Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Cláudio Oscílio Santos de Mello

GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO UTILIZANDO O “RISK MANAGER”

Rio de Janeiro

2010

Cláudio Oscílio Santos de Mello

GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO UTILIZANDO O "RISK MANAGER"

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro

2010

Cláudio Oscilio Santos de Mello

GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO UTILIZANDO O "RISK MANAGER"

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2010.

Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Dedico este trabalho a duas pessoas muito especiais as quais sempre se sacrificaram para dar uma educação em cima dos pilares da honestidade, amor e da família. Pai e mãe, agradeço de coração toda a dedicação de vocês.

AGRADECIMENTOS

Gostaria de agradecer ao meu gerente Gilmar Martins pela grande batalha, junto à direção do Datasus, à concretização deste curso.

RESUMO

MELLO, Cláudio Oscílio Santos de. **GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO UTILIZANDO O "RISK MANAGER"**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

Esta monografia consiste em contribuir para os profissionais que trabalham com Segurança da Informação, principalmente os da área de TI (Tecnologia da Informação) que terão como responsabilidade a realização da Gestão de Riscos nos ativos da organização. Com o *framework* do *Risk Manager* veremos que é possível estruturar a Gestão de Riscos.

ABSTRACT

MELLO, Cláudio Oscílio Santos de. **GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO UTILIZANDO O "RISK MANAGER"**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

This monograph is to help professionals work with Information Security, especially the area IT (Information Technology) that will have the responsibility the implementation of Risk Management in the organization's assets. With framework of the Risk Manager will see that it is possible to structure the Risk Management.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

TI	Tecnologia da Informação
SI	Segurança da Informação
CERT.br	Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil
DoS	*Denial of Service*
GR	Gestão de Riscos
AAR	Análise e Avaliação de Riscos
ROI	Retorno sobre o investimento
RM	*Risk Manager*

SUMÁRIO

1 INTRODUÇÃO

Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e o uso de computadores de grande porte a estrutura de segurança ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda centralizados. Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados.

Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente, não apenas a imagem da organização perante terceiros, como também o andamento dos negócios organizacionais. É possível inviabilizar a continuidade de uma organização se não for dada a devida atenção à segurança de suas informações.

> *"Neste mundo globalizado, onde as informações atravessam fronteiras com velocidade espantosa, a proteção do conhecimento é de vital importância para a sobrevivência das organizações. Uma falha, uma comunicação com informações falsas ou um roubo ou fraude de informações podem trazer graves consequências para organização, como perda de mercado, de negócios e, consequentemente, perdas financeiras."*
> (NAKAMURA, 2002, pág. 28).

Na sociedade da informação, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isso, a segurança da informação tornou-se um ponto crucial para a sobrevivência das instituições. Os desafios da segurança da informação aumentam de tamanho a cada dia. São tantos os problemas, que os profissionais da área têm uma grande dificuldade de se manter atualizados dada a quantidade de novas vulnerabilidades e as necessidades constantes de correção dos sistemas.

O processo de Gestão de Riscos torna possível a identificação e a correta avaliação dos riscos associados aos ativos de informação que sustentam os negócios das organizações. Com um processo sistemático de identificação, análise, avaliação, tratamento, comunicação e revisão dos riscos, é possível traçar a evolução do nível do risco nos ativos, priorizando, desta forma, os investimentos e iniciativas para a redução dos riscos.

Com o *framework* do *Risk Manager* (RM) é possível estruturar conhecimentos associados a riscos de uma determinada área de conhecimento. Isso é possível pois todo o sistema está baseado nos conceitos de Gestão de Riscos.

2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um ponto crítico para a sobrevivência das organizações na era da informação. A segurança da informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança.

2.1 A TRÍADE DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação tem como objetivo a preservação de três princípios básicos:

2.1.1 **Confidencialidade**

Este princípio diz respeito ao sigilo da informação. A informação deve ser protegida, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.

2.1.2 **Integridade**

Este princípio diz que a informação deve ser protegida contra alterações em seu estado original. Estas alterações podem ser tanto intencionais quanto acidentais.

2.1.3 **Disponibilidade**

Este princípio diz que a informação deve está disponível no momento do acesso por aqueles que dela necessitam.

2.2 CONCEITOS DE SEGURANÇA

2.2.1 **Ativo**

Tudo aquilo que uma organização possui e consequentemente demanda proteção. Existem diversos tipos de ativos. Eles podem ser organizados e classificados através de diversas propriedades, como podemos ver nas Tabelas 1 e 2.

Tabela 1 – Exemplo de classificação dos ativos

Categoria dos ativos	**Exemplo**
Tangíveis	Informações impressas ou digitais Computadores Móveis de escritórios
Intangíveis	Imagem de uma empresa Marca de um produto Confiabilidade de um órgão federal

Tabela 2 – Exemplo de classificação dos ativos

Categoria dos ativos	**Exemplo**
Lógicos	Dados armazenados em um servidor Sistema de ERP Rede de VOIP
Físicos	Estação de trabalho Sistema de ar-condicionado Fábrica
Humano	Empregados Prestadores de serviços

2.2.2 **Ameaça**

Evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas. Um incêndio ou um roubo são exemplos de ameaça.

Há quatro categorias de ameaças possíveis:

- **Interrupção**, na qual o ativo é destruído ou torna-se indisponível (ou inutilizável), caracterizando um ataque contra a disponibilidade. Por exemplo, a destruição de um disco rígido;
- **Interceptação**, na qual um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador), caracterizando um ataque contra a confidencialidade. Por exemplo, cópia não autorizada de arquivos ou programas;
- **Modificação**, na qual um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador) e ainda alterado, caracterizando um ataque contra a integridade. Por exemplo, mudar os valores em um arquivo de dados;
- **Fabricação**, na qual uma parte não autorizada (pessoa, programa ou computador) insere objetos falsificados em um ativo, caracterizando um ataque contra a autenticidade. Por exemplo, a adição de registros em um arquivo.

2.2.3 **Vulnerabilidade**

A ausência de um mecanismo de proteção ou falha em um mecanismo de proteção existente. São as vulnerabilidades que permitem que as ameaças se concretizem.

2.2.4 **Impacto**

Abrangência do prejuízo que a concretização de uma ameaça causará nos processos de negócio. Pode ser avaliado de propriedades mensuráveis, como o seu valor financeiro, o lucro que ele provê ou o custo de substituí-lo, ou propriedades

abstratas, como o comprometimento da imagem da organização por causa do vazamento de uma informação sigilosa.

2.2.5 **Incidente**

Evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade. Segundo a ISO/IEC TR 18044:2004 estes eventos possuem grande probabilidade de comprometer as operações do negócio.

2.2.6 **Risco**

Probabilidade de ameaças explorarem vulnerabilidades. Quanto maior a probabilidade de uma determinada ameaça ocorrer e o impacto que ela trará, maior será o risco associado a este incidente.

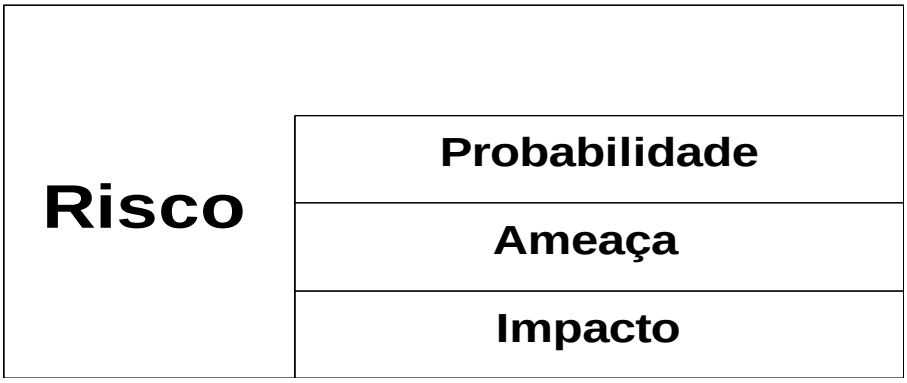


Figura 1 – Risco

2.2.7 **Risco Residual**

É porção que sobra do risco após o tratamento, ou seja, após a aplicação de algum controle para diminuir a sua probabilidade de ocorrência.

2.2.8 **Critério de Risco**

É o que a organização define como risco tolerável. Um risco acima do tolerável terá que ser tratado. Ele se baseia, entre outras coisas, no apetite ao risco, na disponibilidade financeira da organização e nos fatores de mercado aos quais ela está sujeita como o ramo de atuação na qual ela compete.

2.2.9 **Proteção**

São as medidas que adotamos para fornecer segurança aos ativos. Podemos classificar as proteções de diversas formas, como podemos ver nas Tabela 3 e 4.

Tabela 3 – Exemplo de classificação das proteções

Tipo de proteção	**Exemplo**
Lógica	Permissão em sistemas de arquivos *Firewalls* Perfis de usuários em aplicações
Física	Portas Fechaduras Guardas
Administrativa	Políticas de Segurança Normas Procedimentos

Tabela 4 – Exemplo de classificação das proteções

Tipo de proteção	**Descrição**
Preventiva	Evitam que incidentes ocorram
Desencorajadora	Desencoraja a prática de ações
Limitadora	Diminui danos causados
Monitoradora	Monitora estado e funcionamento
Detectora	Detecta a ocorrência de incidentes
Reativa	Reage a determinados incidentes
Corretiva	Repara falhas existentes
Recuperadora	Repara danos causados por incidentes

2.3 A INTERAÇÃO ENTRE OS COMPONENTES DA SEGURANÇA DA INFORMAÇÃO

Na Figura 1 podemos ter uma visão ampla de como os componentes da segurança da informação integarem. Esta figura apareceu pela primeira vez na norma *Trusted Computer System Evaluation Criteria*, popularmente conhecido como *Orange Book.*

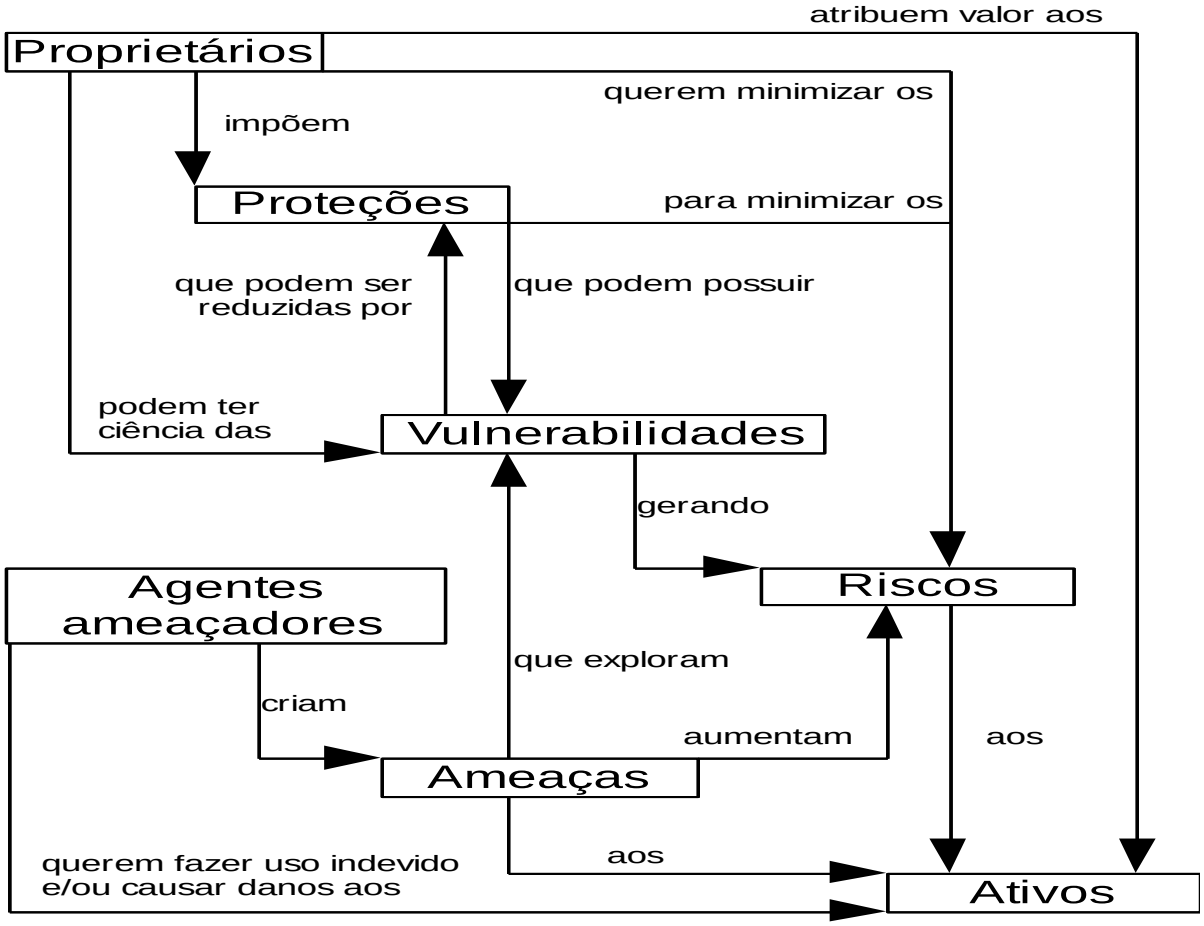


Figura 2 – Interação entre os componentes da segurança da informação

2.4 A IMPORTÂNCIA DA INFORMAÇÃO

Ao longo da história, o ser humano sempre buscou o controle sobre as informações que lhe eram importantes de alguma forma: isso é verdadeiro mesmo na mais remota Antiguidade. O que mudou desde então foram as formas de registros e armazenamento das informações; se na Pré-história e até mesmo nos primeiros

milênios da Idade Antiga o principal meio de armazenamento e registros de informações era a memória humana, com o advento dos primeiros alfabetos isso começou a mudar. Mas foi somente nos últimos dois séculos que as informações passaram a ter importância crucial para as organizações humanas.

Atualmente, não há organização humana que não seja altamente dependente da tecnologia de informações, em maior ou menor grau. E o grau de dependência agravou-se muito em função da tecnologia de informática, que permitiu acumular grandes quantidades de informações em espaços restritos. O meio de registro é, ao mesmo tempo, meio de armazenamento, meio de acesso e meio de divulgação.

