PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE INFORMÁTICA
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ANDREY BEVILACQUA
JÔNATAS JOSUÉ KIRSCH

VIA ANÁLISE:
Ferramenta de Auxílio à Análise de Riscos de Segurança da Informação e Comunicações em Organizações da Administração Pública Federal

Porto Alegre
2013

ANDREY BEVILACQUA
JÔNATAS JOSUÉ KIRSCH

VIA ANÁLISE: Ferramenta de Auxílio à Análise de Riscos de Segurança da Informação e Comunicações em Organizações da Administração Pública Federal

Monografia de trabalho de conclusão de curso de graduação apresentado à Faculdade de Informática da Pontifícia Universidade Católica do Rio Grande do Sul, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Professor orientador: Prof. Me. Leonardo Garcia de Mello

Porto Alegre
2013

RESUMO

A gestão de riscos de segurança da informação pode vir a ser uma atividade dispendiosa para a organização, observados os controles necessários e sua implementação de forma efetiva. Atualmente, as organizações lidam com uma grande quantidade de ameaças que, em sua maioria, podem eventualmente concretizar-se devido a falta de um processo adequado para a análise e gestão dos riscos. A necessidade de mapear previamente os riscos e preveni-los é uma necessidade atual e de extrema importância para as organizações, assim, minimizando ao máximo suas ocorrências e seus possíveis impactos.

Este trabalho trata da criação de um sistema de informação que facilita a atividade de análise de riscos, o qual segue as diretrizes da Norma Complementar número 04/IN01/DSIC/GSIPR. Ele possui as funcionalidades de mapeamento dos ativos, riscos, ameaças, controles, critérios de avaliação e aceitação de risco, definição de probabilidade de ocorrência de cada risco e do impacto caso esse risco se concretize. Como saída, a ferramenta gera relatórios contendo análise, avaliação e proposta de tratamento dos riscos.

Palavras-chave: Segurança da informação. Análise de riscos.

ABSTRACT

The risk management of information security can be an expensive activity for the organization owing to necessary controls and its effective implementation. Currently organizations deal with a large number of threats which the most part of them can eventually happen due to inexistence of an appropriate process for risk analysis and risk management. The need to map previously risks and preventing them is a current need and is extremely important for organizations, thus minimizing their occurrence and their potential impacts.

This work involves the creation of an information system that facilitates the activity of risk analysis, which follows the guidelines of the Standard Supplementary 04/IN01/DSIC/GSIPR. It has the functionality mapping of assets, risks, threats, controls, criteria for evaluation and acceptance of risk, definition of probability of each risk and the impact whether the risk becomes reality. As output, the tool generates reports containing analysis, proposal evaluation and treatment of risks.

Keywords: Information Security. Risk Analysis.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Cada organização pode vir a apresentar peculiaridades no que tange a técnicas e controles para gestão de riscos de segurança da informação e comunicações. Por exemplo, empresas brasileiras que possuam capital aberto em bolsas de valores norte-americanas devem atender os requisitos de controle da Lei Sarbanes-Oxley. Ao levarem-se em conta as características dos órgãos e entidades da administração pública federal, direta e indireta, bem como um conjunto de melhores práticas, tornou-se necessário aos integrantes desse grupo seguirem o disposto na Norma Complementar nº 04/IN01.

Essa norma foi editada pelo Departamento de Segurança da Informação e Comunicações (DSIC), órgão vinculado diretamente ao Gabinete de Segurança Institucional da Presidência da República (GSIPR). Seu objetivo é especificar diretrizes a serem observadas na gestão de riscos vinculados à Tecnologia da Informação e Comunicações.

Todavia, a gestão de riscos de segurança da informação pode ser uma tarefa dispendiosa em vista dos controles eventualmente implementados de modo efetivo. Isso deverá ser feito de modo criterioso, posto que sempre incorrerá algum ônus e raramente conseguirá abranger todas as ameaças às quais uma organização está sujeita.

Segundo publicação do Comitê Gestor da Internet no Brasil (CGI.br), somente em 2012 já foram reportados mais de duzentos mil incidentes de segurança da informação (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012a). Neste cenário de intensos e constantes ataques pela internet, as questões relacionadas a segurança da informação devem ser tratadas como tema sensível nas organizações governamentais. E as questões estratégicas da área de Tecnologia da Informação devem ser discutidas e tratadas de maneira a aprimorar os mecanismos de gestão governamental, visando à melhoria contínua da qualidade dos processos internos e dos serviços prestados à população.

Dessa forma, faz-se necessário a análise, avaliação e tratamento dos riscos, bem como a elaboração sistemática de relatórios para os Gestores de Segurança da Informação e Comunicações. Em seu conteúdo deve constar a análise quanto à

aceitação dos resultados obtidos, e consequente proposição de ajustes e de medidas preventivas e proativas à Alta Administração.

Idealmente, as tarefas de análise de riscos e geração dos respectivos relatórios poderiam ser realizadas com a máxima eficiência através do apoio de um sistema automatizado para essa tarefa. Isso representaria uma sensível melhora no cumprimento dessa obrigação para todo um conjunto de organizações públicas.

Contudo, a análise e gestão de riscos para a segurança da informação tornou-se vital para as organizações, pois a informação é o ativo mais importante para elas. Uma informação confidencial que acabe sendo divulgada põe em risco toda uma possível estratégia da organização, pode impactar em seu futuro, ou gerar uma enorme vantagem competitiva para seus concorrentes.

Devido a isso, a gestão de riscos dos ativos definidos e utilizados dentro da entidade é de extrema importância. Todos os ativos tem um risco que deve ser definido conforme sua probabilidade de ocorrência e seu impacto. Tendo esses dados em vista, é possível direcionar os investimentos da forma correta, a fim de minimizar ou evitar grande parte das ameaças aos ativos definidos como mais prioritários.

Como exemplo da importância da gestão de riscos, pode-se citar a descoberta de uma falha de segurança no *Bilhete Único*, sistema público de transporte coletivo de São Paulo. Trata-se de um meio de incluir créditos em um cartão e dessa forma utilizá-lo sem pagar (BRANCATELLI; RIBEIRO, 2012). Apontado como “infalível” em 2005 e fonte de uma receita de mais de trezentos milhões de Reais por mês, o sistema é considerado o segundo maior sistema de bilhetagem eletrônico do mundo, atrás apenas do cartão *Octopus* do transporte público de Hong Kong. Tal falha exemplifica a não mitigação de um risco com baixa probabilidade de ocorrência, porém alto impacto. Contudo, a análise e gestão dos riscos do *Bilhete Único* deveriam indicar maiores esforços à minimização dessa ameaça.

Para facilitar o trabalho de análise e gestão dos riscos dos ativos, foi desenvolvida uma ferramenta que auxilia em: mapeamento dos ativos, mapeamento dos riscos, definição de probabilidade para cada risco, do impacto caso esse risco se torne realidade e a forma na qual a entidade deve exercer suas atividades de prevenção de risco. A criação dessa ferramenta vai ao encontro do princípio da *eficiência* previsto no Artigo 37 da Constituição Federal (BRASIL, 1988): “A

administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência". Aliás, trata-se do mais recente princípio da Administração Pública, pois foi inserido no texto constitucional apenas em 1998, pela Emenda Constitucional nº 19, ao contrário dos demais princípios que já constavam na redação da Constituição desde a data da sua promulgação. A ferramenta ajuda na automação de todo o processo de gestão de riscos dos ativos de segurança da informação, tornando-o mais viável - em relação a tempo e custo de execução - para a organização e disseminando a cultura de gestão de riscos ao mostrar a sua importância e os resultados obtidos no final do processo.

2 OBJETIVOS

Este capítulo apresenta o objetivo geral e os objetivos específicos que devem ser alcançados neste trabalho de conclusão de curso.

2.1 OBJETIVO GERAL

O objetivo do trabalho de conclusão proposto é desenvolver um sistema de informação capaz de auxiliar na análise de riscos dos ativos de segurança da informação e comunicações em órgãos e entidades da Administração Pública Federal, seguindo as diretrizes da Norma Complementar nº 04/IN01/DSIC/GSIPR.

2.2 OBJETIVOS ESPECÍFICOS

a) Revisar a bibliografia sobre gestão de riscos;
b) Revisar a bibliografia sobre análise e mapeamento de riscos, obtendo um maior conhecimento sobre o processo de tomada de decisão a respeito das atividades;
c) Revisar a bibliografia sobre avaliação e impacto de risco, no intuito de definir os métodos a serem implementados na ferramenta *Via Análise*;
d) Revisar a bibliografia sobre estimativa de riscos, com o objetivo de definir o cálculo de avaliação da probabilidade e gravidade dos riscos a serem implementados na ferramenta *Via Análise*;
e) Revisar a bibliografia sobre segurança da informação e comunicações;
f) Revisar a bibliografia sobre a Norma Complementar nº 04/IN01/DSIC/GSIPR;
g) Revisar a bibliografia sobre a Norma Brasileira ABNT NBR ISO/IEC 27001;
h) Revisar a bibliografia sobre a Norma Brasileira ABNT NBR ISO/IEC 27002;
i) Analisar a relação risco/impacto na gestão de riscos;
j) Estudar as ferramentas de análise de riscos existentes;
k) Especificar, projetar e desenvolver um sistema de auxílio à análise de riscos de segurança da informação e comunicações em órgãos e entidades da Administração Pública Federal.

3 EMBASAMENTO TEÓRICO

Este capítulo aborda tópicos para entendimento da motivação que envolve os objetivos a serem alcançados, apresentando os conceitos que serão utilizados.

3.1 ATIVO DE INFORMAÇÃO

A Norma Complementar nº 04/IN01/DSIC/GSIPR (BRASIL, 2009, p. 2) conceitua ativos de informação como “os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.”

Beal (2005, p. xi) apresenta ativo de informação como “qualquer dado ou informação a que esteja associado um valor para o negócio.” Segundo ela, “representam ativos de informação as informações relevantes mantidas na mente dos tomadores de decisão, em base de dados, arquivos de computador, documentos e planos registrados em papel, etc.”

Como exemplos de ativos de informação ligados a segurança da informação e comunicações, pode-se citar mídia digital, impressa ou escrita, equipamentos compostos por unidade de armazenamento, dispositivos digitais móveis e pessoas.

É necessário contabilizar todos os ativos de informação, o que significa organizá-los em um inventário de ativos, documento em que consta a relação de todos os ativos e as informações necessárias para a recuperação das informações em caso de perda. Além disso, é necessário realizar o uso de um sistema de classificação da informação para indicar a importância, prioridade e nível de proteção do ativo. A classificação da informação permite determinar de forma mais precisa os requisitos de tratamento e proteção a eles aplicáveis (BEAL, 2005).

A frase a seguir complementa:

> A classificação da informação e dos ativos associados de acordo com seus requisitos de segurança possibilita que haja uma diferenciação nos recursos usados para armazenar a informação e nos controles aplicados para protegê-la, gerando importantes economias e ganhos de produtividade para a organização (BEAL, 2005, p. 61).

Um ativo pode apresentar exigências referentes a um objetivo e ao mesmo tempo dispensar maiores precauções referentes a outro (relação de probabilidade e

impacto). É o caso, por exemplo, dos dados de acesso a um sistema interno da organização, os quais se forem perdidos, podem causar um impacto pequeno para a organização, mas causariam grande dano se esse acesso fosse realizado por alguém não autorizado e mal intencionado. Portanto, um ativo pode ter características diferentes perante outros ativos, mesmo que eles pertençam à mesma área da entidade que está realizando a análise dos ativos.

3.2 INCIDENTE DE SEGURANÇA

O dicionário Novo Aurélio Século XXI descreve o significado de incidente:

> [...] 1. Que incide, ocorre, sobrevém; superveniente. 2. *E. Ling*. Diz-se da oração acessória que se liga por pronome relativo a uma das palavras da oração principal a fim de completar-lhe a significação. *S. m.* 3. Circunstância acidental; episódio; aventura, peripécia [...]. (FERREIRA, 1999, p. 1092)

"Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores." (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012b, p. 50)

Alguns exemplos de incidentes de segurança são:

> [...] tentativa de uso ou acesso não autorizado a sistemas ou dados, tentativa de tornar serviços indisponíveis, modificação em sistemas (sem o conhecimento ou consentimento prévio dos donos) e o desrespeito à política de segurança ou à política de uso aceitável de uma instituição. (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012b, p. 50)

3.3 AMEAÇA

Ameaça é o "conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (BRASIL, 2009, p. 3). Segundo Beal (2005, p. 14), ameaça é a "expectativa de acontecimento acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação."

As ameaças que implicam em informações e ativos de informação podem ser classificadas como:

> Ambientais – naturais, como fogo, chuva, raio, terremoto ou decorrentes de condições do ambiente, como interferência eletrônica, contaminação por

> produtos químicos, falhas no suprimento de energia elétrica ou no sistema de climatização;
> Técnicas – configuração incorreta de componentes de TI e falhas de hardware e software;
> Lógicas – códigos maliciosos, invasão de sistema;
> Humanas – erro de operação, fraude, sabotagem. (BEAL, 2005, p. 18)

A ameaça, sendo acidental ou proposital, é a fonte geradora de um acontecimento indesejado. Podem-se constituir as ameaças intencionais como sendo ameaças propositais, as quais são desenvolvidas com o propósito de prejudicar seu alvo, em um ou vários aspectos, como por exemplo, ameaças voltadas a fraudes.

As ameaças não-intencionais são aquelas que podem ocorrer de diversas formas. Uma delas é a que não teve intervenção humana, como por exemplo uma ameaça ambiental, como chuva, raio ou terremoto. Ela pode ser também um erro de operação, o qual não foi gerado propositalmente.

3.4 VULNERABILIDADE

Vulnerabilidade é definida pela Norma Complementar nº 04/IN01/DSIC/GSIPR (BRASIL, 2009, p. 3) como o “conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.”

As vulnerabilidades são exploradas pelas ameaças para atingir alvos de ataque. Neste contexto Beal (2005), acredita que as vulnerabilidades determinam se um ativo de informação, ambiente ou sistema estão expostos à determinada ameaça.

Como exemplo de vulnerabilidade, pode-se citar a existência de controles de acesso inadequados, o que pode levar a ameaça de acesso não autorizado. Entretanto, um ativo também pode estar vulnerável a fatores externos, tais como fogo, inundações, entre outros desastres naturais. Dessa forma, é importante a existência de um ambiente estável, tanto para os *hardwares* quanto para os *softwares*.

3.5 IMPACTO

Beal (2005, p. 14) conceitua impacto como “efeito ou consequência de um ataque ou incidente para a organização.”

Destaca-se os aspectos a seguir:

> Três fatores afetam o impacto: sua natureza, seu escopo e seu tempo de ocorrência. A natureza do risco indica os problemas prováveis se ele ocorrer. O escopo de um risco combina a gravidade com sua distribuição global. O tempo de ocorrência de um risco considera quando e por quanto tempo o impacto será sentido (PRESSMAN, 1995, p. 134).

Em suma, se as consequências do risco são conhecidas e também a probabilidade de eles ocorrerem, pode-se estimar o impacto do risco sobre o projeto e o ativo. Esse impacto tem relação direta com o tempo gerencial a ele dedicado. Obtendo-se todas as informações levantadas, pode-se obter a precisão global da projeção do risco.

Como exemplo, pode-se considerar a ameaça de falha de software, a qual tem o software como ativo vulnerável. Caso pessoas não autorizadas invadam o sistema, esse fato ocasiona um impacto: pode haver a divulgação indevida de informações. Neste caso, a análise de riscos pode considerar que se trata de um risco de gravidade alta, bem como um impacto alto, os quais tendem a aumentar caso não haja esforço para minimizar o tempo de ocorrência do risco.

3.6 CONTROLES

Os controles têm como objetivo proteger os ativos contra ameaças de segurança. Todavia, os ativos não podem ser controlados apenas com dispositivos físicos, como cadeados, alarmes ou guardas de segurança. É necessária a existência de procedimentos e medidas para proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por pessoas ou por outros programas de computador. Desta forma, controle é qualquer mecanismo administrativo, físico ou operacional capaz de tratar os riscos da ocorrência de um incidente de segurança.

Para alcançar a segurança da informação é preciso identificar quais controles são necessários para mitigar riscos associados aos ativos. A identificação evita custos e retrabalho com duplicação de controles e assegura que os mesmos estejam funcionando de forma adequada e tratando os riscos de forma desejada. Contudo, essa atividade tem por saída a lista de todos os controles existentes e planejados, sua implantação e status de utilização.

3.7 RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

O Departamento de Segurança da Informação e Comunicações (BRASIL, 2009, p. 3) conceitua:

> Riscos de Segurança da Informação e Comunicações - potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

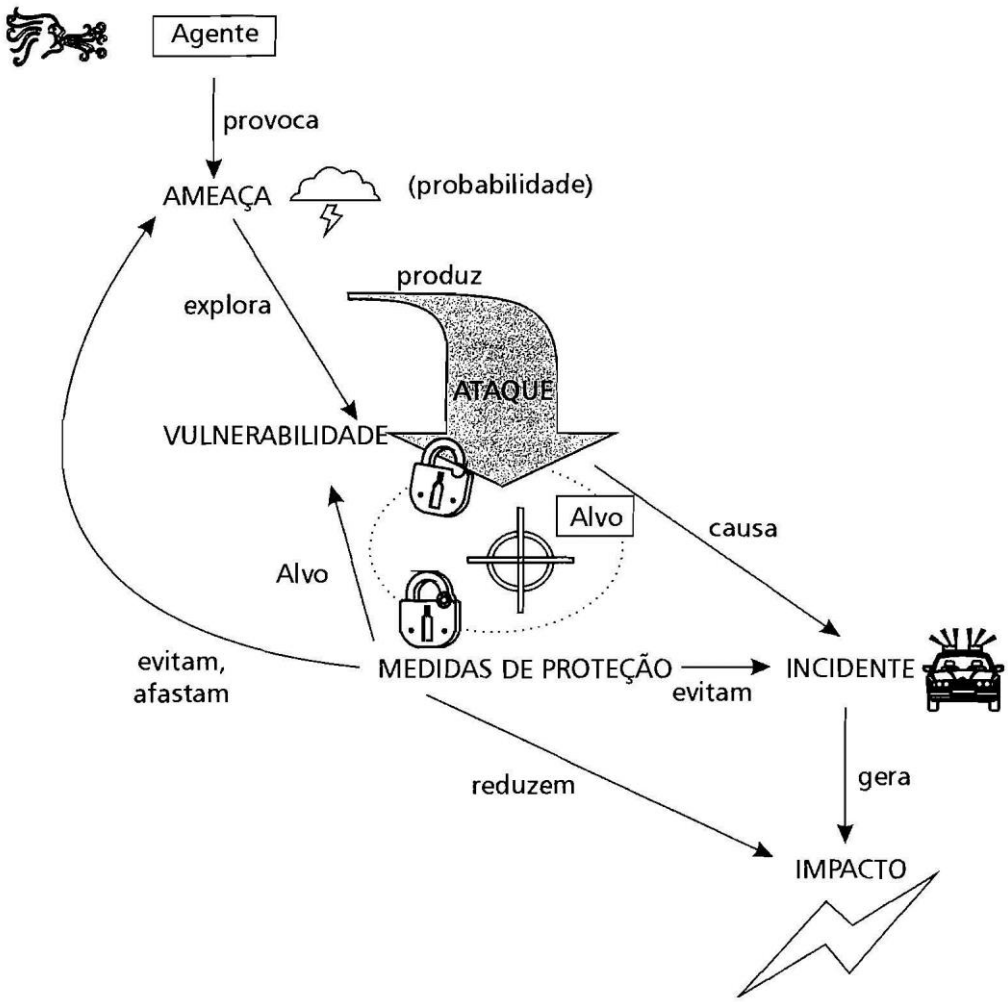
Segundo Weege (2012):

> Um risco existe quando uma ameaça, com potencial para causar algum dano, possui uma vulnerabilidade correspondente com alto nível de probabilidade de ocorrência no ambiente computacional e um baixo nível de proteção. É, portanto, muito importante que a empresa tenha claramente o seu nível de risco desejado, para que possa ter uma visão da priorização dos investimentos de segurança.
> Os riscos surgem em decorrência da presença de fraquezas, e, por conseguinte, vulnerabilidades. Isto ocorre pelo fato de que todos os ativos da empresa estão sujeitos a vulnerabilidades em maior ou menor escala e,

> neste caso, estas vulnerabilidades proporcionam riscos para a empresa, e são causadas muitas vezes por falhas nos seus controles.

A figura a seguir ilustra o relacionamento entre os termos associados ao risco para a segurança da informação.

Figura 4 – Relacionamento entre os termos associados ao risco



Fonte: Beal (2005, p. 16)

3.8 SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

O artigo 2º da Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 (BRASIL, 2008, p. 1), traz os seguintes conceitos:

> I - Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;
> II - Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
> III - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
> IV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
> V - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
> VI - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

A expressão *segurança da informação* é normalmente usada para referenciar a proteção de informações mantidas em componentes de tecnologia da informação (TI) contra as ameaças a que estão expostas, mas também considera a proteção dos ativos de informação que se encontram armazenados em outros meios, tais como na mente humana ou em um pedaço de papel (BEAL, 2005, p. 1).

3.9 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Sobre gestão de riscos de segurança da informação e comunicações, tem-se a definição:

> Gestão de Riscos de Segurança da Informação e Comunicações – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos (BRASIL, 2009, p. 2)

O mesmo conceito é dado por Beal (2005, p. 11), que complementa:

> Tendo em vista a complexidade e o alto custo de manter os ativos de informação a salvo de ameaças à sua confidencialidade, integridade e

> disponibilidade, é de extrema importância para o alcance dos objetivos de segurança adotar um enfoque de gestão baseado nos riscos específicos para o negócio.

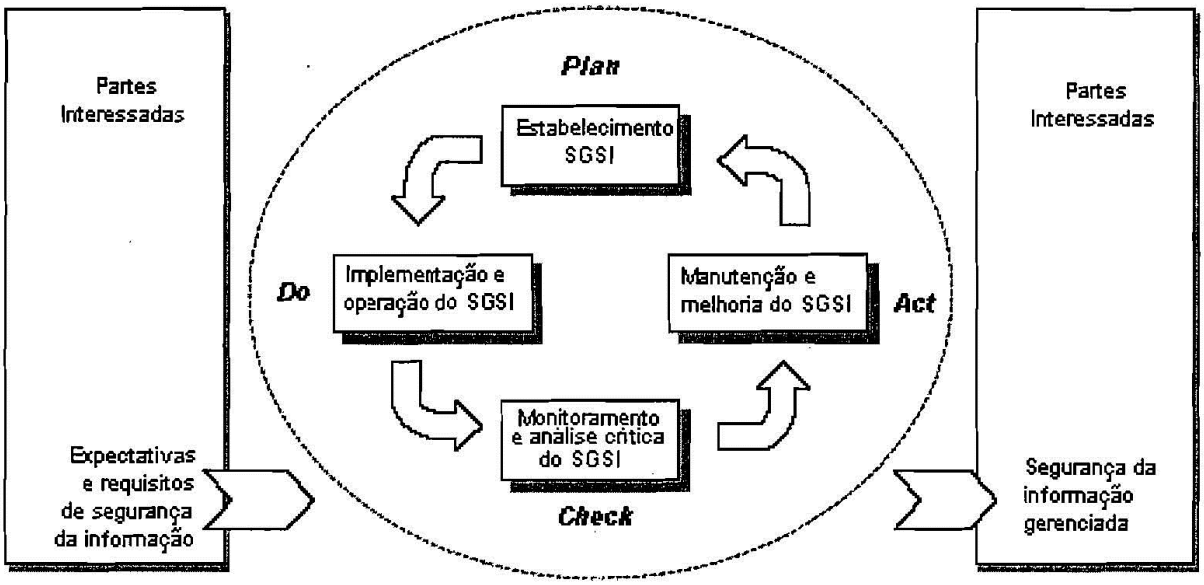
"A gestão de riscos está preocupada com a avaliação dos possíveis problemas que possam advir de ataques sobre os ativos no sistema, e equilibrar essas perdas contra os custos dos procedimentos de segurança que podem reduzir essas perdas." (SOMMERVILLE, 2011, p. 369, tradução nossa)

No contexto da Administração Pública Federal, deverá ser feita a elaboração sistemática de relatórios constando a análise quanto à aceitação dos resultados obtidos referentes à análise, avaliação e tratamento dos riscos, e consequente proposição de ajustes e de medidas preventivas e proativas à Alta Administração (BRASIL, 2009).

Segundo a Norma Complementar nº 04/IN01/DSIC/GSIPR (BRASIL, 2009, p. 3), o processo de Gestão de Riscos de Segurança da Informação e Comunicações deve estar alinhado ao modelo PDCA (*Plan-Do-Check-Act*), um ciclo com foco na melhoria contínua, no qual as atividades são planejadas, executadas e verificadas, para então haver a execução de ações visando melhorar o processo. Por tratar-se de um ciclo, o planejamento é feito novamente com base nas ações de melhoria, objetivando a melhoria contínua.

A figura a seguir ilustra o modelo PDCA aplicado aos processos do Sistema de Gestão de Segurança da Informação (SGSI).

Figura 3 – Modelo PDCA aplicado aos processos do SGSI



Fonte: Associação Brasileira de Normas Técnicas (2006, p. vi)

3.10 ANÁLISE DE RISCOS

A análise de riscos identifica os riscos de segurança presentes na organização e fornece conhecimento para que controles sejam implementados. A Associação Brasileira de Normas Técnicas (2005, p. 2) conceitua a análise de riscos como o "uso sistemático de informações para identificar fontes e estimar o risco."

O mesmo conceito é visto na Norma Complementar nº 04/IN01/DSIC/GSIPR, a qual descreve que no contexto da Administração Pública, os riscos devem ser monitorados e analisados criticamente, objetivando verificar regularmente mudanças nas ações da Secretaria da Informação e Comunicações, nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos de informação e nos fatores de risco: probabilidade, impacto, ameaça e vulnerabilidade (BRASIL, 2009, p. 5).

Segundo Peters e Pedrycz (2001, p. 350), a análise de riscos contempla a identificação, estimativa e avaliação dos riscos:

> Identificação dos riscos – Identificar fontes de riscos: custos, segurança, jurídico, erro;
> Estimativa dos riscos – Avaliar a probabilidade e a gravidade dos riscos;
> Avaliação dos riscos – Avaliar, priorizar e recomendar uma conduta e estratégias de prevenção desejáveis.

“A análise dos riscos é composta por quatro atividades distintas: identificação, projeção, avaliação e administração dos riscos.” (PRESSMAN, 1995, p. 131)

A identificação dos riscos abrange relações entre os riscos mapeados e suas categorias. Dessa forma, o projeto da solução neste Trabalho de Conclusão de Curso considera essas relações, pois todos os riscos possuem uma relação durante o projeto. Porém, existem alguns riscos que são difíceis de serem prognosticados de forma antecipada; esses também serão considerados durante o levantamento dos riscos identificados.

