UNIVERSIDADE DE CAXIAS DO SUL

ALLAN CALLONI

AVALIAÇÃO DE SOFTWARES DE GESTÃO DE RISCOS

CAXIAS DO SUL

2012

ALLAN CALLONI

AVALIAÇÃO DE SOFTWARES DE GESTÃO DE RISCOS

Trabalho de Conclusão de Curso para obtenção do Grau de Bacharel em Sistemas de Informação da Universidade de Caxias do Sul.

Orientadora: Maria de Fátima Webber do Prado Lima

CAXIAS DO SUL

2012

AGRADECIMENTOS

Agradeço aos meus familiares pelo apoio e incentivo ao longo de toda esta trajetória.

Agradeço também a Profa. Dra. Maria de Fátima Webber do Prado Lima pelo suporte e aprendizado durante esta etapa, e aos demais professores.

Agradeço ainda aos colegas, amigos e demais pessoas que, de alguma forma, contribuíram para a concretização deste objetivo.

RESUMO

Este trabalho tem como objetivo analisar e avaliar softwares de Gestão de Riscos de Segurança da Informação com o intuito de encontrar o mais apropriado e flexível para adaptar-se às constantes mudanças do ambiente organizacional. Para embasar esta avaliação, foram estudados conceitos de Segurança da Informação, Gestão de Riscos, três das principais metodologias (NBR ISO/IEC 27005, NIST SP 800-30 e OCTAVE) e suas diferenças básicas e, assim, foram definidos os critérios para a comparação dos softwares, de acordo com as funcionalidades fundamentais para realizar este processo. Foram avaliados os softwares VS Risk[1], STREAM[2], SOBF Tool[3] e SecureAware[4], detalhando sobre o funcionamento de cada um. O Método Analítico Hierárquico, uma importante ferramenta para auxiliar a tomada de decisões, foi utilizado para comparar os softwares para cada um dos critérios de avaliação definidos. De acordo com os critérios escolhidos, o software que atingiu a melhor avaliação foi o SecureAware.

Palavras-chave: Segurança da Informação, Gestão de Riscos, Método Analítico Hierárquico, Softwares.

[1] http://www.vigilantsoftware.co.uk

[2] http://www.acuityrm.com

[3] http://www.somap.org/orico/default.html

[4] http://www.neupart.com/products/iso-27005-risk-management.aspx

ABSTRACT

This study aims to analyze and evaluate softwares of Risk Management of Information Security in order to find the most appropriate and flexible to adapt to changing organizational environment. To support this evaluation, it has been studied concepts of Information Security, Risk Management, the three main methods (ISO / IEC 27005, NIST SP 800-30 and OCTAVE) and their basic differences and thus defined the criteria for comparing the softwares, in accordance with the basic functionalities to accomplish this process. We have evaluated the following softwares: VS Risk, STREAM, SOBF and SecureAware detailing on the operation of each one. The Analytic Hierarchy Method, an important tool to aid decision-making, was used to compare the softwares according to some predefined criteria. Given chosen criteria the software that has achieved better evaluation was SecureAware.

Keywords: Information Security, Risk Management, Analytic Hierarchy Process, Softwares.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O crescente avanço da tecnologia fez com que as informações se tornassem um dos principais patrimônios e diferenciais para qualquer organização. Sabendo do valor das informações, é de extrema importância que as mesmas sejam mantidas de forma segura e confiável, como qualquer outro ativo da empresa (ABNT, 2005).

Mas assim como a tecnologia e os sistemas computacionais evoluem, novos riscos surgem e ameaçam a segurança e confiabilidade das informações, através de fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo, inundação, entre outras formas (ABNT, 2005).

A segurança da informação é essencial para proteger estas informações, pois visa minimizar os danos, preservando sua confidencialidade, integridade e disponibilidade, evitando grandes perdas para a organização (ABNT, 2005). Mas para que a segurança da informação seja implantada, é necessário que se definam e implementem controles que sejam continuamente monitorados e analisados, buscando o seu aperfeiçoamento (MORAES, 2003 *apud* VIANEZ, SEGOBIA e CAMARGO, 2008).

Como o risco em relação às informações é uma fonte para possíveis perdas, o processo de identificá-los e reduzi-los é chamado de Gestão de Riscos. Este processo irá identificar as diversas ameaças e atuais vulnerabilidades na organização, verificando quais ações devem ser tomadas para que se antecipe de modo a evitar que impactos negativos sejam gerados, o que possivelmente pode ocasionar em prejuízo financeiro (STONEBURNER, GOGUEN e FERINGA, 2002).

Apesar da Gestão de Riscos tratar de uma área tão crítica para as empresas, não só considerando-se apenas a área da tecnologia da informação, mas todas as áreas da empresa, ela ainda é pouco implantada nas mesmas (STONEBURNER, GOGUEN e FERINGA, 2002). A Gestão de Riscos é o ponto de partida para a implantação dos Sistemas de Gestão da Segurança da Informação (SGSI), planos de continuidade e políticas de segurança.

Dentro das organizações os riscos vão mudando com o tempo, e a gestão de riscos deve ser ágil o bastante para acompanhar estas mudanças. Portanto, a gestão de riscos não trata de um projeto e sim de um processo, que deve atuar

sempre buscando uma melhoria contínua. Para garantir esta agilidade, as organizações necessitam utilizar softwares que sejam ágeis o suficiente para acompanhar as mudanças nas vulnerabilidades, nas ameaças e nos diversos riscos presentes. Também é importante salientar que a gestão de riscos não pode garantir que não existam mais riscos, mas que eles sejam minimizados a índices aceitáveis.

1.1 OBJETIVOS

O objetivo principal deste trabalho é realizar um levantamento de softwares que realizem gestão de riscos e verificar quais deles seriam mais dinâmicos e flexíveis para acompanhar as modificações do contexto organizacional. Os softwares que foram avaliados são aqueles que possuem versões disponíveis para testes.

A avaliação dos softwares leva em consideração os critérios a serem estabelecidos e se utiliza do método analítico hierárquico, que vai indicar, através da atribuição de valores para cada um dos critérios, qual(is) o(s) software(s) mais adequado(s) para realizar a gestão de riscos.

1.1.1 Objetivos secundários

(a) Conhecer alguns conceitos de segurança da informação, pois será o ponto de partida para o estudo do processo de gestão de riscos;
(b) Conhecer os conceitos de gestão de riscos, pois serão essenciais para o desenvolvimento do trabalho e obtenção do objetivo principal;
(c) Conhecer as principais metodologias utilizadas para realizar gestão de riscos;
(d) Estudar o funcionamento dos softwares de gestão de risco;
(e) Estudar o método analítico hierárquico.

1.2 ESTRUTURA DO TRABALHO

Os capítulos 2, 3 e 4 deste trabalho compõem a fundamentação teórica, sendo que no capítulo 2 são descritos conceitos de segurança da informação, no 3 são apresentados conceitos de gestão de riscos e o detalhamento de três metodologias de gestão de riscos: NBR ISO/IEC 27005, NIST SP 800-30 e OCTAVE, fazendo também, uma comparação das mesmas.

O capítulo 4 detalha o Método Analítico Hierárquico, que foi o método utilizado para a comparação dos softwares analisados.

No capítulo 5 são apresentados detalhes sobre o funcionamento dos quatro softwares a serem comparados. O capítulo 6 inicialmente aborda os critérios definidos e após, a avaliação dos softwares para cada um dos critérios, definindo as médias para cada um através do Método Analítico Hierárquico.

Por fim, o capítulo 7 faz uma conclusão do estudo realizado, indicando se algum software está de acordo com o objetivo proposto pelo trabalho.

2 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

Pode-se entender informação como sendo um conjunto de dados armazenados e que organizados possuem um significado (MCGEE e PRUSAK, 1994). As informações representam a inteligência e um ativo intangível que proporciona vantagens competitivas às organizações (SÊMOLA, 2003). A aplicação e o uso produtivo da informação caracterizam o conhecimento (BOISOT, 1998).

A segurança da informação é a forma de proteger as informações das diversas formas de ameaças para garantir confidencialidade, integridade e disponibilidade, minimizando os riscos e maximizando o retorno dos investimentos e as oportunidades de negócios. Mas para isto é preciso que sejam implementados alguns controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles devem ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde e quando necessário, para que os objetivos da organização sejam atendidos (MORAES, 2003 *apud* VIANEZ, SEGOBIA e CAMARGO, 2008).

A segurança da informação atua em três princípios básicos que sempre devem ser respeitados ou a segurança correrá riscos. Estes princípios são (CAMPOS, 2007):

(a) **Confidencialidade:** não permitir o acesso indevido às informações, mantendo-as em sigilo;
(b) **Integridade:** é essencial que a informação não seja modificada indevidamente;
(c) **Disponibilidade:** as informações devem sempre estar disponíveis quando forem necessárias, mas somente às pessoas autorizadas.

2.1 ATIVOS

Um ativo é tudo aquilo que tem valor e relevância para a empresa. Pode ser um recurso tangível ou intangível. Os ativos tangíveis são bens físicos, que podem ser tocados, como máquinas, móveis e materiais. Os ativos intangíveis não têm

existência física, como marcas, patentes, a imagem, nome e a reputação da empresa.

Dentro da área de tecnologia da informação, o hardware, documentos impressos, mídias magnéticas são considerados recursos tangíveis, enquanto os dados, informações, softwares, são ativos intangíveis. Alguns autores também classificam as pessoas como ativos.

Como a informação tem um grande valor para as organizações, é considerada um de seus principais e mais críticos ativos. Portanto, é preciso garantir a segurança deste ativo essencial (ISO/IEC 13335-1:2004).

2.2 AMEAÇA

Uma ameaça é uma fonte que irá explorar as vulnerabilidades podendo causar danos. Elas podem ser criadas intencionalmente ou podem ocorrer acidentalmente. Podem ser de origem natural (enchentes, terremotos, tornados, deslizamento de terra, tempestades de raios), humana (atos dolosos, negligentes, imperitos ou imprudentes de uso de programas maliciosos, de acesso a dados sigilosos, de mau uso dos sistemas), ou ambiental (falta de energia, poluição e substâncias químicas). A fonte de ameaça só irá apresentar riscos se houverem vulnerabilidades (STONEBURNER, GOGUEN e FERINGA, 2002). Os atos intencionais são chamados de ataques, e se bem sucedidos caracterizam uma intrusão.

Nem toda ameaça para uma empresa é para outra, pois se devem levar em conta os aspectos culturais e relacionados ao ambiente (ABNT, 2008).

2.3 VULNERABILIDADES

Vulnerabilidades são falhas nos processos de segurança, nos projetos ou nos controles internos de um sistema, que, se explorados, podem ocasionar danos (STONEBURNER, GOGUEN e FERINGA, 2002). Mas vulnerabilidades só

representam perigo se existir a possibilidade de serem exploradas, ou seja, se houverem ameaças.

Alguns métodos podem ser utilizados para identificar vulnerabilidades, entre eles estão (ABNT, 2008):

(a) Sistemas de varredura e análise de vulnerabilidades;

(b) Testes e simulações;

(c) Testes de invasão de sistemas;

(d) Auditorias em códigos-fonte;

(e) Listas de verificação e análise crítica de segurança.

2.4 RISCOS

Segundo o dicionário Michaelis (2012), o termo risco significa:

> *"sm (ital rischio) Possibilidade de perigo, incerto mas previsível, que ameaça de dano a pessoa ou a coisa. R. bancário, Com: o que decorre do negócio entre banqueiros ou entre o banco e os correntistas. R. profissional, Dir: perigo inerente ao exercício de certas profissões, o qual é compensado pela taxa adicional de periculosidade. A risco de, com risco de: em perigo de. A todo o risco: exposto a todos os perigos. Correr risco: estar exposto a."*

De acordo com Hori (2003), outros autores definem risco como:

"Risco pode ser definido, de forma abrangente, como potencial de eventos ou tendências continuadas causarem perdas ou flutuações em receitas futuras". (MARSHALL, 2002, pág. 19).

"(...) a possibilidade de que os resultados realizados possam ser diferentes daqueles esperados." (GITMAN, 1997, pág. 17).

O risco, na tecnologia da informação é um impacto negativo, uma fonte para possíveis perdas motivadas pela exploração de uma vulnerabilidade (STONEBURNER, GOGUEN, FERINGA, 2002).

2.5 MEDIDAS DE SEGURANÇA

O primeiro passo para aumentar a segurança da informação é através de medidas de segurança, que são ações para eliminar ou reduzir as vulnerabilidades, para que o impacto das ameaças seja o menor possível.

Para cada ponto fraco deve haver medidas de segurança específicas para que a confidencialidade, integridade e disponibilidade das informações não sejam afetadas. As medidas de segurança podem ser preventivas, perceptivas e corretivas. As preventivas evitam que novos pontos fracos e ameaças surjam. As perceptivas são para revelar atos que podem ameaçar as informações. As medidas corretivas são as que corrigem os problemas de segurança quando ocorrem.

As medidas de segurança são um conjunto de práticas que, quando integradas tornam-se uma solução global e eficaz. Algumas das principais medidas (MODULO, 2006):

(a) Análise de riscos: medida que visa encontrar vulnerabilidades nos ativos que podem ser exploradas por ameaças. Resulta em diversas recomendações para a proteção dos ativos;

(b) Diretiva de segurança: medida que estabelece os padrões de segurança a serem seguidos pelos envolvidos no uso e manutenção dos ativos. Faz com que as pessoas se conscientizem com a segurança;

(c) Especificações de segurança: medidas para instruir a implementação correta de um novo ambiente tecnológico através dos detalhes dos elementos que o constituem e da forma como estes devem estar dispostos para atender os princípios de segurança;

(d) Administração da segurança: medidas para realizar a gestão de riscos de uma organização. Envolve as medidas do tipo preventiva, perceptiva e corretiva.

2.6 CONTROLES

Controles são práticas, procedimentos ou mecanismos que podem proteger

um ativo contra uma ameaça, reduzir a vulnerabilidade, limitar o impacto de evento indesejável, detectar incidentes de segurança e facilitar o processo de recuperação do ambiente. A proteção dos ativos requer que sejam feitas diferentes combinações de controles para implementar as camadas de segurança necessárias (OLIVEIRA, 2006).

Os controles são empregados para detecção, proteção, prevenção, limitação, correção, recuperação, monitoramento e conscientização. Alguns exemplos de tipos de controles (ISO IEC TR 13335-1, 1996 *apud* OLIVEIRA, 2006):

(a) Firewalls de rede;

(b) Criptografia;

(c) Antivírus;

(d) Backups;

(e) Mecanismos de controle de acesso;

(f) Geradores de energia;

(g) Assinatura digital;

(h) Procedimentos operacionais.

3 GESTÃO DE RISCOS

O processo que identifica, mensura e planeja os passos para reduzir os riscos à níveis aceitáveis para cada organização, analisando os possíveis acontecimentos e suas consequências, auxiliando na tomada a decisão, é definido como Gestão de Riscos (STONEBURNER, GOGUEN e FERINGA, 2002, ABNT, 2008).

Stoneburner (2002) destaca que o processo de gestão de riscos não é importante apenas para a área de tecnologia da informação e comunicações, mas sim para todas as unidades da empresa.

Ao se tratar de riscos, são três os principais aspectos que não devem ser deixados de lado em um projeto de segurança (WESTERMAN e HUNTER, 2008):

(a) **Processos:** Metodologia, normas e procedimentos;

(b) **Pessoas:** Cultura, capacitação, conscientização;

(c) **Tecnologia:** Recursos físicos e lógicos – infraestrutura e aplicações.

As principais normas que fornecem diretrizes para o processo de gestão de riscos de segurança da informação de uma organização são a NBR ISO/IEC 27005 (ABNT, 2008), NIST SP 800-30 (STONEBURNER, GOGUEN, FERINGA, 2002) e OCTAVE (ALBERTS, 2001).

3.1 NBR ISO/IEC 27005

A NBR ISO/IEC 27005 é uma norma que fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo os requisitos de um SGSI de acordo com a ABNT NBR ISO/IEC 27001. Porém, nesta norma não há uma metodologia específica para a gestão de riscos de segurança da informação, cabendo a organização definir sua abordagem ao processo de gestão de riscos, considerando o escopo do seu SGSI, o contexto da gestão de riscos e o seu setor de atividade econômica.

De acordo com esta norma, a gestão de riscos deve contribuir para (ABNT,

2008):

(a) Identificação de riscos;
(b) Análise e avaliação de riscos que podem prejudicar o negócio e sua probabilidade de ocorrência;
(c) Comunicação e entendimento da probabilidade e das consequências dos riscos;
(d) Estabelecimento de prioridades para tratamento dos riscos;
(e) Priorização das ações para redução de ocorrência de riscos;
(f) Eficácia do monitoramento do tratamento do risco;
(g) Monitoramento e análise crítica regular;
(h) Treinamento de funcionários a respeito dos riscos e ações para mitigá-los.

O processo de gestão de riscos (Figura 1) inicia na definição do contexto, passando a seguir para a fase de análise e avaliação de riscos. Se nesta etapa foi possível determinar as ações para a redução dos riscos, passa-se ao próximo passo, o tratamento do risco. Caso contrário o processo volta à definição do contexto, onde será revisado para avaliar o que pode ter ocasionado os problemas.

Mas para que o tratamento do risco produza resultados satisfatórios, é preciso que os resultados da análise e avaliação dos riscos sejam adequados, caso contrário, deve reavaliar as variáveis do contexto, ou a análise e avaliação dos riscos. No passo seguinte, de aceitação do risco, deve abranger apenas os riscos aceitáveis para a organização.

Durante este processo, deve ser mantida a comunicação dos gestores com suas áreas, para que ações já possam ser tomadas com o intuito de evitar possíveis prejuízos.

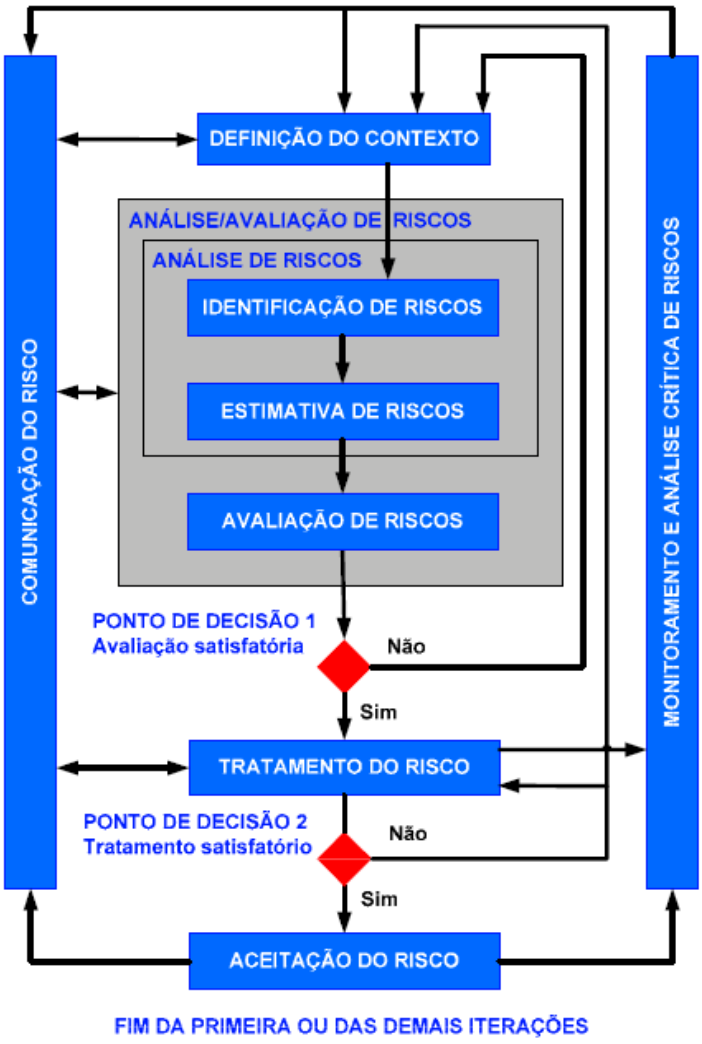


Figura 1: Processo de Gestão de Riscos NBR ISO/IEC 27005 (ABNT, 2008)

3.1.1 Definição do contexto

Nesta fase devem ser consideradas todas as informações que podem ser relevantes para a definição do contexto da gestão de riscos. O contexto deve abordar os critérios básicos, o escopo e limites e a organização para o processo de gestão de riscos da empresa.

O processo de gestão de riscos deve considerar alguns critérios básicos para avaliação de riscos, impacto e aceitação do risco.

Os critérios para avaliação de riscos devem levar em consideração o nível de criticidade dos ativos envolvidos; requisitos legais e obrigações contratuais e a importância da confidencialidade, disponibilidade e integridade.

É importante para o processo que todos os ativos relevantes sejam levantados e seja definido até que ponto o risco é aceitável.

A empresa deve definir o escopo do processo de gestão de riscos, para que todos os ativos relevantes sejam considerados. Também deve identificar os limites, para saber quando um risco passou de determinado limite.

Algumas informações a serem consideradas ao definir o escopo e os limites:

(a) Objetivos estratégicos, políticas e estratégias da organização;
(b) Processos de negócio;
(c) Funções e estrutura da organização;
(d) Requisitos legais, regulatórios e contratuais aplicáveis à organização;
(e) Política de segurança da informação da organização;
(f) Abordagem da organização em relação à gestão de riscos;
(g) Ativos de informação;
(h) Localidades em que a organização se encontra e suas características geográficas;
(i) Restrições que afetam a organização;
(j) Expectativas das partes interessadas;
(k) Ambiente sociocultural;
(l) Interfaces – troca de informações com o ambiente.

Com o desenvolvimento do processo de gestão de riscos para a organização é preciso identificar as partes interessadas, distribuindo seus papéis e responsabilidades e como será a forma da tomada de decisões.

Para que o processo de gestão de riscos seja implementado, os seguintes itens são imprescindíveis (DILLARD, 2004):

(a) **Patrocínio executivo:** a alta direção deve apoiar o processo e não ser resistente às mudanças;
(b) **Lista de interessados:** as pessoas que se interessarem pelo processo de gestão de riscos, poderão ser envolvidos para colaborarem durante as

etapas;

(c) **Maturidade corporativa:** se a empresa tiver pouca experiência nos processos, necessitará mudanças rápidas e radicais;

(d) **Ambiente de comunicação:** toda equipe deve manter uma comunicação aberta e honesta, evitando mal-entendidos e desperdício de tempo;

(e) **Espírito de equipe:** é importante que a equipe esteja engajada e trabalhe em conjunto;

(f) **Visão holística:** o processo de gestão de risco deve ser fundamentado na organização como um todo, não apenas uma área específica;

(g) **Autoridade:** a equipe envolvida precisa ter autoridade para que as mudanças necessárias sejam realmente feitas.

3.1.2 Análise de riscos

Com a definição dos critérios básicos, o escopo e os limites e a organização do processo, os riscos começam a ser analisados e quantificados, de acordo com os critérios estabelecidos. A análise de riscos é composta pela fase de identificação dos riscos e pela estimativa dos riscos.

3.1.2.1 Identificação dos riscos

Nesta fase são analisados todos os eventos que podem causar danos, e como e quando eles podem ocorrer, através da identificação dos riscos, das ameaças e das vulnerabilidades, os ativos de informação são mensurados, os controles existentes são analisados e as consequências são determinadas. As atividades que fazem parte desta fase são:

(a) Identificação dos ativos;

(b) Identificação das ameaças;

(c) Identificação dos controles existentes;

(d) Identificação das vulnerabilidades;

(e) Identificação das consequências.

Na **identificação dos ativos**, pode-se separar os ativos em dois grupos: os ativos primários e os ativos de suporte e infraestrutura. Os ativos primários são os processos e atividades do negócio e a informação. Os ativos de suporte e infraestrutura são:

(a) **Hardware:** Equipamento de processamento de dados; equipamento móvel; equipamento fixo; periféricos de processamento; mídia de dados; mídia eletrônica e outros tipos de mídia.
(b) **Software:** Sistema operacional; software de serviço, manutenção ou administração; software de pacote ou de prateleira.
(c) **Rede:** O meio físico e a infraestrutura; pontes passivas ou ativas; interface de comunicação.
(d) **Recursos Humanos:** Tomador de decisão; usuários; pessoal de produção/manutenção; desenvolvedores.
(e) **Instalações físicas:** Ambiente externo; edificações; servidores essenciais; comunicação; servidores de infraestrutura.
(f) **A estrutura da organização:** Autoridades; a estrutura da organização; organização de projeto e serviço; fornecedores.

Após a identificação dos ativos, deve-se determinar uma escala de medida e os critérios para indicar a posição de um ativo, de acordo com seu valor. A escala pode ser qualitativa ou quantitativa, de acordo com a preferência da organização.

Se for escolhida a escala qualitativa o valor dos ativos pode ser representado por expressões como as seguintes: insignificante, muito pequeno, pequeno, médio, alto, muito alto e crítico. É uma escala simples e permite fácil entendimento.

Já a escala quantitativa é uma representação numérica, onde os valores são determinados de acordo com os custos ou prejuízos dos ativos. Esta escala é mais complexa, mas pode proporcionar maior precisão, porém só é recomendável se todos os ativos puderem ser mensurados.

Na etapa de **identificação das ameaças,** a atividade é identificar as

ameaças que possam comprometer os ativos seja elas de origem natural ou humana, acidentais ou intencionais. As ameaças podem ser internas ou externas à organização, e todos os tipos devem ser identificados.

O anexo C da norma exemplifica algumas ameaças comuns. Estas ameaças podem ser intencionais (I), acidentais (A) ou naturais (N). A tabela 1 relaciona algumas ameaças constantes na norma.

Tabela 1: Exemplos de Ameaças

Tipo	Ameaças	Origem
Dano físico	Fogo, água, poluição, acidente grave, destruição de equipamento, poeira, corrosão, congelamento.	A,I,N
Eventos naturais	Fenômeno climático, sísmico, vulcânico ou meteorológico, inundação.	N
Paralisação de serviços essenciais	Falha do ar condicionado ou sistema de suprimento de água	A,I
	Interrupção da energia.	A, I, N
	Falha do equipamento de telecomunicação.	A, I
Comprometimento da informação	Espionagem à distância, escuta não autorizada, furto de mídia ou documentos, furto de equipamentos, alteração do hardware.	I
	Divulgação indevida, dados de fontes não confiáveis, alteração do software.	A, I
Falhas técnicas	Falha ou defeito de equipamento, defeito de software.	A
	Saturação do sistema de informação	A, I
Ações não autorizadas	Uso não autorizado de equipamento, cópia ilegal de software, comprometimento dos dados, processamento ilegal de dados.	I
	Uso de cópias de software falsificadas ou ilegais.	A, I
Comprometimento das funções	Erro durante o uso.	A
	Abuso de direitos.	A, I
	Forjamento de direitos, repúdio de ações.	I
	Indisponibilidade de recursos humanos	A, I, N

Fonte: ABNT, 2008

Na etapa de **identificação dos controles existentes** se faz uma revisão das documentações dos controles já existentes, analisando se existe duplicação de controles e se os mesmos estão funcionando adequadamente, sem possibilitar a exploração de ameaças. Controles desnecessários significam custos e trabalho desnecessários.

Verificar também, com as pessoas interessadas, se os controles necessários já estão implementados e considerar a possibilidade de controles complementares, caso os existentes falhem em determinado momento.

Ao final desta etapa, será gerada uma lista dos controles existentes e os planejados, juntamente com sua implementação e status de utilização.

Na **identificação de vulnerabilidades**, é preciso listar as vulnerabilidades que podem ser exploradas pelas ameaças já conhecidas.

O resultado será uma lista das vulnerabilidades associadas aos ativos, às ameaças e aos controles e uma lista das vulnerabilidades que não se identifique com nenhuma ameaça analisada.

É importante listar as vulnerabilidades, as quais não existam ameaças para explorá-la, pois não é necessária a implementação de controles, mas deve ser feito o monitoramento da vulnerabilidade, para o caso de mudança de cenário.

As vulnerabilidades podem ser identificadas nas seguintes áreas:

(a) Organização;

(b) Processos e procedimentos;

(c) Rotinas de gestão;

(d) Recursos humanos;

(e) Ambiente físico;

(f) Configuração do sistema de informação;

(g) Hardware, software ou equipamentos de comunicação;

(h) Dependência de entidades externas.

Exemplos de vulnerabilidades e avaliação de vulnerabilidades constam no Anexo D da norma.

A última etapa da análise riscos é a **identificação das consequências.** Nesta etapa se identificam as consequências e o prejuízo que a organização está sujeita a ter com a perda de confidencialidade, integridade e disponibilidade de um ativo, se o mesmo for comprometido por algum incidente. Além do prejuízo, outras consequências podem ser a perda da eficácia, a perda de oportunidades de negócio, reputação afetada, etc.

Podem ser afetados um ou mais ativos, e para mensurar as consequências,

podem ser atribuídos valores correspondendo aos seus custos financeiros ou às consequências ao negócio.

As consequências podem ser de natureza temporária ou permanente, como no caso da destruição de um ativo.

Alguns itens que devem ser considerados para identificação das consequências:

(a) Investigação e tempo de reparo;
(b) Tempo (de trabalho) perdido;
(c) Oportunidade perdida;
(d) Saúde e Segurança;
(e) Custo financeiro das competências específicas necessárias para reparar o prejuízo;
(f) Imagem, reputação e valor de mercado.

Ainda dentro da análise de riscos, é feita a estimativa de riscos, que pode usar a metodologia qualitativa ou quantitativa, ou até mesmo as duas, dependendo do caso.

3.1.2.2 Estimativa de riscos

A etapa de estimativa divide-se na avaliação das consequências, na avaliação da probabilidade dos incidentes e na estimativa do nível de riscos.

Na **avaliação das consequências**, após serem identificados os ativos mais relevantes, devem ser atribuídos valores para o impacto que cada um representa para o negócio, dependendo da sua criticidade e das ameaças e vulnerabilidades envolvidas. Estes valores podem ser determinados pelo custo de reposição do ativo, ou as consequências sobre o negócio em função do ativo que foi afetado. A utilização de métodos qualitativos ou quantitativos dependerá de cada organização, podendo inclusive, serem usados os dois tipos de métodos.

Na **avaliação da probabilidade dos incidentes**, irá se avaliar a probabilidade e o impacto de cada cenário de incidente, verificando sua frequência e

facilidade das vulnerabilidades serem exploradas através de experiências passadas, estatísticas, vulnerabilidades, controles existentes e sua eficácia, fontes de ameaças intencionais, e acidentais.

Após, a **estimativa do nível de riscos**, todos os cenários de incidentes relevantes para a organização devem ser valorados, indicando valores para a probabilidade e para as consequências de um risco, podendo esta estimativa ser qualitativa ou quantitativa.

3.1.3 Avaliação de riscos

Nesta etapa é onde são comparados os riscos estimados com os critérios de avaliação de riscos, definidos durante a definição do contexto, verificando se estão dentro de um nível aceitável de risco. Mas neste momento, é necessário também analisar a probabilidade e as consequências que cada risco pode impactar nos ativos. Os riscos são classificados de acordo com sua criticidade, em função da importância dos ativos para o negócio da organização. Um risco pode ser de alto nível, mas seu impacto financeiro pode ser baixo, portanto, é necessário que se faça a priorização dos riscos.

A avaliação dos riscos pode ser feita com enfoque em alto nível ou mais detalhada.

Por razões como orçamento e tempo, muitas vezes o enfoque em alto nível é mais recomendado, assim apenas os riscos mais críticos serão tratados durante o processo de tratamento do risco. Este enfoque abrange uma visão mais global da organização e de seus sistemas, se preocupa com uma lista menor de ameaças e vulnerabilidades para acelerar o processo. Por não tratar de detalhes tecnológicos, a avaliação de riscos de alto nível é mais adequada para fornecer controles organizacionais e não técnicos. O problema deste tipo de enfoque é que alguns processos importantes podem ser descartados para uma análise mais detalhada.

Para determinar se a avaliação de alto nível é adequada para o tratamento do riscos, é preciso analisar os fatores:

(a) Os objetivos de negócio a serem alcançados através de vários ativos

de informação;

(b) O quanto o negócio da organização depende de cada ativo da informação;

(c) O nível de investimento em cada ativo de informação, considerando o desenvolvimento, manutenção ou reposição do ativo;

(d) Os ativos de informação, para cada um dos quais a organização atribui um valor.

O processo de avaliação detalhada de riscos faz uma minuciosa identificação e valoração dos ativos, avaliação das ameaças aos ativos e avaliação das vulnerabilidades. Os resultados destas atividades serão usados para avaliar os riscos e identificar o tratamento do risco.

A avaliação detalhada demanda bastante tempo, esforço e experiência, e pode ser mais adequada para os sistemas de informação de alto risco.

Outro ponto importante a ser considerado, são os requisitos contratuais, legais e regulatórios.

Ao final desta etapa, o resultado será uma lista com os riscos ordenados por prioridade, associando-os aos cenários de incidentes que os provocam.

3.1.4 Tratamento do risco

Com a lista de riscos gerada na avaliação de riscos, passa-se ao tratamento deles, que podem ser através de redução do risco, retenção do risco, evitar o risco e transferência do risco (figura 2).

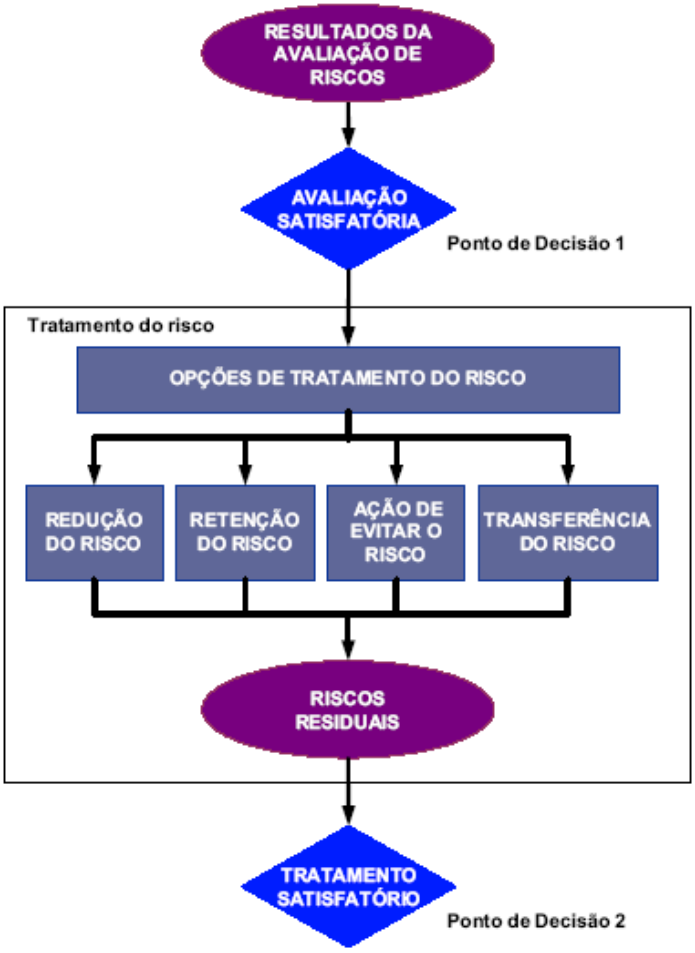


Figura 2: Tratamento do risco (ABNT, 2008)

No caso da redução do risco, deve-se selecionar os controles adequados, para que o risco seja reduzido a um nível aceitável. Prazos e custos para a implementação dos controles devem ser considerados.

O resultado será uma lista de controles, demonstrando seu benefício, prioridade e custo para implementação.

A retenção do risco ocorre quando o nível de risco está dentro do aceitável e novos controles não são necessários.

Mas, se o risco identificado é excessivamente elevado e se os custos para tratá-lo são maiores que os benefícios, pode se decidir que o risco evitado completamente, seja através da eliminação de uma atividade planejada ou existente, seja por meio de mudanças nas condições em que a operação da atividade ocorre.

Um exemplo é para riscos causados por fenômenos naturais, em que a alternativa mais benéfica seja mover fisicamente as instalações de processamento de informações para um local onde o risco não existe ou pode ser controlado.

A transferência do risco se dá quando a empresa contrata uma parceira para monitorar e evitar o risco. Mas isso pode gerar novos riscos ou modificar os já existentes, por isso, pode ser preciso realizar um novo tratamento do risco.

3.1.5 Aceitação do risco

Depois do tratamento dos riscos, os mesmos passarão pela fase de aceitação do risco, que irá determinar quais deles poderão ser aceitos pela organização, dependendo do nível de risco que oferecem aos ativos. Caso o risco não seja alto e o custo para contê-lo seja elevado, às vezes é preferível aceitar este risco.

Será gerada uma lista com os riscos aceitos e especificando o motivo dos que não foram aceitos.

3.1.6 Comunicação do risco

Todas as informações obtidas sobre os riscos deverão ser compartilhadas entre os tomadores de decisão e as partes interessadas.

