Universidade Federal do Rio de Janeiro

Escola Politécnica

Curso de Gerência de Projetos em Sistemas de Informação
(GPSI)

Projeto para análise e implantação de um SOC na BR

Max Boaventura

GPSI

Abril de 2010

Universidade Federal do Rio de Janeiro

Escola Politécnica

Curso de Gerencia de Projetos em Sistemas de Informação (GPSI)

Projeto para análise e implantação de um SOC na BR

Autor:

_____

Max Boaventura

Orientador UFRJ:

_____

Prof. Flávio Mello, Ph. D.

Orientador Petrobras BR:

_____

Américo Batista de Araujo

Examinador(es):

_____

Prof Edilberto Strauss, Ph.D.

_____

Prof Flávio Luis de Mello, Ph.D.

GPSI

Abril de 2010

AGRADECIMENTO

Aos meus gestores pela oportunidade de melhoria e crescimento profissional e por acreditarem em mim e no meu trabalho.

RESUMO

Este trabalho visa demonstrar aspectos necessários e uma proposta de criação de um SOC interno a uma companhia, se beneficiando das vantagens de um ambiente in house.

Palavras-Chave: (SOC, Segurança da Informação)

SIGLAS

SOC – Security Operation Center

PMI – Project Management Institute

EAP – Estrutura Analitica do Projeto

PMBOK – Project Management Body of Knowledge

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

1.1 – Tema

Nos últimos anos tem sido grande a preocupação com a segurança da informação nas empresas. Muito tem sido feito para garantir o sigilo e a integridade da informação. Tentativas de fraudar ou prejudicar são diárias e constantes. Nesse aspecto é preciso monitorar os recursos e garantir a integridade destes, assegurando o correto funcionamento dos serviços e a disponibilidade da informação.

O monitoramento e correlação destes eventos de segurança torna-se algo extremamente difícil quando falamos de milhares destes por dia, sem as ferramentas adequadas e um processo para manter e tratar essas informações.

O SOC (*Security Operation Center*) tem como propósito reunir técnicas e ferramentas capazes de tratar e dar o correto direcionamento destas informações, garantindo um acompanhamento aos incidentes e correlacionamento da massa de dados gerada por todos os ativos computacionais do ambiente.

1.2 – Delimitação

A proposta deste trabalho é propor uma forma de criar um SOC interno à Petrobras Distribuidora, sugerindo um modelo de trabalho a ser aplicado na companhia.

Os trabalhos aqui apresentados se aplicam no atual momento vivido, estando ele sujeito a alterações futuras quando inserido em outro contexto.

1.3 – Justificativa

Há vários anos coletamos os dados e eventos gerados pelos dispositivos e aplicações encontrados no nosso ambiente, demandando um ponto focal para ajudar na visualização da infraestrutura como um todo. Crescente é também a necessidade de possuir todo o histórico associado a determinado ativo, permitindo perceber o seu "comportamento" ao longo do tempo.

O SOC fornece um logico ambiente para a análise e coleta de dados distribuídos para suportar a estratégia de defesa em profundida da empresa. Além de centralizar os eventos registrados estes também são inspecionados e correlacionados entre si, buscando informações não visíveis através de um único elemento, possíveis somente através do agrupamento destes. Essa correlação e visibilidade buscada permite responder a eventos ou incidentes relacionados a segurança através da tecnologia.

Assim, estabelecer tal estrutura viabiliza não somente o crescimento e maturação dos processos de Segurança da Informação na organização, mas também a aderência à padrões regulamentais adotados pela indústria e governo.

1.4 – Objetivos

O objetivo deste trabalho é propor uma avaliação e estudo, sob uma ótica prática do mercado, de um projeto e a implantação de um SOC nas instalações da BR, seguindo práticas conhecidas e difundidas em Gerência de Projetos.

1.5 – Metodologia

Este trabalho foi desenvolvido seguindo uma metodologia de pesquisa teórica e de melhores práticas utilizadas e difundidas no mercado, buscando embasar o trabalho com os conceitos e alimentá-lo com práticas de mercado.

1.6 – Descrição

Além deste capítulo introdutório, o qual apresenta o tema, sua justificativa, delimitação e objetivos, este trabalho foi organizado em mais quatro capítulos conforme detalhado a seguir.

