ESTRATÉGIAS DE MITIGAÇÃO DE RISCOS DE SEGURANÇA DO AMBIENTE AGRIS•

Luiz Fernando Rust da Costa Carmo *(rust@nce.ufrj.br)* **Ricardo de Barros Costa** *(ricardocosta@nce.ufrj.br)*
Gustavo Alberto de Oliveira Alves ***(galberto@nce.ufrj.br)*** **Carlos Augusto Reis Junior** *(carlosjunior@nce.ufrj.br)*
Tiago Monteiro do Nascimento *(tiagomonteiro@nce.ufrj.br)*

Núcleo de Computação Eletrônica
Universidade Federal do Rio de Janeiro,
Caixa Postal 2324, 20001-970, Rio de Janeiro – RJ, Brasil

RESUMO

O Projeto AGRIS (Análise e Gerência de Risco em Segurança) visa à criação de um ambiente integrado de avaliação e gestão de riscos em segurança, consolidando e aprimorando funcionalidades inerentes às ferramentas atuais de segurança da informação, além de propor e avaliar novas funcionalidades, tais como metodologias para calculo de risco, plano estratégico de mitigação de riscos, etc. O ambiente AGRIS faz uso de uma base de dados unificada de vulnerabilidades e controles, gerada através da compilação automática das bases disponíveis pela comunidade de segurança da informação. Este artigo descreve três diferentes propostas de estratégias de mitigação de riscos, bem como a metodologia de avaliação que foi empregada para validação e análise comparativa destas propostas.

ABSTRACT

The AGRIS Project (Security Risk Analysis and Management) aims to develop an integrated environment for risks evaluation and analysis, consolidating and improving inherent functionalities from current security information best practices, and also proposing and evaluating new functionalities, such as new methodologies for risk calculus, risk mitigation strategic plan, etc. The AGRIS environment makes use of a unified database of vulnerabilities and controls, generated through an automatic compilation of available bases from the security information's community. This article describes three different proposals of risks mitigation strategies, as well as the evaluation methodology used for validation and comparative analysis of these proposals.

1 INTRODUÇÃO

A análise de risco, processo de avaliação das vulnerabilidades e potenciais ameaças de um sistema, é um componente essencial de um programa de gerência de segurança da informação. O processo de análise identifica as prováveis conseqüências, ou riscos associados com as vulnerabilidades do sistema, e gera a base para estabelecimento de um programa de segurança que seja custo-efetivo.

A avaliação dos riscos permite identificar as ameaças aos ativos (tudo que representa valor para o negócio – humanos, tecnológicos e físicos), as vulnerabilidades e as suas probabilidades de ocorrência, e também os seus impactos sobre as organizações (Crouhy, 2000). Quanto maior o conhecimento sobre os riscos, mais fácil de tomar a decisão de como tratá-los.

Basicamente, pode-se conduzir o tratamento do risco de três formas: aceitá-lo, reduzi-lo ou mesmo transferi-lo. É através da análise de risco que se tem informação suficiente para identificar qual das três opções melhor se aplica ao cenário, sempre levando em consideração os objetivos de negócio.

Atualmente, nenhum ambiente de análise de riscos de segurança da informação oferece uma solução sem costuras (*seamless*), integrando análise de vulnerabilidades, controles apropriados, riscos e estratégias de mitigação.

O principal objetivo do projeto AGRIS é gerar uma ferramenta integrada de suporte à segurança da informação, capaz de: (i) identificar ameaças, vulnerabilidades e impactos ao negócio das empresas, e (ii) gerar análises criteriosas, na forma de relatórios técnicos e executivos.

Um resultado essencial deste tipo de análise é o provimento de um plano de mitigação de riscos, ou seja, estabelecer uma correlação entre investimentos e riscos mitigados. Este artigo descreve três diferentes propostas de estratégias de mitigação de riscos, bem como a metodologia de avaliação que foi empregada para validação e análise comparativa destas propostas.

O resto deste artigo está estruturado da seguinte forma: a sessão 2 descreve sucintamente as principais funcionalidades previstas no ambiente AGRIS e sua composição arquitetural; o método de cálculo de risco adotado é apresentado na seção 3; a seção 4 descreve as propostas de estratégias para mitigação dos riscos; a seção 5 apresenta a metodologia de avaliação destas propostas e os resultados alcançados; e por último as conclusões e trabalhos futuros são apresentados nas seções 6 e 7.