3.1.7 Monitoramento e análise crítica

Com todas as informações obtidas com a gestão de riscos, estas devem ser permanentemente monitoradas, para verificar se algo mudou em relação a ameaças, vulnerabilidades, ativos, impactos, probabilidade de ocorrência, entre outros fatores.

Os itens que necessitam o monitoramento constante são:

(a) A inclusão de novos ativos;

(b) Alteração nos valores dos ativos;

(c) Novas ameaças, tanto fora quanto dentro da organização;

(d) A possibilidade de vulnerabilidades novas ou ampliadas que possam permitir a entrada de alguma ameaça;

(e) As vulnerabilidades identificadas, verificando se podem ser exploradas pelas novas ameaças.

Um resumo das etapas e das entradas e saídas de cada fase pode ser visto na figura 3.

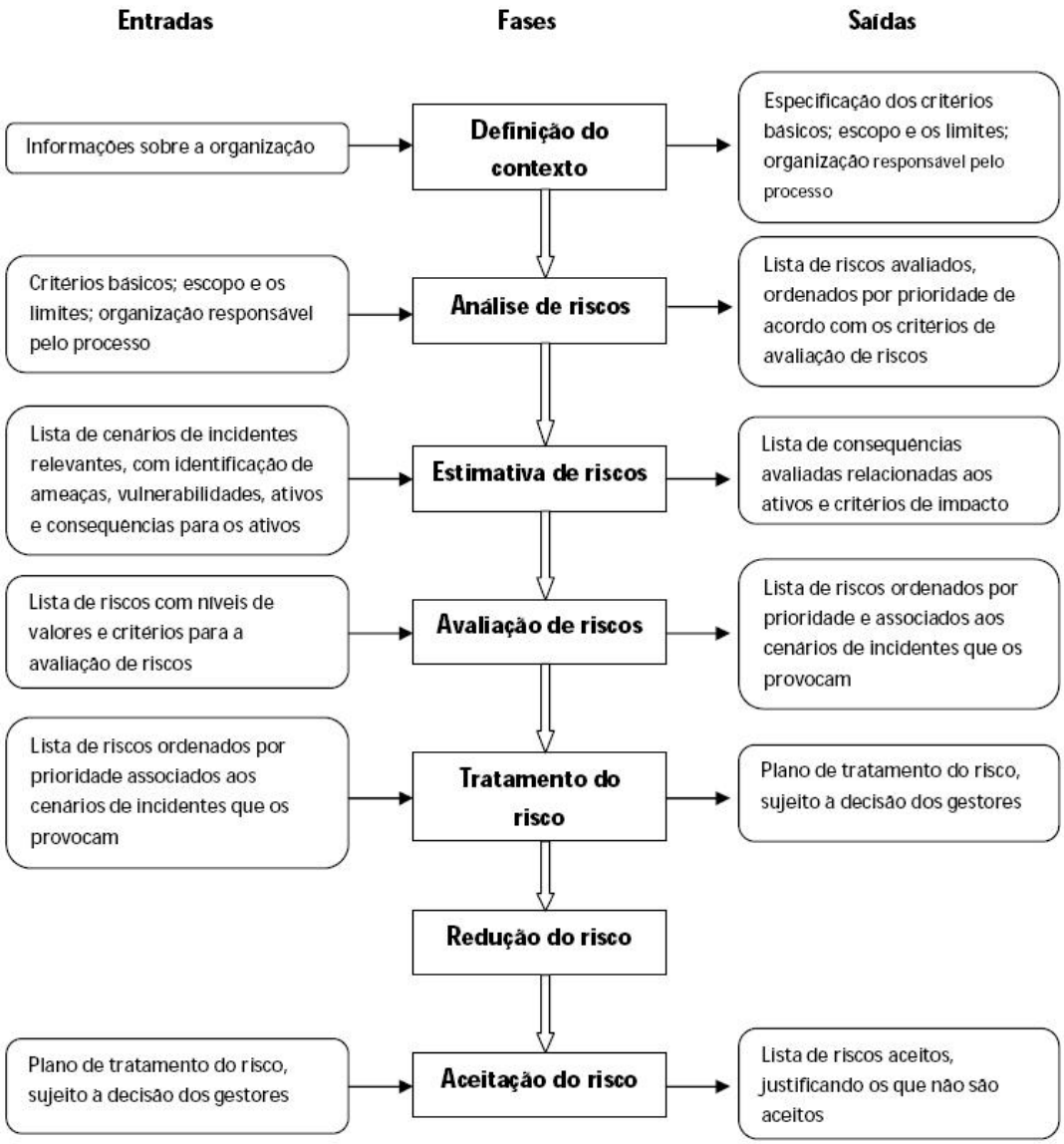


Figura 3: NBR ISO/IEC - Entradas e saídas de cada fase

3.2 NIST SP 800-30

A NIST SP 800-30 é uma publicação composta por orientações detalhadas para fundamentar um processo de gestão de riscos de TI, definindo o que deve ser feito para avaliar e reduzir os riscos.

A metodologia divide-se em duas etapas: avaliação de riscos e atenuação de riscos. Mas, além destas, também é importante que uma revisão periódica seja feita (STONEBURNER, GOGUEN, FERINGA, 2002).

3.2.1 Análise e Avaliação dos Riscos

O processo de avaliação de riscos é responsável por determinar a potencialidade das ameaças e riscos da Tecnologia da Informação.

A avaliação de riscos é composta por uma sequência de nove passos: (i) caracterização do ambiente; (ii) identificação de ameaças; (iii) identificação de vulnerabilidades; (iv) análise de controles; (v) determinação de probabilidades; (vi) análise de impacto; (vii) definição dos riscos; (viii) recomendações de controles e documentação dos resultados (Figura 4).

A **caracterização do ambiente** é responsável por definir o escopo da avaliação de riscos, os limites operacionais, recursos computacionais, pessoas envolvidas e as informações que serão abrangidas no processo de gerenciamento de riscos.

Para coletar informações relacionadas com o ambiente de Tecnologia da Informação, pode se fazer uso de um questionário específico, entrevistas com usuários chave, revisão das documentações, ou uma combinação de várias destas técnicas.

A caracterização do ambiente é semelhante à definição do contexto da norma NBR ISO/IEC 27005, assim como as etapas seguintes do NIST, a identificação de ameaças e a identificação de vulnerabilidades, que são similares às etapas correspondentes da NBR ISO/IEC 27005.

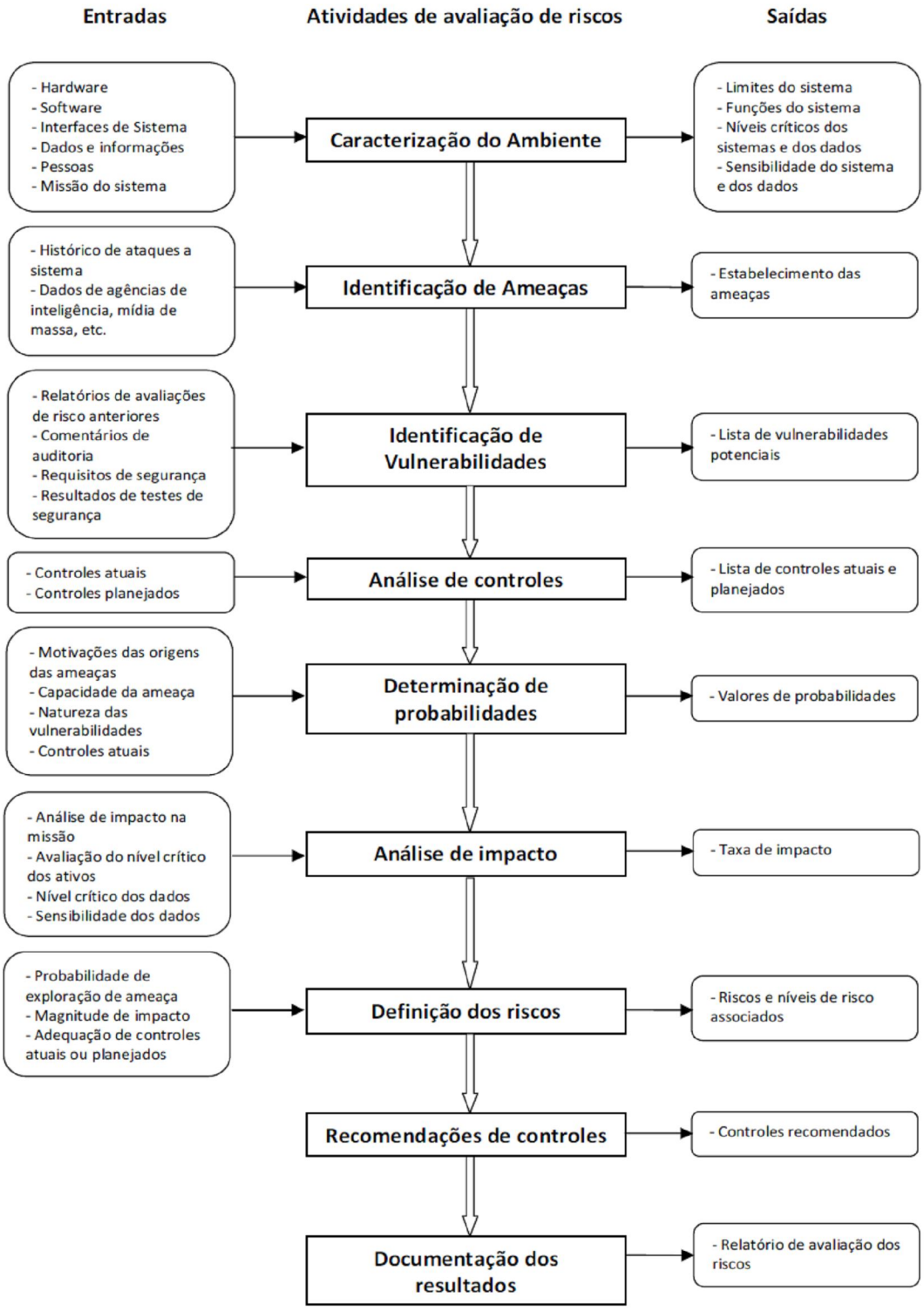


Figura 4: Processo de Avaliação de riscos (STONEBURNER, 2002)

Na **avaliação de controles** são avaliados os controles existentes verificando se estão funcionando e se não existem controles desnecessários, além de planejar novos controles. Existem controles preventivos, que são os que inibem as tentativas de violação de segurança, ou podem visar a detecção de possíveis ataques. Os controles podem ser também classificados como técnicos e não técnicos. Os controles técnicos são os que podem ser incorporados no hardware e software dos sistemas, os controles não técnicos são controles de gerenciamento e operacionais como políticas de segurança, procedimentos operacionais, gestão de pessoal e controles físicos ou ambientais.

Na **definição de probabilidades** são decididos valores para as probabilidades de uma vulnerabilidade ser explorada por uma ameaça. A metodologia define três níveis de probabilidade: alta, média e baixa. Considera-se uma probabilidade alta quando podem ser exercidas ameaças e não existem controles para preveni-las ou estes não estão funcionando devidamente. Probabilidades médias são quando a fonte de ameaça está motivada e pode exercer a ameaça, mas os controles utilizados são efetivos, não permitindo a sua entrada. E as probabilidades são baixas quando não há motivação por parte das fontes de ameaças e os controles existentes são efetivos.

Para definir melhor as probabilidades é interessante considerar as experiências passadas e estatísticas de ocorrência de ameaças; as motivações, competências e ferramentas disponíveis para a realização de atos intencionais, e a percepção de vulnerabilidades em ativos valiosos; as situações que podem produzir erros humanos; e a análise de efetividade dos controles atuais.

A **análise de impacto** é um importante processo da avaliação de riscos, pois determina o resultado do impacto ao sistema e ao negócio caso uma ameaça tenha sucesso na exploração de uma vulnerabilidade.

O impacto pode ser descrito em termos de perda ou degradação de qualquer uma ou da combinação das propriedades de segurança: integridade, disponibilidade e confidencialidade.

Para definir os impactos, é necessário conhecer o objetivo, a criticidade e sensibilidade dos sistemas e dos dados. Os impactos tangíveis podem ser mensurados quantitativamente através de uma unidade de medida conhecida, como:

perda de desempenho, custos de manutenção ou tempo gasto para corrigir o problema. Os de difícil mensuração podem ser definidos qualitativamente como de alto, médio ou baixo impacto (tabela 2), de acordo com o custo pela perda dos ativos ou recursos e significado que o dano representa para o negócio da empresa.

Tabela 2: Definição da magnitude do impacto

	Definição de impacto
Alto	(1) pode resultar em prejuízo muito alto dos principais ativos tangíveis ou recursos; (2) pode significativamente violar, prejudicar ou impedir a missão de uma organização, sua reputação ou interesse; (3) pode resultar em morte humana ou ferimentos graves.
Médio	(1) pode resultar em alto prejuízo de ativos tangíveis ou recursos; (2) pode violar, prejudicar ou impedir a missão de uma organização, sua reputação, ou interesse; (3) pode resultar em ferimentos.
Baixo	(1) pode resultar na perda de alguns ativos tangíveis ou recursos; (2) pode afetar perceptivelmente a missão de uma organização, sua reputação ou interesse.

Fonte: Stoneburner, 2002

Na **definição dos riscos,** determina-se o nível de suscetibilidade ao risco que cada vulnerabilidade representa, considerando a sua probabilidade de ser explorada, o impacto que pode causar e os controles que poderiam reduzir ou eliminar o risco.

Para mensurar os riscos, deve ser feita uma escala de riscos (tabela 4) e uma matriz de nível de riscos (tabela 3).

A determinação do risco é resultado da multiplicação dos valores atribuídos pela probabilidade de ameaça e impacto da ameaça. A tabela 3 mostra como as classificações globais de risco podem ser determinadas com base na entrada das probabilidades de ameaça e categorias de impacto de ameaças. Esta é uma matriz de 3 x 3 de probabilidade de ameaça (alta, média e baixa) e impacto da ameaça (alto, médio e baixo). Dependendo dos requisitos da empresa, podem ser usadas matrizes 4 x 4 ou 5 x 5, incluindo as probabilidades de ameaça muito baixa / muito alta, assim como o impacto muito alto / muito baixo.

A determinação dos níveis de risco ou avaliações pode ser subjetiva. Por exemplo: a probabilidade atribuída para cada nível de probabilidade de ameaça é de 1,0 para alta, de 0,5 para média, 0,1 para baixa.

O valor atribuído para cada nível de impacto é de 100 para alta, 50 para médio e 10 para baixo.

Tabela 3: Matriz de nível de risco

Probabilidade de ameaça	**Impacto**		
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

Fonte: Stoneburner, 2002

A tabela 4 descreve os níveis de risco mostrados na matriz (tabela 3). Esta escala de risco, com suas classificações de alta, média e baixa, representa o grau ou nível de risco a que um sistema de TI, instalação ou procedimento pode ser exposto se a vulnerabilidade em questão for exercida.

As **recomendações de controles** são listas relacionando os riscos identificados com os controles para eliminá-los ou reduzi-los a níveis aceitáveis.

Por fim, na etapa de **documentação dos resultados**, todos os resultados obtidos até este ponto deverão ser documentados, pois apoiarão nas decisões gerenciais, elaboração de políticas, procedimentos e mudanças operacionais e gerenciais dos sistemas.

Este relatório irá demonstrar os riscos ao negócio, justificando investimentos e reduzindo possíveis perdas ou danos. Serão demonstradas as ameaças e vulnerabilidades relacionadas aos riscos encontrados, fornecendo recomendações

dos controles que deverão ser implantados.

Tabela 4: Escala de riscos e ações necessárias

	Descrição do risco e ações necessárias
Alto	Se uma observação é avaliada como um risco elevado, existe uma forte necessidade de medidas corretivas. Um sistema existente pode continuar a operar, mas um plano de ação corretiva deve ser colocado em prática o mais rápido possível.
Médio	Se uma observação é classificada como de médio risco, ações corretivas são necessárias e um plano deve ser desenvolvido para incorporar essas ações dentro de um período razoável de tempo.
Baixo	Se uma observação é descrita como de baixo risco, o responsável pela decisão deve determinar se as ações corretivas são ainda necessárias ou se decidirá aceitar o risco.

Fonte: Stoneburner, 2002

O segundo processo desta metodologia de gestão de riscos é chamado mitigação ou atenuação de riscos, que envolve a priorização, avaliação e implementação dos controles para redução dos níveis de risco. Como a eliminação por completo dos riscos é quase impossível, deve-se implementar os controles para reduzir os riscos a um nível aceitável, cujos impactos sejam os mínimos possíveis para a organização.

A mitigação dos riscos pode ser obtida através da:

(a) **Aceitação dos riscos:** Aceitar o risco potencial e continuar operando o sistema de TI ou implementar controles para reduzir o risco a um nível aceitável;

(b) **Prevenção de riscos:** Evitar o risco através da eliminação da causa de risco e ou sua consequência (por exemplo, abrir mão de certas funções do sistema ou desativar o sistema quando os riscos são identificados);

(c) **Limitação dos riscos:** Limitar o risco através da implementação de

controles que minimizem o impacto negativo que uma ameaça está exercendo sobre uma vulnerabilidade;

(d) **Planejamento de riscos:** Gerenciar o risco através do desenvolvimento de um plano de mitigação de risco que prioriza, implementa e mantém controles;

(e) **Pesquisa e reconhecimento:** Diminuir o risco de perda do reconhecimento da vulnerabilidade ou falha e pesquisar controles para corrigir a vulnerabilidade;

(f) **Transferência de risco:** Transferir o risco usando outras opções para compensar a perda, como a compra de seguros.

Sabendo o potencial dos riscos e os controles recomendados, deve-se seguir uma estratégia que fornece ações a serem seguidas para a mitigação dos riscos (figura 5):

(a) Quando a vulnerabilidade (ou fraqueza, falha) existe: implementar técnicas de garantia para reduzir a probabilidade de uma vulnerabilidade que está sendo exercida.

(b) Quando uma vulnerabilidade pode ser exercida: aplicar as preservações em camadas, projetos de arquitetura e controles administrativos para minimizar o risco ou evitar esta ocorrência.

(c) Quando o custo do atacante é menor que o ganho potencial: aplicar as preservações para diminuir a motivação de um invasor, aumentando o custo do atacante (por exemplo, utilização de sistema de controles, como limitar o que um usuário do sistema pode acessar ou não, pode reduzir significativamente o ganho de um atacante).

(d) Quando a perda é muito grande: aplicar os princípios de design, desenhos arquitetônicos e proteções técnicas e não técnicas para limitar a extensão do ataque, reduzindo o potencial de perda.

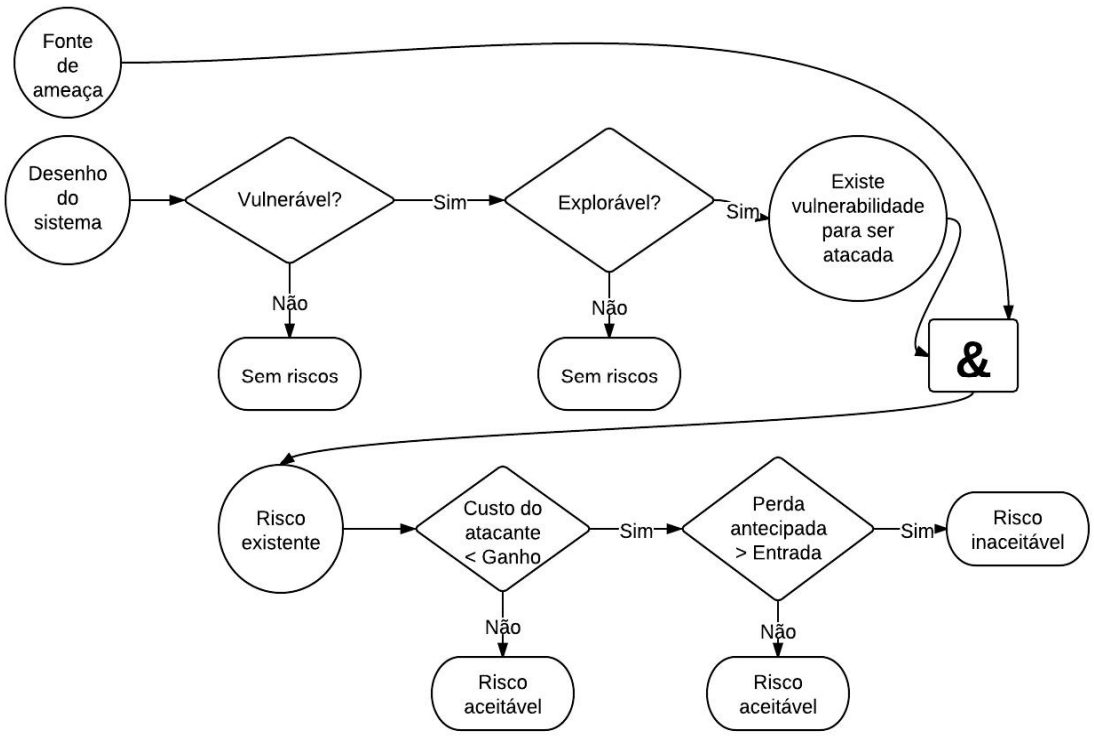


Figura 5: Pontos de ação da mitigação de riscos (STONEBURNER, 2002)

3.3 OCTAVE

A OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation Methodology*) é uma metodologia de análise de risco adaptável que pode ser usada em organizações públicas ou privadas, que possuam mais de duzentos empregados. A OCTAVE possui diversas ferramentas, técnicas e métodos, que permitem que se executem as atividades de (ALBERTS, 2001):

(a) identificar os riscos de segurança das informações da organização;

(b) analisar os riscos e determinar suas prioridades;

(c) planejar as melhorias das estratégias de proteção e controles dos riscos dos ativos mais críticos.

A OCTAVE supõe que as pessoas da organização devem apontar qual é o caminho a ser seguido para a definição de uma estratégia de segurança da informação. Diferentemente de outras metodologias de análise de riscos, a OCTAVE não foca nos riscos tecnológicos e nos problemas táticos, mas nos riscos organizacionais, nas boas práticas e nas estratégias adotadas pela organização. Por ser uma metodologia altamente flexível e evolutiva, pode se adaptar a qualquer organização.

É uma metodologia qualitativa de análise de risco desenvolvida para identificar:

(a) Ativos críticos de informação;

(b) Ameaças que afetam os ativos críticos;

(c) Vulnerabilidades associadas com tais ativos;

(d) Níveis atuais de risco referentes aos ativos críticos.

A metodologia OCTAVE é bastante detalhada e compreende todos os níveis hierárquicos para levantamento das informações pertinentes ao processo de Gerenciamento de Risco de TI. Também prevê uma profunda análise para identificação dos riscos, superior à da NIST 800-30, explicando em detalhes os métodos a serem aplicados para identificar e analisar os ativos de informação, as ameaças, os riscos e formular planos e estratégias para mitigar, transferir ou gerenciar o risco.

Todo o processo de levantamento de informações é realizado por *workshops* que devem ser conduzidos com os profissionais da organização, abrangendo desde a alta administração até a área técnica. A metodologia fornece roteiros detalhados para a condução dos *workshops*, incluindo os questionamentos a serem feitos ao público, conceitos a serem explicados e exemplos de resultados a serem esperados para cada atividade.

Antes do início da avaliação, algumas atividades preliminares devem ser realizadas, além de oito processos relacionados com a análise de riscos, que são divididos em três fases:

Na fase de inicialização a equipe responsável pelo processo executa as atividades preliminares, compostas por: (1) obter o comprometimento da alta

administração, que atuará como responsável durante a implantação do OCTAVE; (2) selecionar os profissionais das áreas de negócio e TI com os conhecimentos necessários para atuarem na equipe de análise, que irá liderar e executar as atividades propostas pela OCTAVE; e (3) treinar a equipe de análise e demais participantes do processo.

As atividades preliminares listadas na OCTAVE são apenas um dos cenários possíveis para iniciar a condução do processo, sendo que outras formas poderão ser escolhidas dependendo da experiência das pessoas envolvidas. Mas existe uma atividade preliminar considerada como imprescindível, que é a obtenção do apoio da alta administração (presidência, diretores, comitê executivo ou demais cargos que tenham autonomia para garantir os recursos necessários ao processo). Para a metodologia, é essencial que a alta administração tenha consciência de como ocorre o processo de avaliação, quais resultados serão obtidos e qual o valor agregado para o negócio, qual a demanda de tempo que essa atividade irá exigir de seus recursos e como será a continuidade do processo, quando se tenha todos os riscos mapeados. Somente com o patrocínio deste nível hierárquico a empresa poderá utilizar recursos financeiros e humanos e dará a importância necessária para os processos de Gerenciamento de Risco de TI.

A OCTAVE é dividida em três fases (figura 6): (1) Construir perfis de ameaças para os ativos; (2) Identificar as vulnerabilidades na infraestrutura e (3) Desenvolver planos estratégicos e de segurança.

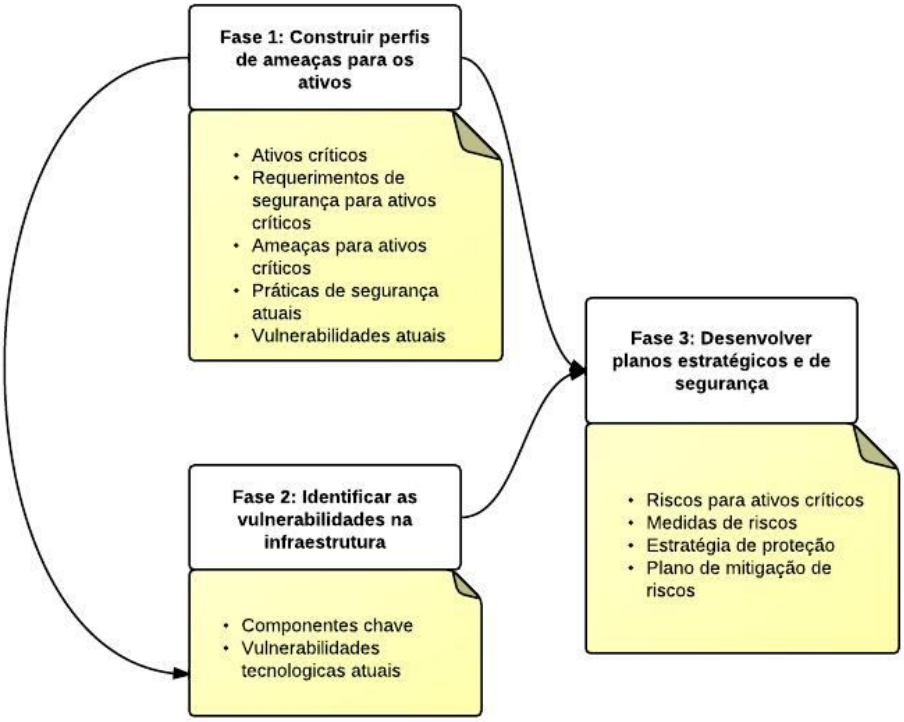


Figura 6: Fases da metodologia OCTAVE (ALBERTS, 2001)

3.3.1 Construir perfis de ameaças para os ativos

Na primeira fase a equipe de análise, com a alta administração e a gerência operacional, através de *workshops*, identifica os ativos críticos de informação e documenta as ameaças que estes ativos estão sujeitos, os requerimentos de segurança, as estratégias atuais de proteção, e as vulnerabilidades relacionadas ao ativo crítico. A OCTAVE divide os ativos de informação hardware, software, dados e informações como “Sistemas” enquanto o ativo “Pessoas” permanece isolado.

Juntamente com a alta administração, esta equipe irá definir as áreas

operacionais que farão parte do escopo de avaliação de riscos. Após esta definição, os gerentes destas áreas podem auxiliar para um detalhamento mais técnico.

Os quatro processos que fazem parte desta fase são:

(a) **Processo 1:** Identificar os gestores seniores que participarão da análise de riscos identificando os ativos mais importantes, ameaças, requerimentos de segurança e vulnerabilidades organizacionais;

(b) **Processo 2:** Identificar o gestor da área operacional que também auxiliará na identificação dos ativos importantes, das ameaças, dos requerimentos de segurança e das vulnerabilidades organizacionais;

(c) **Processo 3:** Identificar a equipe (*Staff*) (a equipe geral e a equipe de TI) para participar das atividades de seleção de ativos, auxiliando a identificação dos recursos críticos para a organização;

(d) **Processo 4:** A equipe de análise irá listar os ativos críticos juntamente com as melhorias dos requerimentos de segurança relacionados a estes ativos e suas ameaças, criando o perfil de ameaças para os ativos da organização.

Para construir os perfis de ameaça, seis atividades são realizadas:

(a) Identificar ativos: listar os ativos de toda organização, identificando quais são mais importantes para a missão e o negócio da empresa;

(b) Identificar práticas de segurança atuais: listar as práticas atuais de segurança para proteger os ativos críticos;

(c) Identificar vulnerabilidades organizacionais atuais: listar as vulnerabilidades existentes nas diversas áreas da organização, tantos as técnicas quanto às de negócios;

(d) Identificar ativos críticos: listar os ativos mais importantes para a organização, seja por sua relevância em relação a infraestrutura ou por obrigações legais;

(e) Descrever requerimentos de segurança para os ativos críticos: cada ativo crítico deverá estar relacionado aos seus requerimentos de segurança;

(f) Criar perfis de ameaça para os ativos críticos: identificar as

ameaças que podem afetar cada ativo;

3.3.2 Identificar as vulnerabilidades na infraestrutura

Na segunda fase a equipe de análise, juntamente com a TI, identifica os sistemas relacionados aos ativos críticos, verificando as vulnerabilidades existentes. Os sistemas são chamados “sistemas de interesse” e os elementos que desempenham um papel importante para que o ativo crítico possa realizar adequadamente sua função são chamados de “componentes de infraestrutura”. Os componentes de infraestrutura dos sistemas de interesse dividem-se em: servidores, componentes de rede, estações de trabalho, notebooks, dispositivos de armazenamento, componentes *wireless* e outros dispositivos.

Os componentes de infraestrutura dos sistemas de interesse são o foco da análise de vulnerabilidades e que, para validar se realmente são recursos pertinentes ao sistema de interesse, devem atender as questões: Os componentes são utilizados quando um usuário legítimo tenta acessar o ativo crítico? Um ator, responsável pela ação de uma ameaça, utiliza tais componentes para obter acesso ao ativo crítico?

Os processos da segunda fase são:

(a) **Processo 5:** A equipe de análise deve identificar as informações chaves para os sistemas para cada um dos ativos críticos, selecionando os que farão parte do escopo da análise;

(b) **Processo 6:** A equipe de análise deve examinar os sistemas chaves para cada fraqueza tecnológica. Os resultados serão examinados de acordo com a relevância dos ativos críticos.

A segunda fase é composta por três atividades:

(a) Selecionar os componentes de infraestrutura para avaliação: levantar os componentes específicos da infraestrutura com relação a suas vulnerabilidades considerando o impacto para organização;

(b) Executar ferramentas de análise de vulnerabilidades: identificar e

listar as vulnerabilidades tecnológicas de cada componente da infraestrutura selecionada. Podem ser utilizadas ferramentas de análise de vulnerabilidades para cada componente;

(c) Revisar as vulnerabilidades e resumir os resultados: listar as vulnerabilidades tecnológicas de cada ativo crítico e melhorar os perfis das ameaças da análise feita na atividade anterior. Revisar os resultados para cada ativo crítico garantindo que todos os envolvidos entendam os resultados.

Com a análise de vulnerabilidades concluída, uma classificação da severidade de cada vulnerabilidade deverá ser gerada para auxiliar na definição de um plano de ação para tratamento dos problemas detectados. A OCTAVE cita os critérios para a definição de um plano de ação para tratamento dos problemas, mas a equipe pode determinar o que será empregado.

3.3.3 Desenvolver planos estratégicos e de segurança

Na terceira fase a equipe de análise completa o processo de análise de risco com as informações obtidas nas fases anteriores. O critério de avaliação de risco é definido para determinar o que será considerado um alto, médio ou baixo impacto para a organização e aplica este critério para cada risco encontrado.

Com as informações da primeira fase serão então comparadas com as práticas de segurança da organização e com o catálogo de práticas, que é o documento contendo as boas práticas de segurança da metodologia OCTAVE. Com o resultado da análise de risco, a equipe elabora um projeto da estratégia de proteção, preservando as boas práticas existentes na organização, mas também contemplando as contramedidas necessárias para as vulnerabilidades organizacionais identificadas durante a execução da OCTAVE.

Após, é desenvolvido um plano de mitigação de risco para os ativos críticos, listando as ações de curto prazo a serem executadas, identificadas como necessárias durante o desenvolvimento das estratégias de longo prazo. A fase é

concluída com a equipe de análise revisando junto à alta administração os principais riscos mapeados durante a fase de levantamento, e ajustando as estratégias de proteção da organização, o plano de mitigação de riscos e lista de ações.

Os processos da terceira fase são:

(a) **Processo 7:** A equipe de análise deve identificar o impacto das ameaças nos ativos críticos, desenvolver um critério para avaliação destes riscos, o que produzirá um perfil de risco para cada ativo crítico;

(b) **Processo 8:** A equipe de analise deve elaborar uma estratégia de proteção e um plano de mitigação de riscos para a organização. As análises realizadas e os relatórios produzidos durante as atividades são a base para a elaboração destes documentos. Por fim, os gestores seniores devem fazer a revisão final do documento, garantindo que todas as informações relevantes estejam presentes.

A terceira fase é composta por sete atividades:

(a) Identificar os riscos para os ativos críticos: descrever os impactos potenciais para a organização em relação as ameaças para cada ativo crítico;

(b) Criar critérios de avaliação de risco: definir o critério de avaliação do impacto estabelecendo uma medida qualitativa aos impactos, determinando o que significa o impacto alto, médio e baixo para a organização. Para os critérios de avaliação podem ser criadas categorias como: Reputação, confiança do cliente; segurança; multas, atribuições legais; impacto financeiro e produtividade;

(c) Avaliar os riscos para os ativos críticos: estabelecer os valores de impacto (alto, médio e baixo) para cada ameaça aos ativos;

(d) Criar um plano de proteção estratégica: revisar as práticas de segurança mapeadas, as vulnerabilidades identificadas e os perfis de risco para cada ativo crítico e, baseado nestas práticas, desenvolver um plano estratégico de segurança;

(e) Criar planos de mitigação dos riscos: o plano de mitigação deve conter ações para prevenir a exploração de ameaças aos ativos críticos;

(f) Revisar o plano de proteção estratégica e de mitigação dos riscos com os gestores: os gestores seniores devem revisar o plano estratégico de segurança e os planos de mitigação de riscos com a equipe de análise, fazendo alterações e melhorias, se necessário;

(g) Identificar os próximos passos: os gerentes seniores devem determinar o que a organização deve fazer para implementar o plano de estratégico de segurança e os planos de mitigação de riscos, assegurando que isto irá melhorar os níveis de segurança.

A estrutura da OCTAVE é composta por um conjunto de princípios, atributos e saídas.

Os princípios são os conceitos fundamentais que definem a forma como a análise e a avaliação são conduzidas. Estes princípios são agrupados nas seguintes áreas:

(a) Princípios de Avaliação de Riscos na Segurança da Informação: aspectos chaves que fundamentam a gestão de riscos relacionados a informação.

    (a) Auto direção: quando as pessoas controlam e gerenciam o risco da informação para sua organização;

    (b) Medidas flexíveis: o processo de gestão de riscos deve ser flexível para adaptar-se rapidamente às mudanças e os avanços tecnológicos;

    (c) Processo definido: necessidade de um processo de gestão de riscos baseado em procedimentos padronizados e definidos;

    (d) Bases para um processo contínuo: executar estratégias e planos de segurança para melhorar seus níveis de segurança em determinado tempo.

(b) Princípios de Gestão de Riscos: princípios básicos comuns a uma gestão de riscos eficaz para a organização.

    (a) Visão estratégica: ter uma visão além dos problemas comuns, focando nos problemas mais críticos aos ativos mais importantes da organização;

(b) Foco nos pontos mais críticos;

(c) Gestão integrada: as políticas e estratégias de segurança devem ser consistentes com as políticas e as estratégias organizacionais.

(c) Princípios organizacionais e culturais: cultura que é essencial a um processo de gestão de riscos bem sucedida.

(a) Comunicação aberta: não haverá sucesso na gestão de riscos sem um comunicação aberta considerando os problemas relacionados a segurança;

(b) Perspectiva global: os membros da organização devem ter uma visão comum do que é mais importante para a organização;

(c) Trabalho em equipe: apenas com um trabalho em equipe pode se compreender melhor os problemas de segurança da informação da organização.