Essa característica acarreta consequências graves para essas mesmas organizações, por facilitar os ataques de pessoas não autorizadas.

Independente do setor da economia em que a organização atue, as informações estão relacionadas com seus processos de produção e negócios, políticas estratégicas, de marketing, cadastro de clientes, etc. Não importa o meio físico em que as informações residam, elas são de valor inestimável não só para a empresa que as gerou como também para seus concorrentes. Em último caso, mesmo que as informações não sejam sigilosas, na maioria das vezes elas estão relacionadas com as atividades diárias da empresa e sem elas poderia haver dificuldades.

É importante ressaltar que muitas empresas não sobrevivem mais que poucos dias a um colapso do fluxo de informações, não importando o meio de armazenamento das informações. A atual dependência das organizações, em relação a informática, está se estendendo por toda a economia, tornando aos poucos todas as organizações altamente dependentes dos computadores e, consequentemente, cada vez mais sensíveis aos riscos representados pelo eventual colapso do fluxo de informações de controle.

2.5 POLÍTICA DE SEGURANÇA

A Política de Segurança da Informação de uma organização é um conjunto de documentos que descreve quais são os objetivos que todas as atividades ligadas à SI (Segurança da Informação) devem atingir. Em linhas gerais, a política resume os princípios de SI que a organização reconhece como sendo importantes e que devem estar presentes no dia-a-dia de suas atividades. A existência desses princípios na política também significa que a organização os vê de forma alinhada aos objetivos de negócio.

As políticas são importantes, pois servem como linhas-mestres para todas as atividades de SI desempenhadas em uma organização. São de extrema importância, pois é por meio delas que a estratégia de SI é montada e passada para todas as áreas envolvidas nas mais diversas esferas.

As políticas também demonstram o comprometimento da alta direção da organização com a segurança, ponto fundamental para que ela possa ser gerida de forma eficaz, contando com o apoio da maior quantidade possível de colaboradores.

Podemos dizer que a política trabalha como viabilizador estratégico para objetivos maiores que estão aninhados às necessidades de negócio de cada organização.

O momento ideal para o desenvolvimento da política é antes que um problema de segurança mais grave ocorra, pois a prevenção e o preparo são justamente a sua principal finalidade.

Os problemas relacionados à SI estão no topo da lista de prioridades de muitas organizações. O desenvolvimento de políticas é o ponto crucial na criação de um plano de SI coeso, que possa ser gradualmente implementado e sirva como um norte, evitando iniciativas isoladas que, muitas vezes, desperdiçam recursos e têm a sua efetividade comprometida em virtude da falta de uniformidade.

A necessidade da política também surge quando analisada por uma perspectiva de conformidade legal. Muitas organizações têm seu funcionamento controlado por entidades externas que impõem requisitos em relação à SI. O desenvolvimento das políticas é ponto fundamental em uma série de normas e regulamentações, além de ser incentivado por normas internacionais de melhores práticas. Este fator é importante, pois o não desenvolvimento de políticas pode ser considerado como negligência administrativa, caso a organização seja processada por problemas de SI que tenham causado danos a terceiros como acionistas ou funcionários.

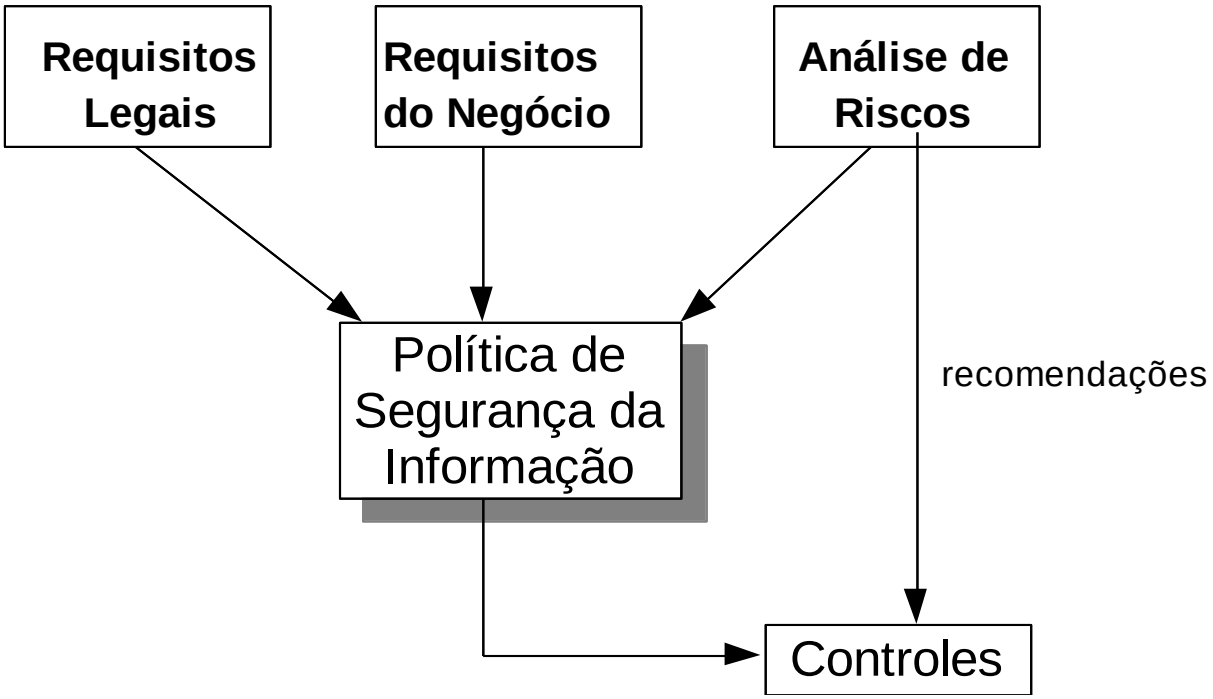


Figura 3 – Requisitos da Política de Segurança

Podemos dizer também que um passo fundamental para o desenvolvimento da política é a realização de uma Análise e Avaliação de Risco, pois através dessa tarefa é possível levantar os pontos prioritários de atenção aos dispositivos e processos de manipulação das informações que estão aninhados às necessidades

de negócio da organização. A prioridade pode ser afetada pela existência ou ausência de controles e vulnerabilidades.

2.6 CLASSIFICAÇÃO DA INFORMAÇÃO

A quantidade de informações que uma organização manipula para desenvolver suas atividades é muito diversa. Mesmo empresas de médio porte possuem pelo menos um servidor de banco de dados contendo bases de clientes e fornecedores, além de informações de cunho financeiro. Da mesma forma que variam os tipos de informações que uma organização possui, variam também suas respectivas necessidades de proteção e, consequentemente, as estratégias utilizadas para alcançar os níveis de segurança desejados.

O processo de classificação da informação consiste em identificar quais são os níveis de proteção que as informações demandam e estabelecer classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas.

No âmbito governamental temos o Decreto nº 4.553, emitido pela Subchefia de Assuntos Jurídicos da Casa Civil, que define níveis de classificação para informações a serem utilizadas na esfera do Governo Federal, conforme podemos ver na Tabela 5.

Tabela 5 – Rótulos de classificação da informação do Decreto nº 4.553

Ultra-secreto
Secreto
Confidencial
Reservado

Já na iniciativa privada há maior liberdade para criação de níveis e atribuição de nomes de acordo com as necessidades de cada empresa, conforme podemos ver um exemplo na Tabela 6.

Tabela 6 – Exemplo rótulos de classificação da empresa privada

Interna
Pública
Restrita
Privada

3 GESTÃO DE RISCOS

Os incidentes relacionados à segurança de dados em empresas seguem aumentando, proporcionalmente ao risco de ataques futuros. É o que se concluiu no relatório estatístico emitido pelo CERT.br [2] acerca dos incidentes de segurança reportados no terceiro trimestre de 2009.

Figura 4 - Incidentes reportados ao CERT.br de Julho a Setembro de 2009

- **Worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **DoS** (*Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **Invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- ***Web***: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

- ***Scan***: notificações de varreduras em redes de computadores com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **Fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **Outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

Como podemos observar, na Figura 4, os ataques estão bem mais direcionados, com alvos bem definidos. O Brasil, por ter uma economia crescente, se torna um foco interessante para os atacantes. O que contribui, também, para o aumento das ameaças é a falta de maturidade das empresas brasileiras nos investimentos em tecnologia. Nos dias atuais não dá mais para pensar em SI pontualmente. As empresas devem encarar o problema de forma mais ampla, pensando no conceito de GR (gestão de riscos).

3.1 OBJETIVOS E BENEFÍCIOS

O processo de GR visa identificar os riscos e tratá-los de forma sistemática e contínua. A GR é composta de quatro atividades principais:

1. Análise e avaliação;
2. Tratamento;
3. Aceitação;
4. Comunicação.

Os benefícios trazidos pelo uso sistemático de um processo de GR são muitos e podemos citar:

- Priorização dos riscos e ações;
- Maior conhecimento sobre o risco;
- Mecanismo para obtenção de consenso;
- Embasamento para as proteções atuais;
- Métrica e indicadores de resultados.

3.1.1 **Priorização dos Riscos e Ações**

Podemos dizer que o principal benefício da GR se confunde com seu próprio objetivo, que é a identificação, priorização e tratamento dos principais riscos aos quais uma organização está sujeita. Dessa forma, seu uso garante que o gestor de SI tem uma ferramenta apropriada para guiar todos os investimentos e iniciativas relacionadas à segurança, fazendo que eles estejam alinhados com os objetivos de negócio da organização.

3.1.2 **Maior Conhecimento Sobre o Risco**

A organização, com a GR, passa a ter um maior entendimento dos próprios riscos aos quais está sujeita. Quando a GR é incorporada à questão operacional da organização, esses riscos passam a ser considerados de forma mais estruturada e próxima ao dia-a-dia. Isso leva a um aumento da consciência a respeito dos riscos e a um compartilhamento sobre o método utilizado, pulverizando o conhecimento e fazendo com que a organização melhor compreenda como funciona a GR como um todo. Todos os funcionários passam a ter uma maior visibilidade da responsabilidade de cada um.

3.1.3 **Mecanismo para Obtenção de Consenso**

Nem sempre é fácil obter consenso sobre quais as melhores medidas de segurança a serem tomadas. Por utilizar um método mais empírico, de fácil

verificação e comprovação, a GR ajuda no processo de obtenção de consenso em relação ao assunto.

3.1.4 **Embasamento para as Proteções Atuais**

A GR pode facilmente justificar os controles existentes, uma vez que a sua remoção levaria a uma vulnerabilidade que seria apresentada na análise, mostrando uma direta elevação do risco.

3.1.5 **Métrica e Indicadores de Resultados**

Em última instância, o risco é a métrica mais importante do processo de Gestão de Segurança. A eficácia de todas as medidas, bem como os resultados trazidos por elas são, na grande maioria, justificada por meio da medição do risco.

3.2 ANÁLISE E AVALIAÇÃO

Durante o processo de AAR (Análise e Avaliação de Risco) é que serão feitos todos os levantamentos em relação às ameaças, vulnerabilidades, probabilidades e impacto aos quais os ativos estão sujeitos. Este é o processo mais trabalhoso e de maior duração na GR. Este é o processo mais crítico, pois todas as informações identificadas aqui irão embasar decisões estratégicas e táticas relacionadas a segurança. Um erro neste processo poderá levar a julgamentos incorretos, comprometendo a efetividade de todo o programa de segurança de uma organização.

Existem basicamente dois métodos que podem ser utilizados para executar esse processo de AAR: quantitativo e qualitativo.

- **Método Quantitativo** – neste tipo de método, a métrica do risco é feita através de uma metodologia na qual tentamos quantificar em termos

numéricos os componentes associados ao risco. Como resultado, o risco é representado em termos de possíveis perdas financeiras, isto é, em termos monetários. Do ponto de vista gerencial, expressar os riscos de maneira monetária permite que pessoas menos familiarizadas com a segurança, especialmente os gestores que serão responsáveis pela liberação de recursos, entendam os riscos com maior clareza.[07]

Mais uma grande vantagem desse método, talvez a melhor, é podermos efetuar uma relação custo / benefício das proteções que desejamos implementar para reduzir os riscos tratados.

Temos como desvantagem o imenso trabalho que envolve uma análise desse tipo, que muitas vezes torna-se impraticável a sua utilização;

- **Método Qualitativo** – neste tipo de método, em vez de usarmos valores numéricos para estimar os componentes do risco, trabalhamos com menções mais subjetivas como alto, médio e baixo. Utilizando este método, os resultados dependem muito do conhecimento do profissional que atribui as notas aos componentes do risco que foram levantados. A necessidade de se ter profissionais capacitados no processo é maior. Podemos claramente citar a velocidade e a menor demanda de recursos como sendo os mais claros benefícios desse método.

A AAR contempla as seguintes etapas:

- Definição do escopo;
- Identificação das ameaças;
- Estimativa da probabilidade de ocorrência das ameaças;
- Estimativa do impacto das ameaças;
- Identificação dos ativos de maior risco;
- Avaliar as melhores proteções;
- Implementar as proteções.

3.2.1 **Definir o Escopo**

Todo projeto deve começar com a definição de seu escopo e a implementação da GR não foge a regra. A definição do tamanho do escopo é um dos principais fatores de sucesso ou fracasso do projeto. Quanto maior o escopo, maior a probabilidade de insucesso no projeto. Para uma organização que vai começar a fazer a GR, digamos, do zero, o melhor é começar com um escopo pequeno, aprender com o processo e aprimorar a forma como ele será implementado aos poucos. Só depois desse "piloto" deve-se pensar em expandir o escopo.