• *Projeto financiado pelo Programa FRIDA - Fundo Regional para a Inovação Digital na América Latina e Caribe*

2 AMBIENTE AGRIS

2.1 Funcionalidades

A Tabela 1 fornece um panorama funcional das principais ferramentas de gerência de Risco de Segurança para a área de Tecnologia da Informação. Estas ferramentas cobrem alguns aspectos importantes na gerência de risco, mas não há nenhuma que ofereça todas as funcionalidades essenciais, o que provoca atualmente a necessidade do uso de mais de uma delas para uma completa realização de um processo de Gerência de Risco. Este procedimento pode levar a uma desnecessária repetição de testes (pelo fato dessas ferramentas possuírem características em comum) ou mesmo a uma possível incompatibilidade de resultados (pelo fato dessas ferramentas utilizarem métricas diferentes). A seguir são descritos as principais funcionalidades da ferramenta AGRIS

- *Visualização por ativos*

A ferramenta faz uso de um nível de abstração que permite ao usuário definir ações sobre cada ativo individualmente. Nessa mesma linha, os resultados da análise (vulnerabilidades encontradas e gráficos de tendência gerados) são mostrados por ativo. Como os prejuízos de uma empresa podem ser quantificados em termos de seus ativos (tecnológicos ou não), é importante que a ferramenta identifique quais ativos estão (ou não) dentro dos parâmetros estabelecidos pela empresa e, qual o prejuízo estimado para essa falta de conformidade.

- *Definição do valor do ativo*

Ativos iguais podem assumir diferentes graus de importância em diferentes empresas, mesmo quando estas empresas pertencem a segmentos de mercado semelhantes. Desta forma, para que a ferramenta reflita com fidelidade o impacto que a indisponibilidade do mesmo causaria, é

Tabela 1 - Quadro comparativo das principais ferramentas de análise de riscos

	Visual Assurance	**Compliance Guardian**	**Ecora**	**Check-up tool**	**Foundstone**	**BindView**
Visualização por ativos	Sim, *em árvore*	Não	Não, *nível Tecnologia*	Sim	Sim	Sim
Definição do valor do ativo (customização)	Não	Não	Não	Não	Sim	Não
Definição de políticas por ativos	Sim	Não	Não	Sim	Sim	Sim
Uso de Templates	Não	Não	Sim	Não	Sim	Sim
Benchmark e Conformidade	Não	Não	Não	Não	Não, *só interno*	Não, *só interno*
Relatórios (Empresariais)	Sim, *resumo*	Sim	Não	Sim, *Risk Wizard*	Sim	----
Relatórios (Técnicos)	Sim	Sim	Sim, *nível Tecnologia*	Sim	Sim, *detalhado*	Sim
Controle de Correções e falhas	Não	Não	Não	Não	Sim, *apenas Ticket*	Sim
Correção de Falhas	Não	Não	Sim, *patch manager*	Não	Não	Não, *módulo de migração*
Suporte a Sistemas Heterogêneos	Não	Sim	Sim	Não	Sim	Sim
Associação do Risco à KB	Sim	Não	Não	Sim	Sim	----
Atualização da KB	Sim	---	Não	Sim		----
Análise de Risco	Qualitativa e Quantitativa	Quant.	Quant.	Quant.	Qual. e Quant.	Quant.

necessário que além do valor de mercado que o ativo possua, seja possível realizar ajustes individualizados.

- *Definição de políticas por ativos*

  Além de uma visão especializada por ativo, é importante que a ferramenta também permita a definição de políticas diferenciadas para cada ativo de uma mesma empresa. Para isso, a ferramenta precisa prover informações sobre a maturidade (em termos de gerência e análise de risco em redes) de empresas do mesmo segmento, e de ativos, que possam pertencer, ou não, ao mesmo segmento.

- *Uso de templates*

  A configuração de uma ferramenta deste porte pode ser extremamente complexa, restringindo o uso da mesma a profissionais com razoável experiência em processos de análise de risco de segurança. Para que isso não seja um impeditivo ao uso da ferramenta, é necessário disponibilizar modelos básicos - *templates* - (baseados nos diferentes tipos de empresas) que sejam apropriados a todos os tipos de usuários da ferramenta. O uso de *templates* possibilita: (i) uma avaliação mais acurada da ferramenta no que diz respeito à adoção da mesma ou não; e (ii) um aprendizado sobre o uso da ferramenta e das técnicas de análise de risco, à medida que o modelo vai sendo ajustado à realidade da empresa.