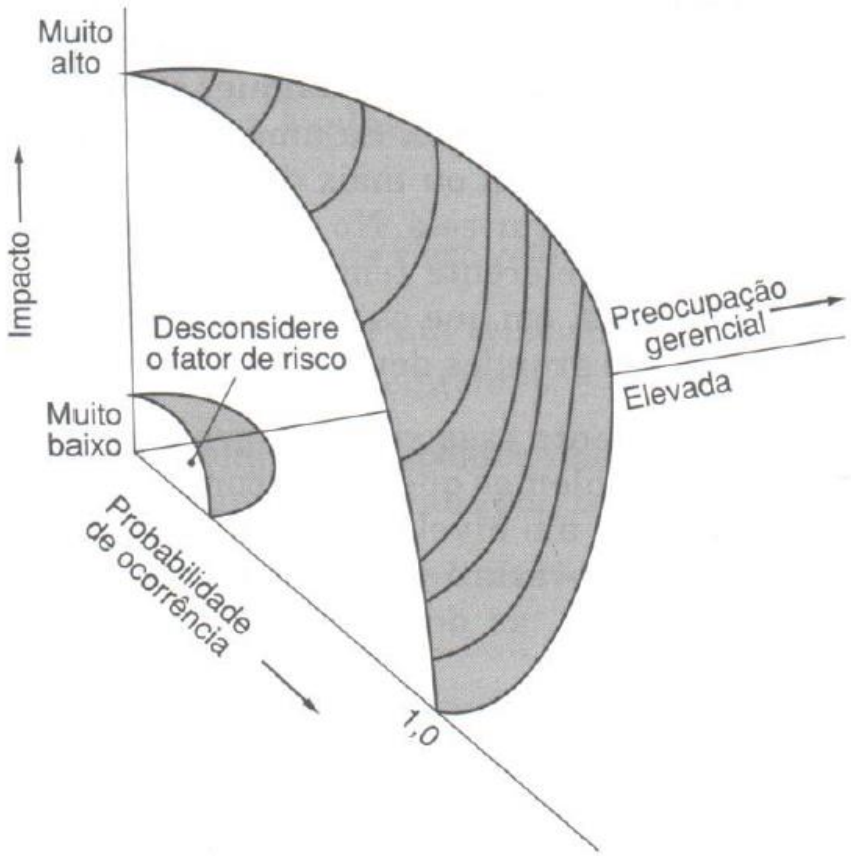
Pressman (1995) complementa essa afirmação ao escrever que, para estabelecer uma escala de probabilidade, pode-se utilizar uma escala de probabilidade qualitativa, contendo, segundo Charette[1] (1989 apud PRESSMAN, 1995), os seguintes valores: “altamente improvável, improvável, moderado, provável e altamente provável”. Após, o risco pode ser ponderado segundo as suas consequências (o impacto percebido), para então ser definida uma ordem de prioridade.

Pressman (1995, p. 134) descreve a figura 1 a seguir:

> Consultando a Figura [...], observamos o impacto e a probabilidade de riscos exercerem uma pressão diferente sobre a preocupação gerencial. Um fator de risco que tenha um peso de elevado impacto, mas uma probabilidade de ocorrência muito baixa, não absorverá uma significativa quantidade de tempo gerencial. Porém, os riscos de elevado impacto com probabilidade de ocorrência variando de moderada a alta e os riscos de baixo impacto com probabilidade elevada devem ser transportados para as etapas de análise dos riscos que se seguem.

[1] CHARETTE, Robert. **Software Engineering Risk Analysis and Management**. New York: McGraw-Hill, 1989.

Figura 1 – Risco e preocupação gerencial



Fonte: Pressman (1995, p. 135)

Quanto a administração dos riscos, Pressman (1995, p. 138) descreve que “parte da administração dos riscos significa avaliar quando os benefícios advindos das atividades tomadas para evitá-los são ultrapassados pelos custos associados à implementação dos mesmos.” O autor observa que é necessário executar uma análise de custo-benefício para a mitigação do risco, observando o custo do projeto e a sua duração, encontrando um equilíbrio que definirá se a administração irá implementar ou não os passos para minimização do risco.

Na prática, os funcionários podem fazer uma auto-avaliação através de um questionário. Este questionário possui objetivos específicos de controle e técnicas contra as quais um sistema pode ser avaliado. Consequentemente, tem-se um melhor entendimento do *status* dos programas e controles de segurança, a fim de surgir julgamentos e investimentos que mitiguem apropriadamente os riscos para um nível aceitável (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2001, tradução nossa).

A norma norte-americana, criada pelo National Institute of Standards and Technology (2001, p. 5, tradução nossa), defende o uso do questionário de auto-avaliação:

> O uso efetivo do questionário presume um compreensivo conhecimento dos valores dos sistemas e das informações a serem avaliados. O valor pode ser expresso em termos do grau de sensibilidade ou criticidade do sistema e informações relativas a cada uma das cinco categorias de proteção [...], integridade, confidencialidade, disponibilidade, autenticidade e não repúdio.

Nesse sentido, autenticidade e não repúdio referem-se, respectivamente, a qualidade de ser autêntico e a capacidade de alguém provar que a informação recebida de outra pessoa veio realmente dela. Já o significado de integridade, confiabilidade e disponibilidade é apresentado pela norma da seguinte forma:

> Integridade: a informação deve ser protegida de modificações não autorizadas, imprevistas ou não intencionais. Isto inclui, mas não está limitado a: autenticidade, “não repúdio” e responsabilidade;
> Confidencialidade: informação que requer proteção para divulgação não autorizada;
> Disponibilidade: o recurso de tecnologia da informação (sistema ou dados) deve estar disponível em tempo hábil, para atender a exigências […] ou evitar perdas substanciais. Disponibilidade também incluí a garantia de que os recursos são usados apenas para fins planejados. (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2001, p. 5, tradução nossa)

O National Institute of Standards and Technology (2001, p. 6, tradução nossa) também define que se deve relacionar a informação processada para cada um dos três requisitos descritos (integridade, confidencialidade e disponibilidade). Para categorizar a informação, o documento apresenta três exemplos de tais categorias de informação:

> Alto: prejuízo extremamente grave para os interesses [...]; se a informação fosse comprometida poderia causar a perda da vida, prisão, perda financeira maior, ou exigir uma ação legal para a correção.
> Médio: perda grave para os interesses [...]; se a informação fosse comprometida poderia causar perda financeira significativa ou exigir uma ação legal para a correção.
> Baixo: prejuízo para os interesses [...]; se a informação fosse comprometida causaria apenas menor perda financeira ou exigem apenas ações administrativas para a correção.

Segundo o National Institute of Standards and Technology (2001, tradução nossa), faz-se necessário o uso do questionário para a análise de diversos fatores referentes aos sistemas de tecnologia da informação, dados e informações das organizações, auxiliando nas tomadas de decisões referentes aos riscos analisados.

Os resultados encontrados favorecem a organização para as futuras decisões, que necessariamente serão analisadas para definir a avaliação dos riscos.

Segundo a norma norte-americana:

> Com o objetivo de medir o progresso da implementação efetiva do controle de segurança necessários, cinco níveis de eficácia são fornecidos para cada resposta para a questão de controle de segurança:
> Nível 1 - objetivo de controle documentado em uma política de segurança;
> Nível 2 - controles de segurança documentados como procedimentos;
> Nível 3 - procedimentos foram implementados;
> Nível 4 - procedimentos e controles de segurança são testados e revisados;
> Nível 5 - procedimentos e controles de segurança são totalmente integrados em um amplo programa.
> O método para responder as perguntas podem ser baseado principalmente em uma análise da documentação relevante e um rigoroso exame e teste dos controles. (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2001, p. 10, tradução nossa).

A figura a seguir ilustra um questionário sugerido pela norma norte-americana.

Figura 2 – Exemplo de questionário

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Risk Management *OMB Circular A-130, III*								
1.1 Critical Element: Is risk periodically assessed?								
1.1.1 Is the current system configuration documented, including links to other systems? *NIST SP 800-18*								
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? *FISCAM SP-1*								
1.1.3 Has data sensitivity and integrity of the data been considered? *FISCAM SP-1*								

Fonte: National Institute of Standards and Technology (2001)

Sobre a análise do questionário, tem-se:

> Devido ao fato de ser uma auto-avaliação, idealmente os indivíduos que avaliam o sistema são os donos do sistema ou os responsáveis pela operação ou administração do sistema. Os mesmos indivíduos que completaram o questionário podem conduzir as análises do questionário concluído. Por ser familiar com o sistema, a documentação de apoio, e os resultados da avaliação, o próximo passo que o avaliador realiza é uma análise, que resume as conclusões. Um grupo centralizado, como um Programa de Segurança de Sistemas de Informação de uma agência, pode também conduzir as análises desde que a documentação de apoio seja suficiente. Os resultados das análises devem ser descritos em o plano de ação, e o plano do sistema de segurança deve ser criado ou atualizado para refletir cada objetivo de controle e decisões técnicas (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2001, p. 10, tradução nossa).

3.11 IDENTIFICAÇÃO DE RISCOS

O Departamento de Segurança da Informação e Comunicações (BRASIL, 2009, p. 3) conceitua identificação de riscos como o “processo para localizar, listar e caracterizar elementos do risco.”

Sobre identificação de riscos, a Associação Brasileira de Normas Técnicas (2005, p. 104) descreve: “Convém identificar os eventos que podem causar interrupções aos processos de negócio, junto a probabilidade e impacto de tais interrupções e as consequências para a segurança de informação.”

Pressman (1995, p. 132), em seu livro *Engenharia de Software*, mostra que a identificação dos riscos envolve a relação dos riscos específicos de projeto dentro de categorias definidas de diversas maneiras diferentes e sugere o uso de um *checklist* de itens de risco – uma ou mais perguntas que sejam pertinentes a cada fator de risco. Segundo ele, “um dos melhores métodos para se entender cada um dos riscos é usar um conjunto de perguntas que ajude o planejador do projeto a compreender os riscos em termos técnicos ou de projeto.”

3.12 ESTIMATIVA DE RISCOS

A Norma Complementar nº 04/IN01/DSIC/GSIPR (BRASIL, 2009, p. 2) conceitua a estimativa de riscos como o “processo utilizado para atribuir valores à probabilidade e conseqüências de um risco”. Pressman (1995, p. 133) descreve a estimativa de riscos como:

> A estimativa de riscos tenta classificar cada risco de duas maneiras – a probabilidade de que o risco seja real e as consequências dos problemas associados ao risco, caso ele ocorra. Pode ser executado quatro atividades de projeção dos riscos: (1) estabelecimento de uma escala que reflita a probabilidade percebida de ocorrência de um risco; (2) delineamento das consequências do risco; (3) estimativa do impacto do risco sobre o projeto e o produto; e (4) anotação da precisão global da projeção dos riscos de forma que não haja mal-entendidos.

O estabelecimento de uma escala para a probabilidade da ocorrência dos riscos irá auxiliar na definição dos riscos com maiores chances de ocorrerem, perante a

realidade mapeada. Essa escala irá ajudar o analista de risco a enxergar melhor a relação de probabilidade para cada risco mapeado.

O delineamento das consequências do risco, e a estimativa do impacto do risco apresentam uma limitação do que o risco irá acarretar caso ele venha a se tornar realidade. É necessário ter essa visão durante a estimativa dos riscos, pois assim pode-se definir e limitar até aonde um risco irá impactar a organização. Essas informações são essenciais para a entidade poder definir com mais precisão aonde irá investir seus recursos - tanto financeiros quanto de alocação de recursos e tempo, para minimizar o impacto do risco ou até excluir sua chance de ocorrência (PRESSMAN, 1995).

A anotação da precisão global da projeção dos riscos é a documentação correta deles e a clara apresentação do levantamento dessas informações para os responsáveis. Esse processo também tem grande importância durante a estimativa de risco, pois é ele que irá disseminar a informação de forma correta e coerente (PRESSMAN, 1995).

3.13 AVALIAÇÃO DE RISCOS

Segundo a Norma Complementar nº 04/IN01/DSIC/GSIPR (BRASIL, 2009, p. 2), avaliação de riscos é o “processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco”. Dessa forma, a avaliação de riscos é uma consideração sistemática da probabilidade de uma falha ocorrer e do impacto que esta poderia causar nos negócios da organização, tendo em vista as perdas de confidencialidade, integridade e disponibilidade dos ativos.

A avaliação de riscos pode ser realizada utilizando-se métodos qualitativos, métodos quantitativos ou ambos. *Métodos qualitativos* utilizam técnicas subjetivas e *métodos quantitativos* utilizam técnicas objetivas.

Os *métodos qualitativos* não são apropriados para fornecerem estimativas numéricas e não realizam o tratamento de dados estatísticos e dados históricos. Portanto, não é possível ranquear os riscos identificados. São técnicas que se ajustam muito bem quando não se tem conhecimento profundo do objeto da análise, a incerteza é muito grande e a análise de riscos depende em grande parte da

opinião, conhecimento e experiência de quem realiza a análise de riscos (ROCHA, 2012).

Segundo Beal (2005, p. 23): “Os *métodos qualitativos* trabalham com a descrição literal dos riscos para avaliá-los. Vários métodos de avaliação qualitativa do risco utilizam questionários e matrizes de risco [...].” O quadro a seguir exemplifica uma matriz de risco.

Quadro 1 – Exemplo de matriz de risco

Gravidade do impacto	Probabilidade de ocorrência do incidente					
	F Impossível	E Improvável	D Remota	C Ocasional	B Provável	A Freqüente
I Catástrofe			/////////	XXXXXX	XXXXXX	XXXXXX
II Alta				/////////	XXXXXX	XXXXXX
III Média					/////////	/////////
IV Baixa						

XXXXXX: Imperativo reduzir os riscos.
/////////: Medidas de proteção adicionais requeridas.
Em branco: As medidas básicas de proteção adotadas pela organização são consideradas suficientes para manter os riscos em níveis aceitáveis.

Fonte: Beal (2005, p. 23)

Sobre o quadro anterior, tem-se:

> Nesse exemplo, a probabilidade de um incidente apresenta seis níveis, estimada de acordo com a frequência esperada da ocorrência ao longo de um período ou no grau de confiança na ocorrência do incidente. Já a gravidade do impacto pode ser classificada de catastrófica, quando o dano representar o fracasso da organização, a baixa, quando um ataque bem-sucedido não for capaz de provocar efeitos adversos consideráveis. A matriz resultante da combinação dessas duas dimensões, confrontada com critérios de risco previamente definidos, leva à identificação dos riscos que necessariamente têm que ser reduzidos (neste exemplo pertencentes às células marcadas com XXXXXX e //////// no quadro) pelo uso de medidas de proteção complementares aos controles básicos adotados pela organização (BEAL, 2005, p. 23).

Os *métodos quantitativos* utilizam técnicas mais caras e complexas, mas oferecem como atrativo o fato de suprirem as deficiências dos *métodos qualitativos*. Encontram grande aplicação e produzem ótimos resultados aonde a segurança e a criticidade são requisitos necessários (ROCHA, 2012).

Beal (2005, p. 22) descreve:

> Os *métodos quantitativos* de avaliação do risco são particularmente úteis quando se tenta buscar um equilíbrio entre os custos de implementação de medidas de segurança e o possível custo da não-implantação dessa segurança.

Rocha (2012) escreve:

> Atualmente já são admitidas técnicas mistas, que utilizam características de ambos os grupos, tornando as análises mais simples e ao mesmo tempo mais precisas, pois diminuem as incertezas associadas à análise, como exemplo podemos citar o método da Árvore de Falhas. Estes métodos mistos fornecem estimativas numéricas, e um ranqueamento dos riscos identificados, mas são métodos que não fornecem resultados detalhados da segurança de sistemas , falhas de causa comum e redundâncias.

3.14 COMUNICAÇÃO DO RISCO

Comunicação do risco refere-se a troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas (BRASIL, 2009). Para haver uma comunicação bem sucedida, é necessário que o risco seja comunicado adequadamente de forma que seja compreendido pelos receptores da informação. Portanto, todos os documentos sobre os riscos devem ser de fácil entendimento.

Os responsáveis pela organização devem decidir sobre o tratamento ou aceitação dos riscos. Contudo, a adequada comunicação dos riscos assegura que a decisão final seja tomada com entendimento claro das implicações de segurança, facilitando a aprovação – se for o caso – de outras despesas consideradas necessárias para implementar controles adicionais que garantam a manutenção dos riscos dentro de níveis considerados aceitáveis pelos dirigentes (BEAL, 2005).

3.15 TRATAMENTO DE RISCOS

A Norma Complementar nº 04/IN01/DSIC/GSIPR (BRASIL, 2009, p. 3) define tratamento de riscos como “processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco” e descreve as formas de tratar os riscos:

> Evitar risco – uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

> Reduzir risco – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;
> Reter risco – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;
> Transferir risco – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco.

Como exemplos de tratamento de risco, pode-se citar: o não armazenamento de senhas em meio eletrônico, medida que reduz o risco de acesso não autorizado; a não divulgação de senhas para colegas; a não abertura de arquivos duvidosos que foram enviados por pessoas desconhecidas; a verificação periódica, de possíveis vírus ou programas de má-índole, por *antivírus* e outras ferramentas do ramo; dentre outros.

Entretanto, é possível decidir pela aceitação do risco, ou seja, não tratar o risco. Neste caso, um Plano de Contingência deve ser criado para orientar sobre os procedimentos a serem realizados caso o risco ocorra. Recomenda-se optar pela aceitação do risco apenas quando os danos causados se ele ocorrer forem menores que o esforço ou custo para tratar esse risco.

4 ESTUDO DE SISTEMAS DE ANÁLISE DE RISCOS

Para complementar os estudos, foi desenvolvida uma pesquisa sobre sistemas de análise de riscos existentes. Foram estudadas as características de ferramentas disponíveis no mercado e desenvolvidas em trabalhos acadêmicos. Entretanto, não foi encontrada ferramenta voltada exclusivamente à análise de riscos de segurança da informação e comunicações para organizações da Administração Pública Federal.

O objetivo deste estudo é sustentar de forma mais consistente a necessidade do desenvolvimento da ferramenta *Via Análise*. Todas as informações foram obtidas através das páginas dos desenvolvedores na *internet* e a veracidade das informações contidas nas páginas não foi questionada. Em alguns casos, a omissão ou escassez de informações no site dos desenvolvedores, sobre algum recurso ou característica específica, foi subentendida como um recurso ou característica não disponível.

Dentre as ferramentas analisadas, a ferramenta *Módulo Risk Manager* não dispunha de uma versão de demonstração. Sobre as demais, foi possível instalá-las e obter uma visão melhor a respeito destas.

4.1 CRITÉRIOS DE AVALIAÇÃO

Os sistemas foram avaliados a partir das seguintes características:

a) Documentação: análise sobre a documentação disponível, se foi escrita em idioma Português, bem como sua relevância e abrangência;
b) Idioma Português: análise sobre a versão da ferramenta suportar o idioma Português;
c) Integração: análise sobre a capacidade de o sistema integrar-se com outras áreas da gestão de riscos ou outras ferramentas de segurança da informação e comunicações;
d) Plataforma: análise sobre quais plataformas são suportadas pela ferramenta e se depende de outros sistemas para funcionar;
e) Relatórios: análise sobre a disponibilidade de visualização e impressão de relatórios, verificando o formato e a qualidade do relatório gerado;

f) Sistema *desktop*: análise sobre a disponibilização de informações apenas no computador em que está instalado, sem trafegar informações na internet;
g) Usabilidade: análise da facilidade de uso da ferramenta por parte do usuário.

4.2 SISTEMAS ESTUDADOS

4.2.1 @Risk

O sistema @Risk, desenvolvido pela empresa Palisade, trata-se de um complemento para a ferramenta Microsoft Excel. A seguir é apresentado o resultado da avaliação:

a) Documentação: possui documentação em Português;
b) Idioma Português: suporta diferentes idiomas, inclusive o Português;
c) Integração: possui integração apenas com a ferramenta *Microsoft Excel* e com as ferramentas da *Palisade*;
d) Plataforma: *Windows 95* ou superior. Necessita do *Microsoft Excel* instalado;
e) Relatórios: possibilita a geração de diversos relatórios;
f) Sistema *desktop*: sim;
g) Usabilidade: é necessária muita familiaridade com o *Microsoft Excel* e a ferramenta não suporta múltiplos projetos tampouco múltiplos usuários.

Mais informações podem ser obtidas na página: <http://www.palisade-br.com/risk/>.

4.2.2 Módulo Risk Manager

Desenvolvida pela empresa Módulo, a ferramenta Módulo Risk Manager possui as seguintes características:

a) Documentação: não possui;
b) Idioma Português: suporta diferentes idiomas, inclusive o Português;
c) Integração: possui fácil integração com diversos sistemas;

d) Plataforma: *Windows XP Professional*, *Windows 2000 Server*, *Windows 2000 Professional*, *Windows Vista*, *Windows 2003* (*Domain Controller* e *Member Server*), *Solaris 9*, *Solaris 10*, *IBM AIX 5*, *HP-UX 11*, *FreeBSD*, *Linux* (*Red Hat*, *Fedora*, *Debian*, *Suse*, *Slackware*), *IBM OS/390* e *Novell Netware*;
e) Relatórios: possibilita a geração de diversos relatórios;
f) Sistema desktop: não. A ferramenta é utilizada na internet;
g) Usabilidade: possui interface amigável e intuitiva, bem como oferece a possibilidade de o usuário criar e personalizar as interfaces.

Maiores informações sobre a ferramenta Módulo Risk Manager podem ser encontradas em: < http://www.modulo.com.br/downloads/ema-white-paper.pdf>.

4.2.3 RiskFree

A ferramenta RiskFree foi desenvolvida em 2005 durante o Trabalho de Conclusão de Curso de alunos da Faculdade de Informática da PUCRS. A ferramenta foi desenvolvida com o objetivo de auxiliar equipes de projetos nas tarefas relacionadas à gerência de riscos em projetos de desenvolvimento de software. Possui as seguintes características:

a) Documentação: possui boa documentação em Português;
b) Idioma Português: sim;
c) Integração: possui fácil integração com diversos sistemas;
d) Plataforma: multiplataforma;
e) Relatórios: possibilita a geração de diversos relatórios;
f) Sistema *desktop*: não. A ferramenta é utilizada na *internet*;
g) Usabilidade: possui interface amigável e intuitiva.

Para maiores informações a respeito da ferramenta podem ser obtidas em: < http://www.inf.pucrs.br/~rafael/RiskFree/>.

4.2.4 Risk Radar

A ferramenta Risk Radar foi desenvolvida pela American Systems Corporation. Possui as seguintes características:

a) Documentação: possui documentação mas somente em Inglês;
b) Idioma Português: não. Somente Inglês;

c) Integração: pode integrar outros sistemas;
d) Plataforma: *Windows 2000, Windows NT, Windows XP* ou superior;
e) Relatórios: possibilita a geração de diversos relatórios;
f) Sistema *desktop*: sim;
g) Usabilidade: possui interface amigável e intuitiva.

Para maiores informações a respeito da ferramenta podem ser obtidas em: < http://www.americansystems.com/NR/rdonlyres/BB407D38-1AD5-4AA5-8020-D89B2E1DB357/0/RRE_Overview.pdf> e < http://www.riskradarprogram.com/>.

4.2.5 Risk Trak

A ferramenta Risk Trak foi desenvolvida pela empresa Risk Services & Technology. A seguir são listadas as características da ferramenta:

a) Documentação: possui documentação mas somente em Inglês;
b) Idioma Português: não. Somente Inglês;
c) Integração: não possui integração com outras ferramentas;
d) Plataforma: *Microsoft Windows*;
e) Relatórios: possibilita a geração de relatórios;
f) Sistema *desktop*: sim;
g) Usabilidade: possui interface pouco intuitiva.

Para maiores informações a respeito da ferramenta podem ser obtidas em: <http://risktrak.com/faq/quicktour.htm>.

4.3 ANÁLISE COMPARATIVA

O quadro a seguir apresenta uma comparação entre as ferramentas estudadas.

Quadro 2 – Comparação entre as ferramentas estudadas

Característica	**Ferramenta estudada**				
	@Risk	Módulo Risk Manager	RiskFree	Risk Radar	RiskTrak
Documentação	Sim, em Português	Não	Sim, em Português	Sim, em Inglês	Sim, em Inglês
Idioma Português	Sim	Sim	Sim	Não	Não
Integração	Não	Sim	Sim	Não	Não
Plataforma	Microsoft Windows (necessita do Microsoft Excel)	*Windows XP* ou superior, *Solaris* versões *9* e *10, IBM AIX 5* e *OS/390*, *HP-UX 11*, *FreeBSD*, *Linux* (*Red Hat*, *Fedora*, *Debian*, *Suse* e *Slackware*), *Novell Netware*	Multiplataforma	Microsoft Windows (necessita do Microsoft Access)	Microsoft Windows
Relatórios	Sim	Sim	Sim	Sim	Sim
Sistema *desktop*	Sim	Não	Não	Sim	Sim
Usabilidade	Razoável	Boa	Boa	Boa	Razoável

Fonte: O Autor (2012)

Um fator importante é que a ferramenta *Via Análise* será a única voltada exclusivamente à análise de riscos de segurança da informação e comunicações para organizações da Administração Pública Federal. A ferramenta também fará comunicação com o sistema de gerenciamento de banco de dados *Oracle*, possibilitando o crescimento da ferramenta no futuro.

A ferramenta desenvolvida terá baixo acoplamento e alta coesão, além de ser desenvolvida em uma linguagem atual: *Java*. Esta linguagem apresenta diversas soluções para integração de possíveis funcionalidades que venham a ser acopladas nessa solução.

5 SOLUÇÃO

Este capítulo apresenta a solução, as fases do projeto e os artefatos gerados em cada fase.

5.1 APRESENTAÇÃO

A solução ao problema proposto trata-se de um sistema de informação capaz de analisar de maneira eficiente os riscos de segurança da informação e comunicações em órgãos e entidades da Administração Pública Federal, seguindo as diretrizes da Norma Complementar nº 04/IN01/DSIC/GSIPR. A ferramenta tem como entrada um conjunto de ativos de informação, riscos, ameaças, controles, critérios de avaliação e aceitação de risco, probabilidade de ocorrência dos riscos e seu impacto. Como saída, a ferramenta gera relatórios contendo análise, avaliação e proposta de tratamento dos riscos.

A avaliação de riscos foi implementada como um módulo na ferramenta, para o processo de gestão de riscos de segurança da informação e comunicações (GRSIC). Atualmente ela deve estar alinhada ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme definido na Norma Complementar n° 02/DSIC/GSIPR, no item 4.3 da Norma Complementar nº 04/IN01/DSIC/GSIPR. Entretanto, espera-se obter um modelo que seja extensível, caso haja mudança nessa diretriz. Contudo, as demais funcionalidades do sistema não serão prejudicadas uma vez que o sistema tem uma arquitetura com baixo acoplamento.

A arquitetura de desenvolvimento escolhida foi a *Java Standard Edition* (Java SE), pois atende as necessidades do projeto, trabalha com orientação a objetos e faz *interface desktop*. Optou-se por desenvolver sistema para *desktop* devido a necessidade de maior segurança para as informações – não disponibilização de conteúdo na rede - bem como o sistema será utilizado por poucos usuários e, futuramente, poderá ser feita a comunicação com periféricos de *hardware*, tais como leitor de código de barras, para auxiliar no cadastramento dos ativos.

Foi utilizado o sistema de gerenciamento de banco de dados *Oracle* versão *11g*, devido à simplicidade com que é feita a conexão entre esse sistema e a ferramenta de desenvolvimento. Outra vantagem é que o *Oracle* permite a modelagem

Entidade-Relacionamento das tabelas necessárias, além de ser desenvolvido pela empresa que detém a linguagem de programação *Java* em seu repertório de soluções, facilitando a integração entre elas. Além dessas vantagens, destaca-se o fácil suporte ao usuário, tanto para o sistema de gerenciamento de banco de dados quanto para o *Java*, pois ele é centralizado no mesmo fornecedor, facilitando a busca de solução para qualquer possível defeito encontrado durante o desenvolvimento da solução.

5.2 PROCESSO DE DESENVOLVIMENTO UTILIZADO

Para o desenvolvimento do *software*, foi adotada a metodologia de desenvolvimento de sistemas *Rational Unified Process* (RUP), baseado no ciclo de vida iterativo incremental. A justificativa para a escolha desta metodologia está baseada na flexibilidade da mesma para definir o nível de formalidade necessário ao perfil, tamanho e escopo de cada projeto (KROLL, 2005).

5.3 GERENCIAMENTO DE PROJETO

Os seguintes artefatos foram gerados referentes ao Gerenciamento do Projeto:

a) Estimativas: estimativas de tamanho do sistema e esforço para desenvolvê-lo;
b) Lista de Atividades: planilha com as atividades do projeto agrupadas por iteração, apresentando o período a ser trabalhado em cada atividade e o responsável por ela;
c) Lista de Riscos: lista de riscos para o projeto, classificada por impacto, probabilidade e magnitude, com as estratégias de mitigação de cada risco;
d) Planilha de Custos e Esforço: planilha com o nome dos casos de uso a serem desenvolvidos, as iterações em que serão desenvolvidos, o esforço e prazo para desenvolvê-los;
e) Plano de Iteração: plano com o conjunto de atividades e tarefas divididas por sequências de tempo, com recursos atribuídos e dependências de tarefas, para a iteração;

f) Plano de Projeto: documento que reúne todas as informações necessárias ao gerenciamento do projeto.

