuir pelo menos um dos três tipos de comprometimento: AVC, ACD ou ACI;

- Valor comprometido pela ameaça (AVC), calculado pela contribuição do valor (classificação) das propriedades do ativo comprometidas pela ameaça. A seguinte fórmula pode ser utilizada:

```
AVC = somatório(
      (Se ACC = “Sim” Então ATC Senão 0);
      (Se ACI = “Sim” Então ATI Senão 0);
      (Se ACD = “Sim” Então ATD Senão 0);
)
```

3.3.6 Definição dos Riscos

A metodologia prevê o cálculo do risco para as situações abaixo:

Risco Inicial: é o risco calculado com base na situação do objeto de análise no momento da realização do estudo. O risco inicial é avaliado para cada ameaça existente, a partir de cada ameaça e vulnerabilidade reportada.

Risco Residual: é o risco calculado, considerando que todos os controles propostos foram implementados, indicando a situação esperada para o objeto da análise após o término da implementação das recomendações obtidas no processo de homologação. Este nível de risco é calculado na variável ARR e pode ser agregado conforme descrito acima.

Risco Atual: é o risco calculado levando em conta o conjunto de controles efetivamente implementado até o momento do cálculo, permitindo verificar a evolução do objeto de análise durante o processo de implementação dos controles. Este nível de risco é calculado pelo algoritmo de cálculo da eficácia e pela fórmula de risco residual, ignorando os controles não implementados (ou seja, executando o *loop* apenas para os controles que já tenham sido aplicados).

3.3.7 Avaliação do Risco Inicial

Uma vez que os ativos, vulnerabilidades e ameaças estejam identificados, agrupados e classificados conforme as atividades anteriores, serão tratadas a efetiva avaliação dos níveis de risco do objeto da análise.

Um risco tem a contribuição de dois fatores: o impacto que o risco provocaria no ativo e a probabilidade do risco ocorrer. Associando o impacto a perdas de confidencialidade, integridade e disponibilidade, para isto tem-se o atributo AVC. Já a probabilidade de ocorrência encontra-se associada a APO.

Defini-se, portanto, o risco como a soma da probabilidade de ocorrência (APO) mais o comprometimento da ameaça (AVC). Assim a contribuição de cada ameaça ao nível total de risco antes de qualquer tratamento, também chamado Risco Inicial da ameaça (ARI), é calculada através da seguinte fórmula:

$$ARI = APO + AVC - 1$$

Retira-se 1 da formula com a finalidade de manter-se uma escala iniciando em 1. Com isto, o ARI será calculado sempre numa escala de 1 a 7.

O risco inicial pode então ser agregado por ativo ou grupo de ativos, e posteriormente para todo o objeto da análise através de soma simples dos valores de ARI das ameaças associadas, definindo o Risco Acumulado do Ativo.

3.3.8 Definição de Controles e de suas Ações

Após a identificação e estimativa das vulnerabilidades e ameaças devem-se definir controles que venham a mitigar tais falhas na segurança. Os controles devem ser propostos procurando criar um ambiente mais seguro, propondo ações corretivas para as vulnerabilidades e ameaças. Os seguintes fatores devem ser considerados quando forem selecionados os controles a serem implementados:

- Facilidade de implementação e usabilidade;
- Confiabilidade e repetibilidade do controle;
- Resistência à implantação do controle;
- Tipos de funções desempenhadas.

Os riscos podem ser gerenciados com a combinação de prevenções e controles reduzindo:

- A probabilidade de que a vulnerabilidade seja explorada;
- Possíveis impactos dos riscos caso esses ocorram.

Sempre que possível, os controles devem conter referência aos identificadores de controles do Anexo A da norma ISO 27001. A sua descrição deve indicar claramente a sua natureza, forma sucinta de implementação e como afeta a segurança do objeto da análise. Além da descrição, o controle deve determinar sua ação sobre o risco.

A ação do controle determina quais as vulnerabilidades que esse controle mitiga, se a vulnerabilidade deixa de existir ou se reduz a avaliação de VFE; quais ameaças o controle mitiga e se a ameaça deixa de existir ou se a ameaça é mitigada parcialmente, diminuição da estimativa de AFO e/ou deixa de comprometer alguma criticidade. A ação do risco será utilizada para recalcular o risco, obtendo o risco residual.

4 Desenvolvimento

Com o intuito de obter um aplicativo compilando e funcionando de acordo com os requisitos necessários para a implementação de uma análise de risco, adotou-se um ciclo básico para desenvolvimento do *software* [1]. A metodologia propõe três fases de desenvolvimento:

- Análise
- Projeto
- Implementação

As fases de análise e projeto proporcionam um planejamento anterior ao desenvolvimento de código. Já a fase de implementação consiste na codificação. Visando minimizar as falhas de projeto, propõe-se uma metodologia baseada no modelo em espiral, proposto por Barry Boehm [3], com uma interação constante entre planejamento e codificação.

4.1 Análise

4.1.1 Análise de Requisitos

4.1.1.1 Objetivo

A presente demanda tem como objetivo desenvolver uma ferramenta que automatize o método de análise de risco de ativos em uma corporação, proposto no item 3.3, na página 9 do presente trabalho.

4.1.1.2 Referências

A demanda aqui apresentada deverá ser projetada e analisada pelo aluno de Engenharia Eletrônica e Computação, Tulio Anselmo dos Santos Valentim, e premissas definidas nesta análise de requisitos devem ser seguidas durante as demais fases de desenvolvimento.

4.1.1.3 Referências

Item 3.3 do presente documento.

4.1.2 Casos de Uso

O diagrama de casos de uso permitiu uma visão sistemática ou sistêmica do comportamento do aplicativo, permitindo enxergar todo o projeto e daí determinar as regras de negócio. O principal e único usuário do diagrama de casos de uso e o consultor responsável por implementar a análise de risco.

O diagrama de caso de usos geral encontra-se na Figura 2 – Casos de Uso.