O Capítulo 2 apresenta o embasamento teórico do projeto, abordando os temas: Segurança da Informação e em seguida uma elucidação sobre o que é o SOC.

O Capítulo 3 aborda uma proposta inicial com os principais elementos para implantação de um SOC às necessidades da companhia.

O Capítulo 4 traz uma primeira abordagem para o inicio do projeto.

O Capítulo 5 apresenta as conclusões da pesquisa e as recomendações para trabalhos futuros a serem realizados.

Capítulo 2

Embasamento Teórico

2.1 – Segurança da Informação

Segundo a NBR ISO/IEC 17799 informação é: “um ativo que, como qualquer outro ativo importante é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida.”[1]. Esta mesma também define segurança da informação como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.

A segurança da informação não é apenas uma questão de tecnologia, mas também uma questão de negócio que envolve uma correta gestão de riscos para proteger adequadamente a informação em todos os níveis da organização.

Segundo Charles P. [2], a segurança da informação busca proteger a informação dos riscos a que está exposta para garantir a confidencialidade, a integridade e a disponibilidade.

2.2 – SOC (*Security Operation Center*)

O aumento na sofisticação dos ataques de hackers e o risco interno estão levando as organizações a lidarem com a exposição aos riscos de maneira mais agressiva. Isso está testando a visão tradicional das operações de segurança – limitadas principalmente à coleta e análise de eventos de segurança – e ampliando o escopo das operações. Um recurso avançado atualmente precisa englobar a monitoração e a proteção de informações confidenciais, bem como a infraestrutura em que ele possa residir, e ser capaz de monitorar e emitir relatórios de riscos à segurança de informações de várias origens em toda empresa. Neste contexto é que nasce o SOC.

Apesar de simplório, um conceito que bem se encaixa à palavra SOC é o de um órgão central que entrega serviços de segurança.

Sua principal função é a de tentar previnir acessos não autorizados e gerenciar incidentes relacionados à segurança da informação usando processos e procedimentos. A grande missão é a gerência de risco através de analise centralizada usando recursos combinados, que consistem de pessoas, hardwares dedicados e softwares especializados, operando constantemente.

Os recursos citados oferecem a base para continuamente monitorar o ambiente realizando analise de riscos e garantindo proteção contra intrusões ao ambiente.

2.3 – Gerência de Projetos

O gerenciamento de projetos ou ainda administração de projetos é a aplicação de conhecimentos, habilidades e técnicas na elaboração de atividades relacionadas para atingir um conjunto de objetivos pré-definidos, num certo prazo, com um certo custo e qualidade, através da mobilização de recursos técnicos e humanos.

De acordo com o PMBOK [4], os processos de gerenciamento de projetos podem ser organizados em cinco grupos de processos:

1. **Processos de Iniciação** – autorização do projeto ou fase de prospecção.
2. **Processos de Planejamento** – são processos iterativos de definição e refinamento de objetivos e seleção dos melhores caminhos para atingir os objetivos.
3. **Processos de Execução** – execução dos planos do projeto: coordenação de pessoas e outros recursos para executar o plano
4. **Processos de Monitoramento e Controle** – medição e monitoramento do desempenho do projeto. Garantem que os objetivos do projeto são alcançados através do monitoramento e medição regular do progresso, de modo que ações corretivas possam ser tomadas quando necessário.
5. **Processos de Fechamento** – aceitação formal do projeto (com verificação de escopo) ou fase para a sua finalização.

Os grupos de processo são ligados pelos resultados que produzem: o resultado de um processo frequentemente é a entrada de outro. Os cinco grupos de processos possuem conjuntos de ações que levam o projeto adiante, em direção ao seu término.

Capítulo 3

Proposta Tecnológica

3.1 – Análise inicial – Missão e *Business Case*

Antes de decidir por construir um Centro de Operações em Segurança, faz-se necessário algum tempo para o planejamento. Esse planejamento muitas vezes trata apenas de pessoas, processos e componentes de tecnologia do projeto ignorando os norteadores fundamentais para a real necessidade do SOC, a sua razão e quais os problemas do negócio o SOC busca resolver. Antes da construção, os patrocinadores do projeto precisam olhar fundo no que de fato é a missão e *business case* para o SOC.