Tabela 7 – Exemplo de escopos da AAR

Categorização	**Como é feito**	**Vantagem**	**Desvantagem**
Por processo de negócio	Primeiro é feito o mapeamento dos processos de negócio e, posteriormente, escolhemos os ativos que suportam cada um deles.	Grande alinhamento da AAR com o negócio da organização, já que os ativos são selecionados de acordo com os processos mais importantes.	Impossível de ser executado caso a organização não possua os processos mapeados. Mapear os processos durante a AAR pode encarecer o projeto, porém a prática é razoavelmente comum.
Por localidade física.	Selecionam-se todos os ativos constantes em um local.	O levantamento de ativos pode ser feito de forma bastante rápida.	Não há alinhamento da lista de ativos com os processos de negócio. Todos os ativos do local serão escolhidos, independente da importância.
Por tipo de ativo.	Dá-se foco a ativos de um determinado tipo, geralmente ativos de TI.	Especialmente eficaz quando a AAR é feita pelo departamento de TI da organização e terá foco predominantemente técnico.	Negligencia ativos importantes pelo simples fato de eles não se enquadrarem na categoria em questão, levando a um alinhamento menor com o negócio.
Mista	Combinam-se os critérios acima de acordo com a necessidade.	Varia de acordo com a aboradagem.	Varia de acordo com a abordagem.

No que diz respeito à GR, o tamanho do escopo é definido pela quantidade de ativos que serão analisados. A abordagem mais alinhada com a estratégia da

organização é escolhê-los de acordo com o(s) processo(s) de negócio que eles suportam. Entretanto, o levantamento do escopo com base nos processos de negócios não é a única opção disponível nem é a mais adequada em todos os casos. Podemos ver maiores detalhes na Tabela 7.

3.2.2 **Identificar as Ameaças**

Nesta etapa identificamos as possíveis ameaças às quais estão sujeitos cada um dos ativos. Alguns cuidados devem ser tomados nesta etapa:

- Trabalhe com ameaças mais genéricas – Em vez de criar uma infinidade de ameaças relacionadas à indisponibilidade de um sistema (erro de usuário, falha de sistema, contaminação por vírus etc.) tente trabalhar simplesmente com “indisponibilidade do sistema”. Existem diversas razões para se usar essa abordagem. A principal delas se deve ao fato que, para esse caso específico iremos tratar praticamente todos os problemas de indisponibilidade de forma semelhante: usando algum sistema de redundância. Outra razão é o fato de que existem infinitas formas de se causar indisponibilidade a um sistema, incluindo alguma que pode estar sendo descoberta agora e que não foi considerada. Por isso, devemos trabalhar com ameaças mais genéricas já que elas são duradouras;
- Tenha foco nas ameaças mais comuns – O conjunto de ameaças que assola um ativo tende ao infinito. Por isso, não existe forma de se cobrir todas as situações, nem é necessário fazer isso. Devemos nos concentrar nas ameaças mais comuns que, em muitos casos, podem representar quase 80% dos incidentes de segurança em termos de volume;

- Trabalhe com listas prontas – Compilar a lista de ameaças por conta própria é um trabalho grande que, na maioria das organizações, demanda recursos de tempo e pessoal que não estarão disponíveis. Use listas de ameaças prontas, mantidas por institutos, grupos de pesquisas, comunidades ou embutidas em ferramentas para GR.

3.2.3 **Estimar a Probabilidade de Ocorrência das Ameaças**

Uma vez que as ameaças foram mapeadas, o passo seguinte é avaliar a probabilidade de elas ocorrerem. A probabilidade pode ser analisada, basicamente, através de dois fatores: freqüência e vulnerabilidade.

A freqüência representa o número de vezes esperado no qual uma ameaça tentará causar algum prejuízo ao ativo. A vulnerabilidade, como dito anteriormente, é a ausência de um mecanismo de proteção ou uma falha em um mecanismo de proteção existente.

3.2.4 **Estimar o Impacto das Ameaças**

Nesta etapa devemos avaliar o impacto que a concretização da ameaça naquele determinado ativo irá causar. Diferentes ameaças causarão diferentes impactos. Porém quanto maior o número de ameaças maior será o risco.

Além do estrago que a ameaça pode causar, outro componente primordial para a definição do impacto seria o valor do ativo para a organização. Este valor pode ser:

- **Absoluto** - como o preço para se adquirir outro ativo igual;
- **Relativo** - associado ao benefício que aquele ativo traz.

3.2.5 **Identificar os Ativos de Maior Risco**

Os ativos sujeitos aos maiores níveis de risco serão priorizados em termos de recursos e proteções.

Entretanto existem proteções cujo custo é reduzido e a adoção é simples. Por exemplo: entre comprar um sistema de redundância para servidores e desenvolver uma norma de acesso físico a um *datacenter*, muitas organizações tenderão priorizar a segunda opção, não por causa do risco e sim por causa do custo. Não há problema em implementar proteções baratas que não afetem necessariamente os ativos de maior risco, desde que essas proteções sejam complementares àquelas que endereçam os riscos mais elevados.

3.2.6 **Avaliar as Melhores Proteções**

É fato de que é muito pouco provável que uma organização tenha recursos disponíveis para, em primeiro momento, trazer todos os riscos identificados para patamares aceitáveis, conforme estabelecido pelo critério de risco.

Por conta dessa escassez de recursos, devemos priorizar os maiores riscos.

O profissional de segurança terá de escolher entre as proteções que tenham a melhor relação custo / benefício. Existem diversas formas de identificar essa relação para soluções em segurança. O ROI (Retorno sobre o Investimento) é uma ótima ferramenta. Ela realiza o cruzamento de dados reais relacionados a custo diretos, indiretos e intangíveis com a projeção de investimentos. Analisando o seu resultado ela consegue, muitas vezes, justificar altos investimentos.

3.2.7 **Implementar as Proteções**

Neste processo, que pode durar vários meses, são implementadas as proteções escolhidas para os ativos.

3.3 TRATAMENTO

Toda vez que um determinado risco estiver acima do critério de risco aceito pela organização ele deverá ser tratado.

Esse tratamento do risco visa trazê-lo para patamares aceitáveis, previamente estabelecido pela organização, através do critério de risco.

Há uma série de medidas que podem ser tomadas para se tratar um risco:

- Evitar – não se expor a uma situação de risco;
- Transferir – compartilhar com um terceiro o ônus de eventuais prejuízos;
- Reter – conviver com o risco;
- Reduzir – implementar uma proteção que reduza o risco;
- Mitigar – tomar medidas que diminuam apenas o impacto.

3.4 ACEITAÇÃO

A aceitação do risco ocorre quando o custo de proteção contra um determinado risco não vale a pena. Isso normalmente ocorre quando o custo de proteção é maior que o custo do próprio ativo que está sendo protegido ou figura numa escala muito próxima a isso. A aceitação também pode ocorrer quando os riscos identificados já se encontram dentro dos patamares de riscos aceitáveis pela organização.

3.5 COMUNICAÇÃO

A comunicação do risco é o último processo de GR e tem o propósito de divulgar todas as informações sobre os riscos que foram identificados a todas as partes envolvidas que precisem ter conhecimento a respeito deles.

Mesmo que o risco não tenha sido tratado ele deve ser comunicado também. Quando estamos compartilhando os riscos às partes envolvidas estamos compartilhando a responsabilidade a respeito deles.

3.6 RESUMO DA GERÊNCIA DE RISCOS

A Figura 5 mostra as etapas da Gerência de Riscos.

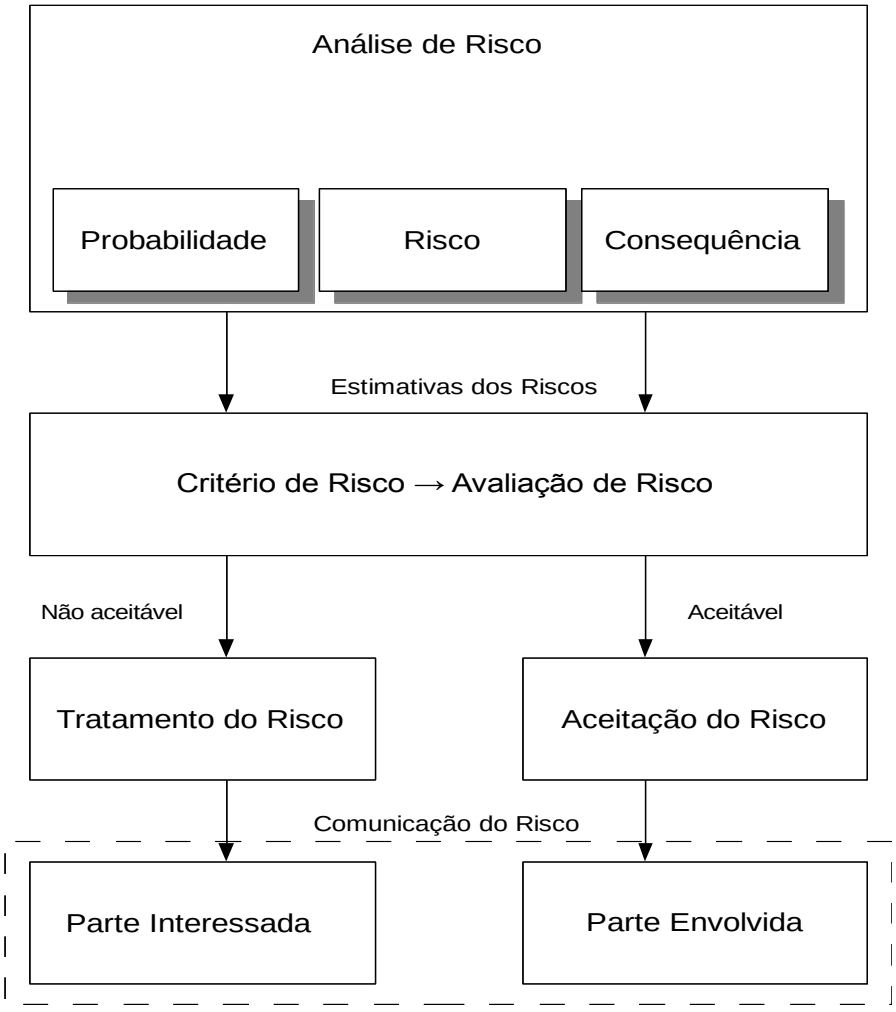


Figura 5 – Gerência de Riscos

4 FERRAMENTA RISK MANAGER

A ferramenta RM [7] é um aplicativo da empresa Módulo que provê um *framework* para automação da Gestão de Riscos, possibilitando o gerenciamento dos riscos em ativos tecnológicos e não tecnológicos (pessoas, ambiente e processos), bem como seus respectivos eventos de tratamento.

4.1 FUNCIONAMENTO

Através do ciclo Inventariar, Analisar, Avaliar e Tratar, o RM permite mensuração e controle dos riscos (Figura 6).

Figura 6 – Ciclo de Gestão de Riscos

- **Inventariar:** Mapeamento dos ativos da organização, processos de negócios, sistemas, serviços e ameaças. A estruturação do inventário é facilmente implementada pela definição de perímetros organizacionais, físicos ou processuais, além do uso de recursos que automatizam toda a atividade de levantamento.

- **Analisar:** A partir de Bases de Conhecimento atualizadas constantemente por uma equipe de pesquisadores da Módulo, o RM auxilia a realização de análises de riscos de ativos dos mais diversos tipos. As análises podem ser automatizadas com o uso de coletores automáticos, questionários *WEB*, questionários *offline* e PDA. São mais de 4.000 coletores automáticos para diversos ativos (tecnológicos ou não), compreendendo mais de 11.000 controles.
- **Avaliar:** Cada recurso é pontuado de acordo com sua relevância para os negócios da organização. A Avaliação dos Riscos é realizada por meio da geração de relatórios objetivos e práticos, em visões executivas, táticas e operacionais, que podem ser apresentadas em diferentes formas, viabilizando verificar quais os ativos ou processo de negócio possuem riscos mais elevados. Através de um módulo específico, os riscos podem ser categorizados como aceitáveis ou então endereçados para tratamento.
- **Tratar:** No tratamento dos riscos é onde implementamos os controles de forma a reduzir os riscos, que já foram identificados, para patamares aceitáveis. O acompanhamento da evolução dos riscos pode ser medido através de análises consecutivas.

4.2 PRINCIPAIS CARACTERÍSTICAS

- Interface simples e intuitiva;
- Visão dos ativos integrados aos processos de negócios da organização;
- Análise integrada de tecnologia, processos, pessoas e ambiente físico;
- Informações consolidadas sobre análise de riscos;
- Geração automática de relatórios, gráficos e estatísticas;

- Coletores automáticos para os mais diversos ativos tecnológicos;
- Conjunto de Bases de Conhecimento com mais de 11.000 controles;
- Controle de acesso, auditoria e proteção de dados com criptografia;
- *Live Update*: Atualização automática de versões e Bases de Conhecimento;
- Repositório centralizado de ativos;
- Permite que os riscos sejam visualizados de diferentes formas: por ativos, perímetros, componentes de negócios, ameaças, entre outros;
- Customização de perímetros, adaptando-os à realidade da organização;
- Mais de 4.000 coletores automáticos para diversos ativos tecnológicos;
- Inclusão de fotos e arquivos como evidências em análises de segurança e em processos de auditoria;
- Customização de entrevistas via *Web* para adaptar o padrão de linguagem usada nos questionários gerados à realidade da organização.

4.3 BENEFÍCIOS

- Criação de *Risk Scorecard*, provendo um ponto-de-vista executivo sobre os riscos para a organização incluindo índices e métricas;
- Visão dos riscos relacionados ao negócio, permitindo priorizar investimentos de acordo com a importância de cada ativo;
- Mapeamento da evolução dos riscos;
- Console único para gestão de riscos;
- Planejamento e gestão da segurança: utilização de conhecimento e monitorando os riscos de maior impacto negativo para o negócio;
- Visão georreferenciada dos riscos;
- Auditorias mais efetivas e menos dispendiosas;

- Gerenciamento dos requisitos de segurança, reduzindo custos com múltiplas auditorias e eliminando controles redundantes;
- Demonstração clara da performance da Gestão de Riscos, de acordo com leis, regulamentações e padrões;
- Maior produtividade da equipe interna e qualificação da força de trabalho através do uso de Bases de Conhecimento constantemente atualizadas.

4.4 CÁLCULO DO RISCO

O RM utiliza um método de cálculo de riscos que calcula um índice denominado PSR (Probabilidade, Severidade e Relevância).

- **Probabilidade** – a ocorrência da vulnerabilidade ser explorada pela ameaça;
- **Severidade** – a consequência da vulnerabilidade ser explorada pela ameaça;
- **Relevância** – o comprometimento da segurança do ativo.