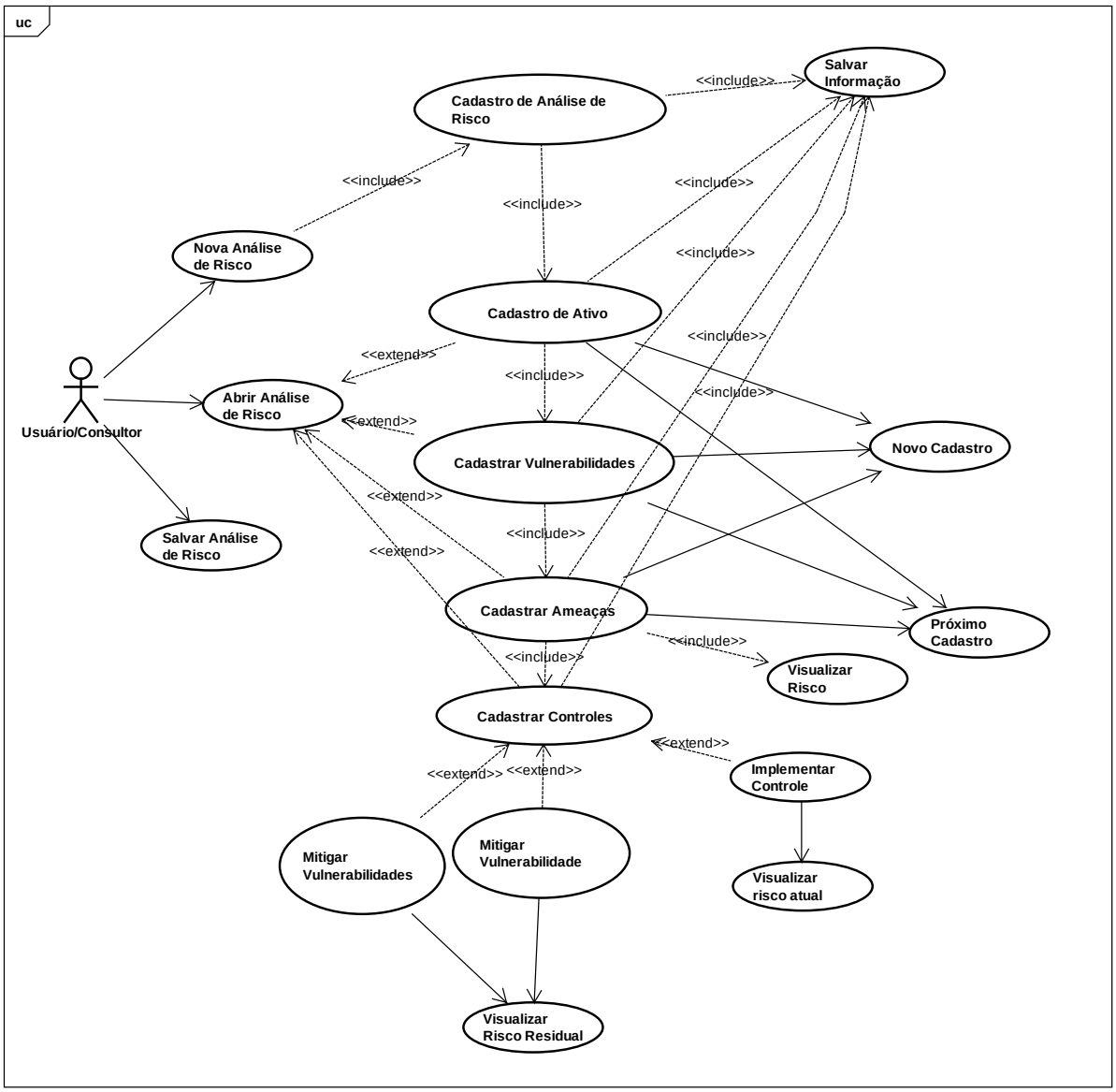

Figura 2 – Casos de Uso

4.1.3 Especificação de Casos de Uso

Título: iniciar nova análise de risco

Atores: consultor.

Descrição: o usuário pode começar uma nova análise de risco quando se inicia o programa, assim como em qualquer momento do processamento.
Pré-condições: o usuário deverá estar com o sistema rodando.
Pós-condições: - (não há)
Fluxo Principal:

Usuário	Sistema
Usuário aciona item novo, no menu Arquivo.	
	Sistema habilita text Box da aba análise de risco e inicia todos os objetos da análise.

Diagrama de seqüência: (não há)

Título: abrir análise de risco
Atores: consultor.
Descrição: o usuário pode abrir uma análise de risco quando se inicia o programa, assim como em qualquer momento do processamento.
Pré-condições: o usuário deverá estar com o sistema rodando.
Pós-condições: (não há)
Fluxo Principal:

Usuário	Sistema
Usuário aciona item abrir, no menu Arquivo.	
	Sistema abre a determinada análise de risco pré-armazenada e envia para as respectivas text Box.

Diagrama de seqüência: -

Título: cadastrar análise de risco

Atores: consultor.

Descrição: o usuário insere informações relacionadas ao tipo de análise de risco que se deseja realizar na aba análise de risco.

Pré-condições: o usuário deve estar com o sistema rodando. O usuário deve ter iniciado ou aberto uma nova análise de risco.

Pós-condições: habilitar aba ativo.

Fluxo Principal:

Usuário	Sistema
O usuário seleciona a aba análise de risco.	
	Sistema exibe aba da análise de risco.
Usuário insere informações nas text Box da aba análise de risco.	
	-

Diagrama de seqüência: (não há)

Título: cadastrar ativo

Atores: consultor.

Descrição: o usuário insere informações, na aba ativo, relacionadas ao tipo de ativo que se deseja realizar.

Pré-condições: o usuário deve estar com o sistema rodando. O usuário deve ter cadastrado uma análise de risco.

Pós-condições: habilitar aba vulnerabilidade.

Fluxo Principal:

Usuário	Sistema
O usuário seleciona a aba ativo.	
	Sistema exibe aba do ativo.
Usuário insere informações nas text Box da aba ativo.	
	-

Diagrama de seqüência: (não há)

Título: cadastrar vulnerabilidades

Atores: consultor.

Descrição: o usuário insere informações, em text Box da aba vulnerabilidade, relacionadas à vulnerabilidade que compõe o ativo que se deseja analisar.

Pré-condições: o usuário deve estar com o sistema rodando. O usuário deve ter iniciado ou aberto um ativo.

Pós-condições: habilitar aba ameaça.

Fluxo Principal:

Usuário	Sistema
O usuário seleciona a aba vulnerabilidade.	
	Sistema exibe aba vulnerabilidade.
Usuário insere informações nas text Box da aba vulnerabilidade.	
	-

Diagrama de seqüência: (não há)

Título: cadastrar ameaça

Atores: consultor.

Descrição: o usuário insere informações, na aba vulnerabilidade, relacionadas ao tipo de vulnerabilidade que compõe o ativo

Pré-condições: o usuário deve estar com o sistema rodando. O usuário deve ter iniciado ou aberto uma nova análise de risco.

Pós-condições: habilitar aba ativo.

Fluxo Principal:

Usuário	Sistema
O usuário seleciona a aba análise de risco.	
	Sistema exibe aba da análise de risco.
Usuário insere informações nas text Box da aba análise de risco.	
	-

Diagrama de seqüência: (não há)

Título: cadastrar controle

Atores: consultor.

Descrição: o usuário insere informações, na aba controle, relacionadas ao tipo de controle proposto para mitigar ameaças e vulnerabilidade.

Pré-condições: o usuário deve estar com o sistema rodando. O usuário deve ter iniciado ou aberto pelo menos uma ameaça.

Pós-condições: (não há)

Fluxo Principal:

Usuário	Sistema
O usuário seleciona a aba controle.	
	Sistema exibe aba controle.
Usuário insere informações nas text Box da aba controle.	
	-

Diagrama de seqüência: (não há)

Título: mitigar vulnerabilidades.

Atores: consultor.

Descrição: o usuário define o que o controle será de mitigado, na aba controle, na vulnerabilidade selecionada.

Pré-condições: o usuário deve estar com o sistema rodando. O usuário deve ter cadastrado pelo menos um controle.

Pós-condições: (não há)

Fluxo Principal:

Usuário	Sistema
Usuário seleciona uma vulnerabilidade na lista de vulnerabilidades existente.	
	Sistema abre um popup menu com as opções de mitigação para a vulnerabilidade escolhida.
Usuário seleciona uma das opções de mitigação do popup menu.	

	Sistema mitiga o controle.

Diagrama de seqüência: (não há)

Título: mitigar ameaça.

Atores: consultor.

Descrição: o usuário define o que o controle ira mitigar, na aba controle, na ameaça selecionada.

Pré-condições: o usuário deve estar com o sistema rodando. O usuário deve ter cadastrado pelo menos um controle.

Pós-condições: (não há)

Fluxo Principal:

Usuário	Sistema
Usuário seleciona uma ameaça na lista de ameaças existente.	
	Sistema abre um popup menu com as opções de mitigação pra a ameaça escolhida.
Usuário seleciona uma das opções de mitigação do popup menu.	
	Sistema mitiga o controle e calcula o risco residual.

Diagrama de seqüência: (não há)

Título: salvar informação.

Atores: consultor.

Descrição: o usuário após inserir informações para cadastro de determinado elemento da análise de risco, deve salvar tal informação.

Pré-condições: o usuário deve estar com o sistema rodando. O usuário deve ter inserido todas as informações a serem cadastradas.

Pós-condições: (não há)

Fluxo Principal:

Usuário	Sistema
Usuário aciona o botão salvar informação	
	Sistema chama objeto do elemento da análise de risco cadastrado e set as informações nesse objeto.

Diagrama de seqüência: (não há)

Título: novo cadastro.

Atores: consultor.

Descrição: o usuário após salvar informações um cadastro de determinado elemento da análise de risco, inicia um novo cadastro.

Pré-condições: o usuário deve estar com o sistema rodando.

Pós-condições: (não há)

Fluxo Principal:

Usuário	Sistema
Usuário aciona o botão novo cadastro.	
	Sistema limpa text Box da aba do elemento que terá novo cadastro.

Diagrama de seqüência: (não há)

Título: próximo cadastro.