- *Benchmarks e conformidade*

  É importante para uma empresa saber como a mesma está situada (no que diz respeito à gerência de risco – implementação de políticas e alocação de recursos) em relação a outras empresas do mesmo segmento. A comparação é uma importante fonte de inspiração para o processo de alocação de recursos em segurança, ou ainda na estratégia de marketing. Por isso a ferramenta deve fornecer diferentes subsídios sobre implementação de políticas de segurança:

  - comparação entre a empresa e outras do mercado;
  - comparação entre o momento atual da empresa e algum momento anterior;
  - comparação entre diferentes setores e/ou ativos da mesma empresa;
  - comparação com algum padrão pré-estabelecido (compliance).

- *Relatórios*

  O ponto crucial de uma ferramenta de análise de risco de segurança é a sua capacidade de apresentar os resultados das análises de uma forma completa e didática, de acordo com o público alvo a que estes se destinam. A partir destes resultados serão definidas as políticas que devem ser adotadas e a prioridade que cada uma deve ter. Como a linguagem utilizada por profissionais de TI, gerentes e executivos é diferente, os relatórios produzidos devem adequar-se a cada um desses grupos:

  - relatórios técnicos - informando com detalhes que dispositivos e qual o nível de exposição cada um possui, exemplos:
    - Gráficos: importância do ativo x dificuldade de implementação do controle;
    - Gráficos: ativo x nível de exposição.
  - Relatórios empresariais: relatórios com formatação e características próprias para empresários e administradores; exemplos:
    - Gráficos: custo x benefício na implementação de controles;
    - Gráfico gasto com segurança x retorno obtido.

- *Controle e correção de falhas*

  Além da identificação de riscos, é importante a prover estratégias de seleção e verificação dos controles apropriados para mitigar as vulnerabilidades encontradas. Tais estratégias devem ter a função de instruir, acompanhar a implementação dos controles, verificar se o controle foi corretamente aplicado e quais riscos foram mitigados. Para isso, deve-se integrar à ferramenta de análise de risco, todas as funcionalidades comumente encontradas em ferramentas de análise de vulnerabilidades. Este tipo de abordagem permite ao usuário interagir com apenas uma única ferramenta, criando um ambiente de análise "sem costuras" (*seamless*) - o que não é atualmente disponível em nenhuma ferramenta disponível no mercado. Para isso, outras características se fazem necessárias:

  - Disponibilização de uma KB - visando orientar o profissional de TI na correção de riscos encontrados é importante viabilizar um mecanismo de associação com documentos informativos sobre o problema e sua precisa correção;
  - Mecanismos para ampliação da KB - possivelmente alguma estratégia implementada por um profissional de TI pode não estar prevista em nenhuma KB e ainda assim se mostrar mais eficiente

que as existentes; para isso é prevista na ferramenta, uma interface para a atualização da KB, com informações geradas pelo próprio usuário;

- Sincronização da KB - é importante que a ferramenta possa sincronizar (com freqüência definida pelo usuário) sua base com a de um servidor central constantemente atualizada;
- Plano estratégico de mitigação dos riscos - estabelecer uma correlação entre investimentos e riscos mitigados.

2.2 Arquitetura

A ferramenta AGRIS está estruturada em três blocos principais: inicialização, processamento e gerenciamento (figura 1).

2.2.1 Inicialização

Provê todas as condições necessárias para a validação de usuários, configuração e execução da ferramenta. É responsável pelas seguintes funções:

- Valida acesso ao sistema;
- Cria ou recupera o escopo da aplicação;
- inicializa configurações;
- Verifica a integridade/disponibilidade da base do sistema e novas bases;
- Carrega os módulos de vulnerabilidades de acordo com o tipo de ativo selecionado;
- Carrega os controles de acordo com o tipo de ativo selecionado;
- Carrega as dependências entre vulnerabilidades e controles;
- Atualização remota da base de dados;

2.2.2 Processamento

Processamento das funcionalidades da ferramenta, sendo a sua execução customizada para cada cenário através de ajuste feitos pelos usuários. Funções:

