

**CENTRO UNIVERSITÁRIO EUROAMERICANO – UNIEURO
PRÓ-REITORIA E PÓS-GRADUAÇÃO, PESQUISA E EXTENSÃO
COORDENAÇÃO DE PÓS-GRADUAÇÃO LATO SENSU
CURSO DE MBA EM GESTÃO DE PROJETOS DE SOFTWARE**

**ANTÔNIO CARLOS PEREIRA DE BRITTO
JOÃO ALBERTO PINCOVSCY**

IMPLEMENTAÇÃO DE ANÁLISE DE RISCO SEGUINDO O PMBOK

Brasília, Maio / 2008



**ANTÔNIO CARLOS PEREIRA DE BRITTO
JOÃO ALBERTO PINCOVSCY**

IMPLEMENTAÇÃO DE ANÁLISE DE RISCO SEGUINDO O PMBOK

**Trabalho de Conclusão de Curso – Monografia,
apresentada como pré-requisito parcial para
conclusão do curso de MBA em Gestão de Projeto de
Software do Centro Universitário
EUROAMERICANO – UNIEURO.**

Orientadora: Prof.^a MSc. Edna Dias Canedo

**Brasília
Maio, 2008**

Ficha catalográfica elaborada pela Bibliotecária Fulana de tal, CRB1/0000

M672 Miranda, José Luis Carneiro de.

Como escrever um artigo científico/ José Luís Carneiro de Miranda; Brasília : UNIEURO, 2007.

vii, 27p. : il.

Monografia (Pós-graduação) – Curso de Especialização em Gestão de Segurança em Redes de Computadores. Centro Universitário Euroamericano.

1. Palavra chave. 2. Palavra chave 3. Palavra chave 4. Palavra chave. 5. Palavra chave. I. Silva, Rosana Pio da, (Orientadora) II. Título.

CDU: 000000000000

**ANTÔNIO CARLOS PEREIRA DE BRITTO
JOÃO ALBERTO PINCOVSCY**

IMPLEMENTAÇÃO DE ANÁLISE DE RISCO SEGUINDO O PMBOK

Esta monografia foi julgada adequada à obtenção do grau de Especialista em Gestão de Projetos de Software e aprovada em sua forma final pelo curso de MBA em Gestão de Projeto de Software do Centro Universitário EUROAMERICANO – UNIEURO.

Data de aprovação:

Banca Examinadora

Profª. Msc. Edna Dias Canedo - Orientadora
Centro Universitário UNIEURO

Profº Msc. Cleber Machado Ortiz
Centro Universitário UNIEURO

Profº Msc. Leônicio Regal Dutra
Centro Universitário UNIEURO

RESUMO

A Segurança da Informação é hoje uma área de conhecimento da Gestão Estratégica da Informação, e é responsável por assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade das informações organizacionais, corporativas e pessoais, de forma a preservar seu valor intrínseco. As metodologias de Gestão de Risco para a Segurança da Informação possuem uma visão da segurança dos negócios da organização, que não poderia ser alcançada considerando-se apenas os aspectos da infra-estrutura técnica, tanto do setor privado como do público. A abordagem para a Gestão de Riscos operacionais relativos à missão e aos negócios da Administração Pública Federal - APF no Brasil leva a uma visão totalizante e abrangente, no caso a metodologia *Operacional Critical Threat, Asset and Vulnerability Evaluation - OCTAVE* fornece essa abordagem se comparadas às outras que focam nos aspectos tecnológicos. Este trabalho tem a finalidade de elaborar uma implementação da metodologia de análise de risco operacional, metodologia OCTAVE, seguindo o *Project Management Body of Knowledge - PMBOK*. Esse trabalho aproveitou da sinergia dessa afinidade OCTAVE e PMBOK e principalmente da oportunidade de formalizar-se o gerenciamento de projetos, fator de sucesso do empreendimento de implantar a Gestão da Segurança da Informação e Comunicação na Administração Pública Federal, via gestão de risco nos sistemas da Tecnologia da Informação e Comunicação.

Palavras-Chaves: Sociedade da Informação, Segurança da Informação e Comunicação, Gestão de Riscos, OCTAVE e PMBOK.

ABSTRACT

The Information Security is today an area of knowledge of the Strategic Management of the Information, and is responsible for assuring the availability, the integrity, the authenticity and the confidencialidade of the organization is, corporative and personal information, must to preserve its intrinsic value. Being the information a strategically resource of the necessary organization to be considered and with priority treated to a form integrated with it's strategically components in this management. The approach for the Risks Management of relative operational to the mission and the businesses of the Administração Pública Federal APF in Brazil leads to a completely and including vision, in the case the *Operational Critical Threat, Asset and Vulnerability Evaluations - OCTAVE supplies* this approach if to the others that focus in the technological aspects. This work has the purpose to elaborate an implementation of the methodology of analysis of operational risk, methodology OCTAVE, being followed the Project Management Body of Knowledge - PMBOK. This work used to advantage of the synergy of this affinity OCTAVE and PMBOK and mainly of the chance to validate the management of projects, factor of success of the enterprise to implant the Management of the Security of the Information and Communication in the Federal Public Administration, saw management of risk in the systems of the Technology of the Information and Communication.

Key-Words: Information Society, Information and Communication Security, Risk Management, OCTAVE and PMBOK.

SUMÁRIO

1. INTRODUÇÃO.....	1
1.1. A Tecnologia da Informação e Sociedade da Informação.....	1
1.2. A Segurança da Informação e Comunicação.....	1
1.3. Gestão da Segurança da Informação	2
1.4. Proteção da Infra-estrutura Crítica no governo do Brasil.....	3
1.5. O Modelo de Gestão de Segurança	4
1.6. A Gestão do Risco	4
1.7. Metodologia de Analise de Risco para a APF.....	6
1.8. A Metodologia OCTAVE.....	7
1.9. A Metodologia OCTAVE e o Gerenciamento de Projetos (PMBOK).....	10
2. O MÉTODO OCTAVE	11
2.1. Objetivo e âmbito do método OCTAVE	11
2.2. Os Métodos de Implementação OCTAVE e OCTAVE-S	12
2.3. A Abordagem OCTAVE	12
2.4. Os Princípios da Abordagem OCTAVE.....	15
2.5. A Abordagem de Três Etapas.....	16
2.6. Os Fundamentos do Método OCTAVE	17
2.7. Os Critérios do Método OCTAVE	18
2.8. A abrangência do método OCTAVE.....	21
2.9. Os processos do método OCTAVE.....	22
2.10. Documentação do método OCTAVE	23
3. CONCEITOS DO PMBOK.....	25
3.1. Descrição dos conceitos utilizados	26
3.2. Área de conhecimento em gerenciamento de projetos	27
3.3. Gerenciamento da Integração	27
3.4. Gerenciamento de Escopo	28
3.5. Gerenciamento de Tempo.....	30
3.6. Gerenciamento de Custos	31
3.7. Gerenciamento de Qualidade	31
3.8. Gerenciamento de Recursos Humanos	33
3.9. Gerenciamento das Comunicações.....	34
3.10. Gerenciamento de Riscos	35
3.11. Gerenciamento de Aquisições	36
4. PLANO DE PROJETO PARA O MÉTODO OCTAVE	38
4.1. Gerenciamento da Integração	38
4.2. Gerenciamento de Escopo	38
4.3. Gerenciamento de Tempo.....	41
4.4. Gerenciamento de Custos	45
4.5. Gerenciamento de Qualidade	45
4.6. Gerenciamento de Recursos Humanos	45
4.7. Gerenciamento das Comunicações.....	46
4.8. Gerenciamento de Riscos	47
4.9. Gerenciamento de Aquisições	47
5. CONCLUSÃO.....	48
5.1. Trabalhos futuros.....	48
6. REFERÊNCIAS BIBLIOGRÁFICAS	49

APÊNDICE - (todos os documentos dessa seção foram adaptados do livro: Manual Prático do Plano de Projeto, Ricardo Vargas, 3 ^a Edição)	51
APÊNDICE A - <i>Template Apresentação</i>	51
APÊNDICE B - <i>Template Termo de Abertura do Projeto</i>	52
APÊNDICE C - <i>Template Sistema de Controle Integrado de Mudanças</i>	54
APÊNDICE D - <i>Template Registro de Lições Aprendidas no Projeto</i>	55
APÊNDICE E - <i>Template da Declaração de Escopo</i>	57
APÊNDICE F - <i>EAP</i>	64
APÊNDICE G - <i>Template do Dicionário da EAP</i>	65
APÊNDICE H - <i>Template do Plano de Gerenciamento do Escopo</i>	66
APÊNDICE I - Gráfico de Gantt do Projeto.....	69
APÊNDICE J - <i>Template do Plano de Gerenciamento do Tempo</i>	70
APÊNDICE K - <i>Template do Plano de Gerenciamento da Qualidade</i>	74
APÊNDICE L - <i>Template do Plano de Gerenciamento de Recursos Humanos</i>	79
APÊNDICE M - <i>Template do Plano de Gerenciamento das Comunicações</i>	83
APÊNDICE N - <i>Template do Plano de Gerenciamento de Riscos</i>	90

1. INTRODUÇÃO

1.1. A Tecnologia da Informação e Sociedade da Informação

Os centros de pesquisas e de novas tecnologias dos EUA e do Japão na década de 80 propiciaram a explosão na indústria da computação, software e hardware, a integração dos computadores e telecomunicações, criando o conceito de Tecnologia da Informação e Comunicação TIC. Os contextos criados pela utilização da TI na década de 90 fomentou o nascimento da Sociedade da Informação, que desencadeou uma nova forma de organização social, política e econômica que recorre ao intensivo uso da Tecnologia da Informação para coleta, produção, processamento, transmissão e armazenamento de informações (MALTA, 2002).

A Tecnologia da Informação abrange hoje a microeletrônica, a computação (software e hardware), as telecomunicações, a optoeletrônica, a engenharia genética e os processos tecnológicos, onde a informação é gerada, armazenada, recuperada, processada, transmitida e descartada. Tem ligações com a Teoria Geral dos Sistemas, Teoria dos Jogos e Cibernética (MALTA, 2002).

1.2. A Segurança da Informação e Comunicação

A Informação consiste em dados ou conjunto de dados, processado ou não, em qualquer suporte, capaz de produzir conhecimento, podendo ser: imagem, som e documento físico ou eletrônico. Ela é o fator estratégico mais relevante se comparada aos recursos energéticos e naturais de um país. Ela é um recurso ou ativo estratégico da organização.

Hoje no mundo, a Informação é um importante vetor para a geração de riquezas no contexto da produção globalizado, levando a necessidade de se promover uma “gestão mais eficiente” dos seus recursos, originando a nova especialidade denominada Segurança da Informação e Comunicações (MALTA, 2002).

A Segurança da Informação e Comunicação é uma área de conhecimento responsável por assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade das informações institucionais, corporativas e pessoais, de forma a preservar seu valor intrínseco. A Segurança da Informação e Comunicação fundamenta-se nos seguintes propriedades basilares:

- Disponibilidade: propriedade de que as informações podem ser acessadas e utilizadas por indivíduos, equipamentos ou sistemas autorizados;

- Integridade: propriedade de que as informações não foram modificadas, inclusive quanto à origem e ao destino;
- Autenticidade: propriedade de que as informações foram produzidas, expedidas, recebidas ou modificadas por determinado indivíduo, equipamento ou sistema;
- Confidencialidade: propriedade de que as informações não foram acessadas por pessoas, equipamentos ou sistemas não autorizados.

Mais recentemente outros dois objetivos têm sido bastante discutidos:

- Irretratabilidade (ou Não Repúdio): propriedade de que as informações estão garantidas quanto a autoria em determinadas ações e impede o repúdio (a negação) da mesma;
- Legalidade (ou Conformidade): propriedade de que as informações estão garantidas quanto com relação a medidas legais cabíveis e aplicadas quando necessárias.

A Informação associada aos processos de apoio, os sistemas de telecomunicações e as redes tornam-se importante ativo para os negócios e para a infra-estrutura de um país. Os princípios de: confidencialidade, integridade, disponibilidade e autenticidade da informação podem ser essenciais para preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e à imagem da organização ou do país (MALTA, 2002).

Cada vez mais as organizações, seus sistemas de informação e redes de computadores são colocados à prova por diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, roubo de informação, espionagem, sabotagem, vandalismo, fogo, inundação e outros acidentes. Problemas causados por “vírus”, “worms”, “hackers”, “crackers”, empregados insatisfeitos ou ex-empregados, programas maliciosos e ataques de negação de serviço (“denial of service” DoS) estão se tornando cada vez mais comuns, mais freqüentes e incrivelmente mais sofisticados (NAKAMURA, 2004).

1.3. Gestão da Segurança da Informação

Alguns modelos de Gestão da Segurança da Informação e Comunicação são de conhecimento mundial e têm servido de referência para organizações e países, permitindo o aperfeiçoamento e a criação de modelos adequados para as necessidades específicas. Dentre eles, podemos citar a ABNT NBR ISO/IEC 17799:2005 (Código de Prática para a Gestão da Segurança da Informação), ABNT NBR ISO/IEC 27001:2006 – (Sistema de Gestão de Segurança da Informação SGSI) - Requisitos, e o *Information Technology Infrastructure Library ITIL* (*ITIL - Security Management Process*). Embora estas referências estejam

disponíveis, a adoção de um modelo de gestão não é uma tarefa simples e imediata, requerem um conjunto de ações coordenadas, constantes e gradativas, com o apoio executivo, orçamento, tecnologia e o mais importante, pessoas conscientizadas.

A Gestão da Segurança da Informação e Comunicação refere-se ao processo de desenvolver, implementar, direcionar e monitorar as estratégias e a atividade de segurança da organização.

A segurança é um problema organizacional que precisa ser considerado e tratado de forma integrada com os seus componentes estratégicos. No entanto muitas organizações adotam uma abordagem centrada na tecnologia. Uma abordagem independente da tecnologia leva à necessidade da Gestão do Risco, pois existe a tendência das organizações em caracterizar os problemas de segurança em termos técnicos, geralmente ignorando as falhas operacionais e de gestão que podem ser as reais causa raiz ou fator contribuinte, por outro lado, a convergência dessas metodologias pode propiciar resultados satisfatórios como apoio à tomada de decisão, considerando principalmente o contexto atual da chamada sociedade do conhecimento: rápidas mudanças, elevado grau de incertezas e uso intensivo das Tecnologias de Informação e Comunicação TIC (CANONGIA, 2001).

1.4. Proteção da Infra-estrutura Crítica no Governo do Brasil

Nesse contexto no qual a interdependência entre diferentes infra-estruturas críticas é cada vez maior, a preocupação com a sua proteção é inegável. Muitos países já tomaram consciência da importância da Segurança da Informação e Telecomunicações e muitos deles possuem trabalhos específicos sobre o assunto, possuindo inclusive órgãos governamentais responsáveis exclusivamente por essa proteção. No Brasil temos: o Departamento de Segurança da Informação e Comunicações DSIC, o Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações CEPESC e o Comitê Gestor de Segurança da Informação CGI, orgões do Gabinete de Segurança Institucional GSI da Presidência da República. O GSI/PR tem a responsabilidade de promover a Segurança da Informação e Telecomunicações no âmbito da Administração Pública Federal APF e em consonância com os esquemas normativos internacionais dos quais é participante e colaborador.

A abordagem com que a Segurança da Informação e Comunicação é tratada varia de país para país; alguns a destacam em termos de uma infra-estrutura crítica, a informação é a prioridade, o que é justificado pela variedade de serviços básicos que possuem dependência da infra-estrutura de rede: os serviços de emergência, os sistemas de navegação para tráfego

aéreo e entregas, a distribuição de energia elétrica e os sistemas de controle de água (NAKAMURA, 2004).

Internacionalmente existe um esforço para a convergência de um conjunto de princípios para a Segurança da Informação e Comunicação, uma base doutrinária, que leve a construção de padrões e de normas para subsidiar modelos de Gestão de Segurança da Informação e Comunicação.

1.5. O Modelo de Gestão de Segurança

O Modelo de Gestão da Segurança da Informação e Comunicação deve ser considerado como uma ação estratégica, estabelecendo um conjunto de recurso e princípios nos quais projetos devem ser priorizados e gerenciados, com o objetivo de atingir as determinações e orientações de uma Política de Segurança. O Modelo de Gestão da Segurança deve estar integrado ao planejamento de orçamentário da organização.

É preciso ter clareza que o Modelo de Gestão Estratégico não é a razão de existência da organização. Um do propósito é o fornecimento de serviços de segurança e suporte para o negócio. O Modelo de Gestão Estratégico não é um produto que visa gerar lucros. Deve ser entendido como um processo que agrupa valor e minimiza os custos para a organização (CANONGIA, 2001).

1.6. A Gestão do Risco

A evolução de um Modelo de Segurança baseado em Gestão de Risco permite uma visão mais acurada do nível de segurança adequado ao negócio, que não pode ser alcançado considerando-se apenas os aspectos da infra-estrutura técnica. A organização estará tendo uma falsa sensação de segurança se concentrar suas ações de segurança apenas na infra-estrutura técnica. A segurança é um problema organizacional que precisa ser considerado e tratado de forma integrada com os seus componentes estratégicos. No entanto muitas organizações adotam uma abordagem centrada na tecnologia.

A evolução do Modelo de Segurança baseado em Gestão de Risco permite uma visão mais clara de que o nível de segurança adequado não pode ser alcançado considerando apenas aspectos da infra-estrutura técnica. A organização estará tendo uma falsa sensação de segurança se concentrar suas ações de segurança apenas na infra-estrutura técnica.

A Gestão de Riscos é um dos processos de gestão das organizações e depende do contexto em que é utilizada, desta forma, a ABNT ISO/IEC Guia 73:2005 (Gestão de Riscos –

Vocabulário – Recomendações para uso em normas) fornece uma referência para a coerência da terminologia adotada, na introdução declara-se que:

Todos os tipos de empreendimentos se deparam com situações (ou eventos) que constituem oportunidades de benefício ou ameaças ao seu sucesso. Oportunidades podem ser aproveitadas ou ameaças podem ser reduzidas por uma gestão efetiva. Em certos campos, tal como o financeiro, a gestão de riscos trata das flutuações monetárias como uma oportunidade de ganhos ou como um potencial de perda. Conseqüentemente, o processo de gestão de riscos é cada vez mais reconhecido como sendo relacionado aos aspectos positivos e negativos dessas incertezas. Este Guia trata a gestão de riscos, tanto da perspectiva positiva como da negativa. (ABNT ISO/IEC Guia 73:2005)

A Gestão de Riscos se constitui no processo fundamental da Gestão da Segurança; não se faz segurança sem gerenciar os riscos. A Gestão de Risco de Segurança da Informação é o processo de identificar e avaliar os riscos, reduzindo-os a um nível aceitável e implementando os mecanismos para a manutenção deste nível. Quando se trata de riscos de segurança da informação, estamos interessados naqueles eventos que endereçam à quebra dos princípios básicos da segurança da informação: integridade, disponibilidade, confidencialidade e autenticidade. Os controles ou salvaguardas de segurança devem sempre ser adotados como consequência da avaliação dos riscos. A abordagem da gestão de riscos também depende da cultura de segurança da organização.

Segundo a ABNT NBR ISO/IEC 17799:2005, os gastos com a implementação de controles de segurança precisam ser balanceados de acordo com os danos aos negócios causados por potenciais falhas na segurança da informação, os quais devem ser identificados por meio de uma análise/avaliação sistemática e periódica dos riscos de segurança. É na fase de análise e avaliação que são identificadas as ameaças aos ativos e as vulnerabilidades destes, e será realizada a estimativa das probabilidades da ocorrência das ameaças e dos impactos potenciais aos negócios. Os resultados da análise/avaliação de riscos irão ajudar a direcionar e a determinar as ações gerenciais apropriadas e as prioridades na implementação dos controles para a proteção contra estes riscos. É na fase do tratamento de riscos que são definidos os controles a serem utilizados e estes controles podem ser escolhidos a partir desta norma, baseados tanto em requisitos legais como nas melhores práticas de segurança para confrontar as ameaças mapeadas.

Dois outros conceitos citados pela norma podem ser mais bem explicitados com a ajuda da ABNT NBR ISO/IEC 17799:2005.

- Ameaça: causa potencial de um incidente que pode resultar em dano para o sistema ou para a organização.

- Vulnerabilidade: fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Quando se trata de riscos, estamos apontando para o estudo das ameaças que exploram as vulnerabilidades existentes nos ativos ou sistemas e nos impactos decorrentes para os processos de negócios associados a esses ativos. Basicamente os riscos podem ser evitados, reduzidos, transferidos ou aceitos, mas nunca ignorados. Um plano de ação deve ser definido e controlado para a implementação das salvaguardas, de forma a garantir que os riscos serão efetivamente mitigados. Os riscos e seus componentes são inaceitáveis para o negócio e devem ser devidamente tratados.

Outro ponto a destacar no tratamento de riscos é o custo benefício. O custo decorrente da redução de um risco não deve ser maior do que o custo da exposição ao risco. Para garantir que os riscos estão controlados e se mantém dentro do nível definido como aceitável, devem ser realizadas avaliações periódicas, isto porque, uma redução de risco fornece subsídios para a ação conjunta do processo de gestão da informação e gestão do conhecimento, ambas em apoio as estratégia e missão organizacional, apresentam para o processo de tomada de decisão uma propriedade emergente que é a inteligência institucional. (TARAPANOFF, 2004).

1.7. Metodologia de Analise de Risco para a APF

A abordagem para a Gestão de Risco Operacional relativo à missão e aos negócios da APF (Administração Pública Federal) no Brasil leva a uma visão totalizante e abrangente. Essa visão necessita de uma categorização dos sistemas críticos para o cumprimento da missão do Estado. Necessitamos de uma metodologia para a avaliação de riscos e planos da gestão de riscos na grande diversidade que é a APF.

No nosso caso, a partir de um estudo comparativo das metodologias de gestão de risco e de trabalhos para a categorização de infra-estrutura críticas, chegamos à metodologia *Operacional Critical Threat, Asset and Vulnerability Evaluation OCTAVE*, que fornece uma avaliação do risco do operacional, está baseado nos fatores críticos de sucesso da organização, e endereça para um plano de gerenciamento do risco para a organização. Esses fatores críticos de sucesso são mapeados em termos de Ativos Críticos.

A APF é um Cosmos em termos de diversidade e estrutura, necessitamos de processo de avaliação de riscos que viabilize a implementação de um plano de gerenciamento de risco que contemple o tamanho, a forma e o significado. Devem constar desse plano, as melhores práticas de segurança da informação com as recomendações da classificação e do tratamento dos ativos críticos para cada contexto da APF.

1.8. A Metodologia OCTAVE

A Metodologia OCTAVE, *Operational Critical Threat, Asset and Vulnerability Evaluation*, foi elaborada e desenvolvida pelo *Software Engineering Institute da Carnegie Mellon University*.

O que a diferencia de outras metodologias são os seguintes conceitos;

- A missão da organização;
- Os ativos /ativos críticos;
- A estratégia de negócio da organização;
- As necessidades de segurança da informação;
- O risco ao negócio;
- O plano estratégico de segurança.

Tem uma abordagem em que o tratamento dos ativos críticos da organização é feito em nível de importância estratégica, pois impacta na missão da organização.

De acordo com o *Software Engineering Institute SEI*, um Ciclo de Vida para um Plano de Gerenciamento de Riscos possui as seguintes fases:

- Fase 1 - Identificação e Quantificação;
- Fase 2 - Análise e Classificação;
- Fase 3 - Planejamento e Implantação;
- Fase 4 - Monitoramento e Controle.



Figura 1 - Paradigma do gerenciamento de risco (Software Engineering Institute- Carnegie Mellon SEI/CMU)

A metodologia OCTAVE é uma metodologia de avaliação de riscos de segurança que engloba basicamente as três primeiras fases do SEI.

A metodologia OCTAVE é diferente de outras consideradas, que são quase todas direcionadas a uma visão tecnológica, onde se avaliam os riscos tecnológicos, sendo que a metodologia OCTAVE está direcionada pela análise dos riscos operacionais e imediata avaliação da efetividade das práticas de segurança. Desta forma a metodologia OCTAVE é aplicada no âmbito da organização, nas questões estratégicas, nos aspectos dos ativos críticos, com o foco nas práticas de segurança por meio da utilização de controles. Essa visão está apoiada na abordagem de que os fatores críticos de sucesso da organização estão apoiados em uma infra-estrutura crítica, e esta é baseada em informação ou em sistemas de informações, levando a análise de risco a verificar se o mapeamento da organização em termos dos ativos críticos para o negócio e a área de TIC está alinhado com negócios da organização (ALBERTS, *Introduction to the OCTAVE® Approach*).

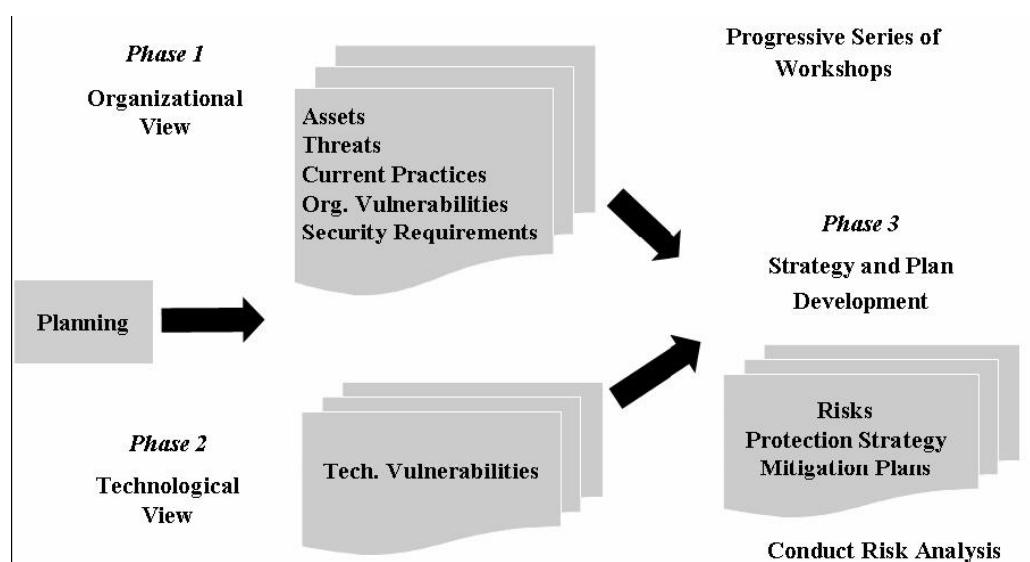


Figura 2 - Principais fases da OCTAVE (ALBERTS, OCTAVE Criteria v2.0).

- Fase 1. Visão organizacional.

Nesta fase é feita a avaliação da organização. Esta fase pode conter quatro processos:

- Processo 1: categoriza o conhecimento da gerência sênior;
- Processo 2: categoriza o conhecimento da gerência da área operacional;
- Processo 3: categoriza o conhecimento do “Staff”;

- Processo 4: criação do perfil (*profile*) de (ameaças x vulnerabilidades x impactos) para os ativos elencados.
- Fase 2 - Visão Tecnológica

Nesta fase é feita a identificação das vulnerabilidades tecnológicas da infra-estrutura de TIC, temos dois processos:

- Processo 5: Identificação dos componentes-chaves: o analista identifica um conjunto representativo de componentes-chaves de um sistema que suporta os processos de negócio, é definida como uma abordagem para avaliação dos componentes-chaves da tecnologia empregada.
- Processo 6: O analista avalia os componentes-chaves selecionados, pode utilizar inúmeras ferramentas para avaliar os componentes-chaves selecionados, por isso um criterioso planejamento deve ser elaborado para a condução desse processo.

Os resultados são analisados para refinar o perfil de ameaças.

- Fase 3 – Estratégia e Planos de Segurança

O objetivo desta fase é avaliar os riscos aos ativos críticos e desenvolver uma estratégia de proteção por meio de um ou mais planos de controle e redução de riscos. Temos dois processos:

- Processo 7: Condução da análise de riscos: um conjunto de critérios de impacto organizacional será definido para estabelecer uma linha de base para determinação do valor de impacto (alto, médio, baixo) devido às ameaças aos ativos críticos. Todos os riscos são avaliados contra cada critério de impacto organizacional.
- Processo 8: Desenvolvimento da estratégia de proteção: o analista desenvolve uma estratégia de proteção para toda a organização, baseada na melhoria das práticas de segurança e nos planos de controle de redução dos riscos.

Justifica-se o emprego de uma metodologia de análise de risco com a abordagem da OCTAVE pela necessidade de caracterizar a infra-estrutura crítica da APF, com a informação e seus sistemas permeando todo o contexto. A seguir á apresentada uma figura que mostra as áreas de influência do Método OCTAVE.



Figura 3 - Áreas de influência do Método OCTAVE

1.9. A Metodologia OCTAVE e o Gerenciamento de Projetos (PMBOK)

Este trabalho visa utilizar a abordagem do Gerenciamento de Projetos PMBOOK para administrar a complexidade organizada que a implementação da metodologia OCTAVE exige na Administração Pública Federal APF.

No Capítulo 2 será detalhado o Método OCTAVE, em seguida, no Capítulo 3 será apresentados os conceitos fundamentais do PMBOK, no Capítulo 4 será demonstrada a seqüência de preenchimento dos *Templates* ou modelos de documentos que subsidiarão a implantação do OCTAVE em uma organização ou setor da APF. Todos os modelos de documentos ou Templates estão apresentados no Apêndice.

2. O MÉTODO OCTAVE

2.1. Objetivo e âmbito do método OCTAVE

Este capítulo descreve a abordagem da Metodologia de Avaliação e Gerenciamento de Risco Operacional, *Operationally Critical Threat, Asset, Vulnerability e Evaluation OCTAVE®*. Embora a OCTAVE® não seja uma abordagem de Gestão dos Riscos específica para a segurança da informação, ela tem uma aspecto operacional, mas fundamenta-se conceitualmente no nível do Planejamento Estratégico da Organização.

A abordagem OCTAVE® tem princípios, métodos e processos desenvolvidos pelo *Software Engineering Institute SEI, Carnegie Mellon University (USA)*. Outras metodologias competem com a primazia de fornecer uma estratégia para tratar a segurança da informação e comunicação, mas a OCTAVE tem o subsídio do Governo Americano para o desenvolvimento, e diferenciou-se por endereçar o tema da Governança de Tecnologia da Informação, e ocupam a posição de destaque com os outros modelos de projeção internacional como os “frameworks”: COBIT, ITIL e o *Committee of Sponsoring Organizations of the Treadway Commission COSO*. Essa habilidade está fundamentada em princípios, atributos e recomendações utilizados pelo Governo Americano e seus prestadores de serviço comprometidos com a proteção da estrutura crítica do país.