Atores: consultor.

Descrição: o usuário após salvar informações um conjunto de cadastro para determinado elemento da análise de risco, seleciona visualizar cadastro pré-realizados.
Pré-condições: o usuário deve estar com o sistema rodando. O usuário já deve ter inserido ao menos um cadastro.
Pós-condições: (não há)
Fluxo Principal:

Usuário	Sistema
Usuário aciona o botão próximo cadastro.	
	Sistema inseri informações do próximo cadastro na text Box da aba do elemento da análise de risco.

Diagrama de seqüência: (não há)

Título: visualizar risco
Atores: consultor.
Descrição: o usuário poderá visualizar os riscos associados à determinada ameaça.
Pré-condições: o usuário deve estar com o sistema rodando. O usuário deve ter inserido ao menos uma ameaça.
Pós-condições: (não há)
Fluxo Principal:

Usuário	Sistema
Usuário seleciona aba risco	
	Sistema exibe aba risco.

Diagrama de seqüência: (não há)

Título: visualizar risco residual
Atores: consultor.
Descrição: o usuário poderá visualizar o risco residual associados à determinada ameaça.
Pré-condições: o usuário deve estar com o sistema rodando. O usuário deve ter inserido ao menos um controle.

Pós-condições: (não há)

Fluxo Principal:

Usuário	Sistema
Usuário seleciona aba risco	
	Sistema exibe aba risco.

Diagrama de seqüência: (não há)

Título: visualizar risco atual

Atores: consultor.

Descrição: o usuário poderá visualizar o risco atual associados à determinada ameaça.

Pré-condições: o usuário deve estar com o sistema rodando. O usuário deve ter implementado ao menos um controle.

Pós-condições: (não há)

Fluxo Principal:

Usuário	Sistema
Usuário seleciona aba risco	
	Sistema exibe aba risco.

Diagrama de seqüência: (não há)

Título: salvar análise de risco

Atores: consultor.

Descrição: o usuário faz persistência das informações da análise de risco.

Pré-condições: o usuário deve estar com o sistema rodando.

Pós-condições: (não há)

Fluxo Principal:

Usuário	Sistema
Usuário pressiona o botão salvar, no menu arquivo	
	Sistema salva todos os objeto que contem o conjunto da análise de risco.

Diagrama de seqüência: (não há)

4.2 Projeto

4.2.1 Diagrama de Classes

A metodologia de análise de risco supõe a existência de agentes capazes de realizar e armazenar as estruturas que determinam uma estimativa do risco. Na programação orientada a objetos as estruturas responsáveis por modelar tarefas em um computador são chamadas de classes [1].

A primeira atividade da elaboração do projeto [1] consiste em descrever as classes que modelam a análise de risco, determinando um diagrama de classes. Nosso trabalho consiste nas seguintes etapas:

1. Descobrir as classes necessárias;
2. Determinar as responsabilidades de cada classe;
3. Descrever os relacionamentos entre as classes;

Abaixo se encontram listadas todas as classes necessárias para implementação da análise de risco [6] e ilustradas na Figura 3 – Diagrama de Classes:

- RiskAnalysis: Criar a análise de risco e propor um conjunto de controles para mitigar os risco encontrados;
- Asset: Definir ativo sobre análise e seu comprometimento referente à sua disponibilidade, confidencialidade e integridade. Catalogar vulnerabilidade e ameaças associadas ao ativo;
- Vulnerability: Define características da vulnerabilidade e sua facilidade de exploração. Catalogar todas as ameaças associadas a essa vulnerabilidade;
- Threat: Define características da ameaça, a freqüência de ocorrência, possibilidade de comprometimento da confidencialidade, disponibilidade, integridade;
- RiskInicial: Calcular o risco inicial associado à determinada ameaça, antes de aplicarmos uma série de controles;
- RiskResidual: Calcular o risco residual associado à determinada ameaça;
- RiskCurrent: Calcular o risco atualmente associado à determinada ameaça;
- Controle: Define que ações podem ser realizadas para mitigar determinada ameaça e/ou vulnerabilidade;
- Action: Define como a ação determinada pelo controle reduz uma ameaça ou vulnerabilidade na pratica, reduzindo determinados parâmetros;
- DeleteThreat: Mitiga risco, deletando a ameaça associada;

- DeleteVulnerability: Mitiga risco, deletando a vulnerabilidade associada;
- ReduceThreat: Mitiga risco, reduzindo a criticidade do risco da ameaça associada;
- ReduceVulnerability: Mitiga risco, reduzindo a criticidade do risco da vulnerabilidade associada;

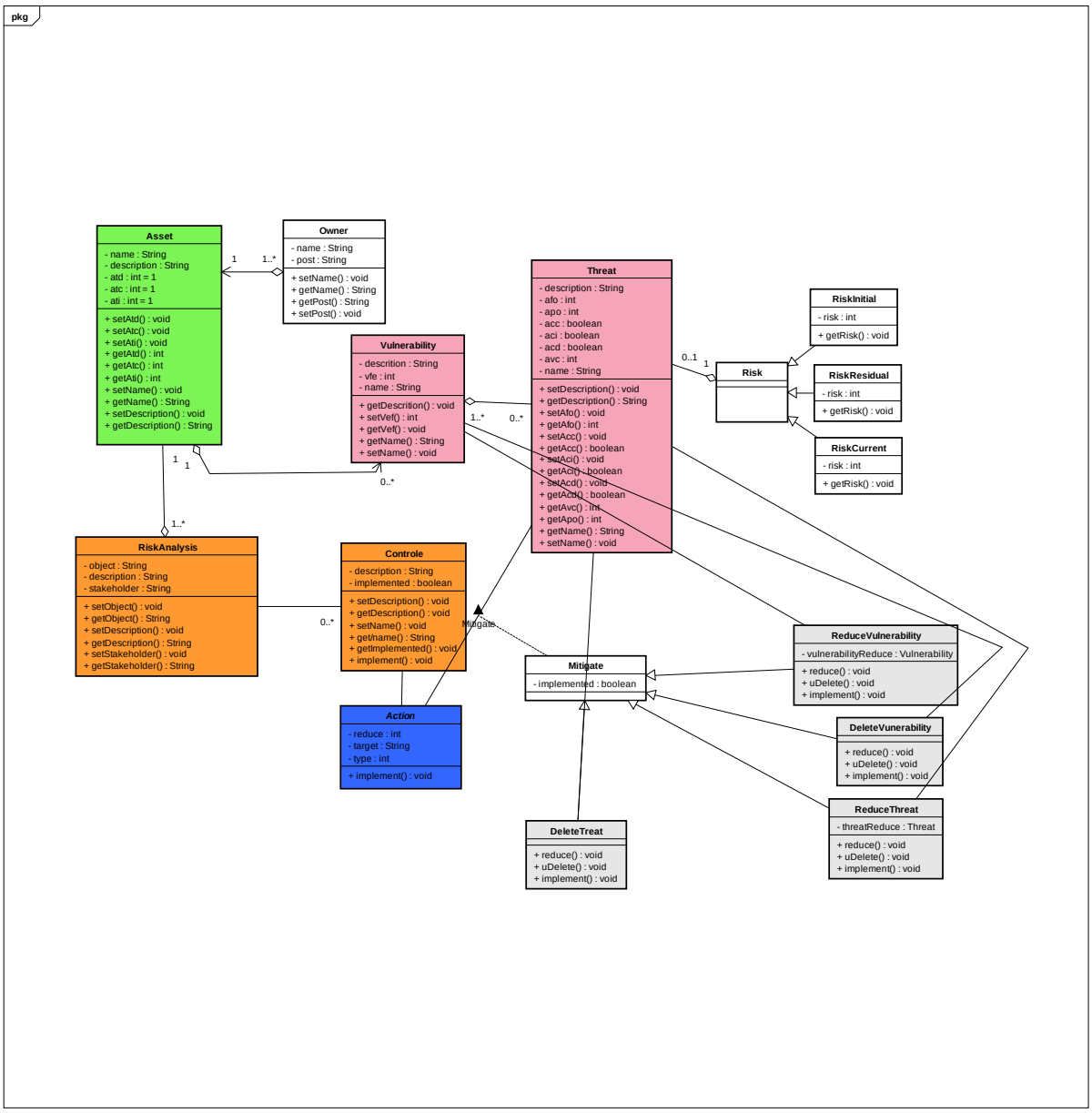

Figura 3 – Diagrama de Classes

Abaixo se encontram listadas todas as classes necessárias para implementação das regras de negócios, criação e armazenamento das instancias utilizadas nas regras de negócios:

CreateAnalysisEvent: Instancia o objeto da classe *RiskAnalysis* e armazena essa classe durante a utilização do programa;

CreateAssetEvent: Instancia o objeto da classe *Asset* e armazena essa classe durante a utilização do programa;

CreateVulnerabilityEvent: Instancia os diversos objetos da classe *Vulnerability* e armazena esses objetos durante a utilização do programa.