- Carrega agentes de inspeção necessários;
- Verifica as vulnerabilidades/controles existentes;
- Executa análise selecionada;
- Calcula risco;
- Gera gráficos;
- Realiza compliance com norma de segurança;
- Realiza benckmark;
- Gera relatórios técnicos e gerencias;
- Mede nível de maturidade de segurança;
- Salva contexto do usuário;
- Salva os logs atualizados;
- Calcula custo de implementação dos controles;

2.2.3 Gerenciamento

Administração das configurações dos controles, vulnerabilidades, usuários, permissionamentos e da ferramenta em geral. Controla as funções de:

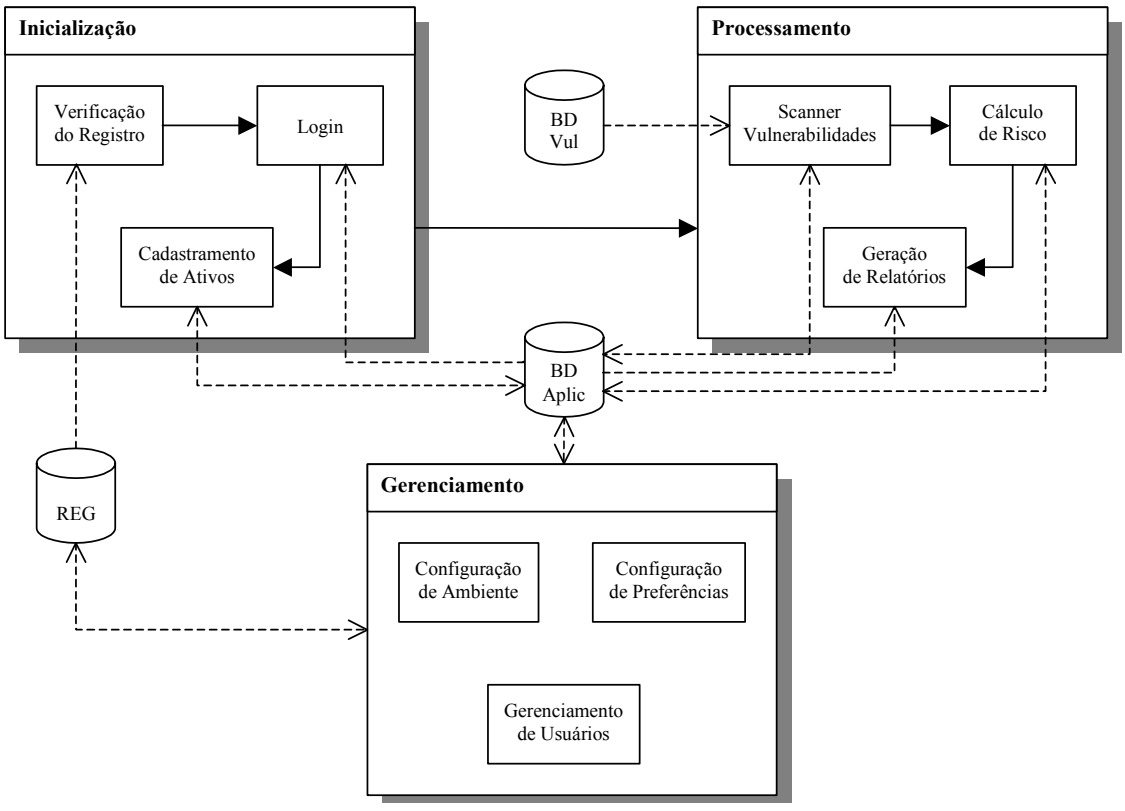

Figura 1 – Arquitetura da ferramenta AGRIS

- configurar controles (customização);
- customizar entradas e saídas;
- cadastrar usuários;
- definir permissão de usuários;
- Inserir ameaças, vulnerabilidades e controles específicos.

3. CÁLCULO DE RISCO

O método utilizado no Ambiente AGRIS tem como base o cálculo de risco sobre ativos utilizado pelo método de CRAMM (CCTA, 1991) - *Government's Risk Analysis and Management Method*.