5.4 GERENCIAMENTO DE CONFIGURAÇÃO

Referente ao Gerenciamento de Configuração foi criado um Plano de Gerenciamento de Configuração. Esse documento descreve todas as atividades do Gerenciamento de Controle de Configuração e Mudança que serão executadas durante o ciclo de vida do produto.

5.5 MODELAGEM DE NEGÓCIO

Os seguintes artefatos foram gerados na Modelagem de Negócio:

a) Casos de Negócio - objetos: Modelagem de caso de negócio para cada funcionalidade da ferramenta, tanto de cadastro, quanto análise de risco e cálculo de risco, e suas relações com o usuário.
b) Casos de Negócio: Utilização e finalidade da ferramenta para o usuário final.
c) Especificação de Requisitos: Especificar os requisitos de alto nível que o sistema deve prover, identificando os requisitos funcionais, não-funcionais, as restrições e as premissas.
d) Glossário.doc: Definir a terminologia específica do projeto Via Análise.
e) VisaoDeNegocio.doc: Objetivos e propostas de solução da ferramenta, a nível de proposição de valor de negócio para o projeto.

5.6 MODELAGEM DE SISTEMA

Os seguintes artefatos foram gerados na Modelagem de Sistema:

a) Diagrama de Componentes: apresenta os componentes que formam o sistema e suas relações entre eles;
b) Documento de Arquitetura: descreve a estrutura básica do sistema.

5.7 MODELAGEM DE TESTES

Os seguintes artefatos foram gerados na Modelagem de Testes:

a) Casos de Testes: apresenta o passo a passo e respectivos resultados esperados referente aos testes de cada funcionalidade;
b) Registro de Testes: descreve o resultado dos testes.

CONCLUSÃO

Com esse trabalho torna-se possível analisar com maior facilidade os riscos de segurança da informação e comunicações em organizações da Administração Pública Federal. Através do mapeamento dos ativos, riscos, ameaças, controles, critérios de avaliação e aceitação de risco, definição de probabilidade de ocorrência de cada risco e do impacto caso o risco se concretize, a ferramenta gera relatórios contendo análise, avaliação e proposta de tratamento dos riscos.

A ferramenta foi implementada seguindo as diretrizes da Norma Complementar número 04/IN01/DSIC/GSIPR. Entretanto, a estrutura modular como foi desenvolvida possibilita que novas funcionalidades sejam implementadas utilizando a mesma metodologia para o cálculo de risco ou que essas regras sejam substituídas por outras. Desta forma, o sistema pode ser adaptado a qualquer norma.

Como perspectivas para trabalhos futuros, pode-se implementar mais metodologias para cálculo de risco, possibilitando que o usuário da ferramenta escolha uma dentre as várias regras implementadas. Além disso, podem vir a ser implementados recursos para tratamento de incidentes. Também, pode-se aumentar o número de relatórios gerados pela ferramenta. Enfim, o auxílio do sistema Via Análise representa uma sensível melhora no cumprimento da obrigação de analisar riscos de segurança e elaborar sistematicamente os relatórios para os Gestores de Segurança da Informação e Comunicações para todo um conjunto de organizações públicas.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**: Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2006. 34 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002**: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. 120 p.

ADENS, G.; ARMSTRONG, R.; JANTZEN, K. **Estimating the effects of project risks in software development projects**. Postdam: 16th International Workshop on Software Measurement and Dasma Metrik Kongress, 2006. Disponível em: <http://www.tassc-solutions.com/downloads/EstimatingRisks.pdf>. Acesso em: 26 ago. 2012.

AMERICAN SYSTEMS CORPORATION. **Risk Radar Enterprise**. Chantilly, 2010. Disponível em: <http://www.americansystems.com/NR/rdonlyres/BB407D38-1AD5-4AA5-8020-D89B2E1DB357/0/RRE_Overview.pdf>. Acesso em: 2 set. 2012.

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

BRASIL. Constituição (1988). **Emenda constitucional nº 19**, de 4 de junho de 1998. Modifica o regime e dispõe sobre princípios e normas da Administração Pública, servidores e agentes políticos, controle de despesas e finanças públicas e custeio de atividades a cargo do Distrito Federal, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc19.htm#art37>. Acesso em: 6 set. 2012.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Instrução Normativa GSI/PR nº 1**, de 13 de junho de 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf>. Acesso em: 29 ago. 2012.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. **Norma Complementar nº 04/IN01/DSIC/GSIPR**, de 14 de agosto de 2009. Disponível em: <http://www.governoeletronico.gov.br/anexos/norma-complementar-04-2009/download>. Acesso em: 24 ago. 2012.

BRASIL. Tribunal de Contas da União. Secretaria de Fiscalização de Tecnologia da Informação. **Boas práticas em segurança da informação**. Brasília: Tribunal de Contas da União, 2012. 103 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF>. Acesso em: 5 abr. 2013.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para Internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2012. 126 p. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 28 ago. 2012.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Estatísticas dos Incidentes Reportados ao CERT.br**. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: < http://www.cert.br/stats/incidentes/>. Acesso em: 5 set. 2012.

ENTERPRISE MANAGEMENT ASSOCIATES. **Gestão de GRC**: Módulo Risk Manager - A Nova Geração em Automatização de Governança, Riscos e Compliance. [S.l.], 2010. Disponível em: < http://www.modulo.com.br/downloads/ema-white-paper.pdf>. Acesso em: 1 set. 2012.

RIBEIRO, Bruno; BRANCATELLI, Rodrigo. Falha de segurança permite fraudar bilhete único em apenas 5 segundos. **O Estado de São Paulo**, São Paulo, 12 fev. 2012. Disponível em: <http://www.estadao.com.br/noticias/cidades,falha-de-seguranca-permite-fraudar-bilhete-unico-em-apenas-5-segundos,835002,0.htm>. Acesso em: 6 set. 2012.

FERREIRA, Aurélio Buarque de Holanda. **Novo Aurélio Século XXI**: o dicionário da língua portuguesa. Rio de Janeiro: Nova Fronteira, 1999. 2128 p.

KROLL, Per; KRUCHTEN, Philippe. **The rational unified process made easy: a practitioner's guide to the RUP**. Boston: Addison-Wesley, 2005. 416p.

MÓDULO. **Módulo Risk Manager**. Rio de Janeiro, [2012]. Disponível em: < http://www.modulo.com.br/software>. Acesso em: 2 set. 2012.

MOEN, Ronald; NORMAN, Clifford. **Evolution of the PDCA Cycle**. Detroit: [s.n.], [2009]. 11 p. Disponível em: <http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf>. Acesso em: 1 set. 2012.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Computer Security**: Security Self-Assessment Guide for Information Technology Systems. Washington: 2001. Disponível em: <http://www.cio.gov/Documents/sp800-26.pdf>. Acesso em: 4 set. 2012.

NETTO, Geraldo da Silva Rocha. **E agora qual método utilizar?**: ¿Porque estudar métodos diferentes de análise de riscos? [S.l.: s.n.] Disponível em: <http://www.forodeseguridad.com/artic/pt/9001.htm>. Acesso em: 1 set. 2012.

PALISADE. @**Risk**: Um novo padrão em Análise de Risco. Rio de Janeiro, [2012]. Disponível em: < http://www.palisade-br.com/risk/>. Acesso em: 1 set. 2012.

PETERS, James F.; PEDRYCZ, Witold. **Engenharia de software**. Tradução de: Ana Patricia Garcia. Rio de Janeiro: Campus, 2001. 602 p.

PRESSMAN, Roger S. **Engenharia de software**. Tradução de: José Carlos Barbosa dos Santos.São Paulo: Makron Books, 1995. 1056 p.

PRO-CONCEPTS. **Risk Radar 2012 Information**. Virginia Beach, 2012. Disponível em: <http://www.proconceptsllc.com/Risk_Radar_2012.html>. Acesso em: 2 set. 2012.

RISK SERVICES & TECHNOLOGY. **RiskTrak Quick Tour**. Milford, 2010. Disponível em: <http://risktrak.com/faq/quicktour.htm>. Acesso em: 3 set. 2012.

SILVA, Luiz Fernando Costa Pereira da. **Gestão de Riscos em Tecnologia da Informação como fator crítico de sucesso na Gestão da Segurança da Informação dos órgãos da Administração Pública Federal**: estudo de caso da Empresa Brasileira de Correios e Telégrafos – ECT. 2010. 160 p. Dissertação (Mestrado em Ciência da Informação) – Faculdade de Economia Administração e Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2010.

SILVEIRA, Filipi Pereira da; KNOB, Flávio Franco. **RiskFree**: Uma ferramenta de apoio à gerência de riscos em projetos de software. 2005. 77 p. Monografia (Graduação em Ciência da Computação) – Faculdade de Informática, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2005.

SOMERVILLE, Ian. **Software engineering**. Boston: Addison-Wesley, 2011. 773 p.

VOLPI, Angelo**;** FREITAS, Cinthia O. de A. Documentos na internet e a sociedade da exposição. **Document Management**, São Paulo, n. 24, p. 48, jun. 2011.

WEEGE, José Fernando Marques. **Gestão de Risco**: Segurança da Informação. [S.l.], [2005]. Disponível em: <http://www.ftec.com.br/empresajr/revista/autor/pdf/jose.pdf>. Acesso em: 26 ago. 2012.

GLOSSÁRIO

Agente – Executor de uma ação que pode ter efeitos adversos sobre um ativo de informação;

Alvo – Ativo que pode ser objeto de um ataque ou incidente;

Antivírus – Sistema de computador desenvolvido para prevenir, detectar e eliminar vírus de computador;

Ataque - Evento decorrente da exploração de uma vulnerabilidade por uma ameaça;

Baseline - Definição de marcos de um determinado projeto.

Fator de Risco – Aquilo que contribui para a ocorrência de um risco;

Hardware – Conjunto de unidades físicas, componentes, circuitos integrados, discos e mecanismos que compõem um computador ou seus periféricos;

Plano de Contingência – Documento que descreve as ações a serem tomadas caso determinados problemas aconteçam, voltado a minimizar as interrupções de atividades na organização e proteger a perda de informações causadas por possíveis ameaças;

Sistemático - Pertencente ou relativo ao sistema. Conforme a um sistema. Que observa um sistema. Metódico, ordenado. Feito com intenção determinada;

Software - Qualquer programa ou grupo de programas que instrui o *hardware* sobre a maneira como ele deve executar uma tarefa, inclusive sistemas operacionais, processadores de texto e programas de aplicação;

Stakeholder - Pessoa ou organização que tenha interesse ou é afetada pelo projeto.

Vírus de computador – Sistema malicioso de computador desenvolvido com o intuito de causar danos ou prejudicar o sistema, o usuário do computador ou um determinado ativo.

APÊNDICE A – Plano de Projeto

Plano de Projeto

Via Análise

Responsáveis:
Andrey Bevilacqua
Jônatas Josué Kirsch

Descrição Geral do Projeto

Criação de um sistema de informação capaz de analisar de maneira eficiente os riscos de segurança da informação e comunicações em órgãos e entidades da Administração Pública Federal, seguindo as diretrizes da Norma Complementar nº 04/IN01/DSIC/GSIPR. A ferramenta terá como entrada um conjunto de ativos de informação, riscos, probabilidade de ocorrência dos riscos e seu impacto. Como saída, a ferramenta gerará relatórios contendo análise, avaliação e proposta de tratamento dos riscos.

Este projeto trata do planejamento e execução de todas as fases do ciclo de desenvolvimento do sistema em questão.

Premissas e Restrições

Premissas

- Os membros da equipe não sairão do projeto antes da sua conclusão;
- O projeto será gerenciado de forma conjunta entre os membros da equipe.

Restrições

- As linguagens de programações utilizadas para o desenvolvimento do sistema serão: Java e SQL;
- Será usado o sistema gerenciador de banco de dados Oracle;
- Deve haver uma máquina local para prover suporte a um banco de dados.

Stakeholders Relevantes

Papel(eis)	**Nome**
Gerente do Projeto, Analista de Negócios, Administrador de Banco de Dados, Arquiteto, Analista de Sistemas, Desenvolvedor.	Andrey Bevilacqua
Gerente do Projeto, Analista de Negócios, Analista de Sistemas, Analista de Testes, Desenvolvedor, Testador.	Jônatas Kirsch
Patrocinador do Projeto	Prof. Leonardo Garcia de Mello

Escopo do Projeto

Os itens trabalhados no projeto são descritos no documento *Work_Item_List.xls*.

O detalhamento das entregas, iterações, custos e prazos são descritos no documento PlanilhaD*eCustosEsforco.xls.*

Cronograma Macro

O cronograma do projeto é apresentado juntamente com a lista de itens trabalhados no projeto. Documento *ListaDeAtividades.xls*.

Recursos Necessários

Serão utilizados os seguintes *softwares* para o desenvolvimento do trabalho:

- 2 (dois) computadores portáteis: equipamentos utilizados;
- Astah: a ser utilizado para criação de diagramas durante a análise de sistema;
- *Drivers* de impressoras: para digitalizar imagens a serem adicionadas nos documentos;
- *Google Docs*: a ser utilizado para cadastro de defeitos da ferramenta;
- *Google Gmail*: correio eletrônico, utilizado para comunicação e troca de documentos entre os integrantes do trabalho;
- *Microsoft Office:* a ser utilizado para edição de textos, apresentações e planilhas eletrônicas;
- *Microsoft Windows 7* e *Mac OS Snow Leopard*;
- *NetBeans:* ambiente de desenvolvimento de *software*;
- *Notepad:* utilizado para edição rápida de textos que não necessitam de formatação;

- *Oracle 11g Enterprise Edition*: sistema de gerenciamento de banco de dados;
- *Oracle Database 11g Client*: *software* para comunicação entre o cliente e o servidor, para a ferramenta *Via Análise*;
- *Paint* e *Gimp:* edição de imagens;
- *Google Chrome*, *Mozilla Firefox* e *Safari*: navegadores de *internet*.

Riscos do Projeto

Os Riscos do Projeto são descritos no documento ListaDeRiscos.xls.

Equipe

Nome	Responsabilidades
Andrey Bevilacqua	Gerência do Projeto, Análise de Negócio, Arquitetura de Software, Análise de Sistemas, Administração de Banco de Dados e Desenvolvimento
Jônatas Kirsch	Gerência do Projeto, Análise de Negócio, Análise de Sistemas, Análise de Testes, Desenvolvimento e Testes

Gerenciamento das Comunicações

A seguir tem-se o detalhamento das formas de comunicação que serão utilizadas no projeto.

- Reunião sobre o andamento das atividades todas as quintas-feiras;
- Reuniões quinzenais de avaliação de equipe;
- Reuniões quinzenais de avaliação do plano do projeto;
- Reunião de encerramento do projeto ao finalizar o projeto.

APÊNDICE B – Plano da Primeira Iteração

Plano da Primeira Iteração

Via Análise

Responsáveis:

Andrey Bevilacqua

Jônatas Josué Kirsch

Marcos do Projeto

Os marcos do projeto são apresentados juntamente com as iterações, no documento *ListaDeAtividades.xls.*

Objetivos em Alto-Nível

Para a primeira iteração o principal objetivo foi:

- Definir a análise e visão do negócio;
- Realizar a análise dos requisitos do sistema e definição da arquitetura;
- Criar um protótipo inicial do sistema;
- Mitigar riscos;
- Criar plano e casos de testes.

Trabalho e Atribuições

Os detalhamentos dos trabalhos e atribuições são apresentados juntamente com as iterações, no documento *ListaDeAtividades.xls*.

Questões

Issue	Status	Nota
Definição do banco de dados	Ok	Surgiu uma dúvida durante o projeto sobre qual banco de dados deveria ser utilizado. A questão fora esclarecida.

Critérios de Avaliação

Os objetivos iniciais foram alcançados devido ao grande esforço da equipe em buscar conhecimentos sobre o negócio do projeto.

Avaliação

Alvo de avaliação	Métrica de horas trabalhadas por pessoa

Data da avaliação	23/11/2012
Participantes	Andrey Bevilacqua, Jônatas Kirsch
Status do Projeto	OK

- **Avaliação em relação aos objetivos**
  Objetivos foram abordados tendo como premissa o Plano de Iteração.

  Objetivos alcançados para essa iteração.

- **Itens de Trabalho: Planejamento comparado com a atualização completa.**
  Todos os itens planejados foram abordados e concluídos..

APÊNDICE C – Plano da Segunda Iteração

Plano da Segunda Iteração

Via Análise

Responsáveis:

Andrey Bevilacqua

Jônatas Josué Kirsch

Marcos do Projeto

Os marcos do projeto são apresentados juntamente com as iterações, no documento *ListaDeAtividades.xls.*

Objetivos em Alto-Nível

Para a segunda iteração o principal objetivo foi:

- Revisar a análise e visão do negócio;
- Revisar a análise dos requisitos do sistema e definição da arquitetura;
- Revisar plano e casos de testes;
- Criar o plano de configuração;
- Modelar o sistema;
- Modelar e criar o banco de dados;
- Desenvolver todas as funcionalidades de cadastro e o módulo de cálculo do risco;
- Mitigar riscos.
- Gerar os relatórios.

Trabalho e Atribuições

Os detalhamentos dos trabalhos e atribuições são apresentados juntamente com as iterações, no documento *ListaDeAtividades.xls*.

Questões

Issue	Status	Nota
Problemas técnicos relativos a linguagem de programação Java.	Ok	Surgiram dúvidas durante o projeto sobre aspectos técnicos da linguagem de programação Java. As questões foram esclarecidas.

Critérios de Avaliação

Os objetivos foram alcançados devido ao grande esforço da equipe em buscar conhecimentos sobre o negócio do projeto, linguagem de programação Java e banco de dados Oracle.

Avaliação

Alvo de avaliação	Métrica de horas trabalhadas por pessoa
Data da avaliação	14/06/2013
Participantes	Andrey Bevilacqua, Jônatas Kirsch
Status do Projeto	OK

- **Avaliação em relação aos objetivos**
  Objetivos foram abordados tendo como premissa o Plano de Iteração.

  Objetivos alcançados para essa iteração.

- **Itens de Trabalho: Planejamento comparado com a atualização completa.**
  Todos os itens planejados foram abordados e concluídos.

APÊNDICE D – Visão de Negócio

Visão de Negócio

Via Análise

Responsáveis:

Andrey Bevilacqua

Jônatas Josué Kirsch

Dados de Identificação

Projeto: Via Análise

Área de atuação: Desenvolvimento de sistema de análise de riscos de segurança da informação.

Visão de Negócios

Negócio Principal

Via Análise é um projeto de desenvolvimento de software com foco em soluções de análise de riscos de segurança da informação. Seu produto é voltado à organizações da administração pública federal.

Vantagens Competitivas

Tem-se os principais diferenciais competitivos:

- Foco no que diz respeito ao negócio;
- Profissionais altamente capacitados.

Valores

Os valores do projeto Via Análise são:

- Busca contínua pela excelência;
- Cooperação e relações saudáveis;
- Satisfação de desenvolvimento das pessoas.

Fornecedores

O projeto Via Análise não possui necessidade em fornecimento de produto ou mão de obra externa.

Clientes

O sistema Via Análise será desenvolvido para organizações da Administração Pública Federal.

Especificidades

O projeto Via Análise é focado no desenvolvimento de sistema de auxílio a análise de riscos de segurança da informação para organizações da Administração Pública Federal.

Contextualização

Oportunidade de Negócio

As organizações devem lidar com uma quantidade de ameaças muito grande nos dias atuais. Grande parte delas pode eventualmente concretizar-se pela falta de um processo adequado para análise e gestão dos riscos. Portanto, lidamos atualmente com a necessidade de mapear previamente os riscos e preveni-los, minimizando ao máximo sua ocorrência e seus possíveis impactos.

Não praticar gerenciamento de riscos seria ignorar décadas de experiência de muitas empresas bem sucedidas ao redor do mundo, além de criar diversas oportunidades para que esses riscos se tornassem problemas reais. Problemas os quais poderiam definir o futuro de um projeto ou da organização, dependendo do seu impacto.

A análise e gestão de riscos para a segurança da informação tornou-se vital para as organizações, pois a informação é o ativo mais importante para elas. Uma informação confidencial que acabe sendo divulgada põe em risco toda uma possível estratégia da organização, pode impactar em seu futuro, ou gerar uma enorme vantagem competitiva para seus concorrentes.

Devido a isso, a gestão de riscos dos ativos definidos e utilizados dentro da entidade é de extrema importância. Todos os ativos tem um risco que deve ser definido conforme sua probabilidade de ocorrência e seu impacto. Tendo esses dados em vista, é possível direcionar os investimentos da forma correta, a fim de

minimizar ou evitar grande parte das ameaças aos ativos definidos como mais prioritários.

Como exemplo da importância da gestão de riscos, pode-se citar a descoberta de uma falha de segurança no *Bilhete Único*, sistema público de transporte coletivo de São Paulo. Trata-se de um meio de incluir créditos em um cartão e dessa forma utilizá-lo sem pagar (BRANCATELLI; RIBEIRO, 2012). Apontado como “infalível” há sete anos e fonte de uma receita de mais de trezentos milhões de Reais por mês, o sistema é considerado o segundo maior sistema de bilhetagem eletrônico do mundo, atrás apenas do cartão *Octopus* do transporte público de Hong Kong. Tal falha exemplifica a não mitigação de um risco com baixa probabilidade de ocorrência, porém alto impacto. Contudo, a análise e gestão dos riscos do *Bilhete Único* deveriam indicar maiores esforços à minimização dessa ameaça.

Para facilitar o trabalho de análise e gestão dos riscos dos ativos, pode-se desenvolver uma ferramenta que auxilie em: mapeamento dos ativos, mapeamento dos riscos, definição de probabilidade para cada risco, do impacto que esse risco terá caso venha a se tornar realidade e a forma na qual a entidade deve exercer suas atividades de prevenção de risco. A criação dessa ferramenta vai ao encontro do princípio da *eficiência* previsto no Artigo 37 da Constituição Federal (BRASIL, 1988): “A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência”. Aliás, trata-se do mais recente princípio da Administração Pública, pois foi inserido no texto constitucional apenas em 1998, pela Emenda Constitucional nº 19, ao contrário dos demais princípios que já constavam na redação da Constituição desde a data da sua promulgação. A ferramenta poderá ajudar na automação de todo o processo de gestão de riscos dos ativos de segurança da informação, tornando-o mais viável - em relação a tempo e custo de execução - para a organização e disseminando a cultura de gestão de riscos ao mostrar a sua importância e os resultados obtidos no final do processo.

Declaração do Problema

Cada organização pode vir a apresentar peculiaridades no que tange a técnicas e controles para gestão de riscos de segurança da informação e comunicações. Por exemplo, empresas brasileiras que possuam capital aberto em bolsas de valores norte-americanas devem atender os requisitos de controle da Lei Sarbanes-Oxley. Ao levarem-se em conta as características dos órgãos e entidades da administração pública federal, direta e indireta, bem como um conjunto de melhores práticas, tornou-se necessário aos integrantes desse grupo seguirem o disposto na Norma Complementar nº 04/IN01.

Essa norma foi editada pelo Departamento de Segurança da Informação e Comunicações (DSIC), órgão vinculado diretamente ao Gabinete de Segurança Institucional da Presidência da República (GSIPR). Seu objetivo é especificar diretrizes a serem observadas na gestão de riscos vinculados à Tecnologia da Informação e Comunicações.

Contudo, a gestão de riscos de segurança da informação pode ser uma tarefa dispendiosa em vista dos controles eventualmente implementados de modo efetivo. Isso deverá ser feito de modo criterioso, posto que sempre incorrerá algum ônus e raramente conseguirá abranger todas as ameaças às quais uma organização está sujeita.

Segundo publicação do Comitê Gestor da Internet no Brasil (CGI.br), somente em 2012 já foram reportados mais de duzentos mil incidentes de segurança da informação (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012a). Neste cenário de intensos e constantes ataques pela internet, as questões relacionadas a segurança da informação devem ser tratadas como tema sensível nas organizações governamentais. E as questões estratégicas da área de Tecnologia da Informação devem ser discutidas e tratadas de maneira a aprimorar os mecanismos de gestão governamental, visando a melhoria contínua da qualidade dos processos internos e dos serviços prestados à população.

Dessa forma, faz-se necessário a análise, avaliação e tratamento dos riscos, bem como a elaboração sistemática de relatórios para os Gestores de Segurança da Informação e Comunicações. Em seu conteúdo deve constar a análise quanto a aceitação dos resultados obtidos, e consequente proposição de ajustes e de medidas preventivas e proativas à Alta Administração.

Idealmente, as tarefas de análise de riscos e geração dos respectivos relatórios poderiam ser realizadas com a máxima eficiência através do apoio de um sistema automatizado para essa tarefa. Isso representaria uma sensível melhora no cumprimento dessa obrigação para todo um conjunto de organizações públicas.

O problema	Incidentes de segurança da informação e comunicações
Afeta	Organizações da administração pública federal
O impacto é	Alto
Uma solução bem-sucedida seria	Desenvolver um sistema de auxílio a análise de riscos de segurança da informação e comunicações

Tabela 1 – Visão do problema

Objetivos da Modelagem de Negócio

Os objetivos da Modelagem de Negócio são:

- Estimar o tempo e custo necessários para a realização do projeto;
- Priorizar a qualidade do produto.