CreateThreatEvent: Instancia os diversos objetos da classe *Threat* e armazena esses objetos durante a utilização do programa.

CreateControlEvent: Instancia os diversos objetos da classe *Controle* e armazena e esses objetos durante a utilização do programa.

CreateRiskEvent: Instancia os diversos objetos das classes *RiskInitial, RiskResidual, RiskCurrent* e armazena e esses objetos durante a utilização do programa.

4.2.2 Regras de Negócio

As regras de negócios são implementadas dentro da estrutura da interface GUI, definindo as atividades que serão realizadas pelo aplicativo a fim de executar a análise de risco. Através de eventos decorrentes da interatividade com o usuário serão feitas chamadas a objetos responsáveis por gerenciar a análise de risco.

Seguindo a metodologia desenvolvida para análise de risco, serão propostos nove grupos de procedimentos responsáveis por desenvolver as regras de negócios e interagir entre si, garantindo o funcionamento do aplicativo conforme esperado:

- Análise de Risco: Responsável por receber informações referentes à análise de risco que será implementada e gerenciar esta informação com as etapas posteriores da análise. Sua implementação é ilustrada na Figura 4 – Aba Análise de Risco.
    - Os procedimentos dessa regra de negócio devem incluir:
    - Criar objeto *RiskAnalysis*, caso o mesmo não tenha sido criado. Este objeto deve ser chamado assim que se habilita a *checkbox* **Salvar Informação** (saveAnalysis).
    - Salvar Objetivo, Descrição dos Sistemas e Processos, Nome, Parceiros no objeto *analyse* da Classe *RiskAnalysis*;
    - Desabilitar todas as *text Box*, após as informações serem salvas;
    - Habilita Aba Ativo;

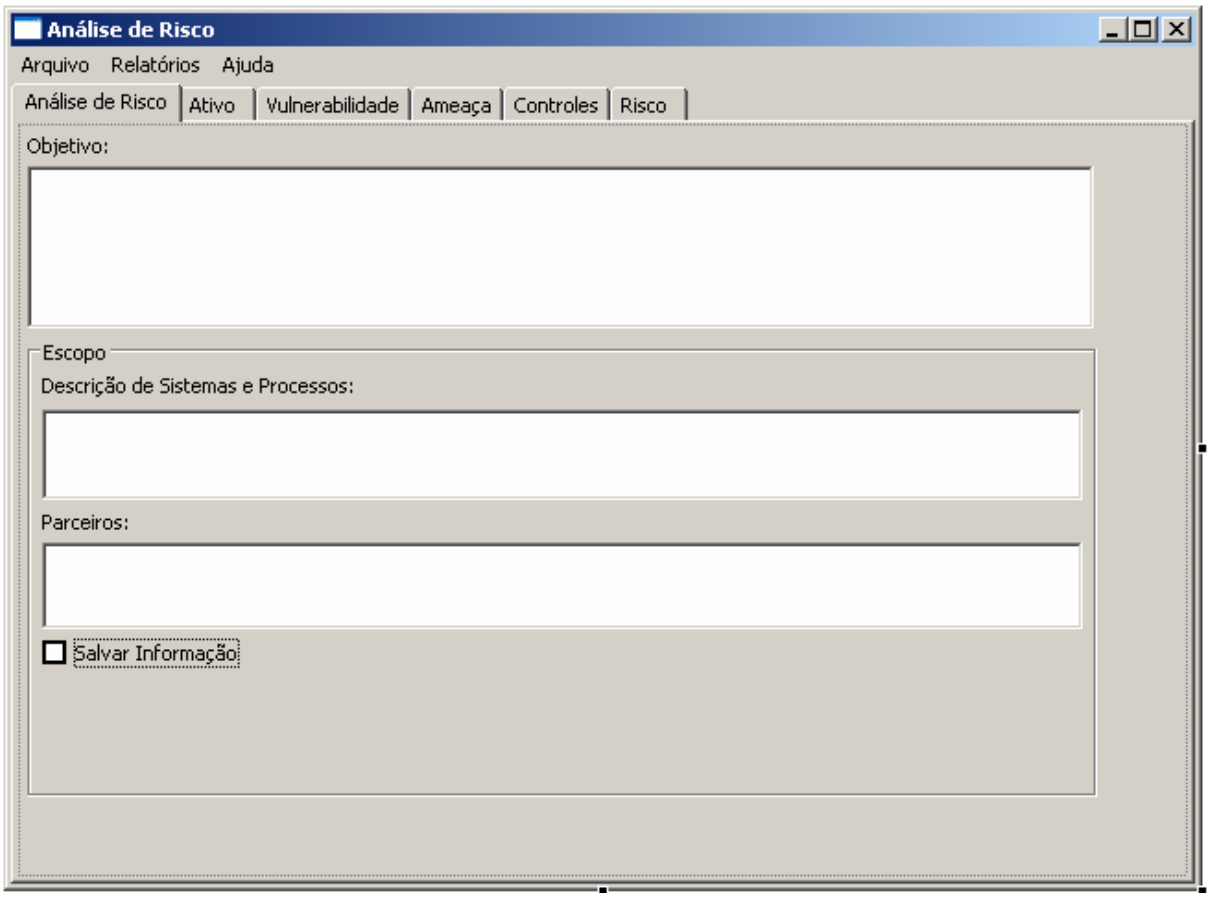

Figura 4 – Aba Análise de Risco

- Ativo: Responsável por receber informações referentes ao ativo que se deseja analisar e suas características. Esta regra é ilustrada na Figura 5 – Aba Ativo.Os procedimentos dessa regra de negócio devem incluir:
    - Criar o objeto *asset*, caso o mesmo não tenha sido criado. Este objeto deve ser chamado toda vez que o *checkbox* **Salvar Informação** (*saveAsset*) da Aba Ativo for habilitada.
    - Salvar o nome, descrição, comprometimento de integridade, comprometimento de disponibilidade, comprometimento de confidencialidade do ativo no objeto *asset*;
    - Desabilitar todas as *text Box*, após as informações serem salvas;
    - Habilita Aba Vulnerabilidade, Ameaça e Controles.