A base do método é a dependência direta que o risco possui da tríade **ativo** (valor), **ameaças** e **vulnerabilidade**. Calcula-se o produto entre os valores associados à relevância do ativo, ao Impacto associado à vulnerabilidade, e a probabilidade que a mesma tem de ser explorada**.**

- A relevância de um ativo está associada à importância que o mesmo tem para a realização do negócio e/ou o prejuízo (normalmente em termos financeiros) que o mesmo trará caso seu serviço fique indisponível.
- O Impacto de uma vulnerabilidade é medido baseado em classificações realizadas por órgãos responsáveis por coletar informações sobre vulnerabilidades.
- A probabilidade de exploração é uma medida (normalmente empírica ou baseada em histórico de ocorrências) sobre a possibilidade que uma vulnerabilidade possui de ser explorada.

4. ESTRATÉGIAS DE MITIGAÇÃO DE RISCOS

Uma estratégia de mitigação de riscos é definida como um processo de seleção de controles (a ser implementado em um dado sistema de informação) de forma a minimizar os riscos residuais de segurança, em função de um orçamento pré-estabelecido. Nesta seção são propostas três diferentes estratégias: (i) orientada a ativo, (ii) orientada a controle de maior risco, (iii) orientada ao controle de menor custo.

4.1 Orientada a Ativo

Após o cálculo de Riscos, os ativos são classificados em ordem decrescente, em função do risco associado. Para cada ativo, investiga-se a vulnerabilidade de maior impacto e qual o controle de menor custo necessário para sua mitigação, atualizando o orçamento residual. Em seguida, verifica-se a possibilidade desse controle mitigar também outras vulnerabilidades deste mesmo ativo. Caso existam, atualiza-se risco o residual levando em conta a anulação destas vulnerabilidades. Este procedimento é repetido até que os riscos sejam eliminados ou o orçamento inicial seja exaurido.

pseudo-algoritmo:

- Enquanto (houver ativos com vulnerabilidades) e (orçamento > custo do menor controle aplicável):
  - Listar os ativos em ordem decrescente de vulnerabilidade e escolher o primeiro ativo da lista. Seja esse A;
  - Escolher a vulnerabilidade de A que apresenta maior impacto e probabilidade de exploração. Seja essa V;
  - Descobrir o controle de menor custo que mitiga a vulnerabilidade V. Seja esse C;
  - Retirar da lista de vulnerabilidades de A todas as vulnerabilidades mitigadas por C;
  - Diminuir do Orçamento o custo associado ao controle C;
  - Diminuir o Risco total do risco mitigado em A por C;
- Ao final tem-se o total de risco mitigado e o custo total para isso.

4.2 Orientada a controle de maior risco

Nesta estratégia, ao invés de uma ordenação dos ativos em função dos riscos associados, ordena-se os controles segundo a soma dos riscos que os mesmos eliminariam em cada um dos ativos analisados. A partir dessa lista, os controles são eliminados sequencialmente, sendo que o custo de implementação de cada controle é debitado do orçamento residual. Este procedimento é repetido até que riscos sejam completamente eliminados ou o orçamento inicial seja exaurido.

pseudo-algoritmo:

- Enquanto (houver ativos com vulnerabilidades) e (Orçamento > custo do menor controle aplicável):
  - Descobrir o controle que mitiga o maior Risco. Seja esse C;
  - Descobrir o ativo que possui esse risco. Seja esse A;
  - Retirar da lista de vulnerabilidades de A todas as vulnerabilidades mitigadas por C;
  - Diminuir do Orçamento o custo para implementação do controle C;
  - Diminuir o Risco total do risco mitigado em A por C;
- Ao final gera-se o total de risco mitigado e o custo total para isso.

4.3 Orientada a controle de menor custo

Essa estratégia se apóia em duas considerações: custo de implementação do controle e ativo de maior risco eliminado com a aplicação desse controle.

Inicialmente, os controles são listados em ordem crescente de custo. Escolhe-se o controle de menor custo e ordena-se decrescentemente os ativos eliminados pela implementação desse controle.

O custo da implementação do controle é computado e o ativo em questão é retirado da lista. Caso a lista fique vazia (não existem mais ativos cuja implementação desse controle é necessária), o controle em questão é retirado da lista e um novo controle é escolhido, segundo os mesmos critérios de escolha do controle inicial.