As organizations increase security measures and attempt to identify vulnerabilities in critical assets, many are looking for a mechanism to ensure an efficient investment of resources to counter physical and cyber threats. One method is a risk management model that not only assesses assets, threats, and vulnerabilities but also incorporates a continuous assessment feature. This allows organizations to tailor their management of risk to the current situation as well as assess future risks. The management of risk impacts the bottom line of every organization, either in monetary terms or in terms of operational readiness and capability. Security managers and decision-makers that operate in any sector of the national infrastructure must have a sound methodology to manage both physical and cyber risks to their organization.

(Risk Management: An Essential Guide to Protecting Critical Assets, National Infrastructure Protection Center, November 2002.)

Para uma descrição da abordagem consubstanciado na metodologia OCTAVE é necessário destacar em primeiro lugar a sua visão global, a de infra-estrutura crítica, e em seguida no detalhamento, a do foco nas características operacional da organização.

A missão, os fatores críticos de sucesso, os pontos fracos e fortes e o seu desdobramento nos níveis tático e operacional, implicam numa consideração estratégica do

processo de mapeamento das necessidades de Segurança da Informação e Comunicação e dos resultados desse processo em termos de planos para a proteção dos ativos críticos da organização.

Em todos os níveis de consideração da abordagem OCTAVE é contemplado o valor do ativo a partir da Segurança da Informação, que está diretamente relacionado com o cumprimento da missão da Organização. Os ativos estão elencados como: informação, sistemas, processos, pessoas e estrutura.

Os ativos podem ser categorizados por sua importância para o cumprimento da missão organizacional, e destacam-se a importância maior par os ativos que afetam e diferenciam o comportamento da organização (TARAPANOFF, 2004).

2.2. Os Métodos de Implementação OCTAVE e OCTAVE-S

Temos dois métodos de implementação da abordagem OCTAVE dependendo da complexidade da organização: um método OCTAVE para grandes organizações e um método OCTAVE-S para as pequenas organizações. A métrica da complexidade para essa avaliação pode ser o tamanho ou a distribuição geográfica, mas pode também ser considerado o aspecto da Inteligência Competitiva e da Gestão do Conhecimento (TARAPANOFF, 2004).

Muitas vezes, algumas Organizações adotam uma combinação híbrida de dois métodos, ou até uma versão parcial da OCTAVE, quando conjugada com outras abordagens, como, por exemplo, a da Governança nos moldes da combinação COBIT/ITIL.

Este texto foi baseado no documento da versão 2.0 do Método da OCTAVE, embora o Método OCTAVE-S não seja, ainda, tão amplamente documentado como o OCTAVE, não há problemas de documentação: o *OCTAVE Method Implementation Guide Version 2.0 OMIG* possui 18 volumes, muito fáceis de acessar e ler e extrair-se uma linha de aplicação. A localização e fornecida na bibliografia é <http://www.sei.cmu.edu/publications/pubweb.html>, (ALBERTS, *Introduction to the OCTAVE® Approach*) (ALBERTS, *OCTAVE Criteria v2.0*).

2.3. A Abordagem OCTAVE

Varias são as maneiras de enfocar e interpretar os riscos associados à necessidade de Segurança da Informação e Comunicação nas Organizações, mas uma abordagem metodológica é necessária para administrar a complexidade da tarefa.

A abordagem OCTAVE busca a efetividade na avaliação do risco associados à Segurança da Informação e Comunicação examinando os três fatores chaves: o Risco

Operacional, a Tecnológica e as Práticas de Segurança. Esses fatores chaves definem uma representação gráfica em três dimensões.

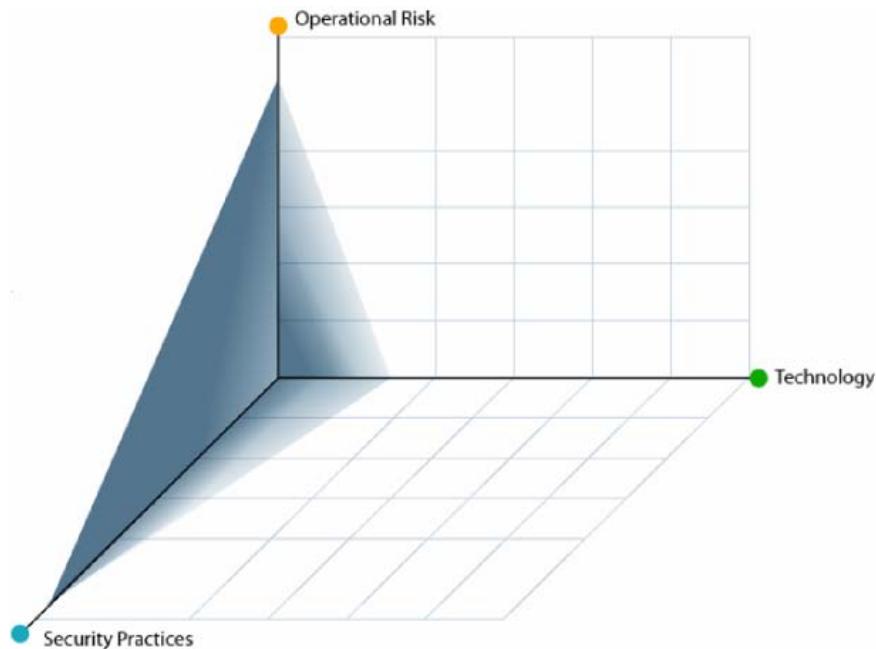


Figura 4 - A abordagem OCTAVE e os três fatores chaves (ALBERTS, Introduction to the OCTAVE® Approach)

O Método OCTAVE começa com uma avaliação estratégica no plano definido pelos dois fatores chaves, o Risco Operacional e as Práticas de Segurança. Essa avaliação é de importância vital para a melhoria da Segurança da Informação em qualquer iniciativa ou empreendimento da Organização, isto gera uma visão de nível estratégico no tratamento dos riscos, e proporcionando uma “linha de base” para a melhoria continuada do aspecto da Segurança da Informação e cumprimento da missão. Dessa forma o método OCTAVE não foca como prioridade nos seus esforços os aspectos Tecnológicos. Os planos definidos a partir das dimensões definidas pelo Risco Operacional, Tecnologia e Práticas de Segurança englobam outras abordagens, temos os modelos de Gestão da Segurança da Informação e Comunicação, Processos de Auditoria e Governança de TI convivendo em vários tipos de esquemas de interação. Destaca-se hoje uma integração das abordagens da Governança de TI e Inteligência Competitiva (CANONGIA, 2001).

A organização deve compreender suas necessidades de segurança da informação, logo inicialmente quando da elaboração de seus planos de negócio. O Método OCTAVE sendo uma avaliação estratégica do risco serve de base para o planejamento da segurança, e também,

para a conformidade da organização frente a processos de certificação da auditoria de segurança de sistemas de informação.

O Método OCTAVE é autodirecionado, o que significa que as pessoas de uma organização assumem a responsabilidade de definir a estratégia de segurança da organização de forma comprometida e proativa. As técnicas da metodologia OCTAVE alavancam o incremento do conhecimento das necessidades de Segurança da Informação e Comunicação da Organização, aprimorando as práticas e os processos de captura, e aprendizado na coleta dos dados da situação atual, e dai elaborar de forma planejada o tratamento dos riscos a Segurança da Informação.

O conhecimento dos riscos aos ativos críticos é usado para priorizar e definir a melhoria das áreas e para a elaboração de uma estratégia de segurança para toda a Organização.

Contrapondo as outras metodologias que dirigem os seus esforços aos riscos tecnológicos e as questões táticas apenas, a abordagem da metodologia OCTAVE visa o Risco Organizacional, e concentra-se na estratégia, nas questões relacionadas com a previsão do impacto se una concretização de uma ameaça explorar com sucesso uma vulnerabilidade de um ativo.

A partir das decisões tomadas com relação aos conhecimentos obtidos na avaliação OCTAVE, planos de mitigação desses riscos trataram essas ameaças. Isto porque a avaliação é flexível e robusta, pode ser adaptada para a maioria das organizações.

Na aplicação da OCTAVE, nas três fases, uma pequena equipe de pessoas composta pelas unidades operacionais (áreas de negócio) juntamente com o departamento de Tecnologia da Informação e Comunicação (área de TI), identifica as necessidades de segurança da organização, e conseguem equilibrar os três fatores chaves: o Risco Operacional, a utilização da Tecnológica e as Práticas de Segurança, como ilustrado na Figura 1.

Desta forma, a abordagem OCTAVE é impulsionada primeiramente por dois aspectos básicos: o Risco Operacional e as Práticas de Segurança. Nessa abordagem, a tecnologia é examinada apenas em relação às Práticas de Segurança, permitindo à organização refinar o seu ponto de vista das atuais Práticas de Segurança. Ao usar abordagem OCTAVE, uma organização aprende a tomar decisões de proteção as informações críticas relacionadas com ativo, baseadas nos riscos à confidencialidade, integridade, disponibilidade e autenticidade. Todos os aspectos de risco (ativos, ameaças, vulnerabilidades e o impacto organizacional) são integrados na tomada de decisões, habilitando a organização a combinar sua estratégia com a prática de segurança; pode-se assim elaborar uma “linha de base” de proteção relacionada à

informação e relacioná-la aos riscos de segurança. O monitoramento dessa linha de base fornece os elementos para o controle e colaboram no refinamento dos Planos de Segurança (ALBERTS, *Introduction to the OCTAVE® Approach*).

Desta forma podemos diferenciar a abordagem OCTAVE de outras metodologias a partir de uma rápida comparação dada pela tabela abaixo.

Tabela 1 - Comparação da abordagem OCTAVE e outras abordagens

OCTAVE	Outros Métodos
Avaliação Organizacional	Avaliação de Sistemas de TI
Focado nas práticas de segurança	Focado nas tecnologias de TI utilizadas
Aprecia as decisões de caráter estratégico	Aprecia as decisões de caráter tático
Autodirigida, liderada pela equipe de análise	Centralizada em um líder do time de TI

2.4. Os Princípios da Abordagem OCTAVE

A abordagem OCTAVE fundamenta-se em conjunto de princípios que a caracterizam e a diferencia. Por exemplo, o princípio de ser um método autodirecionado exige mais da Organização em termos da gestão do processo de avaliação e da tomada de decisões. Este princípio apóia a necessidade de uma equipe interdisciplinar, a equipe de análise, para conduzi-la no processo de avaliação. Essa necessidade é o requisito para um dos atributos desse princípio, o grau de maturidade da equipe de análise na aplicação do método. A equipe deve incluir pessoas de varias unidades: desde áreas de negócios até do departamento da TI, ambas as perspectivas são importantes para a construção visão dos riscos aos ativos e a necessidade de Segurança da Informação e Comunicação. Já em nível estratégico, a Organização deve conhecer o impacto nos ativos pela exposição a esses riscos, e como afetam o cumprimento da missão.

Desta forma, as ações tomadas com eficácia incorporando-se no comportamento da Organização pela capacitação do seu capital intelectual, em níveis de maturidade crescente, sempre preparados para responder pro-ativamente (CANONGIA, 2001) (TARAPANOFF, 2004)

Algumas atividades são categorizadas abaixo:

- Identificação das informações relacionadas com ativos críticos (por exemplo, informação, pessoas, processos e sistemas) importantes para o cumprimento da missão da organização;

- Priorização das atividades de análise dos riscos sobre os ativos julgados críticos para a Organização;
- Levantamento das relações entre os ativos críticos, as ameaças, vulnerabilidades desses ativos (tanto organizacional como tecnológica) que expõem os ativos às ameaças produzindo impactos e perdas;
- Avaliação dos riscos no contexto operacional - como eles são utilizados para conduzir os negócios de uma organização, como esses ativos estão expostos aos riscos e como as ameaças estão mapeadas;
- Criação de uma estratégia de proteção baseada na prática da melhoria continuada da segurança da organização, por meio da elaboração de planos de mitigação e de redução de riscos aos ativos críticos e lições aprendidas.

2.5. A Abordagem de Três Etapas

A avaliação de risco da segurança da informação é complementada por uma abordagem de três etapas. A metodologia OCTAVE está organizado em torno destes três aspectos básicos (ilustrado na Figura 2), permitindo ao pessoal organizacional montar um quadro das necessidades de Segurança Informação e Comunicações independentes da tecnologia atual na Organização. O progresso entre as fases é feito via reuniões do tipo workshop e pela utilização de ferramentas de coleta de dados aplicadas na plataforma técnica.

As fases estão descritas abaixo:

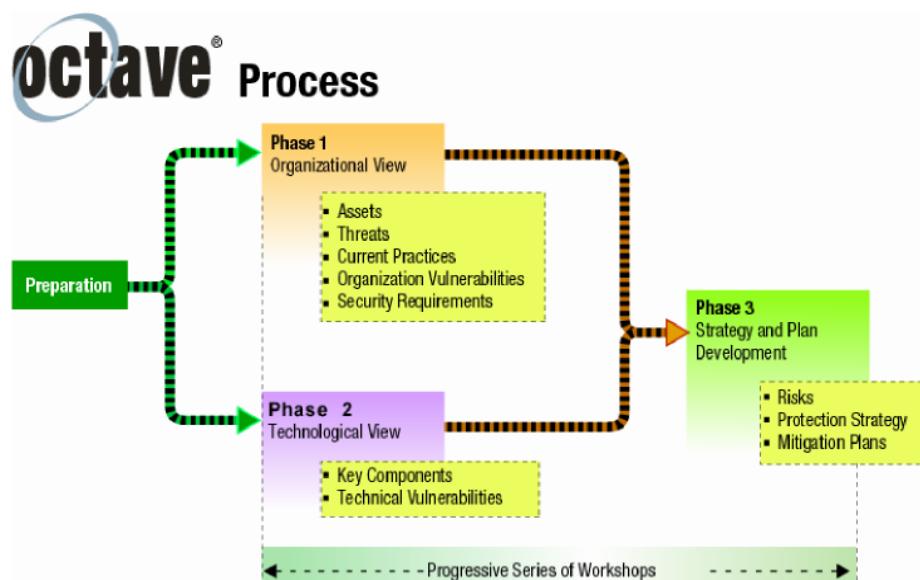


Figura 5 - As fases do método OCTAVE (ALBERTS, Introduction to the OCTAVE Approach)

- Fase 1: Criação do Perfil de Ameaça do Ativo – Esta é uma fase de avaliação Organizacional. A equipe de análise determina o que é importante para a

organização (as informações relacionadas com ativos), bem como o que está sendo feito para proteger os ativos. A equipe, em seguida, escolhe aqueles bens que são mais importantes para a organização (os ativos críticos), e descreve os requisitos de segurança para cada ativo crítico. Finalmente, identifica as ameaças para cada ativo crítico, criando o Perfil de Ameaça do Ativo;

- Fase 2: Identificação da Vulnerabilidade da Infra-estrutura - Esta é fase de avaliação Tecnológica, trata-se de uma avaliação da vulnerabilidade da infra-estrutura de TI da Organização. A equipe analisa os caminhos de acesso à rede, identifica e classifica os componentes de tecnologia da informação e os relacionamentos com cada um dos ativos críticos já caracterizados. A equipe de análise então determina uma avaliação qualitativa, isto é, em que medida cada classe desses componentes é resistente a ataques das ameaças caracterizadas no perfil do ativo. A documentação vai compor um banco de dados orientados aos ativos críticos, vulnerabilidades, ameaças e controles de segurança;
- Fase 3: Desenvolvimento da Estratégia da Segurança Informação e Comunicação e dos Planos de Segurança - Esta é uma fase de tomada de decisão e planejamento na Organizacional, a equipe de análise identifica riscos aos ativos críticos, avalia o nível de risco e decidem quais vai tratar e quais vão assumir. A equipe de análise cria a estratégia para a proteção da organização e mitigação de risco por meio de planos e com o conhecimento obtido nas duas fases anteriores (ADAILTO, OCTAVE - Como Gerenciar Riscos em Segurança da Informação, 2007) (ALBERTS, *Introduction to the OCTAVE® Approach*, 2007).

2.6. Os Fundamentos do Método OCTAVE

Os elementos essenciais; os princípios e requisitos da abordagem OCTAVE são consubstanciados num conjunto de critérios. Pode haver muitos métodos compatíveis com estes critérios, mas só há um conjunto de critérios para a abordagem da OCTAVE. Neste ponto, há dois métodos consistentes com os critérios que foram desenvolvidos pelo *National Institute of Standards and Technology - NIST*. O método OCTAVE, documentado no *OCTAVE Método Implementação Guide, v2.0*, foi concebido para grandes organizações em mente, enquanto que o OCTAVE-S foi desenvolvido para as pequenas organizações. Além disso, outros métodos podem ser definidos para contextos específicos, mas que estejam em consonância com aquele conjunto de critérios. Os requisitos relacionados a esses métodos têm por finalidade desenhar metodologias de uma forma coerente, que a partir de um elenco de

princípios, das estruturas e dos processos agreguem uma sinergia na interação com os métodos e técnicas, monitorando o desenvolvimento da aplicação do método. A Figura 3 ilustra essa inter-relação.

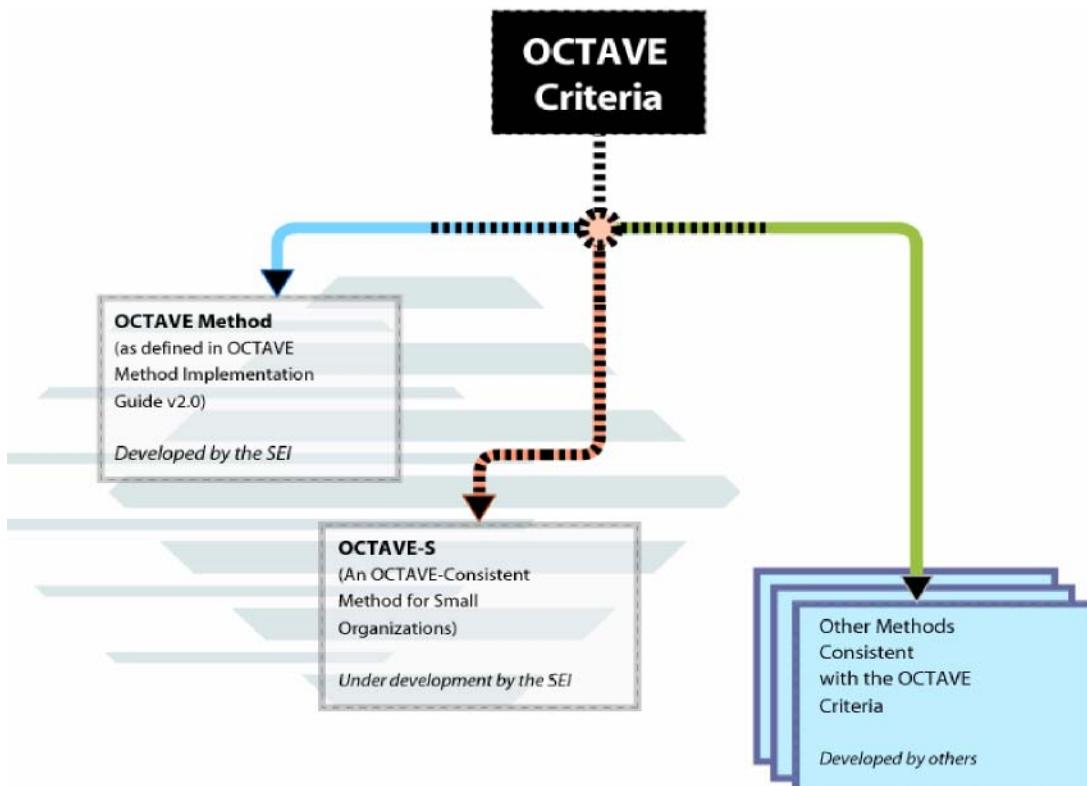


Figura 6 - Critérios da OCTAVE (ALBERTS, Introduction to the OCTAVE® Approach)

2.7. Os Critérios do Método OCTAVE

Os critérios estão baseados em um conjunto de princípios, atributos e elementos de saída em termos de resultado: saída/resultados, cujos conceitos são de natureza fundamental para o processo de condução da avaliação, é a filosofia subjacente ao processo de avaliação. Eles moldam a abordagem e fornecem uma base de conhecimento para o processo de avaliação. Por exemplo, o princípio de autodirecionamento na OCTAVE é um conceito que significa de que forma uma categoria de pessoas dentro da Organização desenvolverá as suas atividades de avaliação, e nos consequentes resultados da tomada de decisão.

Os requisitos para os critérios da avaliação estão autocontidos em termos de atributos e de suas saídas/resultados. Os atributos são as qualidades distintivas, as características, ligadas aos princípios. Existem requisitos para todos os elementos da abordagem OCTAVE, e são necessários para uma avaliação com êxito, tanto na perspectiva do processo de avaliação OCTAVE, como na perspectiva dos fatores críticos de sucesso da Organização. Os

atributos derivam dos princípios OCTAVE. Por exemplo, um dos atributos da OCTAVE é que uma equipe interdisciplinar (equipe de análise) compõe de pessoas das áreas da Organização que conduzirão os processos de avaliação. O princípio por trás da criação de uma equipe multidisciplinar de análise com pessoal da organização é do autodirecionamento.

Finalmente, as saídas/resultados são resultados necessários de cada fase da avaliação. Elas definem os achados que a equipe deve procurar em cada fase. A Tabela 2 relaciona os princípios e atributos na OCTAVE. A tabela 3 relaciona as saídas (ALBERTS, *Introduction to the OCTAVE® Approach*, 2007) (ALBERTS, *OCTAVE Criteria v2.0*, 2007).

Tabela 2 - Princípios e atributos no método OCTAVE

Princípio	Atributo/Requisito
Auto direcionamento	Comprometer a equipe de análise
	Incrementar as habilidades do time de análise
Medidas flexíveis	Catalogo de práticas
	Perfil de ameaças genérico
Processo definido	Catalogo de vulnerabilidades
	Atividades de avaliação definidas
Continuidade de processo	Resultados de avaliação documentados
	Avaliação do escopo
Visão voltada ao futuro	Descrição dos próximos passos
	Catalogo de práticas
Foco nos elementos críticos essenciais	Foco no risco
	Ações proativas
Gestão Integrada	Avaliação do escopo
	Foco nas atividades
Comunicação aberta	Questões organizacionais e tecnológicas
	Participação da área de negocio e da área da tecnologia da informação
Perspectiva Global	Participação dos gerentes sênior
	Abordagem colaborativa
Equipe de trabalho	Questões organizacionais e tecnológicas
	Participação da área de negocio e da área da tecnologia da informação
	Comprometer a equipe de análise
	Incrementar as habilidades do time de análise
	Participantes da área de negocio e da área da tecnologia da informação
	Abordagem colaborativa

Tabela 3 - Saídas/resultados do método OCTAVE

Fase	Saída - Resultado
Fase 1	Ativos críticos
	Requisitos de segurança para os ativos críticos
	Ameaça aos ativos críticos
	Atuais práticas de segurança
	Atuais vulnerabilidades organizacionais
Fase 2	Componentes chaves
	Atuais vulnerabilidades Tecnológicas
Fase 3	Catalogo de Risco aos ativos Críticos
	Estratégia de Proteção
	Planos de Mitigação de Risco

A metodologia OCTAVE cria uma visão global dos riscos atuais à segurança da informação para a organização, fornecendo um instantâneo no tempo, ou uma “linha de base”, que pode ser usado para a mitigação dos riscos e melhoria das atividades.

Durante a aplicação do OCTAVE, a equipe de análise realiza um conjunto de atividades que estão categorizados em três macros processos summarizados abaixo:

- Identificar os riscos a segurança da informação da organização;
- Analisar os riscos para determinar prioridades de tratamento;
- Planejar a melhoria através do desenvolvimento de uma estratégia de proteção para a organização, por meio de planos de mitigação e redução dos riscos aos ativos críticos.

Uma organização não vai melhorar a menos que implemente os planos específicos, desta forma, as seguintes atividades são realizadas após OCTAVE ser concluída com a equipe de análise, ou junto com outro pessoal designado.

- Planejar como implementar o plano estratégico de proteção composto de planos de ação específicos de redução dos riscos, através do desenvolvimento de linhas de ação pormenorizadas. (Esta atividade pode incluir uma detalhada análise de custo-benefício entre as estratégias e ação);
- Implementar os planos de ação pormenorizados;
- Monitorar, e acompanhar a implementação dos planos de ação para a eficácia de todo o processo de proteção. (Esta atividade inclui o monitoramento dos riscos específicos apontados na avaliação e os que porventura já tenha sido mapeado);
- Controlar as variações no plano de implementação e tomar as adequadas ações corretivas.

A Avaliação Risco Segurança a Informação faz parte de uma atividade da organização para a Gestão dos Riscos a Segurança Informação. A Figura 4 mostra a relação entre estas atividades e onde se encaixa o método OCTAVE. Nota-se que as atividades de Gerenciamento de Risco definem o Ciclo de Gestão do tipo plan-do-check-act.

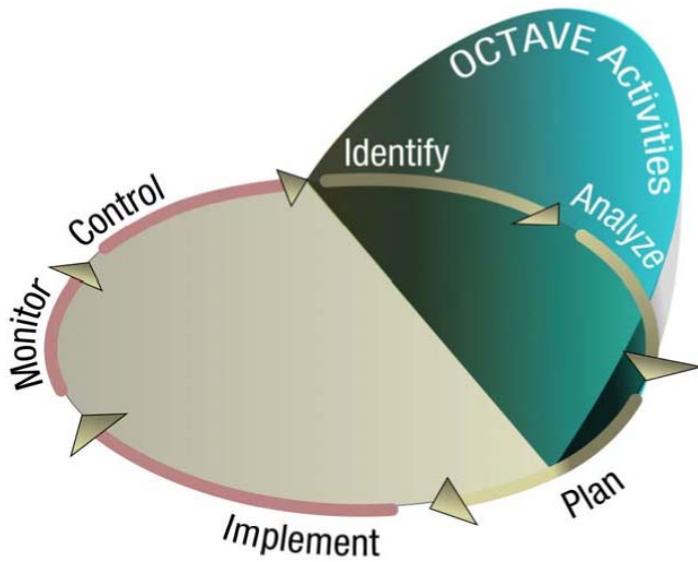


Figura 7 - O método OCTAVE as atividades de gerenciamento de risco(ALBERTS, Introduction to the OCTAVE® Approach)

Periodicamente, a organização terá de "redefinir" ou atualizar o seu perfil de segurança, "linha de base", realizando outra avaliação OCTAVE. O tempo entre as avaliações pode ser predeterminado (por exemplo, anualmente) ou desencadeado por eventos importantes (por exemplo, reorganização societária ou redesenho da infra-estrutura computacional da organização). Entre essas avaliações, uma organização pode periodicamente identificar novos riscos, analisar estes riscos em relação aos riscos existentes, e desenvolver planos de mitigação para eles (ADAILTO, 2007) (ALBERTS, *Introduction to the OCTAVE® Approach*, 2007) (ALBERTS, *OCTAVE Criteria v 2.0*, 2007).

2.8. A abrangência do método OCTAVE

O método OCTAVE foi desenvolvido para grandes organizações em mente (por exemplo, 300 ou mais empregados). O Tamanho não é a única consideração para decidir-se utilizar o método OCTAVE. Grandes organizações geralmente têm uma hierarquia multicamadas e são freqüentemente distribuídas em rede ou geograficamente distribuídas. A atividade de formalização de coleta de dados para determinar qual a formação relacionadas com ativo são importantes, como são utilizados e como eles são ameaçados é parte essencial da realização OCTAVE em grandes organizações. Finalmente, uma grande organização é susceptível de manter a sua própria infra-estrutura informática e ter a capacidade interna para executar as ferramentas de avaliação de vulnerabilidade e da interpretação dos resultados em relação aos seus ativos críticos.

2.9. Os processos do método OCTAVE

O OCTAVE Método compreende as três fases exigidas pelos critérios OCTAVE. Os processos nessas fases são descritas a seguir:

- Fase 1: Criação do Perfil de Ameaça do Ativo - As duas principais funções desta fase são a reunião das informações de toda a organização e definição dos perfis ameaça para os ativos críticos. A equipe de análise coleta informações sobre os ativos críticos, os requisitos de segurança, as ameaças, e os atuais pontos fortes e vulnerabilidades da organização junto aos representantes do quadro de superior. É composta de quatro processos:
 - Processo 1: Identificar o Conhecimento de Gerência Sênior - A equipe análise recolhe informação sobre ativos importantes, requisitos de segurança, as ameaças e as vulnerabilidades, os pontos fortes e fracos da organização, informações coletadas junto aos gerentes seniores;
 - Processo 2: Identificar o Conhecimento da Área Operacional - A equipe análise recolhe informação sobre ativos importantes, requisitos de segurança, as ameaças e as vulnerabilidades, os pontos fortes e fracos da organização, informações coletadas junto aos gerentes das áreas operacionais selecionadas;
 - Processo 3: Identificar o Conhecimento dos Funcionários - equipe de análise coleta do Staff em geral e dos membros de TI as informações sobre os ativos importantes, requerimentos de segurança, as ameaças, as vulnerabilidades e os pontos fortes da organização.
 - Processo 4: Criar os Perfis de Ameaça - a equipe de análise seleciona os ativos críticos e define os perfis, profile, de ameaça do ativo,
- Fase 2: Identificar as Vulnerabilidades da Infra-estrutura - Durante esta fase, a equipe de análise identifica e avalia os principais componentes dos sistemas que suportam os ativos críticos em termos da vulnerabilidade tecnológica. Inclui dois processos:
 - Processo 5: Identificar os componentes-chaves: a equipe de análise identifica um conjunto representativo de componentes-chaves dos sistemas de informação que suporta os ativos críticos, e é desenvolvida uma avaliação desses componentes;
 - Processo 6: Avaliação os componentes selecionados: a equipe de análise utiliza as ferramentas para avaliar os componentes selecionados, refinando os perfis de ameaças.

- Fase 3: Desenvolver a Estratégia de Segurança e Planos - O principal objetivo desta fase é a de avaliar os riscos para os ativos críticos e desenvolver uma estratégia organizacional, proteção e os planos de redução dos riscos.
 - Processo 7: Conduzir a análise de risco - A avaliação do impacto organizacional devido às ameaças nos ativos críticos é definida por um conjunto de critérios que estabelece e determina o valor impacto (alto médio ou baixo);
 - Processo 8: Desenvolver a Estratégia de Proteção - a equipe de análise desenvolve uma estratégia de proteção para toda a organização baseada na melhoria das práticas de segurança e nos planos de controle e redução dos riscos (ALBERTS, *Introduction to the OCTAVE® Approach*, 2007).

2.10. Documentação do método OCTAVE.

O OCTAVE Método está documentado no “OCTAVE Método Implementação Guide (OMIG)”, disponível a partir do seguinte site <<http://www.cert.org/octave>>.

A documentação é composta de 18 volumes de informações em tanto no formato Microsoft Word e quanto no PowerPoint. A lista abaixo descreve brevemente o conteúdo de cada volume.