APÊNDICE E – Estimativas

Conversão de Tamanho em Esforço		
1 UCP =	15	Horas

Distribuição do Esforço no Ciclo de Vida	
Disciplina	**Percentual**
Management (PM+CCM)	10%
Environment	10%
Requirements (+BM)	10%
Analysis & Design	15%
Implementation	25%
Assessment (Test)	25%
Deployment	5%
	100,00%

Complexidade de Use Case			
	Min Transações	**Max Transações**	**UUCP**
Simples		3	5
Médio	4	7	10
Complexo	8		15

Complexidade de Atores			**UUCP**
Simples	através de API	1	1
Médio	através de protocolo	2	2
Complexo	através de GUI	3	3

Fator de Complexidade Técnica
1,085

Fator Ambiental
0,83

Fator de Complexidade Técnica (TCF)	Peso	Influência	Valor
Distributed system	1	0	0
Response or throughput performance objectives	1	4	4
End-user efficiency	1	3	3
Complex internal processing	2	5	10
Code must be reusable	1	5	5
Easy to install	0,5	2	1
Easy to use	0,5	3	1,5
Portable	0,5	5	2,5
Easy to change	1	5	5
Concurrent	1	3	3
Includes special security features	2	5	10
Provides direct access for third parties	1	3	3
Special user-training facilities are required	0,5	1	0,5
TCF = 0.6 + (0.01 * SUM(Peso * Influência))		***1,085***	

Influência	
0	Não há
1	Incidental
2	Moderada
3	Média
4	Significativa
5	Forte

Limites
0,6 <= TCF <= 1,35
0,425 <= EF <= 1,7

Fator Ambiental (EF)	Peso	Influência	Valor
Familiar with development methodology	2	3	6
Application experience	0,5	2	1
Object-oriented experience	1	3	3
Analyst capability	0,5	4	2
Motivation	1	5	5
Stable Requirements	2	5	10
Part-time workers	-1	5	-5
Difficult programming language	-1	3	-3
EF = 1.4 + (-0.03 * SUM(Peso * Influência))		**0,83**	

Tamanho Use Cases		
Use Case	**Qtde Transações**	**UUCP**
UC1 - Cadastramento de mecanismos de controle	1	5
UC2 - Cadastramento de controles	2	5
UC3 - Cadastramento de fontes de vulnerabilidades	1	5
UC4 - Cadastramento de vulnerabilidades	2	5
UC5 - Cadastramento de impactos	1	5
UC6 - Cadastramento de ameaças	2	5
UC7 - Cadastramento de categorias de ativos	1	5
UC8 - Cadastramento de proprietários de ativos	1	5
UC9 - Cadastramento de ativos	8	15
UC10 - Cálculo de risco	20	15
UC11 - Geração de fronteiras de sistemas	6	10
UC12 - Geração de ativos críticos	6	10
UC13 - Geração de ativos sensíveis	6	10
UC14 - Geração de relatório de ameaças, impactos, vulnerabilidades e controles	20	15
	Peso Use Cases	55

Tamanho Atores		
Ator	**Tipo**	**UUCP**
Andrey	3	3
Jônatas	3	3
Peso Atores	**6**	

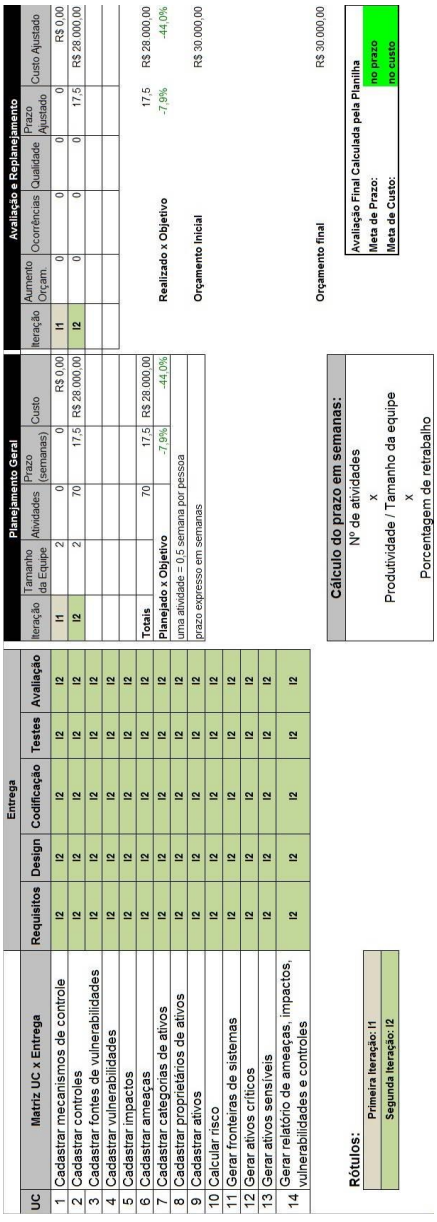
UCP = (Peso Use Cases + Peso Atores) * TCF * EF

⇩

Tamanho =	**55**	**UCPS**
Esforço =	**824**	**horas**

Distribuição do Esforço	
Disciplina	**Esforço**
Management (PM+CCM)	82,40
Environment	82,40
Requirements (+BM)	82,40
Analysis & Design	123,60
Implementation	206,00
Assessment (Test)	206,00
Deployment	41,20
	824,00325

APÊNDICE F – Lista de Atividades



	Entrega					
UC	Matriz UC x Entrega	Requisitos	Design	Codificação	Testes	Avaliação
1	Cadastrar mecanismos de controle	I2	I2	I2	I2	I2
2	Cadastrar controles	I2	I2	I2	I2	I2
3	Cadastrar fontes de vulnerabilidades	I2	I2	I2	I2	I2
4	Cadastrar vulnerabilidades	I2	I2	I2	I2	I2
5	Cadastrar impactos	I2	I2	I2	I2	I2
6	Cadastrar ameaças	I2	I2	I2	I2	I2
7	Cadastrar categorias de ativos	I2	I2	I2	I2	I2
8	Cadastrar proprietários de ativos	I2	I2	I2	I2	I2
9	Cadastrar ativos	I2	I2	I2	I2	I2
10	Calcular risco	I2	I2	I2	I2	I2
11	Gerar fronteiras de sistemas	I2	I2	I2	I2	I2
12	Gerar ativos críticos	I2	I2	I2	I2	I2
13	Gerar ativos sensíveis	I2	I2	I2	I2	I2
14	Gerar relatório de ameaças, impactos, vulnerabilidades e controles	I2	I2	I2	I2	I2

Planejamento Geral				
Iteração	Tamanho da Equipe	Atividades	Prazo (semanas)	Custo
I1	2	0	0	R$ 0,00
I2	2	70	17,5	R$ 28.000,00
Totais		70	17,5	R$ 28.000,00
Planejado x Objetivo			-7,9%	-44,0%
uma atividade = 0,5 semana por pessoa				
prazo expresso em semanas				

Avaliação e Replanejamento					
Iteração	Aumento Orçam.	Ocorrências	Qualidade	Prazo Ajustado	Custo Ajustado
I1	0	0	0	0	R$ 0,00
I2	0	0	0	17,5	R$ 28.000,00
Realizado x Objetivo				17,5	R$ 28.000,00
				-7,9%	-44,0%
Orçamento Inicial					R$ 30.000,00
Orçamento final					R$ 30.000,00

Cálculo do prazo em semanas:

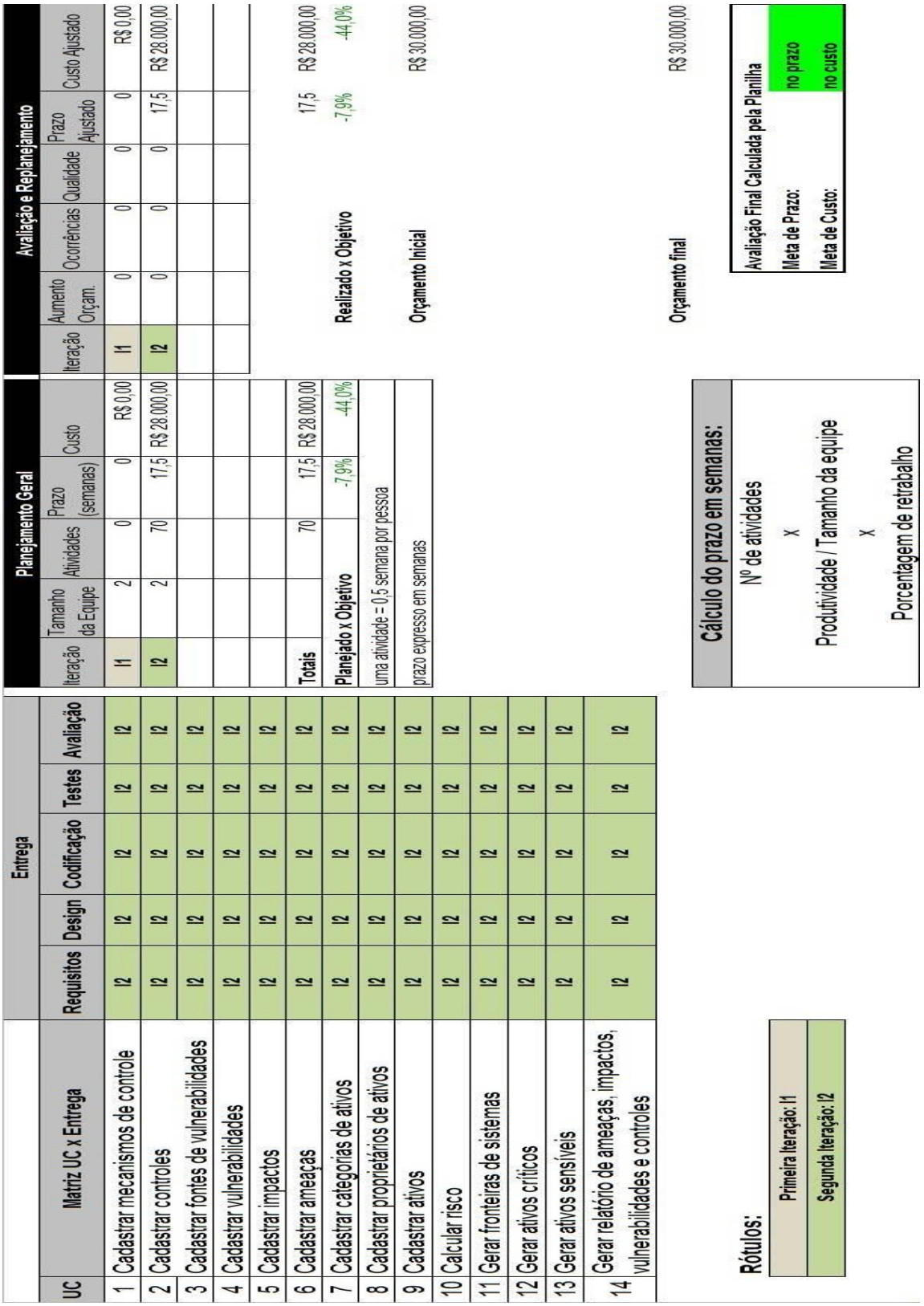
Nº de atividades
x
Produtividade / Tamanho da equipe
x
Porcentagem de retrabalho

Avaliação Final Calculada pela Planilha	
Meta de Prazo:	no prazo
Meta de Custo:	no custo

Rótulos:

- Primeira Iteração: I1
- Segunda Iteração: I2

APÊNDICE G – Planilha de Custo e Esforço



UC	Matriz UC x Entrega	Entrega					
		Requisitos	Design	Codificação	Testes	Avaliação	
1	Cadastrar mecanismos de controle	I2	I2	I2	I2	I2	
2	Cadastrar controles	I2	I2	I2	I2	I2	
3	Cadastrar fontes de vulnerabilidades	I2	I2	I2	I2	I2	
4	Cadastrar vulnerabilidades	I2	I2	I2	I2	I2	
5	Cadastrar impactos	I2	I2	I2	I2	I2	
6	Cadastrar ameaças	I2	I2	I2	I2	I2	
7	Cadastrar categorias de ativos	I2	I2	I2	I2	I2	
8	Cadastrar proprietários de ativos	I2	I2	I2	I2	I2	
9	Cadastrar ativos	I2	I2	I2	I2	I2	
10	Calcular risco	I2	I2	I2	I2	I2	
11	Gerar fronteiras de sistemas	I2	I2	I2	I2	I2	
12	Gerar ativos críticos	I2	I2	I2	I2	I2	
13	Gerar ativos sensíveis	I2	I2	I2	I2	I2	
14	Gerar relatório de ameaças, impactos, vulnerabilidades e controles	I2	I2	I2	I2	I2	

Rótulos:

Primeira Iteração: I1
Segunda Iteração: I2

Planejamento Geral				
Iteração	Tamanho da Equipe	Atividades	Prazo (semanas)	Custo
I1	2	0	0	R$ 0,00
I2	2	70	17,5	R$ 28.000,00
Totais		70	17,5	R$ 28.000,00
Planejado x Objetivo			-7,9%	-44,0%
uma atividade = 0,5 semana por pessoa				
prazo expresso em semanas				

Avaliação e Replanejamento					
Iteração	Aumento Orçam.	Ocorrências	Qualidade	Prazo Ajustado	Custo Ajustado
I1	0	0	0	0	R$ 0,00
I2	0	0	0	17,5	R$ 28.000,00
				17,5	R$ 28.000,00
Realizado x Objetivo				-7,9%	-44,0%
Orçamento Inicial					R$ 30.000,00
Orçamento final					R$ 30.000,00

Cálculo do prazo em semanas:
Nº de atividades
x
Produtividade / Tamanho da equipe
x
Porcentagem de retrabalho

Avaliação Final Calculada pela Planilha	
Meta de Prazo:	no prazo
Meta de Custo:	no custo

APÊNDICE H – Lista de Riscos

Via Análise - Lista de Riscos

ID	Data de Identificação	Nome	Descrição	Tipo	Impacto	Probabilidade	Magnitude	Responsável	Estratégia de Mitigação	Ações Tomadas
1	02/04/2013	Impossibilidade de entregar determinada funcionalidade no prazo.	A equipe não ser capaz de entregar alguma funcionalidade do projeto no prazo estimado por motivos de falta de conhecimento, falta de mão de obra ou problemas de saúde.	Agendamento	5	10%	0,5	Andrey B.	Realizar o monitoramento das atividades e acompanhar possíveis pendências. Utilizar uma ferramenta para auxílio na gerência do projeto.	Analisar possíveis ferramentas gratuítas para auxílio em gestão de projetos.
3	03/04/2013	Ocorrer uma alteração muito grande na norma complementar NC04.	O governo realizar uma alteração muito grande na norma complementar NC04, antes da finalização da criação da ferramenta	Agendamento	5	5%	0,3	Jonatas K.	Acompanhar as notícias e tendências decisivas na área de análise e gestão de riscos do governo federal.	Acompanhamos os processos e novidades da área para sempre estarmos atualizados quanto a sua
4	03/04/2013	Cancelar o projeto por motivos de saúde dos profissionais.	O projeto vir a ser cancelado por motivos de saúde dos profissionais que estão atuando.	Agendamento	5	2%	0,7	Andrey B.	Verificar constantemente o estado de saúde dos profissionais.	A equipe manterá um controle sobre seu estado de saúde para conseguir
5	03/04/2013	Especificações do projeto estarem inválidas com o necessário para a	As especificações mapeadas para o projeto não abrangem todo o necessário para a solução.	Agendamento	3	3%	0,5	Jonatas K.	Validar as especificações do projeto com o proposto na proposta de solução.	Validações realizadas e documento validado.
6	04/04/2013	Ferramenta de desenvolvimento não suportar as especificações do projeto.	A ferramenta que foi selecionada para desenvolver (programar) a solução, não suportar determinadas especificações do projeto.	Agendamento	5	1%	1,0	Andrey B.	Pesquisar e validar se a ferramenta selecionada suporta tal projeto.	Pesquisas e testes foram realizados e a ferramenta foi validada.
7	04/04/2013	Testes não abrangerem todas as funcionalidades desenvolvidas.	A realização/execução dos casos de testes não abrangerem todos os cenários possíveis.	Agendamento	5	2%	0,5	Jonatas K.	Realizar um treinamento para os profissionais de testes.	O profissional que realizou os testes é especialista na área.
8	04/04/2013	Relatórios estarem com informações inválidas.	As informações impressas no relatório estarem inválidas, pois foram inseridas incorretamente no sistema.	Agendamento	4	2%	0,8	Andrey B.	Filtrar qualquer forma de inserir dados incorretos no sistema.	Realizamos diversos filtros ao longo do desenvolvimento do sistema, para prevenir que informações incorretas sejam

APÊNDICE I – Especificação de Requisitos

Especificação de Requisitos

Via Análise

Responsáveis:

Andrey Bevilacqua

Jônatas Josué Kirsch

Introdução

Este documento tem por objetivo descrever os requisitos funcionais e não funcionais do sistema Via Análise. Destina-se a todos os integrantes do projeto.

Propósito

Este documento especifica o sistema Via Análise a ser desenvolvido como Trabalho de Conclusão de Curso na PUCRS, como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação. Seu propósito é especificar os requisitos de alto nível que o sistema deve prover, identificando os requisitos funcionais, não-funcionais, as restrições e as premissas.

Público Alvo

Esse documento destina-se a todos os integrantes do projeto.

Convenções, termos e abreviações

Esta seção explica o conceito de alguns termos importantes que serão mencionados no decorrer deste documento. Estes termos são descritos na tabela a seguir, estando apresentados em ordem alfabética.

Outros termos e abreviações, que sejam padrões do processo estão descritos no documento de Glossário.

Termo	Descrição
Requisitos funcionais	Requisitos técnicos do software que compõe o sistema e que descrevem ações que o sistema deve estar apto a executar, ou seja, o que o sistema deve fazer.
Requisitos não funcionais	Requisitos técnicos do software que compõe o sistema e que descrevem atributos que o sistema deve possuir ou restrições sob as quais ele deve operar.

Prioridades dos requisitos

Para estabelecer a prioridade dos requisitos foram adotadas as denominações “essencial”, “importante” e “desejável”. A prioridade dos requisitos é utilizada no gerenciamento do escopo das etapas do projeto e na definição das prioridades durante o desenvolvimento do sistema.

- **Essencial:** requisito sem o qual o sistema não entra em funcionamento. Requisitos essenciais são requisitos imprescindíveis, os quais devem ser implementados desde as primeiras implantações do sistema.
- **Importante:** requisito sem o qual o sistema entra em funcionamento, porém de forma não satisfatória. Requisitos importantes devem ser implantados o mais rápido possível, mas, se não forem, parte do sistema poderá ser implantada mesmo assim.
- **Desejável:** requisito que não compromete as funcionalidades básicas do sistema, isto é, o sistema pode funcionar de forma satisfatória sem ele. Requisitos desejáveis são requisitos que podem ser implantados por último, ou não implementados, sem comprometer o funcionamento do sistema.

Visão Geral do Sistema

O sistema deverá auxiliar em: mapeamento dos ativos, mapeamento dos riscos, definição de probabilidade para cada risco, do impacto que esse risco terá caso venha a se tornar realidade e a forma na qual a entidade deve exercer suas atividades de prevenção de risco. A criação dessa ferramenta vai ao encontro do princípio da *eficiência* previsto no Artigo 37 da Constituição Federal (BRASIL, 1988): “A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência”. A ferramenta deverá ajudar na automação de todo o processo de gestão de riscos dos ativos de segurança da informação, tornando-o mais viável - em relação a tempo e custo de execução - para a organização e disseminando a cultura de gestão de riscos ao mostrar a sua importância e os resultados obtidos no final do processo.

Restrições e Premissas

Esta seção apresenta todas as Restrições e Premissas do sistema Via Análise.

REST01 - Desenvolvimento e Banco de Dados - Mesmo Fornecedor
O sistema deve ser criado utilizando uma ferramenta de desenvolvimento que seja do mesmo fornecedor do banco de dados que virá a ser utilizado, pois assim existe uma facilitação na manutenção de qualquer uma das soluções, caso venha a ser encontrado algum defeito durante o desenvolvimento do sistema. Posto isto, obtém-se maior segurança para utilizar as soluções existentes no mercado. Esta restrição impacta todos os requisitos funcionais e não funcionais.

REST02 - Cálculo de Risco – Norma Americana
O sistema deve realizar a validação e o cálculo do risco conforme a norma norte-americana *Risk Management Guide for Information Technology Systems*, a qual apresenta a seguinte escala de probabilidade de ameaças: Baixa, Média ou Alta. Para cada uma das escalas, obtém-se os seguintes valores a serem representados: Baixa (de 1 a 10), Média (maior que 10 até 50) e Alta (maior que 50 até 100). Para seguir as definições de valores dos níveis dos riscos, deve ser seguida a tabela *Matriz de Nível de Risco*, conforme o RF009, a qual apresenta a localização dos valores e aonde eles se enquadram, para cada um dos níveis. Esta restrição impacta o requisito funcional RF009 - Cálculo de Risco.

Requisitos Funcionais

Cadastros

Esta seção agrupa os requisitos funcionais relativos à criação, leitura, atualização e remoção de informações no sistema.

RF001 – Mecanismos de Controle
Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

Os requisitos funcionais que possuem dependência com este Requisito Funcional são:

- RF002 – Controles.

O sistema deverá possuir interfaces para cadastro, edição e exclusão de Mecanismos de Controle. Cada mecanismo deverá possuir os seguintes atributos:

Nome	Tipo	Tamanho mínimo	Tamanho máximo
Nome	Alfanumérico	1	250
Descrição	Alfanumérico	0	250

RF002 – Controles

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

Os requisitos funcionais que possuem dependência com este Requisito Funcional são:

- RF003 – Vulnerabilidades;

O sistema deverá possuir interfaces para cadastro, edição e exclusão de Controles. Cada controle deverá possuir os seguintes atributos:

Nome	Tipo	Tamanho mínimo	Tamanho máximo	Opções
Nome	Alfanumérico	1	250	
Descrição	Alfanumérico	0	250	
Tipo	Seleção	1	1	Técnico; Não-Técnico.
Categoria	Seleção	1	1	Preventivo; Detectivo.
Status	Seleção	1	1	Ativo; Inativo.

Restrição da organização	Alfanumérico	1	250	
Custo para implementar em R$	Moeda	1	10	
Tipo de proteção	Seleção	1	1	Correção; Eliminação; Prevenção; Minimização do impacto; Dissuasão; Detecção; Recuperação; Monitoramento; Conscientização.
Forma de Tratamento de Risco	Seleção	0	1	Evitar risco; Reduzir risco; Reter risco; Transferir risco;

Deverá ser possível, mas não obrigatório vincular cada controle a um ou mais mecanismos de controle.

O campo *Restrição da organização* somente deverá ficar habilitado para edição caso o usuário selecione o status *Inativo*.

RF003 – Vulnerabilidades

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

Os requisitos funcionais que possuem dependência com este Requisito Funcional são:

- RF004 – Fontes de vulnerabilidades;
- RF006 – Ameaças;
- RF009 – Ativos.

O sistema deverá possuir interfaces para cadastro, edição e exclusão de Vulnerabilidades. Cada vulnerabilidade deverá possuir os seguintes atributos:

Nome	Tipo	Tamanho mínimo	Tamanho máximo
Nome	Alfanumérico	1	250
Descrição	Alfanumérico	0	250

Deverá ser obrigatório vincular cada vulnerabilidade a uma e apenas uma fonte de vulnerabilidades.

Deverá ser possível, mas não obrigatório vincular cada vulnerabilidade a um ou mais controles.

RF004 – Fontes de Vulnerabilidades

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

O sistema deverá possuir interfaces para cadastro, edição e exclusão de Fontes de Vulnerabilidades. Cada fonte deverá possuir os seguintes atributos:

Nome	Tipo	Tamanho mínimo	Tamanho máximo
Nome	Alfanumérico	1	250
Descrição	Alfanumérico	0	250

Por padrão, no sistema deverão estar cadastradas as seguintes fontes:

- Avaliação de risco anterior;

- Lista de vulnerabilidades;
- Avisos do fornecedor;
- Análise de segurança do sistema.

RF005 - Impactos

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

Os requisitos funcionais que possuem dependência com este Requisito Funcional são:

- RF006 – Ameaças;

O sistema deverá possuir interfaces para cadastro, edição e exclusão de Impactos. Cada impacto deverá possuir os seguintes atributos:

Nome	Tipo	Tamanho mínimo	Tamanho máximo	Opções
Nome	Alfanumérico	1	250	
Descrição	Alfanumérico	0	250	
Tipo	Seleção	1	1	Confidencialidade; Integridade; Disponibilidade.
Gravidade	Seleção	1	1	Alta; Média; Baixa.

RF006 – Ameaças

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

Os requisitos funcionais que possuem dependência com este Requisito Funcional são:

- RF009 – Ativos.

O sistema deverá possuir interfaces para cadastro, edição e exclusão de Ameaças. Cada ameaça deverá possuir os seguintes atributos:

Nome	Tipo	Tamanho mínimo	Tamanho máximo	Opções
Nome	Alfanumérico	1	250	
Descrição	Alfanumérico	0	250	
Origem	Seleção	1	1	Natural; Humana; Ambiental.
Probabilidade de ocorrência de incidente referente a ameaça	Seleção	1	1	A – Frequente; B – Provável; C – Ocasional; D – Remota; E – Improvável; F – Impossível.

Deverá ser obrigatório vincular cada ameaça a, no mínimo, um impacto.

Deverá ser obrigatório vincular cada ameaça a, no mínimo, uma vulnerabilidade. Diz-se que as ameaças exploram determinadas vulnerabilidades.

Como exemplos de ameaças, pode-se citar: desastres naturais, furto, vírus, *hacking*, código escondido, falha de hardware, falha de software, erro humano.

RF007 – Categorias de Ativos

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

Os requisitos funcionais que possuem dependência com este Requisito Funcional são:

- RF009 – Ativos.

O sistema deverá possuir interfaces para cadastro, edição e exclusão de Categorias de Ativos. Cada categoria deverá possuir os seguintes atributos:

Nome	Tipo	Tamanho mínimo	Tamanho máximo
Nome	Alfanumérico	1	250
Descrição	Alfanumérico	0	250

Por padrão, no sistema deverão estar cadastradas as seguintes Categorias de Ativos:

- Ativos de Informação;
- Ativos de Software;
- Ativos Físicos;
- Serviços;
- Pessoas e suas habilidades;
- Intangíveis.

RF008 – Responsáveis por Ativos

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

Os requisitos funcionais que possuem dependência com este Requisito Funcional são:

- RF009 – Ativos.

O sistema deverá possuir interfaces para cadastro, edição e exclusão de Responsáveis por Ativos. Cada responsável deverá possuir os seguintes atributos:

Nome	Tipo	Tamanho mínimo	Tamanho máximo

Nome	Alfanumérico	1	250
Telefone	Alfanumérico	1	15
Registro na organização	Alfanumérico	1	250
Email	Alfanumérico	1	255

RF009 – Ativos

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

Os requisitos funcionais que possuem dependência com este Requisito Funcional são:

O sistema deverá possuir interfaces para cadastro, edição e exclusão de Ativos. Cada ativo deverá possuir os seguintes atributos:

Nome	Tipo	Tamanho mínimo	Tamanho máximo	Opções
Nome	Alfanumérico	1	250	
Descrição	Alfanumérico	0	250	
Formato	Seleção	1	1	Físico; Eletrônico.
Localização	Alfanumérico	1	250	
Informações sobre cópias de segurança	Alfanumérico	1	250	
Informações sobre licenças	Alfanumérico	1	250	
Importância do ativo para o negócio	Seleção	1	1	Muito importante; Importante; Média importância; Pouco importante;

				Sem importância.
Custo em R$	Moeda	1	10	

Cada ativo deverá pertencer a uma categoria de ativos, descrita no RF007 – Categorias de Ativos.

Cada ativo deverá possuir um responsável por ativo, descrito no RF008 – Responsáveis por Ativos.

Deverá ser possível, mas não obrigatório vincular cada ativo a uma ou mais ameaças.

Ao criar ou editar o cadastro de um ativo, se o usuário selecionar uma ameaça, então o sistema deverá exibir uma lista de todas as vulnerabilidades vinculadas a ameaça selecionada.

Deverá ser possível, mas não obrigatório vincular cada ativo a uma ou mais vulnerabilidades.

Ao criar ou editar o cadastro de um ativo, se o usuário selecionar uma vulnerabilidade, então o sistema deverá exibir uma lista de todos os controles vinculados à vulnerabilidade selecionada.

Deverá ser possível, mas não obrigatório vincular cada ativo a um ou mais controles.

RF010 – Incidentes

Prioridade: ☐ Essencial ☐ Importante ☑ Desejável

O sistema deverá possuir interfaces para cadastro, edição e exclusão de Incidentes. Cada incidente deverá possuir os seguintes atributos:

Nome	Tipo	Tamanho mínimo	Tamanho máximo	Opções
Nome	Alfanumérico	1	250	
Descrição	Alfanumérico	0	250	
Data	Data, formato	1	1	

	dd/mm/aaaa			
Característica de segurança	Seleção	1	3	Confidencialidade; Disponibilidade; Integridade.
Perda para o negócio	Seleção	1	1	Alta; Média; Baixa.

Deverá ser obrigatório selecionar no mínimo um ativo ao qual o incidente aconteceu.

Após o usuário selecionar o ativo, o sistema deverá carregar a lista de ameaças às quais o ativo está sujeito. Deverá ser possível, mas não obrigatório, relacionar o incidente a uma ou mais ameaças em cada ativo. Caso não haja ameaça relacionada a um ativo selecionado, o campo de seleção de ameaças deverá ficar desabilitado.

Metodologia

Esta seção apresenta os requisitos funcionais referentes à forma como os riscos são calculados pelo sistema.

RF011 – Cálculo de Risco

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

O sistema deverá possuir uma funcionalidade para calcular a relação probabilidade/impacto dentro das informações inseridas pelo usuário, gerando as informações de cálculo de risco. Essa funcionalidade tem como entrada as informações de ameaças, vulnerabilidades e impactos.

O sistema deverá realizar a validação e o cálculo do risco conforme a norma norte-americana *Risk Management Guide for Information Technology Systems*, a qual apresenta a seguinte escala de probabilidade de ameaças: Baixa, Média ou Alta. Para cada uma das escalas, obtém-se os seguintes valores a serem representados:

Baixa (de 1 a 10), Média (maior que 10 até 50) e Alta (maior que 50 até 100). Para seguir as definições de valores dos níveis dos riscos, deverá ser seguida a tabela *Matriz de Nível de Risco* a seguir, a qual apresenta a localização dos valores e aonde eles se enquadram, para cada um dos níveis.

Essa funcionalidade deverá realizar o cálculo do risco da seguinte forma:

Probabilidade de ocorrência da Ameaça	**Impacto**		
	Baixo (10)	**Médio** (50)	**Alto** (100)
Alta (1.0)	**Baixo** 10 x 1,0 = 10	**Médio** 50 x 1,0 = 50	**Alto** 100 x 1,0 = 100
Média (0.5)	**Baixo** 10 x 0,5 = 5	**Médio** 50 x 0,5 = 25	**Médio** 100 x 0,5 = 50
Baixa (0.1)	**Baixo** 10 x 0,1 = 1	**Baixo** 50 x 0,1 = 5	**Baixo** 100 x 0,1 = 10

Matriz de Nível de Risco

Relatórios

Esta seção descreve as saídas geradas pelo sistema Via Análise.