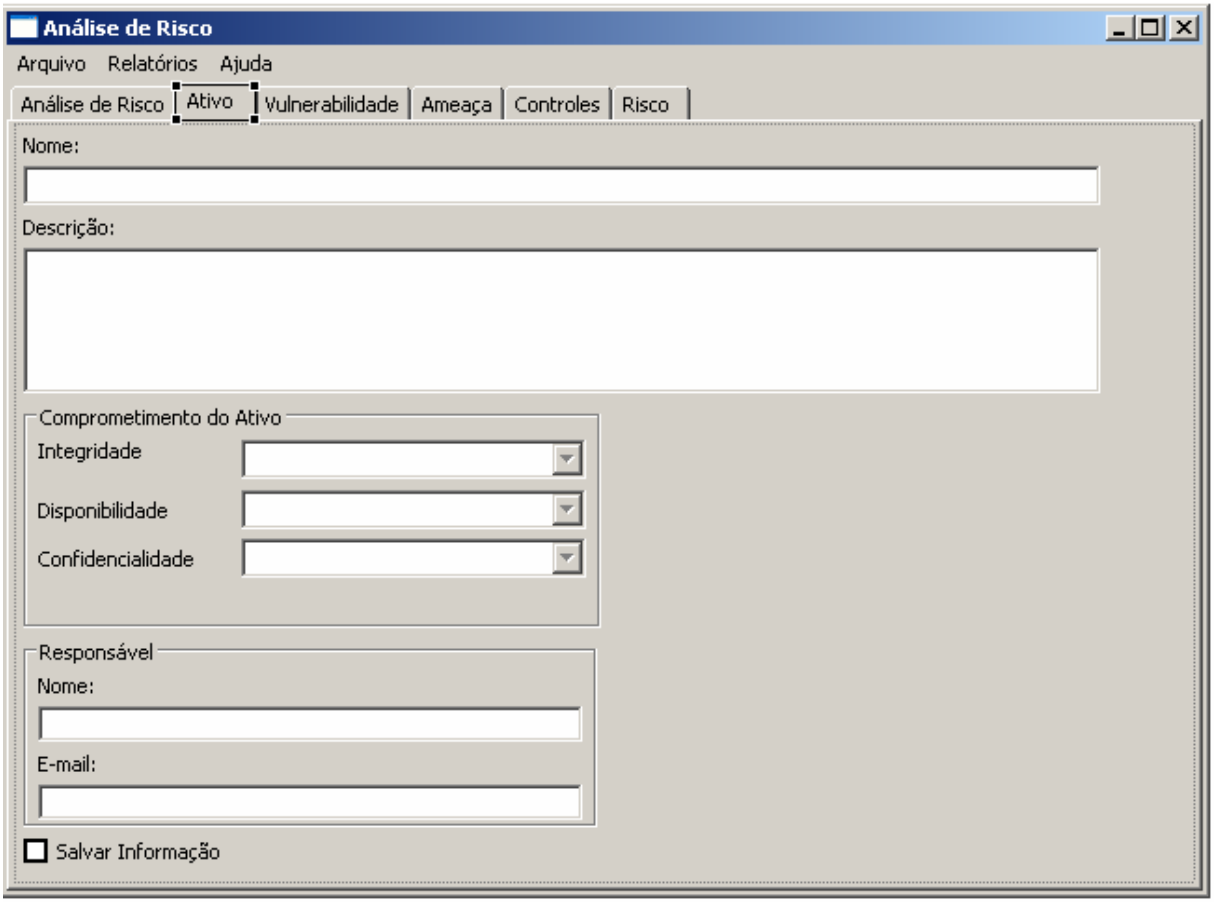

Figura 5 – Aba Ativo

- Vulnerabilidade: Conjunto de procedimentos que visam controlar a exclusão, adição e manipulação dos objetos do tipo vulnerabilidade que compõe a análise de risco, conforme apresentado na Figura 6 – Aba Vulnerabilidade. Os procedimentos dessa regra de negócio devem incluir:
    - Criar objeto *vulnerability*, caso o mesmo não tenha sido criado. Este objeto deve ser chamado toda vez que o *checkbox* **Salvar Informação** (*saveVulnerability*) da Aba Vulnerabilidade for habilitada.
    - Salvar nome, descrição, facilidade de exploração da vulnerabilidade no objeto *vulnerability*;
    - Associar toda nova vulnerabilidade ao objeto *asset* correspondente;
    - Inserir vulnerabilidade na lista de vulnerabilidade (*vulnerabilityTree*) da aba ameaças;
    - Inserir ameaça na lista de ameaça (*threatTree*) da aba Controle;
    - Habilitar e limpar *text box* quando o botão **Nova Vulnerabilidade** (*newVulnerabilityButton*) é acionado;

- Retirar informações da vulnerabilidade atual e adicionar informações referentes à vulnerabilidade anterior na *text box* e na lista de ameaças quando o botão **Próxima Vulnerabilidade** (*previousVulnerabilityButton*) for acionado;
- Apagar todas as referências ao objeto *vulnerability* quando o botão **Apagar Vulnerabilidade** (*deleteVulnerabilityButton*) for acionado.

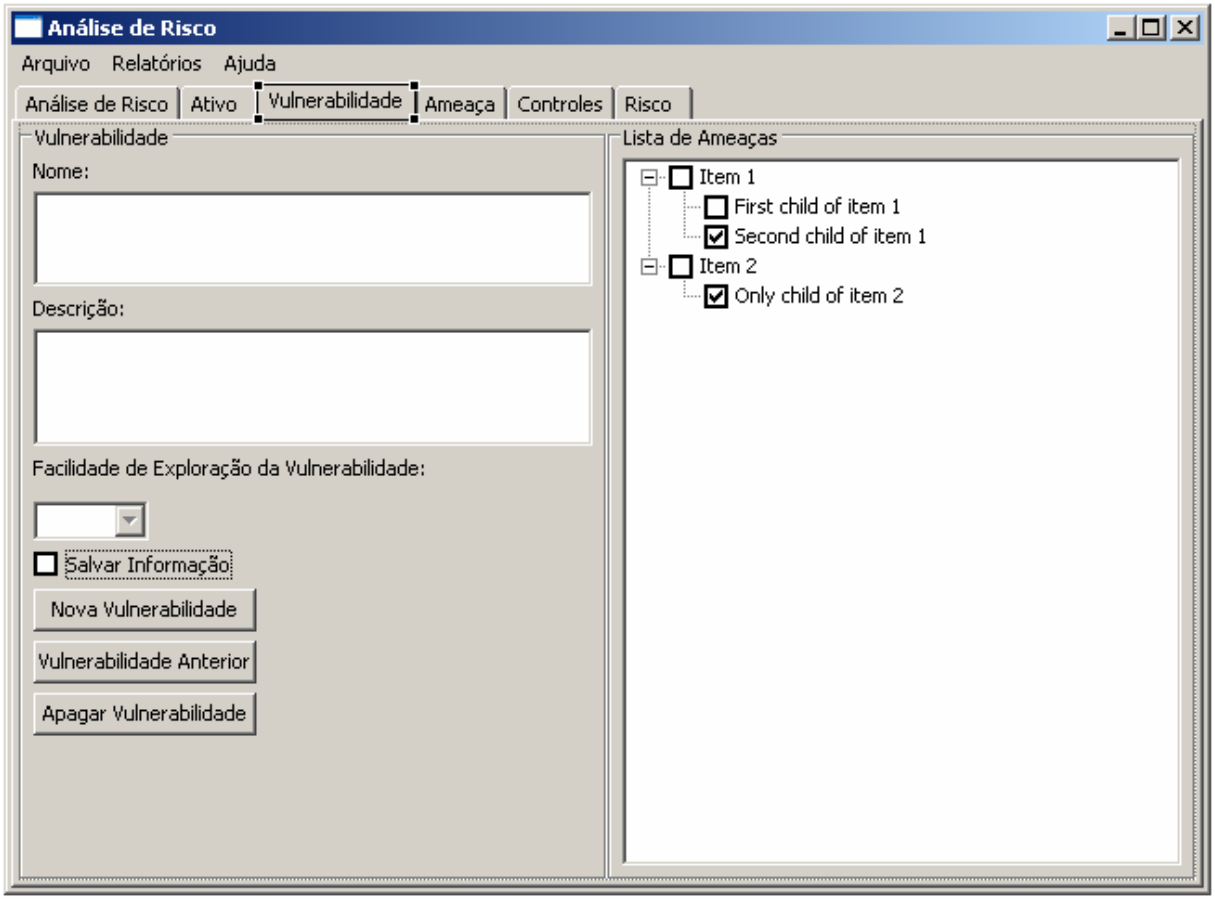

Figura 6 – Aba Vulnerabilidade

- Ameaça: Conjunto de procedimentos que visam controlar a exclusão, adição e manipulação dos objetos do tipo ameaça que compõe a análise de risco. A Figura 7 – Aba Ameaçailustra a materialização desta regra, cujos procedimentos devem incluir:
  - Criar objeto *threat*, caso o mesmo não tenha sido criado. Este objeto deve ser chamado toda vez que o *checkbox* **Salvar Informação** (*saveVulnerability*) da Aba Vulnerabilidade for habilitada.
  - Salvar toda *threat* em *HashMap* [4] no objeto *createThreat*, associando cada nova ameaça a este objeto;
  - Salvar nome, descrição, freqüência de ocorrência da ameaça, possibilidade de comprometimento da confidencialidade, possibilidade de comprometimento da

disponibilidade, possibilidade de comprometimento da integridade no objeto *threat*;

- Garantir que esta ameaça encontra-se associada a uma vulnerabilidade pelo menos;
- Garantir que pelo menos um dos tipos possíveis de comprometimento encontra-se assinalado, antes de criar a ameaça;
- Associar toda ameaça ao objeto *asset* correspondente;
- Inserir ameaça na lista de ameaça (*threatTree*) da aba vulnerabilidade;
- Inserir ameaça na lista de ameaça (*threatTree*) da aba Controle;
- Habilitar e limpar *text box* quando o botão **Nova Ameaça** (*newVulnerabilityButton*) é acionado;
- Retirar informações da ameaça atual e adicionar informações referentes à ameaça anterior na *text box* e na lista de ameaças quando o botão **Próxima Ameaça** (*previousThreatButton*) é acionado;
- Apagar todas as referências ao objeto *threat* quando o botão **Apagar Ameaça** (*deleteThreatButton*) é acionado.