- Volume 1: *Introduction*: esse volume inclui uma descrição do OCTAVE, orientações de como usar o guia, algumas sugestões relativas ao treinamento da equipe de análise;
- Volume 2: *Preliminary Activities*: Atividades preliminares, este volume contém as orientações de preparo para se fazer uma avaliação OCTAVE, incluindo a seleção do time de análise e os seus participantes, organização e logística. Também neste volume você encontrará uma orientação personalizada, e uma visão executiva para os gerentes sênior e participante;
- Volumes 3 – 12: *The OCTAVE Processo*: Este volume prove um conjunto completo de informação para as três fases e os oito processos do método OCTAVE;
- Volume 13: *After the Evaluation*: Esta curta seção proporciona uma orientação e um exemplo do que fazer antes de concluir a validação;
- Volume 14: *Bibliography and Glossary*: Fornece uma longa, mas não exaustiva lista de referências, sites web e outras fontes de informações relativas à segurança

da informação, práticas, e padrões Standards. Um glossário prove definições para os termos chaves usadas através do guia;

- Volume 15: Appendix A: OCTAVE Catalog of Practices: catálogo de práticas do OCTAVE
- Esse volume prove um conjunto de boas práticas de segurança da informação as quais a organização basea-se para leva a cabo a avaliação OCTAVE;
- Volume 16: Appendix B: *OCTAVE Data Flow*: este volume contém um fluxo de dados que retrata, e uma forma concisa, todas as atividades, entradas, saídas, e as estruturas de dados na forma “worksheets” do método OCTAVE;
- Volume 17: Appendix C: *Complete Example Results*: Esse volume provê um conjunto completo dos exemplos resultados (os quais são encontrados em partes através do guia);
- Volume 18: Appendices D and E: *White Papers: Apêndices D e E* (ALBERTS, 2002).

3. CONCEITOS DO PMBOK

A área de Tecnologia de Informação e Comunicação TIC nas duas últimas décadas tem apresentado uma grande evolução em diversas áreas de conhecimento, criando necessidades, principalmente nas áreas de gestão e de gerenciamento de projetos. Essas necessidades estão ligadas a vários fatores, mas três são essenciais para mudanças nas formas de planejar, projetar, usar e extrair benefícios da TIC: a evolução dos modelos de gestão aceitos internacionalmente, a convergência tecnológica que permite a integração desses modelos em ambientes organizacionais reais e o uso de indicadores da governança nas práticas de gestão de TIC. A abordagem do gerenciamento de projetos demonstra-se como fator crítico de sucesso para os empreendimentos nesses contextos mudança e de superação de expectativa. (RALHA e FERREIRA, 2007)

Hoje, a abordagem do gerenciamento de projetos mais bem sucedida está mapeada em padrões, terminologia e um elenco de boas práticas em um guia nomeado *Project Management Body of Knowledge – PMBOK Guide*, o Corpo de Conhecimento em Gerência de Projetos. O Guia PMBOK é um padrão internacionalmente aceito.

O PMBOK é um guia de conhecimento e de melhores práticas para a profissão de Gerência de Projetos foi aprovada como padrão a nível governamental pela *American National Standard - ANSI* nos Estados Unidos reúne o conhecimento comprovado internacionalmente na área de gerência de projetos, através das práticas tradicionais e práticas inovadoras e avançadas. Fornece um guia genérico para todas as áreas de projetos, seja uma obra da construção civil, um processo de fabricação industrial ou a produção de software. Destaca-se no aspecto da padronização dos termos utilizados na gerência de projetos. (RALHA e FERREIRA, 2007)

O PMBOK é uma formulação do *Project Management Institute – PMI*, organização que estabelece padrões, prove seminários, programas educacionais e certificação profissional para as organizações nas exigências de gerenciamento de projetos.

O PMI teve a sua fundação em 1969 e cresceu para ser uma organização reconhecida internacionalmente como a organização dos profissionais de gerência de projetos, com cerca de 80.000 membros em todo o mundo, é a organização mais importante da área de gerenciamento de projetos. (ROCHA, 2008)

3.1. Descrição dos conceitos utilizados

Este trabalho está baseado no PMBOK e os conceitos necessários e desenvolvidos foram extraídos do livro “Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projeto”, terceira edição, Norma Nacional Americana ANSI/PMI 99-001-2004. Uma breve descrição é desenvolvida a seguir para fins de coerência e compreensão do trabalho elaborado.

Um projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo. (Guia PMBOK®, 2004). Um projeto é um empreendimento com características próprias, tendo princípio e fim, conduzido por pessoas, para atingir metas estabelecidas dentro de parâmetros de prazo, custos e qualidade. Ele é um empreendimento temporário cujo objetivo é criar um produto ou serviço distinto e único.

A gerência é a ação que consiste em executar atividades e tarefas que têm como propósito planejar e controlar atividades de outras pessoas para atingir objetivos que não podem ser alcançados caso as pessoas atuem individualmente ou sem coordenação.

O gerente de projetos é a pessoa responsável pela realização dos objetivos do projeto. (Guia PMBOK®, 2004)

O gerente de projetos é o profissional responsável pelo gerenciamento, administração e controle de projetos, o chefe da equipe de projeto. As ações que afetam o projeto decorrem das decisões.

Partes interessadas no projeto são pessoas e organizações ativamente envolvidas no projeto ou cujos interesses podem ser afetados como resultado da execução ou do término do projeto. Eles podem também exercer influência sobre os objetivos e resultados do projeto. A equipe de gerenciamento de projetos precisa identificar as partes interessadas, determinar suas necessidades e expectativas e, na medida do possível, gerenciar sua influência em relação aos requisitos para garantir um projeto bem sucedido. (Guia PMBOK®, 2004)

O gerenciamento de projetos é a aplicação de conhecimento, habilidades, ferramentas e técnicas às atividades do projeto a fim de atender aos seus requisitos. O gerenciamento de projetos é realizado através da aplicação e da integração dos seguintes processos de gerenciamento de projetos: iniciação, planejamento, execução, monitoramento e controle, e encerramento. (Guia PMBOK®, 2004)

O ciclo de vida do projeto define as fases que conectam o início de um projeto ao seu final, quando uma organização identifica uma oportunidade que deseja aproveitar, poderá autorizar um estudo de viabilidade para decidir se deve realizar o projeto. A definição do ciclo de vida do projeto pode ajudar o gerente de projetos a esclarecer se deve tratar o estudo de

viabilidade como a primeira fase do projeto ou como um projeto autônomo separado. A abordagem de ciclo de vida para o projeto ajuda a administrar a complexidade organizada que é o gerenciamento de projetos e suas áreas de conhecimento. (Guia PMBOK®, 2004)

3.2. Área de conhecimento em gerenciamento de projetos

Uma área identificada de gerenciamento de projetos definida por seus requisitos de conhecimentos é descrita em termos dos processos que a compõem, suas práticas, entradas, saídas, ferramentas e técnicas. (Guia PMBOK®, 2004)

O PMBOK é organizado em áreas e conhecimento, onde cada uma destas áreas é descrita através de processos. Cada área de conhecimento se refere a um aspecto a ser considerado dentro da gerência de projetos. A não execução de um dado processo de uma área afeta negativamente o projeto, pois o projeto é um esforço integrado.

São nove as áreas de conhecimento do PMBOK: gerenciamento de integração do projeto, gerenciamento do escopo do projeto, gerenciamento de tempo do projeto, gerenciamento de custos do projeto, gerenciamento da qualidade do projeto, gerenciamento de Recursos humanos do projeto, gerenciamento das comunicações do projeto, gerenciamento de riscos do projeto e gerenciamento de aquisições do projeto.

3.3. Gerenciamento da Integração

A área de conhecimento em gerenciamento de integração do projeto inclui os processos e as atividades necessárias para identificar, definir, combinar, unificar e coordenar os diversos processos e atividades de gerenciamento de projetos dentro dos grupos de processos de gerenciamento de projetos.

Os processos de gerenciamento da integração do projeto incluem os seguintes: desenvolver o termo de abertura do projeto, desenvolver a declaração do escopo preliminar do projeto, desenvolver o plano de gerenciamento do projeto, orientar e gerenciar a execução do projeto, monitorar e controlar o trabalho do projeto, controle integrado de mudanças e encerrar o projeto. (Guia PMBOK®, 2004)



Figura 8 - Mapa mental do Gerenciamento da Integração (Guia PMBOK®, 2004)

- O processo de desenvolvimento do termo de abertura do projeto autoriza formalmente um projeto ou uma fase do projeto;
- O processo de desenvolvimento da declaração do escopo preliminar do projeto fornece uma descrição de alto nível do escopo do projeto;
- O processo de desenvolvimento do plano de gerenciamento do projeto documenta as ações necessárias para definir, preparar, integrar e coordenador todos os planos auxiliares em um plano de gerenciamento do projeto;
- O processo de orientar e gerenciar a execução do projeto realiza o trabalho definido no plano de gerenciamento do projeto para atingir os requisitos do projeto definidos na declaração do escopo do projeto;
- O processo de monitorar e controlar o trabalho do projeto monitora e controla os processos usados para iniciar, planejar, executar e encerrar um projeto para atender aos objetivos de desempenho definidos no plano de gerenciamento do projeto;
- O processo de controle integrado de mudanças faz a revisão de todas as solicitações de mudança, aprovação de mudança e controle de mudanças nos produtos e ativos de processos organizacionais;
- O processo de encerramento do projeto faz a finalização de todas as atividades em todos os grupos de processos de gerenciamento de projetos para encerrar formalmente o projeto ou uma de suas fases.

Esse processo tem como saída principal o plano global do projeto, ele é o documento que descreve os procedimentos a serem conduzidos durante a sua execução. É esqueleto (*framework*) de toda a execução, nele estão contidos os planos secundários, cronogramas, aspectos técnicos e outros documentos e informações para a equipe de projeto.

3.4. Gerenciamento de Escopo

O gerenciamento do escopo do projeto inclui os processos necessários para garantir que o projeto inclua todo o trabalho necessário, e somente ele, para terminar o projeto com sucesso. O escopo pode ser dividido em: escopo funcional, escopo técnico e escopo de atividade.

O escopo funcional é o conjunto de características funcionais do produto, ou serviço, a ser desenvolvido pelo projeto, tais como capacidade, mercado, filosofia etc. Normalmente são direcionados ao cliente e são também denominados requisitos funcionais.

O escopo técnico é composto das características técnicas do projeto, destacando os padrões e as especificações a serem utilizadas, normas legais a serem obedecidas, procedimentos de qualidade (ISO) etc. Normalmente são direcionados para a equipe do projeto e são também denominados requisitos técnicos.

O escopo de atividades é o trabalho a ser realizado para prover os escopos técnico e funcional do produto, ou serviço, do projeto, normalmente evidenciado na Estrutura Analítica do Projeto (EAP).

O gerenciamento do escopo do projeto trata principalmente da definição e controle do que está e do que não está incluído no projeto.

Os processos de gerenciamento da integração do projeto incluem os seguintes: planejamento do escopo, definição do escopo, criação das EAP (Estrutura Analítica do Projeto). (Guia PMBOK®, 2004)

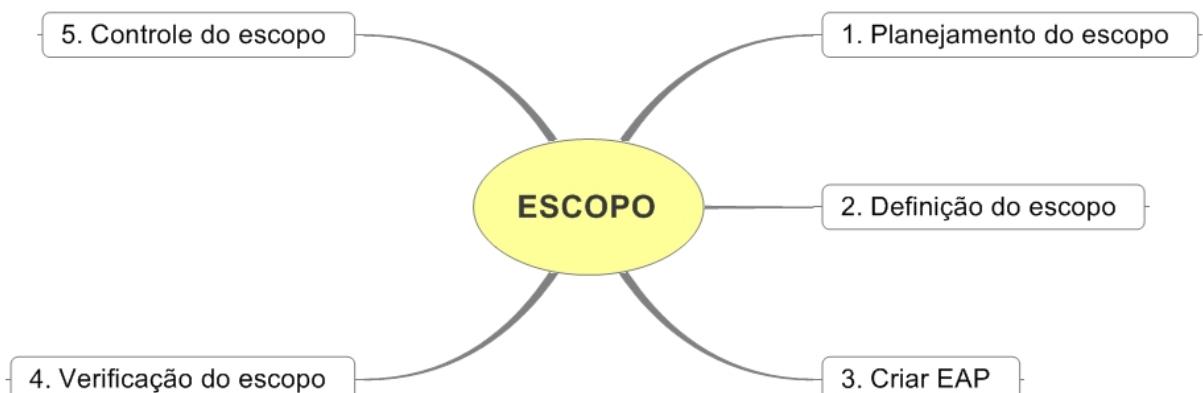


Figura 9 - Mapa mental do Gerenciamento de Escopo (Guia PMBOK®, 2004)

- O processo de planejamento do escopo elabora um plano de gerenciamento do escopo do projeto que documenta como o escopo do projeto será definido, verificado e controlado e como a estrutura analítica do projeto (EAP) será criada e definida;
- O processo de definição do escopo desenvolve uma declaração de escopo do projeto como a base para futuras decisões do projeto;
- O processo de criação da Estrutura Analítica do Projeto faz a subdivisão dos principais produtos do projeto e do trabalho do projeto em componentes menores e mais facilmente gerenciáveis;
- O processo de verificação do escopo faz a formalização da aceitação dos produtos do projeto que foram concluídos;
- O processo de controle de escopo faz o controle das mudanças no escopo do projeto.

Esse processo tem como saída principal o plano de gerenciamento do escopo, ele é o documento formal que descreve os procedimentos que serão utilizados para gerenciar todo o escopo do projeto.

3.5. Gerenciamento de Tempo

O gerenciamento de tempo do projeto inclui os processos necessários para realizar o término do projeto no prazo. Os processos de gerenciamento de tempo do projeto incluem os seguintes: definição de atividade, seqüenciamento de atividades, estimativa de recursos de atividades, desenvolvimento do cronograma e controle do cronograma. (Guia PMBOK®, 2004)

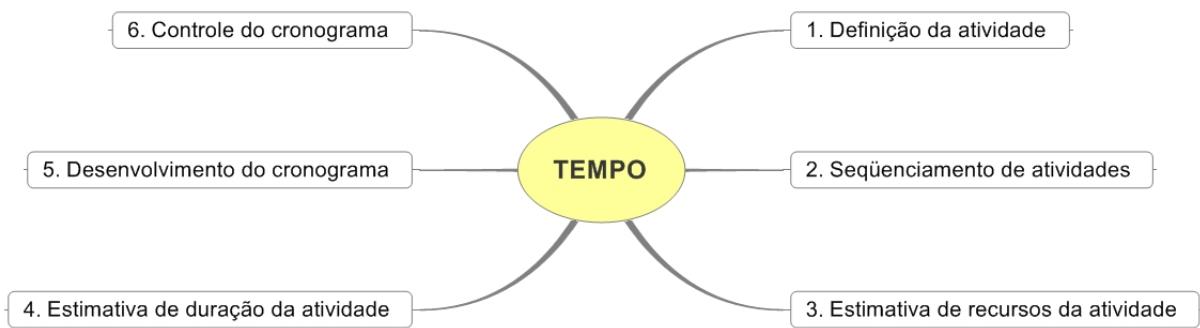


Figura 10 - Mapa mental do Gerenciamento de Tempo (Guia PMBOK®, 2004)

- O processo de definição da atividade identifica as atividades específicas do cronograma que precisam ser realizadas para produzir os vários produtos do projeto;
- O processo de seqüenciamento de atividades identifica e documenta as dependências entre as atividades do cronograma;
- O processo de estimativa de recursos da atividade faz a estimativa do tipo e das quantidades de recursos necessários para realizar cada atividade do cronograma.
- O processo de estimativa de duração de atividade faz a estimativa do número de períodos de trabalho que serão necessários para terminar as atividades individuais do cronograma;
- O processo de desenvolvimento do cronograma faz a análise dos recursos necessários, restrições do cronograma, durações e seqüências de atividades para criar o cronograma do projeto;
- O processo de controle do cronograma faz o controle das mudanças no cronograma do projeto.

Esse processo tem como saída principal o plano de gerenciamento do cronograma, ele é o documento formal que descreve os procedimentos que serão utilizados para gerenciar todos os prazos do projeto

3.6. Gerenciamento de Custos

O gerenciamento de custos do projeto inclui os processos envolvidos em planejamento, estimativa, orçamentação e controle de custos, de modo que seja possível terminar o projeto dentro do orçamento aprovado.

Os processos de gerenciamento de custo do projeto incluem os seguintes: estimativa de custos, orçamentação e controle de custos. (Guia PMBOK®, 2004)

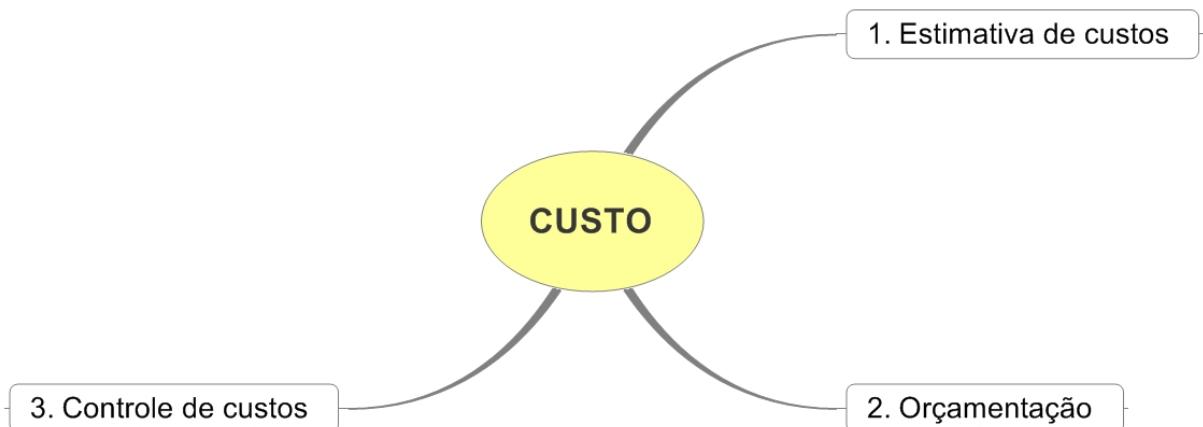


Figura 11 - Mapa mental do Gerenciamento de Custos (Guia PMBOK®, 2004)

- O processo de estimativa de custos desenvolve uma estimativa dos custos dos recursos necessários para terminar as atividades do projeto;
- O processo de orçamentação faz a agregação dos custos estimados de atividades individuais ou dos pacotes de trabalho para estabelecer uma linha de base dos custos;
- O processo de controle de custos faz o controle dos fatores que criam as variações de custos e controles das mudanças no orçamento do projeto.

Esse processo tem como saída principal o plano de gerenciamento de custos, ele é o documento formal que descreve os procedimentos que serão utilizados para gerenciar todos os custos do projeto.

3.7. Gerenciamento de Qualidade

Os processos de gerenciamento da qualidade do projeto incluem todas as atividades da organização executora que determinam as responsabilidades, os objetivos e as políticas de

qualidade, de modo que o projeto atenda às necessidades que motivaram sua realização. Eles implementam o sistema de gerenciamento da qualidade através da política, dos procedimentos e dos processos de planejamento da qualidade, garantia da qualidade e controle da qualidade, com atividades de melhoria contínua dos processos conduzidas do início ao fim, conforme adequado.

Os processos de gerenciamento da qualidade do projeto incluem os seguintes: planejamento da qualidade, realizar a garantia da qualidade, realizar o controle da qualidade. (Guia PMBOK®, 2004)

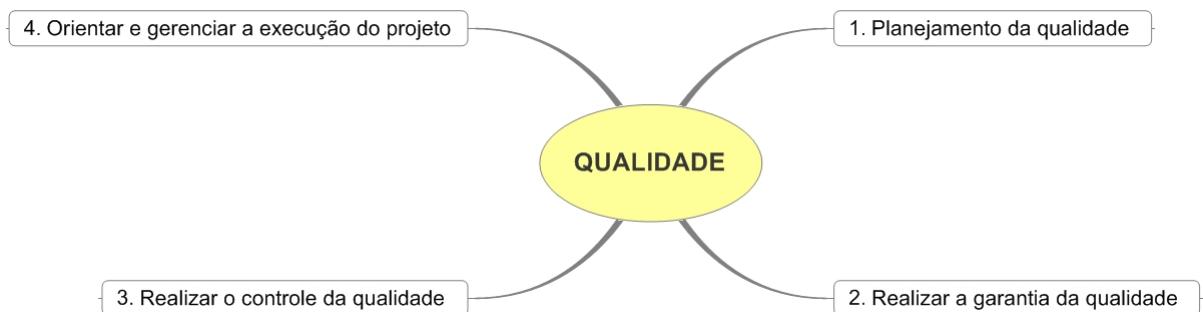


Figura 12 - Mapa mental do Gerenciamento de Qualidade (Guia PMBOK®, 2004)

- O processo de planejamento da qualidade faz a identificação dos padrões de qualidade relevantes para o projeto e a determinação de como satisfazê-lo;
- O processo da realização da garantia da qualidade faz a aplicação das atividades de qualidade planejadas e sistemáticas para garantir que o projeto empregue todos os processos necessários para atender aos requisitos;
- O processo da realização o controle da qualidade faz monitoramento dos resultados específicos do projeto a fim de determinar se eles estão de acordo com os padrões relevantes de qualidade e identificação de maneiras para eliminar as causas de um desempenho insatisfatório;
- O processo de orientar e gerenciar a execução do projeto faz atualização das ações corretivas e preventivas recomendadas e o reparo de defeito recomendado concluindo com os produtos validados.

Esse processo tem como saída principal o plano de gerenciamento da qualidade, ele é o documento formal que descreve os procedimentos que serão utilizados para gerenciar todos os aspectos da qualidade do projeto.

3.8. Gerenciamento de Recursos Humanos

O gerenciamento de recursos humanos do projeto inclui os processos que organizam e gerenciam a equipe do projeto. A equipe do projeto é composta de pessoas com funções e responsabilidades atribuídas para o término do projeto. Embora seja comum falar-se de funções e responsabilidades atribuídas, os membros da equipe devem estar envolvidos em grande parte do planejamento e da tomada de decisões do projeto.

O envolvimento dos membros da equipe desde o início acrescenta especialização durante o processo de planejamento e fortalece o compromisso com o projeto. O tipo e o número de membros da equipe do projeto muitas vezes podem mudar conforme o projeto se desenvolve. Os membros da equipe do projeto podem ser chamados de pessoal do projeto.

A equipe de gerenciamento de projetos é um subconjunto da equipe do projeto e é responsável pelas atividades de gerenciamento de projetos, como planejamento, controle e encerramento. Esse grupo de pessoas pode ser chamado de equipe principal, executiva ou líder.

Os processos de gerenciamento de recursos humanos do projeto incluem: planejamento dos recursos humanos, contratar e mobilizar as equipe de projeto, desenvolver a equipe de projeto e gerenciar a equipe do projeto. (Guia PMBOK®, 2004)



Figura 13 - Mapa mental do Gerenciamento de Recursos Humanos (Guia PMBOK®, 2004)

- O processo de planejamento de recursos humanos faz a identificação documentação de funções, responsabilidades e relações hierárquicas do projeto, além da criação do plano de gerenciamento de pessoal;
- O processo de contração ou mobilização da equipe do projeto obtém os recursos humanos necessário para terminar o projeto;
- O processo de desenvolver a equipe do projeto faz a melhoria das competências e interação de membros da equipe para aprimorar o desempenho do projeto;

- O processo de gerenciar a equipe do projeto faz acompanhamento do desempenho de membros da equipe, fornecimento de realimentação (*feedback*), resolução de problemas e coordenação de mudanças para melhorar o desempenho do projeto;
- O processo de gerenciar a equipe do projeto faz o gerenciamento do desempenho da equipe de projeto solucionando os conflitos que ocorrem entre o projeto e a organização.

Esse processo tem como saída principal o plano de gerenciamento de pessoal, ele é o documento formal que descreve os procedimentos que serão utilizados para gerenciar todos os recursos humanos do projeto. Também conhecido como Plano de Gerenciamento de Recurso Humanos.

3.9. Gerenciamento das Comunicações

O gerenciamento das comunicações do projeto é a área de conhecimento que emprega os processos necessários para garantir a geração, coleta, distribuição, armazenamento, recuperação e destinação final das informações sobre o projeto de forma oportuna e adequada. Os processos de gerenciamento das comunicações do projeto fornecem as ligações críticas entre pessoas e informações que são necessárias para comunicações bem-sucedidas. Os gerentes de projetos podem gastar um tempo excessivo na comunicação com a equipe do projeto, partes interessadas, cliente e patrocinador. Todos os envolvidos no projeto devem entender como as comunicações afetam o projeto como um todo.

Os processos de gerenciamento das comunicações do projeto incluem os seguintes: planejamento das comunicações, distribuições das informações, relatório de desempenho e gerenciar as partes interessadas. (Guia PMBOK®, 2004)

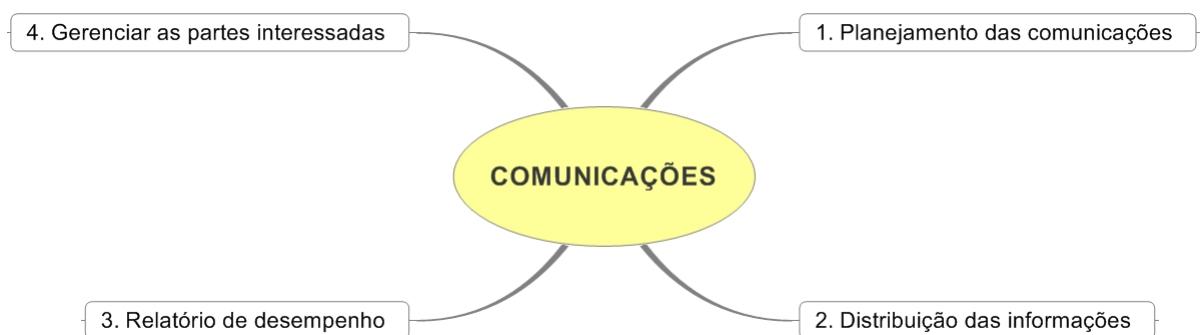


Figura 14 - Mapa mental do Gerenciamento das Comunicações (Guia PMBOK®, 2004)

- O processo de planejamento das comunicações determina as necessidades de informações e comunicações das partes interessadas no projeto;

- O processo de distribuição das informações disponibiliza as informações necessárias à disposição das partes interessadas no projeto no momento adequado;
- O processo que elabora o relatório de desempenho faz a coleta e distribuição das informações sobre o desempenho, composto das informações do andamento, a medição do progresso e previsão de custos e prazos;
- O processo de gerenciar as partes interessadas faz o gerenciamento das comunicações das comunicações para satisfazer os requisitos das partes interessadas no projeto e resolver os conflitos.

Esse processo tem como saída principal o plano de gerenciamento das comunicações, ele é o documento formal que descreve os procedimentos que serão utilizados para gerenciar todo o processo de comunicação no projeto.

3.10. Gerenciamento de Riscos

O gerenciamento de riscos do projeto inclui os processos que tratam da realização de identificação, análise, respostas, monitoramento e controle e planejamento do gerenciamento de riscos em um projeto; a maioria desses processos é atualizada durante todo o projeto. Os objetivos do gerenciamento de riscos do projeto são aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e o impacto dos eventos adversos ao projeto.

Os processos de gerenciamento de riscos do projeto incluem os seguintes: planejamento do gerenciamento de riscos, identificação dos riscos, análise qualitativa dos riscos, análise quantitativa dos riscos, planejamento de respostas a riscos e monitoramento e controle de riscos. (Guia PMBOK®, 2004)

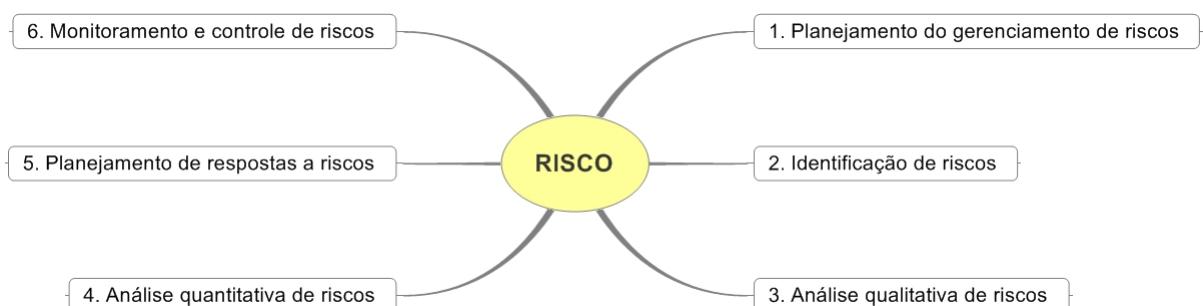


Figura 15 - Mapa mental do Gerenciamento de Risco (Guia PMBOK®, 2004)

- O processo de planejamento do gerenciamento de riscos desenvolve os meios para a decisão de como abordar, planejar e executar as atividades de gerenciamento de riscos de um projeto;
- O processo de identificação de riscos determina os riscos que podem afetar o projeto e faz a documentação de suas características;

- O processo de análise qualitativa de riscos faz uma priorização dos riscos para a análise ou para ação adicional subsequente através de avaliação e combinação de sua probabilidade de ocorrência e impacto;
- O processo de análise quantitativa de risco faz a análise numérica do efeito dos riscos identificados nos objetivos gerais do projeto;
- O processo de resposta a risco desenvolve as opções e ações para aumentar as oportunidades e reduzir as ameaças aos objetivos do projeto;
- O processo de monitoramento e controle de riscos faz o acompanhamento dos riscos identificados, a monitoração dos riscos residuais, identificação dos novos riscos, execução de planos de respostas a riscos e avaliação da sua eficácia durante todo o ciclo de vida do projeto.

Esse processo tem como saída principal o plano de gerenciamento de riscos, ele é o documento formal que descreve os procedimentos que serão utilizados para gerenciar os riscos através do projeto. O plano de riscos é um dos planos secundários do plano geral do projeto.

3.11. Gerenciamento de Aquisições

O gerenciamento de aquisições do projeto inclui os processos para comprar ou adquirir os produtos, serviços ou resultados necessários de fora da equipe do projeto para realizar o trabalho. Este capítulo apresenta duas perspectivas de aquisição. A organização pode ser o comprador ou o fornecedor do produto, serviço ou resultados sob um contrato. O gerenciamento de aquisições do projeto inclui os processos de gerenciamento de contratos e de controle de mudanças necessários para administrar os contratos ou pedidos de compra emitidos por membros da equipe do projeto autorizados. O gerenciamento de aquisições do projeto também inclui a administração de qualquer contrato emitido por uma organização externa (o comprador) que está adquirindo o projeto da organização executora (o fornecedor) e a administração de obrigações contratuais estabelecidas para a equipe do projeto pelo contrato.