Os critérios de parada desse método, em ordem de verificação, são:

- o orçamento atual destinado à mitigação é menor que o custo de implementação do controle de menor custo;
- não existem mais controles de possível utilização;
- não existem mais riscos a serem mitigados.

pseudo-algoritmo:

- Enquanto (houver ativos com vulnerabilidades) e (Orçamento > custo do menor controle aplicável):
  - Descobrir o controle de menor custo. Seja esse C;
  - Descobrir o maior risco associado a esse controle Seja esse R;
  - Descobrir o ativo de maior valor (relevância) que possua o Risco R. Seja esse A;
  - Retirar da lista de vulnerabilidades de A todas as vulnerabilidades mitigadas por C;
  - Diminuir do Orçamento o custo para implementação do controle C;
  - Diminuir o Risco total do risco mitigado em A por C;
- Ao final teremos o total de risco mitigado e o custo total para isso.

5 AVALIAÇÃO DAS ESTRATÉGIAS

A metodologia empregada para uma avaliação comparativa das diversas estratégias é baseada na estimativa de risco residual não mitigado em cada estratégia, quando apenas uma porcentagem pré-determinada do orçamento total necessário para uma completa mitigação dos riscos esteja disponível (denominada perTot).

Para isso foi concebido um simulador de cenários aleatórios que retorna o risco residual em função da variável de entrada **perTot.**

5.1 Simulador de cenários aleatórios

Cada cenário de uma das iterações da simulação é caracterizado por um conjunto de variáveis cujos valores são arbitrados:

- O número total de ativos (A);
- O número total de vulnerabilidades (V);
- O número total de controles (C);
- Porcentagem para cálculo do montante disponível para mitigar riscos (perTot).

Com base nessas variáveis são criadas as seguintes matrizes:

- Valor de um ativo
  vetor de tamanho A com valores escolhidos uniformemente do conjunto inteiro {1, 2, ..., 10};

- Impacto de vulnerabilidade
  vetor de tamanho V, cujos valores são escolhidos aleatoriamente do conjunto {1, 3, 5, 7,9}, sendo considerado a seguinte associação:
  - Muito Baixo (MB) = 1;
  - Baixo (B) = 3;
  - Médio (M) = 5;
  - Alto (A) = 7;
  - Muito Alto (MA) = 9;

- Probabilidade de Exploração
  vetor de tamanho V cujos valores são escolhidos uniformemente no intervalo [0,1];

- Custo de cada controle
  vetor de tamanho C cujos valores são escolhidos uniformemente no intervalo (0,100];

- Associação entre ativo e vulnerabilidade
  dada pela matriz M_{AXV}, onde:
  - a_{ij} tem o valor escolhido segundo experimentos de Bernoulli (sucesso-fracasso, onde sucesso=1 e fracasso=0);
  - $a_{ij} = 1 \rightarrow$ Ativo i possui a vulnerabilidade j;
  - $a_{ij} = 0 \rightarrow$ em caso contrário;
  - $i \in \{1, ..., A\}$;
  - $j \in \{1,...,V\}$;

- Associação vulnerabilidade e probabilidade de exploração dada pelo vetor M_{1xV}, onde:
  - a_{1j} tem o valor escolhido entre [0,1];
  - $j \in \{1,...,V\}$;