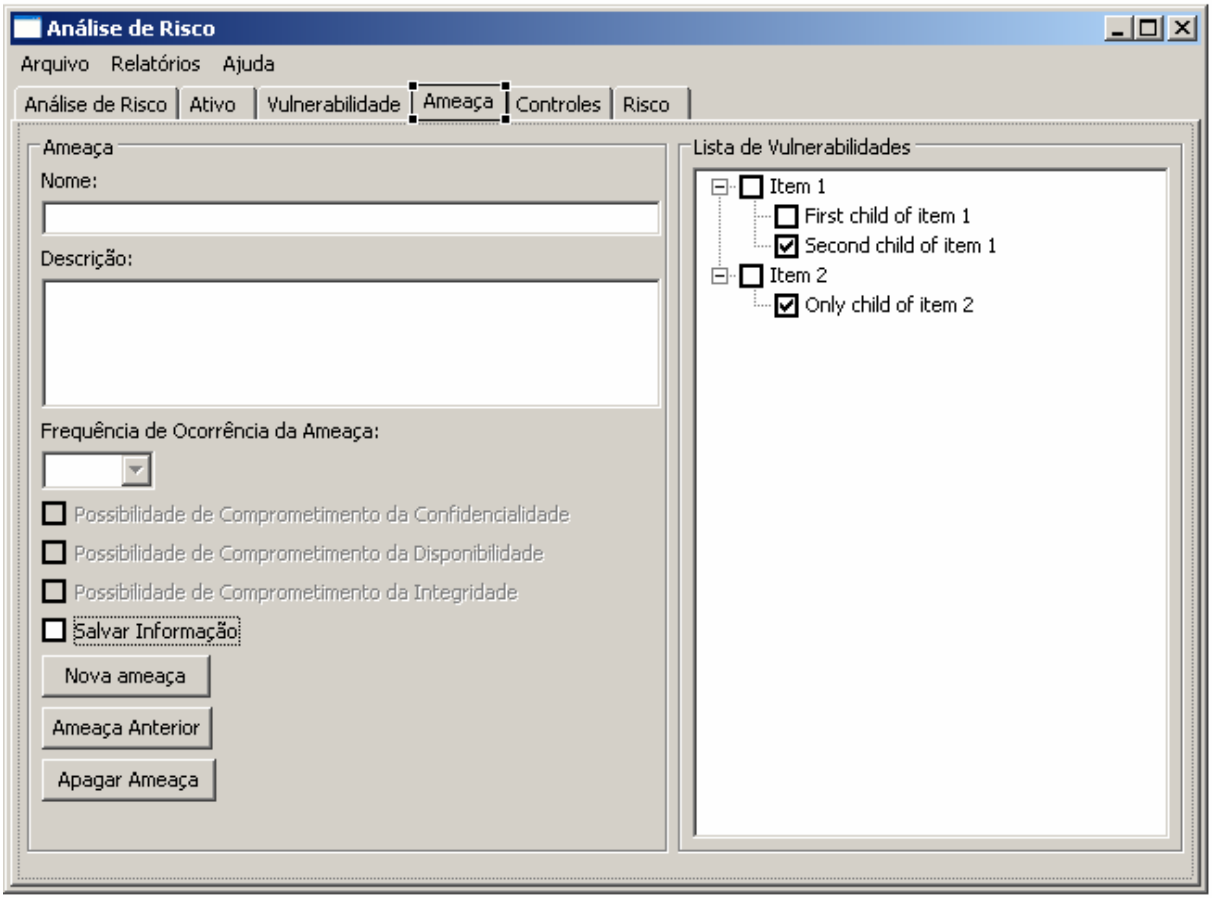

Figura 7 – Aba Ameaça

- Relação entre ameaça e vulnerabilidade: Uma ameaça pode estar relacionada a uma ou mais vulnerabilidades. Assim como uma vulnerabilidade pode estar relacionada a uma ou mais ameaças. Essa regra de negócio deve gerenciar esta relação, impedindo que uma ameaça que já esteja relacionada com uma vulnerabilidade seja relacionada novamente com esta vulnerabilidade, mas desta vez com a vulnerabilidade sendo relacionada com a ameaça. Os procedimentos dessa regra de negócio devem incluir:
    - Cada item selecionado na lista de vulnerabilidades da aba Ameaças deve ser relacionado à ameaça em análise no momento;
    - Cada item selecionado na lista de ameaças da aba Vulnerabilidades deve ser relacionado à vulnerabilidade em análise no momento;
    - Cada item desmarcado na lista de vulnerabilidades da aba Ameaças deve ser retirado o relacionamento à vulnerabilidade em análise no momento;
    - Cada item desmarcado na lista de ameaças da aba de Vulnerabilidades deve ser retirado o relacionamento à ameaça em análise no momento.
- Controles: Um controle propõe medidas que visa mitigar determinadas vulnerabilidades ou ameaças. Um determinado controle pode agir em uma ameaça ou vulnerabilidade com diferentes níveis de mitigação. Esse objeto gerencia os quatro tipos de ações possíveis de um controle. Os procedimentos do controle, ilustrado na Figura 8 – Aba Controle, devem incluir:
    - Criar objeto *control*, caso o mesmo não tenha sido criado. Este objeto deve ser chamado toda vez que o *checkbox* **Salvar Informação** (*saveControl*) da Aba Controles for habilitada;
    - Salvar nome, descrição no objeto *control*;
    - Associar todo controle da ameaça ao objeto *riskAnalysis*;
    - Habilitar e limpar *text box* quando o botão **Novo Controle** (*newControlButton*) é acionado;
    - Retirar informações do controle atual e adicionar informações referentes ao controle anterior na *text box* e na lista de controles quando o botão **Próximo Controle** (*previousControlButton*) é acionado;
    - Apagar todas as referências ao objeto *control* quando o botão **Apagar Controle** (*deleteControlButton*) é acionado.

