**CENTRO UNIVERSITÁRIO EUROAMERICANO – UNIEURO PRÓ-REITORIA E PÓS-GRADUAÇÃO, PESQUISA E EXTENSÃO COORDENAÇÃO DE PÓS-GRADUAÇÃO LATO SENSU**

**CURSO DE MBA EM ENGENHARIA DE SOFTWARE**

**MURILO SILVA ANDRADE SOUZA**

**NAYARA SOUZA DUARTE**

**ROSANA OLIVEIRA RAMOS DA COSTA**

QUALIDADE DE SOFTWARE COM O RUP

**Brasília, Abril / 2014**



**MURILO SILVA ANDRADE SOUZA**

**NAYARA SOUZA DUARTE**

**ROSANA OLIVEIRA RAMOS DA COSTA**

**QUALIDADE DE SOFTWARE COM O RUP**

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

**Orientadora: Prof.ª MSc. Edna Dias Canedo**

**Brasília**

**Abril, 2014**

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

**MURILO SILVA ANDRADE SOUZA**

**NAYARA SOUZA DUARTE**

**ROSANA OLIVEIRA RAMOS DA COSTA**

**QUALIDADE DE SOFTWARE COM O RUP**

Esta monografia foi julgada adequada à obtenção do grau de Especialista em Engenharia de Software e aprovada em sua forma final pelo curso de MBA em Engenharia 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. Leôncio Regal Dutra

Centro Universitário UNIEURO

**RESUMO**

A qualidade está cada vez sendo mais difundida dentro das grandes empresas, com propósitos de melhorar sua gestão e as negociações com seus clientes. Em questão, estaremos abordando como atingir qualidade no desenvolvimento de software utilizando como processo de engenharia o RUP. Confiabilidade, segurança, robustez e práticas deste processo de engenharia serão exemplificadas para fácil entendimento.

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 3

1.1. A Tecnologia da Informação e Sociedade da Informação 3

1.2. A Segurança da Informação e Comunicação 3

1.3. Gestão da Segurança da Informação 3

1.4. Proteção da Infra-estrutura Crítica no Governo do Brasil 3

1.5. O Modelo de Gestão de Segurança 3

1.6. A Gestão do Risco 3

1.7. Metodologia de Analise de Risco para a APF 3

1.8. A Metodologia OCTAVE 3

1.9. A Metodologia OCTAVE e o Gerenciamento de Projetos (PMBOK) 3

2. O MÉTODO OCTAVE 3

2.1. Objetivo e âmbito do método OCTAVE 3

2.2. Os Métodos de Implementação OCTAVE e OCTAVE-S 3

2.3. A Abordagem OCTAVE 3

2.5. A Abordagem de Três Etapas 3

2.6. Os Fundamentos do Método OCTAVE 3

2.7. Os Critérios do Método OCTAVE 3

**Índice de Tabelas**

Tabela 1-Comparação da abordagem OCTAVE e outras abordagens 3

Tabela 2 - Princípios e atributos no método OCTAVE 3

Tabela 3 - Saídas/resultados do método OCTAVE 3

**Índice de Figuras**

Figura 1 - Paradigma do gerenciamento de risco 3

Figura 2 Principais fases da OCTAVE (ALBERTS, OCTAVE Criteria v2.0). 3

Figura 3 - Áreas de influência do Método OCTAVE 3

Figura 4 - A abordagem OCTAVE e os três fatores chaves (ALBERTS, Introduction to the OCTAVE® Approach) 3

Figura 5 - As fases do método OCTAVE (ALBERTS, Introduction to the OCTAVE Approach) 3

# 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-estrura 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 coloborador.

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 agrega 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 conseqüência 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, *Operacional 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.