Os processos de gerenciamento de aquisições do projeto incluem: planejar a compra, planejar contratações, solicitar respostas de fornecedores, selecionar fornecedores, administração de contrato encerramento do contrato. (Guia PMBOK®, 2004)

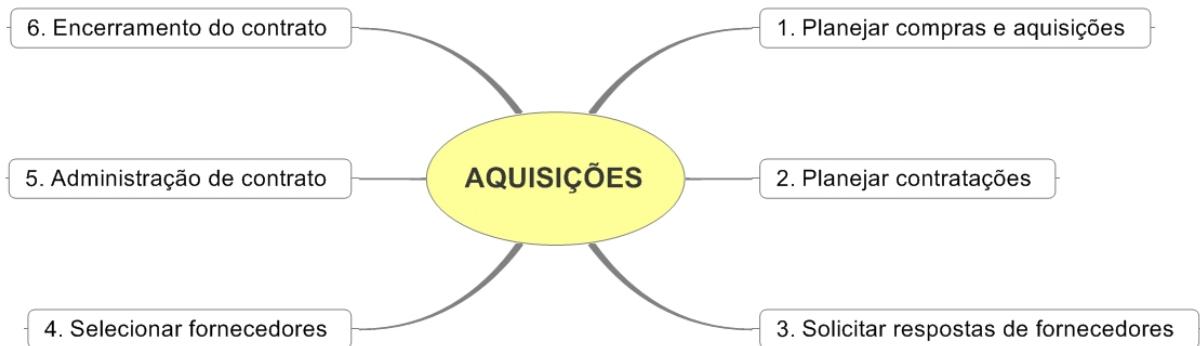


Figura 16 - Mapa mental do Gerenciamento de Aquisições (Guia PMBOK®, 2004)

- O processo de planejar compras e aquisições determina o que comprar ou adquirir, quando e como efetuar essas atividades;
- O processo de planejar as contratações faz a documentação dos requisitos de produtos, serviços e resultados e identificação de possíveis fornecedores;
- O processo de respostas de fornecedores obtém informações, cotações, preços, ofertas ou propostas, conforme a acordado no planejamento do gerenciamento do projeto;
- O processo de seleção dos fornecedores faz a análise de ofertas, escolha entre possíveis fornecedores e negociação de um contrato por escrito com cada fornecedor;
- O processo de administração de contratos faz o gerenciamento do contrato e da relação entre o comprador e o fornecedor, análise e documentação do desempenho atual ou passado de um fornecedor a fim de estabelecer ações corretivas necessárias e fornecer uma base para futuras relações com o fornecedor.

Esse processo tem como saída principal o plano de gerenciamento das aquisições, ele é o documento formal que descreve os procedimentos que serão utilizados para gerenciar todos os contratos do projeto.

4. PLANO DE PROJETO PARA O MÉTODO OCTAVE

4.1. Gerenciamento da Integração

Na área de gerenciamento da integração têm-se tradicionalmente os seguintes documentos:



Figura 17 - Documentos da Gerencia da Integração (adaptado de VARGAS, 2007)

Os documentos Apresentação do Projeto e Termo de Abertura do projeto são essenciais e estão apresentados em forma de *Templates* nos Apêndices A e B.

Para o caso específico de aplicação do método OCTAVE, o Gráfico de GANTT (*Project Gantt Chart*) terá variação apenas dos prazos e possivelmente na freqüência das reuniões agendadas, ele é construído e mantido no Microsoft Project, de onde pode ser impresso em formato de formulário/relatório. A seguir é apresentado o formato.

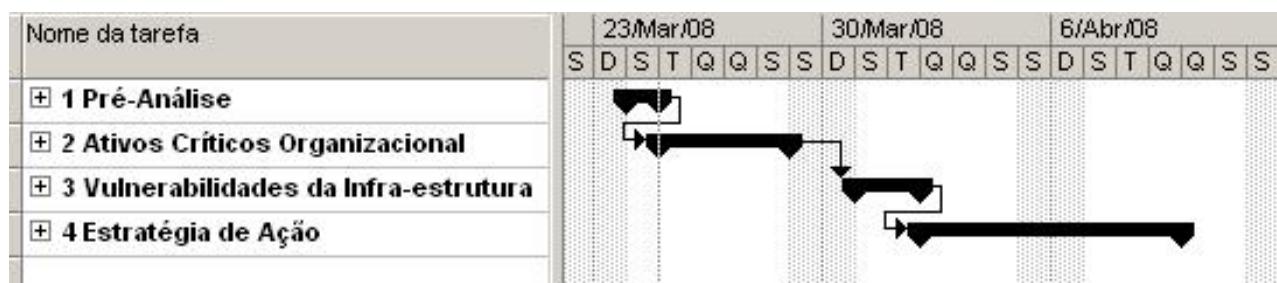


Figura 18 - Formato do Gráfico de Gantt

O Sistema de Controle Integrado de Mudanças para o caso específico é fixo e está apresentado no Apêndice C.

O Modelo de Registro de Lições Aprendidas para o caso específico é fixo e está apresentado no Apêndice D.

4.2. Gerenciamento de Escopo

Na área de gerenciamento de escopo têm-se tradicionalmente os seguintes documentos:

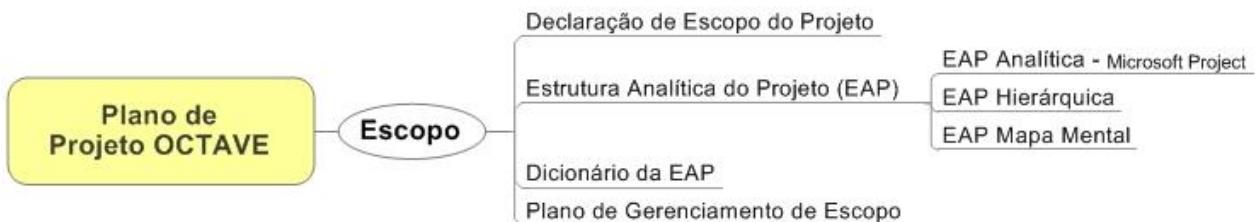


Figura 19 - Documentos da Gerencia de Escopo (adaptado de VARGAS, 2007)

A Declaração de Escopo tem que ser preenchida a cada novo projeto, está apresentada no Apêndice E.

A Estrutura Analítica de Projeto (EAP), não deve ter variação, pois reflete as atividades a serem desenvolvidas pelo método OCTAVE. O que pode ocorrer é a necessidade de Atividades complementares resultantes da execução do método, como o treinamento da Equipe da Empresa Cliente ou desenvolvimento de uma Política de Segurança com base nas contra-medidas resultantes do método. A EAP em sua forma hierárquica, que é a mais tradicional, está apresentada no Apêndice F. A EAP Analítica é fornecido com a impressão das listas de atividades constantes no Microsoft Project, como é mostrado a seguir:

Nome da tarefa
<input checked="" type="checkbox"/> 1 Pré-Análise
<input checked="" type="checkbox"/> 1.1 Apresentar o Método o Octave
1.1.1 Apresentar a Metodologia
1.1.2 Definir o Escopo Inicial
1.1.3 Estabelecer o Cronograma Inicial
1.1.4 Levantar e Identificar os Recursos
1.1.5 Documentar a Pré-Análise
1.1.6 Entrega da Documentação de Pré-Análise
<input checked="" type="checkbox"/> 2 Ativos Críticos Organizacional
<input checked="" type="checkbox"/> 2.1 Identificar as Informações Estratégicas
2.1.1 Detalhar o Escopo da Pré-Análise
2.1.2 Detalhar o Cronograma Inicial
2.1.3 Identificar a Missão Organizacional
2.1.4 Identificar os Requisitos do Negócio Organizacional
2.1.5 Identificar o Grupo de Entrevistados
2.1.6 Solicitar os Documentos Estratégicos da Organização
2.1.7 Documentar a Identificação das Informações Estratégicas
2.1.8 Entrega da Documentação da Identificação das Informações Estratégicas

Figura 20 - Formato da EAP Analítica

A EAP na forma de mapa mental é apresentada como a seguir:

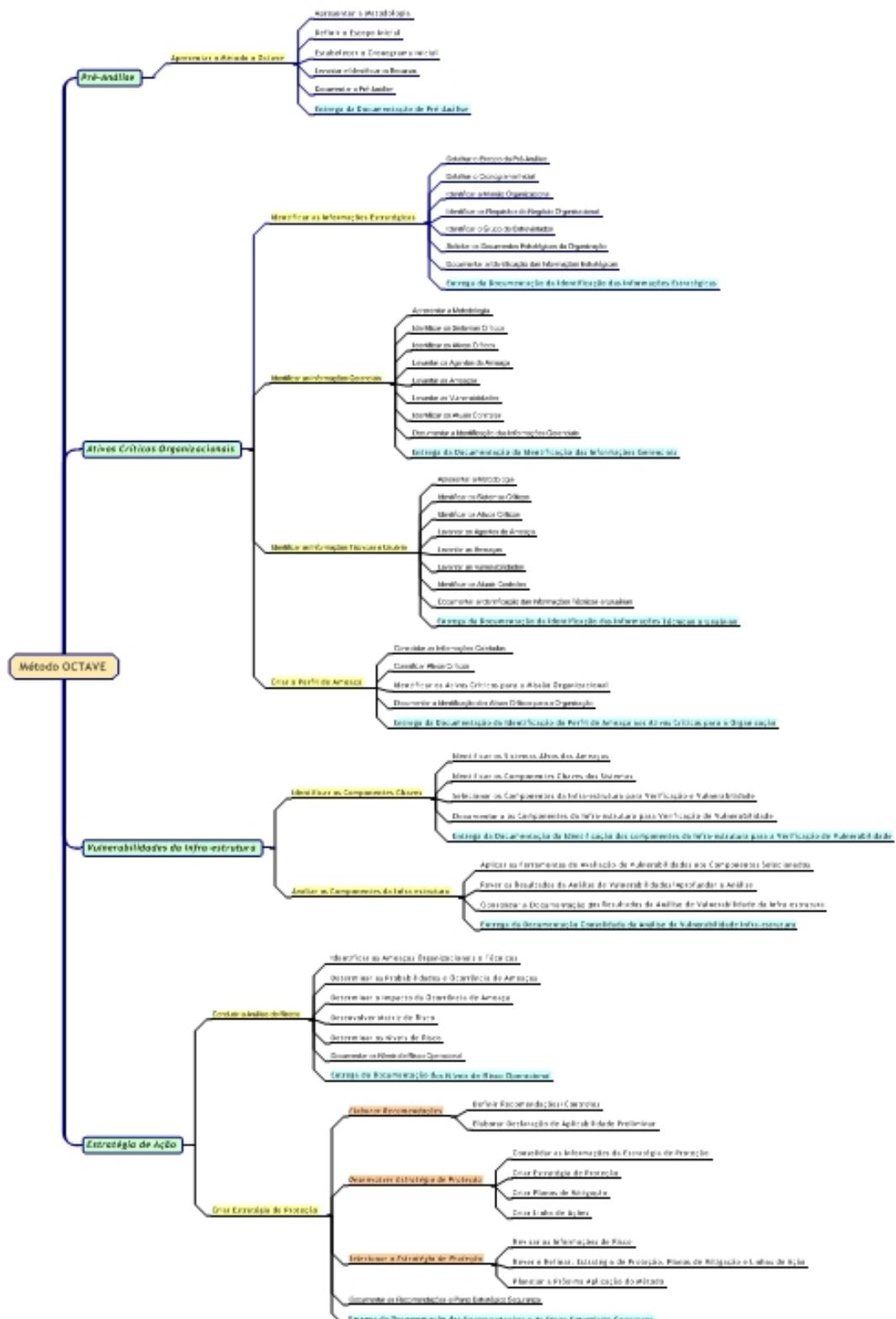


Figura 21 - Formato da EAP Mapa Mental

O dicionário da EAP pode ser preenchido como está apresentado no Apêndice G, ou apenas imprimir as anotações das tarefas constantes no Microsoft Project. Pela especificidade do projeto, em se tratando da aplicação do método OCTAVE, torna-se mais simples e rápido a utilização do Microsoft Project, como mostrado a seguir:

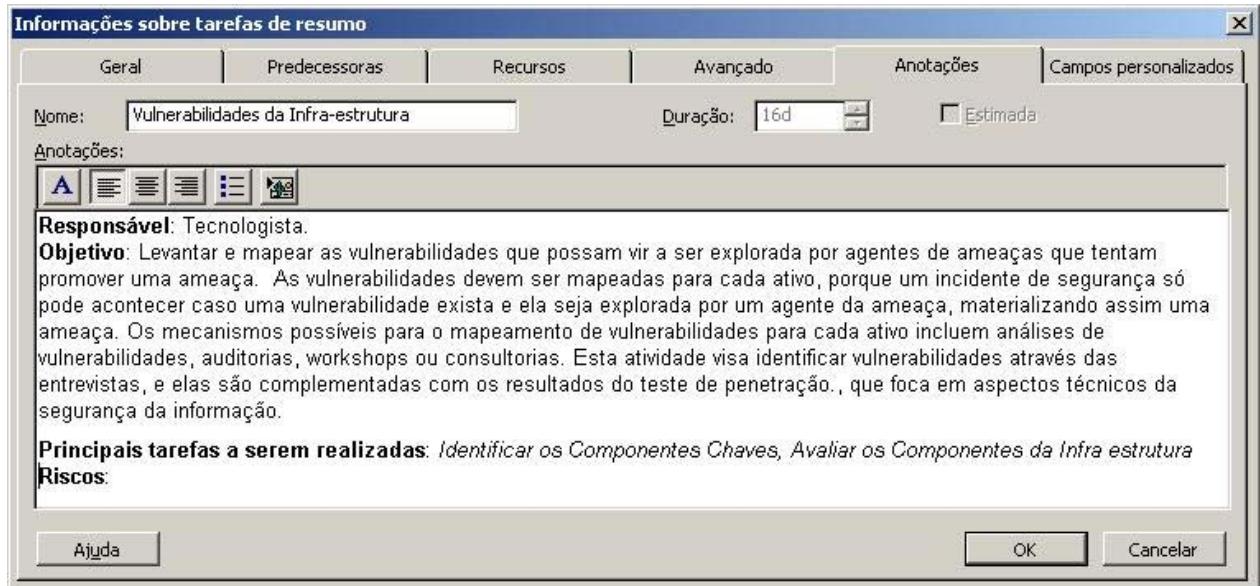


Figura 22 - Dicionário da EAP no Microsoft Project

O *Template* do Plano de Gerenciamento de Escopo é um documento essencial e se encontra no Apêndice H.

4.3. Gerenciamento de Tempo

Na área de gerenciamento de tempo têm-se tradicionalmente os seguintes documentos:



Figura 23 - Documentos da Gerencia de Tempo (adaptado de VARGAS, 2007)

A Lista de Atividades e a Lista de Atividades com Duração são construídas e mantidas no Microsoft Project, de onde podem ser impressas em formato de formulário/relatório. A seguir é apresentado o formato com duração, os valores de duração são meramente ilustrativos:

Id	Nome da tarefa	Duração
1	1 Pré-Análise	1 dia
2	1.1 Apresentar o Método o Octave	1 dia
3	1.1.1 Apresentar a Metodologia	1 dia
4	1.1.2 Definir o Escopo Inicial	1 dia
5	1.1.3 Estabelecer o Cronograma Inicial	1 dia
6	1.1.4 Levantar e Identificar os Recursos	1 dia
7	1.1.5 Documentar a Pré-Análise	1 dia
8	1.1.6 Entrega da Documentação de Pré-Análise	1 dia
9	2 Ativos Críticos Organizacional	4 dias
10	2.1 Identificar as Informações Estratégicas	1 dia
11	2.1.1 Detalhar o Escopo da Pré-Análise	1 dia
12	2.1.2 Detalhar o Cronograma Inicial	1 dia
13	2.1.3 Identificar a Missão Organizacional	1 dia
14	2.1.4 Identificar os Requisitos do Negócio Organizacional	1 dia
15	2.1.5 Identificar o Grupo de Entrevistados	1 dia
16	2.1.6 Solicitar os Documentos Estratégicos da Organização	1 dia
17	2.1.7 Documentar a Identificação das Informações Estratégicas	1 dia
18	2.1.8 Entrega da Documentação da Identificação das Informações Estratégicas	1 dia

Figura 24 - Formato da Lista de Atividades com Duração

A Lista de Recursos do Projeto é construída e mantida no Microsoft Project, de onde pode ser impressa em formato de formulário/relatório. A seguir é apresentado o formato, os valores constantes na figura são meramente ilustrativos:

		Nome do recurso	Tipo	Unidade do Material	Iniciais	Grupo	Unid. máximas	Taxa padrão	Taxa h. extra	Custo/uso	Acumular	Calendário base	Código
1		Gerente	Trabalho	G	Gerente de Projetos	1.700%	R\$ 0,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão		
2		Analista 1	Trabalho	A	Facilitador	1.700%	R\$ 0,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão		
3		Analista 2	Trabalho	A	Documentador	1.700%	R\$ 0,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão		
4		Analista 3	Trabalho	A	Redator	1.700%	R\$ 0,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão		
5		Analista 4	Trabalho	A	Entrevistador	1.700%	R\$ 0,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão		
6		Analista 5	Trabalho	A	Tecnologista	600%	R\$ 0,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão		
7		Analista 6	Trabalho	A	Tecnologista	600%	R\$ 0,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão		
8		Analista 7	Trabalho	A	Tecnologista	600%	R\$ 0,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão		
9		Analista 8	Trabalho	A	Tecnologista	600%	R\$ 0,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão		

Figura 25 - Formato da Lista de Recursos

O documento de Alocação de Recursos é construído e mantido no Microsoft Project, de onde pode ser impresso em formato de formulário/relatório. A seguir é apresentado o formato, os valores constantes na figura são meramente ilustrativos:

	i	Nome da tarefa	Unidades de atribuição	Duração	Trabalho
1		□ 1 Pré-Análise		5 dias	600 hrs
		Gerente	100%		40 hrs
		Analista 1	100%		40 hrs
		Analista 2	100%		40 hrs
		Analista 3	100%		40 hrs
		Analista 4	100%		40 hrs
2		□ 1.1 Apresentar o Método o Octave		5 dias	400 hrs
		Gerente	100%		40 hrs
		Analista 1	100%		40 hrs
		Analista 2	100%		40 hrs
		Analista 3	100%		40 hrs
		Analista 4	100%		40 hrs
3		□ 1.1.1 Apresentar a Metodologia		1 dia	40 hrs
		Gerente	100%		8 hrs
		Analista 1	100%		8 hrs
		Analista 2	100%		8 hrs
		Analista 3	100%		8 hrs
		Analista 4	100%		8 hrs
4		□ 1.1.2 Definir o Escopo Inicial		1 dia	40 hrs
		Gerente	100%		8 hrs
		Analista 1	100%		8 hrs
		Analista 2	100%		8 hrs
		Analista 3	100%		8 hrs
		Analista 4	100%		8 hrs

Figura 26 - Formato da Lista de Recursos

O Gráfico de GANTT é construído e mantido no Microsoft Project, de onde pode ser impresso em formato de formulário/relatório, entretanto, como ele retrata o cronograma do projeto, deve ser aprovado no formato sugerido no Apêndice I.

O Diagrama de Rede é um tradicional documento utilizado para cálculo de folgas e avaliação do caminho crítico, mas em se tratando especificamente do projeto de aplicação de Análise de Risco segundo o método OCTAVE, não há possibilidade de haver paralelismo entre as atividades, pois o resultado de uma fase é necessariamente utilizado nas seguintes, tornando-o seqüencial. Mesmo assim é possível obtê-lo no Microsoft Project, de onde pode ser impresso em formato de formulário/relatório, como é mostrado a seguir:

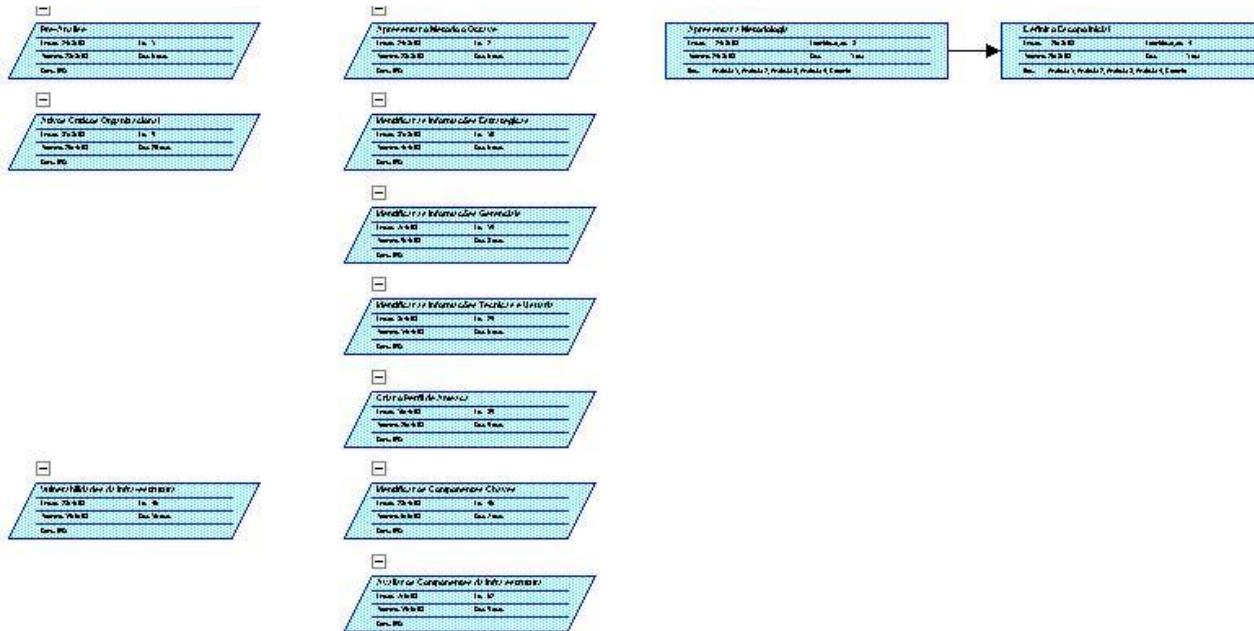


Figura 27 - Formato do Diagrama de Rede

O Gráfico de Marcos é obtido conjuntamente com o Gráfico de Gantt, pois no momento da inserção das atividades, as entregas dos documentos são lançadas com duração zero, e, por conseguinte constituem-se nos marcos, como podemos observar os pontos assinalados na figura a seguir:

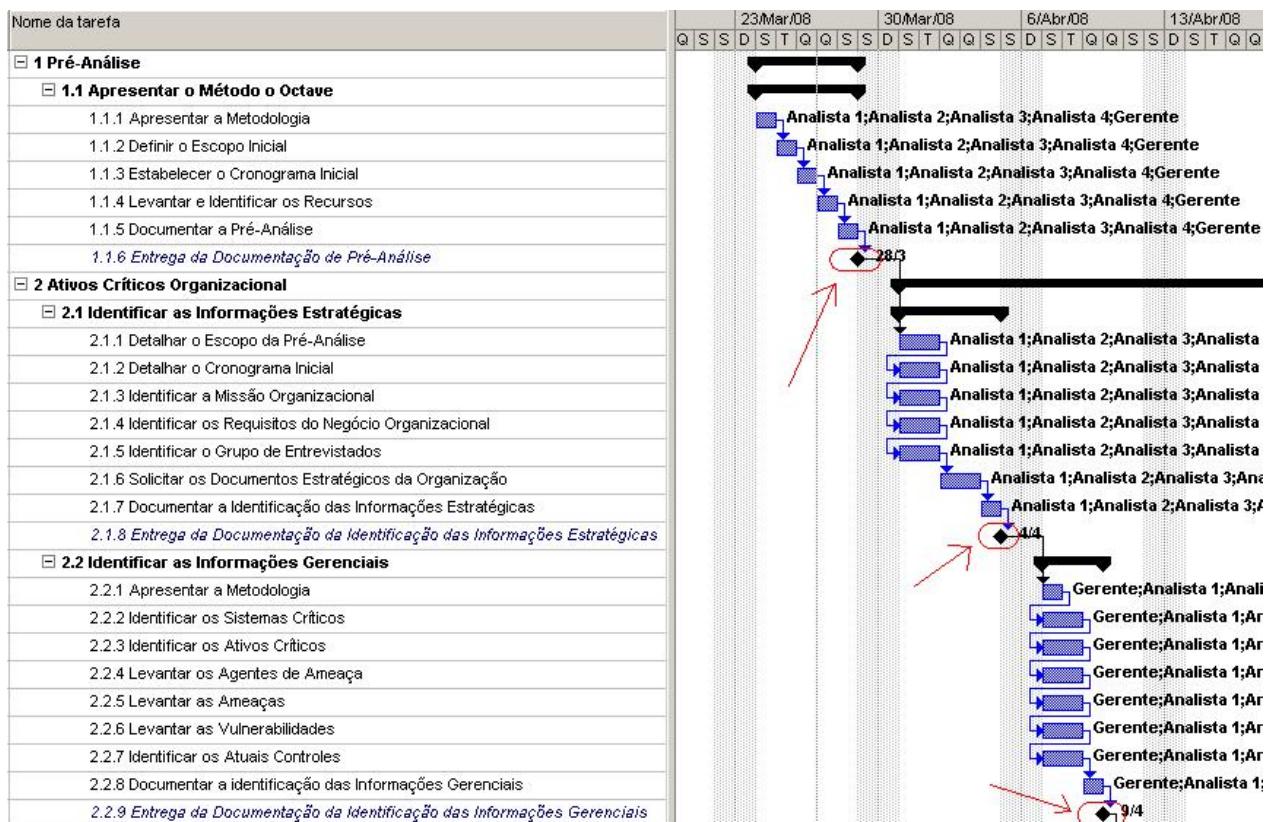


Figura 28 - Formato do Gráfico de Marcos e Gantt em conjunto

O *Template* do Plano de Gerenciamento de Tempo é um documento essencial e se encontra no Apêndice J.

4.4. Gerenciamento de Custos

Nesta proposta de projeto onde as duas organizações envolvidas são instituições governamentais, e os trabalhos realizados são firmados através de Termos de Cooperação ou Convênios, a área de custos não é abordada. Nestes projetos existe apenas a previsão de gastos com passagens e diárias dos funcionários e colaboradores, se for o caso, não impactando na execução do projeto. Neste contexto, não abordaremos esta área de gerenciamento. Para estudos futuros sobre os documentos tradicionalmente utilizados, recomendamos consultar o livro Manual Prático do Plano de Projeto: utilizando o PMBOK Guide, cujo autor é Ricardo Viana Vargas.

4.5. Gerenciamento de Qualidade

Na área de gerenciamento de Qualidade tem-se tradicionalmente apenas o Plano de Gerenciamento da Qualidade. O *Template* do Plano de Gerenciamento de Qualidade se encontra no Apêndice K.



Figura 29 - Documento da Gerencia de Qualidade (adaptado de VARGAS, 2007)

4.6. Gerenciamento de Recursos Humanos

Na área de gerenciamento de Recursos Humanos têm-se tradicionalmente os seguintes documentos:

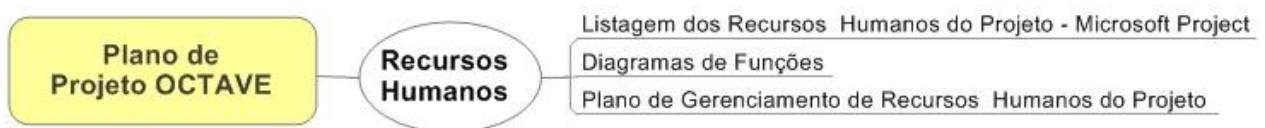


Figura 30 - Documentos da Gerencia de Recursos Humanos (adaptado de VARGAS, 2007)

O documento contendo a Listagem dos Recursos Humanos do Projeto é construída e mantida no Microsoft Project, de onde pode ser impressa em formato de formulário/relatório. A seguir é apresentado o formato:

Nome do recurso	Tipo	Iniciais	Grupo	Unid. máximas	Taxa padrão	Taxa h. extra	Custo/uso	Acumular	Calendário base
Gerente	Trabalho	G	Gerente de Projetos	1.700%	R\$ 10,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão
Analista 1	Trabalho	A	Facilitador	1.700%	R\$ 8,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão
Analista 2	Trabalho	A	Documentador	1.700%	R\$ 8,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão
Analista 3	Trabalho	A	Redator	1.700%	R\$ 8,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão
Analista 4	Trabalho	A	Entrevistador	1.700%	R\$ 8,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão
Analista 5	Trabalho	A	Tecnologista	600%	R\$ 8,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão
Analista 6	Trabalho	A	Tecnologista	600%	R\$ 8,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão
Analista 7	Trabalho	A	Tecnologista	600%	R\$ 8,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão
Analista 8	Trabalho	A	Tecnologista	600%	R\$ 8,00/hr	R\$ 0,00/hr	R\$ 0,00	Rateado	Padrão

Figura 31 - Formato da Listagem de Recursos Humanos

Documento contendo o Diagrama de Funções é obtido no Microsoft Project, podendo ser impressa em formato de formulário/relatório. A seguir é apresentado o formato:



Figura 32 - Formato do Diagrama de Funções

O *template* do Plano de Gerenciamento de Recursos Humanos é bastante simplificado, pois no serviço público existe toda uma dinâmica diferenciada, se encontra no Apêndice L.

4.7. Gerenciamento das Comunicações

Na área de gerenciamento de Comunicações tem-se tradicionalmente apenas o Plano de Gerenciamento das Comunicações. O *template* do Plano de Gerenciamento de das Comunicações é essencial e se encontra no Apêndice M.



Figura 33 - Documento da Gerencia de Comunicações (adaptado de VARGAS, 2007)

4.8. Gerenciamento de Riscos

Na área de gerenciamento de Riscos tem-se tradicionalmente apenas o Plano de Gerenciamento das Comunicações. O *template* do Plano de Gerenciamento de das Comunicações é essencial e se encontra no Apêndice N.

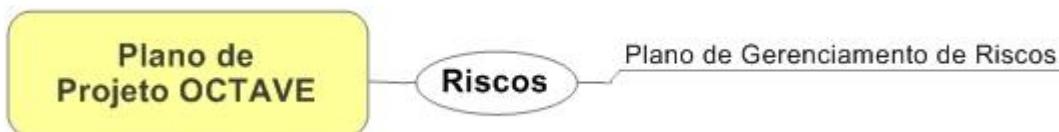


Figura 34 - Documento da Gerencia de Riscos (adaptado de VARGAS, 2007)

As tabelas e estruturas de Risco (identificação qualificação e respostas) foram criadas especificamente voltadas para o Projeto de Aplicação de uma Análise de Risco (BARALDI, 2006). O *template* do Apêndice N se refere ao Projeto de execução/aplicação do método OCTAVE, que também é uma Análise de Risco.