Os atributos são características especificas do processo de gestão de riscos, e são relacionados aos princípios da OCTAVE (tabela 5). São os atributos que definem o que é necessário para fazer a avaliação dos riscos:

(a) Equipe responsável pela análise: equipe multidisciplinar incluindo a área técnica e a de gestão. A equipe será responsável por gerenciar as informações da análise de riscos e tomar as decisões necessárias;

(b) Aumento das habilidades da equipe responsável pela análise: possibilidade de incluir novos recursos a equipe de análise quando necessite conhecimentos adicionais;

(c) Catálogo de práticas: definir um catálogo de boas práticas que estejam de acordo com as leis, regulamento e padrões;

(d) Perfil genérico da ameaça: avaliar as ameaças aos ativos através de um perfil genérico da ameaça, previamente definido;

(e) Catálogo de Vulnerabilidades: manter um catálogo das vulnerabilidades conhecidas para os componentes computacionais chaves;

(f) Definição das atividades de avaliação: os procedimentos para executar cada atividade da gestão de riscos devem ser definidos e

documentados;

(g) Avaliação dos resultados documentados;

(h) Escopo: o escopo para o processo de gestão de riscos deve ser claramente definido, mas sem ser demasiadamente grande, para não dificultar a análise de todas as informações.

(i) Etapas posteriores: a equipe de análise deve identificar as etapas seguintes requeridas para executar estratégias e planos de segurança;

(j) Foco no risco: o processo de gestão de riscos deve focar em avaliar os riscos da informação relacionando-os com as ameaças, ativos críticos e vulnerabilidades;

(k) Atividades focadas: focar as atividades mais críticas da organização;

(l) Problemas organizacionais e tecnológicos: avaliar o nível estratégico e o tecnológico;

(m) Participação do negócio e da tecnologia da informação: o processo deve incluir participantes da área de negócio e de TI;

(n) Participação da gerência sênior: durante o processo os gestores seniores devem ter papéis definidos;

(o) Participação colaborativa: os participantes de cada atividade devem interagir e colaborar.

O texto acima citado sobre a OCTAVE foi baseado no trabalho de Azevedo e Nazareth (2009), que se basearam em Alberts (2001).

Tabela 5: Atributos dos Princípios

Princípio	Atributo
Auto direção	Equipe de análise
	Aumentando as habilidades da equipe de análise
Medidas flexíveis	Catálogo de práticas
	Perfil genérico da ameaça
	Catálogo de vulnerabilidades
Processo definido	Definição das atividades de avaliação
	Avaliação dos resultados documentados
	Escopo
Bases para um processo contínuo	Etapas posteriores
	Catálogo de práticas
Visão estratégica	Foco no risco
Foco nos pontos mais críticos	Escopo
	Atividades focadas
Gestão integrada	Problemas organizacionais e tecnológicos
	Participação do negócio e da TI
	Participação da gerência sênior
Comunicação aberta	Participação colaborativa
Perspectiva global	Problemas organizacionais e tecnológicos
	Participação do negócio e da TI
Trabalho em equipe	Equipe de análise
	Aumentando as habilidades da equipe de análise
	Participação do negócio e da TI
	Participação colaborativa

Fonte: Alberts, 2001

3.4 COMPARAÇÃO ENTRE NBR ISO/IEC 27005, NIST SP 800-30 E OCTAVE

Analisando as informações supracitadas a respeito das três metodologias de gestão de riscos, conclui-se que as mesmas possuem diversas atividades semelhantes, como a identificação de ativos críticos, identificação de vulnerabilidades e ameaças e estratégias de mitigação dos riscos.

Oliveira (2006) realizou uma comparação entre as metodologias NIST SP 800-30 e OCTAVE, onde destacou as diferenças dos principais aspectos da gestão de riscos. Este trabalho se baseou na comparação realizada por Oliveira (2006) utilizando alguns dos mesmos critérios abordados sobre a NIST e a OCTAVE, mas

está acrescentando a análise da NBR ISO/IEC 27005 como complemento ao trabalho realizado pelo autor.

Para a comparação das metodologias, os aspectos utilizados serão:

(a) Escopo da metodologia;
(b) Pré-requisitos do processo de Gestão de Riscos;
(c) Identificação dos ativos críticos;
(d) Mapeamento de vulnerabilidades;
(e) Identificação de ameaças;
(f) Análise dos controles atuais;
(g) Análise do impacto no ambiente;
(h) Determinação do risco;
(i) Controles para mitigação dos riscos;
(j) Continuidade do processo de Gestão de Riscos;
(k) Tratamento do risco residual;

3.4.1 Escopo da metodologia

A NIST SP 800-30 abrange todo o ciclo de Gestão de Riscos de TI, a identificação dos riscos, a mitigação e o monitoramento de forma detalhada. A NBR ISO/IEC 27005 também se baseia no ciclo completo.

A OCTAVE além de explicar detalhadamente todas as atividades do processo de Gestão de Riscos de TI, inclui ainda roteiros e questionamentos para a execução dos *workshops*, utilizados durante o processo de levantamento de informações.

3.4.2 Pré-requisitos do processo de Gestão de Riscos

A NIST SP 800-30 não menciona os requisitos necessários para iniciar o processo de Gestão de Riscos de TI. A NBR ISO/IEC 27005 também não apresenta muitos detalhes sobre atividades preliminares, mas para a fase inicial de Definição

do contexto, é necessário levantar todas as informações relevantes para a organização e que se determine o propósito da gestão de riscos antes do seu iniciá-la.

A metodologia OCTAVE é a que mais aprofunda este aspecto, embora não seja obrigatório que se inicie o processo por estas atividades, dependendo da experiência dos envolvidos. Mas a atividade preliminar que é considerada imprescindível é a obtenção do apoio da alta administração.

As atividades preliminares da OCTAVE são:

(a) Obtenção do patrocínio da alta administração;
(b) Seleção dos membros da equipe de análise;
(c) Definição dos aspectos logísticos como reserva de sala de reunião, projetores, etc.;
(d) Coleta de documentação existente referente ao escopo da análise (inventário de hardware e software, políticas e procedimentos de segurança existentes, relatórios de auditoria);
(e) Treinamento da equipe de análise;
(f) Seleção dos participantes das áreas de negócio e TI que contribuirão;

3.4.3 Identificação dos ativos críticos

Durante a etapa de Estimativa de Riscos da metodologia NBR ISO/IEC 27005 é definida a criticidade dos ativos, mas sem informar maiores detalhes sobre como determinar o risco de criticidade dos ativos. A NIST SP 800-30 também não detalha o que são os ativos críticos.

A metodologia que apresenta a melhor identificação dos ativos críticos é a OCTAVE, que identifica quais são os ativos mais críticos para o negócio da empresa. Isto é determinado através de *workshops* com a alta administração, gerência operacional e a área de TI e negócio.

3.4.4 Mapeamento de vulnerabilidades

A NIST SP 800-30 propõe que se faça uma lista com as vulnerabilidades relacionando-as aos às fontes de ameaça que podem explorá-la. Para identificar as vulnerabilidades podem ser usadas ferramentas automatizadas para diagnóstico do sistema e a elaboração de roteiros de testes específicos para avaliar a eficiência dos controles de segurança.

A OCTAVE propõe que a análise das vulnerabilidades seja focada nos componentes de infraestrutura dos sistemas relacionados aos ativos críticos. Para a análise de vulnerabilidades podem ter a colaboração de consultores externos ou pela própria equipe, com o auxilio de ferramentas automatizadas.

A NBR ISO/IEC 27005 propõe que para a identificação de vulnerabilidades sejam utilizados métodos como o uso de ferramentas automatizadas, avaliação e testes da segurança, testes de invasão e análise crítica de código. A metodologia também traz uma lista de vulnerabilidades comuns relacionando-as à exemplos de ameaças.

3.4.5 Identificação de ameaças

A NIST SP 800-30 propõe que sejam mapeadas todas as fontes de ameaças aos sistemas de TI, classificadas em ameaças naturais, humanas ou ambientais. O mapeamento das ameaças deve contemplar a fonte de ameaça, sua motivação e a ação da ameaça. Mas, apesar de trazer alguns exemplos de fontes de ameaça, não propõe uma lista para ser utilizada como base.

Já a OCTAVE classifica as ameaças pela sua fonte de origem, como atores humanos utilizando acesso via rede ou acesso físico, problemas nos sistemas e outros problemas como desastres naturais. A OCTAVE tem como vantagem, na identificação das ameaças, também analisar dados levantados de diferentes áreas da organização.

A OCTAVE também apresenta uma tabela relacionando os requisitos de segurança dos ativos com os resultados esperados pela ação de uma ameaça.

Na metodologia NBR ISO/IEC 27005 utiliza as informações coletadas a partir da análise crítica de incidentes, dos responsáveis pelos ativos, de usuários e outras fontes para identificar as ameaças e as suas fontes. Uma tabela com exemplos de fontes de ameaças semelhante a da NIST SP 800-30 é apresentada, além de outra classificando as ameaças por tipo e identificando suas origens.

3.4.6 Análise dos controles atuais

Todas as três metodologias abordam a análise dos controles atuais, mas enquanto a NBR ISO/IEC 27005 e a NIST SP 800-30 fazem esta identificação durante a determinação do risco, a OCTAVE apenas aborda este aspecto durante a definição da estratégia de mitigação.

3.4.7 Análise do impacto no ambiente

Na NIST SP 800-30, para se definir o impacto negativo resultante da exploração de uma vulnerabilidade por uma ameaça, é necessário conhecer a finalidade do sistema, a importância do sistema para a organização e a sensibilidade dos dados manipulados pelo mesmo.

Devido a dificuldade de se mensurar em termos quantitativos impactos como a perda da confiabilidade ou perda de credibilidade, a NIST adota a análise qualitativa para tratamento do impacto, classificando-o em alto, médio e baixo. Contém uma tabela com definições para cada tipo de magnitude.

Estes critérios qualitativos para definição do impacto causado pela exploração de uma vulnerabilidade por uma ameaça também são adotados pela metodologia OCTAVE. Assim como a NIST SP 800-30, também são utilizadas as magnitudes alta, média e baixa, mas na OCTAVE a organização deverá definir o que será considerado de alta, média ou baixa magnitude.

Cada ativo crítico deve ser relacionado com o impacto da exploração de suas ameaças

Neste aspecto a metodologia NBR ISO/IEC 27005 diferencia das outras duas, pois o valor do impacto pode ser expresso de forma qualitativa ou quantitativa, embora um método designando valores monetários pode fornecer mais informações úteis para a tomada de decisões. No entanto, para os ativos que possuem valores de difícil mensuração, o ideal é que se utilize a forma qualitativa. Os valores do impacto estão diretamente relacionados com os valores dos ativos.

3.4.8 Determinação do risco

Para a metodologia NIST SP 800-30, para determinar o risco deve ser levado em consideração a probabilidade de uma fonte de ameaça explorar as vulnerabilidades existentes, a magnitude do impacto que a ameaça pode causar e a eficácia dos controles empregados. A metodologia propõe uma matriz considerando o impacto e a probabilidade, atribuindo valores de alto, médio e baixo. A determinação da magnitude fica a critério de cada organização. Também é apresentada uma tabela com recomendações para cada nível de risco identificado, neste caso alto, médio e baixo.

Já para a metodologia OCTAVE, o nível do impacto causado por uma determinada ameaça irá definir o nível de risco que a empresa está sujeita. A OCTAVE considera a probabilidade de uma ameaça trazer impacto como uma métrica complexa de ser calculada e imprecisa. Neste aspecto a NIST SP 800-30 é mais completa que a OCTAVE.

A metodologia NBR ISO/IEC 27005 determina os riscos baseada nas consequências e na probabilidade estimadas, também pode considerar o custo-benefício, as preocupações das partes interessadas e outras variáveis. O risco estimado é uma combinação entre a probabilidade de um cenário de incidente e suas consequências e seus valores podem ser de natureza quantitativa ou qualitativa, dependendo da organização.

3.4.9 Controles para mitigação dos riscos

A NIST SP 800-30 é a metodologia que aborda a mitigação do risco de forma bastante detalhada. Ela apresenta como opções para a mitigação do risco: aceitar o risco, evitar o risco, limitar o risco, planejar o risco, pesquisa e reconhecimento e transferência do risco.

A OCTAVE propõe a elaboração de três tipos de plano de ação para a mitigação do risco: a estratégia de proteção, o plano de mitigação, e a lista de ação. A estratégia de proteção define as estratégias que a organização utiliza para habilitar, iniciar, implementar e manter a segurança interna do ambiente e são ações de longo prazo. Os planos de mitigação visam reduzir os riscos para os ativos críticos e são ações de média duração. As listas de ações são ações de rápida implementação que não requerem maior detalhamento sobre a forma de implementação.

A metodologia NBR ISO/IEC 27005 apresenta quatro formas para tratamento dos riscos: redução do risco, retenção do risco, ação de evitar o risco e transferência do risco.

3.4.10 Continuidade do processo de Gestão de Riscos

As três metodologias propõem que o processo de gestão de riscos deve ocorrer de maneira contínua, pois como a área de tecnologia está em constante mudança, novos riscos podem surgir e é imprescindível que o processo de gestão de riscos possa acompanhar estas mudanças.

3.4.11 Tratamento do risco residual

A forma da metodologia ABNT ISO/IEC 27005 tratar os riscos residuais é que se estes estão acima do limite aceitável, deverão passar novamente pela etapa de tratamento de riscos. Algo semelhante acontece com a NIST SP 800-30, que

descreve que sempre haverá um risco residual, mas se estes riscos não estão dentro dos limites da organização, deverão ser tratados novamente.

Embora a OCTAVE proponha que todas as ameaças e vulnerabilidades dos ativos críticos sejam tratadas, não prevê um tratamento para os riscos residuais.

3.5 CONSIDERAÇÕES FINAIS

As três metodologias, além de serem baseadas no ciclo completo da gestão de riscos, apresentam alguns aspectos bastante similares, como a identificação dos riscos, ativos, vulnerabilidades e controles existentes, porém cada metodologia com suas peculiaridades. As três formas vêem como necessário ao processo de gestão de riscos, que o mesmo funcione de maneira contínua.

A OCTAVE traz mais detalhes sobre os pré-requisitos para o início da gestão de riscos e a identificação de ativos críticos. Referente ao impacto dos riscos, enquanto a OCTAVE e a NIST SP 800-30 indicam a forma qualitativa para determinar o impacto dos possíveis riscos, a NBR ISO/IEC 27005 permite que a organização escolha entre a abordagem qualitativa e a quantitativa, dependendo do caso.

Em relação ao tratamento dos riscos, a NIST SP 800-30 e a NBR ISO/IEC recomendam que os riscos sejam tratados até que estejam a um nível aceitável, já a OCTAVE propõe que todas as ameaças e vulnerabilidades sejam tratadas, mas sem indicar um tratamento para os riscos residuais. Em relação à determinação dos riscos, a NIST SP 800-30 é a metodologia que explica de forma mais detalhada.

Com base no estudo destas metodologias, foram definidos os critérios para a avaliação dos softwares.

4 SOFTWARES DE GESTÃO DE RISCOS

Antes da seleção dos softwares a serem analisados, foram realizadas pesquisas de diversos softwares que realizam gestão de riscos (tabela 12).

Como a maioria dos softwares de gestão de riscos disponíveis é comercial, apenas poderão ser avaliados aqueles que disponibilizam versões de testes. Entre eles, o Vs Risk, o SecureAware e o Acuity STREAM SU v2 foram os selecionados por possuírem versões disponíveis para avaliação. Além destes, o SOBF Tool, que não é um software comercial, também será avaliado no trabalho.

Tabela 6: Lista de softwares pesquisados

Nome	URL	Tipo
Modulo Risk Manager	http://www.modulo.com.br/software	Comercial
Vs Risk	http://www.vigilantsoftware.co.uk	Comercial
GSTool 4.5	https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/Download/download_node.html	Comercial
SOBF Tool	http://www.somap.org/orico/default.html	*Free*
Ballot 7.1.1	http://www.bpsresolver.com/software/ballot-risk-assessment	Comercial
Pilar	https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=187&lang=em	Comercial
Risk Manager Edition	http://www.countermeasures.com/manager.htm	Comercial
RM Studio	http://www.riskmanagementstudio.com/	Comercial
Cramm	http://www.cramm.com/	Comercial
Acuity STREAM SU v2	http://www.acuityrm.com/	Comercial
Alien Vault OSSIM	http://communities.alienvault.com/community	*Free*
ESIS	http://esis.sourceforge.net/ESIS/Home.html	*Free*
SecureAware	http://www.neupart.com/products/iso-27005-risk-management.aspx	Comercial

Para realizar os testes nas ferramentas é importante utilizar os mesmos

dados, para que a comparação reflita realmente a diferença dos softwares.

Por questões de segurança, os testes não foram realizados utilizando dados reais de uma organização. Optou-se por utilizar um caso fictício desenvolvido na disciplina de Tópicos Especiais – Segurança da Informação (CASAGRANDE et al., 2012), ocorrida no primeiro semestre de 2012. O estudo de caso completo consta no Anexo A.

4.1 VS RISK

O Vs Risk é um software de gestão de riscos desenvolvido pela Vigilant Software. Como este é um software pago, sua avaliação foi realizada em uma versão de testes, com restrições de funcionalidades.

O Vs Risk foi desenvolvido para atender as metodologias ISO 27001 e ISO/IEC 27002, mas também está em conformidade com a ISO/IEC 27005 e NIST SP 800-30. O programa possui interface amigável e sem grande complexidade, facilitando o seu uso.

Durante a instalação do software é solicitado que se informe o tamanho da matriz de riscos e a de probabilidades, podendo ser entre 3 e 7 (figura 8). Estas matrizes não poderão ser alteradas depois. Também é necessário informar o nível de aceitação dos riscos, ou seja, definir até que ponto os riscos serão aceitos para os ativos envolvidos. Este nível poderá ser alterado durante a utilização do software (figura 9), mas afetará todos os ativos utilizados, não permitindo que sejam definidos níveis de aceitação diferentes para cada ativo.

Figura 7: Vs Risk - Definição de impacto e probabilidades

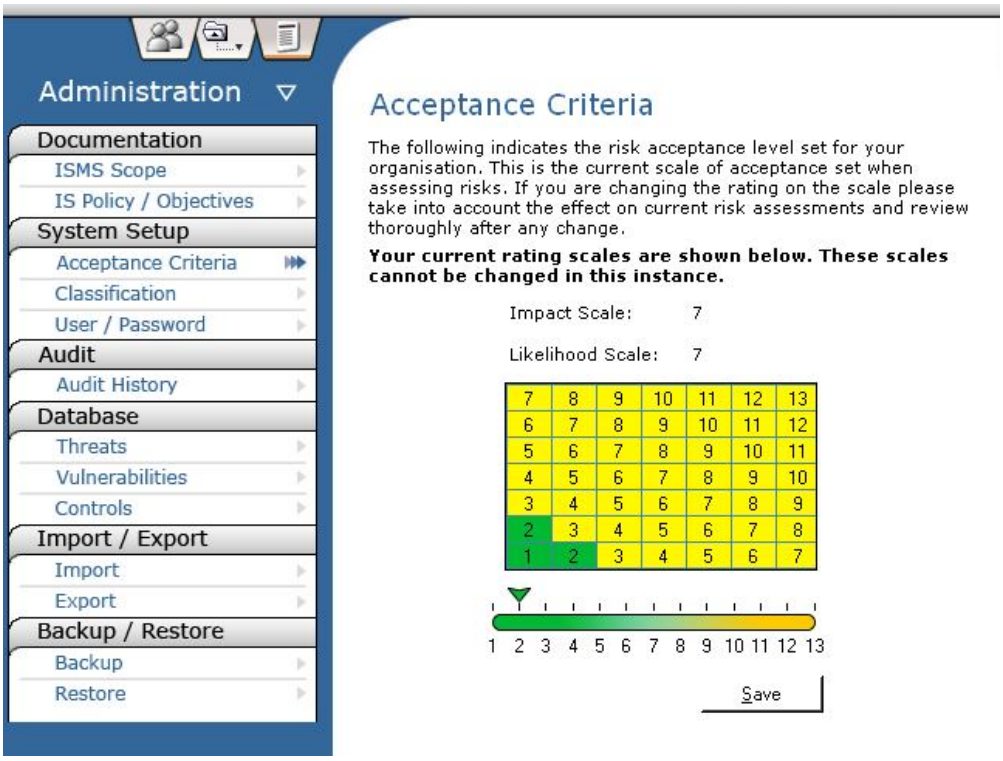


Figura 8: Vs Risk - Definição do nível de risco aceitável

Ao incluir um ativo, além de informações como seu nome e descrição, é necessário informar seu tipo (hardware, software, informação, serviço, pessoa, processo), sua classificação (privada, restrita, confidencial, pública) e também descrever seus requerimentos legais, contratuais e de negócio (figura 10).

O Vs Risk permite que os ativos sejam incluídos e avaliados de acordo com seus requisitos legais, contratuais e de negócio, e, para cada um dos requisitos, podem ser avaliados três atributos: disponibilidade, confidencialidade e integridade. Como ilustrado na figura 11, os ativos estão localizados no quadro à esquerda, enquanto a tabela à direita contém estas informações de cada um dos ativos.

Esta tabela ainda possui as colunas de *Risk Rating*, *Residual Rating* e *Action*. A coluna de *Risk Rating* apresenta o valor do risco calculado automaticamente após serem incluídas as ameaças e vulnerabilidades da ameaça. A coluna *Residual Rating*, apresenta o novo cálculo para o risco após serem associados os controles para conterem as ameaças deste ativo. A coluna *Action* possui as opções de *Edit* e *View*. Através do *Edit* é feita edição desta propriedade do ativo, onde são associadas as ameaças, vulnerabilidades e controles, enquanto o *View* apenas permite a visualização destas informações.

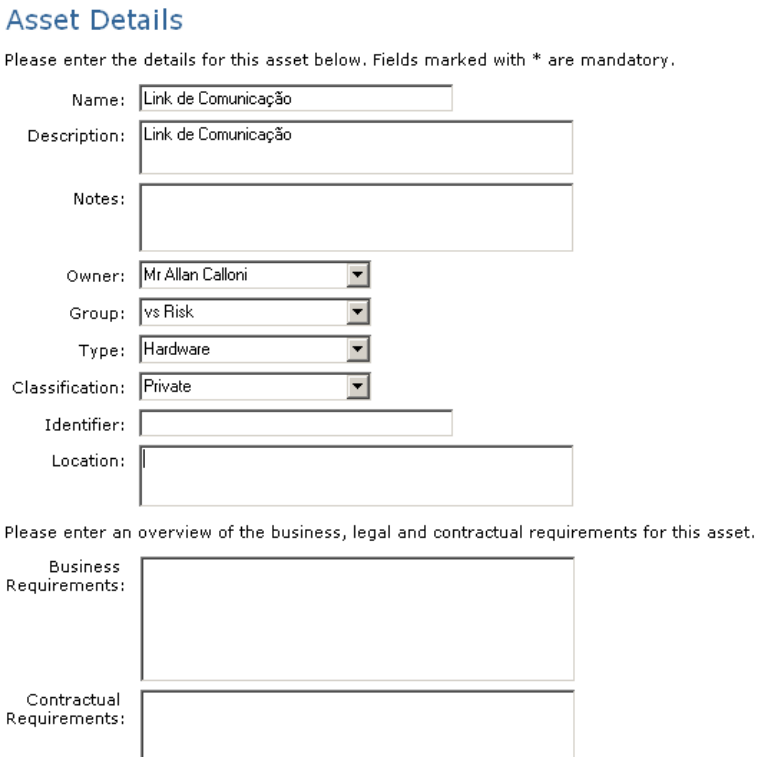


Figura 9: Vs Risk - Inclusão de Ativos

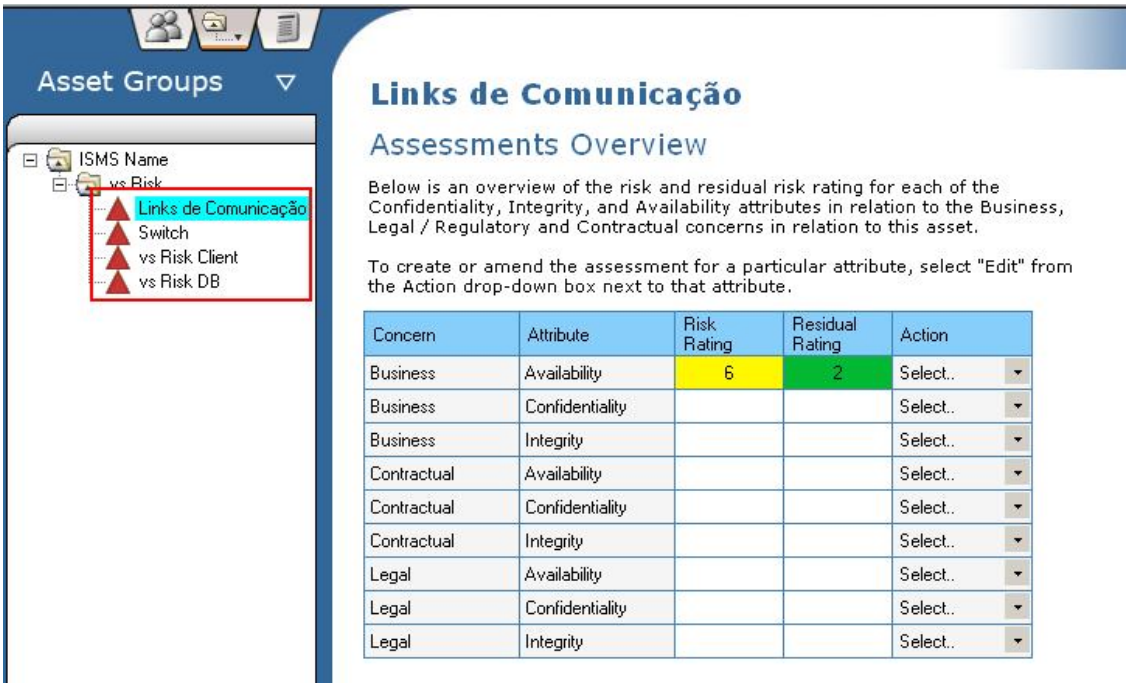


Figura 10: Vs Risk - Avaliação dos Ativos

Para cada um dos atributos de um ativo (disponibilidade, confidencialidade e integridade) é informado, através de uma escala, o valor que representaria a perda dos mesmos, caso uma ameaça se concretizasse, ou seja, o valor do impacto do atributo em questão (figura 12).

Figura 11: Vs Risk - Valor de impacto para o ativo

Podem ser associadas a cada um dos atributos de um ativo, diversas ameaças e dentro destas ameaças são associadas as vulnerabilidades que podem ser exploradas pelas respectivas ameaças, como mostra a figura 13. A seguir, para cada vulnerabilidade é definida a probabilidade de ocorrência da ameaça através de uma escala de 1 a 7 (figura 14).

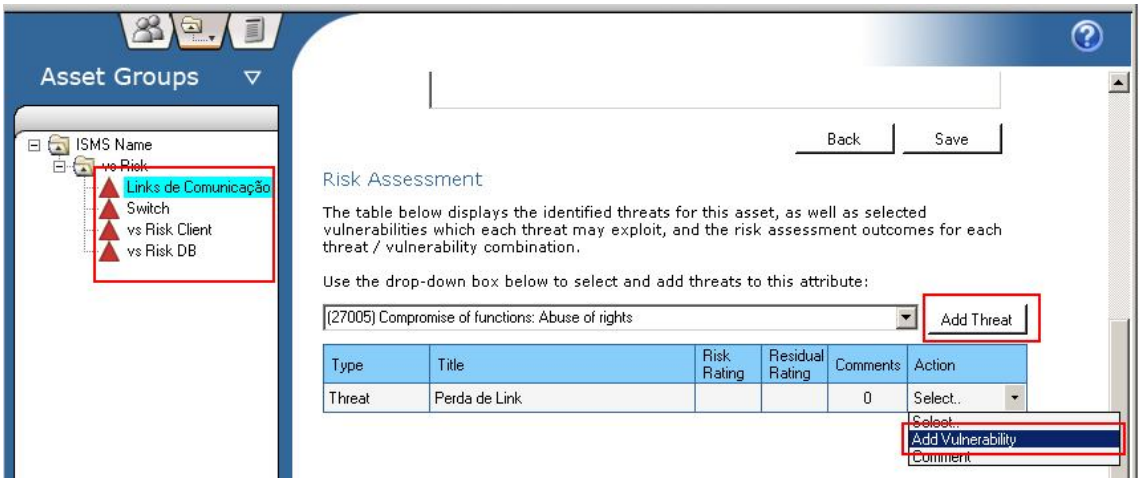


Figura 12: Vs Risk - Inclusão de ameaças e vulnerabilidades aos ativos

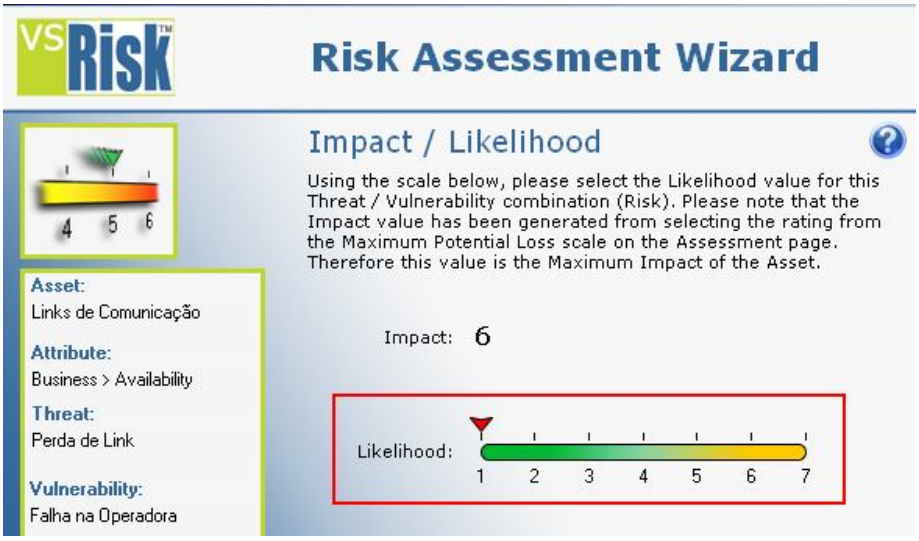


Figura 13: Vs Risk - Definição da probabilidade de ocorrência da ameaça

A partir do valor de impacto do atributo em relação à probabilidade de ocorrência da ameaça, o programa calcula automaticamente o valor deste risco, conforme a figura 15. Este valor para o risco é também mostrado na coluna *Risk Rating* da figura 11.

Figura 14: Vs Risk - Risco calculado antes dos controles

Como soluções às vulnerabilidades e ameaças identificadas, podem ser adicionados controles para garantir a segurança dos ativos, indicando se os mesmos

são controles existentes ou planejados, para serem implantados no futuro (figura 16).

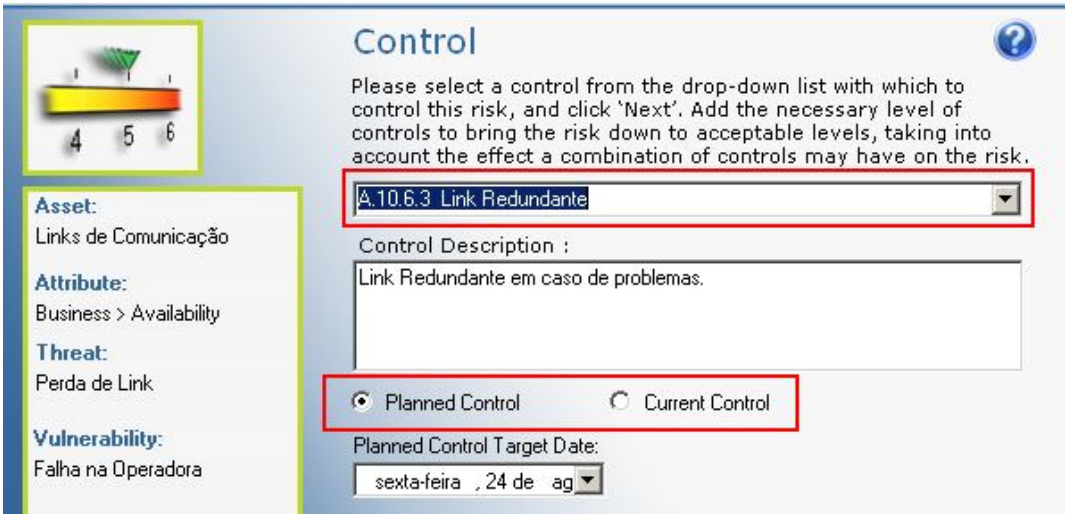


Figura 15: Vs Risk - Inclusão de controles às vulnerabilidades

Após selecionar os controles, devem-se informar os novos valores de impacto e probabilidade do risco considerando o funcionamento dos controles, como no destaque da figura 17, resultando em um novo valor do risco, que é representado na coluna *Residual Rating* (Risco Residual) da figura 11.

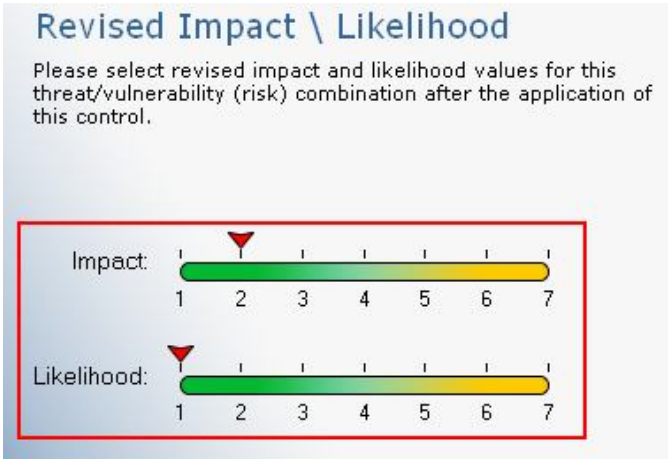
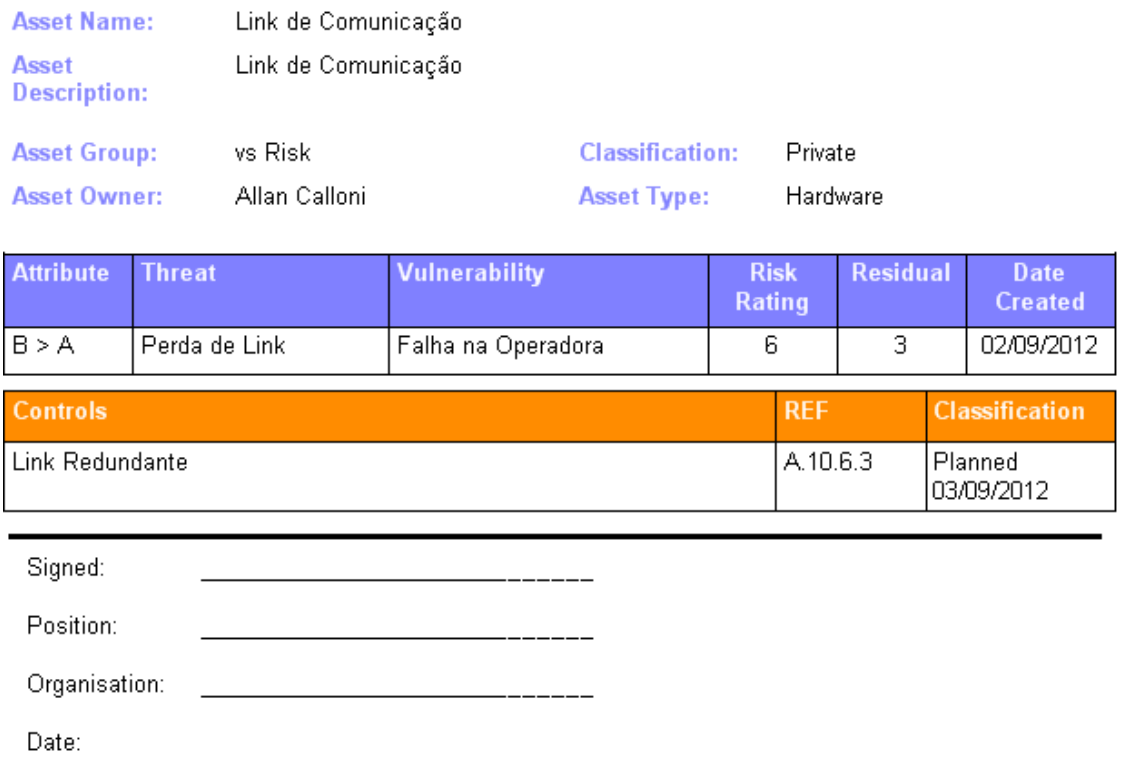


Figura 16: Vs Risk - Revisão do impacto e probabilidade após a inclusão dos controles

O Vs Risk também possui uma base de dados consistente, com milhares de ameaças, vulnerabilidades e controles previamente cadastrados, além de permitir a inclusão de novos.

Outras funcionalidades do Vs Risk são o histórico e os relatórios. No histórico podem ser visualizadas todas as ações, alterações, inclusões, realizadas durante a utilização do programa, com a sua respectiva data.

Já a geração de relatórios, que pode ser por homologação de aplicabilidade, riscos residuais, avaliação de riscos e relatório dos comentários adicionados. Além destes, existe o plano de tratamento de riscos, que consiste na relação de ações e controles necessários para tratar os riscos existentes para cada um dos ativos, conforme a figura 18. Estes relatórios contêm apenas textos, sem gráficos.