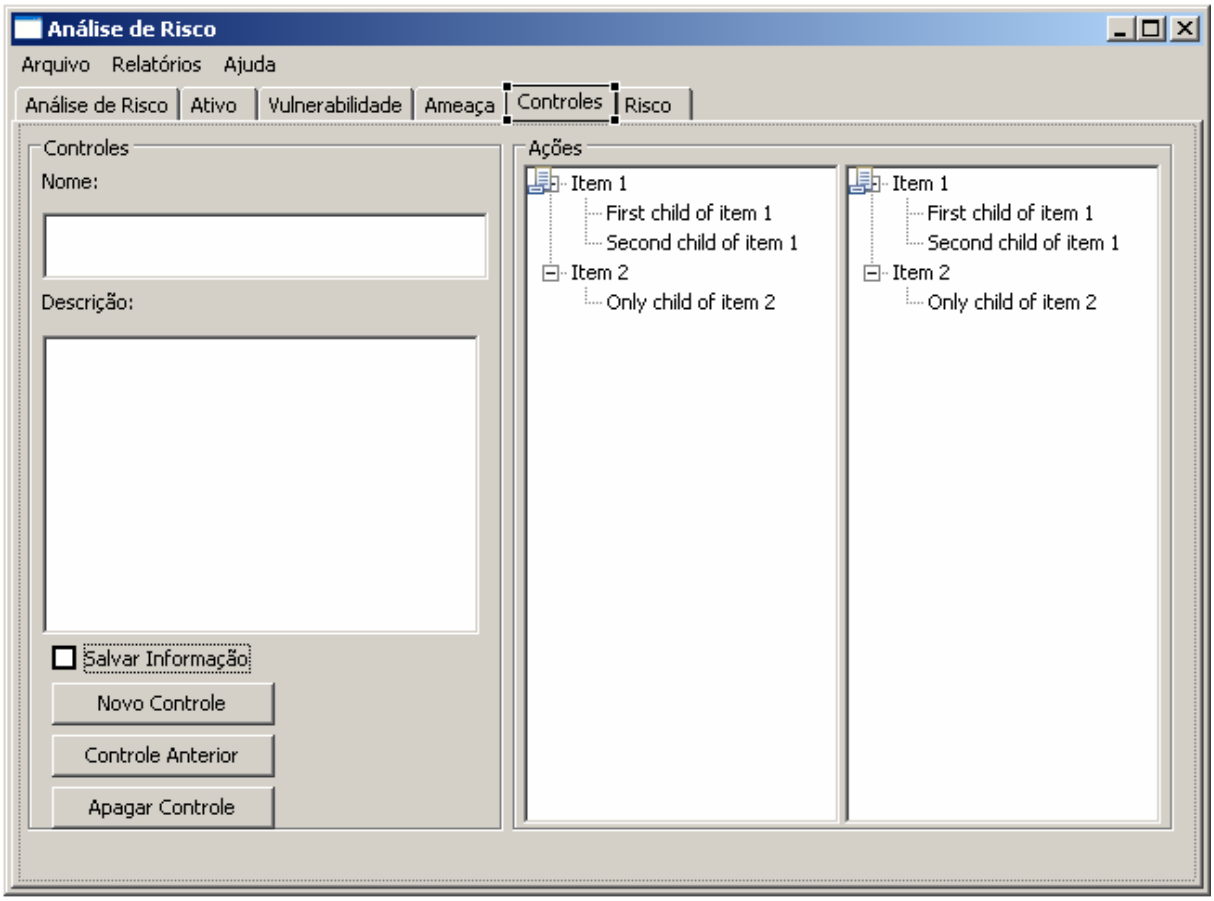

Figura 8 – Aba Controle

- Mitigação de um risco: Um controle deve ser capaz de atuar sobre uma ameaça ou sobre suas vulnerabilidades, mitigando o risco associado à determinada ameaça. Ação que atua sobre um controle só pode ser determinada após cadastrar e salvar as informações do controle. Os procedimentos dessa regra de negócio devem incluir:
    - Clicar na ameaça da lista de ameaças a serem mitigadas ou na vulnerabilidade da lista de vulnerabilidades;
    - Selecionar no *pop-up* menu, ilustrado na Figura 9 – Aba controle – Mitigando Ameaçae 10, que será aberto o tipo de mitigação que será realizada;
    - Instanciar objeto *control* e determinar a ação a ser mitigada;