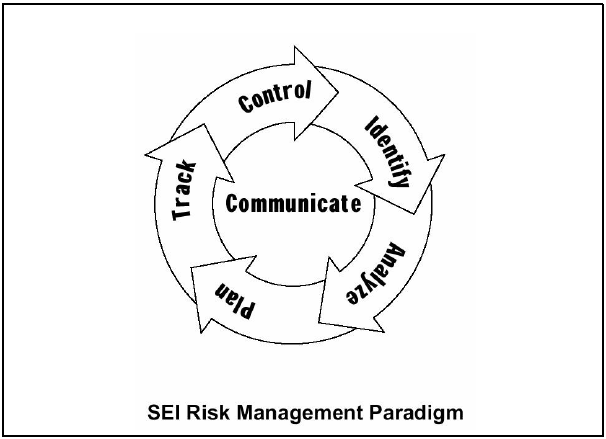


Figura - Paradigma do gerenciamento de risco

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 alinha com negócio da organização (ALBERTS,

*Introduction to the OCTAVE® Approach*).

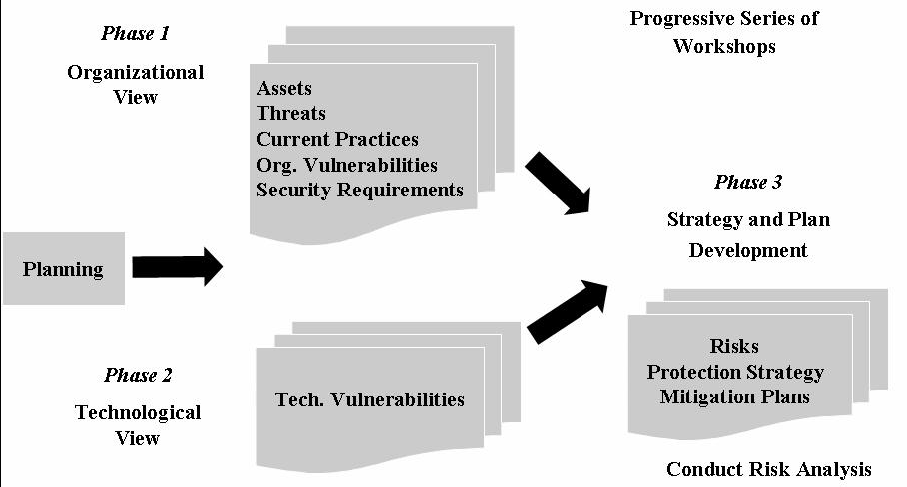


Figura Principais fases da OCTAVE (ALBERTS, OCTAVE Criteria v2.0).

• Fase 1. Visão organizacional.

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

o Processo 1: categoriza o conhecimento da gerência sênior;

o Processo 2: categoriza o conhecimento da gerência da área operacional;

o Processo 3: categoriza o conhecimento do “Staff”;

o 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:

o Processo 5: Identificação dos componentes-chaves: o analista identifica um conjunto representativo de componentes-chaves de um sistema que suporta os processos de negocio, é definida como uma abordagem para avaliação dos componentes-chaves da tecnologia empregada.

o 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:

o 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.

o 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 critica 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 - 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 Evaliation OCTAVE*

*®*. Embora a OCTAVE*®* não seja uma abordagem de Gestão dos Riscos especifica 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 Managemente: Na 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 comprimento 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.](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.

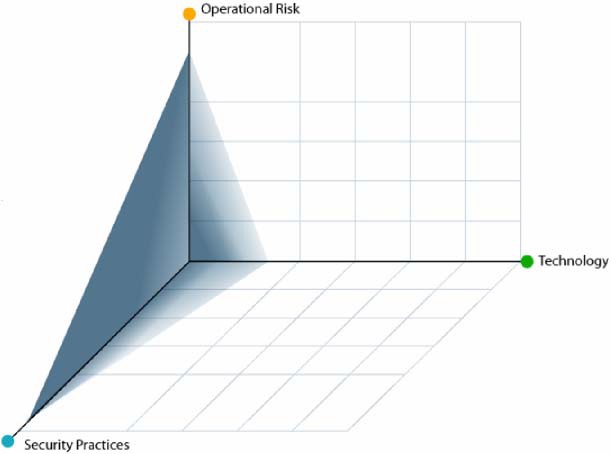


Figura - A abordagem OCTAVE e os três fatores chaves (ALBERTS, Introduction to the OCTAVE® Approach)

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 tácticas 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 -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 principio 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:

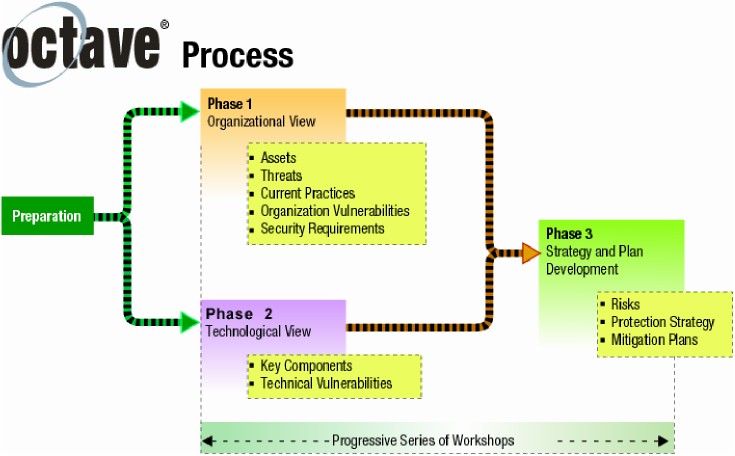


Figura 5 - As fases do método OCTAVE (ALBERTS, Introduction to the OCTAVE Approach)

• 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.

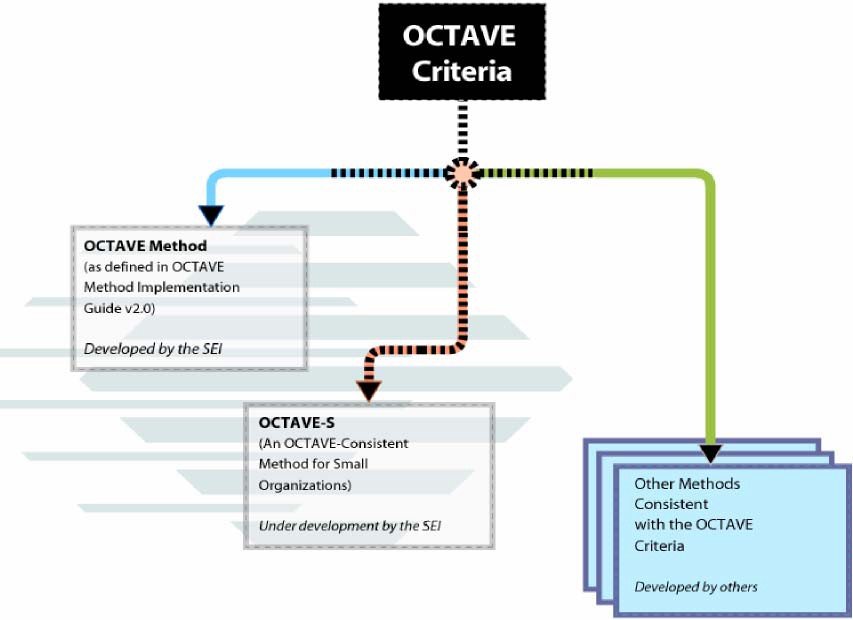


Figura 6 - Critérios da OCTAVE (ALBERTS, Introduction to the OCTAVE® Approach)

## 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 o conceito que significa de que forma uma categoria de pessoas dentro da Organização desenvolverá as suas atividades de avaliação, e nos conseqüentes 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 perpespectiva 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 - Princípios e atributos no método OCTAVE

|  |  |
| --- | --- |
| **Principio** | **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 |
| Catalogo de vulnerabilidades |
| Processo definido | Atividades de avaliação definidas |
| Resultados de avaliação documentados |
| Avaliação do escopo |
| Continuidade de processo | Descrição dos próximos passos |
| Catalogo de práticas |
| Visão voltada ao futuro | Foco no risco |
| Ações proativas |
| Foco nos elementos críticos  essenciais | Avaliação do escopo  Foco nas atividades |
| Gestão Integrada | Questões organizacionais e tecnológicas |
| Participação da área de negocio e da área da tecnologia da informação |
| Participação dos gerentes sênior |
| Comunicação aberta | Abordagem colaborativa |
| Perspectiva Global | Questões organizacionais e tecnológicas |
| Participação da área de negócio e da área da tecnologia da informação |
| Equipe de trabalho | 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 - 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 sumarizados 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 organizacão, 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.