Asset Name: Link de Comunicação

Asset Description: Link de Comunicação

Asset Group: vs Risk **Classification:** Private

Asset Owner: Allan Calloni **Asset Type:** Hardware

Attribute	Threat	Vulnerability	Risk Rating	Residual	Date Created
B > A	Perda de Link	Falha na Operadora	6	3	02/09/2012

Controls	REF	Classification
Link Redundante	A.10.6.3	Planned 03/09/2012

Signed: _____

Position: _____

Organisation: _____

Date:

Figura 17: Vs Risk - Relatório de plano de tratamento

4.2 STREAM INTEGRATED RISK MANAGER

O STREAM Integrated Risk Manager é um software desenvolvido pela Acuity Risk Management. A versão testada do STREAM é a *single-user* (SU), disponibilizada gratuitamente para testes na página do fabricante. Esta versão é executável em Windows XP, Vista e 7.

Sua tela inicial, por meio de gráficos, exibe uma visão geral dos riscos residuais, controles, eventos, ações, avaliações e aprovações, onde é possível ir para tela específica de cada um destes itens (figura 19).

Figura 18: STREAM - Tela principal

O menu principal do programa (parte superior da tela - figura 19) é composto pelas opções *Setup*, *Assets*, *Scope, Dashboard*, *Control Administration, Control Assessment, Events, Actions* e *Reports*.

Abaixo do menu *Setup* existem os sub-menus para as ameaças e controles, onde podem ser visualizados os já cadastrados ou serem incluídos novos. Também

existe a possibilidade de facilmente relacionar as ameaças e controles aos ativos apenas os arrastando. Através dos sub-menus *Threat Asset Class – Control Asset Class* ou *Control Asset Class – Threat Asset Class* são atribuídos controles às ameaças dos ativos. Após a associação do controle, deve ser informado o percentual de redução de risco (figura 20).

Os ativos podem ser consultados e cadastrados através do menu *Assets*. Para a inclusão de novos ativos, é solicitado que o usuário informe um código de referência, o nome e a descrição do ativo. Também é preciso relacionar o ativo com um grupo de testes e com o seu responsável (figura 21).

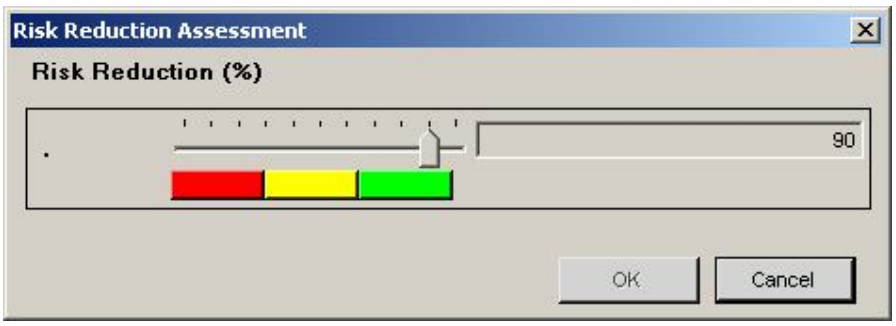


Figura 19: STREAM - Percentual de redução dos riscos após a associação dos controles

No menu *Scope*, através da opção *Risk Register – Assets*, é feita a ligação dos ativos com os seus registros de riscos.

No STREAM, antes que os riscos sejam relacionados, é necessário definir os dois níveis anteriores: *Group* e *Risk Register*. Os grupos (*Group*) podem ser, por exemplo, para separarem os riscos de diferentes unidades de negócio ou áreas da empresa. Dentro destes grupos estão subgrupos de registros de riscos (*Risk Register*) usados para separar os tipos de riscos, tais como de processos, de hardware, de software, entre outros. Dentro destes grupos de riscos é que são incluídos os riscos. No menu *Dashboard* é onde estes dois níveis são incluídos, e dentro deles, seus respectivos riscos (figura 22).

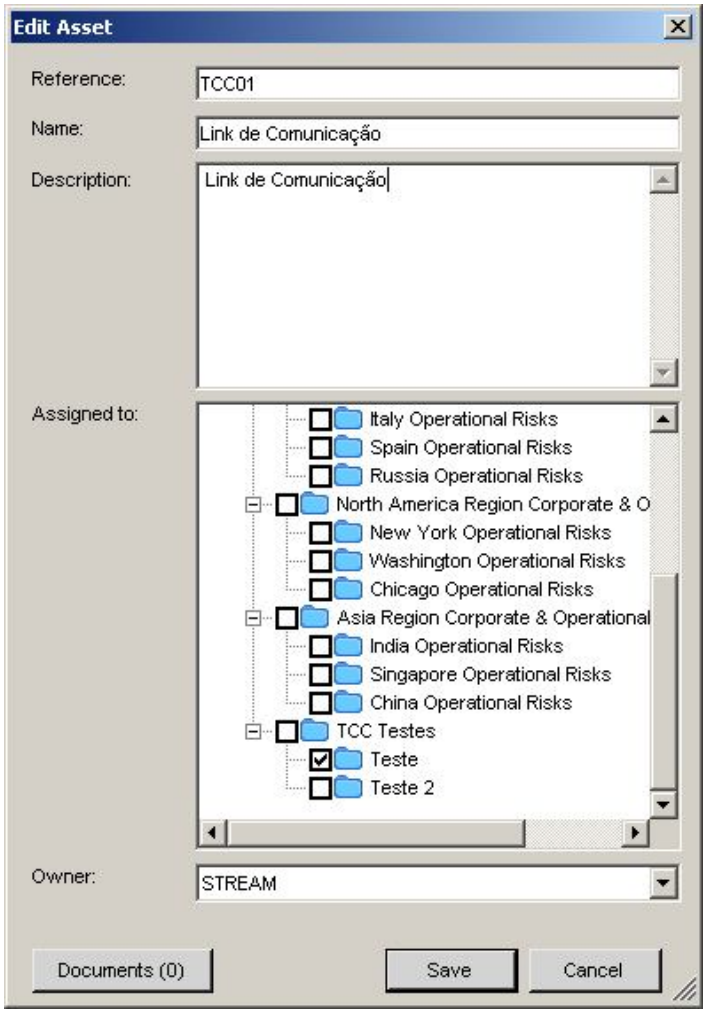


Figura 20: STREAM - Inclusão de ativos

As vulnerabilidades podem ser incluídas tanto para um grupo quanto para um registro de riscos, porém, não há um cadastro de vulnerabilidades. Para relacioná-la ao ativo e a ameaça, apenas é fornecido um campo texto, sem permitir que se selecionem os ativos ou ameaças previamente cadastrados. A tela de registro de vulnerabilidades é ilustrada na figura 23 e estas vulnerabilidades não são utilizadas em outras funcionalidades.

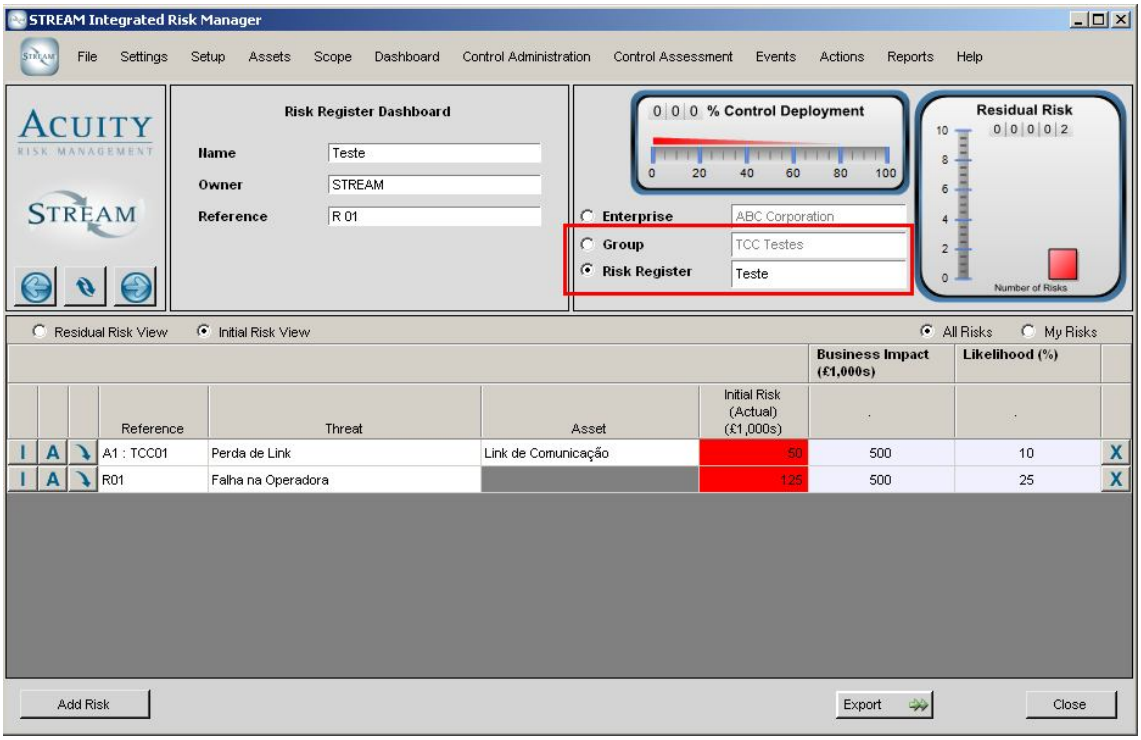


Figura 21: STREAM – Riscos por grupo

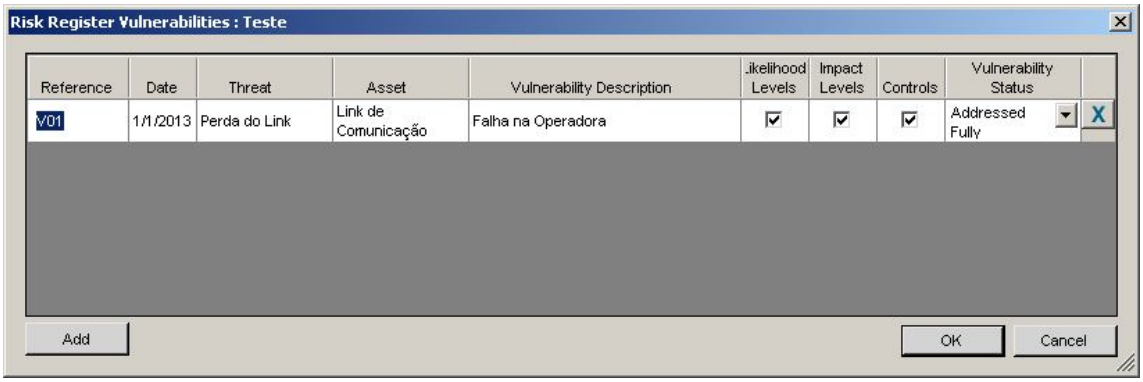


Figura 22: STREAM - Registro de vulnerabilidades do risco

Ao incluir um risco existem duas visualizações: Risco Inicial (*Initial Risk View*) e Risco Residual (*Residual Risk View*). Na tela do Risco Inicial, é solicitado que se informe o seu impacto para o negócio e sua probabilidade de ocorrência por meio de uma escala (muito baixo, baixo, médio, alto e muito alto) como é vista na figura 24. Com base nestes valores o risco é automaticamente calculado e

representado na coluna *Initial Risk* (figura 25). Na visão de Risco Residual, são listados os controles previamente relacionados e também podem ser incluídos novos controles. E com isto, se define o percentual de redução do risco com a implementação dos controles (figura 26). De acordo com o percentual de redução de risco informado é calculado o novo valor para o risco, que é listado na coluna *Potential Risk* (figura 27). Os cálculos para os valores dos riscos não são detalhados pelo *help* do programa.

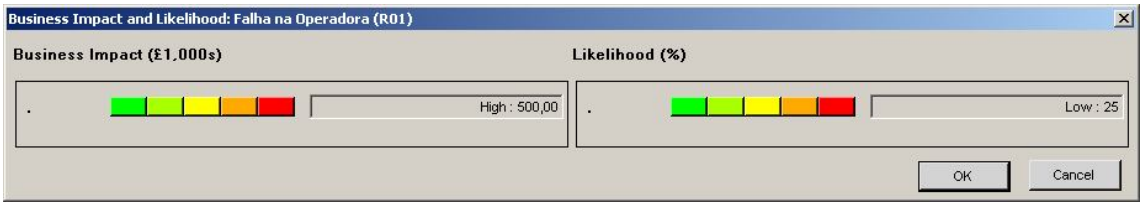


Figura 23: STREAM - Impacto e probabilidade do risco

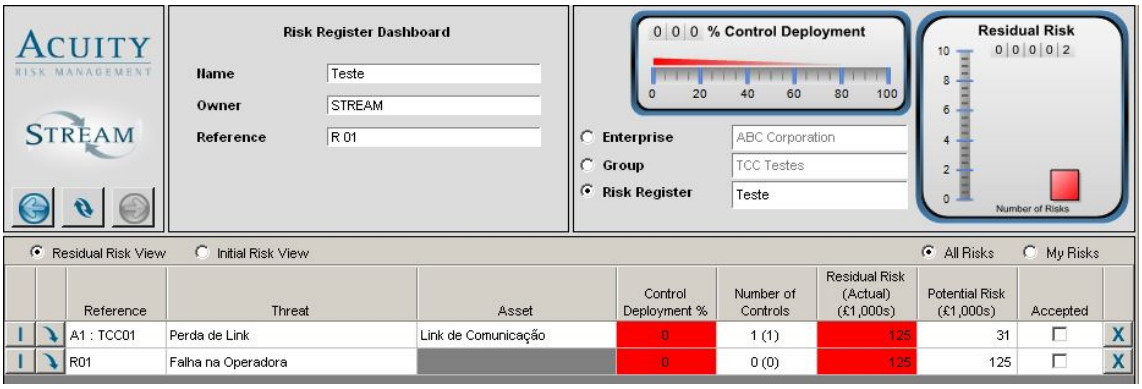


Figura 24: STREAM - Cálculo do risco

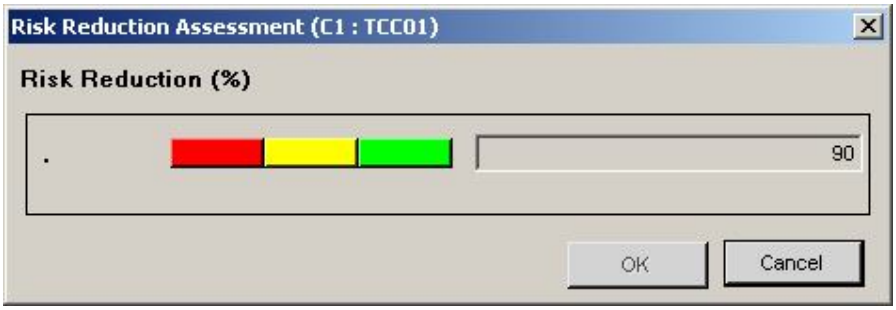


Figura 25: STREAM - Percentual de redução de riscos

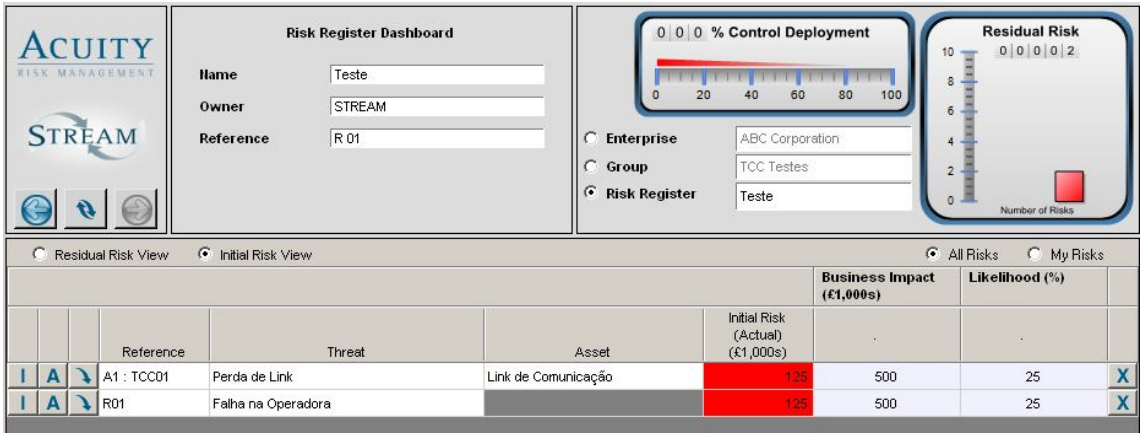


Figura 26: STREAM - Cálculo do risco após a associação dos controles

No menu *Control Assessment*, são visualizadas as datas de avaliação dos controles, os ativos relacionados, o seu percentual de desenvolvimento. Podem ser adicionadas novas datas para avaliações.

Uma particularidade do STREAM são as ações (*Actions*), que podem ser entendidas como os atos de implementar os controles em uma data estipulada. As ações podem ser cadastradas através do menu *Actions*, definindo-se o seu custo, prioridade, status de andamento, sua data de realização, além de permitir que sejam associados os controles necessários. Elas são relacionadas aos riscos no momento em que os riscos são associados aos seus grupos de riscos, conforme quadro em destaque na figura 28.

De forma resumida, a estrutura de como o STREAM trata os riscos funciona da seguinte maneira:

1. *Enterprise Dashboard*: Neste nível podem ser incluídas vulnerabilidades;
   1.1. *Group Dashboard*: Também podem ser incluídas vulnerabilidades neste nível;
   1.2. *Risk Register Dashboard*: Permite a visão dos riscos residuais ou riscos iniciais;
   1.3. *Risk Dashboard*: Pode ser informado o percentual de redução de riscos;
   1.4. *Control Dashboard*: Datas de avaliações e percentual de

desenvolvimento dos controles.

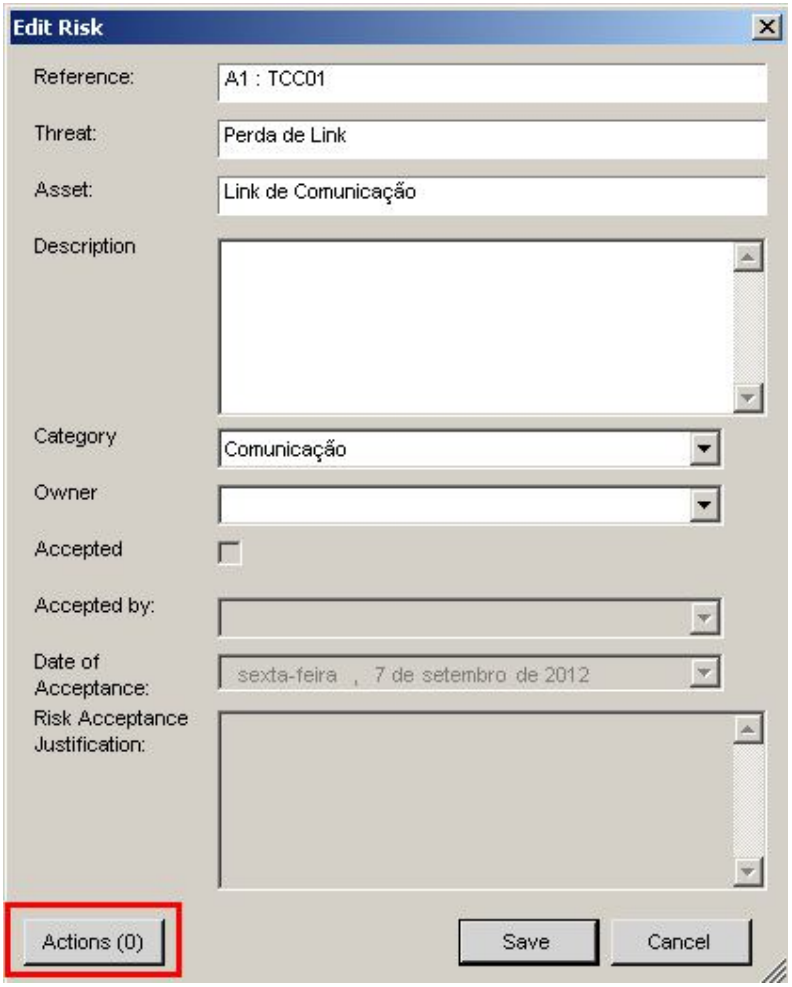


Figura 27: STREAM - Inclusão de ações aos riscos

Outra característica do STREAM são os registros de eventos, localizados no menu *Events*. Os eventos podem ser de dois tipos, os incidentes que impactaram na organização (*incident*) e os eventos que não trouxeram impacto tangível à organização (*near-miss*). Os eventos são registrados com sua data de acontecimento, tipo, categoria (continuidade de negócios, financeiro, segurança da informação, etc) e podem ser relacionados às ameaças, controles e ao impacto envolvido. É definido também o status do evento, que pode ser novo, aberto, em discussão, revisão pós-evento e fechado. Os eventos podem ser acompanhados

através da tela principal (figura 19), cujos status são representados por cores em um gráfico. O status de cada evento pode ser alterado.

O STREAM ainda permite a geração de relatórios com a exibição de gráficos (figura 29). Os relatórios disponíveis podem mostrar gráficos por riscos residuais, controles, riscos, ações e eventos e também os maiores riscos encontrados. O STREAM não gera relatórios em formato texto.

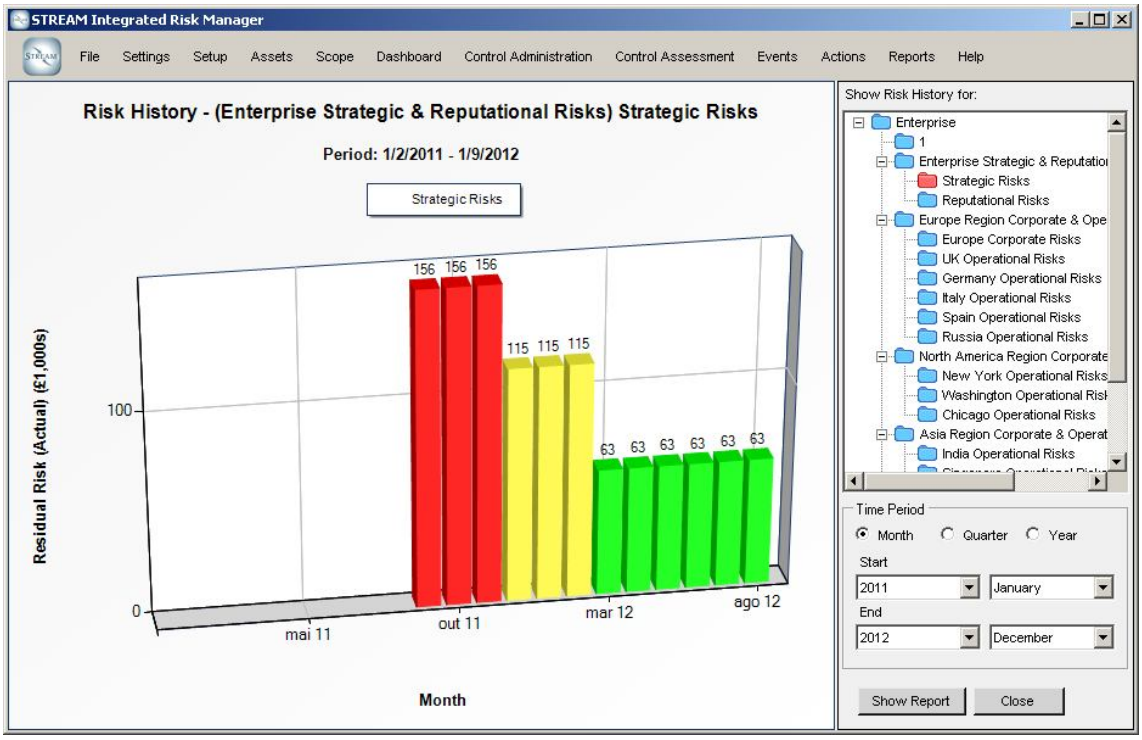


Figura 28: STREAM – Relatórios

4.3 SOBF TOOL

O Secure Officers Best Friend (SOBF) é um software *free* desenvolvido em Java pela Security Officers Management and Analysis Project (SOMAP.org). Como o software ainda está em fase de desenvolvimento, foi testada uma versão beta, a 1.0b1, que ainda não possui todas as funcionalidades implementadas. Por ser desenvolvido em Java, é necessário possuir a versão 1.5 ou superior do Java Runtime para executá-lo.

Os menus mais significativos do software são o *Assessment Workflow* e *Repository.* O menu *Assessment Workflow* contém as mesmas opções visualizadas na tela principal (figura 30) que é divida em três grupos: *Context Establishment, Risk Retention e Risk Treatment*.

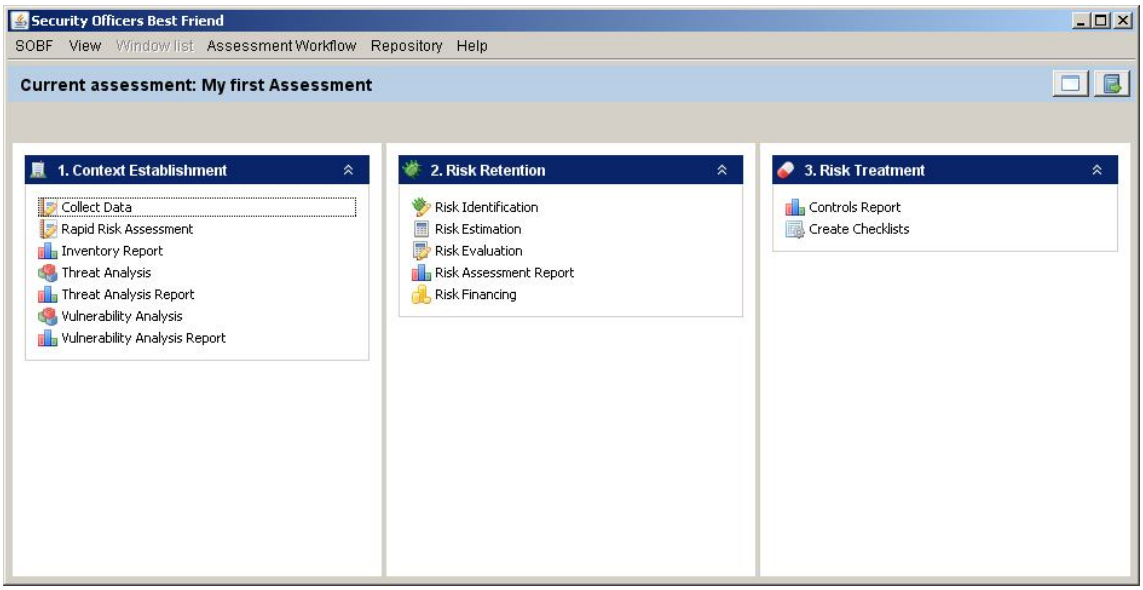


Figura 29: SOBF - Tela principal

No *Context Establishment* é onde pode ser feita a manutenção dos ativos por meio da opção *Collect Data*. No *Collect Data* serão definidos apenas os ativos a serem utilizados no contexto da empresa. Como esta ferramenta é baseada no método qualitativo, ao incluir um novo ativo (figura 31), é solicitado, além de seu nome e descrição, o seu nível de confidencialidade (não aplicável, não confidencial, não muito confidencial, confidencial, muito confidencial e altamente confidencial), o nível de integridade (não aplicável, muito baixo, baixo, médio, alto e muito alto) e o nível de disponibilidade (não aplicável, ser importância, sem muita importância, importante, muito importante e extremamente importante). Também pode ser informado um valor para o ativo.

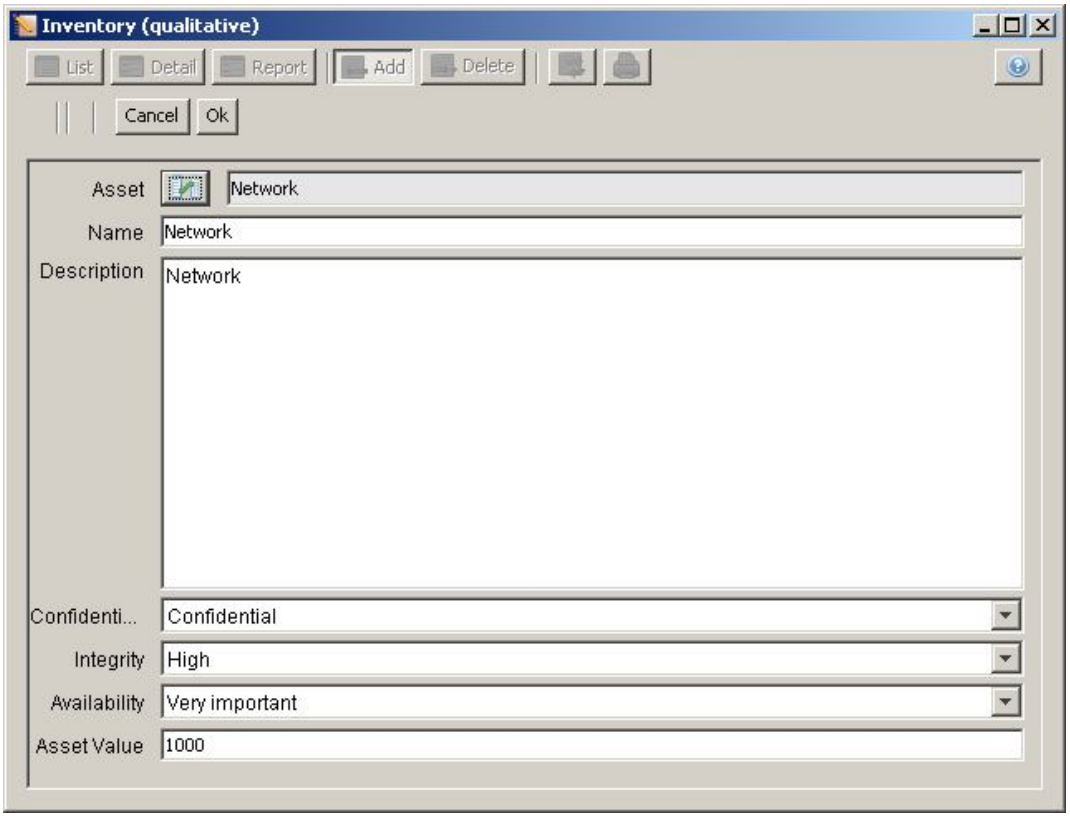


Figura 30: SOBF - Inclusão de ativos

Outras funcionalidades do *Context Establishment* são a *Threat Analysis*, onde as ameaças cadastradas podem ser ativadas ou desativadas e a *Vulnerability Analysis*, que mostra os riscos e vulnerabilidades relacionadas ao ativo.

Neste grupo também existem três tipos de relatórios: a listagem dos ativos (*Inventory Report*), listagem das ameaças ativas (*Threat Analysis Report*) e listagem das vulnerabilidades associadas (*Vulnerability Analysis Report*).

O segundo grupo é o *Risk Retention*, onde, podem ser adicionados os riscos aos ativos na opção *Risk Estimation*. Para adicionar os riscos, deve ser informado seu grau de probabilidade (não aplicável, muito improvável, improvável, possível, provável e muito provável) e impacto (não aplicável, muito baixo, baixo, médio, alto e muito alto). Além disso, é preciso relacionar o risco a uma vulnerabilidade e a um ativo (figura 32). O valor do risco é calculado automaticamente considerando o grau de probabilidade e o seu nível de impacto, ou seja, risco = impacto x probabilidade, onde o valor do impacto pode ir de 1 (muito baixo) até 5 (muito alto) e o valor da

probabilidade pode ir de 1 (muito improvável) até 5 (muito provável). Baseado no resultado do cálculo é definida a intensidade do risco:

(a) De 1 a 4: Baixo risco;

(b) De 5 a 14: Risco médio;

(c) De 15 a 25: Risco alto.

Nas opções *Risk Identification* e *Risk Evaluation* são listadas as proteções e controles dos ativos.

O relatório dos riscos pode ser gerado com o *Risk Assessment Report* que lista as ameaças dos ativos com suas probabilidades e impactos, o cálculo do risco e a vulnerabilidade associada.

No terceiro grupo da tela, o *Risk Treatment*, pode ser gerado um relatório dos controles, com informações sobre o risco relacionado e a efetividade do controle.

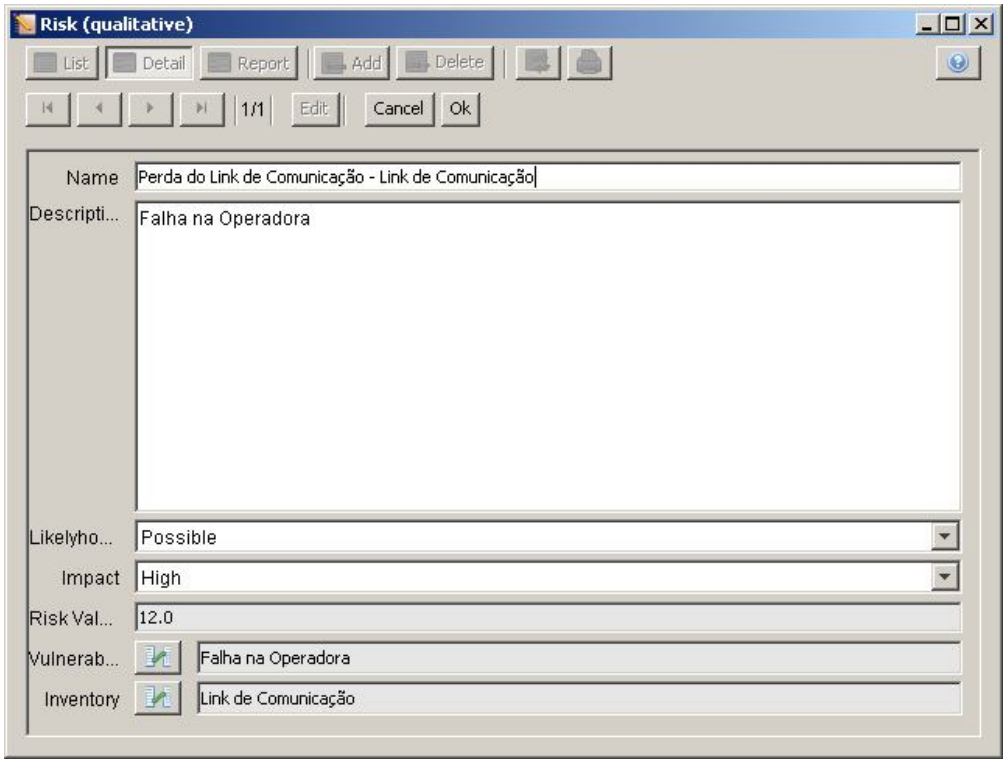


Figura 31: SOBF - Inclusão de riscos

O terceiro grupo é o *Risk Treatment* que permite a geração de relatórios através da opção *Controls Report*.

No menu Repository existe uma funcionalidade para listar e adicionar todos os ativos (*Show asset qual*), diferentemente do que é feito pelo *Collect Data*, que utiliza apenas os ativos que serão utilizados no contexto da empresa. Ao incluir um novo ativo, deve-se informar o seu tipo. Este tipo é cadastrado pela opção *Show Asset Type*, do mesmo menu.

A seguir, existem as funcionalidade para listar e adicionar ameaças (*Show threat*) e listar e adicionar os tipos de ameaças (*Show threat type*). Na inclusão de uma ameaça é definido o seu nome e descrição e o seu tipo, cadastrado previamente (figura 33).