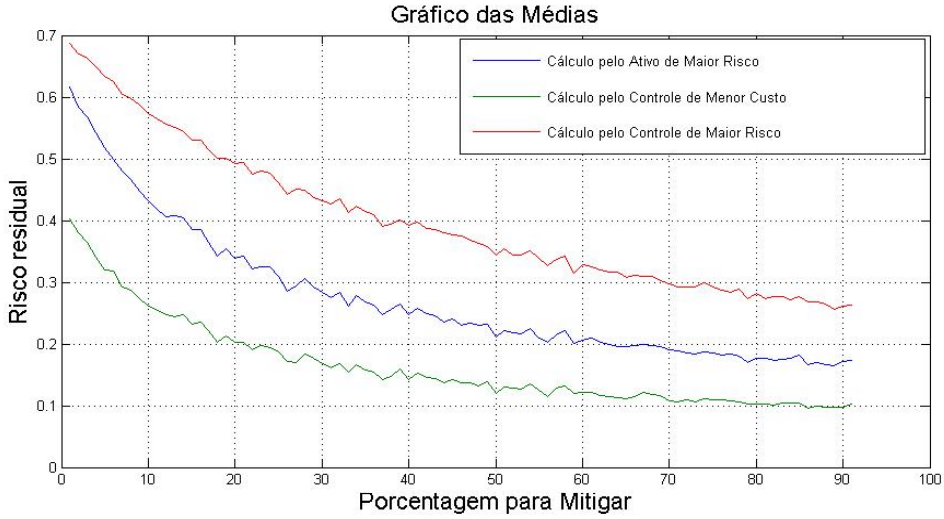

Figura 2 – Risco Residual x Porcentagem para mitigar

- Associação controle e vulnerabilidade dada pela matriz M_{CXV}, onde:
  - a_{ij} tem o valor escolhido segundo experimentos de Bernoulli (sucesso-fracasso, onde sucesso=1 e fracasso=0);
  - $a_{ij} = 1$ → Controle i mitiga a vulnerabilidade j;
  - $a_{ij} = 0$ → Caso contrário;
  - $i \in \{1,...,C\}$;
  - $j \in \{1,..., V\}$;

- Associação controle e custo dada pela matriz M_{1xC}, onde:
  - a_{1j} tem valor escolhido aleatoriamente entre (0,100];
  - $j \in \{1,..., C\}$;

- O Montante para mitigar é estimado segundo a regra:
  - Montante = 0,01*perTot * Σc_i ;
  - c_i → custo do controle i, $i \in \{1,..., C\}$.

5.2 Resultados

Para a avaliação comparativa das três estratégias de mitigação, é necessário verificar o comportamento de cada estratégia em função do orçamento disponível. Para isso varia-se perTot entre {5,6,...,95}, sendo que para cada valor de perTot o simulador de cenário aleatório é executado mil vezes, calculando a média e o desvio padrão do Risco residual em função de perTot.

A figura 2 mostra o resultado do processo de simulação. Pode-se verificar que para quaisquer valores de percentual do orçamento escolhido, a estratégia orientada ao custo do controle exibe sempre riscos residuais significativamente menores.

6 CONCLUSÃO

A estratégia orientada ao controle de menor custo apresentou, em todos os cenários, o melhor resultado para quaisquer valores de ativo, vulnerabilidade, e controle, sendo portanto a estratégia adotada no ambiente AGRIS para geração do plano de mitigação de riscos.

É importante ressaltar que um outro resultado importante da própria execução da estratégia orientada ao controle de menor custo é um plano seqüencial de ações corretivas, ou seja, a ordenação e classificação dos controles a serem utilizados após o cálculo de risco. Esta seqüência de ações pode ser vista como um vetor onde cada elemento é um par ordenado (C_i,A_j), indicando "aplicar o controle i no ativo j", de forma a mitigar o maior risco, dentro do orçamento disponível para esse propósito.

7 TRABALHOS FUTUROS

Como os gráficos provenientes da simulação tiveram comportamentos bem próximos de curvas exponenciais, mesmo para escolhas aleatórias de A, V e C, pode-se vislumbrar o desenvolvimento de um modelo matemático relacionando diretamente o total de investimento para mitigação de risco com o total de risco mitigado. Esse tipo de modelagem permitiria estabelecer funções de maximização do investimento para mitigação dos riscos.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERTS, Christopher, DOROFEE, Audrey, "Managing Information Security Risks: The OCTAVE Approach", 2002, Ed. Addison-Wesley;

CCTA, "CRAMM User's Guide (Version 2.0)", 1991, Technical Report, The UK Central Computer and Telecommunications Agency;

CROUHY, Michel, MARK, Robert, GALAI, Dan, "Risk Management", 2000, Ed. Mc-Graw-Hill;

ELOFF, M.M. & VON SOLMS, S. H. Information security management: A hierarchical framework for various approache, Computers and Security, 19(3):243-256, 2000;

HALLIDAY, S., BADENHORST, K. & VON SOLMS , "A business approach to effectively information technology risk analysis and management", Information Management and Computer Security, 4(1):19, 1996;

JOSANG, A., BRADLEY D., KNAPSKOG, S. J., "Belief-Based Risk Analysis", 2004, Norwegian, Technical report, Department of Telematics, University of Science and Technology;

PELTIER, Thomas R., 'Information Security Policies and Procedures: A Practitioner's Reference", Sec. Edition, 2004, Ed. Auerbach publications;

PRITCHARD, Carl, "Risk Management: Concepts and Guidance", 2001, Ed. ESI International, 218 p;

WOOD, Charles Cresson, "Information Security Policies Made Easy Version 9", 2002, Ed. Information Shield.