RF012 – Fronteiras de Sistemas

Prioridade: ☐ Essencial ☐ Importante ☑ Desejável

O sistema deverá possuir a funcionalidade de geração de relatório com as fronteiras dos sistemas. Esse relatório deverá conter o nome de todos os ativos e, para cada ativo, deverá exibir todos os ativos relacionados a ele agrupados por categoria.

Exemplo de relatório:

Ativo: Banco de Dados Oracle

Fronteiras do sistema:

- Ativos de Software:
    - Via Análise;
- Ativos Físicos:
    - Computador X
- Informações:
    - Análise de Riscos de Segurança da Informação e Comunicações

---

RF013 – Ativos Críticos

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

O sistema deverá possibilitar a geração de relatório contendo o nome, probabilidade de ocorrência, ameaças e responsáveis por todos os ativos cuja importância para o negócio seja Muito Importante, Importante ou Média Importância. As informações deverão estar agrupadas por categoria de ativos.

RF014 – Ativos Sensíveis

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

O sistema deverá possibilitar a geração de relatório contendo todos os ativos vinculados a ameaças cujo risco seja Alto, Médio e/ou Baixo. Para tanto, o sistema deverá executar os passos a seguir:

1º. Para cada ativo cadastrado, o sistema deverá verificar as ameaças vinculadas ao ativo.

2º. Em seguida, o sistema deverá verificar o impacto relacionado a cada ameaça. Tendo verificado o impacto, o sistema deverá verificar a gravidade do impacto.

3º. Então, o sistema deverá realizar o Cálculo de Risco descrito no RF011 para encontrar o risco.

O sistema deverá permitir ao usuário selecionar os níveis de risco que ele deseja visualizar no relatório: Alto, Médio e/ou Baixo.

RF015 – Relatório de Incidentes

Prioridade: ☐ Essencial ☐ Importante ☑ Desejável

Deverá ser possível gerar relatório contendo todos os incidentes e ativos vinculados aos incidentes.

Deverão existir duas opções de geração do relatório de ataques:

1. Todos os incidentes;
2. Incidentes a ativos sem ameaças previstas.

Caso o usuário selecione a primeira opção, o sistema deverá gerar relatório contendo todos os incidentes e seus respectivos ativos e ameaças.

Se o usuário selecionar a segunda opção, o sistema deverá gerar relatório dos incidentes cujos ativos não possuem vínculo com ameaça. Dado um incidente vinculado a um ativo pelo *RF010 – Incidentes*, o sistema deverá verificar os ativos vinculados ao incidente e, para cada ativo, verificar se há alguma ameaça relacionada. Se não houver ameaça relacionada ao ativo, o sistema deverá incluir o incidente e o ativo no relatório.

RF016 – Relatório de Ameaças, Impactos, Vulnerabilidades e Controles

Prioridade: ☐ Essencial ☐ Importante ☑ Desejável

Deverá ser possível gerar relatório contendo todos os dados referentes às ameaças, às vulnerabilidades que exploram cada ameaça, aos impactos relacionados às ameaças e aos controles relacionados às vulnerabilidades, se houver.

O sistema deverá possuir duas opções de geração deste relatório no que tange aos ativos:

1. Exibir ativos relacionados às ameaças;
2. Não exibir ativos relacionados às ameaças.

Se o usuário selecionar a primeira opção, então o sistema deverá gerar o relatório com todas as informações descritas no primeiro parágrafo acrescidas dos ativos vinculados a cada ameaça. Tais ativos deverão ser exibidos agrupados por categoria de ativos.

O sistema também deverá possuir uma opção que permita selecionar os controles a serem exibidos de acordo com o status dos controles, ou exibir as vulnerabilidades que não possuam controles:

1. Exibir apenas controles ativos;
2. Exibir apenas controles inativos;
3. Exibir todos os controles;
4. Exibir vulnerabilidades sem controle

O sistema também deverá exibir os riscos e deverá permitir ao usuário selecionar os níveis de risco que ele deseja visualizar no relatório: Alto, Médio e/ou Baixo.

Para cada risco, o sistema deverá exibir um campo de seleção “Aceitar risco?” através do qual o usuário poderá selecionar se deseja aceitar o risco ou não aceita-lo. Por padrão, o campo deverá estar desmarcado, o que significa não aceitar o risco.

O sistema deverá sinalizar caso o custo para implementar o controle seja maior que o custo do ativo.

Requisitos Não Funcionais

Esta seção apresenta todos os requisitos não funcionais do sistema Via Análise.

RNF01 - Performance

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

Todas as funcionalidades referentes a Cadastro deverão ter seu processamento concluído em menos de 2 segundos, contatos a partir do momento em que o usuário clica em determinado botão ou campo de seleção. Os Requisitos Funcionais impactados são todos os requisitos descritos na seção *4.1 Cadastros*.

A soma do tempo de resposta referente ao processamento das funcionalidades da Metodologia e dos Relatórios deverá ser inferior a 5 segundos. Todos os Requisitos Funcionais das seções *4.2 Metodologia* e *4.3 Relatórios* são impactados por esse requisito.

RNF02 - Segurança

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

Segurança é o Requisito Não Funcional mais importante do sistema Via Análise.

O sistema deverá possuir interface para cadastro de usuários. Somente o usuário com perfil de Administrador deverá ter permissão para cadastrar novos usuários.

Durante o cadastro ou alteração de usuário, o sistema deverá exigir a digitação de senhas com no mínimo os seguintes atributos:

- 4 caracteres especiais;
- 4 números;
- 4 letras;
- 1 letra maiúscula.

Todas as senhas utilizadas no sistema, tais como senhas para comunicação com banco de dados, também deverão seguir as regras descritas no parágrafo anterior.

O sistema não deverá possuir interface web.

O sistema não deverá permitir a exportação dos dados referentes aos Requisitos Funcionais da seção *4.1 Cadastros*.

RNF03 - Usabilidade

Prioridade: ☐ Essencial ☑ Importante ☐ Desejável

O sistema Via Análise será operado por profissionais de Tecnologia da Informação.

O sistema deverá possuir interface gráfica. Todos os nomes de campos e opções deverão possuir nomenclatura que os identifiquem de forma clara.

Todos os componentes de tela deverão estar alinhados.

Todas as funcionalidades do sistema deverão estar acessíveis através de um menu na parte superior da interface gráfica.

Todos os componentes do sistema deverão ser acessíveis através do teclado mediante o uso das teclas *Tab*, S*etas*, *Enter*, ou combinação de teclas.

RNF04 - Confiabilidade

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

Os dados gravados no sistema não poderão ser alterados sem que o usuário confirme a intenção de alterá-los bem como a plataforma deve ser robusta para não haver perda de dados.

Caso um ser humano realize todos os cálculos e verificações do sistema previstas nesta Análise de Requisitos, deverá ser possível prever o resultado a ser gerado pelo sistema.

RNF05 - Portabilidade

Prioridade: ☐ Essencial ☑ Importante ☐ Desejável

Deverá ser possível utilizar o sistema Via Análise em qualquer sistema operacional desktop.

RNF06 – Adequação a padrões

Prioridade: ☑ Essencial ☐ Importante ☐ Desejável

O sistema deverá ser desenvolvido com paradigma de Orientação a Objetos.

Matriz de Rastreabilidade

Esta seção indica o relacionamento existente entre os requisitos funcionais com o objetivo de facilitar as consultas e manutenções no documento. Através da Matriz de

Rastreabilidade é possível identificar rapidamente os vínculos existentes entre os requisitos.

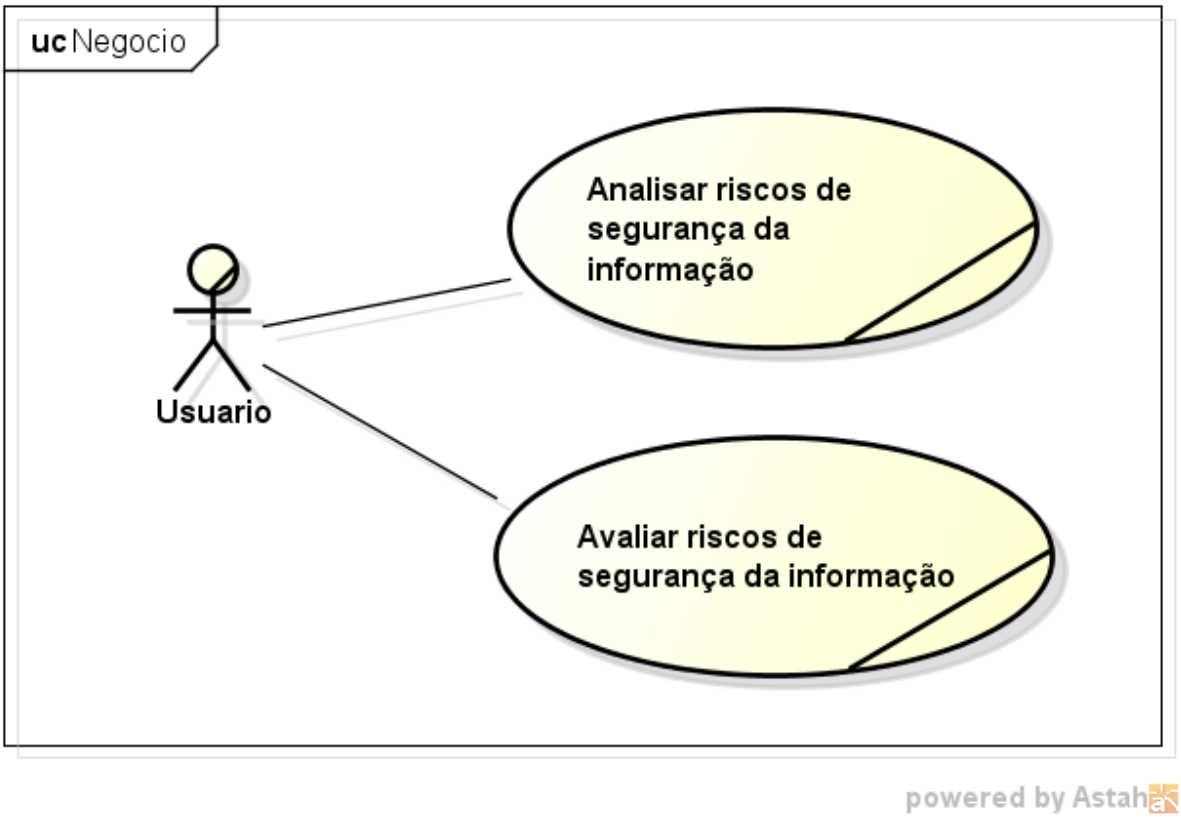
Requisito Funcional	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1		X										X	X	X	X	
2			X									X	X	X	X	
3						X			X			X	X	X	X	
4			X									X	X	X	X	
5									X		X	X	X	X	X	
6									X		X	X	X	X	X	
7									X			X	X	X	X	
8									X							
9												X	X	X	X	
10																X
11												X	X	X	X	
12																
13																
14																
15																
16																

Escopo Negativo

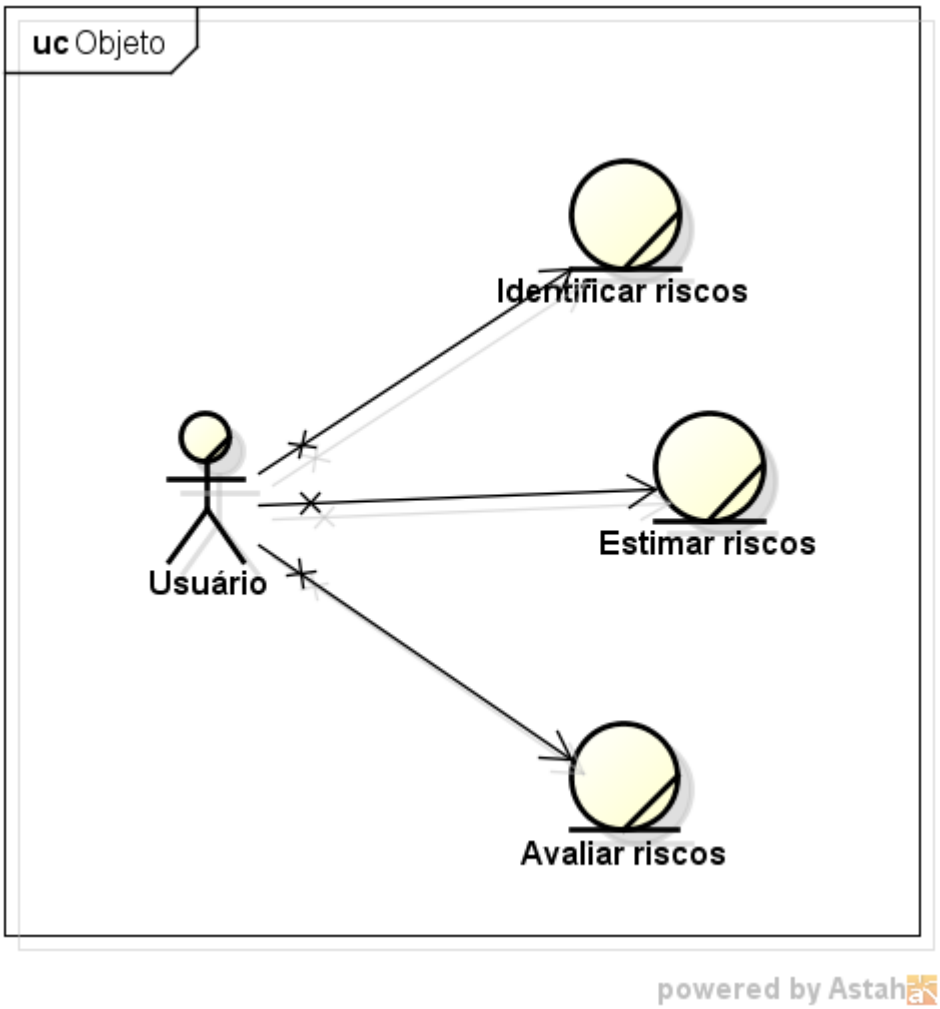
Quanto a funcionalidades futuras, o sistema será desenvolvido com o objetivo de receber diversas alterações e, portanto, estará apto a receber novos tipos de relatórios, alterar sua interface gráfica ou alterar a regra de negócio referente às métricas, caso venha a ser implementada uma nova norma complementar ou alterada a lei referente a qual foi desenvolvido o escopo deste projeto. Além dos

pontos citados acima, futuramente poderão ser implementadas diretivas de acesso com controle de funcionalidades e relatórios para determinados usuários.

APÊNDICE J – Diagrama de Casos de Uso de Negócio



APÊNDICE K – Diagrama de Casos Uso de Negócio - Objetos



APÊNDICE L – Plano de Gerenciamento de Configuração

Plano de Gerenciamento de Configuração

Via Análise

Responsáveis:

Andrey Bevilacqua

Jônatas Josué Kirsch

Introdução

O Plano de Gerenciamento de Configuração descreve todas as atividades do Gerenciamento de Controle de Configuração e Mudança que serão executadas durante o ciclo de vida do produto. Suas atividades envolvem identificar a configuração do software, manter sua integridade durante o projeto e controlar sistematicamente as mudanças. A finalidade deste documento é criar um padrão a ser seguido por todos os membros da equipe com o intuito de garantir o maior controle do produto no decorrer do projeto.

Gerenciamento de Configuração de Software

Papeis na Gerência de Configuração

Andrey Bevilacqua está encarregado de manter a documentação, comunicação com a equipe e auditoria atualizada com todas as partes.

Identificação de documentos

Os documentos do projeto devem ser nomeados seguindo o padrão a seguir:
NomeDoArquivo.ext sendo *ext* a extensão do documento (doc, xls, etc).

Versões dos documentos

O sistema sistema de gerenciamento de configuração gerará uma nova versão do documento a cada vez que o usuário gravar novas alterações. Dessa forma, tem-se a visibilidade de todas as vezes que o documento foi alterado bem como será possível voltar a versão mesmo da alteração mais recente.

Ferramenta de Gerenciamento de Configuração

Será utilizada a ferramenta DropBox para controlar a versão de todos os artefatos gerados no projeto. Trata-se de um disco virtual com funções de armazenamento e compartilhamento de arquivos e pastas on-line. A troca de arquivos entre usuários é totalmente segura, pois a transferência de arquivos usa SSL. Dropbox permite visualizar de forma fácil todas as versões dos arquivos.

Localização dos artefatos

Todos os artefatos do projeto devem ser armazenados no diretório TCC, compartilhado entre os integrantes da equipe.

Critérios de escolha dos itens de configuração

Todos os artefatos do projeto deverão sofrer controle de versão. Isto se deve ao fato de a equipe trabalhar de forma distribuída na maior parte do tempo.

Ferramentas utilizadas

- *Google Docs*: a ser utilizado para cadastro de defeitos da ferramenta;
- *Google Gmail*: correio eletrônico, utilizado para comunicação e troca de documentos entre os integrantes do trabalho;
- *Microsoft Office:* a ser utilizado para edição de textos, apresentações e planilhas eletrônicas;
- *Microsoft Windows 7* e *Mac OS Snow Leopard*;
- *NetBeans:* ambiente de desenvolvimento de *software*;
- *Notepad:* utilizado para edição rápida de textos que não necessitam de formatação;
- *Oracle 11g Express Edition*: sistema de gerenciamento de banco de dados;
- *Oracle Database 11g Client*: *software* para comunicação entre o cliente e o servidor, para a ferramenta *Via Análise*;
- *Paint* e *Gimp:* edição de imagens;
- *Google Chrome*, *Mozilla Firefox* e *Safari*: navegadores de *internet*.

Estrutura do Ambiente

Ambiente	Descrição	Transição
Desenvolvimento	É o ambiente que servirá para o desenvolvimento do Sistema.	O componente atingirá a maturidade quando os requisitos forem supridos e testados pelos desenvolvedores através dos testes unitários.

Integração	É o ambiente que servirá para os testes de integração.	Quando a comunicação entre os módulos atinge o um estagio satisfatório de funcionamento, ou seja, não deverão existir erros de integração entre os subsistemas.
Banco de Dados	É o ambiente onde estará o banco de dados.	Ambiente onde estará o banco de dados do sistema.

***Baselines* do projeto**

Baseline	Descrição	Padrão de identificação
Arquivos de documentação da gestão do projeto.	Todos os arquivos no formato .doc, .pdf, .docx, .xls, .xlsx, .asta devem ser armazenados na respectiva pasta correspondente ao assunto do documento. Ex.: “\Gerenciamento de Projeto” se o documento trata-se de um documento do gerenciamento do projeto.	Ex.: NomeDoArquivo.ext
Projeto de design de interface do projeto	Todos os arquivos no formato png ou jpg relacionados ao projeto de interface	Ex.: NomeDoArquivo.ext
Código do projeto	Tanto o código fonte de	Seguir os padrões de

	build quanto o código fonte da versão em andamento.	nomenclatura do Framework utilizado.

APÊNDICE M – Documento de Arquitetura

Documento de Arquitetura

Via Análise

Responsáveis:

Andrey Bevilacqua

Jônatas Josué Kirsch

Propósito

Este documento descreve a arquitetura que será usada no sistema de auxílio a análise e gestão de riscos de segurança da informação e comunicações Via Análise. Serão apresentados alguns aspectos importantes do sistema, como por exemplo, decisões de quais padrões de projetos que deverão ser adotados e quais os requerimentos mínimos de software/hardware serão requisitos para rodar o sistema.

Objetivos e Filosofia da Arquitetura

O sistema será desenvolvido na linguagem Java, utilizando ambiente Desktop para execução. A escolha do ambiente desktop foi devido a importância da segurança dos dados que serão levantados e gravados nessa aplicação. Como a finalidade dela é a geração de análise de riscos sobre todos os ativos de informação da organização, casos esses dados venham a se tornar expostos de forma incorreta, eles poderiam apresentar um mapa das fraquezas dessa organização. O ambiente sendo desktop consegue-se reduzir a probabilidade de acesso indevido.
O banco de dados a ser utilizado será Oracle, na última versão disponibilizada pelo fornecedor. Essa escolha também foi importante pelo fato de o fornecedor do banco de dados ser o mesmo da linguagem de programação, facilitando qualquer suporte que venha a ser necessário e centralizando a manutenção em apenas um fornecedor, tornando o processo de gestão da aplicação mais simples.

Suposições e Dependências

A arquitetura requer que seja desenvolvida por um time com experiência em Java Desktop, Orientação a Objetos, SQL, performance de consultas e interação humano/computador, para tratamento de interfaces. Será necessário a existência de um servidor provedor do banco de dados e da conexão com a aplicação.

Requisitos da Arquitetura

Itens necessários para o desenvolvimento da arquitetura:

- Interface desktop;
- Sistema de login;

- Algoritmos de criação, atualização, leitura e exclusão de dados referente a todas as funcionalidades descritas no documento de análise de requisitos;
- Abstrações para a camada de persistência;
- Geração dos relatórios solicitados.

Decisões, Restrições e Justificativas

- A arquitetura define que o sistema deverá funcionar em ambiente Oracle, com Java desktop, pois o ambiente de utilização da ferramenta será basicamente em Windows 7 e ambientes Linux.
- Cada funcionalidade do sistema deverá implementar a definição de CRUD (create, read, update e delete), para obter uma interface de geração dos dados a serem inseridos e lidos no sistema.
- Não será aceito que a arquitetura dependa de programas externos ou plataforma.

A interface principal deverá ser simples, utilizando somente o necessário para funcionar. Serão evitadas tecnologias que dependam de sistema operacional ou extensões proprietárias.

Mecanismos Arquiteturais

Interface desktop

O aplicativo irá rodar em ambiente desktop.

Sistema de login

Servirá para garantir a confidencialidade das informações armazenadas no sistema.

Algoritmo para inserção e leitura de dados

Todas as funcionalidades do sistema irão apresentar telas de criação, atualização, leitura e exclusão de dados no sistema. Isso tornará possível a

integridade dos dados inseridos por um usuário conhecedor das regras de negócio da organização e com permissão de acesso e utilização do sistema.

Abstrações para a camada de persistência

A camada de persistência irá definir o tipo de cálculo a ser utilizado para verificação de probabilidade/impacto dos ativos e riscos inseridos no sistema. Ela será uma camada separada, a qual estará apta a ser alterada caso esse cálculo seja alterado futuramente.

Geração de relatórios

- Essa funcionalidade irá permitir a geração de diversos relatórios pré-definidos na ferramenta, os quais irão servir para auxílio na gestão dos riscos dos ativos de informação e comunicações.

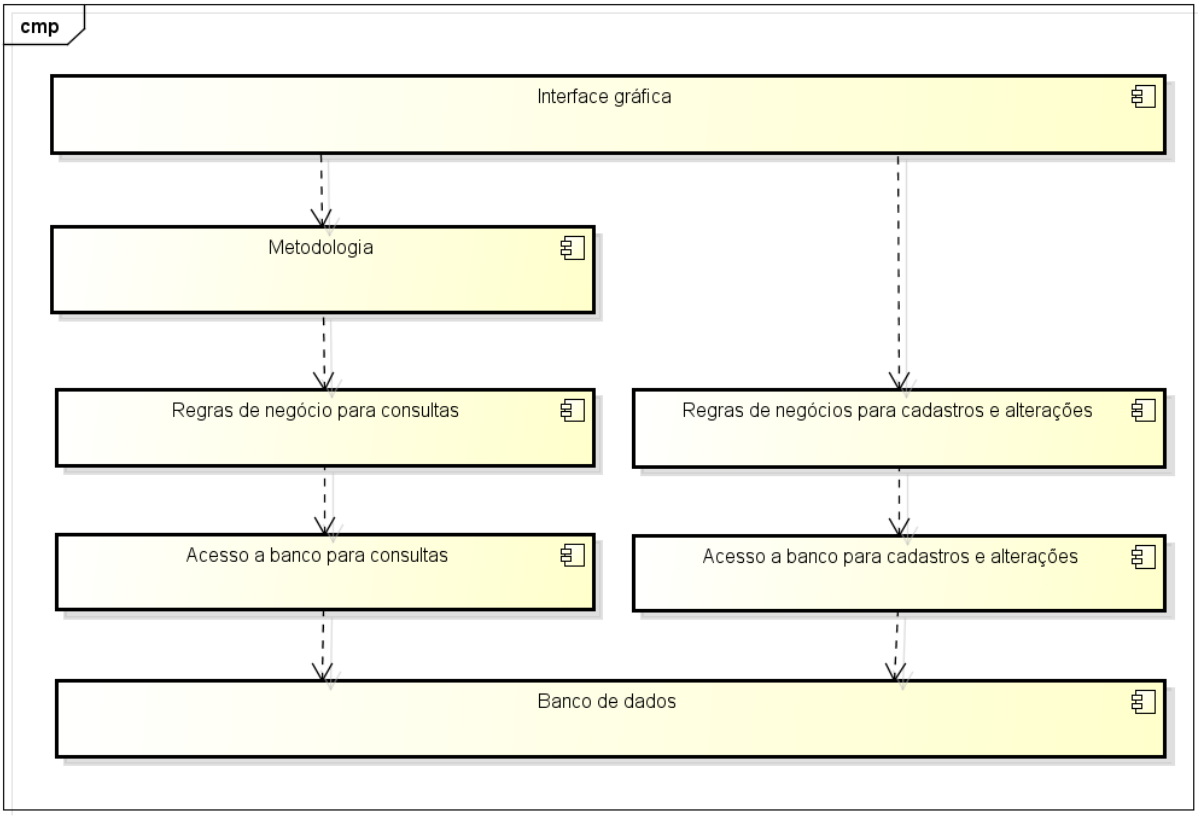
Abstrações-Chave

Abstração do módulo de cálculo de risco, para que possa ser alterado futuramente.