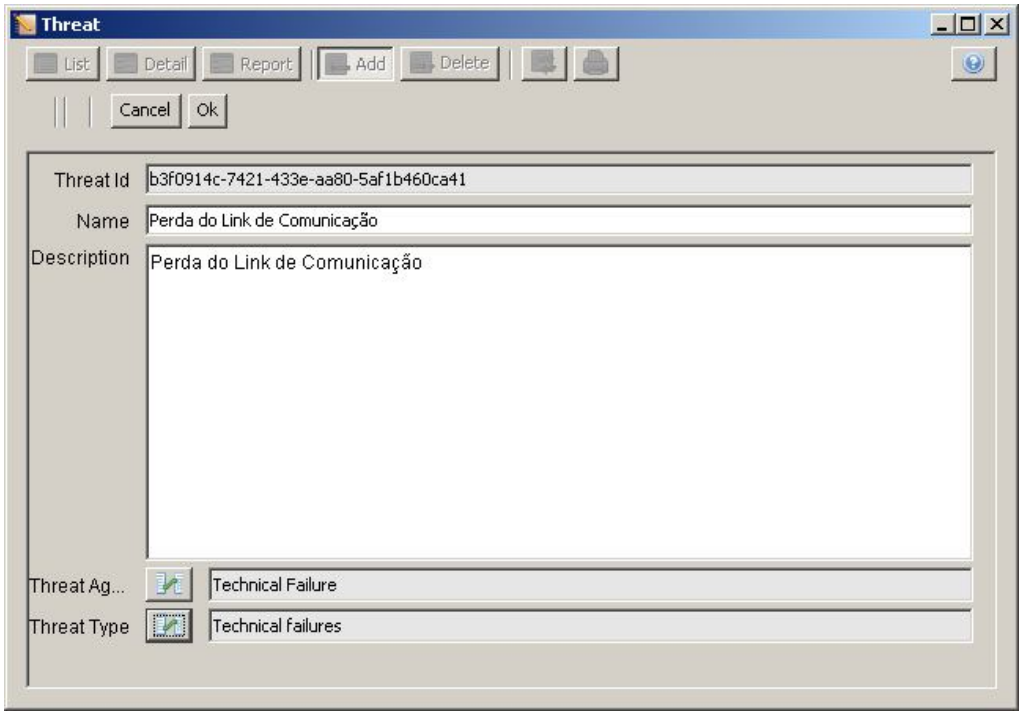


Figura 32: SOBF - Inclusão de ameaças

Existem duas formas para incluir as vulnerabilidades dos ativos: a primeira é pelo *Show Vulnerabilitys*, que exibe uma listagem das vulnerabilidades existentes, permitindo a edição e inclusão de novas. Para incluir uma nova vulnerabilidade, é preciso definir o grau de probabilidade e impacto, e relacioná-la com o respectivo

ativo e com a ameaça (figura 34) cadastrada como da forma apresentada anteriormente.

A outra forma é pela opção *Show Vulnerability Setup*, uma tela que mostra duas tabelas, sendo a primeira contendo os ativos e a segunda com as ameaças. Seleciona-se então, um ativo e sua ameaça e, por meio do botão (+) é incluída uma nova vulnerabilidade em uma terceira tabela, como mostra a figura 35. Nesta terceira tabela, além do ativo e sua ameaça, existem outras colunas onde podem ser informados o nível de probabilidade e o impacto da ameaça.

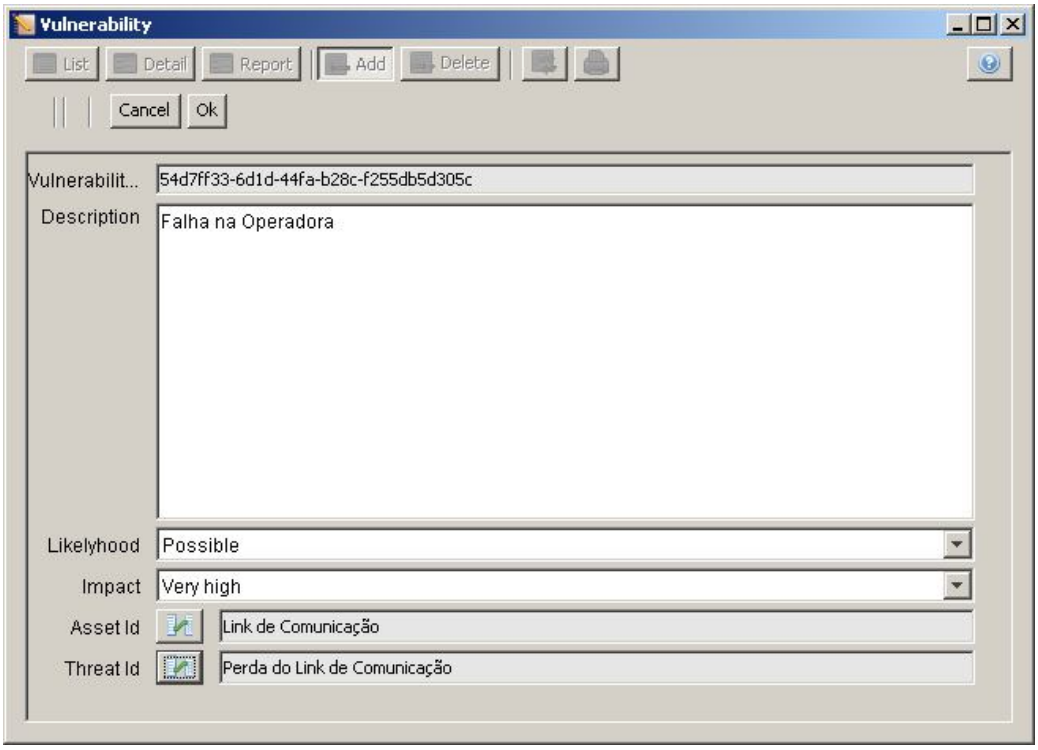


Figura 33: SOBF - Inclusão de vulnerabilidade

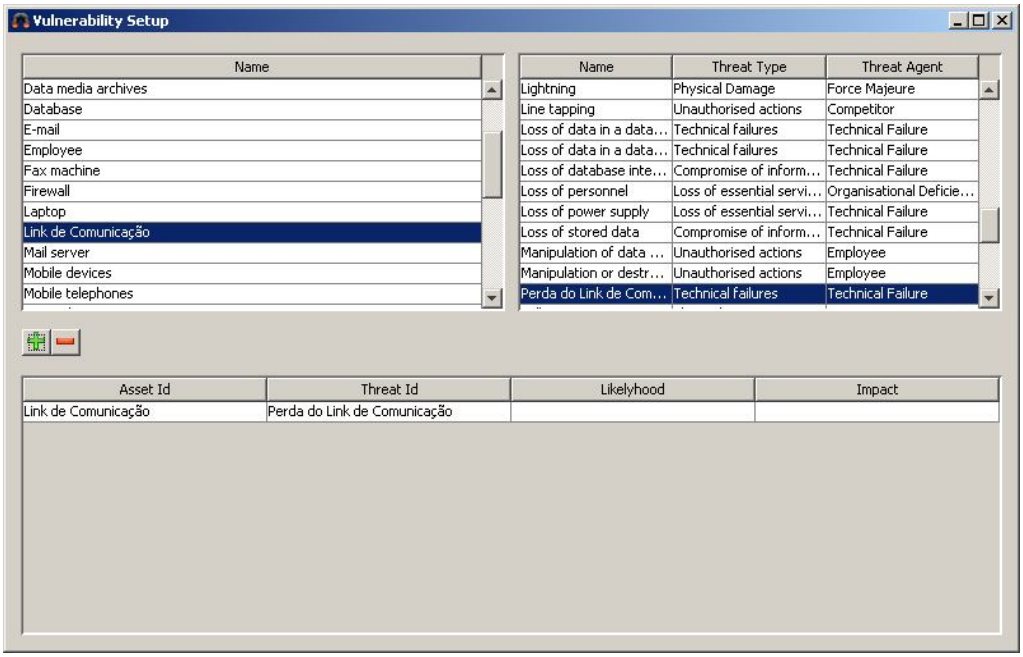


Figura 34: SOBF - Inclusão de vulnerabilidade

No SOBF os controles são chamados de salvaguardas (safeguard). Para o cadastramento dos mesmos existe a opção *Show Safeguards*, no menu *Repository*. Para a inclusão dos controles, deve ser informado seu nome, descrição e o quanto o mesmo é efetivo (nunca, às vezes, frequentemente ou sempre) (figura 36).

A operação de relacionar os controles com os ativos, ameaças e vulnerabilidades é definida como uma prevenção no SBOF. Estas prevenções serão associadas aos riscos através das opções *Risk Evaluation* ou *Risk Identification*, e podem ser definidas como as soluções para os riscos.

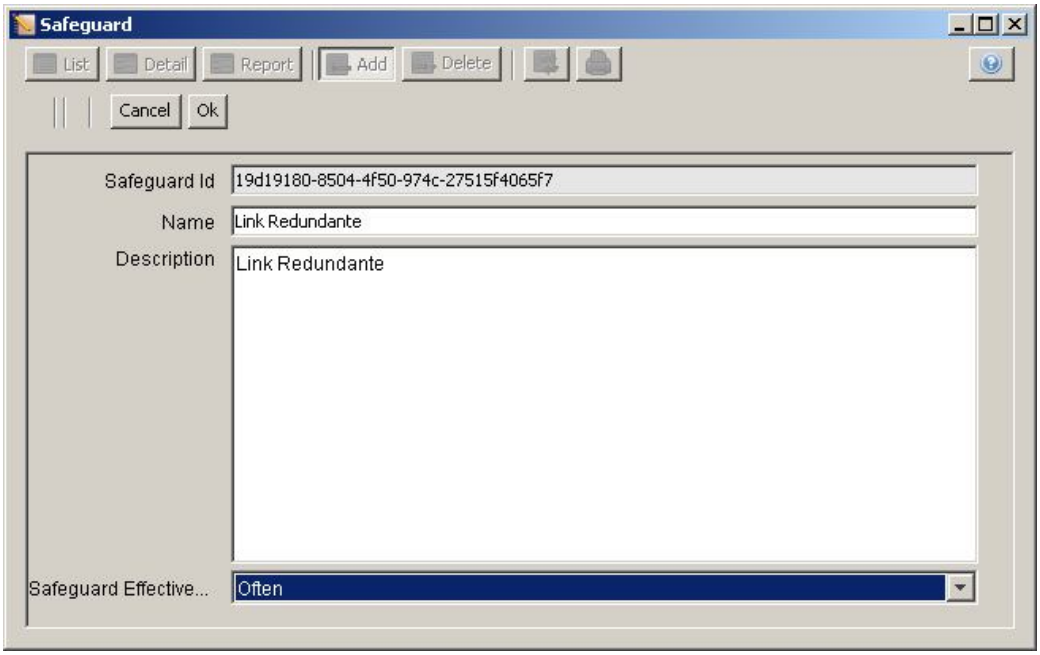


Figura 35: SOBF - Inclusão de controles

Para incluir novas prevenções existem duas formas. A primeira forma pela opção *Show Prevention*, que traz uma listagem das prevenções e permite a criação de novas. Para criar uma nova prevenção é selecionado o controle, a vulnerabilidade, a ameaça e o ativo (figura 37).

A outra forma é realizada por meio do *Prevention Setup* que apresenta em uma primeira tabela os ativos relacionados às suas ameaças e em uma segunda tabela são listados os controles. É feita a conexão entre as duas tabelas criando uma terceira abaixo, mostrando o controle, a vulnerabilidade, a ameaça e o ativo (figura 38).

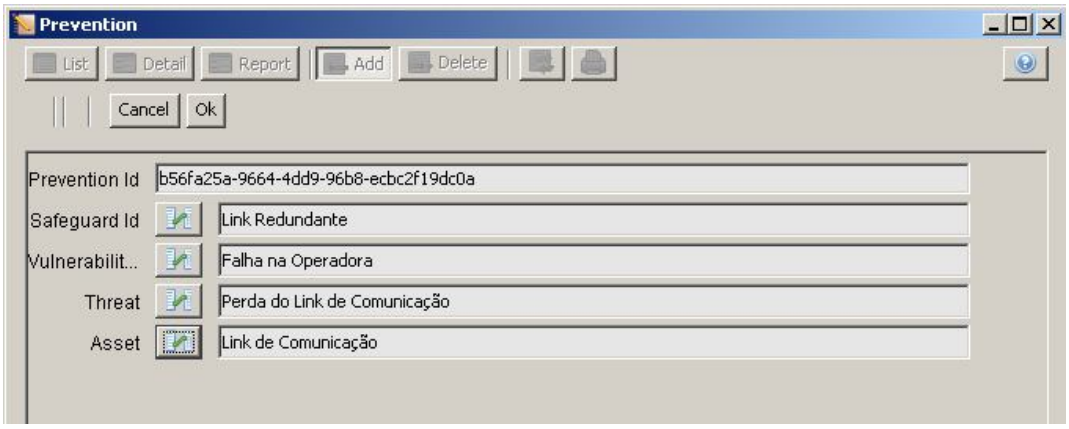


Figura 36: SOBF - Inclusão de prevenções

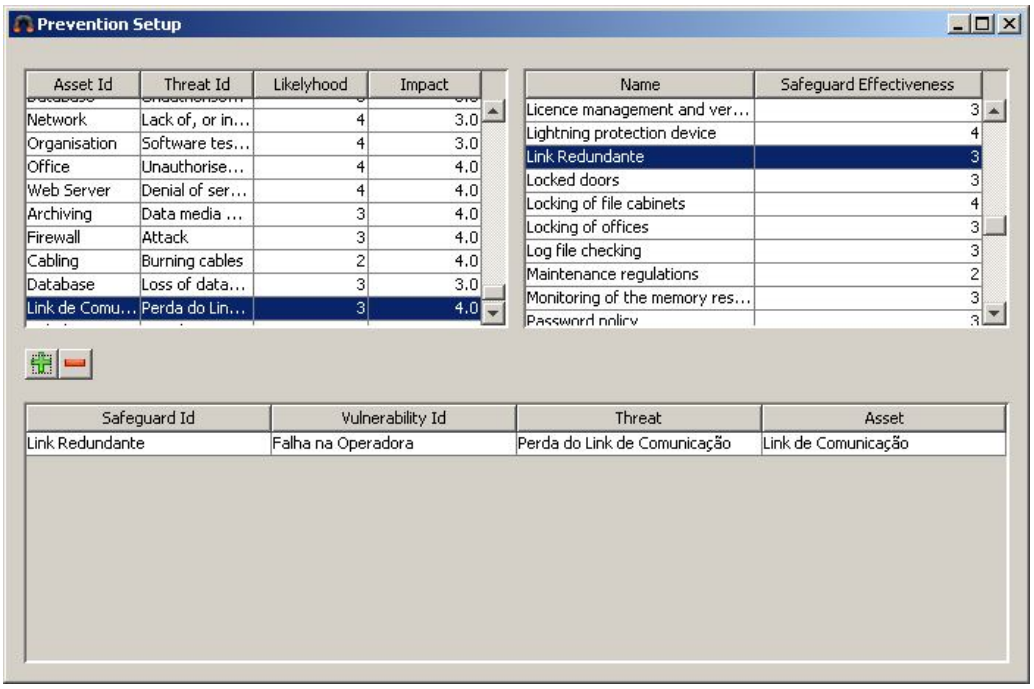


Figura 37: SOBF - Inclusão de prevenções

Desta forma, após a inclusão da prevenção, a mesma estará disponível para ser relacionada aos riscos, pela opção *Risk Evaluation* (figura 39).

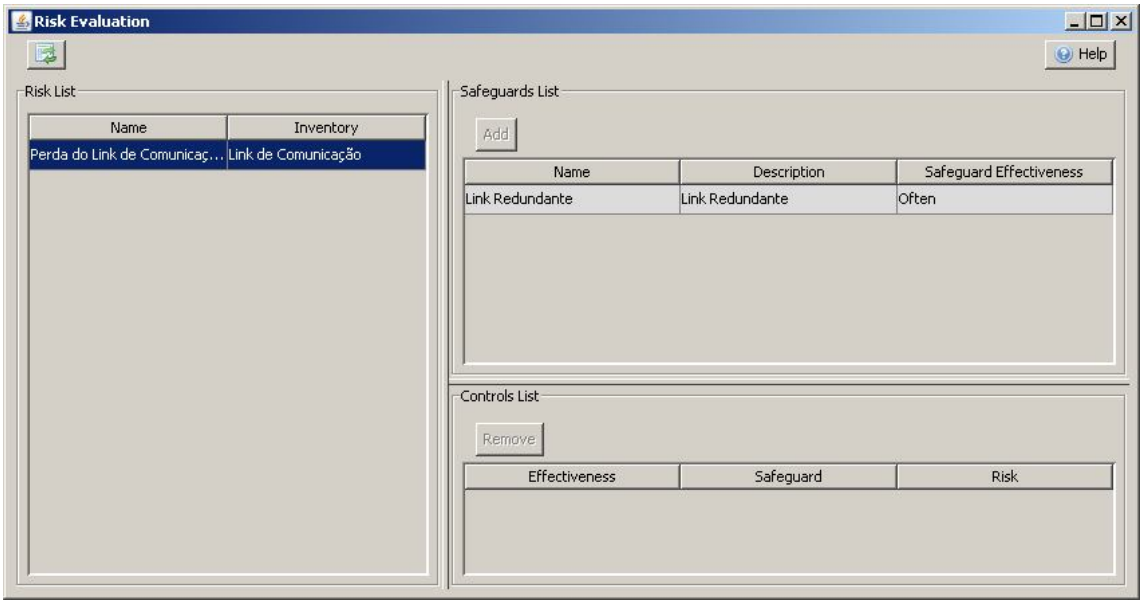


Figura 38: STREAM - Avaliação de riscos

4.4 SECUREAWARE

O SecureAware é um software pago desenvolvido pela Neupart. O sistema é executado através de um navegador.

Inicialmente, a tela mais significativa para a gestão de riscos é a *Risk Home*, onde são visualizadas as opções de ativos (*Assets*), ameaças (*Threats*), avaliações (*Assesments*) e resultados (*Results*) (figura 40).

Ao entrar na tela de Ativos (*Assets*), é exibida uma lista do inventário de ativos, onde é possível cadastrar novos ou editar os já existentes (figura 41). Para incluir um novo ativo, inicialmente é preciso que se informe o seu nome, descrição e o seu tipo (figura 42). O tipo do ativo pode ser, por exemplo: processo, serviço, sistema, Data Center, provedor de serviços ou outros que podem ser incluídos ou editados através da manutenção específica para os tipos. A seguir é solicitada a localização, a classificação de confidencialidade (ultra secreto, secreto, confidencial, restrito, sem classificação e público), a criticidade para o negócio (crítico, importante, não crítico), o valor financeiro. Estes três últimos campos são criados a partir do cadastro *Data List,* e permite que outros campos sejam adicionados para fazer parte

do cadastro de ativos. Além destas informações, existem campos para informar o usuário responsável e o administrador do ativo (figura 43). Outra forma de incluir ativos é por meio da importação de arquivos no formato csv ou xls.

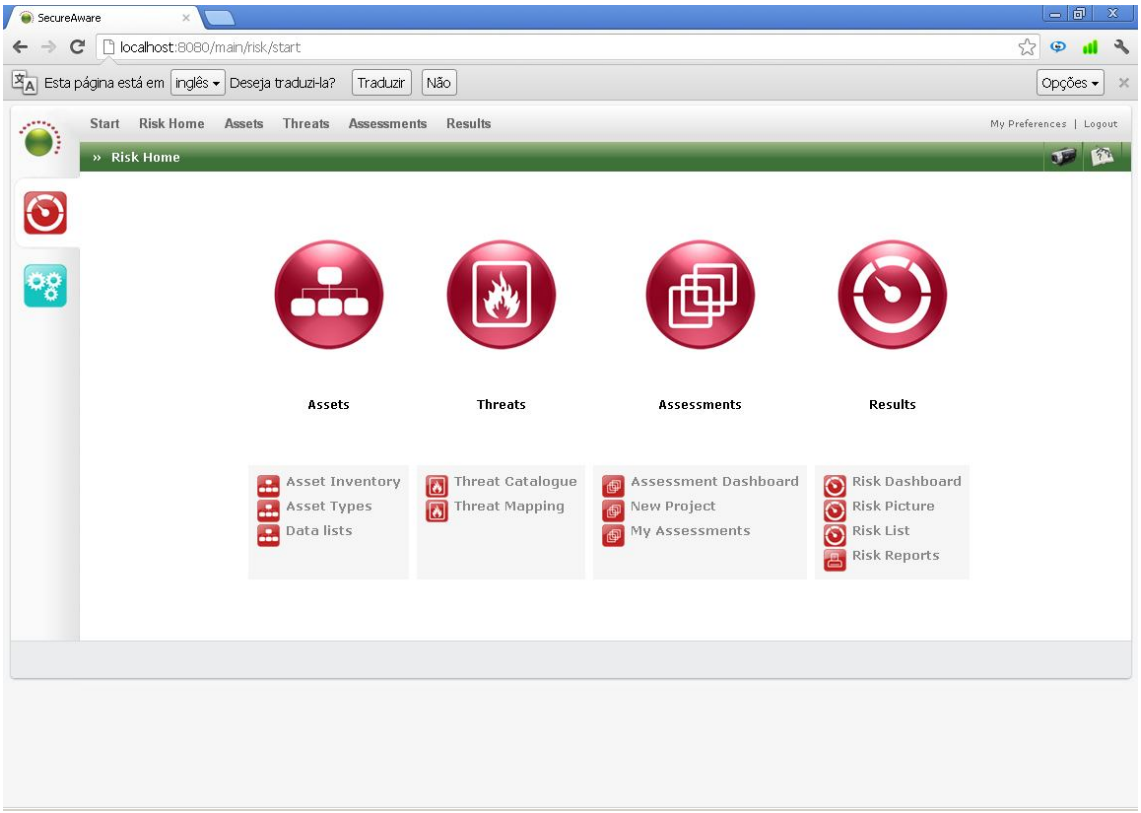


Figura 39: SecureAware - Tela inicial de riscos

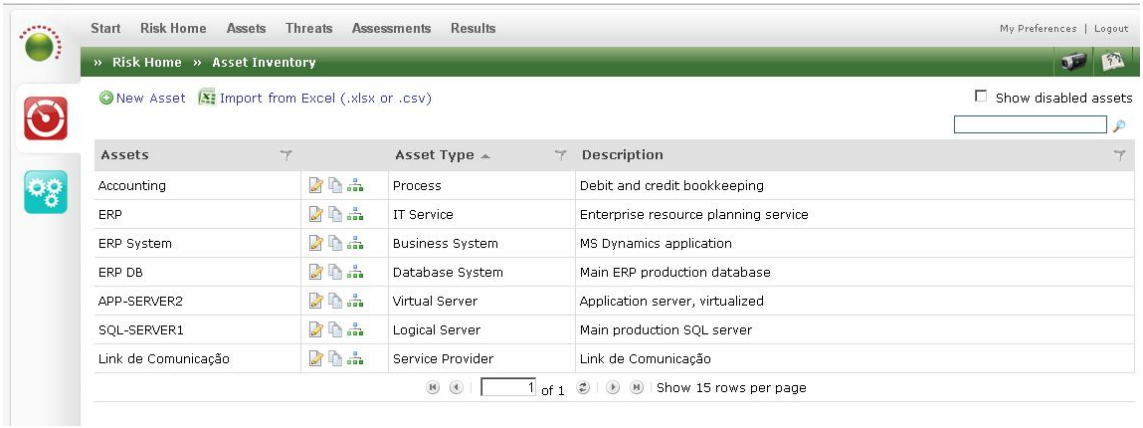


Figura 40: Secure Aware - Listagem de ativos

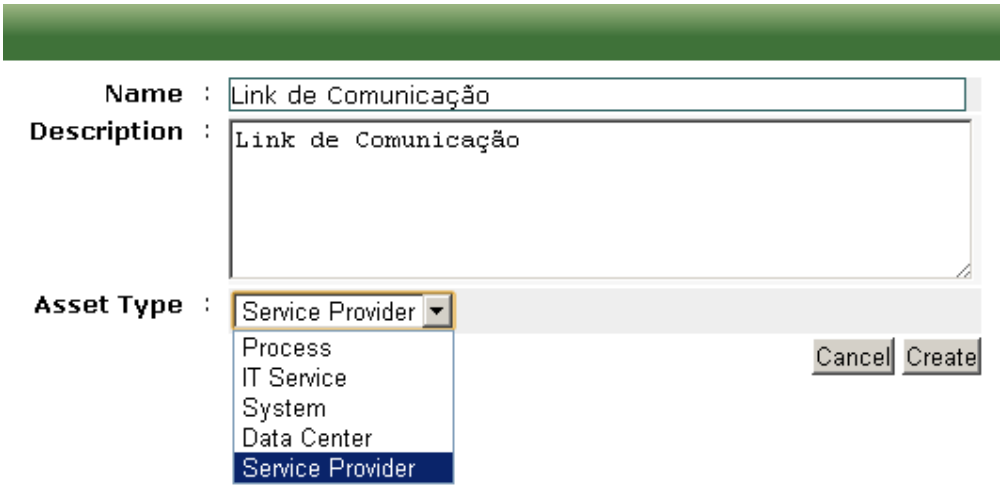


Figura 41: SecureAware - Inclusão de ativos

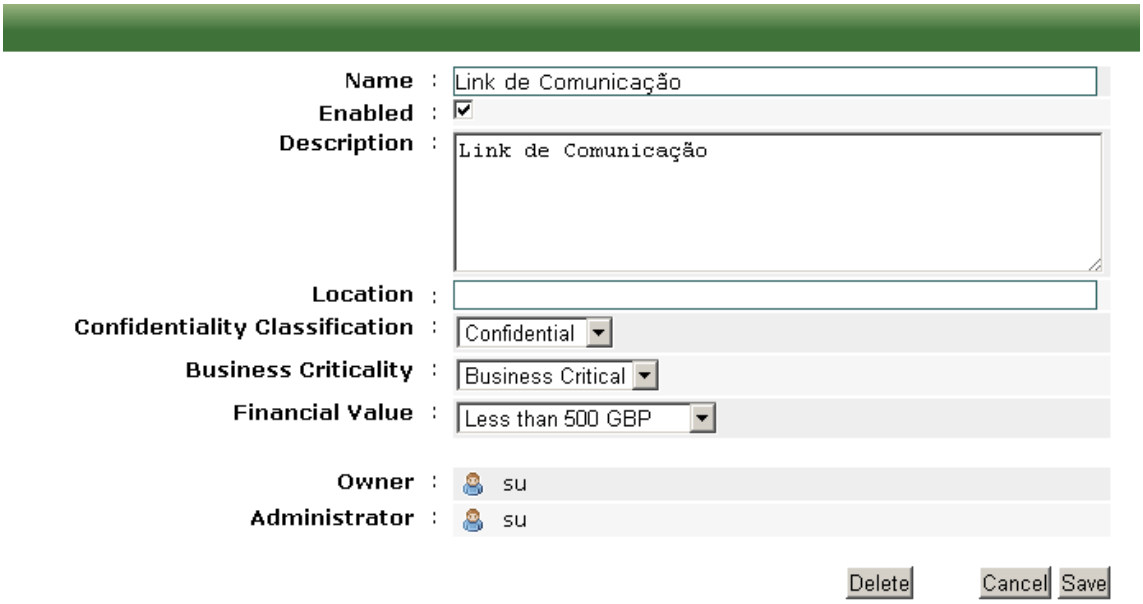


Figura 42: SecureAware - Inclusão de ativos

Para cada um dos ativos cadastrados, é possível incluir uma relação (*relation*) com outros ativos, indicando o seu percentual de dependência quanto à confidencialidade, integridade e disponibilidade (figura 44).

Podem ser relacionadas relações de ativos com maior nível ou com menor nível. Um ativo herdará a avaliação de impacto dos ativos com maior nível e também

as avaliações de vulnerabilidades de ativos de níveis inferiores. Como no exemplo da figura 45, o ativo “Link de Comunicação” possui uma relação de nível inferior com o ativo “Contrato com a Operadora” e estará herdando as avaliações de vulnerabilidades deste ativo de nível inferior. Já o ativo “Contrato com a Operadora”, em suas relações apresentará o ativo “Link de Comunicação” como uma relação de nível superior, e, portanto herdará a avaliação de impacto do ativo relacionado.

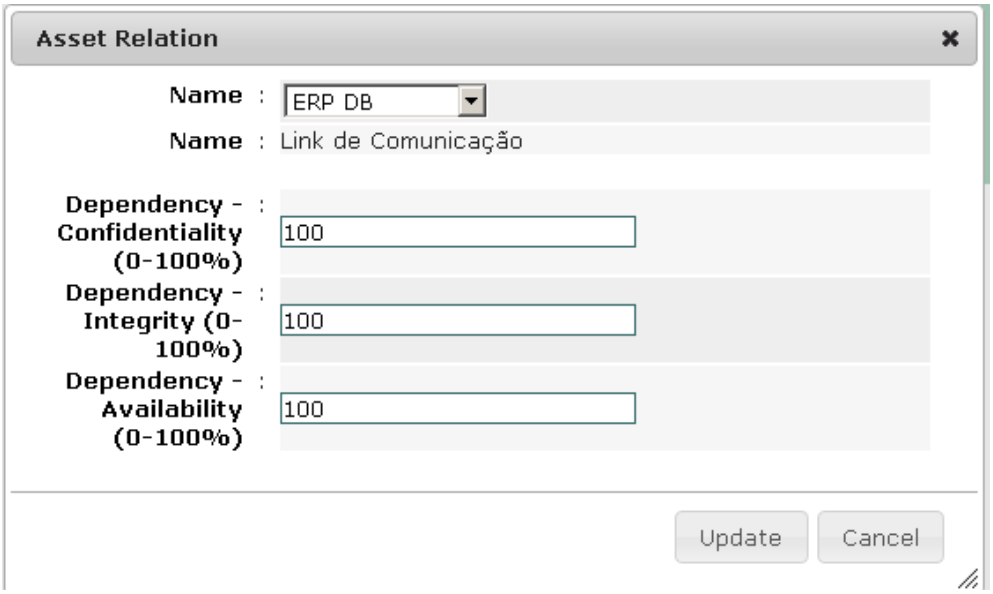


Figura 43: SecureAware - Relacionamento de ativos

Figura 44: SecureAware - Ativo com relações

Ao entrar na opção de ameaças (*Threats*), são listadas todas as ameaças, a sua freqüência e o nível de impacto, representados através de cores. O nível de impacto é mostrado através de três quadros coloridos para cada ameaça pode representar aos ativos, sendo um para a confidencialidade, um para a integridade e outro para a disponibilidade, respectivamente. As cores indicam as seguintes situações:

Freqüência:

(a) Raramente (verde escuro): A ameaça não ocorre há anos;
(b) Ocasionalmente (verde claro): A ameaça ocorre algumas vezes no ano;
(c) Regularmente (amarelo): A ameaça ocorre em média uma vez por mês;
(d) Freqüentemente (laranja): A ameaça ocorre em média uma vez por semana;
(e) Constantemente (vermelho): A ameaça ocorre diariamente.

Impacto:

(a) Muito baixo (verde escuro): Perda insignificante de confidencialidade, integridade ou disponibilidade do ativo;
(b) Baixo (verde claro): Perda limitada de confidencialidade, integridade ou disponibilidade do ativo;
(c) Médio (amarelo): Perda significante de confidencialidade, integridade ou disponibilidade do ativo;
(d) Alto (laranja): Perda grande de confidencialidade, integridade ou disponibilidade do ativo;
(e) Muito alto (vermelho): Perda total de confidencialidade, integridade ou disponibilidade do ativo;

Nesta tela existe um link para a manutenção das fontes de ameaças (*Threat Sources*) (figura 46), que podem ser, por exemplo, estragos ocorridos por fogo, água, erros de software ou hardware, entre outros.

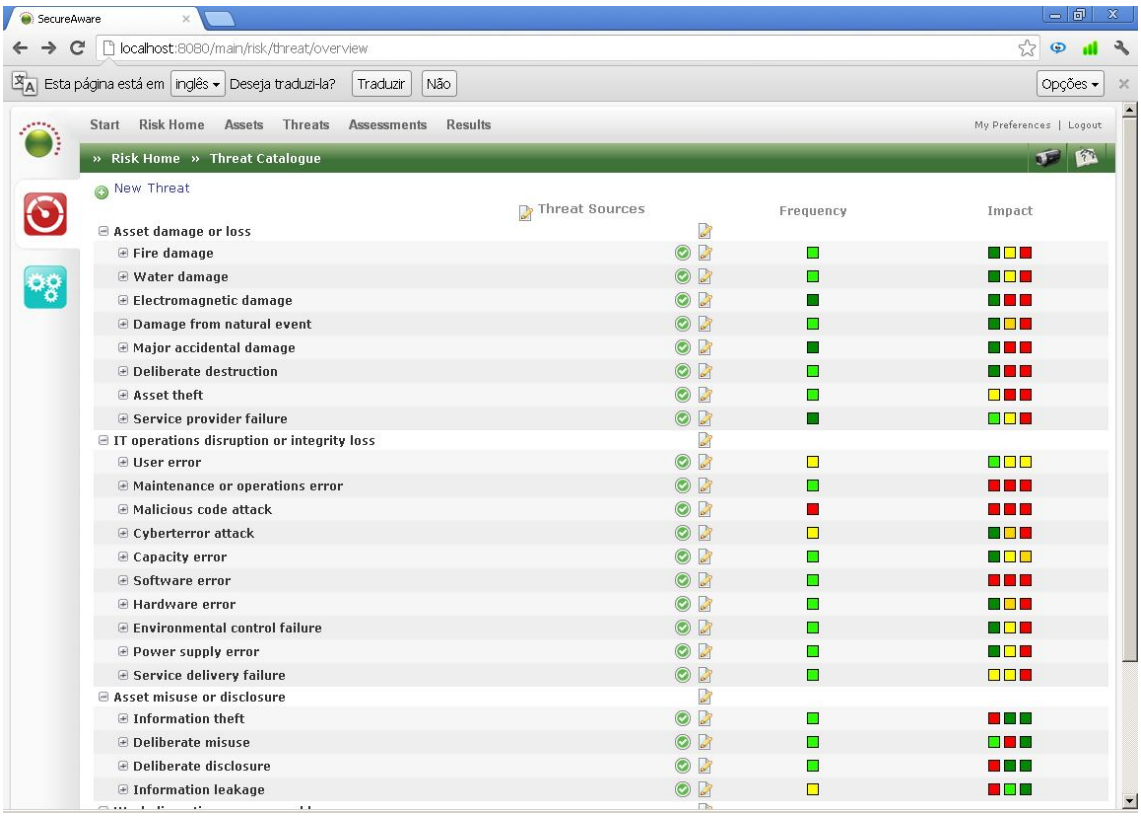


Figura 45: SecureAware - Listagem de ameaças

Para incluir uma ameaça é preciso seguir uma seqüência de passos, iniciando pela seleção do grupo de ameaça (danos ou perda de ativos, perda de integridade de operações de TI, mau uso ou divulgação de ativos, interrupção de trabalho ou perda de pessoal) (figura 47). Em seguida é informado o nome e descrição da ameaça e o seu nível de impacto quanto à confidencialidade, integridade e disponibilidade (figura 48). No passo seguinte são relacionadas as fontes de ameaça e no próximo os tipos de ativos que podem ser afetados por estas fontes de ameaças.

A relação das ameaças aos ativos, diferentemente dos outros softwares, não é feita ligando uma ameaça a um ativo, mas ao tipo do ativo. Por exemplo: se uma ameaça é relacionada com o tipo de ativo “Processo”, significa que todos os ativos deste tipo poderão ser afetados por esta ameaça. Desta forma, a freqüência e os valores de impacto da ameaça serão consideradas para o cálculo do risco do ativo.