Este índice define o risco para cada controle ausente na Análise de Riscos. No RM, a fórmula do risco leva em consideração não apenas os aspectos operacionais que levam ao risco, como a Probabilidade e a Severidade, mas também o quanto este risco irá impactar no negócio da Organização, aspecto esse traduzido através das variáveis Severidade e Relevância.

No RM, a fórmula do risco é calculada, então, pela seguinte equação:

RISCO = Probabilidade X Severidade X Relevância

Este valor de Risco PSR representa o grau de risco associado à ausência de um controle. Os fatores de Probabilidade e Severidade são pontuados durante as análises técnicas, e a Relevância pontuada considerando-se a visão do negócio, em termos da relevância do ativo para a Organização.

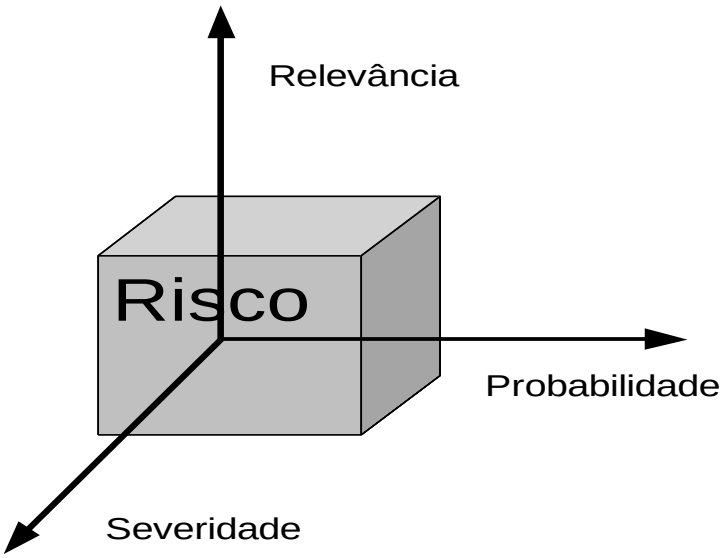


Figura 7– PSR

O valor máximo que o PSR pode assumir é 125. Veja a Tabela 8.

Tabela 8 – Valores Possíveis do PSR

Nível de Risco	**Valores Possíveis do PSR**
Muito baixo	1, 2, 3, 4, 5 ou 6
Baixo	8, 9, 10, 12, 15 ou 16
Médio	18, 20, 24, 25, 27 ou 30
Alto	32, 36, 40, 45, 48 ou 50
Muito alto	60, 64, 75, 80, 100 ou 125

Para os ativos, o seu índice de risco é o resultado da soma algébrica dos PSR dos controles ausentes, ou seja, não implementados.

Quanto ao processo decisório para o tratamento dos riscos, o RM sugere as seguintes interpretações e ações em relação aos resultados do PSR:

- **PSR Muito Alto** - são riscos inaceitáveis, e os gestores dos ativos devem ser orientados para que minimizem imediatamente;
- **PSR Alto** - são riscos inaceitáveis e os gestores dos ativos devem ser orientados para pelo menos controlá-los;

- **PSR Médio** - são riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos, contudo a aceitação do risco deve ser feita por meios formais;
- **PSR Baixo** - são riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos;
- **PSR Muito Baixo** - são riscos aceitáveis e devem ser informados para os gestores dos ativos.

4.5 PROCESSO DE GESTÃO DO RISCO

Conforme já descrito no item 4.1 o RM é fundamentado em um ciclo contínuo para Gestão de Riscos conforme as seguintes fases: Inventariar, Analisar, Avaliar e Tratar. Veremos agora as tarefas a fazer em cada fase no RM.

4.5.1 **Iniciando o *Risk Manager***

Somente pessoas cadastradas no RM estão autorizadas a acessar o sistema para analisar Ativos, gerenciar Projetos de Análises, gerenciar Perímetros ou executar outras funções nos módulos do sistema.

Os usuários devem ser previamente cadastrados de acordo com o seu perfil:

- ***Security Officcer*** – é o usuário com o maior poder de utilização do sistema;
- **Gestor** – tem as mesmas funcionalidades do *Security Officcer*, porém restrito apenas a um Perímetro;
- **Analista** – restrito a realização de Análises sobre sua responsabilidade.

Veja tela inicial do RM na Figura 8.

Figura 8 – Tela inicial do RM

- **Organização –** no RM uma Organização representa uma empresa, órgão ou outra corporação e é o elemento raiz para a estruturação de seus Ativos. O RM é um sistema multi-organizações e permite que uma ou mais Organizações possam ser criadas. No entanto, somente uma Organização pode ser utilizada por vez numa mesma sessão. Veja a Figura 9.

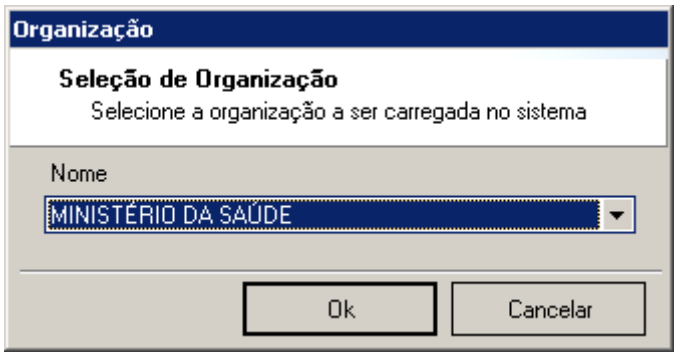


Figura 9 – Tela Organização do RM

- **Recursos Humanos –** os responsáveis por áreas ou processos da Organização devem ser cadastrados utilizando uma funcionalidade do RM que é a Recursos Humanos. Estas pessoas não terão permissões

de acesso ao sistema. A finalidade do seu cadastro é a definição delas como responsáveis por Perímetros ou Ativos. Veja Figura 10.

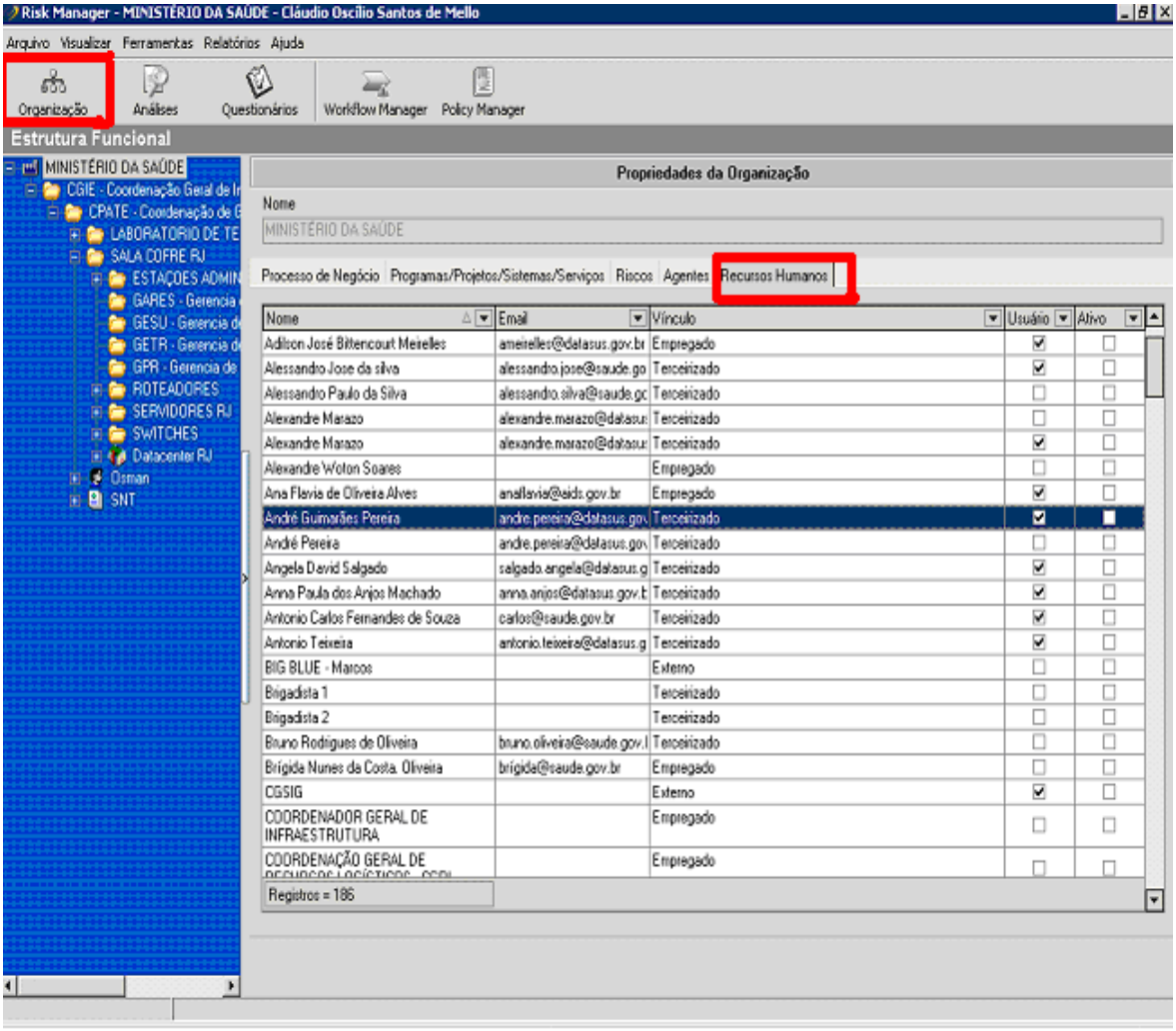


Figura 10 – Tela de Recursos Humanos

- **Processo de Negócio –** é um processo de alto nível (financeiro, comercial, tecnológico, etc.) ou um ativo intangível (imagem, capacidade de controle, etc.) que contribui de forma significativa para a geração de receita da Organização, tem elevada importância estratégica, ou ainda algum outro atributo que o torne merecedor de um tratamento diferenciado dos demais processos da Organização. Em resumo, Processos de Negócio são definidos em função da visão que a

organização tem do que representa “valor relevante”. Sendo assim existem Ativos que suportam esses processos e estes Ativos precisarão ter seus riscos gerenciados. Veja Figura 11.

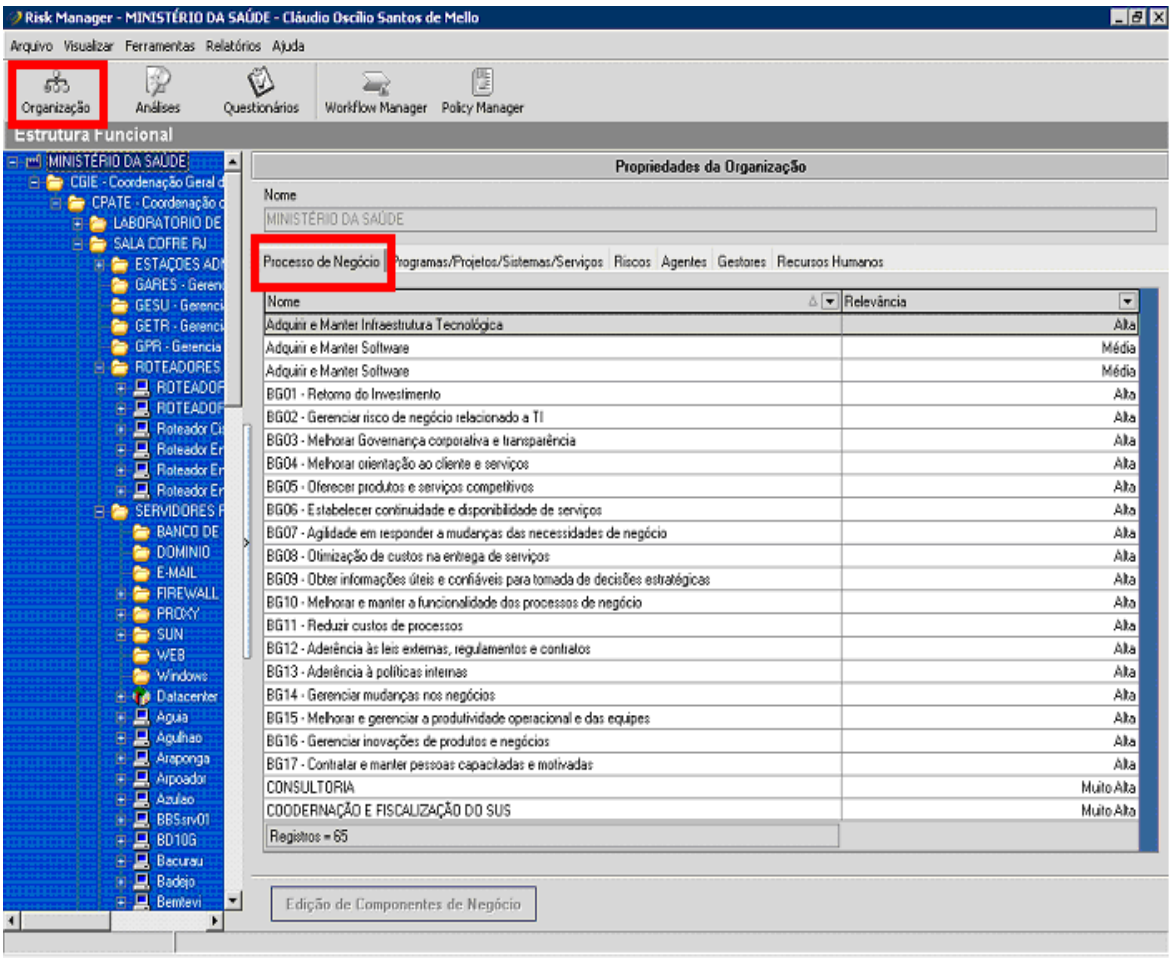


Figura 11 – Tela de Processos de Negócio

- **Sistemas e Serviços –** as Organizações possuem Sistemas e Serviços que sustentam os seus negócios. Normalmente um gestor possui dificuldades para citar quais ativos suportam seus negócios, pois apesar de conhecerem muito bem o negócio da Organização, desconhece em detalhes sua infra-estrutura. Da mesma forma, departamentos mais operacionais possuem domínio da infra-estrutura organizacional, porém não possuem uma visão ampla das áreas de

negócio e suas relações. A Camada de Sistemas e Serviços do RM deve ser utilizada como um tradutor do ambiente operacional para o ambiente de negócios. Veja Figura 12.