3.1.1 – Missão

Para definição e busca da missão do projeto é necessário definir requisitos e validá-los frente ao que se deseja. Antes da construção de um SOC, as perguntas abaixo devem ser respondidas:

- Que necessidades o SOC busca atender para a organização?
- Quais as tarefas atribuídas ao SOC?
- Quem são os consumidores das informações coletadas e analisadas? Que requisitos eles impõem?
- Quem é o patrocinador do projeto? Quem "venderá" o SOC para o resto da organização?
- Quais os tipos de eventos que serão alimentados do SOC para monitoramento?

3.1.2 – Business Case

A aprovação da construção do SOC deverá estar condicionada à definição de custo e estratégias para retorno desses custos. Investimentos em infraestrutura, pessoal,

educação e treinamento, tecnologias de monitoramento e adicionais necessárias ao funcionamento são itens que auxiliam no inicio dessa avaliação.

3.2 – Construção do Projeto

O projeto em questão propõe a construção de um SOC com enfoque na tríade de projetos de TI – pessoas, processos e tecnologia.

3.2.1 – Pessoas

As pessoas são parte na construção e sucesso de um projeto. Logo abaixo temos um organograma sugerido para a execução do projeto.

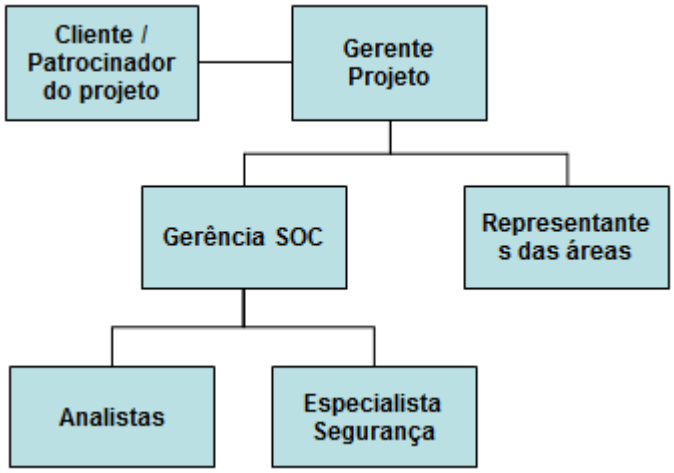

Figura 1 - Organograma

Um SOC normalmente é estruturado em um regime de 24x7x365, garantindo o monitoramento contínuo do ambiente. Tal estrutura deve possuir uma equipe para disponibilizar os serviços de forma continuada, dando o tratamento adequado aos eventos e seguindo os processos definidos.

Abaixo é sugerida uma implementação de alocação de recursos necessários à implantação do SOC, com uma visão da agenda semanal e mensal.