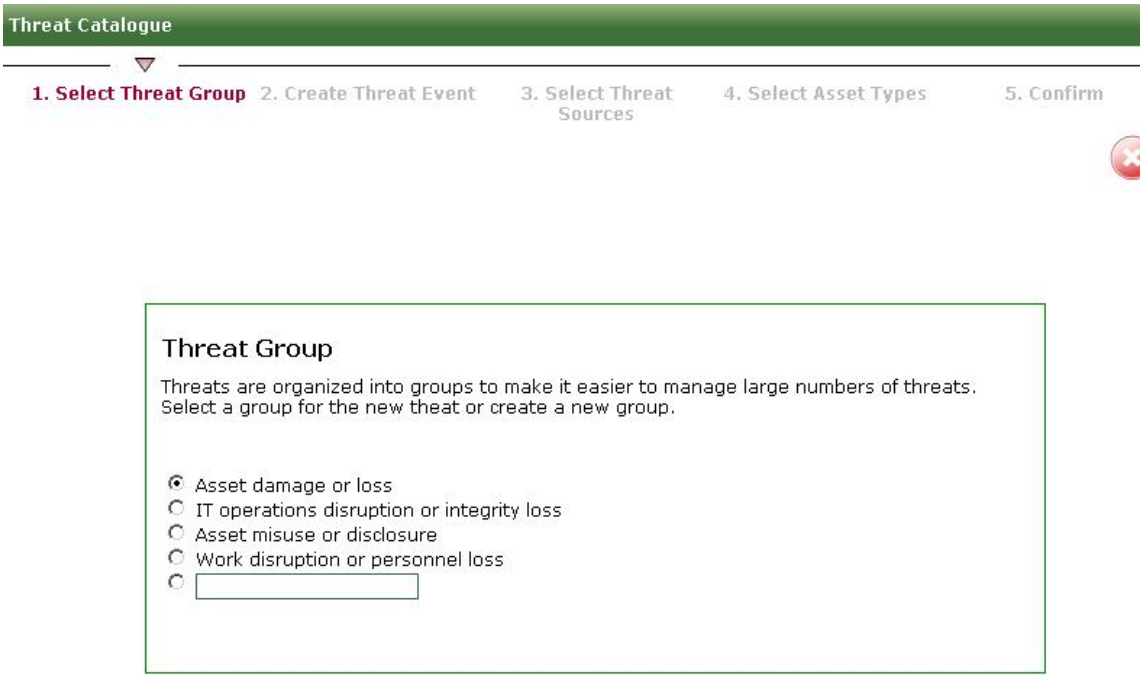


Figura 46: SecureAware - Inclusão de ameaças I

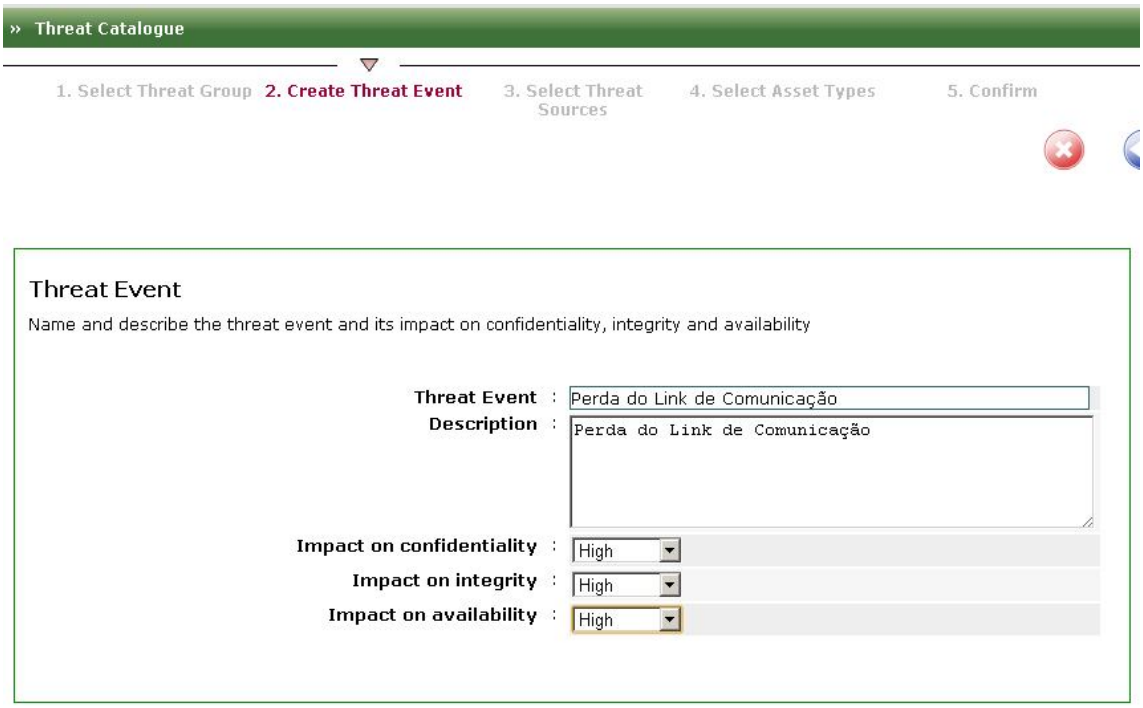


Figura 47: SecureAware - Inclusão de ameaças II

Na tela de avaliação de riscos (*Assessments*), são criados (*New Project*) e gerenciados (*My Assessments*) os projetos de avaliação de riscos. Ao criar um novo projeto, informa-se o seu nome, a data de início e a de término do mesmo, bem como o método de avaliação que será utilizado, podendo ser por vulnerabilidade ou probabilidade, conforme o quadro em destaque da figura 49. Independente do método escolhido para avaliação, também pode ser escolhido se será utilizado o método de impacto no negócio. Neste momento é possível escolher, para cada uma das avaliações, se o enfoque da avaliação será de alto nível ou detalhado, ou os dois.

Em seguida são selecionados os ativos que farão parte deste projeto.

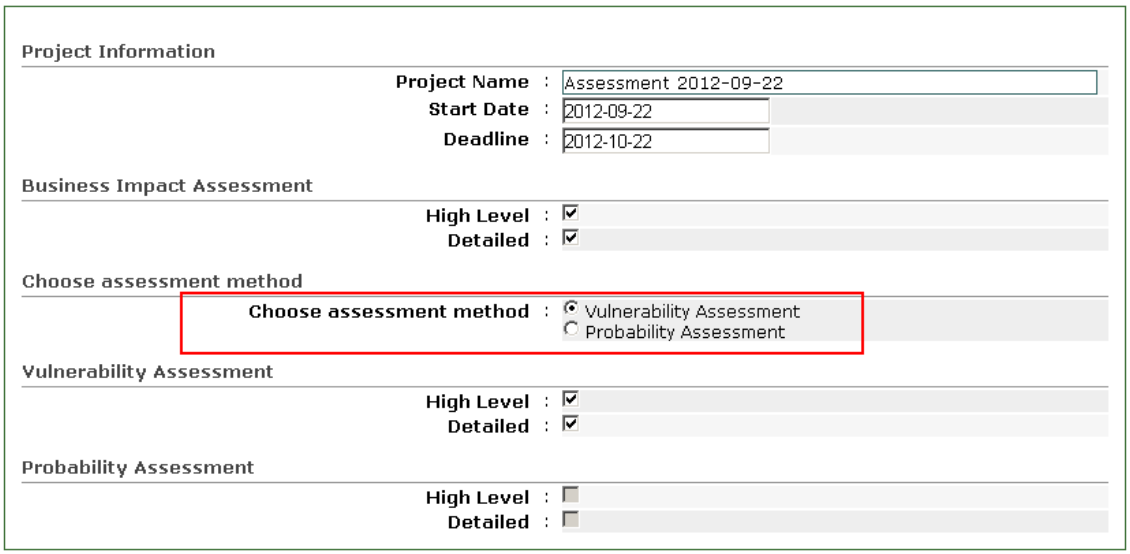


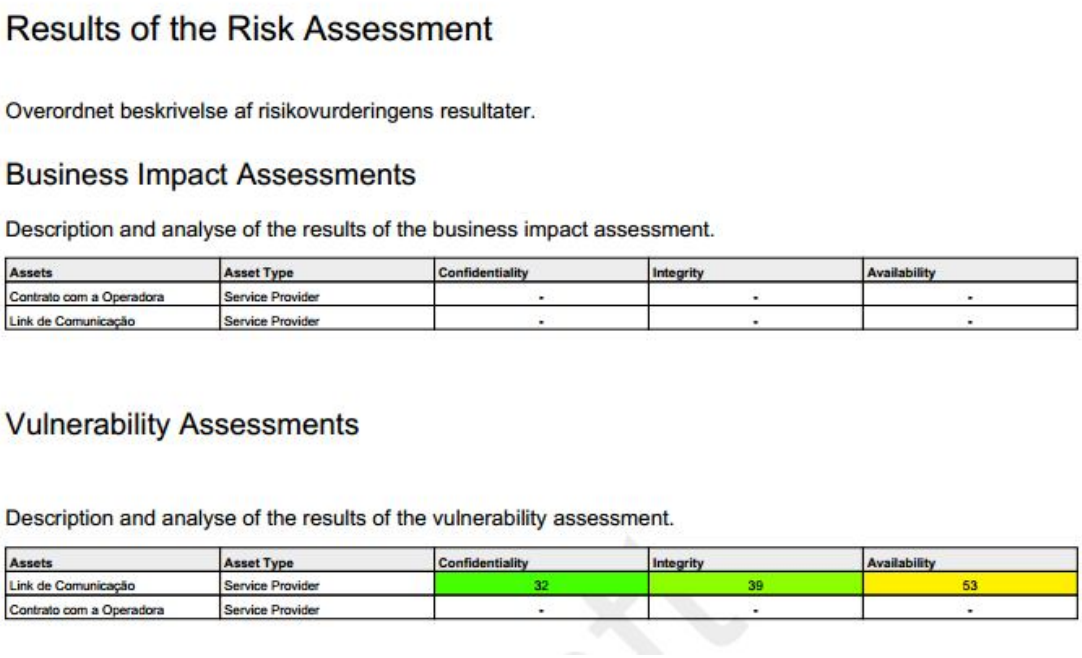
Figura 48: SecureAware - Criação de um projeto de avaliação

Dentro de *Assessments* existe o painel de avaliações (*Assessment Dashboard*) e a visualização das avaliações disponíveis para o usuário (*My Assessments*).

Em *Assessment Dashboard*, são apresentados gráficos com a situação dos projetos e avaliações. São listados os projetos em andamento, que podem ser editados. Para cada um deles existe a opção *Quick Reports* que gera um relatório do projeto. Neste relatório é mostrado o resultado da avaliação do projeto (figura 50).

Em *My Assessments*, são listadas, para cada ativo do projeto, as avaliações

por impacto no negócio, probabilidade e vulnerabilidades, conforme o método de avaliação escolhido na criação dos projetos (figura 51).



Results of the Risk Assessment

Overordnet beskrivelse af risikovurderingens resultater.

Business Impact Assessments

Description and analyse of the results of the business impact assessment.

Assets	Asset Type	Confidentiality	Integrity	Availability
Contrato com a Operadora	Service Provider	-	-	-
Link de Comunicação	Service Provider	-	-	-

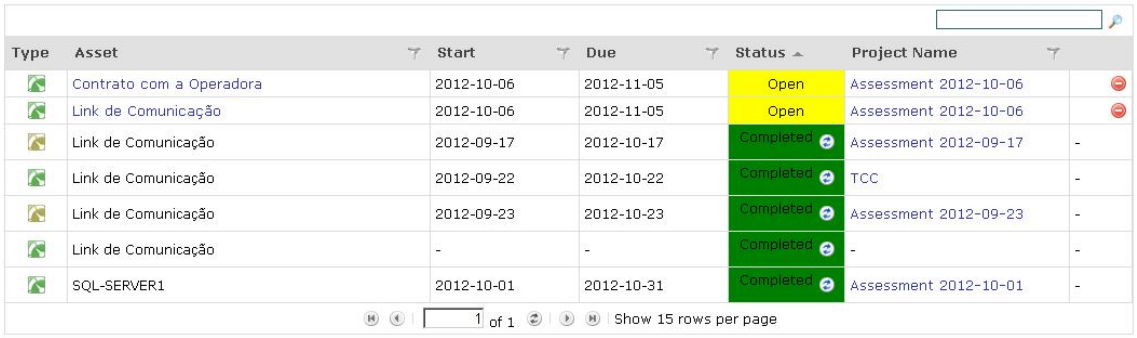
Vulnerability Assessments

Description and analyse of the results of the vulnerability assessment.

Assets	Asset Type	Confidentiality	Integrity	Availability
Link de Comunicação	Service Provider	32	39	53
Contrato com a Operadora	Service Provider	-	-	-

Figura 49: SecureAware - Quick Reports

Para ambos os tipos de métodos, as avaliações podem ser feitas por alto nível ou detalhadas de acordo com a parametrização no momento da criação do projeto. Por exemplo, para o caso do impacto no negócio, na visão de alto nível, são avaliadas as violações de confidencialidade, integridade e disponibilidade para todos os impactos de uma forma geral (figura 52). Já, no caso da visão detalhada, é definida a confidencialidade, integridade e disponibilidade para cada um dos impactos (figura 53). Um processo semelhante ocorre para as avaliações por probabilidade.



Type	Asset	Start	Due	Status	Project Name	
	Contrato com a Operadora	2012-10-06	2012-11-05	Open	Assessment 2012-10-06	
	Link de Comunicação	2012-10-06	2012-11-05	Open	Assessment 2012-10-06	
	Link de Comunicação	2012-09-17	2012-10-17	Completed	Assessment 2012-09-17	-
	Link de Comunicação	2012-09-22	2012-10-22	Completed	TCC	-
	Link de Comunicação	2012-09-23	2012-10-23	Completed	Assessment 2012-09-23	-
	Link de Comunicação	-	-	Completed	-	-
	SQL-SERVER1	2012-10-01	2012-10-31	Completed	Assessment 2012-10-01	-

1 of 1 | Show 15 rows per page

Figura 50: SecureAware – Tela My Assessments

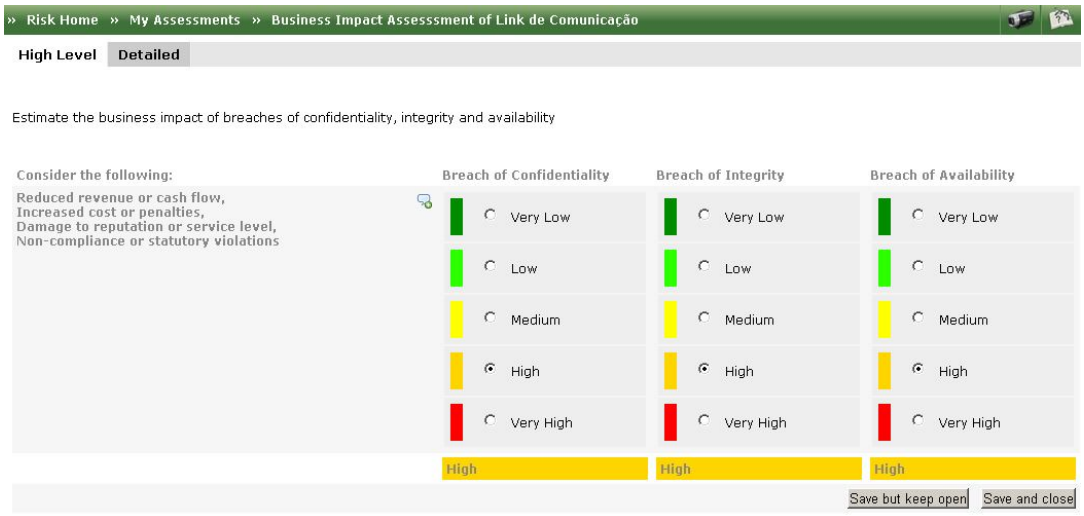


Figura 51: SecureAware - Visão de alto nível da avaliação por impacto no negócio

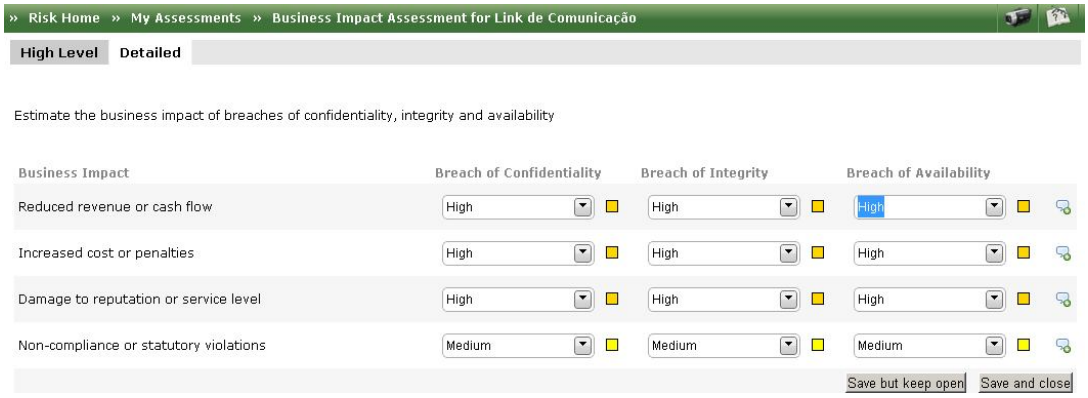


Figura 52: SecureAware - Visão detalhada da avaliação por impacto no negócio

Para a avaliação por vulnerabilidade é preciso definir os valores para os controles de prevenção administrativa, de prevenção técnica, de correção administrativa e de técnica (figura 54). Para os controles de prevenção administrativa e correção administrativa (colunas 1 e 3) pode ser escolhido um dentre os status: otimizado, administrado, definido, repetível e Ad hoc (Controles administrativos para enfrentar as ameaças ou os seus impactos não são sistemáticos).

E para os controles de prevenção técnica e correção técnica (colunas 2 e 4_ pode ser escolhido um dentre os status: Muito efetivo, Efetivo, Implementado, Parcialmente implementado e Inexistente.

Figura 53: SecureAware - Visão de alto nível da avaliação por vulnerabilidade

A quarta opção é a de resultados, que engloba o painel de riscos (*Risk Dashboard)*, a imagem dos riscos (*Risk Picture)*, a lista de riscos (*Risk List)* e os relatórios de riscos (*Risk Reports)*.

O cálculo do impacto de ameaças e de impacto no negócio é feito para a confidencialidade, integridade e disponibilidade, baseado nos seguintes dados de entrada:

(a) Freqüência da ameaça;

(b) Impacto da freqüência;
(c) Eficiência da prevenção administrativa
(d) Eficiência da prevenção técnica
(e) Eficiência da correção administrativa
(f) Eficiência da correção técnica
(g) Impacto para o negócio

A partir destes, os valores que seguem são calculados:

(a) Eficiência preventiva
(b) Eficiência da correção
(c) Probabilidade do incidente
(d) Impacto no ativo
(e) Risco do ativo
(f) Risco de negócio

A documentação do software para o método dos cálculos é bastante detalhada e inclui todas as fórmulas utilizadas para chegar aos resultados finais. Os resultados são obtidos conforme ilustra a figura 55.

O Painel de riscos exibe através de gráficos coloridos os estados dos ativos quanto aos atributos de disponibilidade, integridade e confidencialidade, indicando os com maior e menor risco em cada um destes atributos, de acordo com os valores definidos anteriormente (figura 56). Ativos em verde têm menor risco enquanto ativos em vermelho têm maior risco. Ao clicar nos ativos, são apresentados os detalhes dos ativos, com os valores dos riscos calculados.

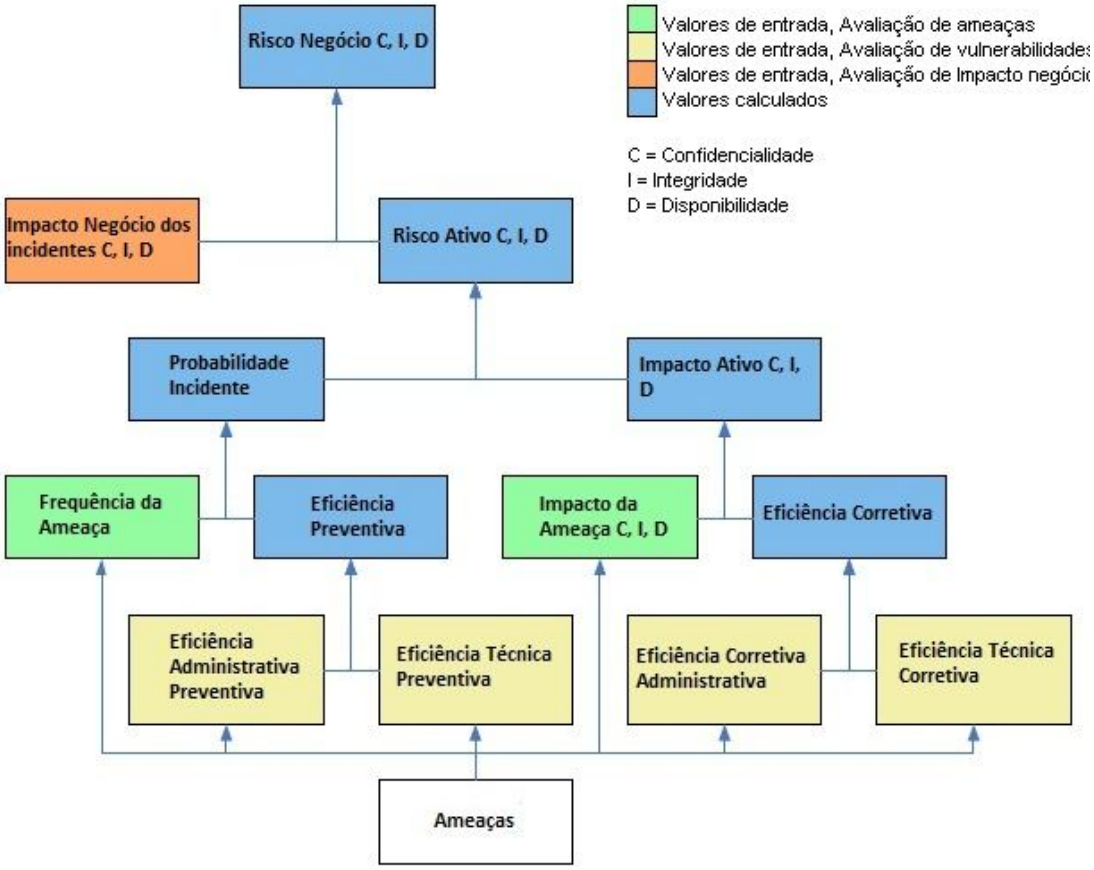


Figura 54: SecureAware - Método de cálculo dos riscos

Ao calcular os valores de um ativo, são levados em consideração os valores das avaliações dos ativos relacionados a este.

Na opção de imagem dos riscos (*Risk Picture*) são listados os tipos dos ativos e o seu nível de riscos, representados através de uma escala de cores, onde o vermelho é quando o ativo possui alto risco (figura 57). Ao clicar no nível de riscos de cada tipo de ativo, é aberta a mesma tela de detalhamento utilizada pelo painel de riscos (figura 58). Nesta tela podem ser encontradas as causas para os riscos, que podem ser decorrentes dos impactos herdados dos ativos relacionados.

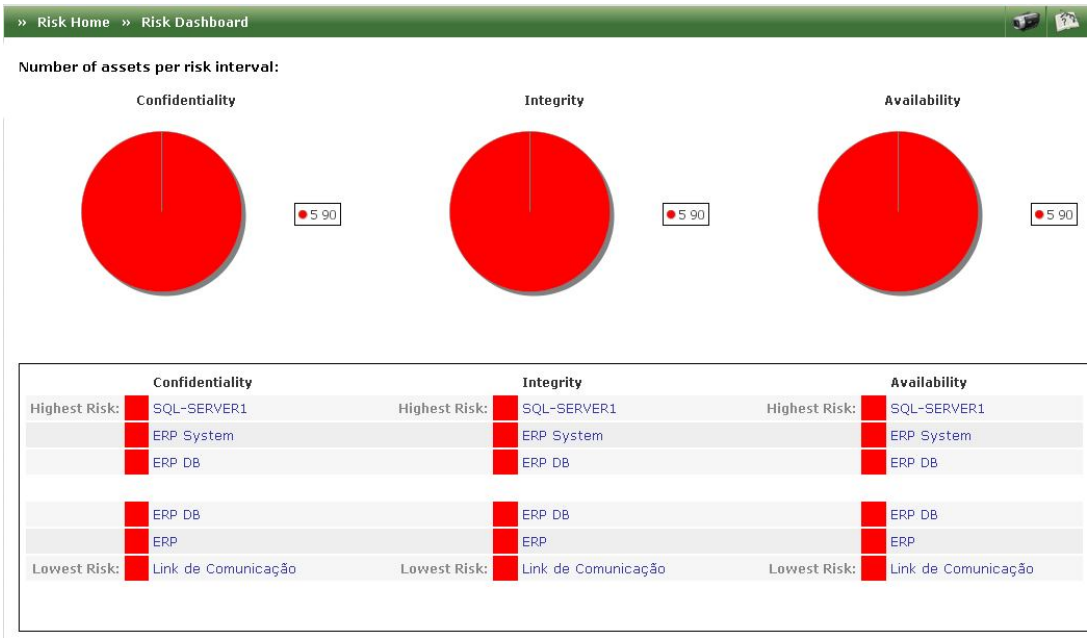


Figura 55: SecureAware - Painel de riscos

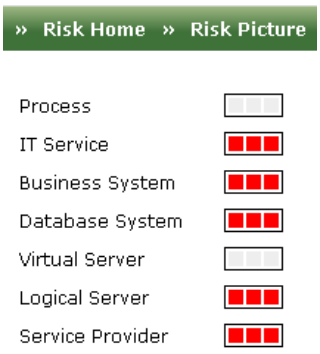


Figura 56: SecureAware - Lista de riscos

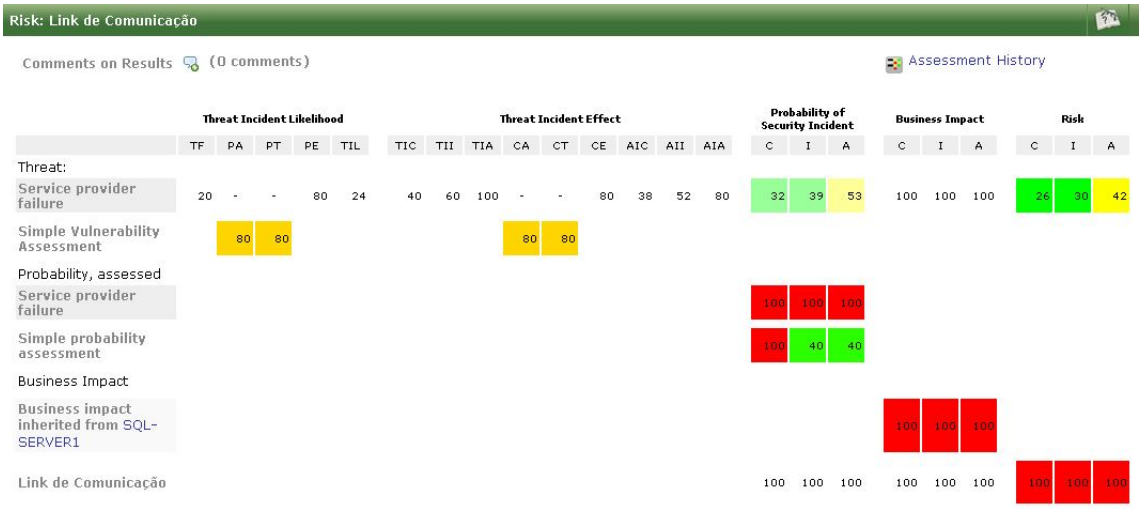


Figura 57: SecureAware - Cálculo dos riscos para o ativo

Os relatórios do SecureAware podem ser gerados utilizando as *templates* definidas, assim como podem ser criadas novas, podendo ser customizadas para conter as informações necessárias para o tratamentos dos riscos. Os relatórios são semelhantes aos *Quick Reports* presentes no painel de avaliações (*Assessment Dashboard*).

O SecureAware também possui um módulo para o tratamento dos riscos, porém, esta funcionalidade não é disponibilizada nesta versão de avaliação, portanto, não pôde ser testada.

5 AVALIAÇÃO DE SOFTWARES DE GESTÃO DE RISCOS

5.1 MÉTODO ANALÍTICO HIERÁRQUICO

O Método Analítico Hierárquico (*Analytic Hierarchy Process*) foi utilizado neste trabalho como forma de avaliação dos softwares de gestão de riscos pesquisados. Este método foi desenvolvido no início da década de 70 por Tomas L. Saaty, sendo fundamentado por conceitos da Álgebra Relacional, da Pesquisa Operacional e da Psicologia, e é um importante instrumento para a tomada de decisões multicritério (GUGLIELMETTI, MARINS e SALOMON, 2003).

O Método Analítico Hierárquico (MAH) se diferencia de outros métodos por aceitar variáveis quantitativas e qualitativas, tornando possível dar valores até mesmo para dados subjetivos (MORAES e SANTALIESTRA, 2008). É um método simples, porém confiável, que facilita a tomada de decisões considerando várias alternativas, baseando-se nos critérios definidos com diferentes pesos (JORDÃO e PEREIRA, 2006).

O MAH pode ser utilizado de várias formas, uma delas é a proposta por Jordão e Pereira (2006), que é de fácil aplicação e usa comparações de matrizes simplificadas. O trabalho será baseado no trabalho de Silveira (2011), que utiliza a forma proposta por Jordão e Pereira (2006). Nesta proposta a aplicação do MAH é composta por seis etapas: (1) Definição do Problema; (2) Estruturação Hierárquica do Problema; (3) Construção de Matrizes de Avaliação; (4) Normalização das Matrizes; (5) Construção das Matrizes de Prioridades e (6) Obtenção dos Resultados:

Na etapa de definição do problema, o problema é entendido como o objetivo a ser atingido através do cruzamento e comparação de todos os critérios entre as diversas alternativas analisadas (figura 7).

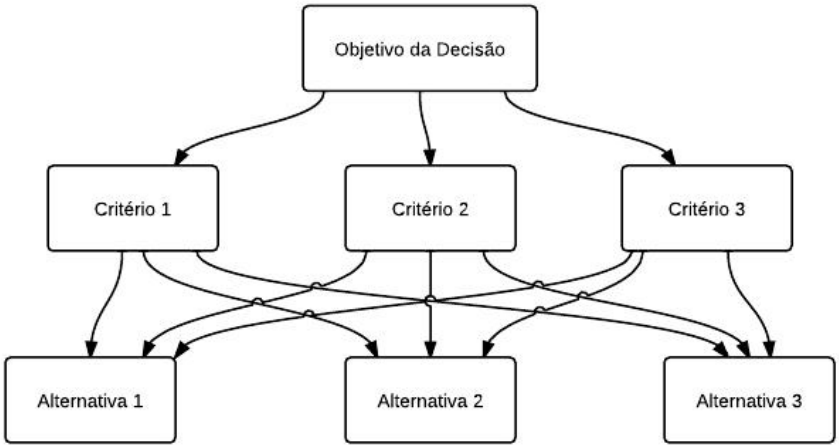


Figura 58: Método Analítico Hierárquico

A segunda etapa, a estruturação hierárquica do problema é representada através de um diagrama composto por diferentes níveis. O nível mais externo da estrutura é a meta final, enquanto nos níveis intermediários são listados os critérios de avaliação, chamados de Objetivos e Subobjetivos. Cada alternativa é interligada com esta estrutura, de modo que todas as alternativas sejam avaliadas de acordo com todos os critérios estabelecidos (MORAES e SANTALIESTRA, 2008).

A Construção de Matrizes de Avaliação é a terceira etapa e trata-se do cruzamento dos critérios de avaliação definidos com todas as alternativas em análise. Duas matrizes são construídas, uma estabelecendo os pesos dos critérios e outra o impacto das alternativas sobre os critérios. Com o cruzamento das matrizes serão feitas comparações binárias para atingir a meta final (MORAES e SANTALIESTRA, 2008).

Na matriz de avaliação, cada célula recebe um valor representando o peso da alternativa ou critério em comparação com os demais. Um item de uma linha com prioridade sobre o item de uma coluna resultará um valor elevado para a célula

equivalente. Mas se um item de uma coluna tem prioridade sobre o item definido na linha, um valor proporcionalmente inferior será atribuído à célula. Se ambos os itens possuam a mesma prioridade, é atribuído o valor 1. No cruzamento entre linha e coluna do mesmo item o resultado sempre é 1 (SALOMON, 2002).

A Escala Fundamenta de Comparações (tabela 6) é a base para atribuição dos pesos, sendo que quanto maior o peso de uma alternativa, maior é o valor atribuído a célula correspondente.

Tabela 7: Escala Fundamental de Comparações

Intensidade da Importância	Definição	Explicação
1	Igual Importância	As duas atividades contribuem igualmente para o objetivo.
3	Fraca importância	A experiência e o julgamento favorecem levemente uma atividade em relação à outra.
5	Forte importância	A experiência e o julgamento favorecem fortemente uma atividade em relação à outra.
7	Importância muito forte	Uma atividade é fortemente favorecida em relação à outra; sua dominação de importância é demonstrada na prática.
9	Importância absoluta	A evidência favorece uma atividade em relação à outra com o mais alto grau de certeza.
2, 4, 6 e 8	Valores intermediários	Quando se procura uma condição e compromisso entre duas definições.
Recíproco dos valores	Se a atividade i recebe uma das designações diferentes de zero, quando comparada com a atividade j, então j tem o valor recíproco quando comparada com i.	Uma designação razoável

Fonte: SAATY, 1995 *apud* JORDÃO; PEREIRA, 2006

A matriz de avaliação para comparação entre os pesos de dois critérios de

avaliação distintos é representada na tabela 7, onde o “Critério 1” possui peso 1 e o “Critério 2” possui peso 6. Quando o critério da linha é igual ao da coluna, é atribuído o peso 1 à célula. Se o critério da linha é superior ao da coluna, é atribuído 6 á célula. Mas se o critério da linha for inferior ao da coluna, é atribuído o peso 1/6.

Tabela 8: Comparação Binária de Critérios

	Critério 1	**Critério 2**
Critério 1	1	1/6
Critério 2	6	1

Fonte: Jordão e Pereira (2006)

Uma matriz de avaliação semelhante é elaborada para as alternativas, como expressado na tabela 8. Nesta representação a “Alternativa 1” possui peso 1, e a “Alternativa 2” possui peso 6, ambas para o mesmo critério de avaliação. A comparação é feita da mesma forma que para os critérios.

Tabela 9: Comparação Binária de Alternativas

	Alternativa 1	**Alternativa 2**
Alternativa 1	1	1/6
Alternativa 2	6	1

Fonte: Jordão e Pereira (2006)

Com estas matrizes elaboradas, é feita a normalização das matrizes, que se trata de operações matemáticas aplicadas a cada coluna. A normalização é feita dividindo os elementos de cada matriz pela soma da coluna a qual pertence, de modo que a soma de todos os seus elementos seja igual a 1. Depois as frações são convertidas em números decimais para encontrar a média aritmética de cada linha da matriz normalizada.

A soma das colunas é apresentada na tabela 9. Na tabela 10, cada elemento da matriz é dividido pela soma encontrada anteriormente e, ao se somar o resultado de cada coluna, deve totalizar 1. Com os novos valores para os elementos da matriz é obtida a média de cada linha. O cálculo da média é feito dividindo o valor de cada célula pela soma de sua coluna, os valores resultantes são somados e divididos pelo número de elementos.

Tabela 10: Normalização da Matriz

	Alternativa 1	**Alternativa 2**
Alternativa 1	1	1/6
Alternativa 2	6	1
	(1 + 6) = 7	(1/6 + 1) = 7/6

Fonte: Jordão e Pereira (2006)

Tabela 11: Normalização da Matriz e Cálculo da Média

	Alternativa 1	**Alternativa 2**	**Média**
Alternativa 1	(1/7) = 1/7	[(1/6) / (7/6)] = 1/7	0,143
Alternativa 2	(6/7) = 6/7	[1 / (7/6)] = 6/7	0,857
	(1/7 + 6/7) = 1	(1/7) + (6/7) = 1	

Fonte: Jordão e Pereira (2006)

Os resultados da normalização das matrizes servirão de base para a Matriz de Prioridades, que é a matriz que lista todas as alternativas e critérios em um único grupo de dados. As linhas representam as alternativas e as colunas os critérios de avaliação. O valor da média encontrado anteriormente é atribuído para cada célula (tabela 11).

Os resultados finais são obtidos através da multiplicação da matriz com o peso dos critérios pela matriz do impacto das alternativas. O resultado será um vetor

com a média final de cada alternativa em relação aos critérios avaliados, assim, a alternativa com a maior média representa a melhor escolha.

Tabela 12: Matriz de Prioridades

	Critério 1
Alternativa 1	0,143
Alternativa 2	0,857

Fonte: Jordão e Pereira (2006)

Como se sabe, o MAH é uma respeitada e importante ferramenta para a avaliação de alternativas por critérios e vem sendo amplamente utilizada para o auxílio à tomada de decisões.

O MAH é baseado em cálculos para determinar os pesos de cada alternativa considerando os critérios estabelecidos, possibilitando que se identifique as melhores alternativas, auxiliando na avaliação dos softwares de gestão de riscos. Como parte deste trabalho é definir critérios para a avaliação dos softwares, serão calculados, através do MAH, os pesos para cada um destes critérios, e após serão calculadas, com este método, as médias de cada alternativa, que representam os softwares, de modo a encontrar o mais adequado.

5.2 COMPARAÇÃO DOS SOFTWARES UTILIZANDO O MÉTODO ANALÍTICO HIERÁRQUICO

Para realizar a avaliação dos softwares através do método analítico hierárquico, foram definidos treze critérios, cada qual com seu peso para o cálculo de comparação.

De acordo com os conceitos de Gestão de Riscos estudados anteriormente, e principalmente através das comparações das metodologias, alguns critérios mostram-se de fundamental importância para a avaliação dos softwares para

qualquer uma das metodologias analisadas:

(a) **Identificação e definição dos valores dos ativos:** o software deve possibilitar que os ativos sejam classificados de acordo com o seu grau de importância, permitindo no mínimo três formas de classificação: alta, média e baixa. Também deve separá-los conforme seu tipo (primários ou de suporte e infraestrutura) e suas avaliações quanto à disponibilidade, confidencialidade e integridade.

(b) **Identificação de ameaças:** o software deve permitir que se cadastre e identifique as ameaças que possam comprometer os ativos, podendo ser classificadas como intencionais, acidentais ou naturais.

(c) **Identificação de vulnerabilidades:** o software também deve identificar as vulnerabilidades existentes relacionando-as com os ativos e ameaças. É importante que as vulnerabilidades possam ser cadastradas ou alteradas.

(d) **Identificação de controles:** o software deve possuir uma manutenção de controles e possibilitar que estes sejam incluídos relacionando-os com ameaças, vulnerabilidades e ativos.

(e) **Biblioteca do software:** este critério avalia a biblioteca do software, analisando se o mesmo já possui uma base consistente previamente definida de ativos, ameaças, vulnerabilidades e controles, ou se é necessário realizar o cadastramento destes itens.

(f) **Definição do impacto e do risco:** analisar se o software permite determinar o valor do impacto e do risco através dos métodos qualitativo e quantitativo, bem como a probabilidade do ativo ser afetado.