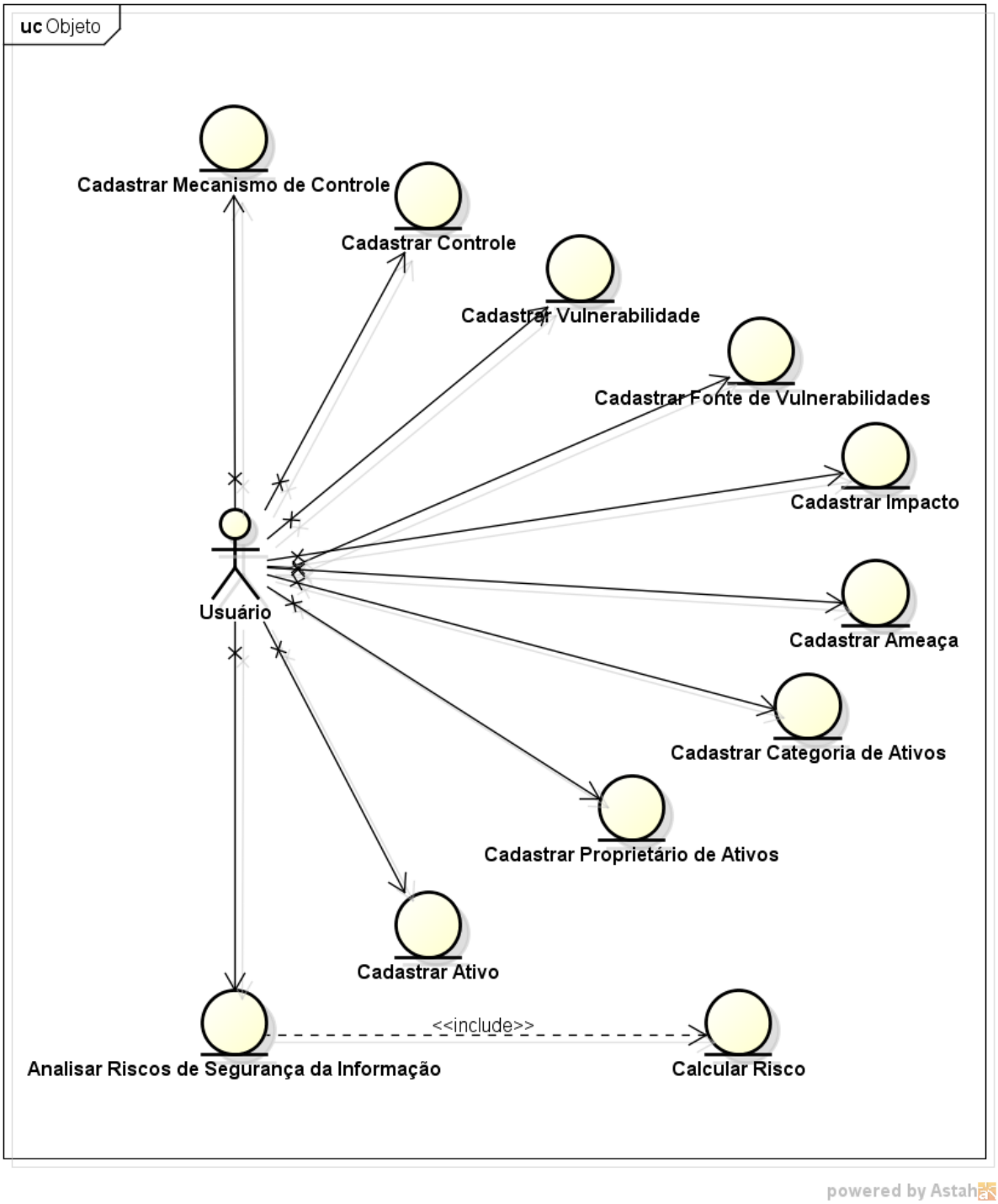
Camadas ou Frameworks da Arquitetura

A arquitetura está separada em cinco camadas distintas: (1) interface gráfica, a qual tratará apenas da interface com o usuário e poderá ser alterada a qualquer momento, sem impactar na aplicação; (2) Metodologia, a qual é a camada que trata do cálculo da probabilidade/impacto dos riscos dos ativos e também poderá ser alterada a qualquer momento, caso o tipo de cálculo venha a ser alterado futuramente; (3) regras de negócio do sistema, separadas em regras de negócio para consultas e regra de negócio para cadastros e alterações; (4) acesso ao banco de dados, camada a qual também se divide em duas partes, uma para consultas e outra para inserções e alterações; e (5) a camada de banco de dados, a qual trata de solicitações, acessos, conexões, dentre outros.

APÊNDICE N – Diagrama de Componentes



APÊNDICE O – Diagrama de Casos de Uso de Sistema - Objetos



APÊNDICE P – Casos de Uso

Casos de Uso

Via Análise

Responsáveis:

Andrey Bevilacqua

Jônatas Josué Kirsch

Introdução

Este documento tem por objetivo descrever os casos de uso do sistema Via Análise. Destina-se a todos os integrantes do projeto.

Público Alvo

Esse documento destina-se a todos os integrantes do projeto.

Casos de Uso

Cadastros

Esta seção agrupa os casos de uso das funcionalidades relativas à inclusão de informações no sistema.

UC001 – Inclusão de Mecanismo de Controle

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Cadastrar mecanismo de controle no sistema.	
Pré-Condições: Estar logado no sistema.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Arquivo > Novo Mecanismo de Controle.
3.	O sistema exibe uma interface solicitando as seguintes informações: 3.1 Nome 3.2 Descrição
4.	O usuário digita as informações nos campos específicos da interface e clica em Gravar.
5.	O sistema verifica se existe um Mecanismo de Controle com o nome informado pelo usuário.
6.	O sistema grava as informações no banco de dados.

Nº	Cenário Alternativo
5.a	O sistema identifica que já existe um Mecanismo de Controle com o nome informado e exibe a mensagem: “Registro já cadastrado. Por favor, escolha outro nome.” e retorna ao passo 3.

UC002 – Inclusão de Controle

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Cadastrar controle no sistema.	
Pré-Condições: Estar logado no sistema.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Arquivo > Novo Controle.
3.	O sistema exibe uma interface solicitando as seguintes informações: 3.1 Nome 3.2 Tipo (Técnico ou Não Técnico) 3.3 Categoria (Preventivo ou Detectivo) 3.4 Status (Ativo ou Inativo) 3.5 Restrição da Organização 3.6 Tipo de Proteção (Correção, Eliminação, Prevenção, Minimização do impacto, Dissuasão, Detecção, Recuperação, Monitoramento, ou Conscientização) 3.7 Forma de Tratamento de Risco (Evitar risco, Reduzir risco, Reter risco, ou Transferir risco) 3.7 Custo para implementar em R$ 3.8 Mecanismos de controle 3.9 Descrição
4.	O usuário digita e seleciona as informações nos campos específicos da interface e clica em Gravar.
5.	O sistema verifica se existe um Controle com o nome informado pelo usuário.

6.	O sistema grava as informações no banco de dados.
Nº	**Cenário Alternativo**
3.5.a	O sistema identifica que o Status é Inativo e desabilita o campo Restrição da Organização.
5.a	O sistema identifica que já existe um Controle com o nome informado e exibe a mensagem: “Registro já cadastrado. Por favor, escolha outro nome.” e retorna ao passo 3.

UC003 – Inclusão de Fonte de Vulnerabilidade

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Cadastrar fonte de vulnerabilidade no sistema.	
Pré-Condições: Estar logado no sistema.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Arquivo > Nova Fonte de Vulnerabilidade.
3.	O sistema exibe uma interface solicitando as seguintes informações: 3.1 Nome 3.2 Descrição
4.	O usuário digita e seleciona as informações nos campos específicos da interface e clica em Gravar.
5.	O sistema verifica se existe uma Fonte de Vulnerabilidade com o nome informado pelo usuário.
6.	O sistema grava as informações no banco de dados.
Nº	**Cenário Alternativo**
5.a	O sistema identifica que já existe uma Fonte de Vulnerabilidade com o nome

	informado e exibe a mensagem: “Registro já cadastrado. Por favor, escolha outro nome.” e retorna ao passo 3.

UC004 – Inclusão de Vulnerabilidade

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Cadastrar vulnerabilidade no sistema.	
Pré-Condições: Estar logado no sistema.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Arquivo > Nova Vulnerabilidade.
3.	O sistema exibe uma interface solicitando as seguintes informações: 3.1 Nome 3.2 Fonte de Vulnerabilidade 3.3 Controles 3.4 Descrição
4.	O usuário digita e seleciona as informações nos campos específicos da interface e clica em Gravar.
5.	O sistema verifica se existe uma Vulnerabilidade com o nome informado pelo usuário.
6.	O sistema grava as informações no banco de dados.
Nº	**Cenário Alternativo**
5.a	O sistema identifica que já existe uma Vulnerabilidade com o nome informado e exibe a mensagem: “Registro já cadastrado. Por favor, escolha outro nome.” e retorna ao passo 3.

UC005 – Inclusão de Impacto

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Cadastrar impacto no sistema.	
Pré-Condições: Estar logado no sistema.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Arquivo > Novo Impacto.
3.	O sistema exibe uma interface solicitando as seguintes informações: 3.1 Nome 3.2 Tipo (Confidencialidade, Integridade ou Disponibilidade) 3.3 Gravidade (Alta, Média ou Baixa) 3.4 Descrição
4.	O usuário digita e seleciona as informações nos campos específicos da interface e clica em Gravar.
5.	O sistema verifica se existe um Impacto com o nome informado pelo usuário.
6.	O sistema grava as informações no banco de dados.
Nº	**Cenário Alternativo**
5.a	O sistema identifica que já existe um Impacto com o nome informado e exibe a mensagem: “Registro já cadastrado. Por favor, escolha outro nome.” e retorna ao passo 3.

UC006 – Inclusão de Ameaça

Ator(es): Todos os usuários cadastrados no sistema.
Objetivo: Cadastrar ameaça no sistema.
Pré-Condições:

Estar logado no sistema.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Arquivo > Nova Ameaça.
3.	O sistema exibe uma interface solicitando as seguintes informações: 3.1 Nome 3.2 Tipo (Confidencialidade, Integridade ou Disponibilidade) 3.3 Gravidade (Alta, Média ou Baixa) 3.4 Descrição
4.	O usuário digita e seleciona as informações nos campos específicos da interface e clica em Gravar.
5.	O sistema verifica se existe uma Ameaça com o nome informado pelo usuário.
6.	O sistema grava as informações no banco de dados.
Nº	**Cenário Alternativo**
5.a	O sistema identifica que já existe uma Ameaça com o nome informado e exibe a mensagem: “Registro já cadastrado. Por favor, escolha outro nome.” e retorna ao passo 3.

UC007 – Inclusão de Categoria de Ativo

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Cadastrar categoria de ativo no sistema.	
Pré-Condições: Estar logado no sistema.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Arquivo > Nova Categoria de Ativo.
3.	O sistema exibe uma interface solicitando as seguintes informações:

	3.1 Nome 3.2 Descrição
4.	O usuário digita e seleciona as informações nos campos específicos da interface e clica em Gravar.
5.	O sistema verifica se existe uma Categoria de Ativo com o nome informado pelo usuário.
6.	O sistema grava as informações no banco de dados.
Nº	**Cenário Alternativo**
5.a	O sistema identifica que já existe uma Categoria de Ativo com o nome informado e exibe a mensagem: “Registro já cadastrado. Por favor, escolha outro nome.” e retorna ao passo 3.

UC008 – Inclusão de Responsável por Ativo

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Cadastrar responsável por ativo no sistema.	
Pré-Condições: Estar logado no sistema.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Arquivo > Novo Responsável por Ativo.
3.	O sistema exibe uma interface solicitando as seguintes informações: 3.1 Nome 3.2 Telefone 3.3 Registro na Organização 3.4 Email
4.	O usuário digita e seleciona as informações nos campos específicos da interface e clica em Gravar.
5.	O sistema verifica se existe um Responsável por Ativo com o nome informado pelo usuário.
6.	O sistema grava as informações no banco de dados.

Nº	Cenário Alternativo
5.a	O sistema identifica que já existe um Responsável por Ativo com o nome informado e exibe a mensagem: “Registro já cadastrado. Por favor, escolha outro nome.” e retorna ao passo 3.

UC009 – Inclusão de Ativo

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Cadastrar ativo no sistema.	
Pré-Condições: Estar logado no sistema.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Arquivo > Novo Ativo.
3.	O sistema exibe uma interface solicitando as seguintes informações: 3.1 Nome 3.2 Descrição 3.3 Formato (Físico ou Eletrônico) 3.4 Localização 3.5 Informações sobre cópias de segurança 3.6 Informações sobre licenças 3.7 Importância do ativo para o negócio (Muito importante, Importante, Média importância, Pouco importante, Sem importância) 3.8 Custo em R$ 3.9 Categoria de Ativo 3.10 Responsável por Ativo 3.11 Ameaças 3.12 Vulnerabilidades 3.13 Controles
4.	O usuário digita e seleciona as informações nos campos específicos da interface e clica em Gravar.

5.	O sistema verifica se existe um Ativo com o nome informado pelo usuário.
6.	O sistema grava as informações no banco de dados.
Nº	**Cenário Alternativo**
5.a	O sistema identifica que já existe um Ativo com o nome informado e exibe a mensagem: “Registro já cadastrado. Por favor, escolha outro nome.” e retorna ao passo 3.

Edição

Esta seção agrupa os casos de uso das funcionalidades relativas à atualização edição de informações no sistema.

UC010 – Edição de Mecanismo de Controle

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Editar mecanismo de controle no sistema.	
Pré-Condições: Estar logado no sistema e ter mecanismos de controles cadastrados.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Mecanismo de Controle.
3.	O sistema exibe uma interface solicitando a seleção de um Mecanismo de Controle cadastrado.
4.	O usuário seleciona um Mecanismo de Controle.
5.	O sistema exibe uma interface com todos os dados do Mecanismo de Controle: 3.1 Nome 3.2 Descrição
6.	O usuário altera as informações nos campos específicos da interface e clica em Gravar.

7.	O sistema grava as informações no banco de dados.

UC011 – Edição de Controle

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Editar controle no sistema.	
Pré-Condições: Estar logado no sistema e ter controles cadastrados.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Controle.
3.	O sistema exibe uma interface solicitando a seleção de um Controle cadastrado.
4.	O usuário seleciona um Controle.
5.	O sistema exibe uma interface com todos os dados do Controle: 3.1 Nome 3.2 Tipo (Técnico ou Não Técnico) 3.3 Categoria (Preventivo ou Detectivo) 3.4 Status (Ativo ou Inativo) 3.5 Restrição da Organização 3.6 Tipo de Proteção (Correção, Eliminação, Prevenção, Minimização do impacto, Dissuasão, Detecção, Recuperação, Monitoramento, ou Conscientização) 3.7 Forma de Tratamento de Risco (Evitar risco, Reduzir risco, Reter risco, ou Transferir risco) 3.7 Custo para implementar em R$ 3.8 Mecanismos de controle 3.9 Descrição
6.	O usuário altera as informações nos campos específicos da interface e clica em Gravar.
7.	O sistema grava as informações no banco de dados.

UC012 – Edição de Fonte de Vulnerabilidade

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Editar fonte de vulnerabilidade no sistema.	
Pré-Condições: Estar logado no sistema e ter fontes de vulnerabilidades cadastradas.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Fonte de Vulnerabilidade.
3.	O sistema exibe uma interface solicitando a seleção de um Fonte de Vulnerabilidade cadastrado.
4.	O usuário seleciona um Fonte de Vulnerabilidade.
5.	O sistema exibe uma interface com todos os dados da Fonte de Vulnerabilidade: 3.1 Nome 3.2 Descrição
6.	O usuário altera as informações nos campos específicos da interface e clica em Gravar.
7.	O sistema grava as informações no banco de dados.

UC013 – Edição de Vulnerabilidade

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Editar vulnerabilidade no sistema.	
Pré-Condições: Estar logado no sistema e ter vulnerabilidades cadastradas.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Vulnerabilidade.

3.	O sistema exibe uma interface solicitando a seleção de uma Vulnerabilidade cadastrada.
4.	O usuário seleciona uma Vulnerabilidade.
5.	O sistema exibe uma interface com todos os dados da Vulnerabilidade: 3.1 Nome 3.2 Fonte de Vulnerabilidade 3.3 Controles 3.4 Descrição
6.	O usuário altera as informações nos campos específicos da interface e clica em Gravar.
7.	O sistema grava as informações no banco de dados.

UC014 – Edição de Impacto

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Editar impacto no sistema.	
Pré-Condições: Estar logado no sistema e ter impactos cadastrados.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Impacto.
3.	O sistema exibe uma interface solicitando a seleção de um Impacto cadastrado.
4.	O usuário seleciona um Impacto.
5.	O sistema exibe uma interface com todos os dados do Impacto: 3.1 Nome 3.2 Tipo (Confidencialidade, Integridade ou Disponibilidade) 3.3 Gravidade (Alta, Média ou Baixa) 3.4 Descrição
6.	O usuário altera as informações nos campos específicos da interface e clica em Gravar.
7.	O sistema grava as informações no banco de dados.

UC015 – Edição de Ameaça

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Editar ameaça no sistema.	
Pré-Condições: Estar logado no sistema e ter ameaças cadastradas.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Ameaça.
3.	O sistema exibe uma interface solicitando a seleção de uma Ameaça cadastrada.
4.	O usuário seleciona uma Ameaça.
5.	O sistema exibe uma interface com todos os dados da Ameaça: 3.1 Nome 3.2 Tipo (Confidencialidade, Integridade ou Disponibilidade) 3.3 Gravidade (Alta, Média ou Baixa) 3.4 Descrição
6.	O usuário altera as informações nos campos específicos da interface e clica em Gravar.
7.	O sistema grava as informações no banco de dados.

UC016 – Edição de Categoria de Ativo

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Editar categoria de ativo no sistema.	
Pré-Condições: Estar logado no sistema e ter categorias de ativos cadastradas.	
Nº	**Cenário Principal**

1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Categoria de Ativo.
3.	O sistema exibe uma interface solicitando a seleção de uma Categoria de Ativo cadastrada.
4.	O usuário seleciona uma Categoria de Ativo.
5.	O sistema exibe uma interface com todos os dados da Categoria de Ativo: 3.1 Nome 3.2 Descrição
6.	O usuário altera as informações nos campos específicos da interface e clica em Gravar.
7.	O sistema grava as informações no banco de dados.

UC017 – Edição de Responsável por Ativo

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Editar responsável por ativo no sistema.	
Pré-Condições: Estar logado no sistema e ter responsáveis por ativos cadastrados.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Responsável por Ativo.
3.	O sistema exibe uma interface solicitando a seleção de um Responsável por Ativo cadastrado.
4.	O usuário seleciona um Responsável por Ativo.
5.	O sistema exibe uma interface com todos os dados do Responsável por Ativo: 3.1 Nome 3.2 Telefone 3.3 Registro na Organização 3.4 Email
6.	O usuário altera as informações nos campos específicos da interface e clica em Gravar.
7.	O sistema grava as informações no banco de dados.

UC018 – Edição de Ativo

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Editar ativo no sistema.	
Pré-Condições: Estar logado no sistema e ter ativos cadastrados.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Ativo.
3.	O sistema exibe uma interface solicitando a seleção de um Ativo cadastrado.
4.	O usuário seleciona um Ativo.
5.	O sistema exibe uma interface com todos os dados do Ativo: 3.1 Nome 3.2 Descrição 3.3 Formato (Físico ou Eletrônico) 3.4 Localização 3.5 Informações sobre cópias de segurança 3.6 Informações sobre licenças 3.7 Importância do ativo para o negócio (Muito importante, Importante, Média importância, Pouco importante, Sem importância) 3.8 Custo em R$ 3.9 Categoria de Ativo 3.10 Responsável por Ativo 3.11 Ameaças 3.12 Vulnerabilidades 3.13 Controles
6.	O usuário altera as informações nos campos específicos da interface e clica em Gravar.
7.	O sistema grava as informações no banco de dados.

Exclusão

Esta seção agrupa os casos de uso das funcionalidades relativas à exclusão de informações no sistema.

UC019 – Exclusão de Mecanismo de Controle

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Excluir mecanismo de controle do sistema.	
Pré-Condições: Estar logado no sistema e ter mecanismos de controles cadastrados.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Mecanismo de Controle.
3.	O sistema exibe uma interface solicitando a seleção de um Mecanismo de Controle cadastrado.
4.	O usuário seleciona um Mecanismo de Controle.
5.	O sistema exibe uma interface com todos os dados do Mecanismo de Controle: 3.1 Nome 3.2 Descrição
6.	O usuário clica em Excluir.
7.	O sistema exclui as informações logicamente no banco de dados.

UC020 – Exclusão de Controle

Ator(es): Todos os usuários cadastrados no sistema.
Objetivo: Excluir controle do sistema.
Pré-Condições: Estar logado no sistema e ter controles cadastrados.

Nº	Cenário Principal
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Controle.
3.	O sistema exibe uma interface solicitando a seleção de um Controle cadastrado.
4.	O usuário seleciona um Controle.
5.	O sistema exibe uma interface com todos os dados do Controle: 3.1 Nome 3.2 Tipo (Técnico ou Não Técnico) 3.3 Categoria (Preventivo ou Detectivo) 3.4 Status (Ativo ou Inativo) 3.5 Restrição da Organização 3.6 Tipo de Proteção (Correção, Eliminação, Prevenção, Minimização do impacto, Dissuasão, Detecção, Recuperação, Monitoramento, ou Conscientização) 3.7 Forma de Tratamento de Risco (Evitar risco, Reduzir risco, Reter risco, ou Transferir risco) 3.7 Custo para implementar em R$ 3.8 Mecanismos de controle 3.9 Descrição
6.	O usuário clica em Excluir.
7.	O sistema exclui as informações logicamente no banco de dados.

UC021 – Edição de Fonte de Vulnerabilidade

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Excluir fonte de vulnerabilidade do sistema.	
Pré-Condições: Estar logado no sistema e ter fontes de vulnerabilidades cadastradas.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Fonte de Vulnerabilidade.

3.	O sistema exibe uma interface solicitando a seleção de um Fonte de Vulnerabilidade cadastrado.
4.	O usuário seleciona um Fonte de Vulnerabilidade.
5.	O sistema exibe uma interface com todos os dados da Fonte de Vulnerabilidade: 3.1 Nome 3.2 Descrição
6.	O usuário clica em Excluir.
7.	O sistema exclui as informações logicamente no banco de dados.

UC022 – Exclusão de Vulnerabilidade

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Excluir vulnerabilidade do sistema.	
Pré-Condições: Estar logado no sistema e ter vulnerabilidades cadastradas.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Vulnerabilidade.
3.	O sistema exibe uma interface solicitando a seleção de uma Vulnerabilidade cadastrada.
4.	O usuário seleciona uma Vulnerabilidade.
5.	O sistema exibe uma interface com todos os dados da Vulnerabilidade: 3.1 Nome 3.2 Fonte de Vulnerabilidade 3.3 Controles 3.4 Descrição
6.	O usuário clica em Excluir.
7.	O sistema exclui as informações logicamente no banco de dados.

UC023 – Exclusão de Impacto

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Excluir impacto do sistema.	
Pré-Condições: Estar logado no sistema e ter impactos cadastrados.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Impacto.
3.	O sistema exibe uma interface solicitando a seleção de um Impacto cadastrado.
4.	O usuário seleciona um Impacto.
5.	O sistema exibe uma interface com todos os dados do Impacto: 3.1 Nome 3.2 Tipo (Confidencialidade, Integridade ou Disponibilidade) 3.3 Gravidade (Alta, Média ou Baixa) 3.4 Descrição
6.	O usuário clica em Excluir.
7.	O sistema exclui as informações logicamente no banco de dados.

UC024 – Edição de Ameaça

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Excluir ameaça no sistema.	
Pré-Condições: Estar logado no sistema e ter ameaças cadastradas.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Ameaça.

3.	O sistema exibe uma interface solicitando a seleção de uma Ameaça cadastrada.
4.	O usuário seleciona uma Ameaça.
5.	O sistema exibe uma interface com todos os dados da Ameaça: 3.1 Nome 3.2 Tipo (Confidencialidade, Integridade ou Disponibilidade) 3.3 Gravidade (Alta, Média ou Baixa) 3.4 Descrição
6.	O usuário clica em Excluir.
7.	O sistema exclui as informações logicamente no banco de dados.

UC025 – Exclusão de Categoria de Ativo

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Excluir categoria de ativo do sistema.	
Pré-Condições: Estar logado no sistema e ter categorias de ativos cadastradas.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Categoria de Ativo.
3.	O sistema exibe uma interface solicitando a seleção de uma Categoria de Ativo cadastrada.
4.	O usuário seleciona uma Categoria de Ativo.
5.	O sistema exibe uma interface com todos os dados da Categoria de Ativo: 3.1 Nome 3.2 Descrição
6.	O usuário clica em Excluir.
7.	O sistema exclui as informações logicamente no banco de dados.

UC026 – Exclusão de Responsável por Ativo

Ator(es):

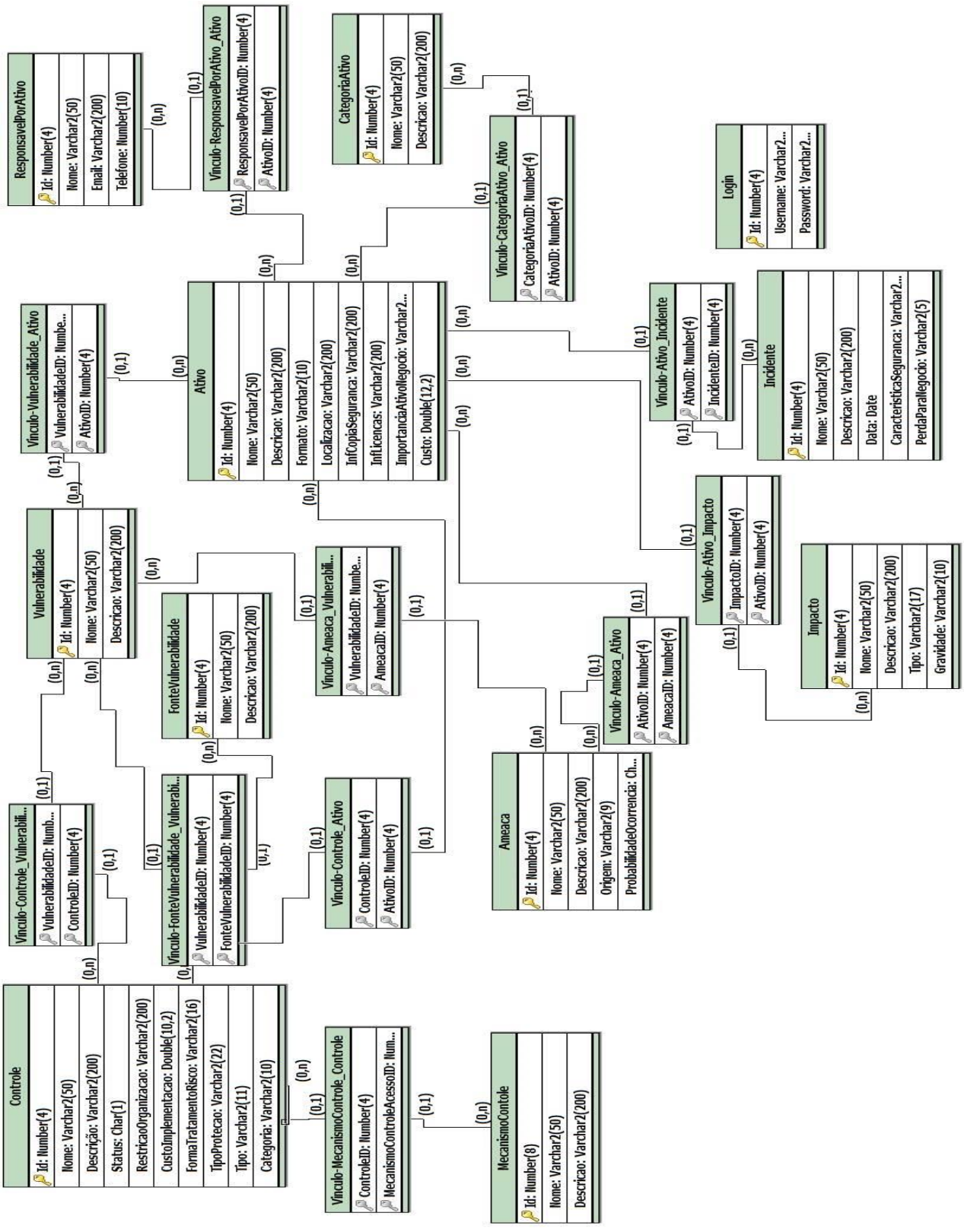
Todos os usuários cadastrados no sistema.	
Objetivo: Editar responsável por ativo no sistema.	
Pré-Condições: Estar logado no sistema e ter responsáveis por ativos cadastrados.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Responsável por Ativo.
3.	O sistema exibe uma interface solicitando a seleção de um Responsável por Ativo cadastrado.
4.	O usuário seleciona um Responsável por Ativo.
5.	O sistema exibe uma interface com todos os dados do Responsável por Ativo: 3.1 Nome 3.2 Telefone 3.3 Registro na Organização 3.4 Email
6.	O usuário clica em Excluir.
7.	O sistema exclui as informações logicamente no banco de dados.

UC027 – Exclusão de Ativo

Ator(es): Todos os usuários cadastrados no sistema.	
Objetivo: Excluir ativo do sistema.	
Pré-Condições: Estar logado no sistema e ter ativos cadastrados.	
Nº	**Cenário Principal**
1.	O sistema apresenta a tela inicial com o nome do sistema.
2.	O usuário acessa o menu Editar > Ativo.
3.	O sistema exibe uma interface solicitando a seleção de um Ativo cadastrado.

4.	O usuário seleciona um Ativo.
5.	O sistema exibe uma interface com todos os dados do Ativo: 3.1 Nome 3.2 Descrição 3.3 Formato (Físico ou Eletrônico) 3.4 Localização 3.5 Informações sobre cópias de segurança 3.6 Informações sobre licenças 3.7 Importância do ativo para o negócio (Muito importante, Importante, Média importância, Pouco importante, Sem importância) 3.8 Custo em R$ 3.9 Categoria de Ativo 3.10 Responsável por Ativo 3.11 Ameaças 3.12 Vulnerabilidades 3.13 Controles
6.	O usuário clica em Excluir.
7.	O sistema exclui as informações logicamente no banco de dados.