4.9. Gerenciamento de Aquisições

Nesta proposta de projeto onde as duas organizações envolvidas são instituições governamentais, todas as aquisições são feitas de forma centralizada pela instituição e com previsão anual, inclusive os treinamento e participação em eventos, não sendo especificados projetos ou ações coordenadas. Neste contexto, não abordaremos esta área de gerenciamento.

A declaração de Trabalho de Consultoria, que regularia a contratação de consultores, não se aplica ao CEPESC – Centro de Pesquisa e Desenvolvimento de Segurança para as Comunicações, pois o Centro trabalha com bolsistas de Universidades com alocação fixa dentro da instituição, com tarefas e alocações em diversos trabalhos técnicos especializados.

Desta forma, o Plano de Gerenciamento das Aquisições fica esvaziado, no que se refere à proposta desta monografia.

Para estudos futuros sobre os documentos tradicionalmente utilizados, recomendamos consultar o livro Manual Prático do Plano de Projeto: utilizando o PMBOK Guide, cujo autor é Ricardo Viana Vargas.

5. CONCLUSÃO

A abordagem para a gestão de riscos operacionais relativos à missão e aos negócios da Administração Pública Federal - APF no Brasil leva a uma visão totalizante e abrangente, no caso a metodologia *Operational Critical Threat, Asset and Vulnerability Evaluation - OCTAVE* fornece essa abordagem se comparadas às outras que focam tão somente em aspectos tecnológicos. A orientação a processos da metodologia *OCTAVE* tem uma grande afinidade com o estilo e a visão da orientação ao gerenciamento de projetos do *PMBOK*, pois, as áreas de conhecimento, as métricas de avaliação e principalmente na documentação gerada pelas lições aprendidas na implementação do projeto de avaliação de risco são fatores críticos e sucesso para a implementação da metodologia e criação da cultura de gestão da Segurança da Informação e Comunicação.

No desenvolver dessa monografia, observamos que mesmo em se tratando de órgãos governamentais, que possuem várias especificidades em sua atuação, não aderente ao *PMBOK*, é claramente possível utilizar todos os métodos e processos conhecidos e desenvolvidos de PMI. Após a geração dos *Templates*, observou-se que o grau de formalidade documental aumentou substancialmente e, por conseguinte, a distribuição de responsabilidades dentro do projeto. A clara atribuição das responsabilidades aumentou a qualidade e a facilidade de detecção de riscos e problemas na aplicação do Método *OCTAVE*.

Outra consequência imediata é a formação de uma base de conhecimento documental padronizada que servirá de referência em trabalhos futuros, além da análise e melhoria dos processos.

Concluindo, certamente este trabalho trará muitos benefícios à Administração Pública Federal, bem como para seus funcionários.

5.1. Trabalhos futuros

É possível que este trabalho se estenda, estruturando um escritório de Projetos (*Project Management Office – PMO*) (VALERIANO, 2005).

Na visão de Escritório de Projetos, teríamos sim a presença de todas as áreas de gerenciamento, inclusive Aquisições e Custo. Além das áreas de Gerenciamento seriam abordadas mais amplamente outros aspectos, tais como: metodologia de definição dos projetos, estruturação de equipes, licitações, rateio de custo entre projetos, sistema de alocação de recursos governamentais, planejamento institucional, missão da instituição, objetivos institucionais.

6. REFERÊNCIAS BIBLIOGRÁFICAS

- ADAILTO, Silva. OCTAVE - Como Gerenciar Riscos em Segurança da Informação, <[http://www.ies.org.br/files/como-gerenciar riscos em seguranca da informacao](http://www.ies.org.br/files/como-gerenciar_riscos_em_seguranca_da_informacao)>. Acesso em 12 de setembro de 2007.
- ALBERTS, Christopher e DOROFEE, Audrey. *Introduction to the OCTAVE® Approach*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001, <http://www.cert.org/octave/approach_intro.pdf> Acesso em 12 de setemnbro de 2007.
- ALBERTS, Christopher e DOROFEE, Audrey. *Managing Information Security Risks*. Boston, MA: Addison-Wesley, 2002.
- ALBERTS, Christopher e DOROFEE, Audrey. *OCTAVE Criteria v2.0*. (CMU/SEI-2001-TR-020, ADA 396654). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. <http://www.sei.cmu.edu/publications/documents/01.reports/01_tr02_0.html>. Acesso em 12 de setembro de 2007.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799: Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2005.
- BARALDI, Paulo. **Gerenciamento de Riscos Empresariais**. 2ª edição, Rio de Janeiro: Elsevier, 2005.
- BRITISH STANDARD. **BS 7799-3: Guidelines for Information Security Risk Management**, London: BS - UK Government, 2004
- CANONGIA, C.; LAMB, Celina; CARVALHO, Cátia Silene P; SOUZA e SILVA, Valdenis. **Convergência da Inteligência Competitiva com Construção de Visão de Futuro: proposta metodológica de Sistema de Informação Estratégica (SIE)**. DataGramZero: Revista de Ciência da Informação, Rio de Janeiro, v. 2, 2001.
- MALTA, Maria Lucia Levy. **Direito da Tecnologia da Informação**. Campinas: Edicamp, 2002.
- NAKAMURA, Emilio Tissato e LIMA, Marcelo BARBOSA. **Estratégia de Proteção da Infra-Estrutura Crítica da Informação**. Campinas: Novatech 2004.
- NATIONAL INFRASTRUCTURE PROTECTION CENTER USA, **Risk Management: Na Essential Guide to Protecting Critical Assets**, <<http://www.iwar.org.uk/comsec/resources/risk/risk-mgmt.pdf>>. Acesso em 24 de março de 2008.
- POSSI, Marcus. et al. **Gerenciamento de Projetos Guia do Profissional: volume1: abordagem geral e definição de escopo**, Rio de Janeiro: Brasport, 2006a.

POSSI, Marcus. et al. **Gerenciamento de Projetos Guia do Profissional: volume2: aspectos humanos e interpessoais**, Rio de Janeiro: Brasport, 2006b.

POSSI, Marcus. et al. **Gerenciamento de Projetos Guia do Profissional: volume3: fundamentos técnicos**, Rio de Janeiro: Brasport, 2006c.

PROJECT MANAGEMENT INSTITUTE (PMI). **Project Management Body of Knowledge Guia 3ª Edição**, Pensilvânia: PMI, novembro de 2004

RALHA, Célia G. e FERREIRA, Rafael G, **Modelagem de Processos Aplicada na Gestão de um Ambiente Real de TI**. Artigo Técnico, Universidade de Brasília: Departamento de Ciência da Computação, 2007

ROCHA, Silvio Jose Jaeger, **Gerência de Projetos de Software CMM&PMBOK**. <<http://www.pmtech.com.br/artigos/CMM&PMBOK.pdf>>. Acesso em 26 de março de 2008.

Software Engineering Institute- Carnegie Mellon SEI/CMU, **Risk Management Paradigm**, <<http://www.sei.cmu.edu/risk/paradigm.html>>. Acesso em 11 de fevereiro de 2008.

TARAPANOFF, Kira. **Inteligência social e inteligência competitiva**. Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação. Disponível em: <http://www.encontros-bibli.ufsc.br/bibesp/esp_01/2_tarapanoff.pdf>. Acesso em: 20 março de 2008.

VALERIANO, Dalton. **Moderno Gerenciamento de Projetos**. 2ª edição, São Paulo: Pearson Prentice Hall, 2005.

VARGAS, Ricardo Viana. **Gerenciamento de Projetos: estabelecendo diferenciais competitivos**. Rio de Janeiro: Brasport, 2005

VARGAS, Ricardo Viana. **Manual Prático do Plano de Projeto: utilizando o PMBOK Guide**, 3ª edição, Rio de Janeiro: Brasport, 2007.

APÊNDICE - (todos os documentos dessa seção foram adaptados do livro: Manual Prático do Plano de Projeto, Ricardo Vargas, 3ª Edição)

APÊNDICE A - *Template Apresentação*

[Digite o nome do Projeto]		
APRESENTAÇÃO DO PROJETO		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

[Contextualize a organização quanto ao seu ramo de atuação, tamanho e importância]

[Digite o histórico anterior da organização em relação à Análises de Risco/Segurança da Informação]

[Informe se foi executado algum trabalho sobre Segurança da Informação anterior na organização, mesmo que de pesquisa]

[Especifique a área na qual será efetuada a análise de risco e contextualize quanto ao resto da organização]

[Informe a importância do trabalho a ser executado para a organização na qual está sendo aplicada a metodologia]

[Escreva sobre as expectativas do Patrocinador]

APÊNDICE B - *Template* Termo de Abertura do Projeto

[Digite o nome do Projeto]		
TERMO DE ABERTURA DO PROJETO PROJECT CHARTER		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

1. Resumo das condições do projeto

[A partir do texto gerado na Apresentação, escreva sobre o cenário no qual o projeto será executado e o problema a ser atacado]

2. Justificativa do projeto

[Escreva o porquê da necessidade do projeto na organização]

3. Nome do gerente do projeto, suas responsabilidades e sua autoridade

[Nome] é o gerente do projeto e [Cargo] do CEPESC. Sua autoridade é total na esfera executiva do projeto, podendo contactar pessoas, contratar, realizar compras e gerenciar o pessoal de acordo com seus próprios critérios.

No caso de necessidade de relacionamento externo à divisão, sua autoridade é a autoridade funcional inerente ao seu posto dentro do CEPESC.

4. Necessidades básicas do trabalho a ser realizado

- Alocação de Recursos Humanos especializados;
- Sala de trabalho para a equipe de projeto com acesso à internet, linha telefônica, computador com impressora e três mesas de trabalho;

5. Principais partes interessadas

- Patrocinador do projeto (membro do *Staff* gerencial da organização);
- *Staff* gerencial do CEPESC;
- equipe do projeto;
- área de tecnologia da organização.

6. Descrição do projeto

6.1. Produto do projeto

Metodologia aplicada e documentada com aprovação do patrocinador, bem como uma apresentação técnica dos resultados.

6.2. Cronograma básico do projeto

A execução dos trabalhos terá início em [Mês] de [Ano] e deve durar aproximadamente [Duração em meses ou semanas].

6.3. Estimativas iniciais de custo

Como o projeto é fruto de um Termo de Cooperação/Convênio entre organizações do Governo, os custos são avaliados de forma simplificada. Existe apenas a previsão de diárias e passagens para a equipe do projeto, caso seja necessário. Tal necessidade será submetida ao gerente de projeto através de um memorando apenas de caráter informativo.

7. Premissas iniciais

- A equipe está motivada para o trabalho no projeto.
- Todas as comunicações serão controladas.
- Todas as ferramentas de *hardware* e *software* estão disponíveis.
- Membros do time terão disponibilidade.
- Não há restrição de custo

8. Restrições iniciais

- O prazo é limitado.
- A agenda dos executivos da empresa limita a disponibilidade de datas para as entrevistas necessárias.

9. Administração

9.1. Necessidade inicial de recursos

O gerente terá uma equipe de [Nº] profissionais. Não se necessita de aquisição de material adicional.

9.2. Necessidade de suporte pela organização

A organização irá atender a todas as necessidades para execução do projeto em suas instalações.

9.3. Comitê Executivo ou Comitê de Controle de Projeto (CCP – *Change Control Project*)

Será criado um comitê executivo, composto pelo patrocinador, pelo gerente de projetos e pelo membro do time responsável pela área de escopo do projeto, totalizando três participantes. Esse comitê será o responsável pela análise e aprovação das mudanças, mediante fluxo de controle de mudanças a ser definido no projeto. O processo de decisão do comitê será baseado em consenso, tendo o patrocinador a prerrogativa de vetar e aprovar decisões caso o consenso não seja obtido.

9.4. Controle e gerenciamento das informações do projeto

O gerente de projeto é o responsável pelas informações. Todas as informações devem ser armazenadas em meio digital.

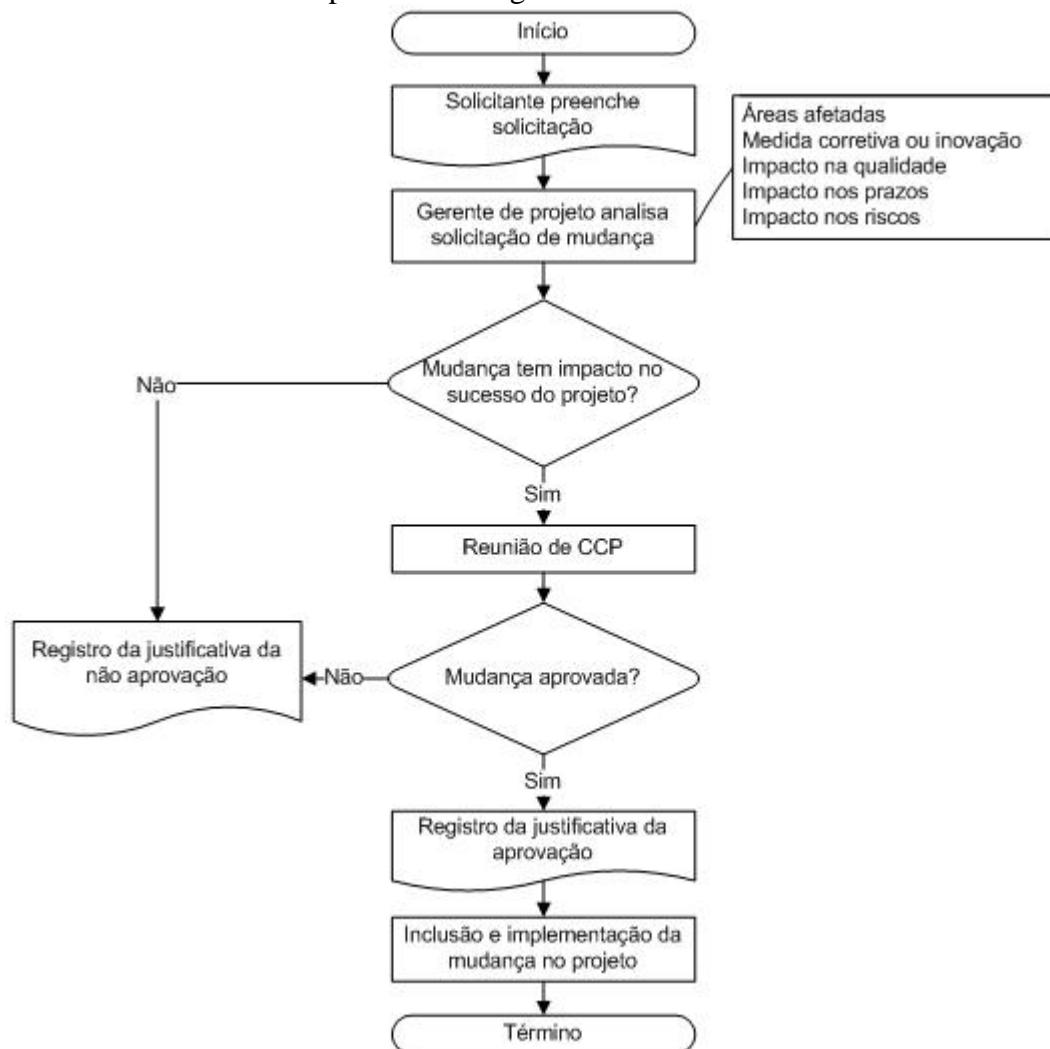
APROVAÇÕES		
[Nome]	[Assinatura]	[Data]
[Cargo]		

APÊNDICE C - *Template* Sistema de Controle Integrado de Mudanças

[Digite o nome do Projeto]		
SISTEMA DE CONTROLE INTEGRADO DE MUDANÇAS INTEGRATED CHANGE CONTROL SYSTEM		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

1. Controle integrado de mudanças

O controle integrado de mudanças a ser utilizado pelo comitê executivo ou CCP, será realizado conforme o fluxo de processos a seguir.



APROVAÇÕES

[Nome] [Cargo]	[Assinatura]	[Data]
-------------------	--------------	--------

APÊNDICE D - *Template* Registro de Lições Aprendidas no Projeto

[Digite o nome do Projeto]

REGISTRO DE LIÇÕES APRENDIDAS NO PROJETO - MODELO PROJECT LESSONS LEARNED LOG

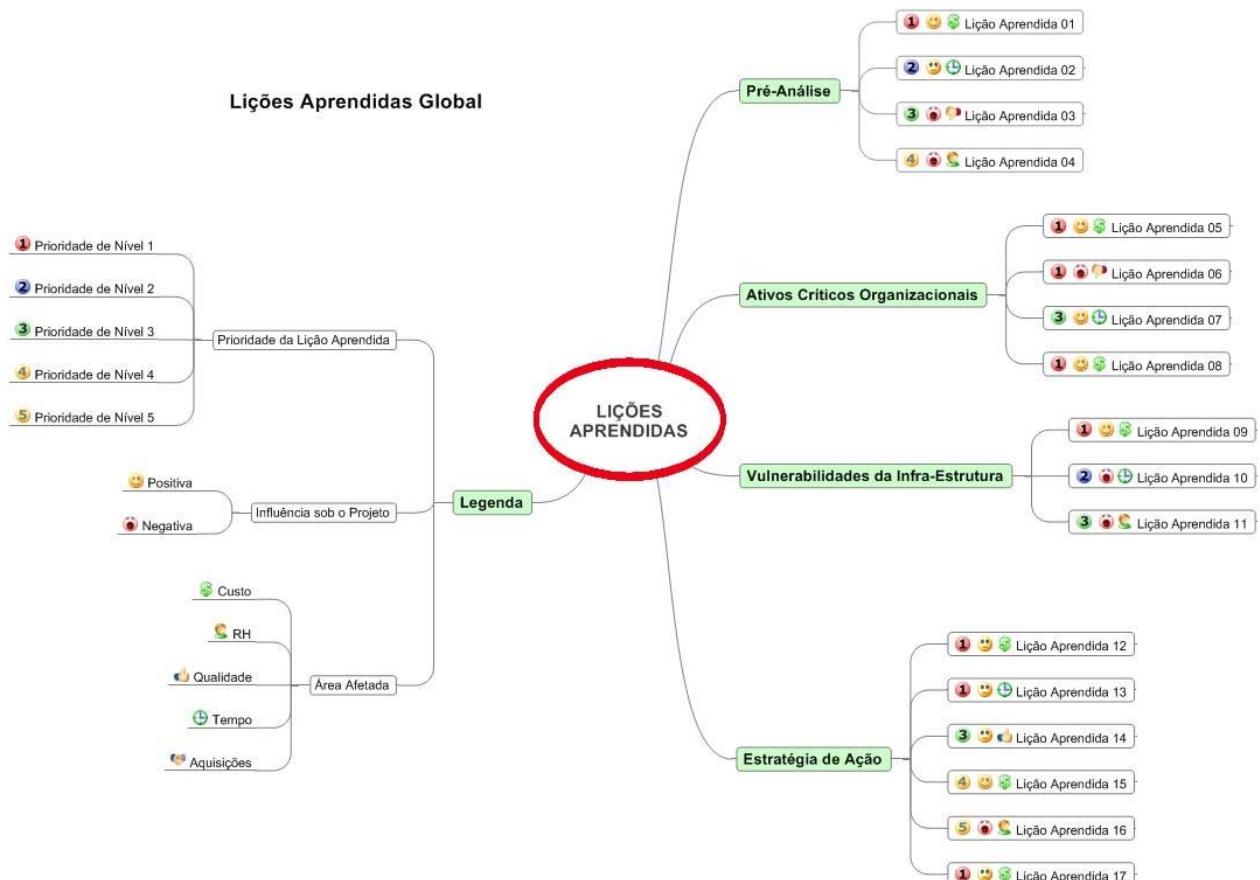
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

1. Registro de lições aprendidas

As lições aprendidas do projeto serão registradas durante todo o ciclo de vida do projeto. As reuniões semanais de CCP irá compilar os registros da semana e o registro será anexado a ata de reunião do projeto.

As lições aprendidas serão classificadas de acordo com a prioridade (1 a 5), com a influência sobre o projeto (Negativa ou Positiva) e área afetada (áreas de conhecimento do PMI), conforme modelos apresentados nos itens a seguir.

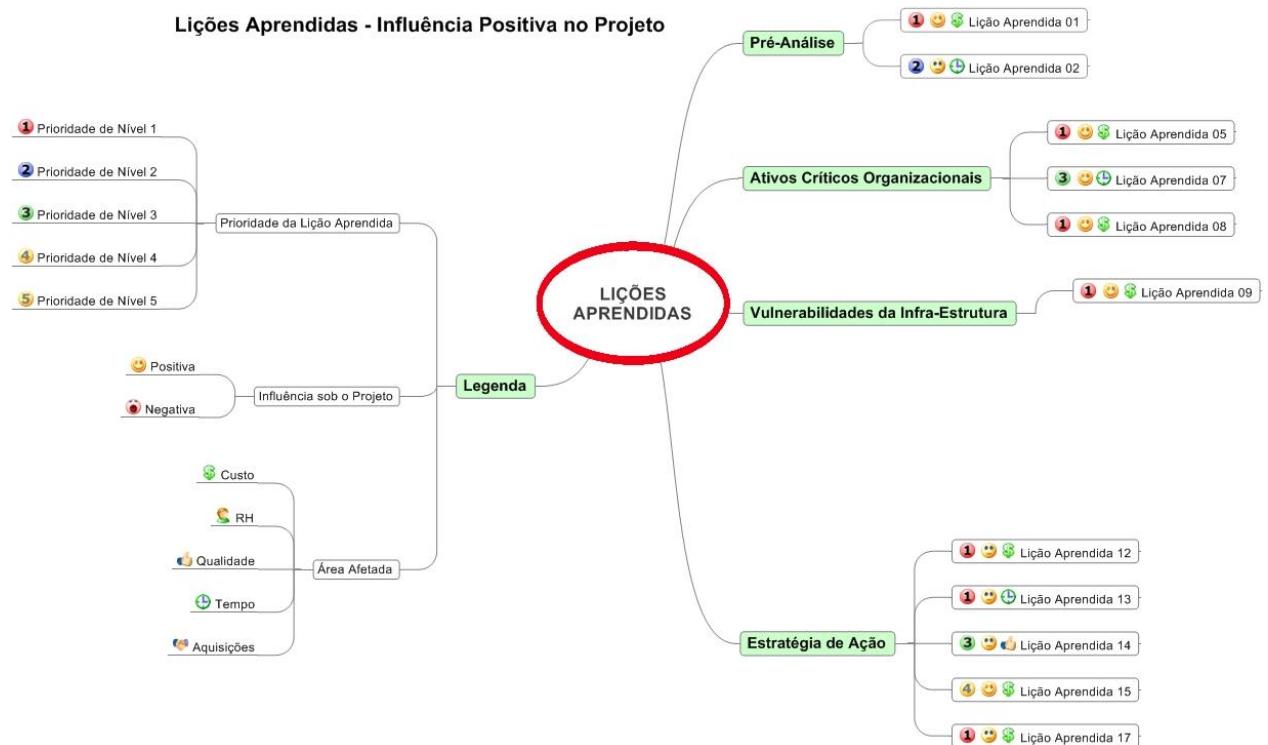
2. Lições aprendidas - Global



3. Lições aprendidas – Influência negativa no projeto



4. Lições aprendidas – Influência positiva no projeto



APROVAÇÕES DO MODELO		
[Nome] [Cargo]	[Assinatura]	[Data]

APÊNDICE E - *Template da Declaração de Escopo*

[Digite o nome do Projeto]		
DECLARAÇÃO DE ESCOPO SCOPE STATEMENT		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

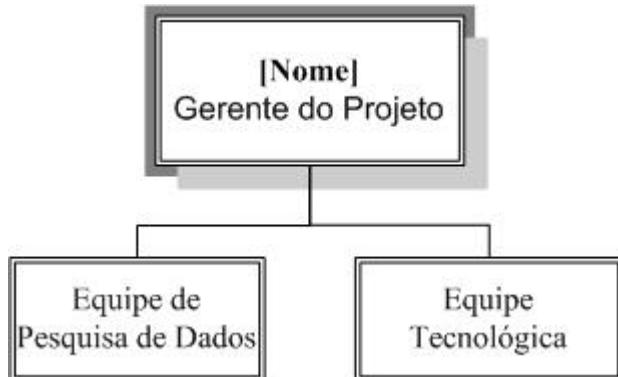
1. Patrocinador

[Nome] – [Cargo na Empresa]

2. Nome do gerente do projeto, suas responsabilidades e sua autoridade

[Nome] é o gerente do projeto e [Cargo] no CEPESC. Sua autoridade é total na esfera executiva do projeto, podendo contactar pessoas e gerenciar o pessoal de acordo com seus próprios critérios.

3. Organograma preliminar



4. Time do projeto

Nome	Função no Projeto
[Nome]	[Função]
[Nome]	[Função]

5. Comitê executivo ou Comitê de Controle do Projeto

O Comitê executivo será formado por:

Nome	Função no Projeto
[Nome]	[Função]
[Nome]	[Função]
[Nome]	[Função]

Esse comitê será o responsável pela análise e aprovação das mudanças, mediante fluxo de controle de mudanças a ser definido no projeto.

6. Descrição do projeto

O projeto envolverá a implantação da Metodologia de Análise de Risco no ambiente da organização, entrega da documentação gerada e apresentação técnica dos resultados e contramedidas.

7. Objetivo do projeto

Implementar a Metodologia de Análise de Risco na **[Nome da organização ou setor]** através de da Equipe Análise de Risco do CEPESC, dentro das metodologias estabelecidas pelo CEPESC, dentro de um prazo máximo de **[Nº]** dias corridos a partir de **[Mês]** de **[Ano]**.

8. Justificativa do projeto

[Escreva o porquê da necessidade do projeto na organização - Tomar como base o Termo de Abertura do Projeto]

9. Produto do projeto

Metodologia implementada e documentada com aprovação do patrocinador, bem como uma apresentação técnica dos resultados.

10. Expectativa do cliente

- Projeto em conformidade com o Termo de Abertura
- Projeto dentro do prazo

11. Fatores de sucesso do projeto

- Comunicação efetiva dentro do time
- Apoio da organização às atividades da Equipe de Projeto
- Disponibilidade de pessoal

12. Restrições

- O prazo é limitado.
- O projeto deve ser mantido em sigilo dentro da esfera dos membros do projeto.

13. Premissas

- As pessoas podem mudar seu comportamento se adequadamente estimuladas e preparadas.
- A comunicação dentro do time será feita através de e-mails.
- É necessário o apoio irrestrito de todos os envolvidos dentro da organização.
- Os membros do time terão dedicação integral ao projeto.
- O time do projeto deverá ter conhecimento de gerenciamento de projetos e de Análise de Riscos.

14. Limites do Projeto e exclusões específicas

- O projeto não tem como objetivo implementar qualquer solução tecnológica.

15. Estrutura Analítica do Projeto (Base)



16. Principais atividades e estratégias do projeto

16.1. Geral

- O objeto dos serviços da implementação da Metodologia de Análise de Risco OCTAVE visa a análise dos ativos críticos da infra-estrutura da organização solicitante, baseando-se nas necessidades de segurança da informação e comunicação;
- A Metodologia OCTAVE produzirá um relatório da situação atual das ameaças e das vulnerabilidades que afligem os sistemas de informação da organização e também, produzirá um conjunto de recomendações e sugestões para a pronta aplicação;
- O padrão adotado para o Gerenciamento de Projeto será o do PMI através do PMBOK Guide® 3rd Edition;
- A solução proposta contará com todo o trabalho necessário para o desenvolvimento da aplicação da metodologia OCTAVE e do uso de ferramentas técnicas desenvolvidas para a utilização na fase de prospecção de vulnerabilidades de TIC;
- Os principais processos são os seguintes: análise de documentos fornecidos pelas áreas e ambientes sensíveis da organização, avaliação das entrevistas, análise de formulários e de questionários.

16.2. Pré-Análise

- Será realizada pela pré-análise o estudo e a preparação com a finalidade de identificar a equipe de análise e os colaboradores externos;
- Deve realizar-se a ambientação da Direção solicitante na Metodologia OCTAVE;
- A escolha dos integrantes da equipe de análise deve ser feita de acordo com o perfil que inclui características que melhor atendem as necessidades de conhecimento, habilidades e competência, conforme acordado anteriormente com a organização;
- Será realizada a capacitação e qualificação da equipe de análise em toda a Metodologia OCTAVE buscando nivlar e igualar o conhecimento das técnicas e procedimentos;

- Está previsto o treinamento em software de gerenciamento de projetos, o MS-Project, para a equipe de análise e colaboradores;
- Deve ser definido o escopo inicial da análise de risco;
- Deve ser estabelecido o cronograma inicial para a análise de risco;

16.3. Ativos Críticos Organizacionais

- Será realizada a identificação dos negócios do órgão bem como da estrutura organizacional e onde será realizada a análise de risco;
- Serão identificados todos os envolvidos no processo de análise de risco;
- Todo o levantamento da análise de risco será realizado pela equipe de análise com acompanhamento da organização;
- Deve ser definido detalhadamente o escopo da análise de risco;
- Deve ser identificada a missão do órgão ou do setor estabelecido no escopo da análise de risco.
- Devem ser identificado, junto ao solicitante, os requisitos do negócio da organização;
- Devem conhecer-se as necessidades do órgão ou setor para o cumprimento da missão e a razão da existência do órgão dentro de sua estrutura organizacional;
- Devem ser solicitado todos os documentos que permitam à equipe de análise conhecer, compreender e analisar os processos nas quais a segurança da informação impacta na missão da organização;
- Deve-se estabelecer o cronograma detalhado com a participação da equipe de análise e a da organização;
- Será definido o perfil de risco dos ativos por meio da classificação dos níveis de risco a que estão submetidos os ativos;
- O nível de risco considera: a vulnerabilidade do ativo, a ameaça e sua probabilidade de ocorrência e impacto resultante na organização.

16.4. Vulnerabilidades da Infra-estrutura

- Será realizado um teste de intrusão para a realização de uma prospecção tecnológica das vulnerabilidades dos ativos críticos da organização, baseado na utilização de ferramentas de avaliação de vulnerabilidades dos componentes de uma infra-estrutura de TIC;
- O acordo para o teste de intrusão está fundamentado nos ativos críticos da TI da organização, assim considerados tanto pelos responsáveis pela área de TI quanto pelos requisitos de negócio definidos pela alta direção;
- O processo de intrusão deve ser operacionalizado de tal forma que satisfaça a todas as condições de execução em situação controlada e confinada ao ambiente TI da Organização;
- Os resultados da primeira fase serão sumarizados e focalizados para cada ativo crítico;

- A sumarização da primeira parte é o insumo para a segunda fase do processo de teste de intrusão, que fará o detalhamento e a avaliação das vulnerabilidades dos ativos críticos na abrangência da plataforma tecnológica de TI, formulada em termos de ações corretivas necessárias para o direcionamento das providências e ações: imediatas, medias, ou de longo prazo;
- A classificação das informações dos resultados de prospecção das vulnerabilidades são Confidenciais, em conformidade com o DL 4335;
- Deve ser acordado com a organização um plano de recuperação, bem como outros procedimentos de avaliação para as perturbações acarretadas quando da operação do teste de intrusão;

16.5. Estratégia de Ação

- Será elaborado um conjunto de recomendações de acordo com a análise de riscos realizada, considerando o níveis de riscos analisados;
- Os riscos serão classificados em: aceitos aqueles que não serão tratados, os mitigados com a implementação dos controles elencados em recomendações e os riscos que podem ser transferidos;
- A decisão do tratamento do risco só pode ser feita analisando-se as recomendações correspondentes para cada risco;
- Deve existir uma avaliação entre o valor da implementação da recomendação e o impacto correspondente;
- O plano de ação deve ser definido para as recomendações geradas levando em consideração o senso de urgência de implementação dos recursos disponíveis.
- O plano de ação será dividido conforme o prazo de implementação, distribuído em curto prazo, médio prazo e longo prazo.
- A estratégia de segurança adotada pelo órgão deve refinar o plano de ação de segurança da informação nos seguintes tópicos: implementação de controles, alterações em controles já existentes, mudanças em processos de negócio, criação de novos processos, definição de políticas-normas-procedimentos, implementação de políticas-normas-procedimentos e treinamento.