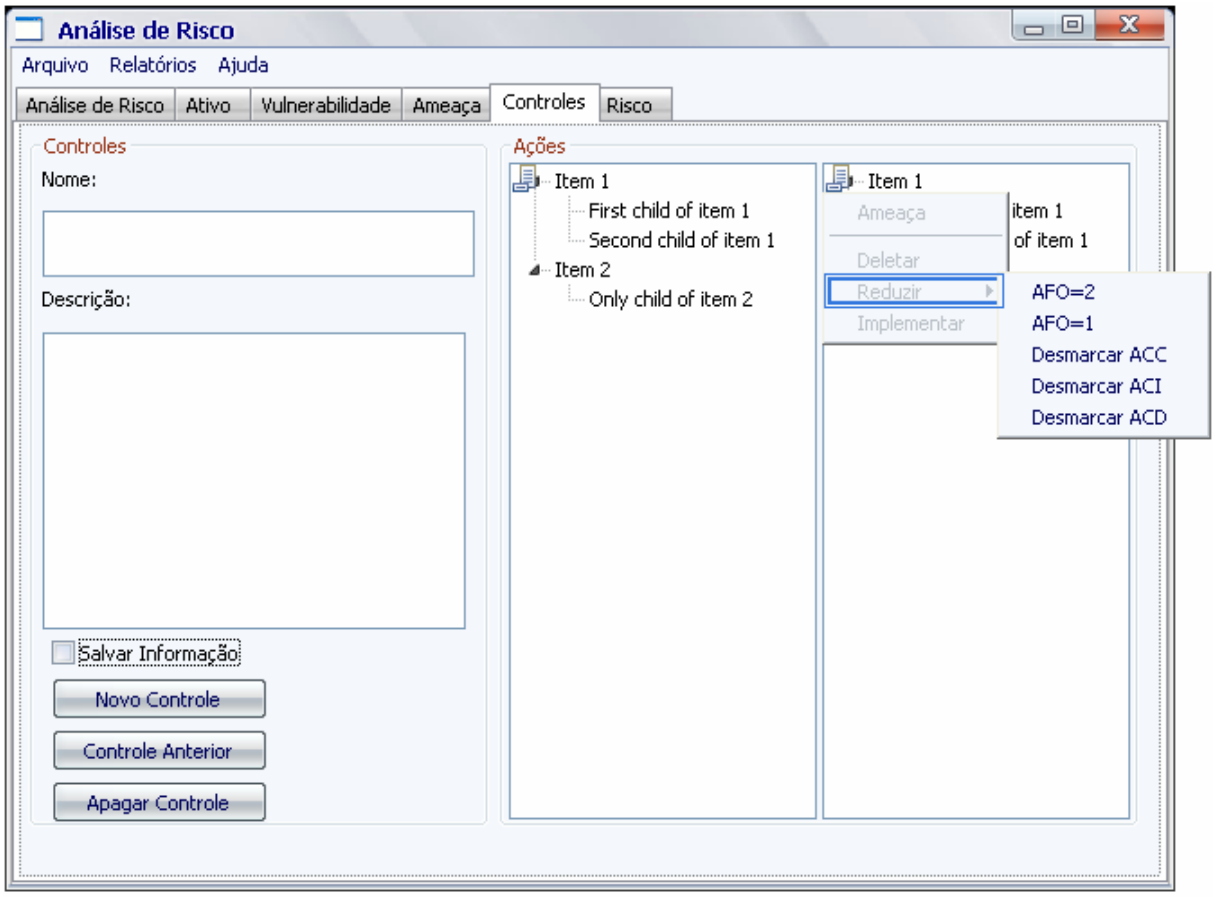

Figura 9 – Aba controle – Mitigando Ameaça

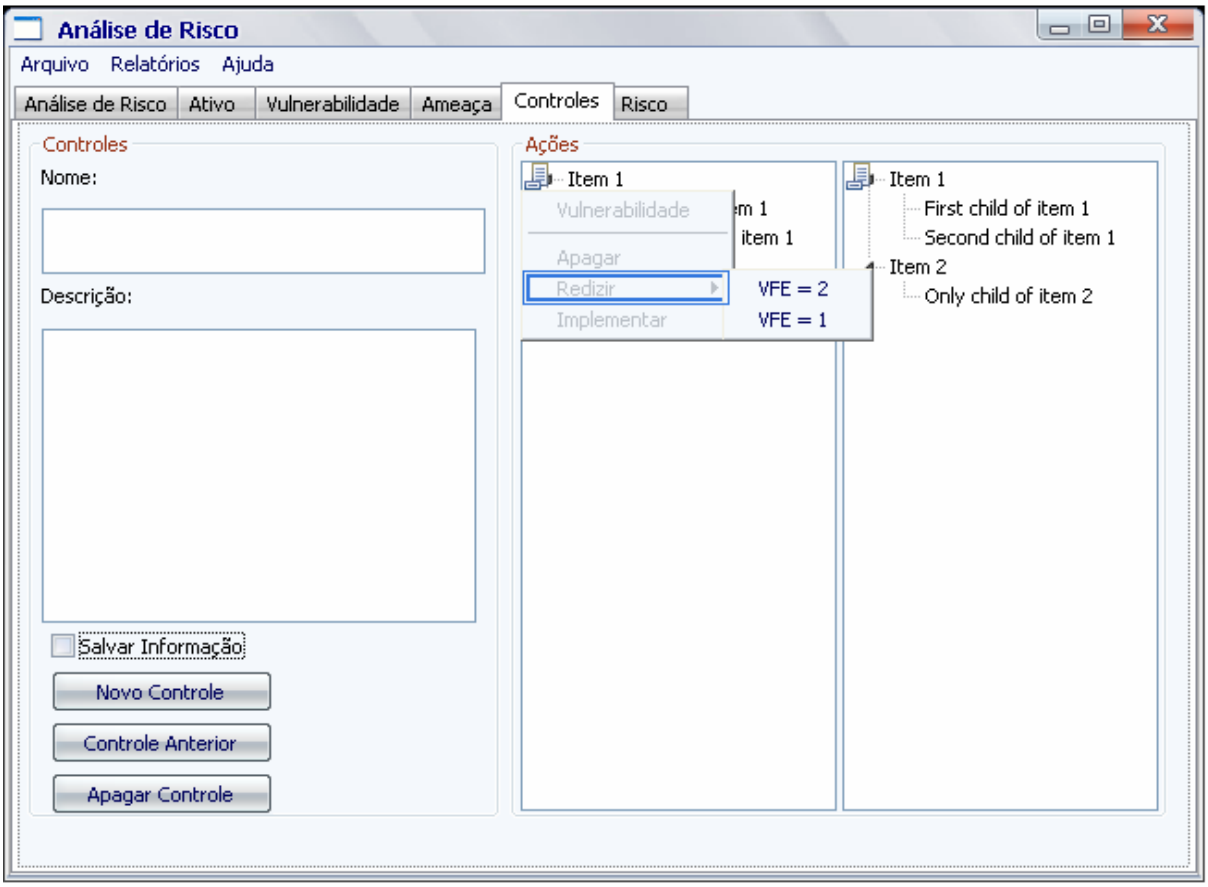

Figura 10 - Aba Controle – Mitigando Vulnerabilidade

- Seqüenciamento das Abas: A Aba Risco deve exibir os riscos que já foram calculados para determinada ameaça. Os riscos são calculados quando associamos uma ameaça à determinada(s) vulnerabilidade(s) ou quando mitigamos a ameaça. Os procedimentos dessa regra de negócio devem incluir:
    - Adicionar uma ameaça, associada ao seu risco inicial, assim que associamos essa ameaça a uma vulnerabilidade na Aba Ameaça;
    - Adicionar um risco residual a determinada ameaça, assim que mitigamos uma vulnerabilidade e/ou ameaça;
    - Adicionar um risco atual a ameaça, assim que determinado controle proposto for implementado;
    - Criar um arquivo XML com todas as ameaças associadas ao risco existentes, quando o botão **Exportar Risco** (*exportXML)* é acionado.
- Visualização dos Riscos: Aba devem ser abertas obedecendo à determinada seqüência, de forma a impedir que determinadas ações sejam efetuadas no momento indevido pelo usuário. Os procedimentos dessa regra de negócio devem incluir:

- Ao abrir o programa todas as *text box* e *combo box* devem se encontrar desabilitadas;
- Após iniciar uma nova análise ou abrir uma análise anterior, algumas abas são habilitadas;
- A aba análise de risco é a primeira a ser habilitada;
- A aba ativo só é habilitada após cadastrar e salvar a análise de risco;
- A aba vulnerabilidade só é habilitada após cadastrar e salvar um ativo;
- A aba ameaça só é habilitada após cadastrar e salvar uma vulnerabilidade;
- A aba controle só é habilitada após cadastrar uma ameaça.

5 Ferramentas utilizadas

5.1 Eclipse 3.4.0

Eclipse é uma IDE desenvolvida em Java e que começou como um projeto da IBM do Canadá e hoje é mantido pela Eclipse Foundation.

Atualmente o Eclipse é uma das plataformas de desenvolvimento em Java mais utilizadas por programadores, com características marcantes como a possibilidade de adição de *plug-ins* que permitem ao desenvolvedor modelar o Eclipse de acordo com suas necessidades.

No Eclipse é possível adicionar construção de UML, desenvolvimento de interface gráfica, etc.

O Eclipse foi utilizado no projeto pra implementação do código de forma totalmente satisfatória, se mostrando uma ferramenta robusta e amigável.

5.2 JUDE

JUDE é uma ferramenta de modelagem de UML [3] criada pela empresa Japonesa ChangeVision, atualmente é uma das ferramentas grátis para UML mais poderosas. Com características que não são encontradas nas outras ferramentas grátis, como adicionar métodos no diagrama de seqüência e a alteração se refletir no diagrama de classes.

O JUDE não possui um apelo gráfico tão bom quanto o Poseidon, ou tantas funcionalidades como Rational Rose, mas seu desempenho impressiona, principalmente tratando-se de uma ferramenta desenvolvida totalmente em Java e Swing.

O JUDE foi utilizado no projeto pra criar diagrama de casos de uso [1] e diagramas de UML [1], atendendo perfeitamente as necessidades do projeto.

5.3 WindowsBuilder – SWT Designer

O WindowsBuilder - SWT Designer é um plug-ins para o Eclipse para desenvolvimento de interface GUI. O SWT Designer gera código de interfaces gráficas com as bibliotecas SWT [5] e Swing.

O SWT foi utilizado para desenvolvimento de toda interface GUI integrado ao Eclipse, atendendo perfeitamente as necessidades do projeto.

5.4 JDOM

O JDOM é a biblioteca *open source* utilizada para modelagem de XML em Java. JDOM é uma integração entre a DOM e a SAX, suportando XPath e XSLT.

O JDOM é utilizado para exportar um arquivo XML, contendo todas as ameaças existentes e seus respectivos riscos.

6 Conclusão

O processo de desenvolvimento deste projeto permitiu a utilização das mais variadas áreas de conhecimento estudadas ao longo do curso de Engenharia Eletrônica e de Computação. Elas abrangeram conhecimentos de Engenharia de Software, programação e desenvolvimento GUI. Este processo foi importante para solidificar os conhecimentos adquiridos na faculdade.

A metodologia utilizada no projeto, a orientação a objeto, foi adequada para o caso e proporcionou que o projeto fosse desenvolvido de forma organizada e objetiva. Através dela conseguimos ver os pontos mais críticos do projeto, assim como planejar as melhores soluções.

Todas as ferramentas utilizadas no projeto atenderam plenamente aos objetivos do sistema, como a linguagem de programação Java e as bibliotecas gráfica SWT, em conjunto com a ferramenta *WindowsBuilder – SWT Designer*.

Algumas propostas futuras podem ser feitas para a melhoria do sistema como:

Geração de Relatório;

Persistência dos dados utilizando XML.

Portanto, pode-se afirmar que o trabalho mostrado neste projeto foi satisfatório, agregando conhecimento ao desenvolvedor, o que será de grande valor ao longo da vida profissional.

7 Referência Bibliograficas

[1] Pressman, Roger S - Software Engineering: A Practitioner's Approach, McGraw-Hill Science/Engineering/Math; 6 edition (2004)

[2] Horstmam, Cay – Big Java, Bookman (2004). Tradução Edson Furmankiewicz.

[3] Furlan, José Davi – Modelagem de Objetos através de UML, Makron Book, 1998.

[4] Introduction to the Collections Framework, http://java.sun.com/developer/onlineTraining/collections/ (Acessado em 25 de julho de 2008);

[5] SWT JFACE Eclipse, http://www.java2s.com/Code/Java/SWT-JFace-Eclipse. (Acessado em 08 de agosto de 2008)

[6] Information Security – Management System – Part 3: Guidelines for information security risk management (BS 7799-3:2006), British Standard Institute