APÊNDICE Q – Esquema Lógico de Banco de Dados



APÊNDICE R – Casos de Testes

Casos de Testes

Via Análise

Responsáveis:

Andrey Bevilacqua

Jônatas Josué Kirsch

Introdução

Este documento tem por objetivo descrever os casos de testes funcionais e não funcionais do sistema Via Análise. Destina-se a todos os integrantes do projeto.

Propósito

O propósito deste documento é descrever os casos de testes do sistema Via Análise cobrindo casos de teste para os requisitos funcionais ou do produto, não-funcionais e restrições/premissas.

Público Alvo

Esse documento destina-se a todos os integrantes do projeto.

Casos de Testes Funcionais

Cadastros

Esta seção agrupa os casos de testes das funcionalidades relativas à criação de informações no sistema.

CT001 – Inclusão de Mecanismo de Controle

Tipo de Teste: Funcional		**Tipo de Execução:** Manual
Objetivo: Testar a inclusão de mecanismo de controle.		
Pré-Condições: Estar logado no sistema.		
Nº	**Passo do Teste**	**Resultado Esperado**
7.	Acessar o menu Arquivo > Novo Mecanismo de Controle.	Tela acessada.
8.	Preencher o campo Nome com caracteres alfanuméricos, anotando a informação digitada	Campo com informações digitadas.

	para futura conferência. Exemplo: asdFj#$%¨0856769	
9.	Preencher o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
10.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
11.	Acessar o menu Editar > Mecanismo de Controle.	Tela acessada.
12.	Selecionar o novo mecanismo de controle através da opção Selecione.	Mecanismo de controle selecionado.
13.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT002 – Inclusão de Controle

Tipo de Teste: Funcional	**Tipo de Execução:** Manual	
Objetivo: Testar a inclusão de controle.		
Pré-Condições: Estar logado no sistema.		
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Arquivo > Novo Controle.	Tela acessada.
2.	Verificar se o campo Restrição da organização está desabilitado para edição.	O campo deve estar desabilitado para edição.
3.	Preencher o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.

4.	Selecionar o tipo Não-Técnico.	Tipo selecionado.
5.	Selecionar a categoria Detectivo.	Categoria selecionada.
6.	Selecionar o status Inativo.	Status selecionado.
7.	Verificar se o sistema habilita para edição o campo Restrição da Organização.	O campo deve estar habilitado para edição.
8.	Selecionar o tipo de proteção Monitoramento.	Tipo de proteção selecionado.
9.	Informar um custo para implementar em R$. Exemplo: 9861,47.	Custo para implementar informado.
10.	Selecionar dois mecanismos de controle.	Mecanismos de controle selecionados.
11.	Preencher o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
12.	Preencher o campo Restrição da organização com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
13.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
14.	Acessar o menu Editar > Controle.	Tela acessada.
15.	Selecionar o novo controle através da opção Selecione.	Controle selecionado.
16.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT003 – Inclusão de Fonte de Vulnerabilidade

Tipo de Teste:	**Tipo de Execução:**
Funcional	Manual

Objetivo: Testar a inclusão de fonte de vulnerabilidade.		
Pré-Condições: Estar logado no sistema.		
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Arquivo > Novo Fonte de Vulnerabilidade	Tela acessada.
2.	Preencher o campo Nome com caracteres alfanuméricos, anotando a informação digitada para futura conferência. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
3.	Preencher o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
4.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
5.	Acessar o menu Editar > Fonte de Vulnerabilidade.	Tela acessada.
6.	Selecionar a nova fonte de vulnerabilidade através da opção Selecione.	Fonte de vulnerabilidade selecionada.
7.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT004 – Inclusão de Vulnerabilidade

Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a inclusão de vulnerabilidade;	
Pré-Condições:	

Estar logado no sistema; Ter cadastrado no mínimo duas fonte de vulnerabilidade; Ter cadastrado no mínimo três controles.		
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Arquivo > Nova Vulnerabilidade.	Tela acessada.
2.	Preencher o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
3.	Selecionar uma fonte de vulnerabilidade.	Fonte de vulnerabilidade selecionada.
4.	Preencher o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
5.	Selecionar dois controles.	Controles selecionados.
6.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
7.	Acessar o menu Editar > Vulnerabilidade.	Tela acessada.
8.	Selecionar a nova vulnerabilidade através da opção Selecione.	Vulnerabilidade selecionada.
9.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT005 – Inclusão de Impacto

Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a inclusão de impacto;	
Pré-Condições: Estar logado no sistema.	

Nº	Passo do Teste	Resultado Esperado
1.	Acessar o menu Arquivo > Novo Impacto.	Tela acessada.
2.	Preencher o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
3.	Preencher o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
4.	Selecionar um Tipo: Confidencialidade, Integridade ou Disponibilidade.	Tipo selecionado.
5.	Selecionar uma Gravidade: Alta, Média ou Baixa.	Gravidade selecionada.
6.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
7.	Acessar o menu Editar > Impacto.	Tela acessada.
8.	Selecionar o novo impacto através da opção Selecione.	Impacto selecionado.
9.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT006 – Inclusão de Ameaça

Tipo de Teste:	**Tipo de Execução:**
Funcional	Manual
Objetivo: Testar a inclusão de ameaça;	
Pré-Condições: Estar logado no sistema; Ter cadastrado no mínimo dois impactos; Ter cadastrado no mínimo três vulnerabilidades.	

Nº	Passo do Teste	Resultado Esperado
1.	Acessar o menu Arquivo > Nova Ameaça.	Tela acessada.
2.	Preencher o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
3.	Preencher o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
4.	Selecionar uma Origem: Natural, Humana ou Ambiental.	Origem selecionada.
5.	Selecionar uma Probabilidade de ocorrência de incidente referente a ameaça: *A – Frequente*, *B – Provável*, *C – Ocasional*, *D – Remota*, *E – Improvável* ou *F – Impossível*.	Informação selecionada.
6.	Selecionar um Impacto.	Impacto selecionado.
7.	Selecionar duas vulnerabilidades.	Vulnerabilidades selecionadas.
8.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
9.	Acessar o menu Editar > Ameaça.	Tela acessada.
10.	Selecionar a nova ameaça através da opção Selecione.	Ameaça selecionada.
11.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT007 – Inclusão de Categoria de Ativos

Tipo de Teste:	**Tipo de Execução:**
Funcional	Manual
Objetivo:	

Testar a inclusão de categoria de ativos;		
Pré-Condições: Estar logado no sistema.		
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Arquivo > Nova Categoria de Ativos.	Tela acessada.
2.	Preencher o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
3.	Preencher o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
4.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
5.	Acessar o menu Editar > Categoria de Ativos.	Tela acessada.
6.	Selecionar a nova categoria de ativos através da opção Selecione.	Categoria de ativos selecionada.
7.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT008 – Inclusão de Responsável por Ativos

Tipo de Teste: Funcional		**Tipo de Execução:** Manual
Objetivo: Testar a inclusão de responsável por ativos;		
Pré-Condições: Estar logado no sistema.		
Nº	**Passo do Teste**	**Resultado Esperado**

1.	Acessar o menu Arquivo > Novo Responsável por Ativos.	Tela acessada.
2.	Preencher o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
3.	Preencher o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
4.	Preencher o campo Registro na Organização com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
5.	Preencher o campo Email com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
6.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
7.	Acessar o menu Editar > Responsável por Ativos.	Tela acessada.
8.	Selecionar o novo responsável por ativos através da opção Selecione.	Responsável por ativos selecionado.
9.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT009 – Inclusão de Ativo

Tipo de Teste:	**Tipo de Execução:**
Funcional	Manual
Objetivo: Testar a inclusão de ativo;	
Pré-Condições: Estar logado no sistema; Ter cadastrado no mínimo duas categorias de ativos; Ter cadastrado no mínimo dois responsáveis por ativos;	

Ter cadastrado no mínimo três ameaças; Ter cadastrado no mínimo três vulnerabilidades; Ter cadastrado no mínimo três controles.		
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Arquivo > Novo Ativo.	Tela acessada.
2.	Preencher o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
3.	Preencher o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
4.	Selecionar um Formato: Físico ou Eletrônico.	Formato selecionado.
5.	Preencher o campo Localização com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
6.	Preencher o campo Informações sobre cópias de segurança com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
7.	Preencher o campo Informações sobre licenças com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
8.	Selecionar a Importância do ativo para o negócio: Muito importante, Importante, Média importância, Pouco importante ou Sem importância.	Informação selecionada.
9.	Preencher o campo Custo em R$ com um número com duas casas decimais. Exemplo: 999,01.	Campo com informações digitadas.
10.	Selecionar a Categoria de ativos.	Categoria de ativos selecionada.
11.	Selecionar o Responsável pelo ativo.	Responsável pelo ativo selecionado.
12.	Selecionar duas ameaças.	Ameaças selecionadas.
13.	Na lista de vulnerabilidades, verificar se o sistema apenas exibe a lista das vulnerabilidades vinculadas às ameaças	O sistema somente deverá exibir as vulnerabilidades vinculadas às ameaças

	selecionadas.	selecionadas.
14.	Selecionar duas vulnerabilidades.	Vulnerabilidades selecionadas.
15.	Na lista de controles, verificar se o sistema apenas exibe a lista dos controles vinculados às vulnerabilidades selecionadas.	O sistema somente deverá exibir os controles vinculados às vulnerabilidades selecionadas.
16.	Selecionar dois controles.	Controles selecionados.
17.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
18.	Acessar o menu Editar > Ativo.	Tela acessada.
19.	Selecionar o novo ativo através da opção Selecione.	Ativo selecionado.
20.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

Edição

Esta seção agrupa os casos de testes das funcionalidades relativas à edição de informações no sistema.

CT019 – Edição de Mecanismo de Controle	
Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a edição de mecanismo de controle.	
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo um mecanismo de controle.	

Nº	Passo do Teste	Resultado Esperado
1.	Acessar o menu Editar > Mecanismo de Controle.	Tela acessada.
2.	No campo “Selecione”, selecionar um Mecanismo de Controle cadastrado.	O sistema deverá popular todos os campos com as informações cadastradas.
3.	Alterar o campo Nome com caracteres alfanuméricos, anotando a informação digitada para futura conferência. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
4.	Alterar o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
5.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
6.	Acessar o menu Editar > Mecanismo de Controle.	Tela acessada.
7.	Selecionar o mecanismo de controle editado através da opção Selecione.	Mecanismo de controle selecionado.
8.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT020 – Inclusão de Controle

Tipo de Teste:	**Tipo de Execução:**
Funcional	Manual
Objetivo: Testar a edição de controle.	
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo um controle.	

Nº	Passo do Teste	Resultado Esperado
1.	Acessar o menu Editar > Controle.	Tela acessada.
2.	Através da opção “Selecione”, selecionar um controle cadastrado.	O sistema deverá popular todos os campos da tela referente as informações cadastradas.
3.	Alterar o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
4.	Alterar o tipo.	Tipo alterado.
5.	Alterar a categoria.	Categoria alterada.
6.	Alterar o status.	Status alterado.
7.	Alterar o tipo de proteção.	Tipo de proteção alterado.
8.	Alterar o custo para implementar em R$. Exemplo: 9861,47.	Custo para implementar alterado.
9.	Alterar os mecanismos de controle.	Mecanismos de controle alterados.
10.	Alterar o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
11.	Alterar o campo Restrição da organização com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
12.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
13.	Selecionar o controle editado através da opção Selecione.	Controle selecionado.
14.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT021 – Edição de Fonte de Vulnerabilidade

Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a edição de fonte de vulnerabilidade.	
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo uma fonte de vulnerabilidade.	

Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Fonte de Vulnerabilidade	Tela acessada.
2.	Selecionar uma fonte de vulnerabilidade através da opção Selecione.	Campos de tela preenchidos pelo sistema com as informações cadastradas.
3.	Alterar o campo Nome com caracteres alfanuméricos, anotando a informação digitada para futura conferência. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
4.	Alterar o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
5.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
6.	Acessar o menu Editar > Fonte de Vulnerabilidade.	Tela acessada.
7.	Selecionar a fonte de vulnerabilidade editada através da opção Selecione.	Fonte de vulnerabilidade selecionada.
8.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT022 – Edição de Vulnerabilidade

Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a edição de vulnerabilidade;	
Pré-Condições: Estar logado no sistema; Ter cadastrado no mínimo uma vulnerabilidade.	

Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Vulnerabilidade.	Tela acessada.
2.	Alterar o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
3.	Selecionar outra fonte de vulnerabilidade.	Fonte de vulnerabilidade selecionada.
4.	Alterar o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
5.	Selecionar outros controles.	Controles selecionados.
6.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
7.	Acessar o menu Editar > Vulnerabilidade.	Tela acessada.
8.	Selecionar a vulnerabilidade editada através da opção Selecione.	Vulnerabilidade selecionada.
9.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT023 – Edição de Impacto

Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a edição de impacto;	
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo um impacto.	

Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Impacto.	Tela acessada.
2.	Selecionar um impacto através da opção Selecione.	Campos preenchidos pelo sistema com as informações cadastradas.
3.	Alterar o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
4.	Alterar o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
5.	Selecionar outro Tipo.	Tipo alterado.
6.	Selecionar outra Gravidade.	Gravidade alterada.
7.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
8.	Acessar o menu Editar > Impacto.	Tela acessada.
9.	Selecionar o impacto editado através da opção Selecione.	Impacto selecionado.
10.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT024 – Edição de Ameaça

Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a edição de ameaça;	
Pré-Condições: Estar logado no sistema; Ter cadastrado no mínimo uma ameaça.	

Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Ameaça.	Tela acessada.
2.	Selecionar uma ameaça através da opção Selecione.	Campos da tela preenchidos com os dados cadastrados.
3.	Alterar o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
4.	Alterar o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
5.	Selecionar outra Origem.	Origem alterada.
6.	Selecionar outra Probabilidade de ocorrência de incidente referente a ameaça.	Informação alterada.
7.	Selecionar outroImpacto.	Impacto alterado.
8.	Selecionar outras vulnerabilidades.	Vulnerabilidades alteradas.
9.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
10.	Selecionar a ameaça editada através da opção Selecione.	Ameaça selecionada.
11.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT025 – Edição de Categoria de Ativos		
Tipo de Teste: Funcional		**Tipo de Execução:** Manual
Objetivo: Testar a edição de categoria de ativos;		
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo uma categoria de ativos.		
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Categoria de Ativos.	Tela acessada.
2.	Selecionar uma categoria de ativos através da opção Selecione.	Campos preenchidos pelo sistema com as informações cadastradas.
3.	Alterar o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
4.	Alterar o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
5.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
6.	Selecionar a categoria de ativos editada através da opção Selecione.	Categoria de ativos selecionada.
7.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT026 – Edição de Responsável por Ativos	
Tipo de Teste:	**Tipo de Execução:**

Funcional	Manual
Objetivo: Testar a edição de responsável por ativos;	
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo um responsável por ativos.	

Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Responsável por Ativos.	Tela acessada.
2.	Selecionar um responsável por ativo através da opção Selecione.	Campos preenchidos com as informações cadastradas.
3.	Alterar o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
4.	Alterar o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
5.	Alterar o campo Registro na Organização com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
6.	Alterar o campo Email com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
7.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
8.	Selecionar o responsável por ativos editado através da opção Selecione.	Responsável por ativos selecionado.
9.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

CT027 – Edição de Ativo

Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a inclusão de ativo;	
Pré-Condições: Estar logado no sistema; Ter cadastrado no mínimo um ativo.	

Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Ativo.	Tela acessada.
2.	Selecionar um ativo através da opção Selecione.	Campos preenchidos com as informações cadastradas.
3.	Alterar o campo Nome com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
4.	Alterar o campo Descrição com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
5.	Selecionar outro Formato.	Formato alterado.
6.	Preencher o campo Localização com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações digitadas.
7.	Alterar o campo Informações sobre cópias de segurança com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
8.	Alterar o campo Informações sobre licenças com caracteres alfanuméricos. Exemplo: asdFj#$%¨0856769	Campo com informações alteradas.
9.	Selecionar outra Importância do ativo para o negócio.	Informação alterada.
10.	Alterar o campo Custo em R$ com um número com duas casas decimais. Exemplo: 999,01.	Campo com informações alteradas.

11.	Selecionar outra Categoria de ativos.	Categoria de ativos alterada.
12.	Selecionar outro Responsável pelo ativo.	Responsável pelo ativo alterado.
13.	Selecionar outras ameaças.	Ameaças alteradas.
14.	Na lista de vulnerabilidades, verificar se o sistema apenas exibe a lista das vulnerabilidades vinculadas às ameaças selecionadas.	O sistema somente deverá exibir as vulnerabilidades vinculadas às ameaças selecionadas.
15.	Selecionar outras vulnerabilidades.	Vulnerabilidades alteradas.
16.	Na lista de controles, verificar se o sistema apenas exibe a lista dos controles vinculados às vulnerabilidades selecionadas.	O sistema somente deverá exibir os controles vinculados às vulnerabilidades selecionadas.
17.	Selecionar outros controles.	Controles alterados
18.	Clicar em Gravar.	O sistema deverá exibir a mensagem: “Gravação realizada com sucesso!”.
19.	Selecionar o ativo editado através da opção Selecione.	Ativo selecionado.
20.	Verificar se as informações exibidas são as mesmas daquelas que foram gravadas.	As informações exibidas pelo sistema devem ser as mesmas informações gravadas nos passos anteriores.

Exclusão

Esta seção agrupa os casos de testes das funcionalidades relativas à exclusão de informações no sistema.

CT028 – Exclusão de Mecanismo de Controle	
Tipo de Teste:	**Tipo de Execução:**

Funcional	Manual
Objetivo: Testar a exclusão de mecanismo de controle.	
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo um mecanismo de controle.	
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Mecanismo de Controle.	Tela acessada.
2.	No campo “Selecione”, selecionar um Mecanismo de Controle cadastrado.	O sistema deverá popular todos os campos com as informações cadastradas.
3.	Clicar em Excluir.	O sistema deverá exibir a mensagem “Esse registro possui vínculos. Você tem certeza que deseja excluir esse registro?” com as opções “Sim” e “Não”.
4.	Clicar em “Não”.	O sistema não poderá remover o registro e o mesmo deve manter-se na opção Selecione.
5.	Executar novamente os passos 1 a 3 para o mesmo registro. Na mensagem, clicar em “Sim”.	O sistema deverá remover o cadastro do registro selecionado, não sendo possível selecioná-lo novamente no sistema.

CT029 – Exclusão de Controle

Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a exclusão de controle.	

Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo um controle.		
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Controle.	Tela acessada.
2.	No campo “Selecione”, selecionar um Controle cadastrado.	O sistema deverá popular todos os campos com as informações cadastradas.
3.	Clicar em Excluir cadastro.	O sistema deverá exibir a mensagem “Esse registro possui vínculos. Você tem certeza que deseja excluir esse registro?” com as opções “Sim” e “Não”.
4.	Clicar em “Não”.	O sistema não poderá remover o registro e o mesmo deve manter-se na opção Selecione.
5.	Executar novamente os passos 1 a 3 para o mesmo registro. Na mensagem, clicar em “Sim”.	O sistema deverá remover o cadastro do registro selecionado, não sendo possível selecioná-lo novamente no sistema.

CT030 – Exclusão de Fonte de Vulnerabilidade

Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a exclusão de fonte de vulnerabilidade.	
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo uma fonte de vulnerabilidade.	

Nº	Passo do Teste	Resultado Esperado
1.	Acessar o menu Editar > Fonte de Vulnerabilidade.	Tela acessada.
2.	No campo “Selecione”, selecionar uma Fonte de Vulnerabilidade cadastrada.	O sistema deverá popular todos os campos com as informações cadastradas.
3.	Clicar em Excluir cadastro.	O sistema deverá exibir a mensagem “Esse registro possui vínculos. Você tem certeza que deseja excluir esse registro?” com as opções “Sim” e “Não”.
4.	Clicar em “Não”.	O sistema não poderá remover o registro e o mesmo deve manter-se na opção Selecione.
5.	Executar novamente os passos 1 a 3 para o mesmo registro. Na mensagem, clicar em “Sim”.	O sistema deverá remover o cadastro do registro selecionado, não sendo possível selecioná-lo novamente no sistema.

CT031 – Exclusão de Vulnerabilidade

Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a exclusão de vulnerabilidade.	
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo uma vulnerabilidade.	

Nº	Passo do Teste	Resultado Esperado
1.	Acessar o menu Editar > Vulnerabilidade.	Tela acessada.

2.	No campo “Selecione”, selecionar um Controle cadastrado.	O sistema deverá popular todos os campos com as informações cadastradas.
3.	Clicar em Excluir cadastro.	O sistema deverá exibir a mensagem “Esse registro possui vínculos. Você tem certeza que deseja excluir esse registro?” com as opções “Sim” e “Não”.
4.	Clicar em “Não”.	O sistema não poderá remover o registro e o mesmo deve manter-se na opção Selecione.
5.	Executar novamente os passos 1 a 3 para o mesmo registro. Na mensagem, clicar em “Sim”.	O sistema deverá remover o cadastro do registro selecionado, não sendo possível selecioná-lo novamente no sistema.

CT032 – Exclusão de Impacto

Tipo de Teste: Funcional	**Tipo de Execução:** Manual
Objetivo: Testar a exclusão de impacto.	
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo um impacto.	
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Impacto.	Tela acessada.
2.	No campo “Selecione”, selecionar um Impacto cadastrado.	O sistema deverá popular todos os campos com as informações cadastradas.

3.	Clicar em Excluir cadastro.	O sistema deverá exibir a mensagem “Esse registro possui vínculos. Você tem certeza que deseja excluir esse registro?” com as opções “Sim” e “Não”.
4.	Clicar em “Não”.	O sistema não poderá remover o registro e o mesmo deve manter-se na opção Selecione.
5.	Executar novamente os passos 1 a 3 para o mesmo registro. Na mensagem, clicar em “Sim”.	O sistema deverá remover o cadastro do registro selecionado, não sendo possível selecioná-lo novamente no sistema.

CT033 – Exclusão de Ameaça

Tipo de Teste: Funcional	**Tipo de Execução:** Manual	
Objetivo: Testar a exclusão de ameaça.		
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo uma ameaça.		
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Ameaça.	Tela acessada.
2.	No campo “Selecione”, selecionar uma Ameaça cadastrada.	O sistema deverá popular todos os campos com as informações cadastradas.
3.	Clicar em Excluir cadastro.	O sistema deverá exibir a mensagem “Esse registro possui vínculos. Você tem

		certeza que deseja excluir esse registro?” com as opções “Sim” e “Não”.
4.	Clicar em “Não”.	O sistema não poderá remover o registro e o mesmo deve manter-se na opção Selecione.
5.	Executar novamente os passos 1 a 3 para o mesmo registro. Na mensagem, clicar em “Sim”.	O sistema deverá remover o cadastro do registro selecionado, não sendo possível selecioná-lo novamente no sistema.

CT034 – Exclusão de Categoria de Ativos

Tipo de Teste: Funcional	**Tipo de Execução:** Manual	
Objetivo: Testar a exclusão de categoria de ativos.		
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo uma categoria de ativos.		
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Categoria de Ativos.	Tela acessada.
2.	No campo “Selecione”, selecionar uma Categoria de Ativos cadastrada.	O sistema deverá popular todos os campos com as informações cadastradas.
3.	Clicar em Excluir cadastro.	O sistema deverá exibir a mensagem “Esse registro possui vínculos. Você tem certeza que deseja excluir esse registro?” com as opções “Sim” e “Não”.

4.	Clicar em “Não”.	O sistema não poderá remover o registro e o mesmo deve manter-se na opção Selecione.
5.	Executar novamente os passos 1 a 3 para o mesmo registro. Na mensagem, clicar em “Sim”.	O sistema deverá remover o cadastro do registro selecionado, não sendo possível selecioná-lo novamente no sistema.

CT035 – Exclusão de Responsável por Ativos

Tipo de Teste: Funcional		**Tipo de Execução:** Manual
Objetivo: Testar a exclusão de responsável por ativos.		
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo um responsável por ativos.		
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Responsável por Ativos.	Tela acessada.
2.	No campo “Selecione”, selecionar um Responsável por Ativos cadastrado.	O sistema deverá popular todos os campos com as informações cadastradas.
3.	Clicar em Excluir cadastro.	O sistema deverá exibir a mensagem “Esse registro possui vínculos. Você tem certeza que deseja excluir esse registro?” com as opções “Sim” e “Não”.
4.	Clicar em “Não”.	O sistema não poderá remover o registro e o mesmo deve manter-se na opção

		Selecione.
5.	Executar novamente os passos 1 a 3 para o mesmo registro. Na mensagem, clicar em “Sim”.	O sistema deverá remover o cadastro do registro selecionado, não sendo possível selecioná-lo novamente no sistema.

CT036 – Exclusão de Ativo

Tipo de Teste: Funcional		**Tipo de Execução:** Manual
Objetivo: Testar a exclusão de ativo.		
Pré-Condições: Estar logado no sistema. Ter cadastrado no mínimo um ativo.		
Nº	**Passo do Teste**	**Resultado Esperado**
1.	Acessar o menu Editar > Ativo.	Tela acessada.
2.	No campo “Selecione”, selecionar um Ativo cadastrado.	O sistema deverá popular todos os campos com as informações cadastradas.
3.	Clicar em Excluir cadastro.	O sistema deverá exibir a mensagem “Esse registro possui vínculos. Você tem certeza que deseja excluir esse registro?” com as opções “Sim” e “Não”.
4.	Clicar em “Não”.	O sistema não poderá remover o registro e o mesmo deve manter-se na opção Selecione.
5.	Executar novamente os passos 1 a 3 para o mesmo registro. Na mensagem, clicar em “Sim”.	O sistema deverá remover o cadastro do

		registro selecionado, não sendo possível selecioná-lo novamente no sistema.

APÊNDICE S – Registro de Testes

Registro de Testes

Via Análise

Responsáveis:

Andrey Bevilacqua

Jônatas Josué Kirsch

Conteúdo

Introdução

Este documento tem por objetivo descrever os resultados dos testes do sistema Via Análise. Destina-se a todos os integrantes do projeto.

Propósito

O propósito deste documento é descrever os resultados dos testes do sistema Via Análise que foram executados cobrindo casos de teste para os requisitos funcionais ou do produto, não-funcionais e restrições/premissas.

Público Alvo

Esse documento destina-se a todos os integrantes do projeto.

Resultados de Testes

Foram realizados três ciclos de testes. O primeiro, após a conclusão das telas de inclusão de registros. O segundo, após a conclusão das telas de edição e exclusão de registros. Já o terceiro ciclo, foi realizado após a conclusão da geração de relatórios.

Não foram encontrados defeitos na fase de Testes, dado que a equipe de desenvolvimento realizou testes unitários e corrigiu os problemas encontrados ainda na fase de Desenvolvimento.

APÊNDICE T – Manual do Usuário

Via Análise

Manual do Usuário

Índice

Introdução Capítulo 1

Visão Geral da Ferramenta

A ferramenta Via Análise tem como objetivo auxiliar a análise de riscos de segurança da informação e comunicações em organizações da Administração Pública Federal.