(g) **Histórico de incidentes:** verificar se o software mantém um histórico dos incidentes ocorridos relacionando-os com os ativos afetados e o tratamento realizado.

(h) **Capacidade de adaptação às mudanças:** é importante que o software consiga adaptar-se em caso de mudanças de ameaças, vulnerabilidades, valores de ativos, controles, recalculando os valores dos riscos quando necessário e de forma automática, além sugerir

controles e listar os ativos relacionados quando ocorrer alguma alteração de vulnerabilidades, ameaças ou controles.

(i) **Dependência dos ativos:** analisar se os ativos podem ser relacionados entre si criando assim dependências entre eles. Verificar se um ativo dependente sofrerá alterações caso os ativos a que depende forem alterados.

(j) **Tratamento do risco:** o software deve prover recomendações para o tratamento dos riscos, indicando controles a serem implementados e realizar a priorização das ações a serem realizadas para eliminar ou tornar os riscos a níveis aceitáveis para a organização.

(k) **Usabilidade do software:** este critério avalia se o software é amigável, intuitivo e de fácil uso.

(l) **Relatórios gerados:** os relatórios gerados pelo software podem ser de grande utilidade para a avaliação e tratamento dos mesmos, ou mesmo uma forma de mostrar à alta direção as necessidades de controles a serem implementados. Este critério avalia as informações contidas nos relatórios dos softwares, e se trazem informações relevantes para o tratamento dos riscos.

(m) **Documentação do software:** para um melhor entendimento do funcionamento e dos processos utilizados pelo software, é importante que a documentação seja detalhada e auxilie o usuário a utilizá-lo. Detalhes sobre as metodologias e fórmulas de cálculos empregados podem ser úteis para o processo de gestão de riscos de uma organização.

Os valores dos pesos dos critérios não foram calculados através do MAH, mas definidos de acordo com a sua relevância, de acordo com o estudado, para o processo de gestão de riscos e para os objetivos deste trabalho (tabela 13). Estes pesos serão multiplicados pelas médias obtidas para cada um dos critérios, onde o maior resultado final indicará o melhor software.

Tabela 13: Critérios de avaliação dos softwares

Legenda	Critério	Peso
C1	**Identificação e definição dos valores dos ativos**	**7**
C2	**Identificação de ameaças**	**7**
C3	**Identificação de vulnerabilidades**	**7**
C4	**Identificação de controles**	**6**
C5	**Biblioteca do software**	**7**
C6	**Definição do impacto e do risco**	**7**
C7	**Histórico de incidentes**	**6**
C8	**Capacidade de adaptação às mudanças**	**9**
C9	**Dependência dos ativos**	**9**
C10	**Tratamento do risco**	**9**
C11	**Usabilidade do software**	**6**
C12	**Relatórios gerados**	**7**
C13	**Documentação do software**	**6**

O método analítico hierárquico será a forma de avaliação comparando cada software com todos, em uma matriz. Quando um software de uma linha é comparado com o mesmo software é atribuído valor 1. Se o software da linha possui a mesma avaliação que o software da coluna, também será atribuído 1 como valor. Se o software da linha possuir melhor avaliação que o da coluna, recebera um valor superior a 1, de acordo com a escala fundamental de comparações (tabela 6). E se o software da coluna possuir uma avaliação superior ao da linha, seu valor será 1/9, por exemplo, de acordo com o grau de superioridade. Para tornar mais simples as comparações serão utilizados valores padrões para a realização das comparações, sendo 9 para casos onde haja grande superioridade por parte de um software para outro, e 6 para casos onde exista a superioridade mas de forma mais intermediária.

A última linha das tabelas utilizadas para as comparações representa a soma de casa coluna. Esta soma será empregada para o cálculo da média, que é a coluna mais a direita da tabela. O cálculo da média, para cada linha, é realizado da seguinte forma: ((valor da linha 1 / soma coluna 1) + (valor da linha N / soma coluna N)) / N, para N de 1 até o número de elementos.

Critério 1: Identificação e definição dos valores dos ativos

Todos os softwares possuem uma manutenção para os ativos associando a

eles o seu respectivo tipo, mas a identificação e definição dos valores dos ativos são feitas de formas diferentes por cada um deles. Nem todos, porém, têm a opção de classificação de disponibilidade, confidencialidade e integridade dos ativos. De acordo com as características dos softwares foi construída uma matriz comparando-os utilizando o Método Analítico Hierárquico para avaliá-los (tabela 14). Os softwares que obtiveram melhor média neste critério foram o SOBF e o SecureAware. O SOBF, além de permitir que seja informado um valor para o ativo, o mesmo pode ser classificado de acordo com seu tipo e sua disponibilidade, integridade e confidencialidade. Semelhante ao SOBF, o SecureAware também permite classificar o ativo por tipos, e ainda por sua criticidade no negócio e nível de confidencialidade. É possível escolher dentre algumas faixas de valores, que podem ser customizadas, qual valor financeiro se enquadra ao ativo.

O VS Risk não atribui um valor financeiro para o ativo, mas sim o valor do impacto que o mesmo representa para a organização, a ser selecionado em uma escala qualitativa de 1 a 7. O valor dos ativos pode ser uma informação importante para a priorização dos tratamentos dos riscos. Além disto, o VS Risk para cada ativo incluído, possibilita que sejam avaliados os atributos de confidencialidade, integridade e disponibilidade dos requisitos legais, contratuais e de negócio. Neste aspecto é mais completo, mas a separação dos requisitos pode tornar-se complexa dependendo do caso.

Por outro lado, o STREAM não associa nenhum tipo de valores aos ativos, sejam financeiros, de impacto ou classificações por confidencialidade, disponibilidade e integridade, por esta razão, obteve neste critério a pior média dentre os softwares testados. Os valores apenas são indicados nas ameaças dos ativos, através do impacto financeiro que representam.

Tabela 14: Matriz de avaliação para o critério C1

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	1	6	1/9	1/9	0,09
STREAM	1/6	1	1/9	1/9	0,03
SOBF	**6**	**9**	**1**	**1**	**0,42**
SecureAware	**6**	**9**	**1**	**1**	**0,42**
Soma	13,16	25	2,22	2,22	

Critério 2: Identificação de ameaças

Todos os softwares testados possuem uma manutenção para a inclusão e edição das ameaças, porém, possuem diferenças na forma como estas ameaças são associadas aos ativos. O VS Risk, o SOBF e o STREAM fazem o relacionamento das ameaças com os ativos simplesmente ligando diretamente uns aos outros. O SecureAware, na manutenção de ameaças, relaciona cada ameaça com um tipo de ativo, o que faz com que todos os ativos do tipo relacionado tornem-se vinculados com a ameaça (tabela 15).

No VS Risk é informada, qualitativamente, a probabilidade da ameaça comprometer o ativo. No SOBF a relação entre a ameaça e o ativo se dá através da inclusão de vulnerabilidades do ativo, onde é informada a ameaça da vulnerabilidade. No SecureAware, cada ameaça possui determinada frequência e classificação de impacto, que podem causar à disponibilidade, integridade e confidencialidade dos tipos de ativos relacionados, com base nestes valores será calculado o risco dos ativos. As ameaças são relacionadas às fontes de ameaças, cuja manutenção também pode ser realizada. No STREAM, depois de relacionadas as ameaças aos ativos, pode-se informar a probabilidade de ocorrência e o valor de impacto no negócio que a ameaça pode trazer, representada como um valor financeiro.

Tabela 15: Matriz de avaliação para o critério C2

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	1	1	1	1/6	0,10
STREAM	1	1	1	1/6	0,10
SOBF	1	1	1	1/6	0,10
SecureAware	**6**	**6**	**6**	**1**	**0,66**
Soma	9	9	9	1,48	

Critério 3: Identificação de vulnerabilidades

O VS Risk e o SOBF têm formas similares de tratarem com as vulnerabilidades. Ambos possuem uma manutenção para a inclusão e edição das vulnerabilidades, e estas são associadas às ameaças e ativos.

O SecureAware possui uma visão diferente das vulnerabilidades. Existem os projetos de avaliação por vulnerabilidades dos ativos. A avaliação das vulnerabilidades funciona verificando se, para cada ameaça do ativo, as medidas e controles corretivos e preventivos são eficazes para prevenir as ameaças. Assim, as vulnerabilidades não são especificadas, e não possui uma manutenção para as mesmas. Já no STREAM, as vulnerabilidades podem ser incluídas a um grupo ou a um registro de riscos, porém, não possui a funcionalidade de uma manutenção para as vulnerabilidades, por isso são informadas através de um campo de texto livre (tabela 16).

Tabela 16: Matriz de avaliação para o critério C3

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	**1**	**9**	**1**	**6**	**0,42**
STREAM	1/9	1	1/9	1/6	0,03
SOBF	**1**	**9**	**1**	**6**	**0,42**
SecureAware	1/6	6	1/6	1	0,11
Soma	2,27	25	2,27	13,16	

Critério 4: Identificação de controles

Quanto aos controles, o VS Risk, o STREAM e o SOBF possuem uma manutenção para a inclusão e edição dos controles, bem como os relacionam com os ativos. O VS Risk e o STREAM são semelhantes ao calcular novamente o risco após a associação dos controles. O VS Risk solicita que se informem novamente os níveis de impacto e probabilidade do risco e no STREAM deve ser informado o percentual de redução do risco para assim ser recalculado o valor do risco. Também no STREAM, é associado aos controles o percentual de seu desenvolvimento, para acompanhamento. Enquanto no VS Risk é informado se é um controle planejado ou já implementado.

O SOBF relaciona os controles às ameaças, vulnerabilidades e ao ativo e solicita que seja informado o quão efetivo é o controle. Como os três softwares mostram similaridades quanto à identificação dos controles, ambos alcançaram igualmente a melhor média (tabela 17), enquanto o SecureAware que, por sua vez, na versão testada, não contempla o módulo de tratamento de riscos, desta forma, não faz a utilização de controles, embora mencione na avaliação por vulnerabilidades controles de prevenção administrativa, de prevenção técnica, de correção administrativa e de técnica, porém, sem especificá-los.

Tabela 17: Matriz de avaliação para o critério C4

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	**1**	**1**	**1**	**9**	**0,32**
STREAM	**1**	**1**	**1**	**9**	**0,32**
SOBF	**1**	**1**	**1**	**9**	**0,32**
SecureAware	1/9	1/9	1/9	1	0,03
Soma	3,11	3,11	3,11	28	

Critério 5: Biblioteca do software

A avaliação da tabela 18 quanto ao critério da biblioteca do software aponta que o VS Risk é o software que possui de forma mais completa as ameaças, vulnerabilidades e controles, previamente cadastrados. O SecureAware e o SOBF também possuem uma base considerável e por isto ficaram nas posições seguintes com médias iguais, enquanto o STREAM, na versão de testes, possui principalmente dados fictícios de exemplo, o que justifica a menor média para este critério. Porém, é importante ressaltar que os testes foram efetuados em versões de avaliação dos softwares, o que pode implicar em limitações por parte destes. Além disto, todas as informações dos softwares estão em inglês, o que pode requerer um recadastramento para adaptá-las a outros idiomas.

Tabela 18: Matriz de avaliação para o critério C5

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	**1**	**9**	**6**	**6**	**0,63**
STREAM	1/9	1	1/6	1/6	0,03
SOBF	1/6	6	1	1	0,15
SecureAware	1/6	6	1	1	0,15
Soma	1,43	22	8,16	8,16	

Critério 6: Definição do impacto e do risco

Cada um dos softwares trata dos valores de impacto ou risco apenas de uma forma, ou qualitativamente ou quantitativamente. No VS Risk, o impacto de um ativo é definido pelo usuário por meio de uma escala qualitativa. Também de forma qualitativa é calculado o risco, considerando os níveis de impacto e probabilidade da ameaça e o calculo é refeito após a associação dos controles. No STREAM os riscos são calculados quantitativamente inicialmente baseados no valor financeiro de impacto ao negócio das ameaças e na probabilidade de ocorrência destas. Após a associação dos controles, o valor do risco é calculado levando em consideração também o percentual de redução com a inclusão destes controles. O SOBF utiliza apenas os métodos qualitativos. O risco é calculado apenas levando em conta o grau de probabilidade e de impacto selecionados, assim ficando com a pior média dos softwares testados. Já o SecureAware utiliza valores de 0 a 100, como resultado dos cálculos de riscos para representá-los. Os cálculos do SecureAware levam em consideração dados de entrada como a freqüência e o impacto das ameaças, a eficiência das prevenções e correções e o impacto para o negócio, entre outros. Por considerar uma gama maior de informações para a realização do cálculo, o SecureAware foi o melhor software neste critério (tabela 19).

Tabela 19: Matriz de avaliação para o critério C6

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	1	1	6	1/6	0,15
STREAM	1	1	6	1/6	0,15
SOBF	1/6	1/6	1	1/9	0,03
SecureAware	**6**	**6**	**9**	**1**	**0,63**
Soma	8,16	8,16	22	1,43	

Critério 7: Histórico de Incidentes

Manter históricos dos incidentes ocorridos para indicar os tratamentos necessários para os riscos seria uma funcionalidade útil para solucioná-los. Neste aspecto nenhum dos softwares executa esta função com tal eficácia. O VS Risk, e o SOBF sequer possuem um registro de histórico de incidentes. Já o SecureAware, que utiliza o conceito de projetos com data de início e término, pode ser apenas uma base para consulta dos riscos calculados anteriormente.

O melhor software com relação a este critério é o STREAM, que possui um histórico dos incidentes ocorridos, mesmo que apenas para consultas posteriores. Além disto, pode gerar relatórios por histórico de riscos, eventos e controles.

Tabela 20: Matriz de avaliação para o critério C7

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	1	1/6	1	1	0,10
STREAM	**6**	**1**	**6**	**6**	**0,66**
SOBF	1	1/6	1	1	0,10
SecureAware	1	1/6	1	1	0,10
Soma	9	1,48	9	9	

Critério 8: Dependência dos ativos

A dependência dos ativos também é um critério que diz respeito à capacidade que o software tem de adaptar-se a mudanças. Neste aspecto, apenas o SecureAware utiliza deste conceito para calcular os riscos de um ativo, considerando também, os valores de outros ativos relacionados. Ao efetuar a manutenção de um ativo, tem-se a possibilidade de incluir os ativos a que este depende, juntamente com o percentual de dependência quanto à confidencialidade, disponibilidade e integridade. Por exemplo: um ativo como um servidor depende de ativos como energia elétrica, ar-condicionado, no-breaks, entre outros. E um ativo

como um determinado sistema irá depender do ativo servidor. Desta forma, ao calcular os valores dos riscos do sistema, serão considerados também a freqüência da ameaça e o impacto que ela traz a confidencialidade, integridade e disponibilidade do servidor.

Nos outros softwares não é feito qualquer relacionamento de dependência de ativos.

Tabela 21: Matriz de avaliação para o critério C8

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	1	1	1	1/9	0,08
STREAM	1	1	1	1/9	0,08
SOBF	1	1	1	1/9	0,08
SecureAware	**9**	**9**	**9**	**1**	**0,75**
Soma	12	12	12	1,33	

Critério 9: Capacidade de adaptação a mudanças

Foi observado que todos os softwares testados são pouco adaptáveis a mudanças, porém, apresentam algumas características importantes. Os valores dos riscos, basicamente são calculados automaticamente baseados nas informações de entrada, mas no VS Risk, no SecureAware e no STREAM, ao serem feitas alterações, como a exclusão ou inclusão de ameaças, vulnerabilidades e controles, isto é automaticamente refletido nos valores dos riscos, de forma direta, sem notificações ao usuário. No SOBF mesmo que se exclua uma vulnerabilidade, por exemplo, os riscos que já a consideravam, não sofrerão alterações e ainda levarão em conta esta vulnerabilidade. Por esta razão, o SOBF não pode ser considerado um software adaptável a mudanças.

O SecureAware leva vantagem neste aspecto pois, como visto no critério 9, os ativos relacionados também possuem influência nos valores dos riscos. Outra característica favorável ao SecureAware neste critério é o modo como relaciona as

ameaças aos ativos. Como as ameaças são relacionadas não diretamente aos ativos, mas sim aos tipos de ativos, se houver a necessidade de alterar o tipo de ativo ou remover a ameaça, todos os ativos deste determinado tipo serão simultaneamente alterados, desconsiderando a ameaça que havia sido relacionada, sem que se precise alterar em cada um deles.

Tabela 22: Matriz de avaliação para o critério C9

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	1	1	6	1/6	0,15
STREAM	1	1	6	1/6	0,15
SOBF	1/6	1/6	1	1/9	0,03
SecureAware	**6**	**6**	**9**	**1**	**0,63**
Soma	8,16	8,16	22	1,43	

Critério 10: Tratamento do risco

O tratamento dos riscos é um critério diretamente ligado com a utilização dos controles pelos softwares, já que estes são indicados para reduzir os riscos existentes. Assim sendo, este critério irá analisar a efetividade dos controles para o tratamento dos riscos.

O SecureAware possui um módulo inteiramente para o tratamento dos riscos, porém, na versão testada esta funcionalidade não está habilitada e portanto não pôde ser avaliada. O restante dos softwares relacionam controles como formas de tratamento, diminuindo assim os riscos dos ativos. O VS Risk e o STREAM, como já detalhados no critério 4, após a inclusão dos controles, realizam um novo cálculo do risco com base na efetividade deste. De forma similar é tratado no SOBF, que solicita que se informe o grau de efetividade dos controles.

Estes softwares, após calcularem os resultados dos riscos e dos controles necessários, funcionam mais como um guia das ações que devem ser tomadas para a redução dos riscos, sem proverem maior efetividade para o tratamento do risco.

No STREAM, porém, existe um melhor controle em relação a isto, pois, podem ser definidos e acompanhados os estados de implementação dos controles. Através de avaliações dos controles, que podem ser feitas periodicamente, com datas a serem definidas, verifica-se os estados dos controles e atualiza-os, caso necessário.

Tabela 23: Matriz de avaliação para o critério C10

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	1	1/6	1	9	0,17
STREAM	**6**	**1**	**6**	**9**	**0,66**
SOBF	1/6	1/6	1	9	0,14
SecureAware	1/9	1/9	1/9	1	0,03
Soma	7,27	1,43	7,27	28	

Critério 11: Usabilidade do software

O software que obteve a melhor média quanto a sua usabilidade foi o VS Risk, por ser o mais intuitivo e fácil de utilizar. Entretanto, algo que pode dificultar o seu uso, é a divisão dentro de cada ativo, como já mencionado no critério 1, onde são separados os riscos para cada requisito legal, contratual e de negócio, para a confidencialidade, integridade e disponibilidade. Com média inferior ao VS Risk, o SecureAware também, em grande parte do software, permite uma fácil utilização, além de contar com a opção de ajuda para maiores detalhes sobre cada uma das funcionalidades. Um de seus problemas são as avaliações por impacto no negócio, vulnerabilidade e probabilidade, que podem complicar a utilização do mesmo. O ponto positivo do STREAM são as informações da tela inicial representadas em gráficos, o que pode facilitar o acesso, mas algo que pode dificultar o seu uso é a forma de utilizar vários níveis (empresa, grupo, registro de riscos, riscos) até chegar ao risco propriamente dito. Já o SOBF não é muito intuitivo e suas funcionalidades não são colocadas na mesma ordem que as operações devem ser realizadas.

Tabela 24: Matriz de avaliação para o critério C11

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	**1**	**6**	**9**	**6**	**0,58**
STREAM	1/6	1	6	1/6	0,11
SOBF	1/9	1/6	1	1/9	0,03
SecureAware	1/6	6	9	1	0,26
Soma	1,43	13,16	25	7,27	

Critério 12: Relatórios gerados

Em relação aos relatórios gerados pelo software, o SecureAware é o que os gera de forma mais detalhada, tanto em gráficos como em texto e ainda pode ser customizado de acordo com a necessidade. O STREAM gera apenas relatórios gráficos, permitindo a visualização de dados importantes para o tratamento dos riscos como: a visualização dos 10 maiores riscos, os estados dos controles, históricos de riscos e controles e o andamento dos tratamentos dos riscos. Os gráficos em 3D gerados facilitam a visualização, embora alguns dados seriam melhor explorados se exibidos em forma de texto.

Já o VS Risk, lista apenas detalhes sobre os riscos das ameaças, relacionando às vulnerabilidades e aos controles. E por último, o SOBF possui relatórios mais simples de ativos, vulnerabilidades, controles e avaliação de riscos. O relatório de avaliação de riscos exibe um resumo para cada ativo relacionando as vulnerabilidades, ameaças, probabilidade, impacto e o valor do risco.

Tabela 25: Matriz de avaliação para o critério C12

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	1	1/6	6	1/6	0,12
STREAM	6	1	6	1/6	0,24
SOBF	1	1/6	1	1/6	0,06
SecureAware	**6**	**6**	**6**	**1**	**0,55**
Soma	14	7,32	19	1,48	

Critério 13: Documentação do software

Quanto a documentação do software, as mais detalhadas e de fácil entendimento são as do VS Risk e do SecureAware. O VS Risk em sua documentação explica detalhes sobre a configuração e o uso do software, utilizando imagens para exemplificar. Um pouco mais completo, o SecureAware disponibiliza no *site* do fabricante os manuais para *download,* de forma bastante completa com ilustrações para facilitar o entendimento. Além disto, cada tela do software possui um botão de ajuda que mostra um texto explicando cada funcionalidade. As fórmulas para os cálculos dos riscos são bem detalhadas na documentação do software. O STREAM traz bastante informações sobre como utilizar o software, mas sem ilustrá-las. Por último o SOBF, que como ainda está em desenvolvimento, possui documentação incompleta para algumas das funcionalidades.

Tabela 26: Matriz de avaliação para o critério C13

Software	VS Risk	STREAM	SOBF	SecureAware	Média
VS Risk	**1**	**6**	**9**	**1**	**0,42**
STREAM	1/6	1	6	1/6	0,11
SOBF	1/9	1/6	1	1/9	0,03
SecureAware	**1**	**6**	**9**	**1**	**0,42**
Soma	2,27	13,16	25	2,27	

5.3 RESULTADO DAS AVALIAÇÕES

Após a avaliação individual dos softwares utilizando o MAH, o resultado final das avaliações foi calculado.

Para realizar o cálculo foi construída uma matriz com as médias encontradas para cada um dos critérios. Para facilitar a visualização, as linhas representam os critérios e as colunas os softwares (tabela 27). A última coluna indica o peso de cada critério, que será utilizado para calcular o valor final de cada software.

Para calcular o valor total de um software, é feito o somatório da multiplicação de todos os critérios pela sua média, resultando no valor final para cada software. Os maiores valores indicam os melhores softwares.

Tabela 27: Matriz de médias dos critérios

Critérios	VS Risk	STREAM	SOBF	SecureAware	Peso Critério
C1 – Ident. e definição dos valores dos ativos	0,09	0,03	**0,42**	**0,42**	7
C2 – Ident. de ameaças	0,10	0,10	0,10	**0,66**	7
C3 – Ident. de vulnerabilidades	**0,42**	0,03	**0,42**	0,11	7
C4 – Ident. de controles	**0,32**	**0,32**	**0,32**	0,03	6
C5 - Biblioteca do software	**0,63**	0,03	0,15	0,15	7
C6 - Definição do impacto e do risco	0,15	0,15	0,03	**0,63**	7
C7 - Histórico de incidentes	0,10	**0,66**	0,10	0,10	6
C8 - Capacidade de adaptação às mudanças	0,08	0,08	0,08	**0,75**	9
C9 - Dependência dos ativos	0,15	0,15	0,03	**0,63**	9
C10 - Tratamento do risco	0,17	**0,66**	0,14	0,03	9
C11 - Usabilidade do software	**0,58**	0,11	0,03	0,26	6
C12 - Relatórios gerados	0,12	0,24	0,06	**0,55**	7
C13 - Documentação do software	**0,42**	0,11	0,03	**0,42**	6
Total	**22,69**	**19,27**	**13,39**	**35,19**	

Tendo em vista as análises realizadas, nenhum dos softwares está adequado totalmente aos critérios propostos, sobretudo, aqueles julgados mais importantes de acordo com o objetivo deste trabalho, como o tratamento dos riscos, capacidade de adaptação a mudanças e dependência entre ativos. Entretanto, o software que demonstrou melhores capacidades e, portanto, obteve o maior valor foi o SecureAware. O SecureAware, mesmo sem o módulo de tratamento de riscos, foi o que mostrou-se o mais preparado na maioria dos critérios, sendo estes critérios o C1, C2, C6, C8, C9, C12 e C13. O valor total do SecureAware se deve, principalmente pelo software ter obtido médias elevadas nos critérios C8 e C9 e, assim, se mostrado o mais apto entre os testados para realizar a dependência dos ativos e ser o mais adaptável a mudanças. Conclui-se então, que com o módulo de tratamento de riscos, este software estaria ainda mais próximo de estar de acordo com os objetivos deste trabalho, embora ainda tenha pontos que poderiam ser melhorados, como permitir uma manutenção para vulnerabilidades e um histórico que pudesse auxiliar na definição de riscos futuros.

O VS Risk é um software que, entre os testados foi o com melhor usabilidade, além disto, permite facilmente a associação de vulnerabilidades e ameaças aos ativos, e ainda contém uma biblioteca bastante completa com relação a ativos, controles e vulnerabilidades. Mas, não apresentou bom desempenho nos principais critérios, por ser pouco adaptável a mudanças, não possuir dependência dos ativos e por não prover um tratamento dos riscos mais efetivo.

O STREAM foi o software com melhores formas para o tratamento dos riscos, através do acompanhamento da implantação dos controles necessários. Também possui uma boa identificação dos controles e permite a geração de relatórios de histórico, o que pode ser de grande ajuda para a gestão dos riscos de uma empresa. Em contrapartida, o STREAM não possui uma manutenção das vulnerabilidades, não define valores para os ativos e a biblioteca da versão testada, apresenta principalmente dados fictícios para demonstração.

O SOBF, mesmo sendo o menos qualificado para os critérios tratados, possui alguns pontos fortes em operações mais básicas, como a identificação e definição dos valores dos ativos, a identificação das vulnerabilidades e controles, associando-os aos seus ativos. Nestes pontos realiza estas funções de forma similar

ou melhor que os outros softwares. Mas como é o software mais simples e ainda sem algumas de suas funcionalidades implementadas, deixa a desejar na definição do impacto e dos riscos, por ser pouco intuitivo e por possuir uma documentação incompleta, e assim, ainda não é uma boa ferramenta para gerenciar o processo de gestão de riscos nas empresas.

6 CONCLUSÃO

A informação é, atualmente, um dos ativos de maior valor e é fundamental para a sobrevivência e competitividade de uma organização. É imprescindível garantir a sua segurança, sempre mantendo a sua integridade, disponibilidade e confidencialidade. A segurança da informação e, mais especificamente, o processo de gestão de riscos, vem sendo cada vez mais empregado nas empresas a fim de analisar e controlar os riscos a ponto de estarem a níveis aceitáveis. Uma forma para auxiliar o processo de gestão de riscos é por meio de softwares específicos para esta finalidade.

Analisando as metodologias de gestão de riscos de segurança da informação, OCTAVE, NBR ISO/IEC 27005 e NIST SP 800-30 percebe-se que mesmo utilizando métodos distintos, existem pontos em comum para o processo de gestão de riscos. Estes pontos comuns serviram de base para a elaboração dos critérios aplicados para a avaliação dos softwares. O principal critério, o qual vai de encontro com o objetivo maior do trabalho, é avaliar e indicar os softwares que realizem a gestão de riscos de forma mais dinâmica e flexível, adaptando-se às mudanças organizacionais.

A avaliação dos softwares VS Risk, STREAM, SOBF e SecureAware, foi realizada utilizando o método analítico hierárquico. Nenhum dos softwares analisados forneceu mecanismos suficientes para proporcionar uma gestão de riscos dinâmica. O software que apresentou uma capacidade de adaptação às mudanças maior e foi mais bem avaliado na maior parte dos critérios foi o SecureAware. Por outro lado, o software mais adequado para o tratamento dos riscos, outra importante fase no processo de gestão de riscos, foi o STREAM.

A capacidade de um software de gestão de riscos ser adaptável a mudanças pode ser entendida, não apenas como algumas das funcionalidades exercidas pelo SecureAware, como a dependência dos ativos ou as ameaças relacionadas aos tipos de ativos. O software poderia, por exemplo, sugerir novos controles ao se adicionar vulnerabilidades ou ameaças ou ainda indicar controles para cada tipo de ativo. Outra característica que tornaria o software mais adaptável seria ao realizar uma operação de alteração ou exclusão de uma determinada ameaça ou

vulnerabilidade, listar todos os ativos que estão relacionados com as mudanças que estão sendo efetuadas, antes de executar a alteração. O software poderia também sugerir, de forma automática, algumas possíveis ações a serem tomadas no momento em que alguma mudança for realizada, seja em ativos, controles, vulnerabilidades ou ameaças.

Algo de grande utilidade no processo de gestão de riscos seria se, ao relacionar as ameaças ou vulnerabilidades aos ativos, o software verificasse o histórico de incidentes para sugerir de alguma experiência passada, as probabilidades e o impacto aos ativos, além das soluções empreendidas anteriormente. Tais funcionalidades, que trariam maior auxilio às organizações, não são contempladas nos softwares avaliados, mas poderiam ser aperfeiçoadas em futuras versões para atenderem tais necessidades.

O processo de gestão de riscos é cada vez mais necessário e útil para as empresas garantirem maior segurança às informações, antecipando-se aos riscos e adotando medidas para preveni-los. Este estudo pode contribuir para esta área, expondo e comparando estas três metodologias, que podem ser mais bem conhecidas e possivelmente implementadas nas organizações. Além disso, este trabalho ao analisar os quatro softwares traz à tona a importância de um software adaptar-se às constantes mudanças em relação aos riscos, ameaças e vulnerabilidades. Outra contribuição a ser ressaltada é o método analítico hierárquico, que pode ser usado para comparações de diversas finalidades, não apenas softwares.

Como sugestão de trabalhos futuros a serem desenvolvidos, poderia ser realizada uma análise para o desenvolvimento de um novo software de gestão de riscos, para atender aos critérios definidos neste estudo, podendo contemplar as melhores funcionalidades dos softwares testados, mas também incluindo as funcionalidades necessárias para torná-lo mais adaptável a mudanças, como já citadas. Outra atividade a ser desenvolvida seria customizar um software como o SOBF, que mesmo sendo o menos preparado dentre os softwares testados, é de código aberto, o que significa que pode ser adaptado, aprimorando suas funcionalidades e incluindo novas, para atender as necessidades de cada organização.

REFERÊNCIAS

ALBERTS, C. J.; DOROFEE, A. J. **Octave Method Implementation Guide v2.0.** USA: Carnegie Mellon University, 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2005:** Tecnologia da Informação: Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2008:** Tecnologia da Informação: Técnicas de Segurança: Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2008.

AZEVEDO, P. O.; NAZARETH, T. L. A. **Definição e Implementação de um Modelo Híbrido Focado na Análise de Risco para Ambientes de TI**. 2009. 147f. Monografia (Ciência da Computação) – Universidade de Brasília, Brasília, 2009.

BOISOT, M. **Knowledge Assets.** Oxford: Oxford University Press, 1998.

CAMPOS, A. **Sistema de segurança da informação: controlando os riscos**. Florianópolis: Visual Books, 2ª ed, 2007.

CASAGRANDE, C; SPOLTI, E.; TOIGO, F. M; DEMICHELI, M. M.; RIZZON, R. F. **Case locação Datacenter Datasecurity.** 2012. 19p. Trabalho para Tópicos Especiais – Segurança da Informação – Universidade de Caxias do Sul, Caxias do Sul, 2012.

DANTAS, M. L. **Segurança da informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011. 152 p.

DILLARD, K.; PFOST, J.; RYAN, S. **Security Risk Management Guide.** [S.1.]: Microsoft Corporation, 2004. Disponível em: <http://technet.microsoft.com/en-us/library/cc163143.aspx>. Acesso em: 18 abr. 2012.

GITMAN, L. J. **Princípios de Administração Financeira.** São Paulo: Harbara Editora, 1997, 7a ed.

GONÇALVES JÚNIOR, A. **Metodologias de Gerenciamento de Riscos em Sistemas de Tecnologia da Informação e Comunicação:** abordagem prática para conscientização e implantação nas organizações. 2008. 56f. Trabalho de Conclusão de Curso (Especialização) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2008. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/15965/000695222.pdf?sequence=1>. Acesso em: 29 mar. 2012.

HORI, A. S. **Modelo de Gestão de Risco em Segurança da Informação: Um estudo de caso no mercado brasileiro de Cartões de Crédito.** 2003. 204f. Dissertação (Mestrado em Administração) – Fundação Getúlio Vargas, São Paulo, 2003.

ISO/IEC 13335-1:2004. Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. EUA: ISO/IEC, 2004.

ISO IEC TR 13335-1. Information technology – Guidelines for the management of IT Security : Part 1 – Concepts and models for IT Security. EUA: ISO/IEC, 1997. 23 p.

MARSHALL, C. **Medindo e Gerenciando Riscos Operacionais em Instituições Financeiras.** Qualitymark Ed., 2002. p. 19-74.

McGEE, J.; PRUSAK, L. **Gerenciamento estratégico da informação:** aumente a competitividade e eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. Tradução de Astrid Beatriz de Figueiredo. Rio de Janeiro: Elsevier, 1994.

OHTOSHI, P. H. **Análise Comparativa de Metodologias de Gestão e de Análise de Riscos sob a Ótica da Norma NBR-ISO/IEC 27005.** 2008. 103f. Monografia (Ciência da Computação) – Universidade de Brasília, Brasília, 2008.

OLIVEIRA, V. L. **Uma análise comparativa das metodologias de gerenciamento de risco FIRM, NIST SP 800-30 e OCTAVE.** 2006. 180f. Dissertação (Mestrado em Computação) – Universidade Federal de Campinas, Campinas, 2006. Disponível em: <http://www.bibliotecadigital.unicamp.br/document/?code=vtls000388175&fd=y>. Acesso em 12 mai. 2012.

MICHAELIS. Moderno Dicionário da Língua Portuguesa. Disponível em:

<http://michaelis.uol.com.br/moderno/portugues/index.php>. Acesso em: 26 jun. 2012.

MÓDULO SECURITY. **Curso básico de segurança da informação.** 2006. Disponível em: <http://pt.scribd.com/doc/38231367/Apostila-Seguranca-da-Informacao>. Acesso em 26 jun. 2012.

MORAES, P. B. Tutorial para o projeto da infra-estrutura de um Internal Data Center. 2003. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialidc/pagina_4.asp>. Acesso em: 30 de setembro de 2007.

MORAES, E. A.; SANTALIESTRA, R. **Modelo de decisão com múltiplos critérios para escolha de software de código aberto e software de código fechado.** Organizações em contexto, Ano 4, n. 7, junho 2008. Disponível em: <http://mjs.metodista.br/index.php/roc/article/viewFile/355/276>. Acesso em 25 jun. 2012.

SÊMOLA, M. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Campus, 2003.

SILVEIRA, T. Z. **A Tecnologia da Informação como Ferramenta de Suporte à Gestão da Inovação.** 2011. 98f. Trabalho de Conclusão de Curso (Sistemas de Informação) – Universidade de Caxias do Sul, Caxias do Sul, 2011.

SOUZA, E. E. **A Proteção do Conhecimento e da Informação nas Organizações Contemporâneas:** um estudo em empresas de base tecnológica. 2008. 115f. Dissertação (Mestrado em Administração) – Faculdades Integradas Dr. Pedro Leopoldo, Pedro Leopoldo, 2008. Disponível em: <http://www.fpl.edu.br/2012/media/pdfs/05.mestrado/dissertacoes_2008/dissertacao_ernani_elias_de_souza_2008.pdf>. Acesso em: 11 abr. 2012.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. **Risk Management Guide for Information Technology Systems.** Gaithersburg: NIST – National Institute of Standards and Technology, 2002. 54p. (Special Publication 800-30). Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. Acesso em: 18 abr. 2012.

VIANEZ, M. S.; SEGOBIA, R. H.; CAMARGO, V. **Segurança de Informação:** Aderência à Norma ABNT NBR ISO/IEC N. 17.799:2005. **Revista de Informática Aplicada**, São Caetano do Sul, n. 1, p. 33-44, 2008. Disponível em:

http://seer.uscs.edu.br/index.php/revista_informatica_aplicada/article/view/307. Acesso em: 11 abr. 2012.

WESTERMAN, G.; HUNTER, R. **O Risco de TI: Convertendo ameaças aos Negócios em Vantagem Competitiva.** São Paulo: M. Books do Brasil Editora, 2008.

ANEXO A

CASE LOCAÇÃO DATA CENTER DATASECURITY

Propósito da Organização: Prestação de Serviços de Data Center em nuvem

O negócio: Disponibilizar uma estrutura para que os clientes deixem seus equipamentos, serviços e dados armazenados com segurança em nossa empresa.