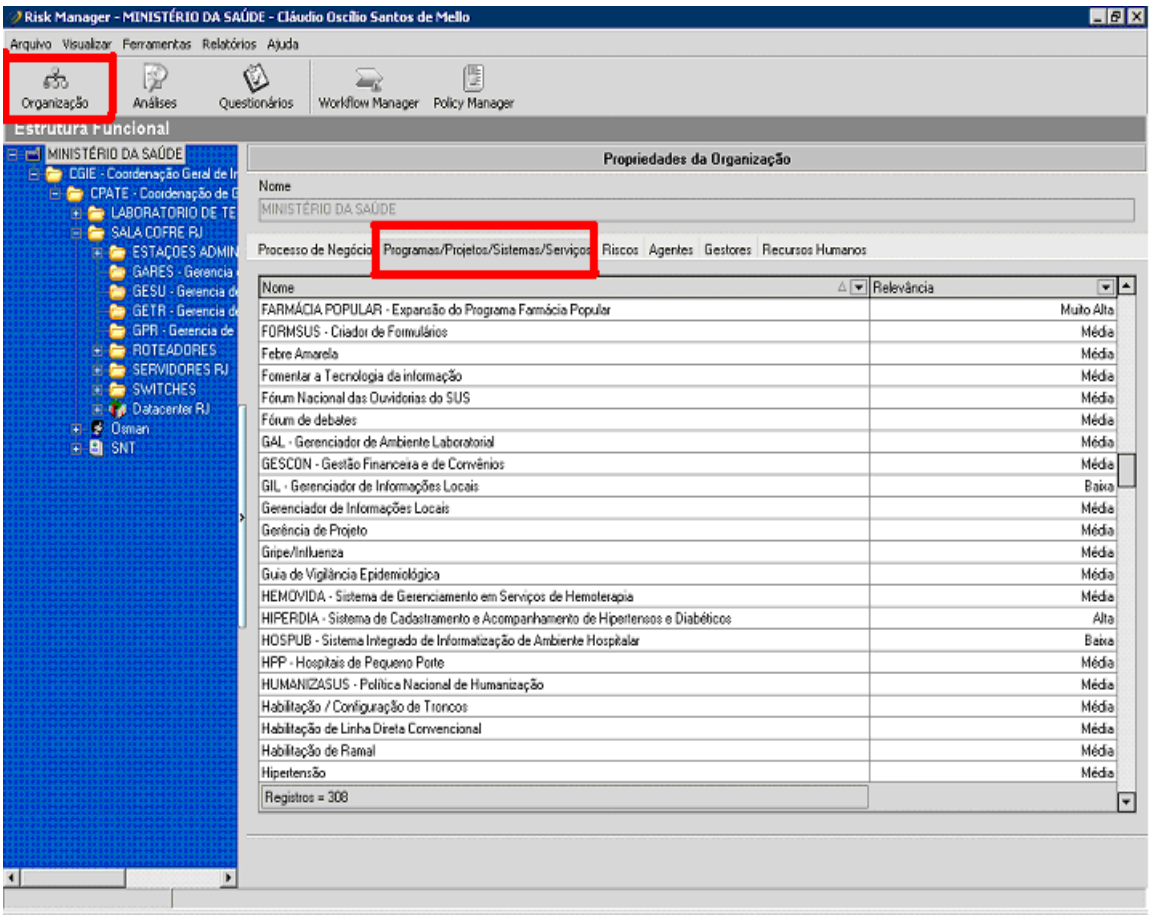


Figura 12 – Tela de Sistemas e Serviços

- **Agentes das Ameaças –** os Agentes são os sujeitos das Ameaças. São os elementos com os quais a alta direção da Organização se preocupa, e devem ser relacionados com as Ameaças. Representam as entidades que através de técnicas, conhecimentos ou acontecimentos podem concretizar incidentes junto aos processos e atividades da Organização.

  As Ameaças por sua vez são de caráter abrangente e cobrem as origens humanas, técnica e ambiental. Caracterizam-se por ações ou

fenômenos internos ou externos à Organização, de caráter acidental ou intencional. Veja Figura 13.

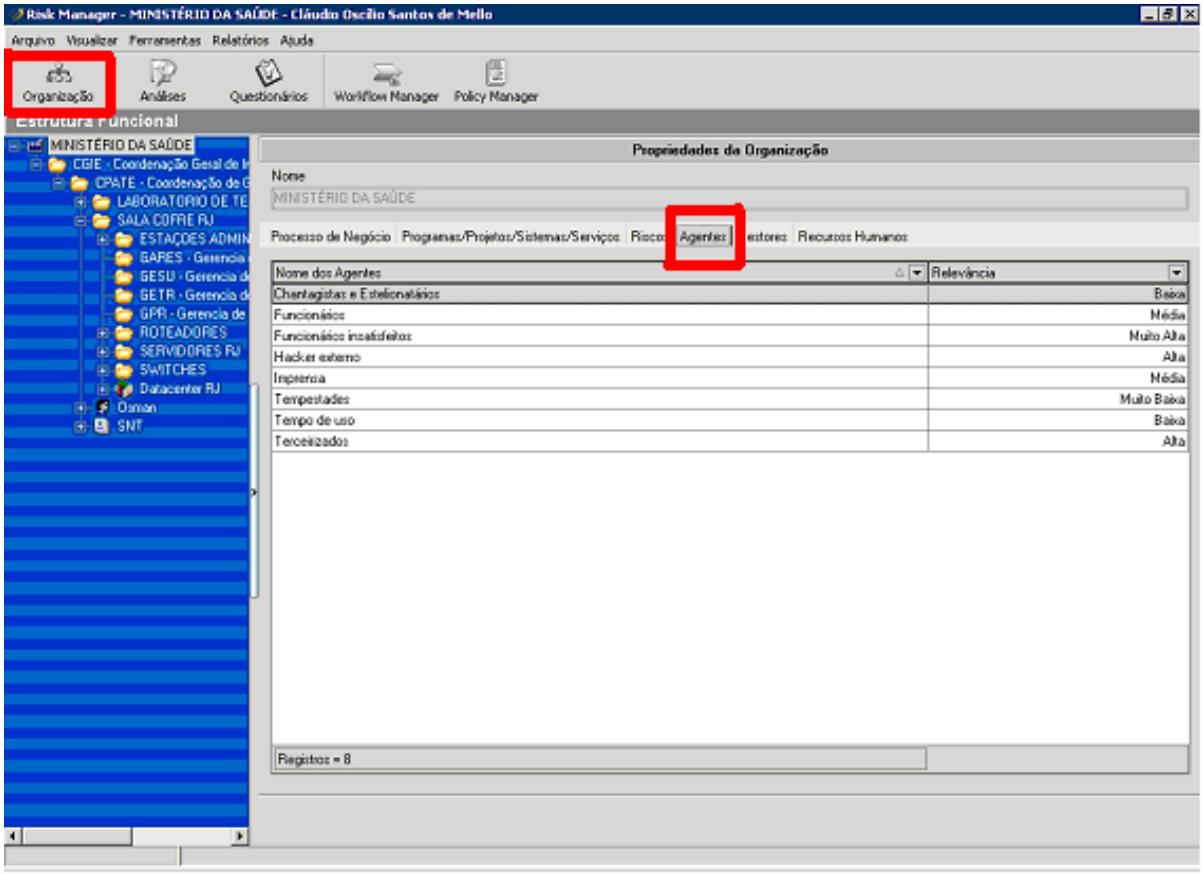


Figura 13 – Tela de Agentes das Ameaças

4.5.2 **Inventariar**

Nesta primeira fase do ciclo de Gestão de Riscos, as tarefas a realizar correspondem ao conjunto de ações necessárias para levantamento, detalhamento e estruturação de Perímetros e Ativos que impactam os objetivos, missão e atividades-fim da Organização.

- **Perímetros –** perímetros são fronteiras físicas ou lógicas que existem dentro da Estrutura Funcional da Organização e servem para organizar a distribuição dos Ativos. Cada Organização pode estruturar seus Perímetros da forma mais particular possível. No entanto, é

fundamental que a Estrutura Funcional reflita a forma como a organização é estruturada. Veja Figura 14.

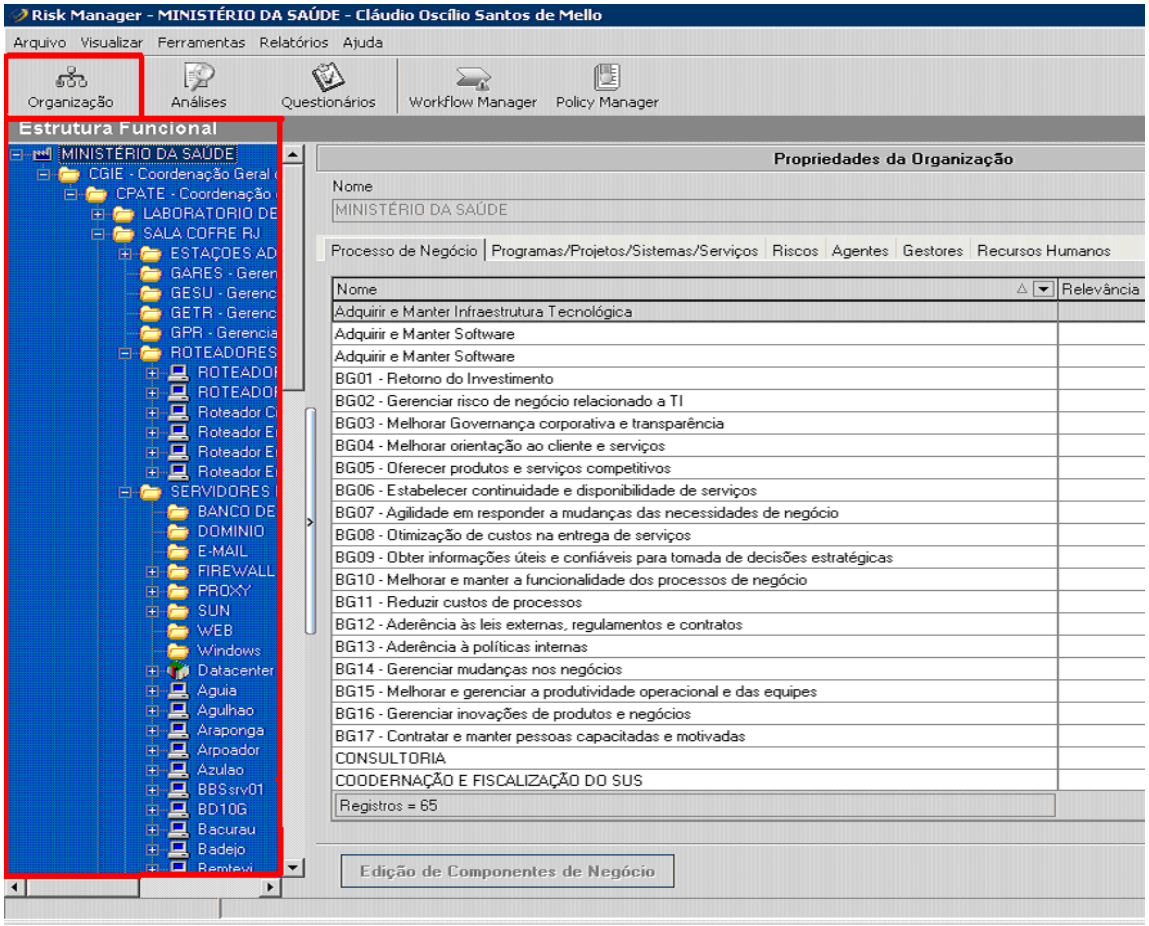


Figura 14 – Tela de Perímetro

- **Ativos –** no RM os Ativos são elementos que devem ser cadastrados dentro de Perímetros que foram criados para esta finalidade. Lembre-se que as Análises de Riscos focarão as atenções nestes elementos, pois são neles que residem vulnerabilidades que deverão ser gerenciadas através da implementação de controles. Veja Figura 15.

  O RM classifica os Ativos em 4 grupos:

  - Processos;
  - Pessoas;
  - Tecnologia;
  - Ambiente.

Cada Ativo no RM possui uma série de atributos que devem ser informados:

- **Relevância –** é o grau de importância do Ativo para o Negócio da Organização, considerando os Sistemas e Serviços que ele suporta. É um campo numérico que informa ao sistema um dos componentes para o cálculo do Risco PSR, ou seja, a variável R.
- **Relacionamento com Sistemas e Serviços –** é fundamental que os Ativos sejam relacionados com os Sistemas e Serviços já cadastrados no RM. Este relacionamento é o caminho para que os riscos, calculados através de análises nestes Ativos, possam ser processados gerando os riscos de cada Sistema e Serviço, da mesma forma como dos Processos de Negócios.