17. Orçamento do projeto

Após a aprovação do Plano de Projeto, é feito um memorando informativo ao gerente de projeto informando a previsão de diárias e passagens, se for necessário o deslocamento da equipe do CEPESC.

18. Plano de entregas e marcos do projeto

A execução dos trabalhos terá início em [Mês] de [Ano] e deve durar aproximadamente [Nº] meses. O planejamento do projeto deverá ser realizadas fora do período descrito.

Entrega	Descrição	Término
Fase de Iniciação	Gerente do Projeto Definido	[Data]
	<i>Project Charter</i> Aprovado	[Data]
Fase de Planejamento	<i>Scope Statement</i> Aprovado	[Data]

	Cronograma definido	[Data]
	Orçamento definido	[Data]
	Plano do Projeto Concluído	[Data]
	Aprovação do Plano do Projeto	[Data]
Fase de Execução	Documentação de Pré-Análise concluída	[Data]
	Documentação da Identificação das Informações Estratégicas concluída	[Data]
	Documentação da Identificação das Informações Gerenciais concluída	[Data]
	Documentação da Identificação das Informações Técnicas e Usuárias concluída	[Data]
	Documentação da Identificação do Perfil de Ameaça aos Ativos Críticos para a Organização concluída	[Data]
	Documentação da Identificação dos componentes da Infra-estrutura para a Verificação de Vulnerabilidade concluída	[Data]
	Documentação Consolidada da Análise da Vulnerabilidade Infra-estrutura concluída	[Data]
	Documentação os Níveis de Risco Operacional concluída	[Data]
	Documentação das Recomendações e do Plano Estratégico Segurança concluída	[Data]
	Apresentação dos resultados executado	[Data]
	Relatório Final concluído	[Data]
Fase de Finalização	Projeto concluído	[Data]
	Lições aprendidas registradas	[Data]

19. Riscos iniciais do projeto

- Falta de disponibilidade dos entrevistados.
- Falta de disponibilidade dos membros da equipe do projeto.
- Atraso na avaliação tecnológica.
- Falta de conhecimento da equipe em implantação de escritórios de projetos.

20. Requisitos de gerenciamento de configuração e mudanças do projeto

Será definido um sistema de controle de mudanças com procedimentos estruturados de avaliação e aprovação de modo a facilitar e acompanhar todo o processo de solicitação de mudanças do projeto.

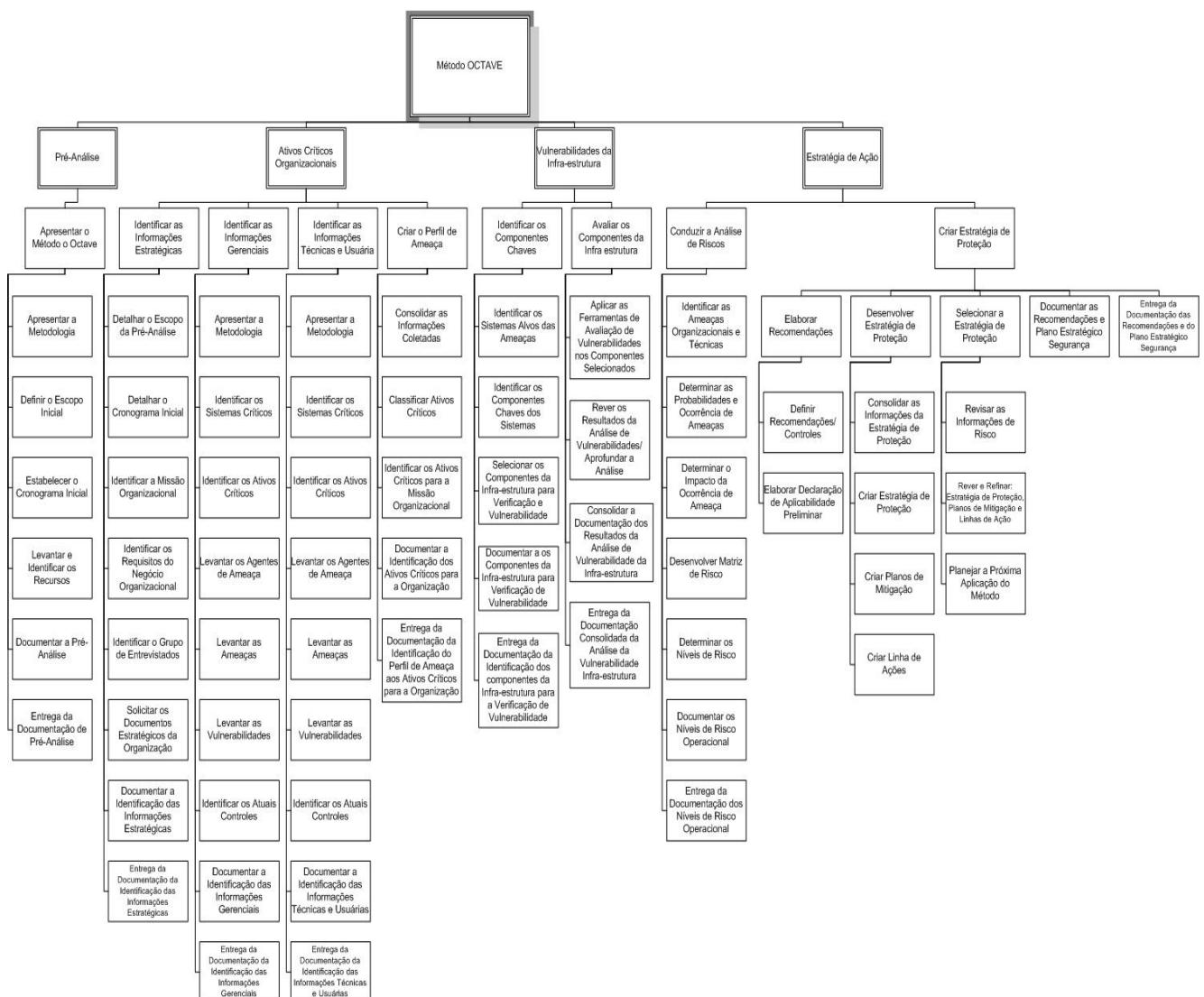
REGISTRO DE ALTERAÇÕES		
Data	Modificado por	Descrição da mudança
[Data]	[Responsável]	[Descrição da mudança].

APROVAÇÕES		
[Nome] [Cargo]	[Assinatura]	[Data]

APÊNDICE F - EAP

[Digite o nome do Projeto]		
ESTRUTURA ANALÍTICA DO PROJETO – ANALÍTICA WORK BREAKDOWN STRUCTURE		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

A EAP reflete a aplicação do método OCTAVE.



APROVAÇÕES		
[Nome] [Cargo]	[Assinatura]	[Data]

APÊNDICE G - *Template do Dicionário da EAP*

[Digite o nome do Projeto]		
DICIONÁRIO DA EAP		
Pacote: [Digite o código da EAP e o nome do pacote]		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

1. Informações básicas

Código EAP	[Código numérico da EAP]
Responsável	[Digite o nome do responsável pelo pacote de trabalho]
Prazo estimado	[Digite o prazo estimado do pacote]
Custo estimado	[Digite o custo estimado do pacote]

2. Principais tarefas a serem realizadas

- **[Digite aqui as tarefas do pacote]**
- **[Digite aqui as tarefas do pacote]**

3. Recursos Humanos previstos

- **[Digite aqui os recursos humanos a serem alocados nas tarefas do pacote]**
- **[Digite aqui os recursos humanos a serem alocados nas tarefas do pacote]**

4. Predecessores principais do pacote de trabalho

- **[Digite aqui os pacotes predecessores]**
- **[Digite aqui os pacotes predecessores]**

5. Sucessoras principais do pacote de trabalho

- **[Digite aqui os pacotes sucessores]**
- **[Digite aqui os pacotes sucessores]**

6. Riscos associados ao pacote

- **[Digite aqui os riscos envolvidos no pacote]**
- **[Digite aqui os riscos envolvidos no pacote]**

REGISTRO DE ALTERAÇÕES		
Data	Modificado por	Descrição da mudança
[Data]	[Responsável]	[Descrição da mudança].

APROVAÇÕES		
[Nome] [Cargo]	[Assinatura]	[Data]

APÊNDICE H - *Template do Plano de Gerenciamento do Escopo*

[Digite o nome do Projeto]		
PLANO DE GERENCIAMENTO DE ESCOPO		
SCOPE MANAGEMENT PLAN		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

1. Descrição dos processos de gerenciamento de escopo

- O gerenciamento do escopo do projeto será realizado com base em documentos específicos: Declaração de escopo para o escopo funcional do projeto e EAP para o escopo das atividades a serem realizadas pelo projeto, com devidas entregas.
- Todas as mudanças no escopo inicialmente previsto para o projeto devem ser avaliadas e classificadas dentro do sistema de controle de mudanças de escopo (*Scope Change Control System*).
- Serão consideradas mudanças de escopo apenas as medidas corretivas. Inovações e novas características do produto/projeto não serão consideradas gerenciamento de escopo.
- Todas as solicitações de mudança no escopo devem ser feitas por escrito através de e-mail, conforme descrito no plano de comunicações do projeto.

2. Priorização das mudanças de escopo e respostas

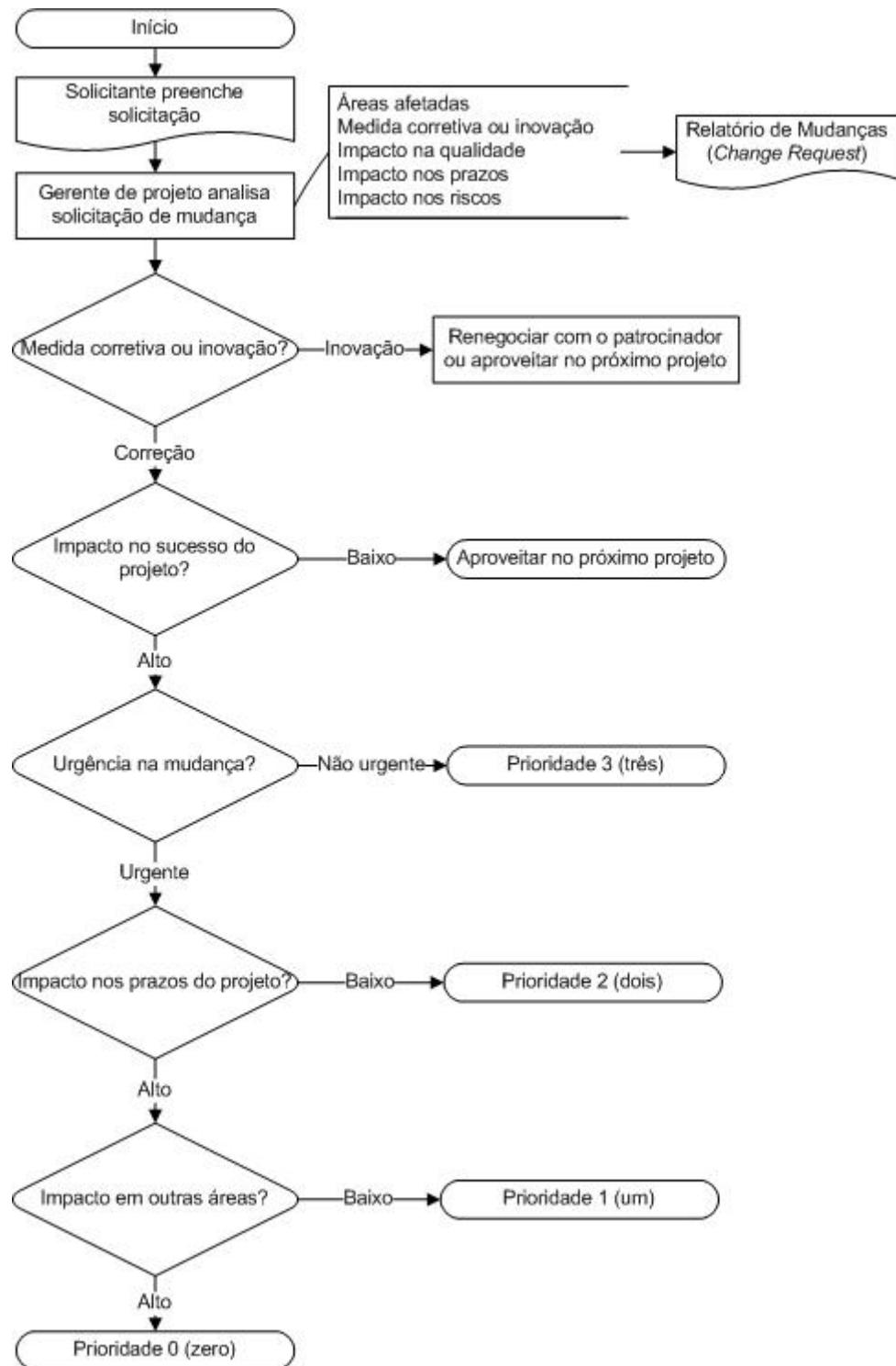
As mudanças de escopo são classificadas em quatro níveis de prioridades

- Prioridade 0 (zero) – Mudanças de prioridade zero requerem uma ação imediata por parte do gerente do projeto, que deve acionar imediatamente o patrocinador, uma vez que se trata de mudança urgente, de alto impacto no projeto e em outras áreas sobre as quais o gerente de projeto não tem autonomia.
- Prioridade 1 (um) - Mudanças de prioridade um requerem uma ação imediata por parte do gerente do projeto, independente das reuniões de controle previstas devido à urgência, acionando imediatamente o patrocinador no caso de necessidade de autorizações para alteração do Plano de Projeto fora da alcada do gerente de projetos.
- Prioridade 2 (dois) – Mudanças de prioridade dois requerem um planejamento da ação através de terceiros ou de equipes que, a princípio, tenham disponibilidade, uma vez que agregam valor ao sucesso do projeto e são urgentes, porém não têm impacto significativo nos prazos do projeto.
- Prioridade 3 (três) – Mudanças de prioridade três podem ser implementadas por terem influência no sucesso do projeto, porém não requerem uma ação imediata por não serem impactantes ou urgentes.

3. Gerenciamento das configurações (*Configuration management*)

O sistema de controle de mudanças de escopo (*Scope Change Control System*) deve proporcionar com que todas as mudanças no escopo do projeto sejam tratadas segundo o fluxo apresentado a seguir com seus resultados apresentados na reunião semanal do Comitê de Controle do Projeto com suas conclusões, prioridades e ações relacionadas. O processo de

gerenciamento das configurações está relacionado diretamente com o sistema de controle de mudanças do projeto.



4. Freqüência de avaliação do escopo do projeto

O escopo do projeto deve ser avaliado semanalmente dentro da reunião do Comitê de Controle do Projeto, prevista no plano de gerenciamento das comunicações.

5. Alocação financeira das mudanças de escopo

Todas mudanças de escopo que requererem gasto adicional deverão ser aprovadas pelo gerente do projeto.

6. Administração do plano de gerenciamento de escopo

6.1. Responsável pelo plano

- [Nome], membro do time do projeto, será o responsável direto pelo plano de gerenciamento de escopo.
- [Nome], membro do time do projeto, será suplente do responsável direto pelo plano de gerenciamento de escopo.

6.2. Freqüência de atualização do plano de gerenciamento de escopo

O plano de gerenciamento de escopo será reavaliado mensalmente na primeira reunião mensal do CCP, juntamente com os outros planos de gerenciamento do projeto.

As necessidades de atualização do plano antes da primeira reunião do Comitê de Controle do Projeto do projeto deverão ser tratadas segundo os procedimentos descritos no item 7, Outros assuntos não previstos neste plano.

7. Outros assuntos relacionados ao gerenciamento do escopo do projeto não previstos neste plano

Todas as solicitações não previstas neste plano deverão ser submetidas a reunião do Grupo de Controle do Projeto para aprovação. Imediatamente após sua aprovação, deverão ser atualizados o plano de gerenciamento de escopo com o devido registro das alterações efetivadas.

REGISTRO DE ALTERAÇÕES		
Data	Modificado por	Descrição da mudança
[Data]	[Responsável]	[Descrição da mudança].

APROVAÇÕES		
[Nome] [Cargo]	[Assinatura]	[Data]

APÊNDICE I - Gráfico de Gantt do Projeto

[Digite o nome do Projeto]		
GRÁFICO DE GANTT DO PROJETO		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]



REGISTRO DE ALTERAÇÕES		
Data	Modificado por	Descrição da mudança
[Data]	[Responsável]	[Descrição da mudança].

APROVAÇÕES		
[Nome] [Cargo]	[Assinatura]	[Data]

APÊNDICE J - *Template do Plano de Gerenciamento do Tempo*

[Digite o nome do Projeto]		
PLANO DE GERENCIAMENTO DO TEMPO SCHEDULE MANAGEMENT PLAN		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

1. Descrição dos processos de gerenciamento de tempo

- O gerenciamento de tempo será realizado a partir da alocação de percentual completo nas atividades do projeto através da utilização do Microsoft Office Project.
- A atualização dos prazos do projeto será realizada no Microsoft Project através da circulação dos seguintes relatórios:
 - Gráfico de Gantt e Diagrama de marcos;
 - Percentual completo;
- Todas as mudanças no prazo inicialmente previsto para o projeto devem ser avaliadas e classificadas dentro do sistema de controle de mudanças de tempo.
- Serão considerados atrasos os decorrentes de medidas corretivas, que, se influenciadoras do sucesso do projeto, deverão ser integradas ao plano. Inovações e novos recursos não serão abordados pelo gerenciamento de tempo e serão passíveis de negociação de prazos ou serão ignorados.
- A atualização da linha de base do projeto somente será permitida com autorização expressa do gerente de projeto e do patrocinador, sendo a linha de base anterior arquivada, documentada e publicada para fins de lições aprendidas.
- Todas as solicitações de mudança nos prazos previamente definidos deverão ser feitas por escrito ou através de e-mail, conforme descrito no plano de comunicações do projeto.

2. Priorização das mudanças nos prazos

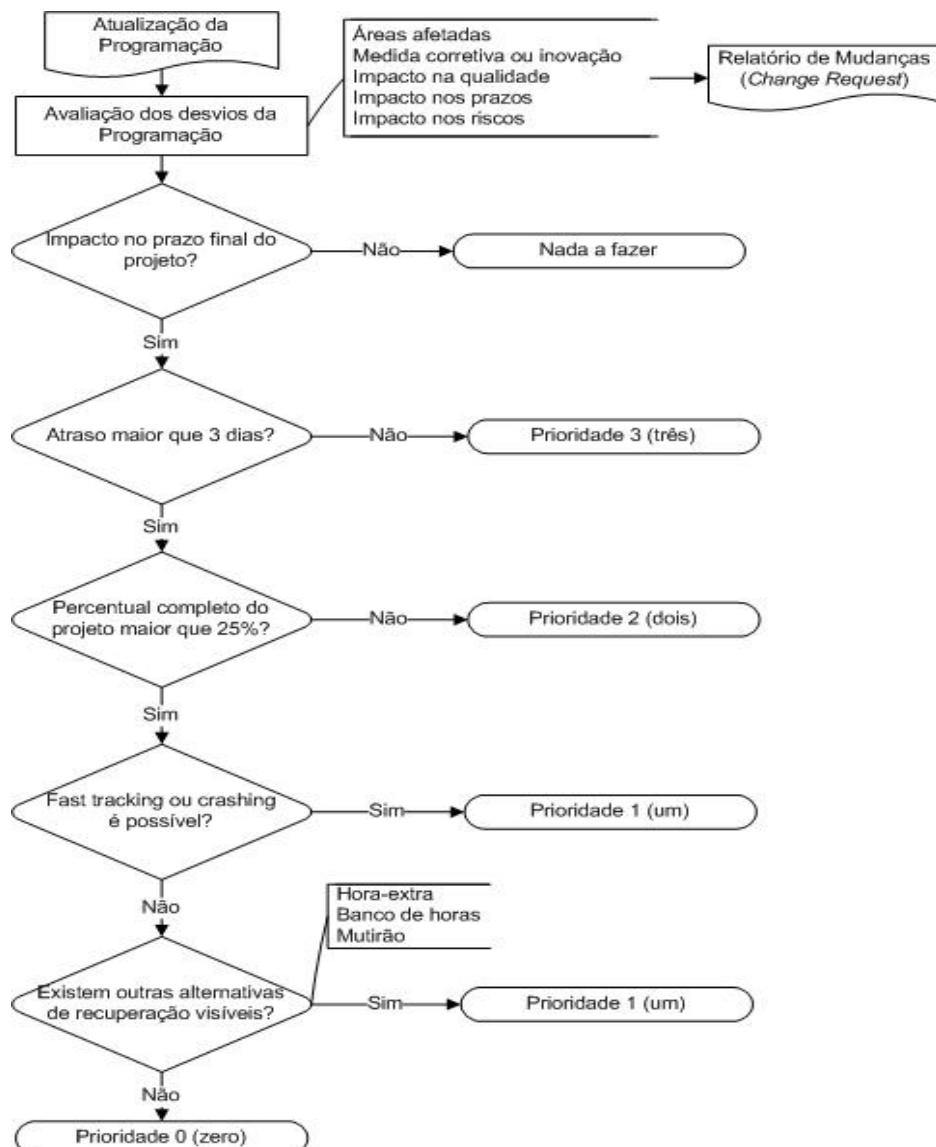
As mudanças nos prazos são classificadas em quatro níveis de prioridade:

- Prioridade 0 (zero) – Atrasos de prioridade zero requerem uma ação imediata por parte do gerente do projeto, que deve acionar imediatamente o patrocinador para discussão e análise, uma vez que é um problema urgente, de alto impacto no projeto e com soluções inicialmente não identificadas.
- Prioridade 1 (um) - Atrasos de prioridade um requerem uma ação imediata por parte do gerente do projeto, independente das reuniões de controle previstas devido à urgência, acionando as medidas de recuperação de prazos disponíveis, tais como o *Fast Tracking*, o *Crashing*, o trabalho em horas-extras, banco de horas e mutirão.
- Prioridade 2 (dois) – Atrasos de prioridade dois requerem um replanejamento das atividades futuras, uma vez que o projeto ainda não completou 25% de conclusão.

- Prioridade 3 (três) – Atrasos de prioridade três são atrasos pequenos se comparados com a duração do projeto e podem ser remanejados sem necessariamente ser preciso replanejar ou acionar algum tipo de mecanismo de recuperação.

3. Sistema de controle de mudanças de prazos (*Schedule Change Control System*)

Todas as mudanças nos prazos e atrasos/adiantamentos do projeto devem ser tratados segundo o fluxo a seguir, com suas conclusões, prioridades e ações relacionadas apresentadas na reunião semanal de CCP.

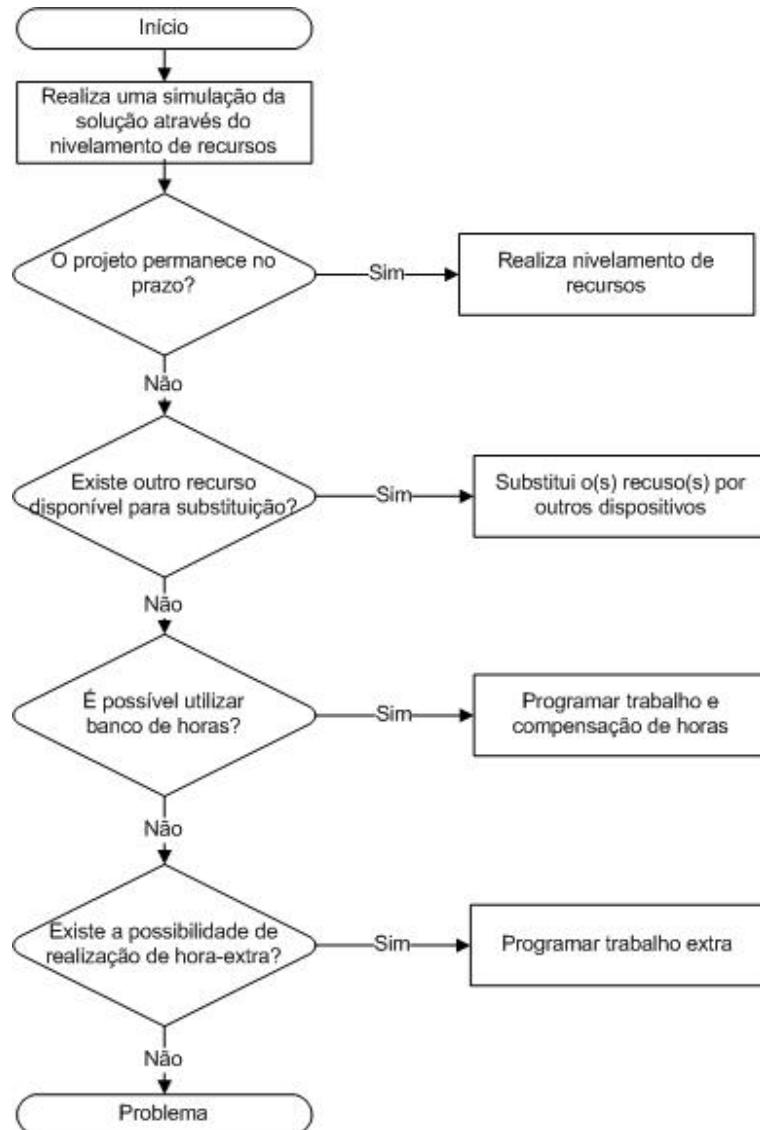


4. Mecanismo adotado para conflitos de recursos

A verificação da utilização do recurso será realizada após terem sido concluídos o cálculo da duração das atividades, a alocação de recursos e os inter-relacionamentos entre as atividades. O processo irá verificar se nenhum recurso está alocado em quantidade superior ao limite máximo disponível para aquele período.

A verificação será realizada através do Microsoft Project no modo de exibição Gantt de Redistribuição diariamente como parte do gerenciamento dos prazos do projeto.

No caso de conflitos de recurso o fluxo a seguir evidenciará o processo de escolha da técnica de conciliamento a ser utilizada.



5. Buffer de tempo do projeto

O projeto não prevê a criação ou a determinação de uma folga ou margem de atraso no término do projeto baseado nos conceitos de corrente crítica, uma vez que a metodologia adotada na construção de cronogramas foi baseada no conceito de caminho crítico, e não no conceito de corrente crítica (Teoria das Restrições).

6. Freqüência de avaliação dos prazos do projeto

Os prazos do projeto deverão ser atualizados e avaliados diariamente, sendo os resultados divulgados nas reuniões diárias da equipe de projetos e apresentados na reunião semanal de CCP (Comitê de Controle do Projeto), prevista no plano de gerenciamento das comunicações.

7. Alocação financeira para o gerenciamento de tempo

Todas as medidas de recuperação de atrasos no projeto que requererem gasto adicional deverão ser aprovadas pelo gerente do projeto.

8. Administração do plano de gerenciamento de tempo

8.1. Responsável pelo plano

- [Nome], membro do time do projeto, será o responsável direto pelo plano de gerenciamento de tempo, suas atualizações e relatórios.
- [Nome], membro do time do projeto, será suplente do responsável direto pelo plano de gerenciamento de tempo.

8.2. Freqüência de atualização do plano de gerenciamento de tempo

O plano de gerenciamento de tempo será reavaliado mensalmente na primeira reunião mensal do CCP, juntamente com os outros planos do projeto. As necessidades de atualização do plano antes da primeira reunião de CCP do projeto deverão ser tratadas segundo os procedimentos descritos no item Outros assuntos não previstos neste plano.

9. Outros assuntos relacionados ao gerenciamento de tempo do projeto não previstos neste plano

Todas as solicitações não previstas neste plano deverão ser submetidas a reunião do CCP (Comitê de Controle do Projeto) para aprovação. Imediatamente após sua aprovação, deverão ser atualizados o plano de gerenciamento de tempo com o devido registro das alterações efetivadas.

REGISTRO DE ALTERAÇÕES		
Data	Modificado por	Descrição da mudança
[Data]	[Responsável]	[Descrição da mudança].