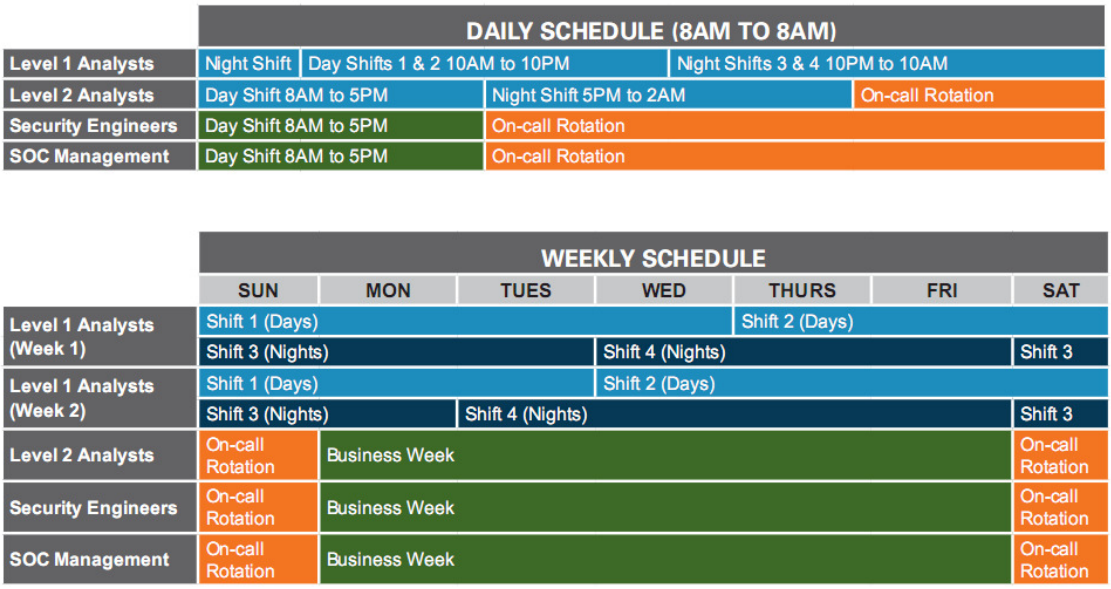

Figura 2 - Exemplo de alocação SOC 24x7x365
Fonte: ArcSight [3]

3.2.2 – Processos

Os processos atuam nos projetos como uma ligação entre a tecnologia e as pessoas que fazem uso desta para obtenção dos resultados e movem ambos de forma ordenada para a obtenção dos resultados.

Para de fato alcançar tais resultados é preciso maturidade nos processos. Maturidade na gerência do processo é inicialmente alcançada com repetição e processo contínuo de melhoramento.

Devido ao fato da necessidade de um grande número de processos, é sugerida uma subdivisão e uma organização hierárquica, demonstrando uma dependência entre processos [3]. São 4 (quatro) os grupos de processos [3]: Processos de negócio, responsável por documentar todos componentes administrativos e de gerenciamento requeridos para a operação do SOC; Processos Tecnológicos, que mantém as informações relacionadas à administração de sistemas, gerência da configuração e projeto conceitual; Processos operacionais, responsáveis por documentar os mecanismos da operação diária do SOC; e por último, Processos analíticos, que englobam todas as atividades de criadas para detectar e melhor entender os eventos maliciosos.

Desta forma, como demonstrado na *Figura 3*, *métricas* suportam *melhoras nos processos*, *projetos tecnológicos* e *gerência de eventos* suportam análise de intrusão e assim por diante.