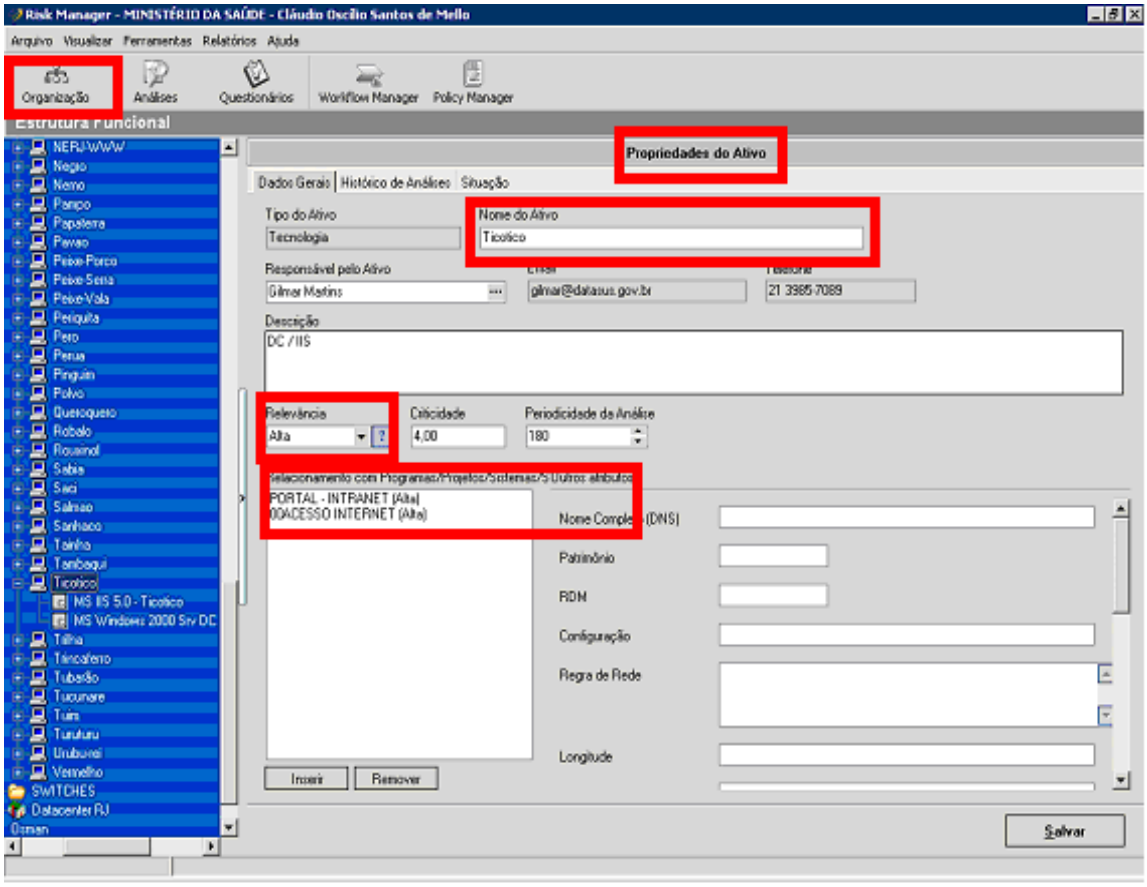


Figura 15 – Tela de Ativo

Cada tipo de Ativos disponibiliza uma lista particular de Componentes que poderão ser associados a ele. Esses Componentes podem ser do tipo: Pessoa, Processo, Tecnologia e Ambiente. Por exemplo: Se um Ativo for do tipo Tecnologia ele pode ter associado a ele um Componente de Sistema Operacional Windows XP.

Cada Componente será analisado utilizando uma *Knowledge Base*. Veja Figura 16.

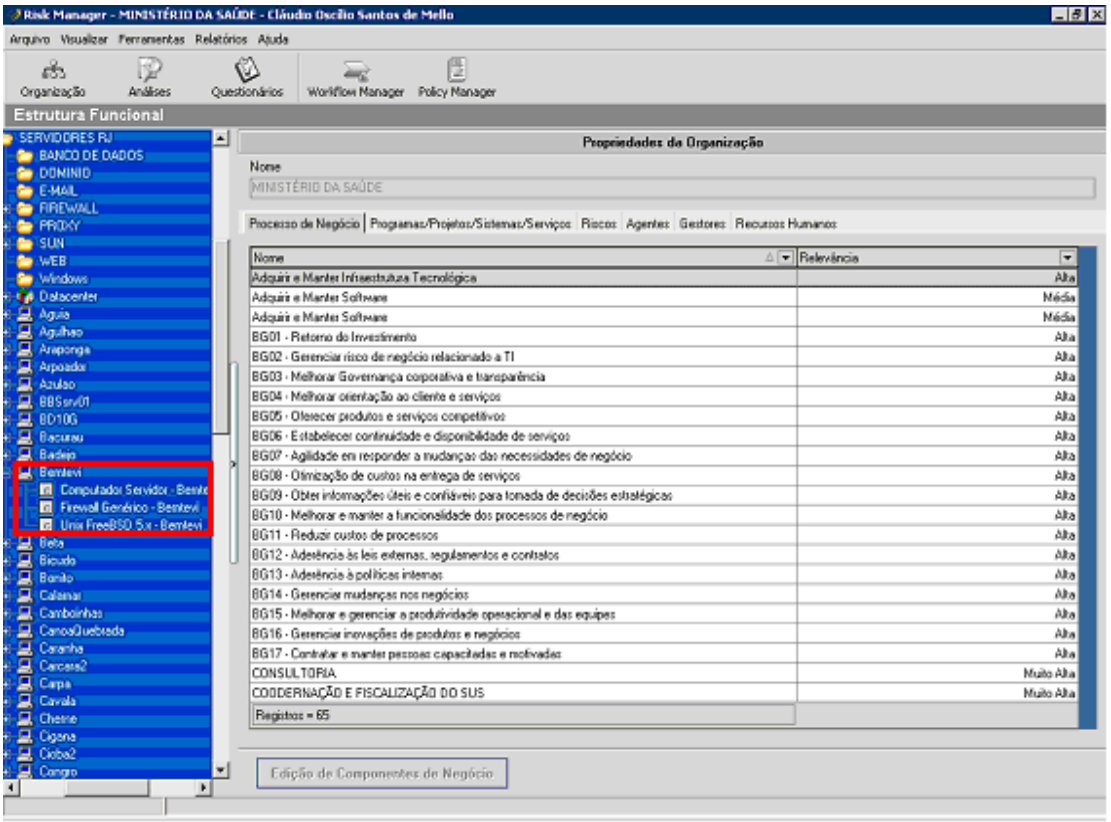


Figura 16 – Tela de Ativo e seus Componentes

4.5.3 **Analisar**

Nesta segunda fase do ciclo de Gestão de Riscos, teremos que criar o Projeto de Análise e definir o Escopo desse Projeto. Este Escopo será composto por

alguns Ativos já cadastrados na primeira fase do ciclo. O Escopo do Projeto corresponde a uma “parte” do Perímetro da Estrutura Funcional da Organização.

É recomendável que se evite definir um Escopo com todos os Ativos da Organização, pois este projeto tende a ser de longa duração e isto prolongará o início das atividades seguintes. O Escopo deve ser bem planejado e atender um objetivo específico. Por exemplo:

- Por localidade física - análise de uma determinada filial, de uma sala contendo equipamentos ou colaboradores específicos;
- Por tipo de ativo - análise dos servidores do escritório.

Veja na Figura 17 a criação do Projeto de Análise e a Figura 18 com a definição do Escopo da Análise.

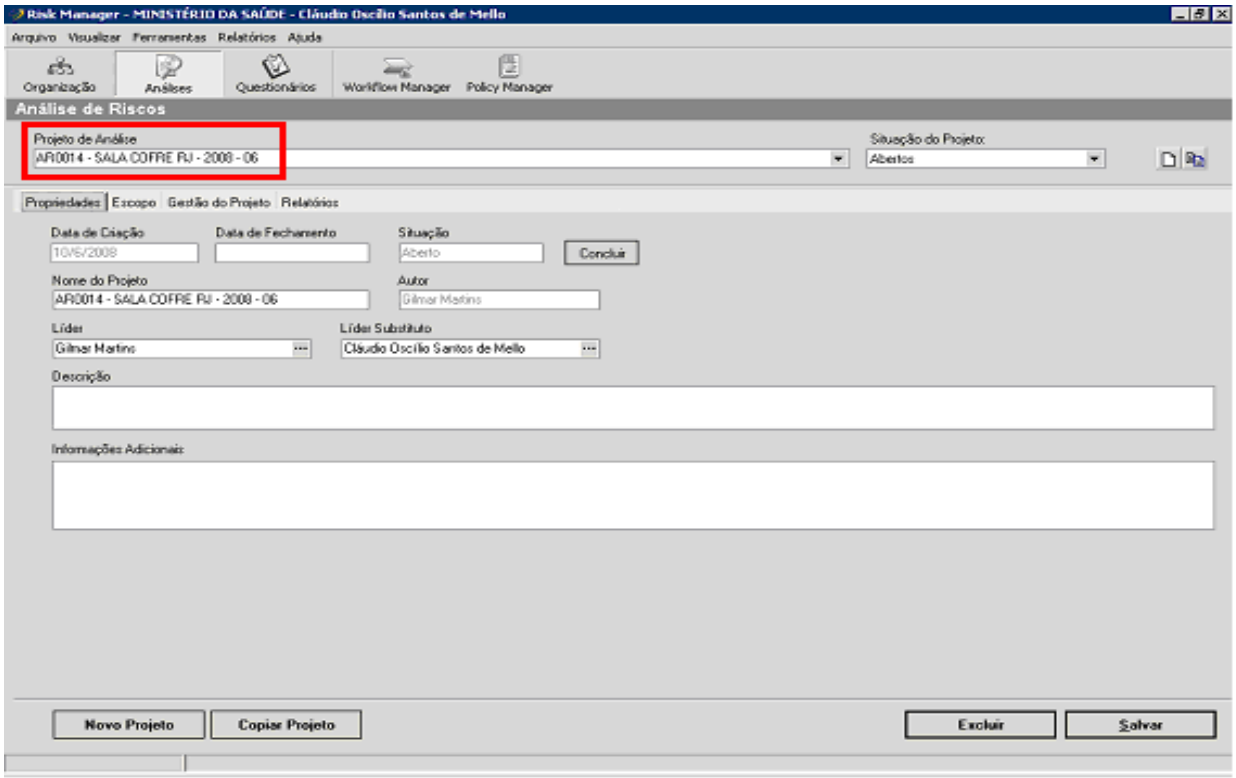


Figura 17 – Tela de Projeto de Análise

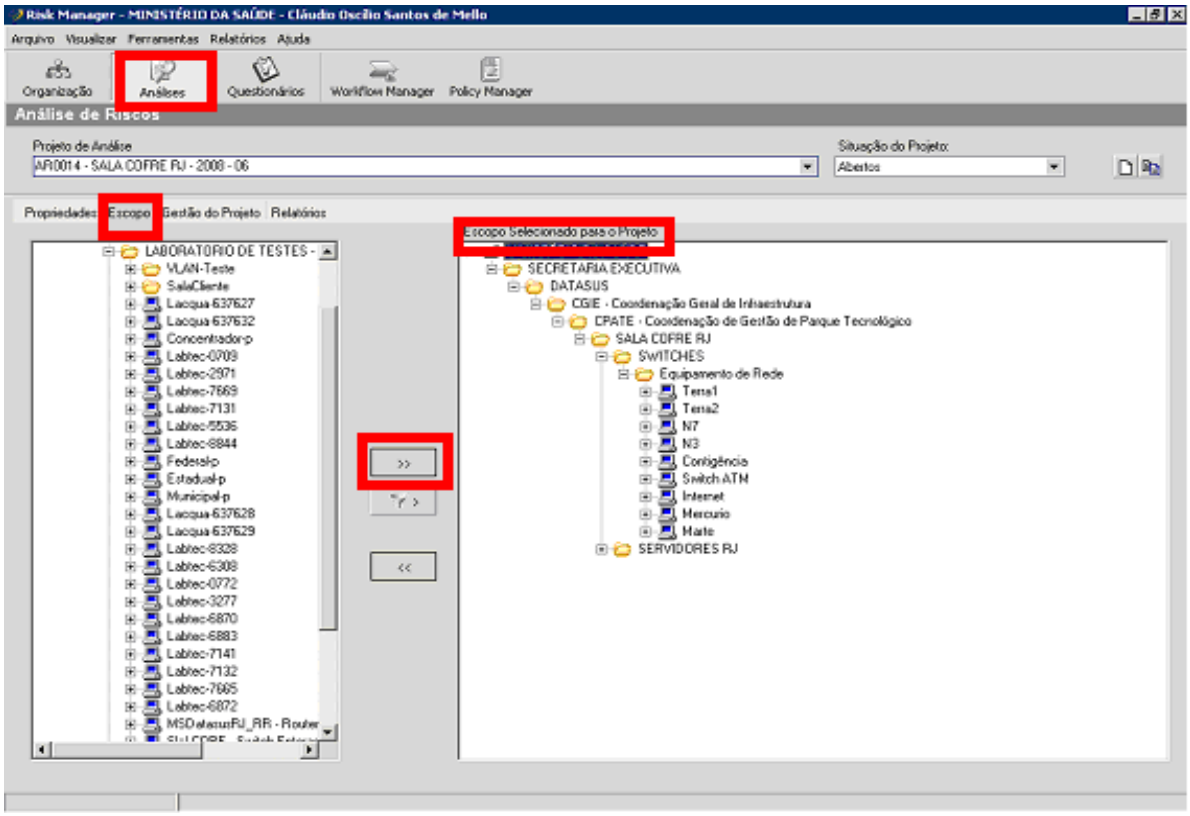


Figura 18 – Tela de Escopo da Análise

O Projeto de Análise consiste de um conjunto de Análises de Componentes incluídos no Escopo, que serão efetuadas a partir do preenchimento dos respectivos Questionários pelos Analistas designados.

A aba Gestão do Projeto da Análise permite acompanhar o andamento das Análises de Componentes desempenhadas pelos Analistas do Projeto. Veja Figura 19. Através de algumas informações nesta tela consegue-se acompanhar algumas informações do Componente do Ativo:

- **Situação** - é o estado associado à geração e ao preenchimento do Questionário referente à Análise do Componente. Pode assumir um dos valores:
    - Não Gerado - é o estado inicial ao ser inserido um novo Componente no Escopo do Projeto;

- Aberto - é o estado em que o Questionário já foi gerado e a Análise está em andamento;
- Fechado - é o estado em que a Análise do Componente foi concluída.

- **% Preenchido** - para os Questionários parcialmente respondidos, este valor é atualizado à medida que a Análise vai sendo executada;
- **PSR** - ao final do preenchimento do Questionário (100% respondido) o valor do Risco do Componente é apresentado neste campo.