APROVAÇÕES		
[Nome]	[Assinatura]	[Data]
[Cargo]		

APÊNDICE K - *Template do Plano de Gerenciamento da Qualidade*

[Digite o nome do Projeto]		
PLANO DE GERENCIAMENTO DA QUALIDADE <i>QUALITY MANAGEMENT PLAN</i>		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

1. Descrição dos processos de gerenciamento da qualidade

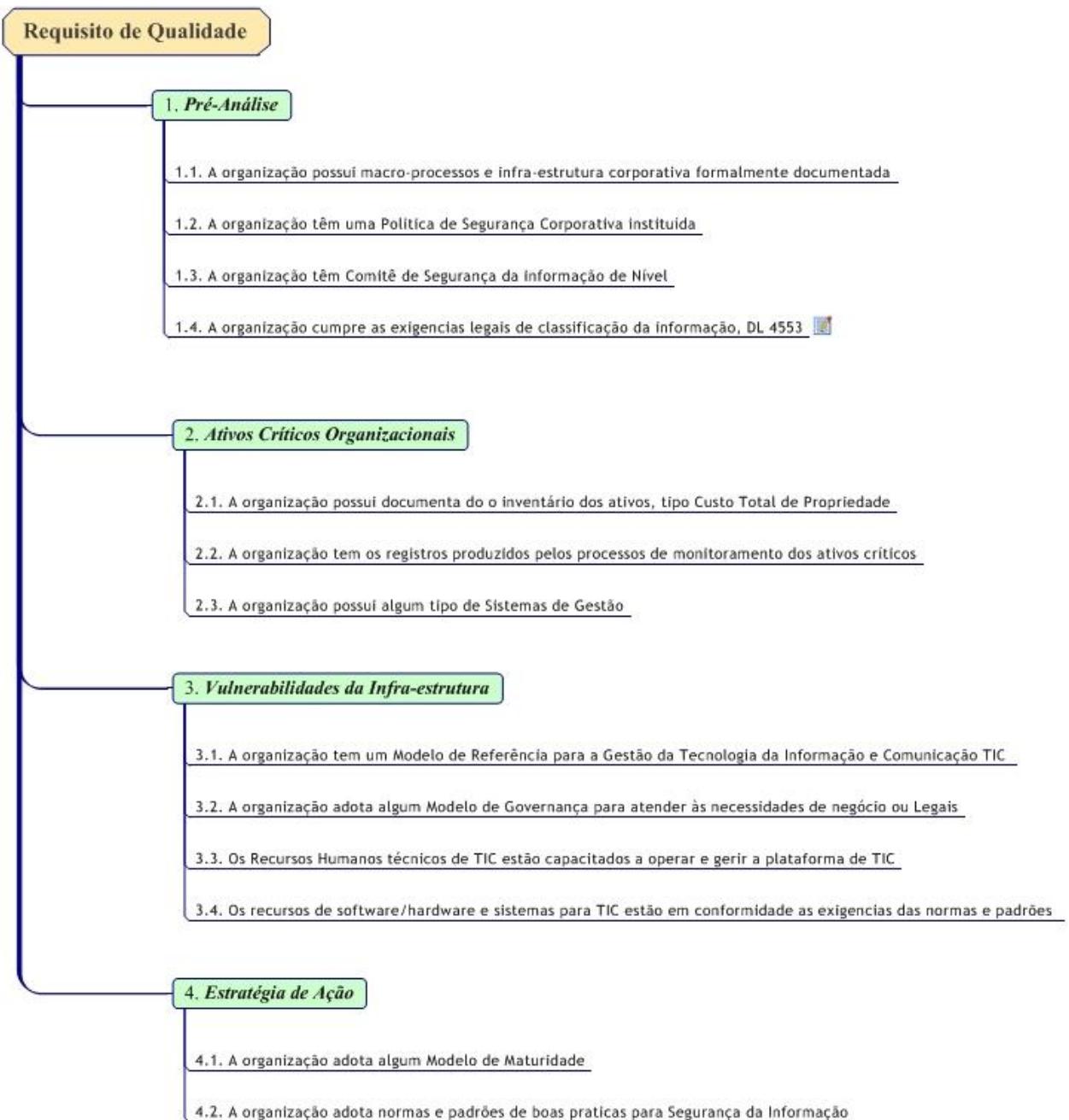
- Todas as reclamações provenientes de clientes, bem como produtos e/ou entregas não conformes com a declaração de escopo deverão ser tratados como medidas corretivas no plano de gerenciamento da qualidade.
- Todas as mudanças nos requisitos de qualidade inicialmente previstas para o projeto devem ser avaliadas e classificadas dentro do sistema de controle de mudanças de qualidade (*Quality Change Control System*).
- Serão consideradas mudanças nos padrões de qualidade apenas as medidas corretivas, que, se influenciadoras no sucesso do projeto, devem ser integradas ao plano. Inovações e novos níveis de qualidade não serão considerados pelo gerenciamento da qualidade.

1.1. Priorização das mudanças nos requisitos de qualidade e respostas

As mudanças dos requisitos de qualidade são classificadas em quatro níveis de prioridade:

- Prioridade 0 (zero) – Mudanças de prioridade zero requerem uma ação imediata por parte do gerente do projeto, que deve acionar imediatamente o patrocinador, uma vez que se trata de mudança urgente, de alto impacto no projeto e em outras áreas sobre as quais o gerente de projeto não tem autonomia.
- Prioridade 1 (um) - Mudanças de prioridade um requerem uma ação imediata por parte do gerente do projeto, independente das reuniões de controle previstas devido à urgência, acionando imediatamente o patrocinador no caso de necessidade de autorizações fora da alcada do gerente de projetos.
- Prioridade 2 (dois) – Mudanças de prioridade dois requerem um planejamento da ação através de terceiros ou de equipes que, a princípio, tenham disponibilidade, uma vez que agregam valor ao sucesso do projeto e são urgentes, porém não têm impacto significativo nos prazos do projeto.
- Prioridade 3 (três) – Mudanças de prioridade três podem ser implementadas por terem influência no sucesso do projeto, porém não requerem uma ação imediata por não serem impactantes ou urgentes.

2. Requisitos de Qualidade



3. Padrões de Qualidade

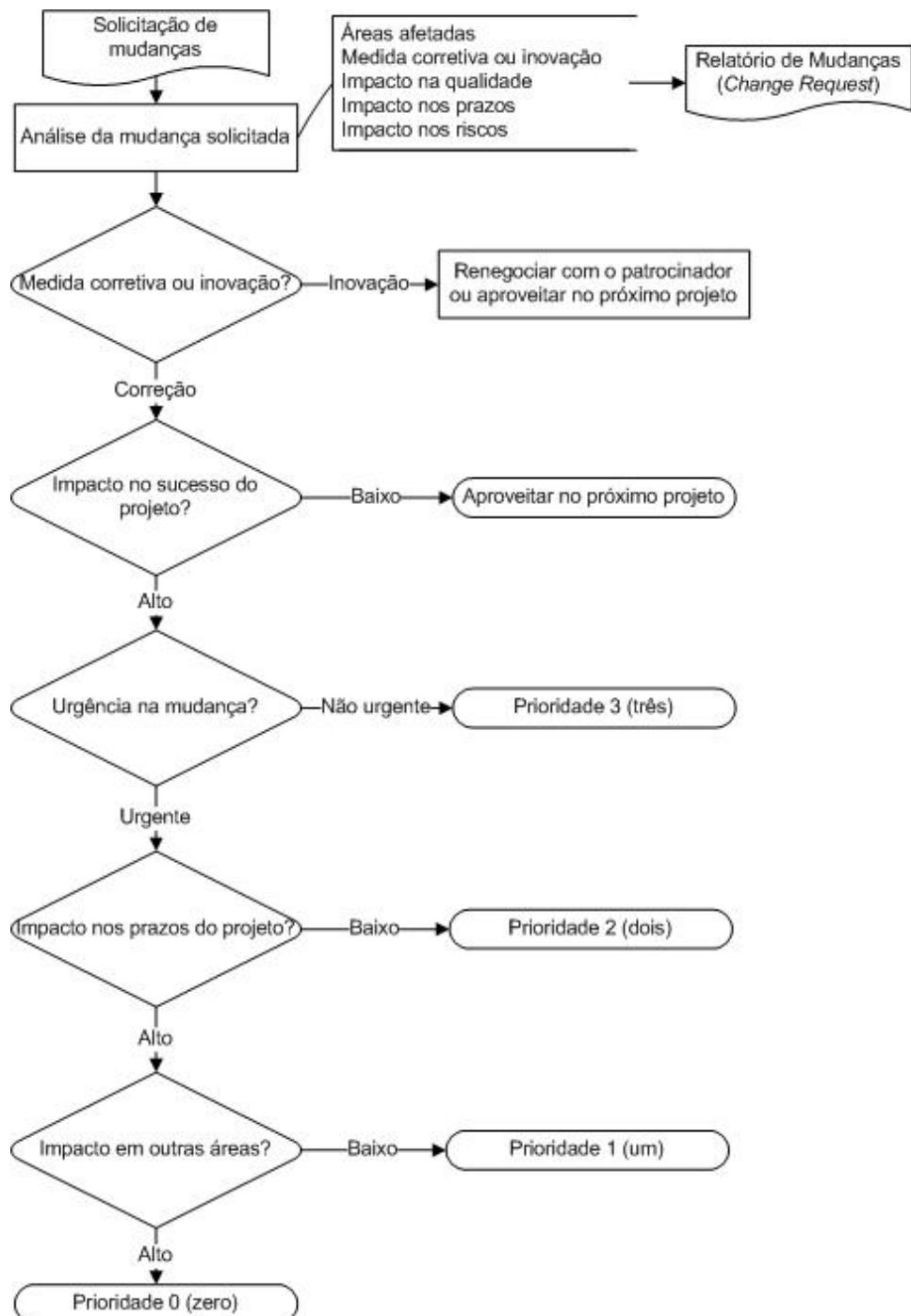
Fase	Requisito	Padrões
1. Pré-Análise	A Organização possui macro-processos e infra-estrutura corporativa formalmente documentada	A Organização deve ter mapeado a missão e os fatores críticos de sucesso para responder as ameaças, Planejamento Estratégico; A Organização deve documentar para a auditória: os processos os planos e os processos de gestão.
1. Pré-Análise	A Organização tem uma Política de Segurança Corporativa instituída a nível executivo.	A Organização deve ter uma Política de Segurança da Informação e Comunicação para atender os requisitos do negócio e da legislação, aderência ao Decreto Lei 3505 de Segurança da Informação;

1. Pré-Análise	A Organização tem o Comitê de Segurança da Informação.	A Organização deve compor um Comitê de Segurança da Informação em nível executivo, para deliberar estrategicamente sobre a proteção e continuidade dos negócios da Organização ; O Comitê de Segurança da Informação é a interface com o Governo Federal para as questões de Segurança da Informação e Proteção da Infra-Estrutura Crítica nacional.
1. Pré-Análise	A Organização cumpre as exigências legais de classificação da informação Decreto Lei n.4553.	A Organização deve cumprir as exigências legais da classificação da informação, quando do trato de assuntos do Governo Federal; Deve estar adequada ao Decreto Lei n.4553 que disciplina a salvaguarda de dados, informações, documentos e materiais sigilosos, bem como das áreas e instalações onde tramitam.
2. Ativos Críticos Organizacionais	A Organização possui documentação do inventário dos ativos no aspecto do Custo Total de Propriedade	A Organização deve ter por necessidade do cumprimento do Decreto Lei n.4553 e da segurança corporativa um inventário dos ativos classificados conforme o nível de importância dado pela classificação da informação.
2. Ativos Críticos Organizacionais	A Organização monitora atividade dos seus ativos críticos;	A Organização deve cumprir as exigências legais quanto aos processos de Auditoria (TCU),
2. Ativos Críticos Organizacionais	A Organização possui algum tipo de Sistemas de Gestão	A Organização deve cumprir as exigências legais e de mercado quanto aos processos Gestão da Qualidade, Segurança da Informação.
3. Vulnerabilidades da Infra-estrutura	A Organização tem um Modelo de Referência para a Gestão da Tecnologia da Informação e Comunicação TIC.	A Organização deve adotar um Modelo de Referência para a Gestão da Tecnologia da Informação e Comunicação TIC, para a certificação em nível internacional, por meio das normas da taxonomia 27000. A Organização deve adotar modelos e normas para viabilizar os processos de auditoria que estão sujeitas via TCU.
3. Vulnerabilidades da Infra-estrutura	A Organização adota algum Modelo de Governança para atender as necessidades de seu negócio ou da legislação	A Organização deve adotar um Modelo de Governança para atender as necessidades de seu negócio ou da legislação
3. Vulnerabilidades da Infra-estrutura	Os Recursos Humanos técnicos de TIC estão capacitados a operar e gerir a plataforma de TIC.	Os Recursos Humanos alocados à TIC da Organização devem estar capacitados na Gestão dos Recursos, apresentando certificações específicas conforme o modelo de referencia adotado.
3. Vulnerabilidades da Infra-estrutura	Os recursos de software/hardware e sistemas para TIC estão em conformidade as exigências das normas e padrões.	Os recursos de software/hardware e sistemas para TIC devem estar em conformidade às exigências das normas e padrões de conformidade com as boas práticas;
4. Estratégia de Ação	A Organização adota algum Modelo de Maturidade	A Organização deve adotar um Modelo de Maturidade baseado em um padrão internacional, promovendo a melhoria contínua da Segurança da Informação e Comunicações.

4. Estratégia de Ação	A Organização adota normas e padrão de boas pratica para Segurança da Informação	A Organização deve adotar normas e padrão de boas prática para Segurança da Informação baseada em conjunto de normas procedimentos que sejam auditáveis.
-----------------------	--	--

4. Sistema de controle de mudanças da qualidade (*Quality change control system*)

Todas as mudanças na qualidade do projeto devem ser tratadas segundo o fluxo apresentado a seguir com suas conclusões apresentadas na reunião semanal de CCP com suas conclusões, prioridades e ações relacionadas.



5. Freqüência de avaliação dos requisitos de qualidade do projeto

Os requisitos da qualidade do projeto devem ser avaliados semanalmente dentro da reunião de CCP (*Change Control Project*), prevista no plano de gerenciamento das comunicações.

6. Alocação financeira das mudanças nos requisitos de qualidade

Todas mudanças na qualidade que requererem gasto adicional deverão ser aprovadas pelo gerente do projeto.

7. Administração do plano de gerenciamento da qualidade

7.1. Responsável pelo plano

- [Nome], membro do time do projeto, será a responsável direta pelo plano de gerenciamento da qualidade.
- [Nome], membro do time do projeto, será suplente do responsável direto pelo plano de gerenciamento da qualidade.

7.2. Freqüência de atualização do plano de gerenciamento da qualidade

O plano de gerenciamento da qualidade será reavaliado mensalmente na primeira reunião mensal do CCP, juntamente com os outros planos de gerenciamento do projeto.

As necessidades de atualização do plano antes da primeira reunião de CCP do projeto deverão ser tratadas segundo os procedimentos descritos no item Outros assuntos não previstos neste plano.

8. Outros assuntos relacionados ao gerenciamento da qualidade do projeto não previstos neste plano

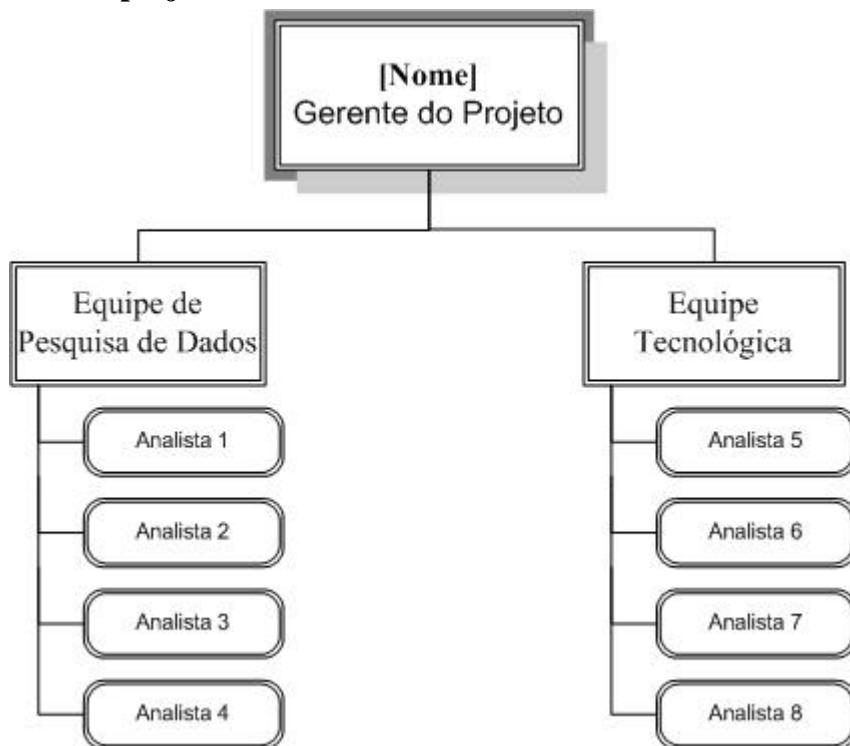
Todas as solicitações não previstas neste plano deverão ser submetidas a reunião do CCP (Comitê de Controle do Projeto) para aprovação. Imediatamente após sua aprovação, deverão ser atualizados o plano de gerenciamento da qualidade com o devido registro das alterações efetivadas.

REGISTRO DE ALTERAÇÕES		
Data	Modificado por	Descrição da mudança
[Data]	[Responsável]	[Descrição da mudança].

APROVAÇÕES		
[Nome] [Cargo]	[Assinatura]	[Data]

APÊNDICE L - *Template do Plano de Gerenciamento de Recursos Humanos***[Digite o nome do Projeto]****PLANO DE GERENCIAMENTO DE RECURSOS HUMANOS
STAFF MANAGEMENT PLAN**

Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

1. Organograma do projeto**2. Diretório do time do projeto (*Team directory*)**

	Nome	Área	e-mail	Telefone
1	[Nome]	Gerente do Projeto	[e-mail]	[Telefone]
2	[Nome]	Equipe de Pesquisa de Dados	[e-mail]	[Telefone]
3	[Nome]	Equipe de Pesquisa de Dados	[e-mail]	[Telefone]
4	[Nome]	Equipe Tecnológica	[e-mail]	[Telefone]
5	[Nome]	Equipe Tecnológica	[e-mail]	[Telefone]
6	[Nome]	Equipe Tecnológica	[e-mail]	[Telefone]

3. Matriz de responsabilidades

Nº	Nome	Área	Pré-Análise	Ativos Críticos Organizacionais	Vulnerabilidade da Infra-estrutura	Estratégia de Ação	Planos					
							Escopo	Tempo	Qualidade	RH	Comunicação	Riscos
1	[Nome]	Gerente do Projeto	R	A		R	R			R		
2	[Nome]	Equipe de Pesquisa de Dados	S	R	A	S		R	S	S	R	R
3	[Nome]	Equipe de Pesquisa de Dados	A	S	A							
4	[Nome]	Equipe Tecnológica			R	A	S	S	R		S	S
5	[Nome]	Equipe Tecnológica			S							
6	[Nome]	Equipe Tecnológica			A							

R- Responsável

A-Apoio

S-Suplente

4. Novos recursos, re-alocação e substituição de membros do time

O gerente de projeto deve se empenhar pessoalmente na permanência de todos os integrantes da equipe durante o projeto.

No caso de re-alocação do profissional integrante do projeto, caberá ao gerente de projeto a identificação do substituto em comum acordo com as diretrizes do projeto e as funções a serem exercidas.

Para novos recursos solicitados para o time caberá ao gerente de projeto providenciar.

5. Treinamento

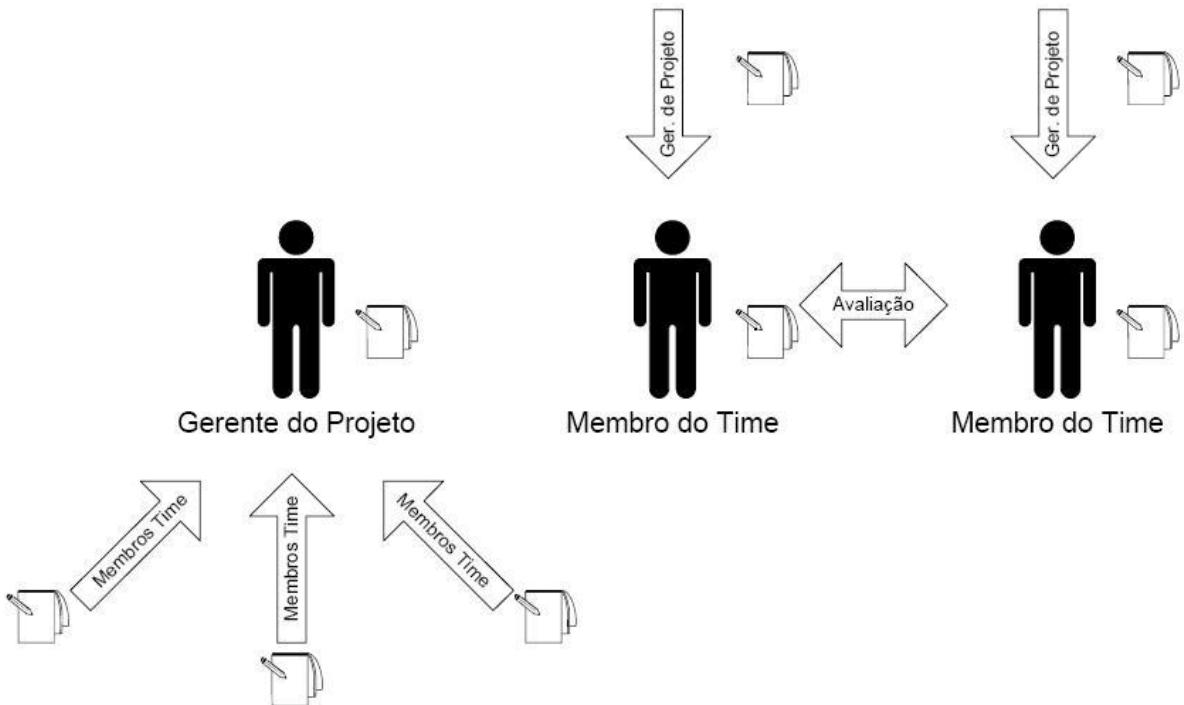
Não estão previstos treinamentos para a equipe de projeto. Qualquer necessidade extraordinária de treinamento deve ser aprovada previamente pelo gerente de projeto.

6. Avaliação de resultados

O resultado do trabalho da equipe será avaliado mensalmente pelo gerente de projeto em reunião individual com cada membro do time do projeto. Ao fim do projeto será realizada uma reunião de avaliação de cada um dos integrantes do projeto e será gerada uma avaliação final compilada.

Essa avaliação final compilada será feita através de um modelo circular sob o qual todos serão avaliados tanto pelas chefias quanto pelos pares e subordinados.

- O gerente de projeto se auto-avaliará e será avaliado, também, por todos os membros do time.
- Cada membro do time se auto-avaliará, será avaliado pelo gerente de projeto e será avaliado por, pelo menos, outros três membros do time, escolhidos por sorteio.
- Todos os resultados serão compilados em uma ficha única que mostrará a percepção de cada um dos envolvidos no processo de avaliação.



7. Bonificação

Caso o resultado compilado da avaliação atinja média superior à 90%, o membro da equipe do projeto, funcionário do CEPESC receberá em sua avaliação institucional nota equivalente a 100 pontos.

A bonificação somente será considerada após o término do projeto, apenas na avaliação institucional que suceder ao projeto e para os membros do time que participaram integralmente dele (ver diretório do projeto), realizando suas atividades previstas quando foram inicialmente alocados no projeto.

Membros do time re-alocados ou substituídos não terão direito à bonificação.

8. Freqüência de avaliação consolidada dos resultados do time

Os resultados nas avaliações mensais do time devem ser compilados e apresentados na última reunião mensal de CCP (*Change Control Project*), prevista no plano de gerenciamento das comunicações.

9. Alocação financeira para o gerenciamento de RH

Todas as medidas de gerenciamento de recursos humanos do projeto que requererem gasto adicional deverão ser aprovadas pelo gerente do projeto.

10. Administração do plano de gerenciamento de recursos humanos

10.1. Responsável pelo plano

- [Nome], gerente do projeto, será o responsável direto pelo plano de gerenciamento de RH.
- [Nome], membro do time do projeto, será suplente do responsável direto pelo plano de gerenciamento de RH.

10.2. Freqüência de atualização do plano de gerenciamento de RH

O plano de gerenciamento de RH será reavaliado mensalmente na primeira reunião mensal do CCP, juntamente com os outros planos de gerenciamento do projeto.

As necessidades de atualização do plano antes da primeira reunião de CCP do projeto deverão ser tratadas segundo os procedimentos descritos no item Outros assuntos não previstos neste plano.

11. Outros assuntos relacionados ao gerenciamento de RH do projeto não previstos neste plano

Todas as solicitações não previstas neste plano deverão ser submetidas a reunião do CCP (Comitê de Controle do Projeto) para aprovação. Imediatamente após sua aprovação, deverão ser atualizados o plano de gerenciamento de RH com o devido registro das alterações efetivadas.

REGISTRO DE ALTERAÇÕES		
Data	Modificado por	Descrição da mudança
[Data]	[Responsável]	[Descrição da mudança].

APROVAÇÕES		
[Nome] [Cargo]	[Assinatura]	[Data]

APÊNDICE M - *Template do Plano de Gerenciamento das Comunicações*

[Digite o nome do Projeto]		
PLANO DE GERENCIAMENTO DAS COMUNICAÇÕES COMMUNICATIONS MANAGEMENT PLAN		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

1. Descrição dos processos de gerenciamento das comunicações

- O gerenciamento das comunicações do projeto será realizado através dos processos de comunicação formal, estando incluído nessa categoria
 - e-mails,
 - publicações web,
 - memorandos,
 - documentos impressos,
 - reuniões com ata lavrada.
- Todas as reuniões formais serão realizadas às **[Dia da semana]** para disponibilizar tempo livre para os trabalhos do projeto nos dias subsequentes.
- Todas as informações do projeto devem ser atualizadas de modo constante no site restrito do projeto, incluindo as atualizações diárias nos custos e nos prazos.
- Todas as solicitações de mudança no processo de comunicação devem ser feitas por escrito ou através de e-mail e aprovadas pelo gerente do projeto.

2. Eventos de comunicação

O projeto terá os seguintes eventos de comunicação:

2.1. Reunião inicial

- Objetivo – Dar a partida no projeto, apresentando as informações quanto ao seu objetivo e à sua importância para a empresa, aos seus prazos, aos seus custos, etc. Devem também ser apresentadas as principais entregas do projeto e os elementos de alto nível no WBS. Outro objetivo do evento é motivar e dar suporte gerencial ao gerente de projeto e ao seu time, de modo a construir um ambiente colaborativo e integrado dentro da organização alvo da Análise de Risco.
- Metodologia – Apresentação em auditório ou sala de treinamento, com utilização de projetor e computadores.
- Responsável - **[Nome], [Função no Projeto]**.
- Envolvidos – Todos os envolvidos no time do projeto, patrocinador e convidados (executivos da empresa).
- Data e Horário – **[Dia e hora]**
- Duração – **[Duração]**.
- Local – **[Local]**.

- Outros – Lista de presença requerida.

2.2. Reunião de CCP (*Change Control Project*)

- Objetivo – Avaliar todos os indicadores do projeto, incluindo os resultados parciais obtidos e a avaliação do cronograma, dos riscos identificados, da qualidade obtida e do escopo. Tem como base garantir o cumprimento do plano do projeto, sendo o processo principal de aprovação das solicitações de mudança apresentadas no Sistema de controle integrado de mudanças.
- Metodologia – Reunião com a utilização de projetor e computadores conectados à base de informações do projeto ou utilização de slides.
- Responsável - [Nome], gerente do projeto.
- Envolvidos – [Nome], gerente do projeto, [Nome], responsável pelo plano de gerenciamento de escopo, e [Nome], patrocinador (participação opcional).
- Freqüência – Semanal, às [Dia da semana] com início dia [Data] e término em [Data].
- Reuniões extraordinárias – Podem ser solicitadas reuniões extraordinárias de CCP através de um pedido formal do gerente de projeto a partir do fluxo do sistema integrado de controle de mudanças do projeto.
- Duração – [Duração], com início às [Hora].
- Local – [Local].
- Outros – Ata de reunião (com lista de presença) requerida.

2.3. Reunião de Avaliação da Equipe

- Objetivo – Avaliar o desempenho do time do projeto, conforme previsto no plano de gerenciamento de RH, na categoria Avaliação de resultados. A pauta da reunião do dia [Data] conterá a avaliação final da equipe, quando todos os resultados do desempenho individual de cada membro do time, incluindo o gerente de projetos, serão encaminhados para o departamento de recursos humanos.
- Metodologia – Reuniões individuais entre os integrantes do time do projeto e o gerente do projeto para o preenchimento da avaliação de desempenho dos profissionais, conforme descrito no plano de RH.
- Responsável - [Nome], gerente do projeto.
- Envolvidos – Integrantes do time do projeto e o gerente do projeto.
- Freqüência – Mensal, toda última segunda-feira de cada mês, com início dia [Data] e término em [Data].
- Duração – [Duração], com início às [Hora]. (imediatamente após a reunião de CCP).
- Local – [Local].
- Outros – Ata de reunião (com lista de presença) requerida.

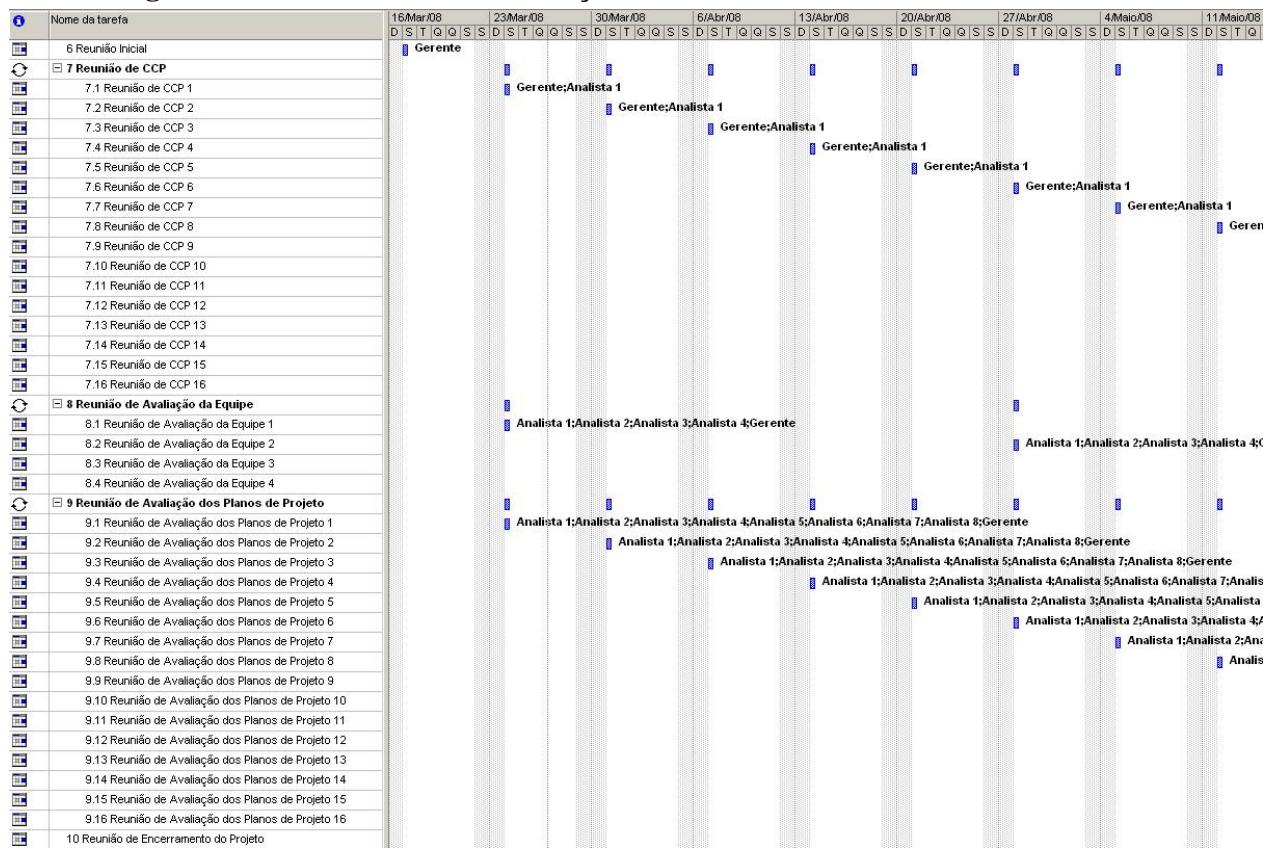
2.4. Reunião de Avaliação dos Planos de Projeto

- Objetivo – Avaliar a efetividade dos planos de gerenciamento do projeto, verificando se o que está estabelecido como regra no plano está sendo cumprido e se o plano precisa de atualização.
- Metodologia – Reunião convencional, onde cada um dos responsáveis pelos planos apresenta os potenciais desvios e necessidades de atualização para os demais integrantes do time, que realizam comentários e sugestões até que o plano seja atualizado e aprovado pelo gerente do projeto.
- Responsável - [Nome], gerente do projeto..
- Envolvidos – Todos os integrantes do time do projeto
- Freqüência – Mensal, toda primeira segunda-feira de cada mês com início [Data] e término em [Data].
- Duração – [Duração], com início às [Hora]. (imediatamente após a reunião de Avaliação da Equipe).
- Local – [Local].
- Outros – Ata de reunião (com lista de presença) requerida.