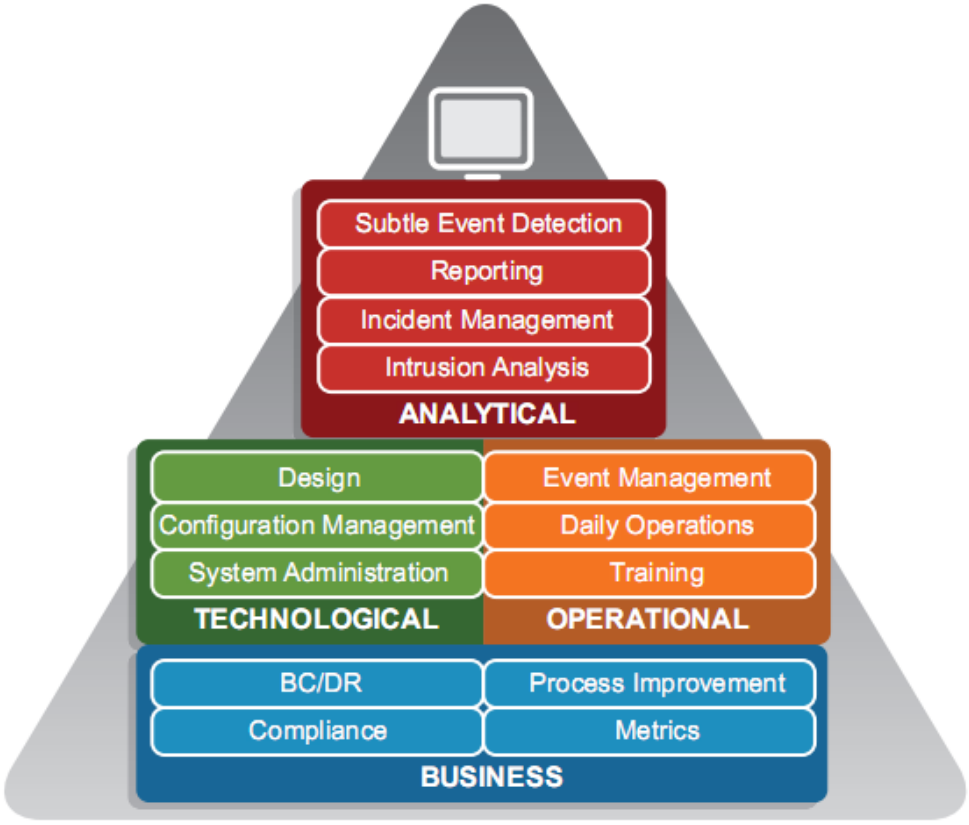

Figura 3 - Hierarquia de Processos
Fonte: ArcSight [3]

Após definidos os grupos, os processos serão definidos e enquadrados em cada um deles para suportar a operação do SOC. A *Tabela 1* exemplifica processos enquadrados em cada área.

Tabela 1 - Exemplo de Processos por Grupo

CATEGORIA DE PROCESSOS	PROCESSO	PROCEDIMENTO	DESCRIÇÃO DO PROCEDIMENTO
BUSINESS	Reporte de Métricas	Reportar KPIs	Define os passos envolvidos no reporte dos KPIs do SOC
TECHNOLOGY	Administração de Sistemas	Gerência de acesso ao usuário	Passos necessários para solicitar, aprovar e conceder acesso a ferramentas do SOC
OPERATIONAL	Gerência de Eventos	Reportar Eventos	Descreve como os eventos devem ser escalados entre as equipes
ANALYTICAL	Análise de Intrusão	Classificar Ameaça	Procedimento para classificar corretamente a ameaça

3.2.3 – Tecnologia

Grande parte do trabalho do SOC está na identificação dos eventos relevantes para análise dentre os milhares de eventos gerados por todo o ambiente.

O trabalho do SOC baseia-se na análise correlacionada destes eventos, e do reporte dos significativos à equipe que dará o correto tratamento. Analisar cada item da estrutura em busca das evidências é algo trabalhoso e pouco produtivo para um grande ambiente, tornando-se indispensável uma ferramenta capaz de coletar e correlacionar tais eventos. As soluções de SIEM (*Security Information and Event Management*) auxiliam nesse trabalho e são atualmente uma das principais ferramentas que compõem um SOC.

O SIEM torna-se essencial pois ele é capaz de agregar, correlacionar, realizar analises históricas e automatizar respostas a eventos importantes lidando com os riscos do mundo digital atual.

Todo o volume de dados coletados deve ser inserido numa base de dados que será consultada para análise, visualização, investigação e relatórios. Após essa etapa, o SIEM será responsável por normalizar, categorizar e correlacionar os dados

provenientes dos diversos ativos que compõem o ambiente. Nesse processo será também aplicada uma lógica de priorização para identificar a relevância do alvo que gerou o evento para o negócio.

Capítulo 4

Estrutura Proposta para o Projeto

4.1 – Elementos propostos

Neste capítulo será mostrado um esboço de artefatos iniciais produzidos na fase de planejamento do projeto, que compõem a proposta do projeto de implantação seguindo as práticas estabelecidas pelo PMI.

Tais documentos visão ser o catalizador para o início do projeto e execução do mesmo, não sendo uma proposta final para o este, devendo esse ser ainda estudado mais a fundo para uma análise ainda mais abrangente.

4.2 – EAP

A EAP, ou Estrutura Analitica do Projeto, é uma visão do projeto divido por pacotes. Tais pacotes são uma macro descrição das tarefas que o compõem e auxiliam na visualização do projeto como um todo, servindo como referencia base para consultas a respeito da estrutura do projeto.

A Figura 4 abaixo exibe a EAP elaborada para este projeto.