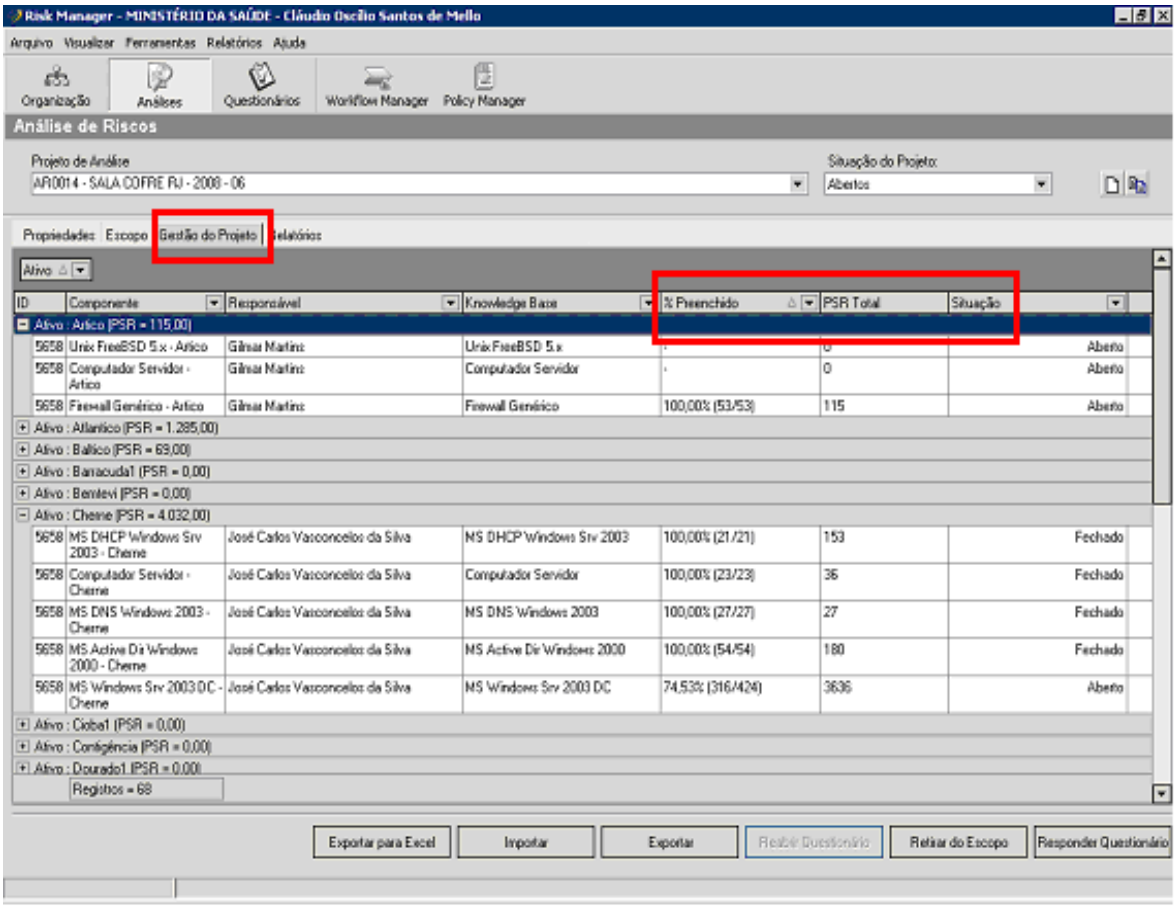


Figura 19 – Tela de Gestão do Projeto da Análise

Para cada Componente de um Ativo teremos um Questionário de respostas associado. Este Questionário é composto por uma série de Controles. Esses

Controles são elementos chaves para a Gestão de Riscos pois representam as boas práticas de segurança aplicáveis à grande parte das Organizações.

Os Controles podem ser respondidos em qualquer ordem. Cada Controle deverá ser respondido segundo uma das opções disponíveis:

- **Implementado** - o Controle está totalmente implementado no Ativo, ou seja, aquela boa prática está aplicada no Ativo;
- **Não Implementado** - o Controle está apenas parcialmente implementado ou não implementado no Ativo, ou seja, aquela boa prática não existe ou está sendo implementada de forma deficiente;
- **Não Aplicável** - o Controle não se aplica ao contexto da Análise.

No Questionário poderemos ver Detalhes da prática do Controle. Veja as Figuras 20 e 21.

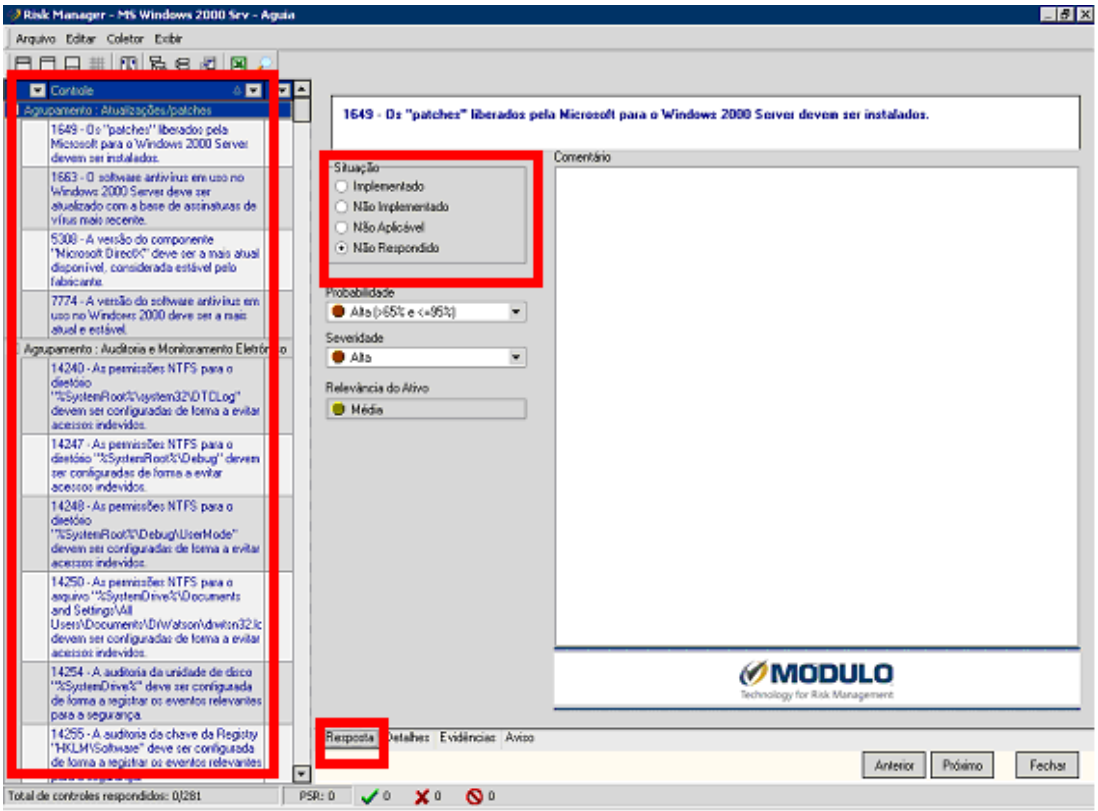


Figura 20 – Tela de Questionário

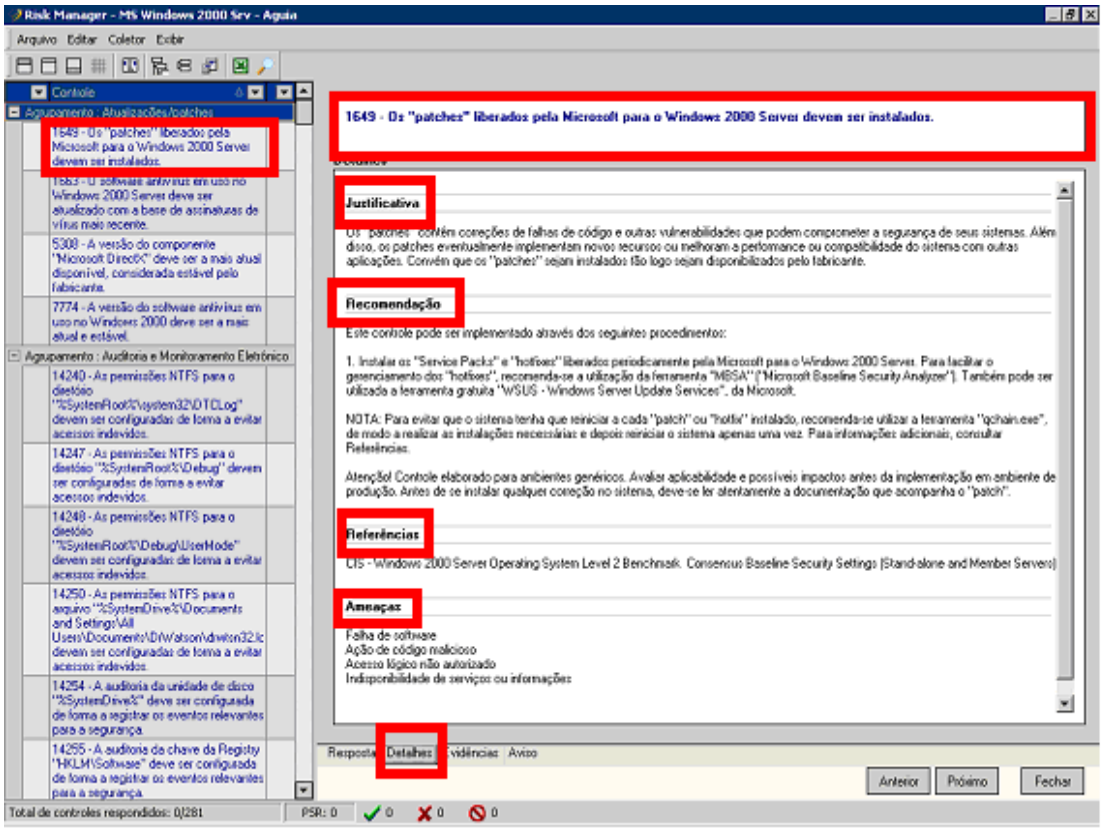


Figura 21 – Tela de Detalhes do Questionário

4.5.4 **Avaliar**

Nesta terceira fase do ciclo de Gestão de Riscos o RM disponibiliza vários tipos de Relatórios. Esses Relatórios podem ser no formato de Tabelas, Gráficos e Documentos. Tais Relatórios são as primeiras ferramentas a serem utilizadas para se realizar a Avaliação dos Riscos.

As Tabelas e Documentos podem ser gerados para o nível técnico ou gerencial. Os Gráficos geralmente são voltados para o nível gerencial ou executivo.

Os resultados desses Relatórios podem ser individuais, referentes a um Componente ou um Ativo, ou geral, consolidando as Análises de vários Componentes e Ativos.

Vários são os Relatórios disponibilizados pelo RM, entre eles temos:

2.1. Controles não Implementados em ativos (Compliance)

A tabela abaixo resume os ***10*** principais ativos com controles não implementados que devem ser priorizados. Na tabela, está sendo considerado apenas o total de controles aplicáveis para os cálculos, desconsiderando-se os não aplicáveis.

Ativo	Tipo do Ativo.	Relevância	Total Aplicável	Controles Implem.	Compliance Index	Controles não Implem.	Non-Compliance Index	CN / Total TA
			TA	CI	CI / TA	CN	CN / TA	
Cherne	Tecnologia	Média	429	276	64.34%	153	35,66 %	15.89%
Jupiter2	Tecnologia	Baixa	114	0	0.00%	114	100,00 %	11.84%
HFRIORJ2	Tecnologia	Muito Baixa	114	68	59.65%	46	40,35 %	4.78%
Atlantico	Tecnologia	Muito Alta	123	93	75.61%	30	24,39 %	3.12%
Artico	Tecnologia	Muito Alta	46	43	93.48%	3	6,52 %	0.31%
Baltico	Tecnologia	Média	46	43	93.48%	3	6,52 %	0.31%
Indico	Tecnologia	Média	45	42	93.33%	3	6,67 %	0.31%
Mar-Vermelho	Tecnologia	Muito Baixa	46	43	93.48%	3	6,52 %	0.31%
Pacifico	Tecnologia	Média	0	0	0.00%	0	0,00 %	0.00%
Terra1	Tecnologia	Média	0	0	0.00%	0	0,00 %	0.00%
TOTAL (10)			**963**	**608**	**63.14%**	**355**	**36,86%**	**36.86%**
OUTROS (13)			**0**	**0**	**0.00%**	**0**	**0,00%**	**0.00%**
TOTAL GERAL (23)			**963**	**608**	**63.14%**	**355**	**36.86%**	**36.86%**

- *Os **10 ativos** acima correspondem a **43,48%** da quantidade total de ativos no escopo **(23)**, e seu índice de compliance foi de **63.14%**.*

2.2. Riscos encontrados nos Ativos (Risk)

A tabela abaixo resume os ***10*** principais ativos com riscos que devem ser priorizados ser priorizados. Estão sendo considerados apenas os controles aplicáveis para os cálculos, desconsiderando os não aplicáveis.

Ativo	Tipo do Ativo.	Relevância	Total Aplicável	Riscos Evitados	Security Index	Riscos Existentes	Risk Index	EX / TOTAL AP
			AP	EV	EV / AP	EX	EX / AP	
Cherne	Tecnologia	Média	11559	7527	65.12%	4032	34,88 %	15.05%
Jupiter2	Tecnologia	Baixa	2148	0	0.00%	2148	100,00 %	8.02%
HFRIORJ2	Tecnologia	Muito Baixa	1048	647	61.74%	401	38,26 %	1.50%
Atlantico	Tecnologia	Muito Alta	6240	4955	79.41%	1285	20,59 %	4.80%
Artico	Tecnologia	Muito Alta	2425	2310	95.26%	115	4,74 %	0.43%
Baltico	Tecnologia	Média	1455	1386	95.26%	69	4,74 %	0.26%
Indico	Tecnologia	Média	1428	1359	95.17%	69	4,83 %	0.26%
Mar-Vermelho	Tecnologia	Muito Baixa	485	462	95.26%	23	4,74 %	0.09%
Pacifico	Tecnologia	Média	0	0	0.00%	0	0,00 %	0.00%
Terra1	Tecnologia	Média	0	0	0.00%	0	0,00 %	0.00%
TOTAL (10)			**26788**	**18646**	**69.61%**	**8142**	**30,39%**	**30.39%**
OUTROS (13)			**0**	**0**	**0.00%**	**0**	**0,00%**	**0.00%**
TOTAL GERAL (23)			**26788**	**18646**	**69.61%**	**8142**	**30.39%**	**30.39%**

- *Os riscos encontrados nestes primeiros 10 ativos correspondem a **30.39%** do total dos riscos aplicáveis no escopo.*

Figura 22 – Tela de Relatório de Análise de Riscos

- **Relatório de Análise de Riscos (RAR)** – o objetivo deste Relatório é apresentar o resultado final de um ou um grupo de Projetos de Análises em termos gerenciais, consolidando os riscos encontrados durante o processo. Veja Figura 22 com parte de um RAR;
- **Relatório Operacional de Riscos (ROR)** – o objetivo deste Relatório é orientar o gestor na priorização das recomendações que devem ser aplicadas, de acordo com o seu nível de risco (PSR).