Noções Básicas Capítulo 2

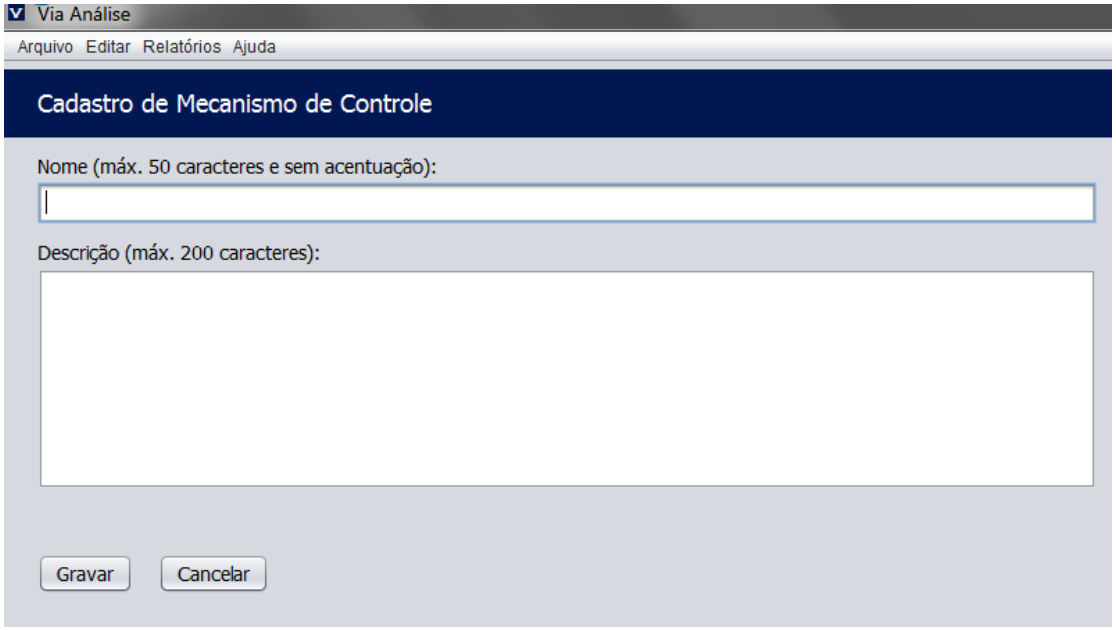
Acessando o sistema

A figura abaixo representa a tela de *login* da ferramenta, onde será necessário informar o usuário e senha. Feito isso, clique na opção "Acessar".

Cadastrando Mecanismo de Controle

Após logar-se no sistema, abrirá a tela inicial da ferramenta, a qual terá um menu na parte superior.

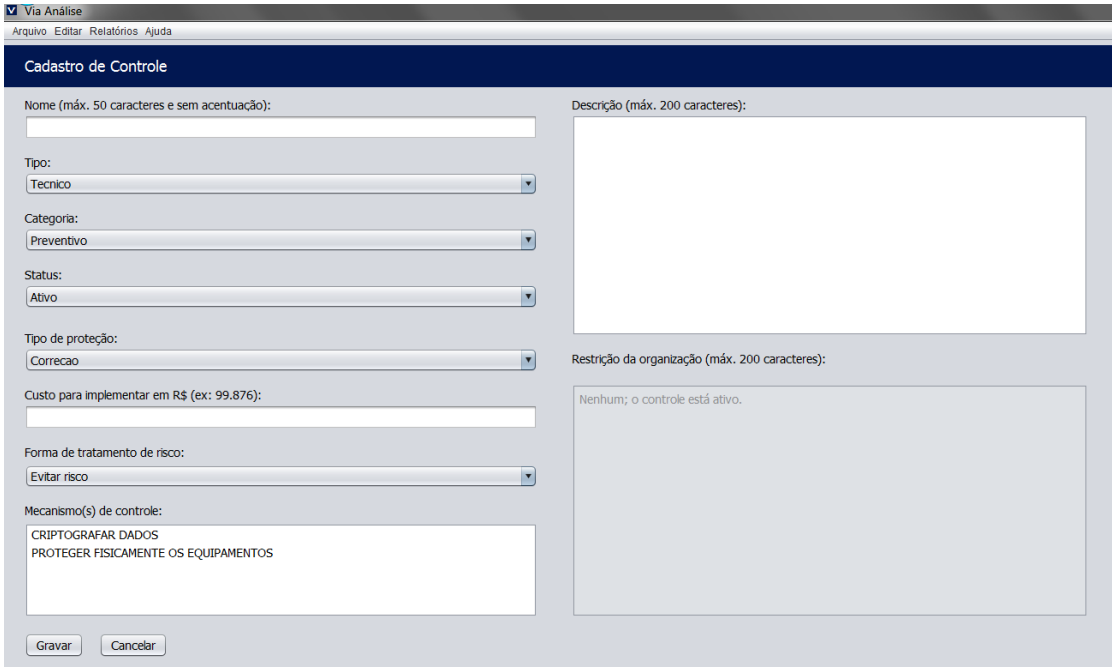
Para cadastrar um Mecanismo de Controle, acesse o menu Arquivo > Novo Mecanismo de Controle.



Será solicitado que o usuário informe o nome e a descrição do Mecanismo de Controle a ser cadastrado. Como exemplo de mecanismo de controle pode-se citar "Criptografar os dados sigilosos".

Cadastrando Controle

Para cadastrar um Controle, acesse o menu Arquivo > Novo Controle.



Será solicitado que o usuário informe as seguintes informações sobre o Controle:

- Nome: nome do controle. Exemplo: Sistema que detecta o tráfego de informações não criptografadas na rede;

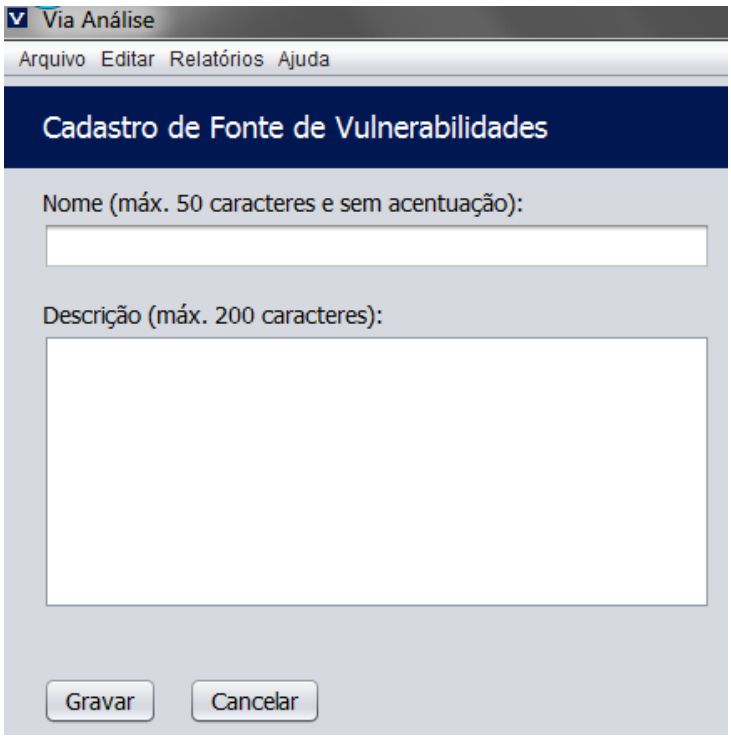
- Tipo: Técnico ou Não-Técnico. Será Técnico quando utiliza técnica (exemplo: técnica baseada em criptografia) e não-técnico quando não utiliza alguma técnica;
- Categoria: Preventivo, Detectivo ou Corretivo. Controle Preventivo é o projetado com a finalidade de evitar a ocorrência de erros ou irregularidades. Exemplo: o fechamento da porta do escritório. Controle Detectivo é o projetado para detectar erros ou irregularidades, permitindo evitar que o incidente ocorra. Exemplo: o alarme do escritório dispara. Controle Corretivo é o projetado para detectar erros ou irregularidades depois que já tenham acontecido, permitindo a adoção posterior de ações corretivas. Exemplo: tendo ocorrido o incidente, medidas de segurança serão providenciadas, tais como a instalação de alarme;
- Status: Ativo ou Inativo. Caso o controle esteja inativo na organização, será solicitado que o usuário especifique a Restrição na Organização que faz com que o controle fique inativo;
- Tipo de proteção. Relativo a abordagem tomada referente ao riso: Correção, Eliminação, Prevenção,

Minimização do impacto, Dissuasão, Detecção, Recuperação, Monitoramento, Conscientização;

- Custo para implementar o controle na organização;
- Forma de tratamento do risco: Evitar risco, Reduzir risco, Reter risco ou Transferir risco;
- Mecanismo(s) de controle: é solicitado que o usuário selecione um ou mais mecanismos de controle vinculados ao controle cadastrado;
- Descrição: descrição completa do controle.

Cadastrando Fonte de Vulnerabilidade

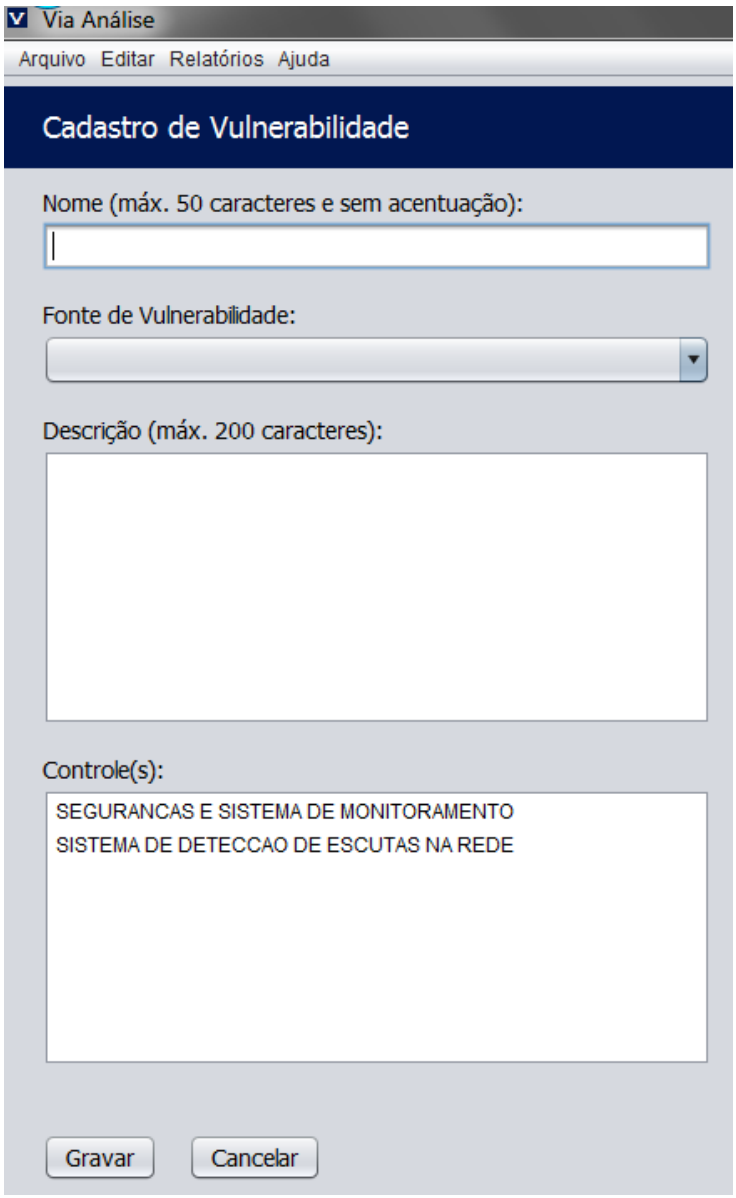
Para cadastrar uma Fonte de Vulnerabilidade, acesse o menu Arquivo > Nova Fonte de Vulnerabilidade.



Será solicitado que o usuário informe o nome e a descrição da Fonte de Vulnerabilidade. Por padrão, a ferramenta Via Análise possui cadastrada as seguintes fontes de vulnerabilidades: Análise de Segurança do Sistema, Avaliação de Risco Anterior, Avisos do Fornecedor e Lista de Vulnerabilidades.

Cadastrando Vulnerabilidade

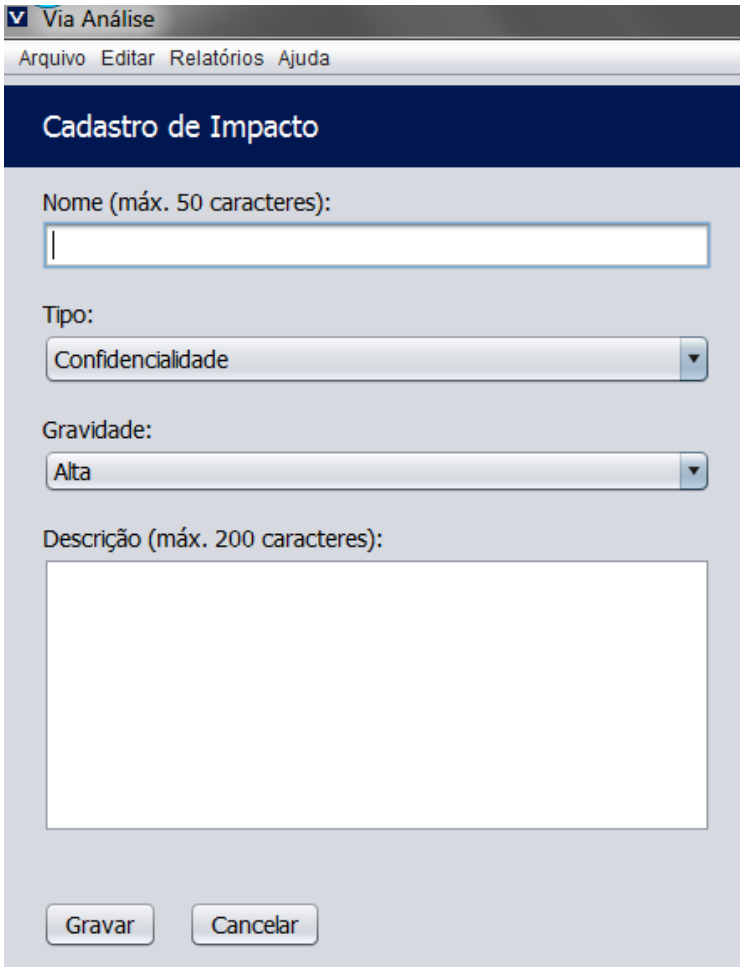
Para cadastrar uma Vulnerabilidade, acesse o menu Arquivo > Nova Vulnerabilidade.



Será solicitado que o usuário informe o nome da vulnerabilidade, a fonte de vulnerabilidade vinculada à ela, além da descrição completa da vulnerabilidade e um ou mais controles para controlar a vulnerabilidade.

Cadastrando Impacto

Para cadastrar um Impacto, acesse o menu Arquivo > Novo Impacto.



Será solicitado que o usuário informe o nome e a descrição do impacto, além das seguintes informações:

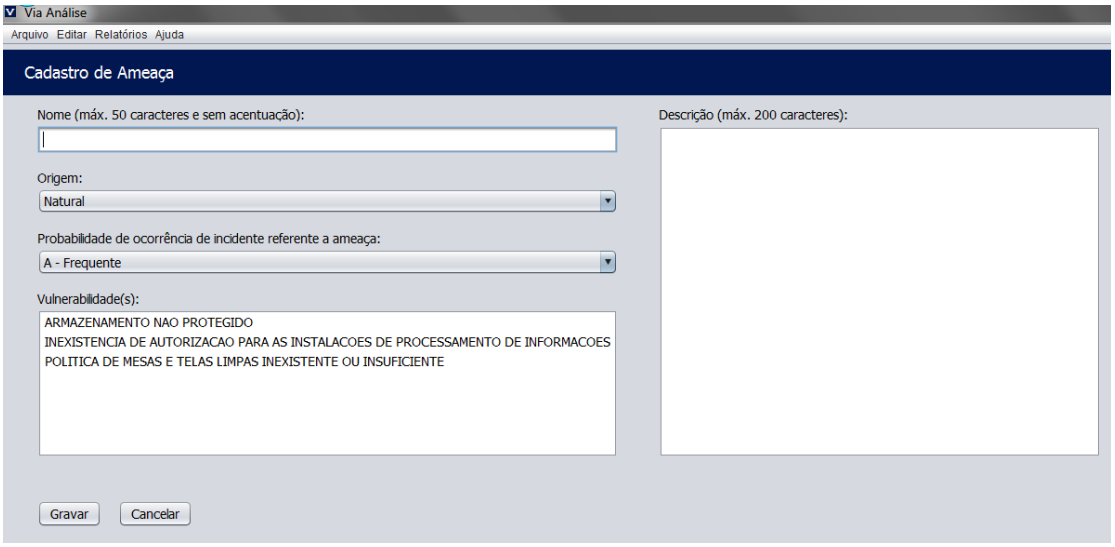
- Tipo: Confidencialidade, Integridade ou Disponibilidade. Confidencialidade é a propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

Integridade trata-se da propriedade de que a informação não é modificada ou destruída de maneira não autorizada ou acidental. Já a Disponibilidade é a propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade que possui autorização de acesso;

- Gravidade: Alta, Média ou Baixa.

Cadastrando Ameaça

Para cadastrar uma Ameaça, acesse o menu Arquivo > Nova Ameaça.

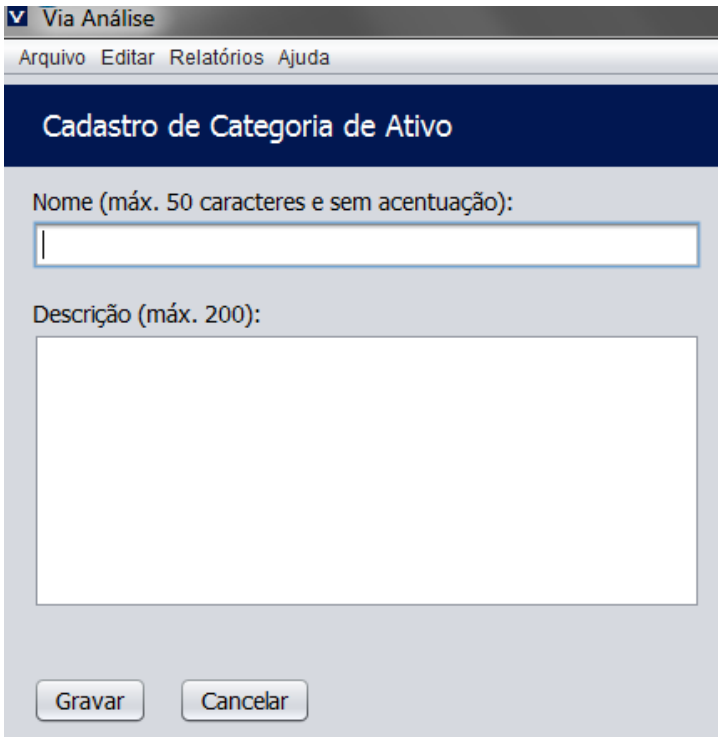


Será solicitado que o usuário informe o nome e a descrição da ameaça, além das seguintes informações:

- Origem: Natural, Humana ou Ambiental;
- Probabilidade de ocorrência de incidente referente a ameaça: Frequente, Provável, Ocasional, Remota, Improvável ou Impossível.

Cadastrando Categoria de Ativo

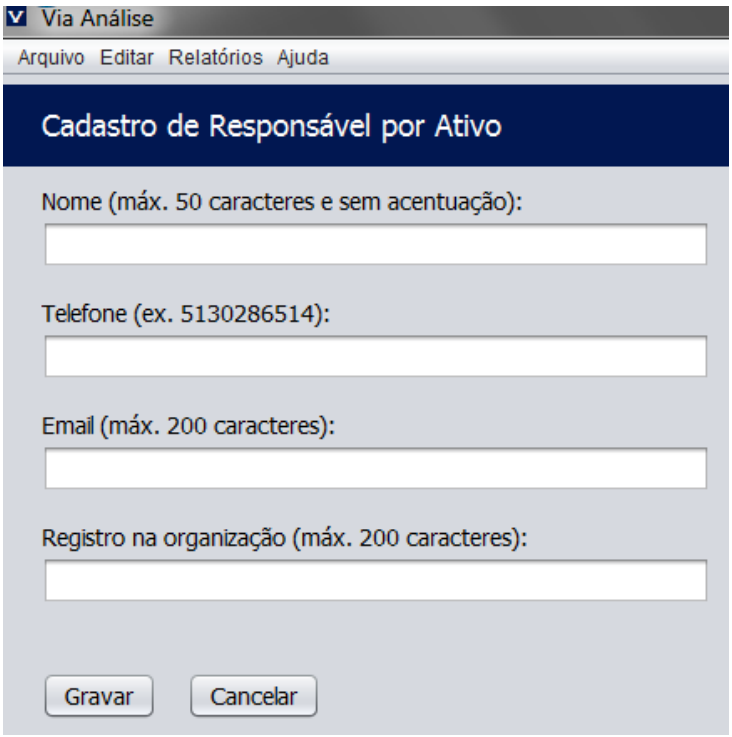
Para cadastrar uma Categoria de Ativo, acesse o menu Arquivo > Nova Categoria de Ativo.



Será solicitado que o usuário informe o nome e a descrição da categoria de ativo. Por padrão, o sistema terá cadastrado as seguintes categorias de ativos: Ativos de Informação, Ativos de Software, Ativos Físicos, Intangíveis, Pessoas e suas Habilidades, além da categoria Serviços.

Cadastrando Responsável por Ativo

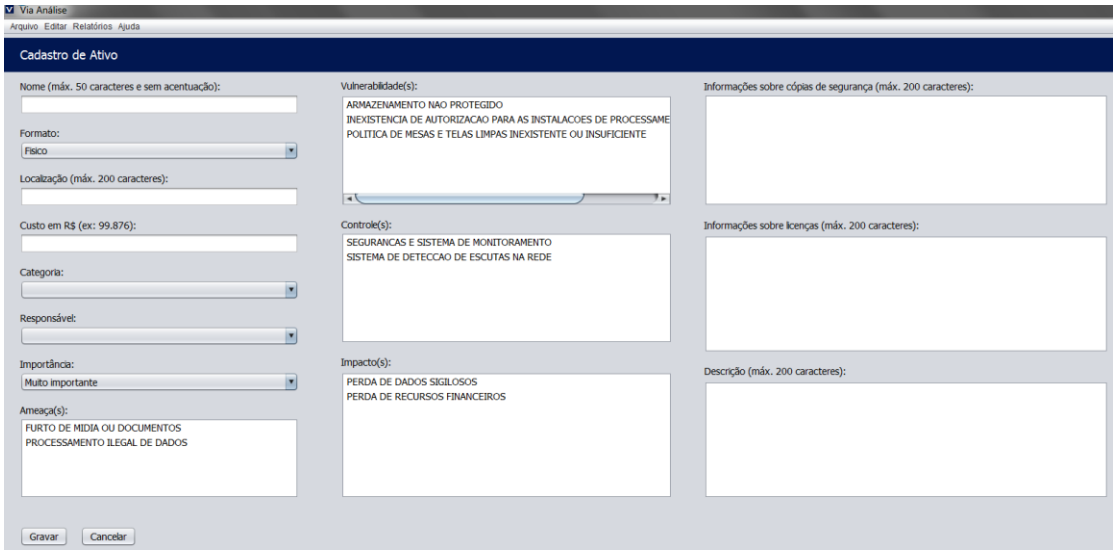
Para cadastrar um Responsável por Ativo, acesse o menu Arquivo > Novo Responsável por Ativo.



É requerido que o usuário informe o nome, telefone, email e registro da pessoa na organização. Ao vincular essa pessoa a um ativo de informação, diz-se que ela é responsável pela segurança do ativo.

Cadastrando Ativo

Para cadastrar um Ativo, acesse o menu Arquivo > Novo Ativo.



Serão solicitadas as seguintes informações:

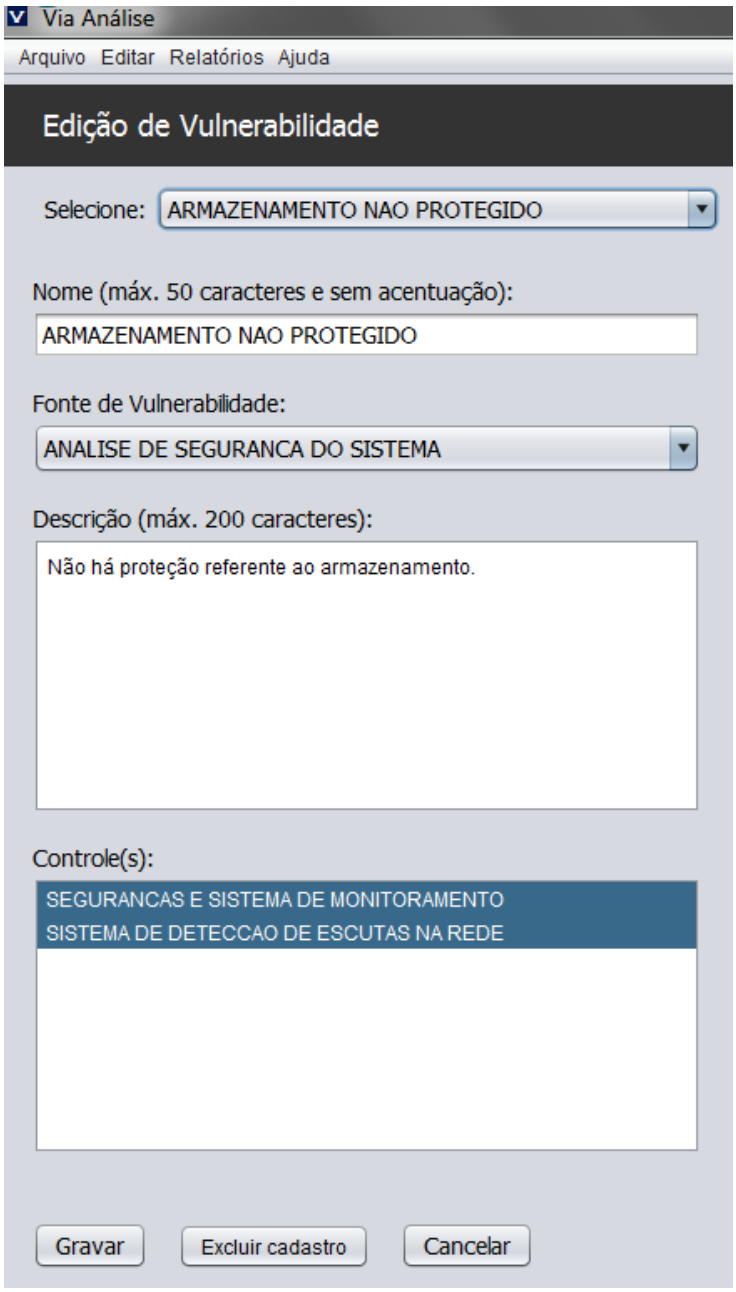
- Nome do ativo;
- Formato: Físico ou Eletrônico;

- Localização do ativo na organização (fisicamente ou o local em meio eletrônico);
- Custo do ativo para a organização (custo de aquisição);
- Categoria à qual o ativo se enquadra;
- Responsável pelo ativo;
- Importância do ativo para a organização: Muito importante, Importante, Média importância, Pouco importante ou Sem importância;
- Ameaça(s) que o ativo está sujeito;
- Vulnerabilidades exploradas pelas ameaças;
- Controle(s) para evitar as ameaças;
- Impacto(s) caso a(s) ameaça(s) se concretize(m);
- Informações sobre cópias de segurança;
- Informações sobre licenças;
- Descrição do ativo.

Edição e Remoção Capítulo 3

A edição para cada entidade do sistema é acessada através do menu Editar e segue as mesmas regras da inclusão. Entretanto, faz-se necessário primeiramente selecionar o registro que se deseja alterar para, em seguida, realizar as alterações.

A figura a seguir ilustra a tela de edição de Vulnerabilidade.



Se o usuário desejar excluir o registro, basta clicar no botão "Excluir cadastro". O sistema exibirá mensagem solicitando que o usuário confirme a operação e, caso o usuário confirme, o registro será removido.

Relatórios Capítulo 4

A ferramenta Via Análise suporta a criação de muitos relatórios. Exemplos de relatórios: Relatório de Ativos Críticos, Relatório de Fronteiras de Sistemas, Ativos Sensíveis e Relatório de Ameaças, Impactos, Vulnerabilidades e Controles. Entretanto, cada organização pode apresentar necessidades diferentes de outras e, portanto, necessitar de relatórios diferentes.

Contudo, na versão de demonstração tem-se um relatório de exemplo que contém os ativos, ameaças e suas respectivas probabilidades de ocorrência, responsável por cada ativo e o risco associado ao ativo.

Para a geração de relatórios, a ferramenta realiza um cálculo de risco citado por norma brasileira para gestão de riscos de segurança da informação e comunicações

A geração do relatório se dá através do menu Relatórios > Gerar Relatórios. Ao clicar no botão "Gerar Relatório de Ativos Críticos" o sistema gera o relatório em formato pdf e armazena-o no local *C:\Temp*.