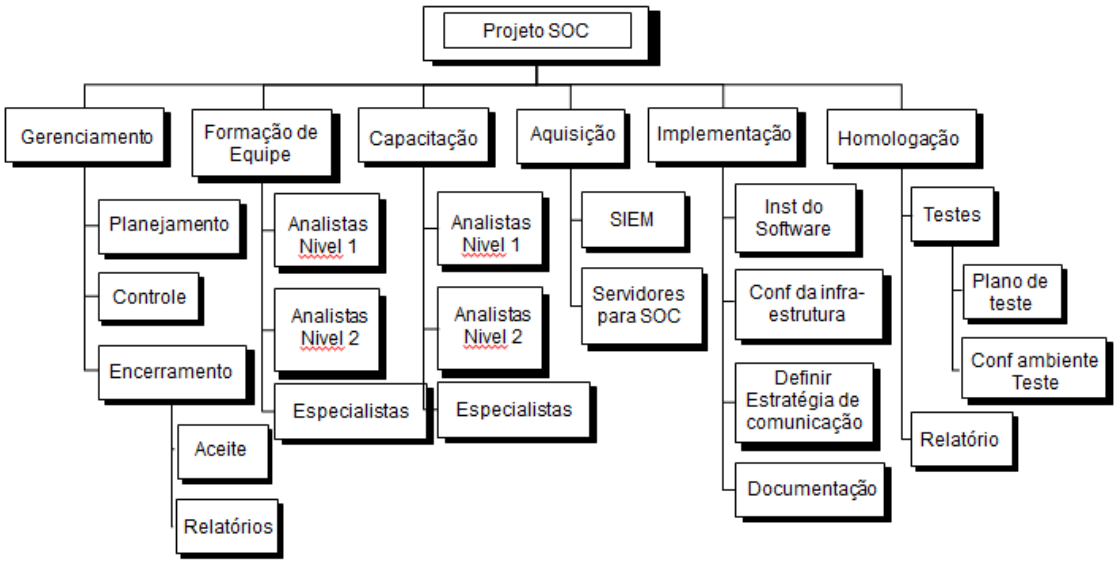

Figura 4 - EAP Projeto

4.3 – Marcos do Projeto

Um cronograma de marcos traz uma grande visão dos principais eventos de um projeto, demonstrando de forma sucinta o macro cronograma do projeto.

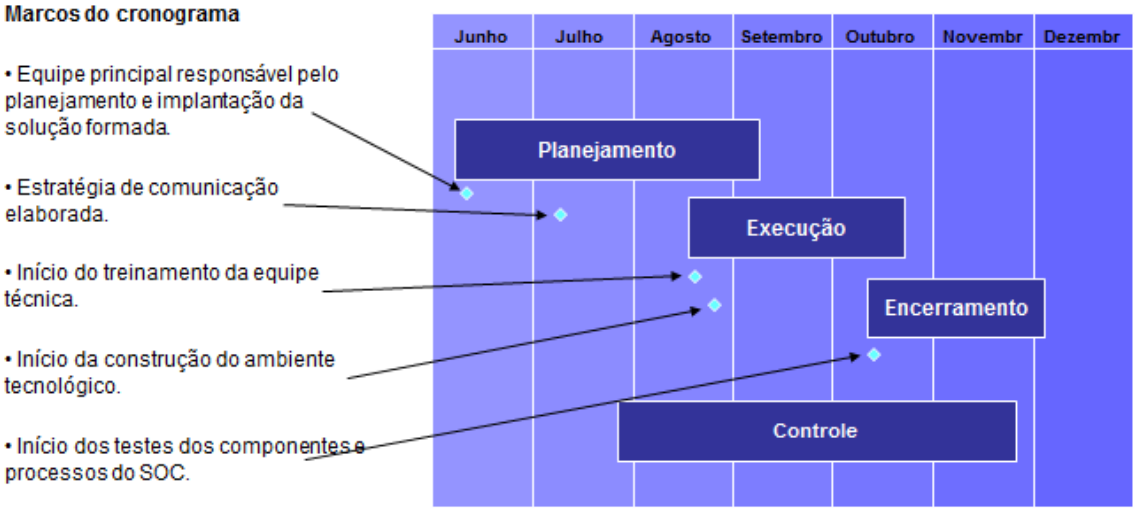

Figura 5 - Marcos do Projeto

4.4 – Estimativas de custos e seus desembolsos

Tal projeto possui um custo total estimado demostrado através dos seus desembolsos planejados, mas que podem ser revistos frente a uma adequação de escopo antes do início do projeto.