Veja Figura 23 com o Relatório dos 10 Controles com Maior Risco de um Ativo e Figura 24 com a Situação dos Riscos dos Ativos do Perímetro selecionado.

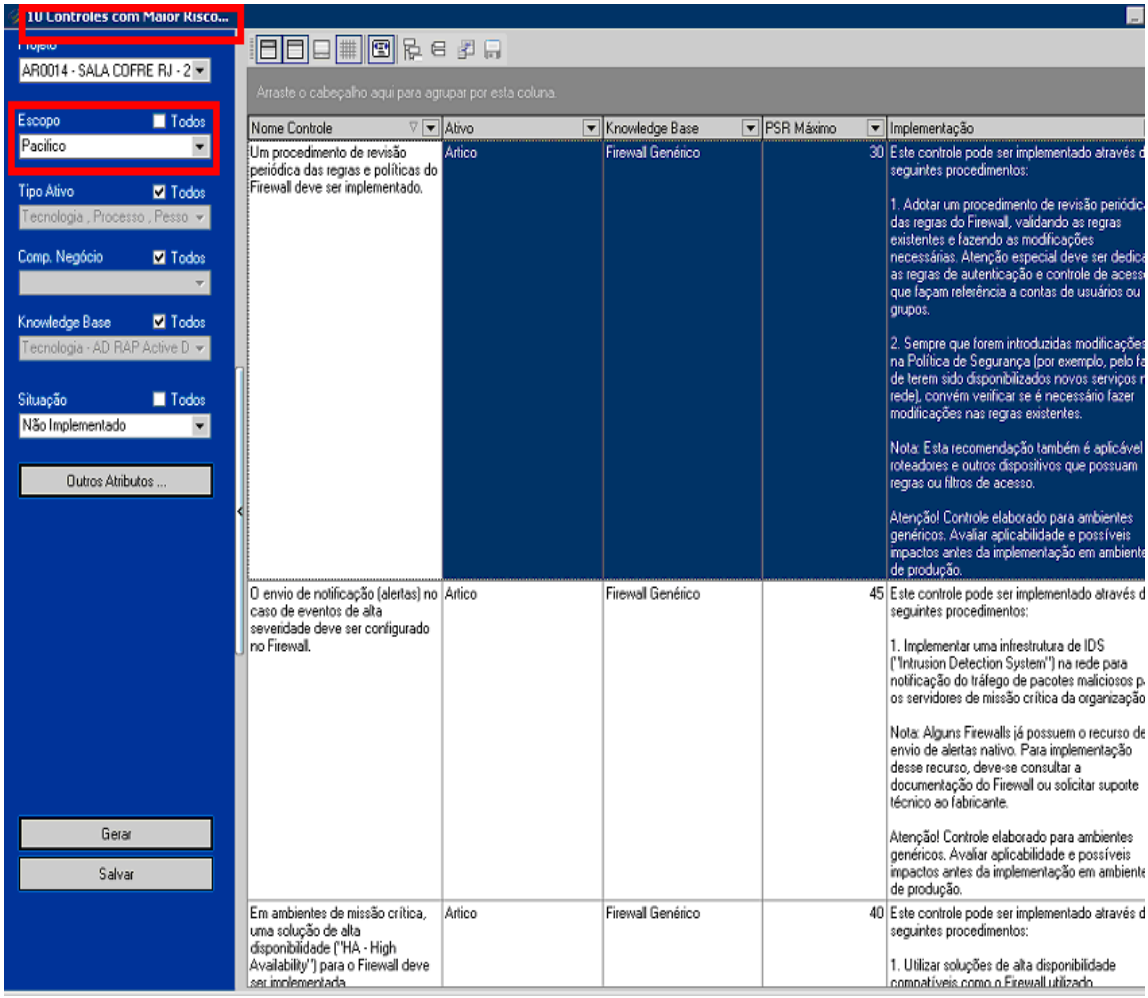


Figura 23 – Tela de Relatório 10 Maiores Riscos de um Ativo

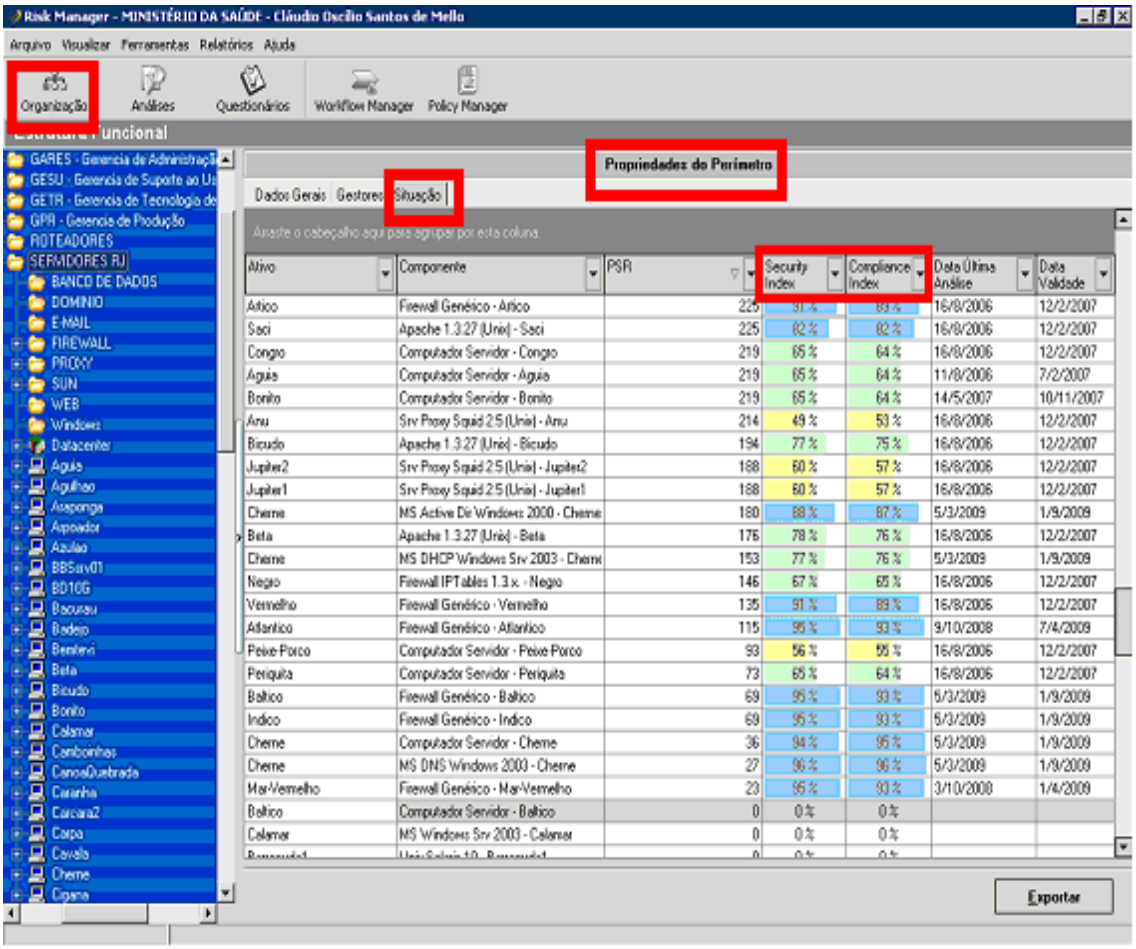


Figura 24 – Tela de Situação dos Riscos dos Ativos do Perímetro

Dois indicadores estão presentes no RM para demonstrar níveis de Conformidade e Risco das Análises realizadas:

- ***Security Index*** – Este é o Indicador de Segurança relativo. É calculado dividindo-se o total de Riscos dos Controles implementados (PSR evitado) pelo total de Riscos dos Controles aplicáveis (PSR total). Este indicador é expresso em números percentuais e pode variar de 0% a 100%;
- ***Complience Index*** – Este é o Indicador de Conformidade. É calculado dividindo-se a quantidade total de Controles implementados pela quantidade total de Controles aplicáveis. Este indicador é expresso em números percentuais e pode variar de 0% a 100%.

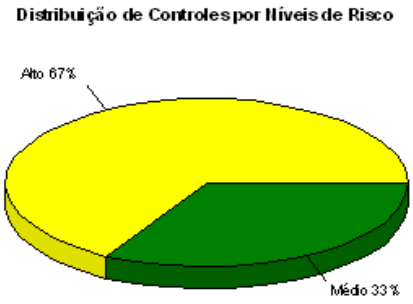
Veja Figura 25 parte de um Relatório de um Ativo.

2.1. Controles por nível de risco

As informações abaixo apresentam o nível de risco dos controles não implementados e o percentual relativo em termos quantitativos e qualitativos.

Nível de Risco		Muito Alto	Alto	Médio	Baixo	Muito Baixo	TOTAL
Quantitativo	QTDE	0	2	1	0	0	3
	%	0.00%	66.67%	33.33%	0.00%	0.00%	100,00%
Qualitativo	PSR	0	85	30	0	0	115
	%	0.00%	73.91%	26.09%	0.00%	0.00%	100,00%

O gráfico abaixo apresenta os totais de controles não implementados por nível de risco.



- ***66,67%*** *dos controles não implementados possuem níveis de risco Alto e Muito Alto.*
- ***33,33%*** *dos controles não implementados possuem níveis de risco Médio.*
- ***0,00%*** *dos controles não implementados possuem níveis de risco Baixo e Muito Baixo*

O gráfico abaixo apresenta os totais de riscos existentes por nível de risco.

Figura 25 – Relatório de Risco de um Ativo

4.5.5 **Tratar**

Esta é a última etapa do ciclo Gestão de Riscos. Os riscos identificados através das Análises deverão ser priorizados e tratados através da implementação dos controles. A priorização está focada nos níveis máximos que uma organização está disposta a tolerar e na relação custo / benefício da implementação do controle.

5 CONCLUSÕES

Ao longo dos capítulos apresentados vimos que gerir a Segurança da Informação de uma organização é uma tarefa bastante complexa.

O processo de Gestão de Riscos, provavelmente, é um dos componentes mais importantes da Gestão da Informação. É por meio desse processo que os riscos são identificados e tratados de forma sistemática e contínua. Um dos pontos a ser observado neste processo é em relação ao escopo que será considerado. Naturalmente, na medida em que o escopo de uma Análise de Risco aumenta, a complexidade e o tempo necessário à conclusão da análise aumentam.

Vale lembrar que a análise de custo / benefício, no tratamento do risco, deve ser uma constante na atividade de Gestão de Riscos. Sabemos que pouco adiantará a implementação de um controle de risco que custe muito mais que o valor do ativo.

A utilização do RM na Gestão de Riscos agrega grande valor ao processo, pois através do seu ciclo “inventariar, analisar, avaliar e tratar” permite mensuração e controle dos riscos. A partir de Bases de Conhecimento atualizadas constantemente o RM auxilia a realização de Análises de Riscos em ativos dos mais diversos tipos.

A Avaliação dos Riscos é realizada por meio da geração de relatórios objetivos e práticos. Dentre eles, temos os de visões executivas, táticas e operacionais que podem ser apresentadas de diferentes formas. Isso ajuda a viabilizar a verificação de quais ativos possuem riscos para que possamos comparar com o nível de risco aceito pela organização.

6 REFERÊNCIAS BIBLIOGRÁFICAS

[01] **NAKAMURA**, E. T.; GEUS, P. L.; Segurança de Redes em Ambientes Cooperativos; Berkeley Brasil, 2002; ISBN 85-7251-609-3; p. 28-29; 165-215.

[02] **CERT.BR** - Centro de Estudos Respostas e Tratamento de Incidentes de Segurança no Brasil. Dados Estatísticos. (2009, Outubro 26). [Online]. Disponível: http://www.cert.br/stats/incidentes

[03] **HAICKEL**, Dalila, VIERA, Elba Lúcia de Carvalho, Normas e Procedimentos de segurança da Informação. 2 ed. - Florianópolis:SENAI/SC, 2009.

[04] **HOLANDA**, Ana Clara Arruda de, A Importância da Segurança da Informação. In. http://edmilsonacre.blogspot.com/2009/06/importancia-da-seguranca-da-informacao.html (acessado em 03 de Agosto de 2009).

[05] **SÊMOLA**, Marcos. Gestão da segurança da informação: uma visão executiva. Rio de Janeiro: Campus, 2003.

[06] **NBRISO/IEC17799**:ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001.

[07] **MÓDULO**, Guia Oficial para formação de Gestores em Segurança da Informação. Porto Alegre: Zouk, 2006.

[08] **RNP** – Escola Superior de Redes – Apostila do curso de Gestão da Segurança da Informação - 2007.

[09] **MÓDULO**, Apostila do curso da ferramenta *Risk Manager* - 2006.

[10] **CULP**, C., The ART of Risk Management – Alternative Risk Transfer; John Wiley & Sons, 2002; ISBN 0-471-12495-8; p. 199-217

[11] **FONTES, E.**, Vivendo a segurança da informação; Sicurezza Editora, 2000; ISBN 85-87297; p. 73-75.

[12] **GREENSTEIN, M. ; FEINMAN, T**.; Security, Risk Management and Control; McGraw-Hill Higher Education, 2000; ISBN 0-07-229289-X; p.171-188.

[13] **MCGEE, J.; PRUSAK, L**., Gerenciamento Estratégico da Informação; Editora Campus, 1994; ISBN 85-7001-924-6; p. 5, 23-24.

[14] **SANTOS, P**., Gestão de Riscos Empresariais; Novo Século Ed., 2002; CDD-658.155; p. 25.

[15] **BRASIL**, Decreto nº 4.553, de 27 de dezembro de 2002. Brasília, 2002. [Online]. Disponível:https://www.planalto.gov.br/ccivil_03/decreto/2002/D4553Compilado.htm, Acesso em: 10/02/2010.