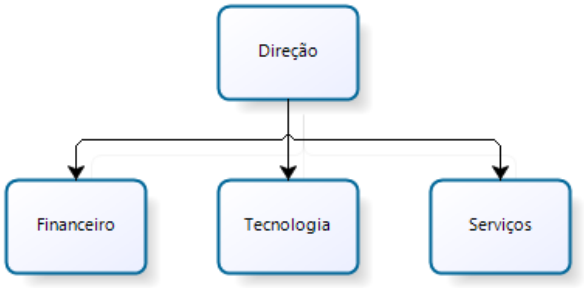
A missão: Viabilizar o sucesso de nossos clientes através de serviços de internet inovadores para seus negócios.

A visão do futuro: Ser uma empresa referência em serviços de locação de Data Center no estado.

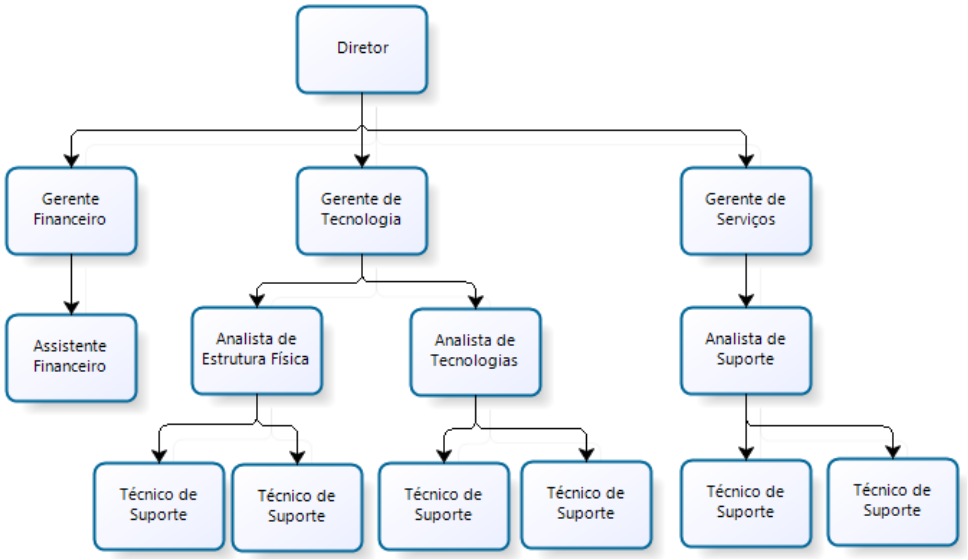
Os valores:

- Criatividade e Realização: Transformamos ideias em realidade.
- Trabalho em equipe: Queremos tirar proveito das diferenças. Confiamos uns nos outros para termos sucesso juntos.
- Persistência: Não desistimos do que acreditamos.
- Honestidade: É um pilar que vivemos e defendemos.

A estrutura organizacional:



O organograma:



As estratégias:
Estratégias de negócio: Fornecer uma estrutura adequada às normas de segurança da informação (ISO 27005 e ISO 27002) e estar de acordo com as melhores práticas do mercado (ITIL v3 e COBIT).
Estratégias de segurança da informação: Manter a política de segurança da informação atualizada e de acordo com as normas ISO 27005 e ISO 27002. Fazer reuniões mensais para avaliação de novos ativos e controles dos existentes.

Os produtos: Armazenamento, locação de estrutura física e Segurança da Informação.

Os parceiros: Dell para Hardware e Microsoft para Software; São escolhidos pela qualidade dos seus produtos, garantias estendidas e SLA's reduzidos; Os parceiros garantem tecnologias de ponta; Os parceiros garantem que os dados contidos em seus equipamentos ou softwares não serão acessados ou utilizados por eles;

Os terceiro: Embratel, OI e GVT para Comunicação, Akron para Rede lógica e Força, STV para segurança, Engenhar para engenharia, Pit para Marketing e comunicação visual e Limpacto para Limpeza;

As instalações: A empresa possui 9 salas sendo elas: Recepção, banheiro masculino e feminino, sala de reuniões, sala da diretoria, área comercial, área de suporte, sala da equipe de tecnologia e Data Center. A área de Data Center possui sistema de prevenção contra incêndios.

Os funcionários: São contratados mediante seleção criteriosa para as áreas técnicas e através de agências de emprego para áreas administrativas. Todos recebem treinamento no dia da integração.

Escopo:
Esta política de segurança tem como finalidade garantir uma estrutura física apropriada para que os clientes deixem seus equipamentos e dados com confiança. Serão analisados os aspectos da estrutura física, politica de acesso presencial e segurança da estrutura.

Restrições: Essa política de segurança não irá tratar dos dados lógicos que estão armazenados nos servidores, bem como nenhum tipo de acesso aos servidores que não seja presencial.
Itens para análise de segurança:
Ar condicionado;
Nobreaks;
Sistema de Segurança;
Funcionários;
Manutenções;
Estrutura física;
Acessos presenciais;

Ativo	**Processo de Negócio**	**Importância**
Sala	Estrutura Física para comportar o Data Center	Alta
Ar condicionado	Renovação/Controle do ar do ambiente	Média – Alta
No Breaks	Controle de Rede Elétrica	Alta

Rede Elétrica	Fornecimento de Energia para os Equipamentos eletrônicos	Alta
Rede Lógica	Disponibilização de Conectividade	Alta
Leitor Biométrico	Equipamento de Controle de Acesso	Média – Alta
Sistema de Acesso do leitor biométrico	Segurança de Acesso Presencial na sala	Alta
Rack Internos do datacenter	Estrutura Física para alocação dos equipamentos de informática	Média – Alta
Câmeras	Estrutura para o monitoramento da sala	Baixa
Sistema de Monitoramento das câmeras	Sistema para Monitoramento	Baixa
Sistema antichamas	Sistema para Controle de Incêndio	Alta
Funcionários	Funcionários que possuem acesso autorizado a sala	Alta
Terceiros	Prestadores de Serviços e Fornecedor	Alta
Links de comunicação	Fornecimento de Serviços de Telefonia	Baixa
Politica de Acesso ao Data Center	Conjunto de regras para acesso a sala	Média – Baixa
Switch	Estrutura que gerencia as conexões da rede lógica	Alta
Contrato com a operadora	Contrato de Serviço que irá distribuir o link de comunicação com o Cliente	Média - Alta

Politica de Segurança da Informação

Desenvolveremos uma política de segurança voltada para a garantia da parte estrutural da sala, como material que deve ser, redes elétrica, hidráulica, de climatização e lógica, bem como a segurança patrimonial, abrangendo desde os acessos físicos à sala até os métodos anti-incêndio e monitoramento por câmeras.

Organizando a Segurança da Informação

A direção deve demonstrar seu comprometimento com a politica de segurança da informação.

A direção deve assinar um documento onde se compromete a:

- Aprovar e apoiar a política de segurança da informação.
- Coordenar e analisar a implementação da segurança da informação.
- Fornecer recursos necessários para a implementação da politica de segurança.
- Analisar a eficácia da implementação da política da segurança da informação.

Representantes das áreas da empresa que deverão ter acesso físico ao datacenter devem acompanhar a implementação da política de segurança da informação.

As áreas da empresa onde não há contato físico com o datacenter, ou sala do datacenter, não será necessário o acompanhamento de seus representantes.

As responsabilidades de cada pessoa pela segurança da informação devem estar claramente definidas.

A empresa deve gerenciar a politica de segurança da informação em intervalos planejados ou quando ocorrerem mudanças relativas a politica de segurança da informação.

Restrições:

Não será necessário realizar uma consultoria com especialistas ou grupos de segurança da informação externos.

Não será necessário contato com autoridades, grupos especializados ou fóruns especializados em segurança da informação.

Não será tratado o controle de acesso a recursos de processamento da informação e ao processamento e comunicação da informação por partes externas.

Segurança em Recursos Humanos

Cada terceiro ou funcionário a ter acesso a estrutura física , terá que ter uma identificação. As portas da sala só liberam o acesso mediante a autorização via sistema por biométrica. Cada pessoa a ter acesso precisa estar de acordo com o termo de Segurança Da Informação da nossa Empresa antes de ter acesso a sala de Datacenter. O acesso será liberado apenas na área que o terceiro ou funcionário foi designado sendo assim o acesso não autorizado em outras áreas além da dele própria. Na hora da pré-contração esses termos são todos apresentados aos futuros empregados ou a um novo terceiro que prestará serviço na empresa. Antes da contratação de um funcionário ou terceiro, é feita conferida no histórico para ver como o futuro funcionário ou terceiro lida com politicas de seguranças.

Segurança Física e Do Ambiente

→ Áreas seguras

A instalação-chave será a sala do DataCenter, onde é executado todo o processamento da informação.

Serão utilizados perímetros de segurança para proteger as áreas que contenham informações e instalações de processamento da informação. As áreas seguras serão protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso, e estas áreas serão localizadas de maneira a evitar o acesso ao público.

Também devem ser projetadas e aplicadas proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem, bem como meios para evitar o trabalho não supervisionado em áreas seguras, tanto por motivos de segurança como para prevenir as atividades mal intencionadas. As áreas seguras não ocupadas serão fisicamente trancadas e periodicamente verificadas.

→ Equipamentos

Os equipamentos-chave serão:

- Portas
- Janelas
- Paredes
- Chão
- Teto

- Ar-condicionados
- Rack
- Rede lógica
- Rede elétrica

Os equipamentos serão protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado, segundo os tratamentos a seguir:

- Os itens que exigem proteção especial devem ser isolados para reduzir o nível geral de proteção necessário;
- Sejam adotados controles para minimizar o risco de ameaças físicas potenciais, como furto ou roubo, incêndio, explosivos, fumaça, água (ou falha do suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;
- Sejam estabelecidas diretrizes quanto a comer, beber e fumar nas proximidades das instalações de processamento da informação;
- As condições ambientais, como temperatura e umidade, sejam monitoradas para a detecção de condições que possam afetar negativamente os recursos de processamento da informação;
- Todos os edifícios sejam dotados de proteção contra raios e todas as linhas de entrada de força e de comunicações tenham filtros de proteção contra raios;
- Os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades;
- O cabeamento de energia e de telecomunicações que tranporta dados ou dá suporte aos serviços de informações seja protegido contra interceptação ou dano.
- A manutenção e os consertos dos equipamentos sejam realizados somente por pessoal de manutenção autorizado;
- Os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanentes;
- Sejam mantidos os registros de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas.

Gerenciamento das operações e comunicações

- Procedimentos e responsabilidades e controle de documentação:
    - Serão definidos todos os procedimentos e responsabilidades pela gestão e operação do datacenter através do desenvolvimento da documentação dos procedimentos operacionais que devem ser sempre mantidos atualizados. Além disso, deve-se utilizar sempre que necessária a segregação de funções (recomenda-se que uma pessoa realize uma ou algumas partes de um processo, mas não todas).

- Troca de informações
    - Somente serão permitidas as trocas de informações sobre o datacenter mediante prévia aprovação. Nenhuma informação estratégica deverá ser disponibilizada para usuários que não tenha acesso a tal. Os terceiros que tiverem acesso ao datacenter somente poderão ter acesso às informações pertinentes ao serviço para o qual foram contratados.

- Monitoramento
    - O acesso ao datacenter como o próprio, terá monitoramento em tempo real por câmeras , permitindo assim a identificação de todas as pessoas que tiveram acesso ao mesmo. Será implementado um sistema de prevenção e detecção de usuários não autorizados e todos os usuários devem estar conscientes sobre isso.

Controle de Acessos

Para o controle de acesso desenvolveremos uma política para utilização de métodos de segurança ao acesso, como fechaduras inteligentes controladas por biometria, cartão ou senha.

Não serão analisadas as políticas voltadas ao controle de liberação de acesso físico e lógico.

Aquisição, desenvolvimento e manutenção de sistemas da informação

Toda a estrutura física atual deve ser analisada afim de desenvolver a politica de segurança da informação que tratará da segurança do local. Os requisitos de segurança devem ser identificados, acordados e documentados.

Restrições: Sistemas operacionais, aplicações de negócios, serviços e aplicações desenvolvidas pelo usuário não serão tratados pela política de segurança.

Gestão de incidentes de segurança da informação

Todas as salas possuem um sistema anti chama para proteger , infraestrutura contra incêndios. Sendo assim acionada imediatamente após o alerta disparado.

Algumas das ameaças a essa Politica de Segurança:

- Perda do equipamento , pode ser por quebra ou falta de manutenção
- Mau funcionamento ou sobre carga de energia
- Erros humanos , falhas
- Não conformidades com as politicas e diretrizes – mediante a punição
- Violação dos procedimentos a parte física.
- Mau funcionamento do Hardware ou Software.

Em caso de algum alerta , imediatamente o terceiro ou funcionário comunicar o responsável pela aquela área. Exemplo: Em caso de incêndio acionar o Corpo de Bombeiros o mais rápido possível.

Caso ocorra algum sinistro com equipamento acionar imediatamente o suporte técnico ou seguro do equipamento , repondo o averiguado por um novo ou provisório (dependendo a situação.

Se ocorrer a situação de emergência ou troca rápida de equipamento , tem que ser registrado via documentos a titulo de relatório do ocorrido para analise posterior.

Todo reparo ou troca de equipamento , para ser efetiva , precisa ser elaborado um plano de ação prevendo impactos e tempo de solução equipe envolvida para assim efetivar o reparo.

Em caso de falha com terceiro – fornecedor exigir o ressarcimento do mesmo através de levantamento de danos e tempo.

Gestão da continuidade do negócio

Um processo de gestão deve ser desenvolvido e mantido para assegurar a continuidade do negócio e a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio. Também deve-se 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. Os planos de continuidade do negócio devem ser testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.

Conformidade

Deve-se garantir e evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação. Para isso, é conveniente contratar, caso necessário, consultoria especializada, bem como analisar criticamente a segurança dos sistemas de informação em intervalos regulares, verificando, sobretudo, sua conformidade e aderência a requisitos legais e regulamentares.

Ativos:

Ativo	**Ameaça**	**Tipo**	**Fonte da Ameaça**
Sala	Fogo	Dano Físico	Equipamentos Elétricos podem pegar fogo
	Água	Dano Físico	infiltrações
	Inundações	Eventos Naturais	Chuvas (Enchentes)
Ar condicionado	Fogo	Dano Físico	Equipamentos Elétricos
	Água	Dano Físico	Infiltrações
	Inundações	Dano Físico	Enchentes
	Falha de equipamento	Falhas Técnicas	Falta de Energia Elétrica
	Defeito do equipamento	Falhas Técnicas	Falta de Devida Manutenção
No breaks	Fogo	Dano Físico	Equipamentos Elétricos
	Água	Dano Físico	Infiltrações
	Inundações	Dano Físico	Enchentes
	Falha de equipamento	Falhas Técnicas	Falta de Energia Elétrica por tempo maior que a autonomia do nobreak
	Defeito do equipamento	Falhas Técnicas	Falta de Devida Manutenção
Funcionários	Acesso de pessoas não autorizadas	Comprometimento da informação	Pessoal interno
	Acesso de pessoas não treinadas	Comprometimento da informação	Pessoal interno
	Furto de equipamento	Comprometimento da informação	Pessoal interno

	Divulgação indevida	Comprometimento da informação	Pessoal interno
	Alteração de Hardware	Comprometimento da informação	Pessoal interno
	Indisponibilidade	Comprometimento de funções	Pessoal interno
Terceiros	Acesso de pessoas não autorizadas	Comprometimento da informação	Pessoal interno
	Furto de equipamento	Comprometimento da informação	Pessoal externo
	Alteração de Hardware	Comprometimento da informação	Pessoal externo
Links de comunicação	Perda de link	Dano Lógico	Cabos Danificados
Política de acesso ao datacenter	Fraudes	Dano Físico	Não Cumprimento da Politica
Rede Elétrica	Fogo	Dano Físico	Equipamentos Elétricos
	Água	Dano Físico	Infiltrações
	Inundações	Dano Físico	Enchentes
	rompimento de cabos	Dano Físico	Acidentes, manutenções incorretas, reformas
Rede Lógica	Fogo	Dano Físico	Equipamento elétrico que pode pegar fogo
	Água	Dano Físico	Infiltrações
	Inundações	Dano Físico	Enchentes
	Falha de parte da rede lógica	Paralisação de serviços essenciais	Manutenção Inadequada
Leitor Biométrico	Fogo	Dano Físico	Equipamento elétrico que pode pegar fogo
	Água	Dano Físico	Infiltrações
	Porta emperrada	Paralisação de serviços essenciais	Manutenção Inadequada
Sistema de acesso do leitor biométrico	falha de comunicação entre sistema e leitor	Paralisação de serviços essenciais	Manutenção Inadequada
	Liberação de acesso à usuários não autorizados	Ações não autorizadas	Hacker, cracker, pessoal interno
Racks do data center	Fogo	Dano Físico	Equipamentos Elétricos
Câmeras	Fogo	Dano Físico	Equipamentos Elétricos
	Água	Dano Físico	Infiltrações
	Inundações	Dano Físico	Enchentes
	Falha de equipamento	Falhas Técnicas	Falta de Energia Elétrica
	Defeito do equipamento	Falhas Técnicas	Falta de Devida Manutenção
Sistema de monitoramento das câmeras	Defeito de Software	Falhas Técnicas	Falta de Devida de Manutenção do software
	Realização de cópia das imagens do sistema sem autorização	Ações não Autorizadas	Funcionários com acesso ao sistema
	Furto de mídia	Comprometimento da informação	Funcionários com acesso ao sistema

Sistema Anti-incêncio	Mal funcionamento	Dano Físico	Equipamento elétrico
Switch	Falha no equipamento	Dano Físico	Sobre Carga de Energia / Desconfiguração

Controles Existentes:

		Situação do Controle		Situação da implementação
Ativo	Descrição do controle	Planejado	Existente	
Sala	Leitor biométrico		X	Adequada
	Câmeras		X	Adequada
	Sistema antichamas		X	Adequada
Ar condicionado	Sensores de temperatura	X		Precisa de revisão
No breaks	Controle de autonomia das baterias		X	Adequada
	Controle da rede elétrica		X	Adequada
Funcionários	Log de acessos		X	Adequada
	Gravação de imagens		X	Adequada
Terceiros	Log de acessos		X	Adequada
	Gravação de imagens		X	Adequada
Links de comunicação	Sistema de administração	X		Precisa de revisão
Politica de Acesso ao Data Center	Controle de versão		X	Precisa de revisão

Vulnerabilidades

Ativo	**Vulnerabilidades**	**Ameaça**	**Controles**
Sala	Faísca, curto circuito	Fogo	Rede elétrica estabilizada
	Infiltrações	Água	Inspeção/Manutenção periódica
	Tsunami, enchente, tempestade	Inundações	Incontrolável
Ar condicionado	Faísca, curto circuito	Fogo	Rede elétrica estabilizada
	Infiltrações	Água	Inspeção/Manutenção

			periódica
	Tsunami, enchente, tempestade	Inundações	Incontrolável
	Falta de manutenção	Falha de equipamento	Manutenção periódica
	Vida útil	Defeito do equipamento	Controle de vida útil
No breaks	Faísca, curto circuito	Fogo	Rede elétrica estabilizada
	Infiltrações	Água	Inspeção/Manutenção periódica
	Tsunami, enchente, tempestade	Inundações	Incontrolável
	Falta de manutenção	Falha de equipamento	Manutenção periódica
	Vida útil	Defeito do equipamento	Controle de vida útil
Funcionários	Falta ou defeito de mecanismos de autenticação	Acesso de pessoas não autorizadas	Leitor biométrico
	Falta de treinamento adequado	Acesso de pessoas não treinadas	Treinamentos periódicos
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Furto de equipamento	Supervisão do trabalho de pessoal autorizado e terceiros
	Divulgação premeditada	Divulgação indevida	Orientação e treinamento
	Trabalho não supervisionado de funcionários	Alteração de Hardware	Supervisão do trabalho de pessoal autorizado
	Ausência do Funcionários	Indisponibilidade	Treinamento para mais de um funcionário
Terceiros	Falta ou defeito de mecanismos de autenticação	Acesso de pessoas não autorizadas	Leitor biométrico
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Furto de equipamento	Supervisão do trabalho de pessoal autorizado e terceiros
	Trabalho não supervisionado de terceiros	Alteração de Hardware	Supervisão do trabalho de pessoal autorizado
Links de comunicação	Falha na operadora	Perda de link	Link redundante
Poítica de acesso ao datacenter	Funcionário mal intencionado	Fraudes	Incontrolável

Rede Elétrica	Faísca, curto circuito	Fogo	Rede elétrica estabilizada
	Infiltrações	Água	Inspeção/Manutenção periódica
	Tsunami, enchente, tempestade	Inundações	Incontrolável
	Má instalação de equipamentos	rompimento de cabos	Inspeção periódica
Rede Lógica	Faísca, curto circuito	Fogo	Rede elétrica estabilizada
	Infiltrações	Água	Inspeção/Manutenção periódica
	Tsunami, enchente, tempestade	Inundações	Incontrolável
	Rompimento de cabos, manutenção inesistente	Falha de parte da rede lógica	Inspeção/Manutenção periódica
Leitor Biométrico	Faísca, curto circuito	Fogo	Rede elétrica estabilizada
	Infiltrações	Água	Inspeção/Manutenção periódica
	Dificulta o acesso à sala	Porta emperrada	Manutenção periódica
Sistema de acesso do leitor biométrico	Sem acesso à sala	falha de comunicação entre sistema e leitor	Utilizar o software adequado
	usuário mal intencionado pode ter acesso à sala	Liberação de acesso à usuários não autorizados	Treinamento , política de acesso
Racks do data center	Faísca, curto circuito	Fogo	Rede elétrica estabilizada
Câmeras	Faísca, curto circuito	Fogo	Rede elétrica estabilizada
	Infiltrações	Água	Inspeção/Manutenção periódica
	Tsunami, enchente, tempestade	Inundações	Incontrolável
	Falta de manutenção	Falha de equipamento	Manutenção periódica
	Vida útil	Defeito do equipamento	Controle de vida útil
Sistema de monitoramento das câmeras	Software novo	Defeito de Software	Teste de software em ambiente de homologação
	Trabalho não supervisionado de pessoal	Realização de cópia das imagens do sistema sem	Supervisão do trabalho de pessoal autorizado e

	da limpeza ou terceiros	autorização	terceiros
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Furto de mídia	Supervisão do trabalho de pessoal autorizado e terceiros
Sistema Anti-incêncio	Falta de manutenção	Mal funcionamento	Manutenção periódica
Switch	Falta de manutenção	Falha no equipamento	Manutenção periódica

Consequências:

Incidente	**Consequência**	**Ativos**
Fogo	Danificação do espaço físico	Sala, Rede Elétrica, Rede Lógica
Infiltração	Danificação do espaço físico	Sala, Rede Elétrica, Rede Lógica
Inundação	Danificação do espaço físico	Sala, Rede Elétrica
Fogo	Danificação do equipamento	Ar Condicionado, No Break, Leitor Biométrico, Racks Internos, Câmeras
Infiltração	Danificação do equipamento	Ar Condicionado, No Break, Leitor Biométrico, Câmeras
Inundação	Danificação do equipamento	Ar Condicionado, No Break, Câmeras
Falha de equipamento	Falha do serviço do equipamento	Ar Condicionado, No Break, Câmeras, Sistema Anti-Incêndio, Switch
Expirou a vida útil	Falha do serviço do equipamento	Ar Condicionado, No Break, Câmeras
Pessoa não autorizada acessou a sala	Roubo de informações, roubo de equipamentos e danificação de equipamentos	Funcionário, Terceiro, Sistema de Acesso do Leitor Biométrico
Pessoa não treinada acessou a sala	Danificação do equipamento	Funcionário
Furto de equipamento	Falha do serviço do equipamento	Funcionário, Terceiro
Pessoa fez uma divulgação indevidamente	Perda de confiabilidade	Funcionário
Alteração de hardware	Falha do serviço do equipamento	Funcionário, Terceiro
Funcionário não compareceu ao estabelecimento	Falha do serviço dependente deste Funcionário	Funcionário
Perda do Link	Perda de confiabilidade	Link de comunicação
Invasão	Política ficou alterada ou plagiada	Política de Acesso ao DataCenter
Rompimento de cabos	Falha do serviço do equipamento	Rede Elétrica, Rede Lógica
Porta Emperrada	Falha no acesso à sala	Leitor Biométrico
Falha de comunicação entre o sistema e o leitor	Falha no acesso à sala	Sistema de Acesso do Leitor Biométrico
Defeito no Software	Falha do serviço do software	Sistema de Monitoramento de Câmeras
Cópia das imagens	Perda de confiabilidade	Sistema de Monitoramento de Câmeras
Furto de mídia	Perda de confiabilidade	Sistema de Monitoramento de Câmeras

Probabilidade e Impacto:

Ativo	Vulnerabilidade	Probabilidade	Impacto
Sala	Faísca, curto circuito	Baixa	Alto (1B,2A,3A)
	Infiltrações	Baixa	Baixo (1C,2C)
	Tsunami, enchente, tempestade	Baixa	Alto (1A,2A,3A)
Ar condicionado	Faísca, curto circuito	Baixa	Baixo (1C,2C)
	Infiltrações	Baixa	Baixo (1C,2C)
	Tsunami, enchente, tempestade	Baixa	Alto (1A,2A,3A)
	Falta de manutenção	Média	Médio (1C,2C)
	Vida útil	Média	Médio (1C,2C)
No breaks	Faísca, curto circuito	Média	Alto (1A,2A,3B)
	Infiltrações	Baixa	Alto (1A,2A,3B)
	Tsunami, enchente, tempestade	Baixa	Alto (1A,2A,3B)
	Falta de manutenção	Média	Médio (1B,2C)
	Vida útil	Média	Alto (1A,2B)
Funcionários	Falta ou defeito de mecanismos de autenticação	Média	Baixo (1C,2C)
	Falta de treinamento adequado	Baixa	Baixo (1C,2C)
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Alta	Baixo (1C,2C)
	Divulgação premeditada	Média	Baixo (1C,2C)
	Trabalho não supervisionado de funcionários	Alta	Baixo (1C,2C)
	Ausência do Funcionários	Alta	Baixo (1C,2C)
Terceiros	Falta ou defeito de mecanismos de autenticação	Média	Baixo (1C,2C)
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Média	Baixo (1C,2C)
	Trabalho não supervisionado de terceiros	Média	Baixo (1C,2C)
Links de comunicação	Falha na operadora	Baixa	Alto (1B,2A)
Política de acesso ao datacenter	Funcionário mal intencionado	Alta	Baixo (1C,2C)
Rede Elétrica	Faísca, curto circuito	Média	Alto (1B,2A,3A)
	Infiltrações	Baixa	Alto (1B,2A,3A)
	Tsunami, enchente, tempestade	Baixa	Alto (1A,2A,3A)
	Má instalação de equipamentos	Média	Médio (1C,2C)
Rede Lógica	Faísca, curto circuito	Baixa	Baixo (1C,2C)
	Infiltrações	Baixa	Baixo (1C,2C)
	Tsunami, enchente, tempestade	Baixa	Alto (1A,2A,3A)
	Rompimento de cabos, manutenção inexistente	Alta	Baixo (1C,2C)
Leitor Biométrico	Faísca, curto circuito	Baixa	Baixo (1C,2C)
	Infiltrações	Baixa	Baixo (1C,2C)
	Dificuldade de acesso à sala	Média	Baixo (1C,2C)
Sistema de acesso do leitor biométrico	Sem acesso à sala	Média	Baixo (1C,2C)

	usuário mal intencionado pode ter acesso à sala	Alta	Baixo (1C,2C)
Racks do data center	Faísca, curto circuito	Baixa	Baixo (1C,2C)
Câmeras	Faísca, curto circuito	Baixa	Baixo (1C,2C)
	Infiltrações	Baixa	Baixo (1C,2C)
	Tsunami, enchente, tempestade	Baixa	Alto (1A,2A,3A)
	Falta de manutenção	Média	Baixo (1C,2C)
	Vida útil	Média	Baixo (1C,2C)
Sistema de monitoramento das câmeras	Software novo	Baixa	Baixo (1C,2C)
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Média	Baixo (1C,2C)
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Média	Baixo (1C,2C)
Sistema Anti-incêndio	Falta de manutenção	Média	Alto (1A,2A,3A)
Switch	Falta de manutenção	Alta	Médio (1C,2A)

Estimativa de Riscos:

Ativo	**Vulnerabilidade**	**Risco**
Sala	Faísca, curto circuito	4
	Infiltrações	2
	Tsunami, enchente, tempestade	4
Ar condicionado	Faísca, curto circuito	2
	Infiltrações	2
	Tsunami, enchente, tempestade	4
	Falta de manutenção	4
	Vida útil	4
No breaks	Faísca, curto circuito	5
	Infiltrações	4
	Tsunami, enchente, tempestade	4
	Falta de manutenção	4
	Vida útil	5
Funcionários	Falta ou defeito de mecanismos de autenticação	3
	Falta de treinamento adequado	2
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	4
	Divulgação premeditada	3
	Trabalho não supervisionado de funcionários	4
	Ausência do Funcionário	4
Terceiros	Falta ou defeito de mecanismos de autenticação	3
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	3
	Trabalho não supervisionado de terceiros	3
Links de comunicação	Falha na operadora	4
Política de acesso ao datacenter	Funcionário mal intencionado	4

Rede Elétrica	Faísca, curto circuito	5
	Infiltrações	4
	Tsunami, enchente, tempestade	4
	Má instalação de equipamentos	4
Rede Lógica	Faísca, curto circuito	3
	Infiltrações	3
	Tsunami, enchente, tempestade	4
	Rompimento de cabos, manutenção inexistente	4
Leitor Biométrico	Faísca, curto circuito	2
	Infiltrações	2
	Dificuldade de acesso à sala	3
Sistema de acesso do leitor biométrico	Sem acesso à sala	3
	usuário mal intencionado pode ter acesso à sala	4
Racks do data center	Faísca, curto circuito	2
Câmeras	Faísca, curto circuito	2
	Infiltrações	2
	Tsunami, enchente, tempestade	4
	Falta de manutenção	3
	Vida útil	3
Sistema de monitoramento das câmeras	Software novo	2
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	3
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	3
Sistema Anti-incêncio	Falta de manutenção	4
Switch	Falta de manutenção	5

Tipo de Tratamento:

Ativo	**Vulnerabilidade**	**Tipo Tratamento**
Sala	Faísca, curto circuito	Reter o Risco
	Infiltrações	Reter o Risco
	Tsunami, enchente, tempestade	Reter o Risco
Ar condicionado	Faísca, curto circuito	Reter o Risco
	Infiltrações	Reter o Risco
	Tsunami, enchente, tempestade	Reter o Risco
	Falta de manutenção	Reter o Risco
	Vida útil	Reter o Risco
No breaks	Faísca, curto circuito	Reter o Risco

	Infiltrações	Reter o Risco
	Tsunami, enchente, tempestade	Reter o Risco
	Falta de manutenção	Reter o Risco
	Vida útil	Reter o Risco
Funcionários	Falta ou defeito de mecanismos de autenticação	Reter o Risco
	Falta de treinamento adequado	Reter o Risco
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Reter o Risco
	Divulgação premeditada	Reter o Risco
	Trabalho não supervisionado de funcionários	Reter o Risco
	Ausência do Funcionários	Reter o Risco
Terceiros	Falta ou defeito de mecanismos de autenticação	Reter o Risco
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Reter o Risco
	Trabalho não supervisionado de terceiros	Reter o Risco
Links de comunicação	Falha na operadora	Reter o Risco
Política de acesso ao datacenter	Funcionário mal intencionado	Reter o Risco
Rede Elétrica	Faísca, curto circuito	Reter o Risco
	Infiltrações	Reter o Risco
	Tsunami, enchente, tempestade	Reter o Risco
	Má instalação de equipamentos	Reter o Risco
Rede Lógica	Faísca, curto circuito	Reter o Risco
	Infiltrações	Reter o Risco
	Tsunami, enchente, tempestade	Reter o Risco
	Rompimento de cabos, manutenção inexistente	Reter o Risco
Leitor Biométrico	Faísca, curto circuito	Reter o Risco
	Infiltrações	Reter o Risco
	Dificuldade de acesso à sala	Reter o Risco
Sistema de acesso do leitor biométrico	Sem acesso à sala	Reter o Risco

	usuário mal intencionado pode ter acesso à sala	Reduzir o Risco
Racks do data center	Faísca, curto circuito	Reter o Risco
Câmeras	Faísca, curto circuito	Reter o Risco
	Infiltrações	Reter o Risco
	Tsunami, enchente, tempestade	Reter o Risco
	Falta de manutenção	Reter o Risco
	Vida útil	Reduzir o Risco
Sistema de monitoramento das câmeras	Software novo	Reter o Risco
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Reter o Risco
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Reter o Risco
Sistema Anti-incêncio	Falta de manutenção	Reduzir o Risco
Switch	Falta de manutenção	Reduzir o Risco

Controle Recomendado:

Ativo	**Vulnerabilidade**	**Controles**	**Controle Recomendado**
Sala	Faísca, curto circuito	Rede elétrica estabilizada	Manter Controle
	Infiltrações	Inspeção/Manutenção periódica	Manter Controle
	Tsunami, enchente, tempestade	Incontrolável	Incontrolável
Ar condicionado	Faísca, curto circuito	Rede elétrica estabilizada	Manter Controle
	Infiltrações	Inspeção/Manutenção periódica	Manter Controle
	Tsunami, enchente, tempestade	Incontrolável	Manter Controle
	Falta de manutenção	Manutenção periódica	Manter Controle
	Vida útil	Controle de vida útil	Manter Controle
No breaks	Faísca, curto circuito	Rede elétrica estabilizada	Manter Controle
	Infiltrações	Inspeção/Manutenção periódica	Manter Controle
	Tsunami, enchente, tempestade	Incontrolável	Incontrolável
	Falta de manutenção	Manutenção periódica	Manter Controle
	Vida útil	Controle de vida útil	Manter Controle
Funcionários	Falta ou defeito de mecanismos de autenticação	Leitor biométrico	Manter Controle
	Falta de treinamento adequado	Treinamentos periódicos	Manter Controle

	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Supervisão do trabalho de pessoal autorizado e terceiros	Manter Controle
	Divulgação premeditada	Orientação e treinamento	Manter Controle
	Trabalho não supervisionado de funcionários	Supervisão do trabalho de pessoal autorizado	Manter Controle
	Ausência do Funcionários	Treinamento para mais de um funcionário	Manter Controle
Terceiros	Falta ou defeito de mecanismos de autenticação	Leitor biométrico	Manter Controle
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Supervisão do trabalho de pessoal autorizado e terceiros	Manter Controle
	Trabalho não supervisionado de terceiros	Supervisão do trabalho de pessoal autorizado	Manter Controle
Links de comunicação	Falha na operadora	Link redundante	Manter Controle
Política de acesso ao datacenter	Funcionário mal intencionado	Incontrolável	Manter Controle
Rede Elétrica	Faísca, curto circuito	Rede elétrica estabilizada	Manter Controle
	Infiltrações	Inspeção/Manutenção periódica	Manter Controle
	Tsunami, enchente, tempestade	Incontrolável	Manter Controle
	Má instalação de equipamentos	Inspeção periódica	Manter Controle
Rede Lógica	Faísca, curto circuito	Rede elétrica estabilizada	Manter Controle
	Infiltrações	Inspeção/Manutenção periódica	Manter Controle
	Tsunami, enchente, tempestade	Incontrolável	Manter Controle
	Rompimento de cabos, manutenção inexistente	Inspeção/Manutenção periódica	Manter Controle
Leitor Biométrico	Faísca, curto circuito	Rede elétrica estabilizada	Manter Controle
	Infiltrações	Inspeção/Manutenção periódica	Manter Controle
	Dificuldade de acesso à sala	Manutenção periódica	Manter Controle
Sistema de acesso do leitor biométrico	Sem acesso à sala	Utilizar o software adequado	Manter Controle
	usuário mal intencionado pode ter acesso à sala	Treinamento , política de acesso	Manter Controle + Exigir Certificações
Racks do data center	Faísca, curto circuito	Rede elétrica estabilizada	Manter Controle
Câmeras	Faísca, curto circuito	Rede elétrica estabilizada	Manter Controle
	Infiltrações	Inspeção/Manutenção periódica	Manter Controle
	Tsunami, enchente, tempestade	Incontrolável	Manter Controle
	Falta de manutenção	Manutenção periódica	Manter Controle + Peças sobressalentes

	Vida útil	Controle de vida útil	Manter Controle
Sistema de monitoramento das câmeras	Software novo	Teste de software em ambiente de homologação	Manter Controle
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Supervisão do trabalho de pessoal autorizado e terceiros	Manter Controle
	Trabalho não supervisionado de pessoal da limpeza ou terceiros	Supervisão do trabalho de pessoal autorizado e terceiros	Manter Controle
Sistema Anti-incêncio	Falta de manutenção	Manutenção periódica	Manter Controle + Peças sobressalentes
Switch	Falta de manutenção	Manutenção periódica	Manter Controle + Peças sobressalentes