2.5. Reunião de Encerramento do Projeto

- Objetivo – Apresentar os resultados obtidos no projeto, bem como discutir as falhas e os problemas ocorridos de modo a fornecer base para o acúmulo de experiências sobre o projeto.
- Metodologia – Apresentação dos resultados pelo gerente do projeto, bem como discussão direta através de mapas mentais sobre todos as questões e melhorias possíveis para futuros projetos.
- Responsável - [Nome], gerente do projeto.
- Envolvidos – Todos os envolvidos no time do projeto.
- Data e Horário – [Dia e hora]. (Uma semana após a apresentação do Projeto ao cliente)
- Duração – [Duração].
- Local – [Local].
- Outros – Lista de presença requerida.

3. Cronograma dos eventos de comunicação



4. Atas de reunião

Todos os eventos do projeto, com exceção da Reunião Inicial e do Encerramento do Projeto, deverão apresentar ata de reunião com, no mínimo, os seguintes dados:

- Lista de presença
- Pauta
- Decisões tomadas
- Pendências não solucionadas
- Aprovações

5. Relatórios do projeto

Os principais relatórios a serem apresentados são mostrados pelos modelos a seguir. Os modelos têm como objetivo apenas caracterizar o layout do relatório. Os dados neles contidos apenas ilustrativos. Todos esses relatórios serão apresentados nas reuniões de Avaliação dos Planos do Projeto.

Qualquer outra necessidade de relatórios de progresso para as reuniões de CCP previstas deverá ser solicitada com antecedência de 48 horas e por escrito com autorização do gerente de projetos.

5.1. Modelo de Gráfico de Gantt

O gráfico de Gantt do projeto será evidenciado através de barras no tempo para todas as atividades do projeto ao longo de sua execução.

Responsável: [Nome]

Área: Gerenciamento de tempo



5.2. Modelo de Relatório de Percentual Completo

Relatório que apresenta o percentual completo de cada uma das atividades previstas (de 0 a 100), identificando as atividades concluídas, as em andamento e as atividades a iniciar. Ao lado do percentual completo existe um indicador tipo “bolo” onde o percentual completo é apresentado através do preenchimento do círculo. A data apresentada no relatório é a data projetada para o término do projeto.

Responsável: [Nome]

Área: Gerenciamento de tempo



6. Ambiente técnico e estrutura de armazenamento e distribuição da informação (EPM)

A estrutura de armazenamento e distribuição da informação será realizada integralmente pela internet através do servidor [Endereço IP], utilizando VPN (Virtual Private Network) Rede Privada Virtual. O servidor está localizado no CEPESC.

O ambiente de trabalho contará com notebooks para geração e armazenamento dos documentos gerados *in loco*.

7. Alocação financeira para o gerenciamento das comunicações

Os custos relativos ao gerenciamento das comunicações não serão considerados pois a infraestrutura necessária já está implantada.

Todas as despesas adicionais no processo de comunicação deverão ser aprovadas pelo gerente do projeto.

8. Administração do plano de gerenciamento das comunicações

8.1. Responsável pelo plano

- [Nome], membro do time do projeto, será o responsável direto pelo plano de gerenciamento das comunicações.

- [Nome], membro do time do projeto, será suplente do responsável direto pelo plano de gerenciamento das comunicações.

8.2. Freqüência de atualização do plano de gerenciamento das comunicações

O plano de gerenciamento das comunicações será reavaliado mensalmente na primeira reunião mensal do CCP, juntamente com os outros planos de gerenciamento do projeto.

As necessidades de atualização do plano antes da primeira reunião de CCP do projeto deverão ser tratadas através dos procedimentos descritos no item Outros assuntos não previstos neste plano.

9. Outros assuntos relacionados ao gerenciamento das comunicações do projeto não previstos neste plano

Todas as solicitações não previstas neste plano devem ser submetidas a reunião do CCP (Comitê de controle de mudanças) para aprovação. Imediatamente após sua aprovação devem ser atualizadas no plano de gerenciamento das comunicações com seu devido registro de alterações.

REGISTRO DE ALTERAÇÕES		
Data	Modificado por	Descrição da mudança
[Data]	[Responsável]	[Descrição da mudança].

APROVAÇÕES		
[Nome] [Cargo]	[Assinatura]	[Data]

APÊNDICE N - *Template do Plano de Gerenciamento de Riscos*

[Digite o nome do Projeto]

PLANO DE GERENCIAMENTO DE RISCOS E DE RESPOSTAS AOS RISCOS *RISK MANAGEMENT PLAN AND RISK RESPONSE MANAGEMENT PLAN*

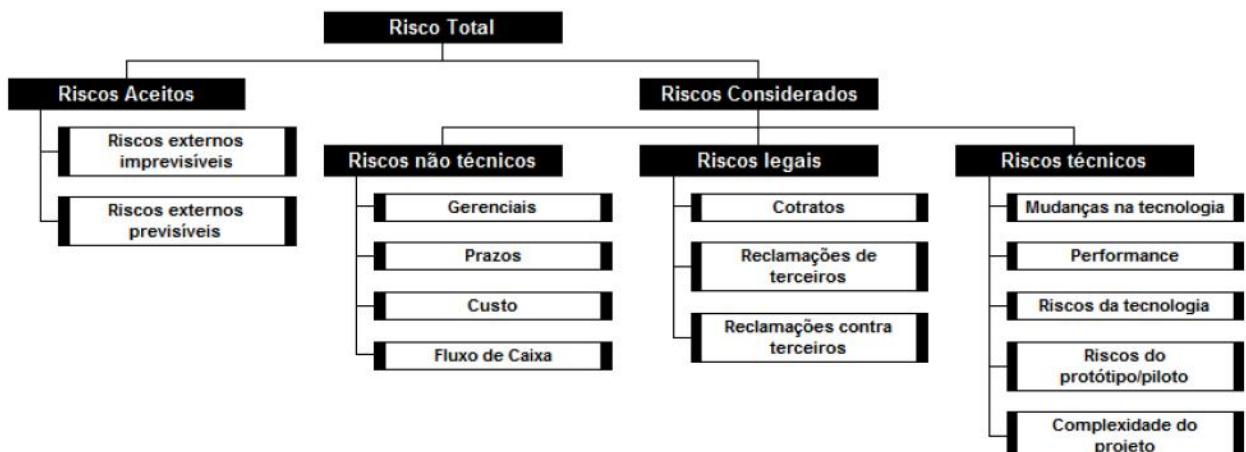
Preparado por	[Nome do responsável pelo documento]	Versão [Versão do documento]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

1. Descrição dos processos de gerenciamento de riscos

- O gerenciamento de riscos do projeto será realizado com base nos riscos previamente identificados, bem como no monitoramento e no controle de novos riscos que podem não ter sido identificados oportunamente.
- Todos os riscos não previstos no plano devem ser incorporados ao projeto dentro do sistema de controle de mudanças de riscos (*Risk Change Control System*).
- Os riscos a serem identificados serão apenas os riscos internos ao projeto. Riscos relacionados ao mercado, ao ambiente macro da empresa ou à sociedade serão automaticamente aceitos sem análise e sem uma resposta prevista (aceitação passiva).
- As respostas possíveis aos riscos identificados pelo projeto serão as aceitações passiva e ativa (através de contingências). Não será aceito como uma possível resposta ao risco o ato de evitá-lo (*avoidance*), uma vez que não serão aceitas alterações no escopo que não sejam de caráter corretivo no produto final do projeto.
- A identificação, a avaliação e o monitoramento de riscos devem ser feitos por escrito ou através de e-mail, conforme descrito no plano de comunicações do projeto.

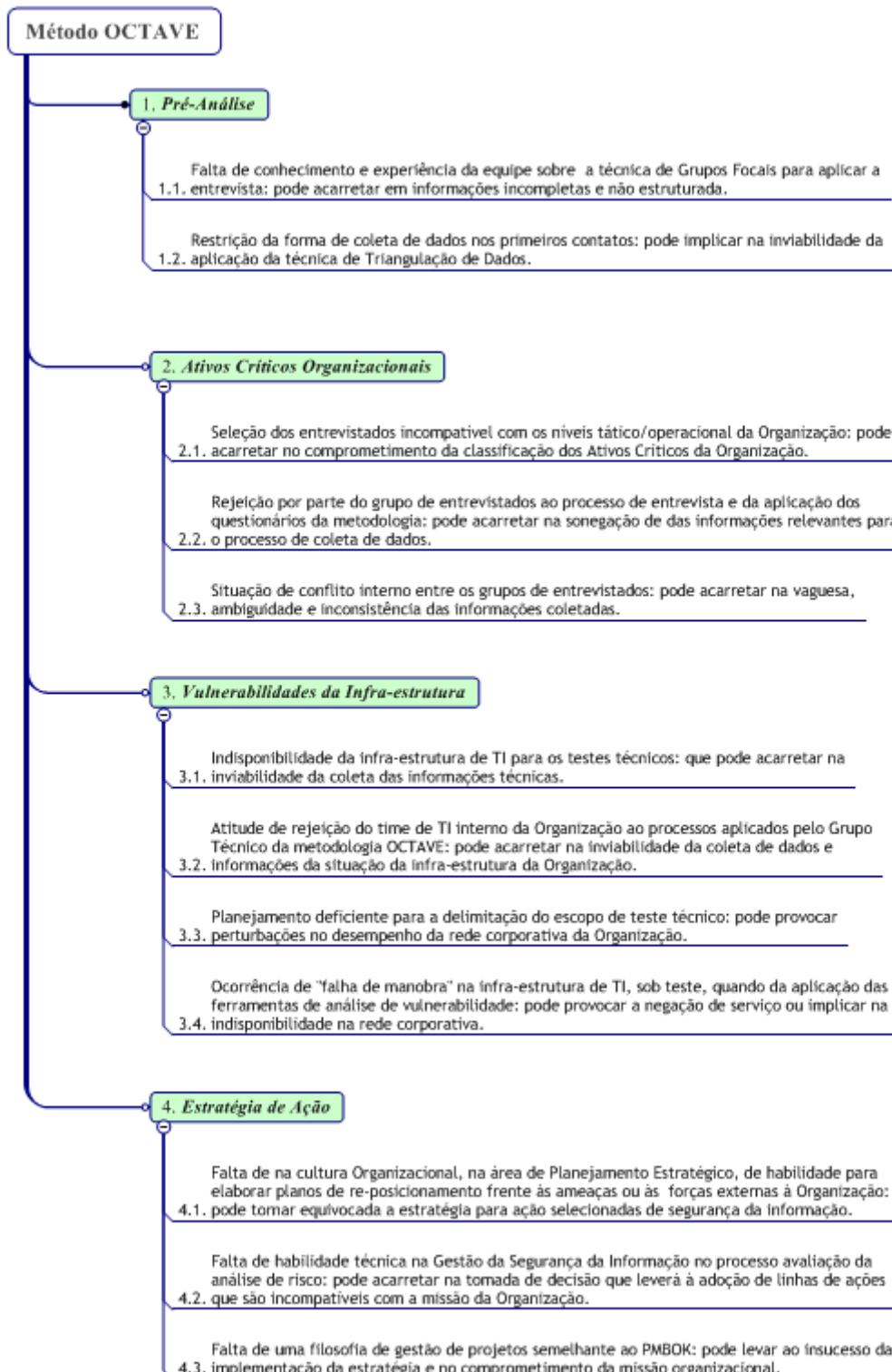
2. RBS – *Risk Breakdown Structure* para a identificação dos riscos

O modelo de estrutura de riscos a ser utilizado pelo projeto será o proposto por Wideman, porém abordando apenas os Riscos internos não técnicos, os Riscos legais e os Riscos técnicos. Riscos externos não serão considerados, conforme já apresentado anteriormente. O modelo a seguir foi utilizado como base para a identificação dos riscos do projeto.



3. Riscos identificados

Os riscos identificados no projeto, segundo o WBS (*Work Brakdown Structure*) do projeto e a RBS anteriormente apresentada estão listados na estrutura a seguir.

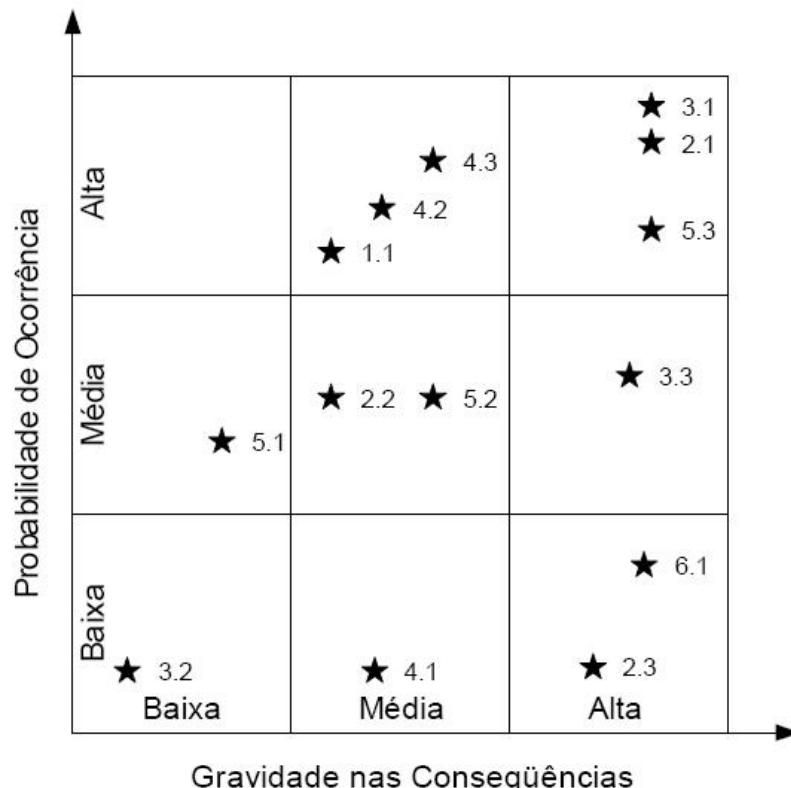


Os riscos anteriores foram identificados pelo time de projeto (incluindo a área de compras e de TI), utilizando-se do RBS através da técnica de *Brainstorming*, da Técnica do Grupo Nominal (NGT) e, em alguns casos, do *Slip de Crawford*.

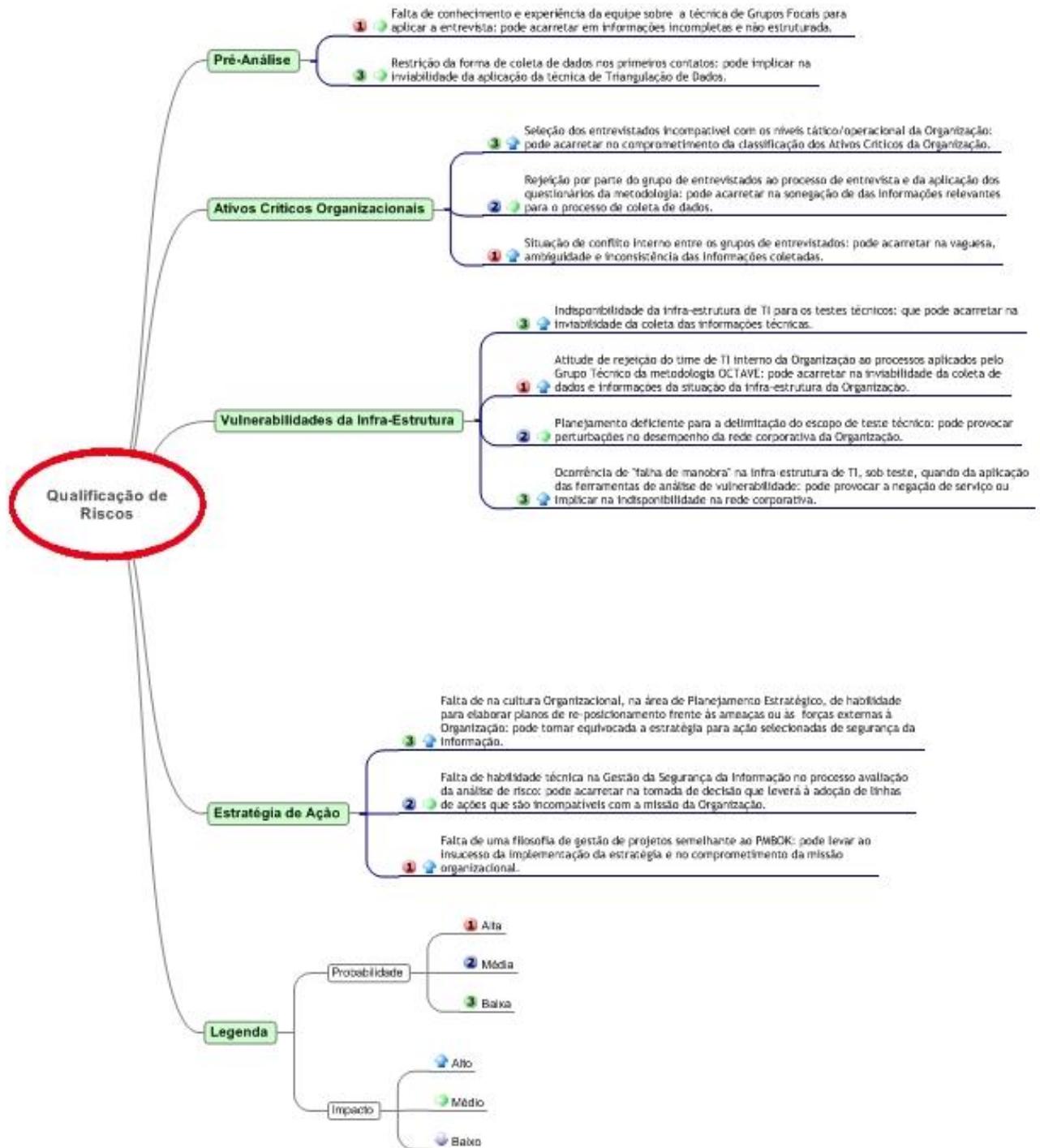
4. Qualificação dos riscos

Os riscos identificados serão qualificados na sua probabilidade de ocorrência e impacto ou gravidade dos seus resultados

- Probabilidade
 - Baixa – A probabilidade de ocorrência do risco pode ser considerada pequena ou imperceptível (menor do que 20%).
 - Média – Existe uma probabilidade razoável de ocorrência do risco (probabilidade entre 20 e 60%).
 - Alta – O risco é iminente (probabilidade maior que 60%).
- Gravidade
 - Baixa – O impacto do evento de risco é irrelevante para o projeto, tanto em termos de custo, quanto de prazos, podendo ser facilmente resolvido.
 - Média – O impacto do evento de risco é relevante para o projeto e necessita de um gerenciamento mais preciso, sob pena de prejudicar os seus resultados.
 - Alta – O impacto do evento de risco é extremamente elevado e, no caso de não existir uma interferência direta, imediata e precisa da equipe do projeto, os resultados serão seriamente comprometidos.



Os riscos foram classificados segundo o modelo de classificação comparativa de riscos (CCR) através de mapas mentais, como o apresentado a seguir. As respostas aos riscos serão planejadas de acordo com a ordem apresentada no gráfico anterior, onde os principais eventos de riscos são os de probabilidade e gravidade altas.



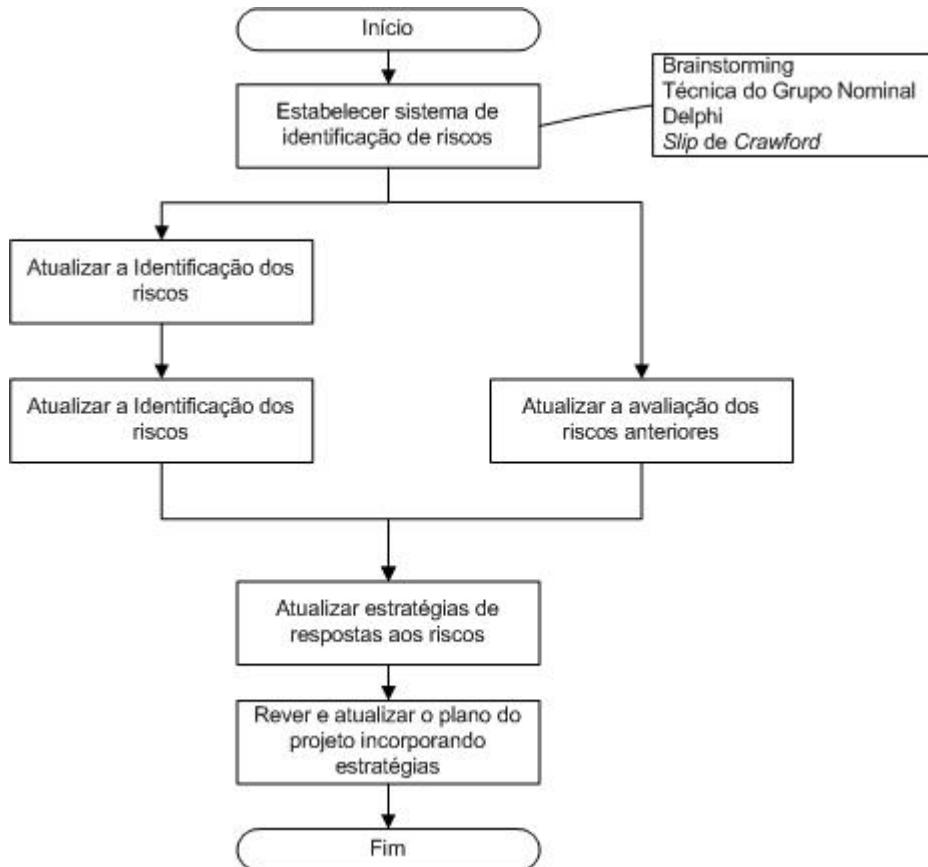
5. Quantificação dos riscos

Por se tratar de um projeto onde somente os riscos internos serão avaliados, optou-se por analisar apenas os riscos segundo aspectos qualitativos, utilizando-se o conceito qualitativo de valor agregado, anteriormente apresentado para os riscos identificados. Portanto, não será feita, neste plano, a análise quantitativa dos riscos.

6. Sistema de controle de mudanças de riscos (*Risk change control system*)

Toda a identificação de riscos e alterações nos riscos já identificados (variação na probabilidade e impacto dos riscos devem ser tratados segundo o fluxo apresentado a seguir

com suas conclusões apresentadas na reunião semanal de CCP com suas conclusões, prioridades e ações relacionadas).



7. Respostas planejadas aos riscos

Para os riscos identificados e qualificados, optou-se por estratégias diferenciadas para cada necessidade, conforme quadro a seguir.

Item	Fase	Risco	Probabi-lidade	Impa-cto	Res-posta	Descrição	Custo	Progressão no Tempo
1.1	Pré-Análise	Falta de conhecimento e experiência da equipe sobre a técnica de Grupos Focais para aplicar a entrevista: pode acarretar em informações incompletas e não estruturada.	Alta	Médio	Atenuação	Realizar o treinamento em Gerenciamento de Projetos para o Gerente de Projeto e de técnicas de coleta de dados (triangulação) para a equipe de análise	Rateado entre as equipes da Gerência do Projeto e da Organização	Diminui
1.2	Pré-Análise	Restrição da forma de coleta de dados nos primeiros contatos: pode implicar na inviabilidade da aplicação da técnica de Triangulação de Dados.	Baixa	Médio	Atenuação	Realizar a “Apresentação OCTAVE” para todos os níveis da Organização da área de abrangência da Metodologia Octave e os seus fatores críticos de sucesso.	Não há custo envolvido.	Constante

Item	Fase	Risco	Probabi-lidade	Impa-cto	Res-posta	Descrição	Custo	Progressão no Tempo
2.1	Ativos Críticos Organizacionais	Seleção dos entrevistados incompatível com os níveis tático/operacional da Organização: pode acarretar no comprometimento da classificação dos Ativos Críticos da Organização.	Baixa	Alto	Atenuação	Realizar a triangulação dos dados coletados na Pré-Análise e verificar a exatidão com o nível estratégico.	Não há custo envolvido.	Agrava
2.2	Ativos Críticos Organizacionais	Rejeição por parte do grupo de entrevistados ao processo de entrevista e da aplicação dos questionários da metodologia: pode acarretar na sonegação de das informações relevantes para o processo de coleta de dados.	Médio	Médio	Atenuação	Realizar conscientização por meio da “Apresentação da Metodologia OCTAVE” e a necessidade da abordagem estratégica para com os ativos críticos da Organização.	Não há custo envolvido.	Diminui
2.3	Ativos Críticos Organizacionais	Situação de conflito interno entre os grupos de entrevistados: pode acarretar na vaguezza, ambigüidade e inconsistência das informações coletadas.	Alta	Alto	Atenuação	Realizar os processos e as técnicas de Grupos Focais aliados à dinâmica de grupo para a homogeneização harmonização dos grupos internos a Organização.	Não há custo envolvido.	Diminui
3.1	Vulnerabilidade da Infra-estrutura	Indisponibilidade da infra-estrutura de TI para os testes técnicos: que pode acarretar na inviabilidade da coleta das informações técnicas.	Média	Alto	Atenuação	Realizar a redução do escopo, escopo reduzido, de teste com reconfiguração das ferramentas de análise.	Não há custo envolvido.	Agrava
3.2	Vulnerabilidade da Infra-estrutura	Atitude de rejeição do time de TI interno da Organização aos processos aplicados pelo Grupo Técnico da metodologia OCTAVE: pode acarretar na inviabilidade da coleta de dados e informações da situação da infra-estrutura da Organização.	Alta	Alto	Atenuação	Realizar a demonstração com acompanhamento e autorização interna em situações de intrusão a rede da Organização. Realizar os processos e as técnicas de Grupos Focais aliadas à dinâmica de grupo para a homogeneização harmonização dos grupos internos a Organização.	Não há custo envolvido.	Diminui
3.3	Vulnerabilidade da Infra-estrutura	Planejamento deficiente para a delimitação do escopo de teste técnico: pode provocar perturbações no desempenho da rede corporativa da Organização.	Média	Médio	Atenuação	Realizar o monitoramento da fase de teste de intrusão e replanejamento dos testes a partir dos resultados preliminares.	Não há custo envolvido.	Agrava

Item	Fase	Risco	Probabi-lidade	Impa-cto	Res-posta	Descrição	Custo	Progressão no Tempo
3.4	Vulnerabilidade da Infra-estrutura	Ocorrência de "falha de manobra" na infra-estrutura de TI, sob teste, quando da aplicação das ferramentas de análise de vulnerabilidade: pode provocar a negação de serviço ou implicar na indisponibilidade na rede corporativa.	Baixa	Alto	Atenuação	Elaborar com a equipe de TI da Organização um plano de recuperação ou recondução para o estado de pré-teste. Planejar a janela de teste e monitorar o ambiente.	Não há custo envolvido.	Constante
4.1	Estratégia de Ação	Falta na cultura Organizacional, área de Planejamento Estratégico, das habilidades para a elaboração de planos de reposicionamento frente às ameaças ou às forças externas à Organização: pode tornar equivocada a estratégia para ações selecionadas de segurança da informação.	Alta	Alto	Atenuação	Realizar a apresentação da abordagem do Gerenciamento de Projetos e da Gestão da Segurança da Informação ISO27002, e adequado ao Planejamento Estratégico da Organização.	Custo da Organização Cliente	Agrava
4.2	Estratégia de Ação	Falta de habilidade técnica na Gestão da Segurança da Informação no processo avaliação da análise de risco: pode acarretar na tomada de decisão que levará à adoção de linhas de ações que são incompatíveis com a missão da Organização.	Baixo	Alto	Atenuação	Realizar o treinamento em Gerenciamento de Projetos, Gestão da Segurança da Informação ISO27002 e metodologia OCTAVE e adequá-las aos modelos de Governança, se houver, se não adotar um modelo inicial de Gestão da Segurança da Informação conforme a norma ABNT ISO27002.	Custo da Organização Cliente	Agrava
4.3	Estratégia de Ação	Falta de uma filosofia de gestão de projetos semelhante ao PMBOK: pode levar ao insucesso da implementação da estratégia e no comprometimento da missão organizacional.	Baixo	Alto	Atenuação	Realizar o treinamento em Gerenciamento de Projetos PMBOK e criar um Escritório de Projetos na Organização.	Custo da Organização Cliente	Constante

8. Freqüência de avaliação dos riscos do projeto

Os riscos identificados no projeto devem ser avaliados semanalmente dentro da reunião de CCP (Comitê de Controle do Projeto), prevista no plano de gerenciamento das comunicações.

9. Alocação financeira para o gerenciamento de riscos

Todas as despesas resultantes no processo de gerenciamento de risco deverão ser aprovadas pelo gerente do projeto.

10. Administração do plano de gerenciamento de riscos

10.1. Responsável pelo plano

- [Nome], membro do time do projeto, será o responsável direto pelo plano de gerenciamento de riscos.
- [Nome], membro do time do projeto, será suplente do responsável direto pelo plano de gerenciamento de riscos.

10.2. Freqüência de atualização do plano de gerenciamento de riscos

O plano de gerenciamento de riscos será reavaliado mensalmente na primeira reunião mensal do CCP, juntamente com os outros planos de gerenciamento do projeto.

Necessidades de atualização do plano antes da primeira reunião de CCP do projeto devem ser tratadas através dos procedimentos descritos no item Outros assuntos não previstos neste plano.

11. Outros assuntos relacionados ao gerenciamento de riscos do projeto não previstos neste plano

Todas as solicitações relacionadas aos riscos do projeto não previstas neste plano deverão ser submetidas a reunião do CCP (Comitê de controle de mudanças) para aprovação. Imediatamente após sua aprovação deverão ser atualizadas no plano de gerenciamento de riscos com seu devido registro de alterações.

REGISTRO DE ALTERAÇÕES		
Data	Modificado por	Descrição da mudança
[Data]	[Responsável]	[Descrição da mudança].

APROVAÇÕES		
[Nome] [Cargo]	[Assinatura]	[Data]