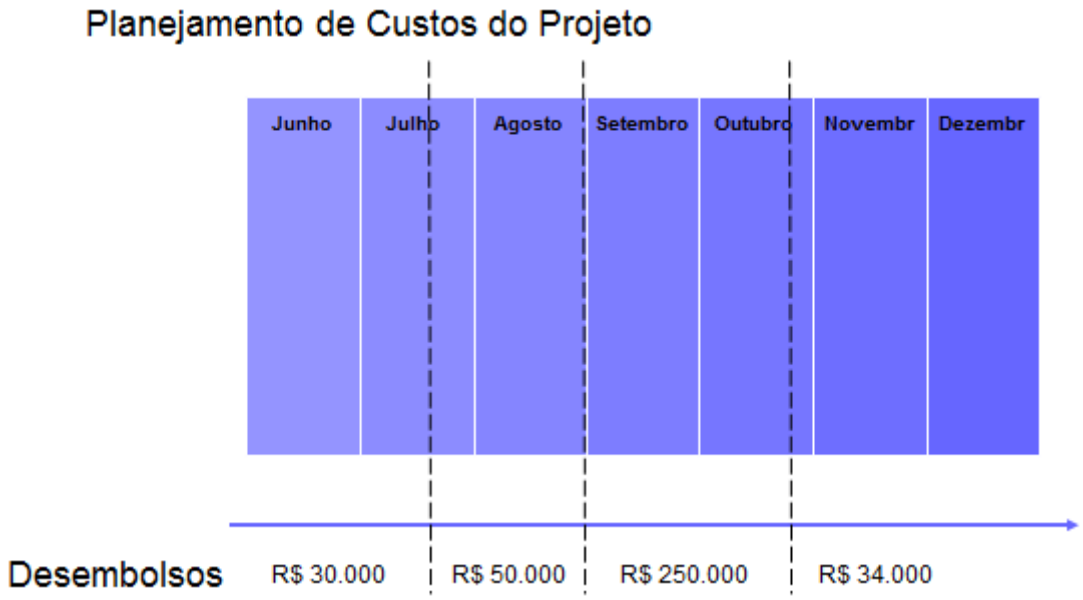

Figura 6 - Plano inicial de custos

Capítulo 5

Conclusão e Trabalhos Futuros

5.1 – Conclusão

Projetar, construir e gerenciar um Centro de Operações de Segurança interno pode melhorar a habilidade da organização em rapidamente reconhecer e responder a eventos de segurança da informação maliciosos. Um SOC pode também auxiliar em garantir um valor agregado para os constantes investimentos realizados ao longo do tempo em tecnologias de segurança e atender às regulamentações impostas pelo mercado e pelo governo.

Focando no desafio de implementar e orquestrar os elementos principais – Pessoas, Processos e Tecnologia – irá garantir a implementação do SOC para efetivamente e eficientemente reconhecer e responder a eventos maliciosos.

5.2 – Trabalhos Futuros

O presente estudo não se esgota com as propostas apresentadas. Propõe-se contribuir para as discussões sobre o tema no âmbito da empresa pesquisada. Diante disto, a corroboração ou contestações aos trabalhos propostos poderão aprimorar ações de melhorias sob a perspectiva da evolução para um modelo mais abrangente e mais completo, contribuindo para um melhor resultado.

Novos estudos podem ser feitos na busca da relação da governança e gestão, além de análises sobre o modelo atual em que se propõem a construção interna.

Dada a amplitude do tema segurança da informação e sua importância estratégica para o negocio, outros estudos podem ainda ser desenvolvidos buscando responder questões como:

- Identificar ações de governança para proteger ativos;

- Investigar e identificar fatores que justifiquem um modelo outsourcing para o projeto;
- Pesquisar e definir novos modelos além dos trazidos aqui.

Finalmente, analisando o cenário atual da companhia, sugere-se como proposta de trabalhos futuros o processo de ações de melhorias da segurança da informação na empresa a qual é sugerida o trabalho.

Bibliografia

[1] ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Norma NBR ISO/IEC 17799: Tecnologia da informação – Código de prática para a gestão da segurança da informação.** Rio de Janeiro, 2001.

[2] PFLEEGER, Charles P., **Security in Computing.** Second Edition, Editorial Precision Graphic Services Inc. NJ 07458. 1997. USA

[3] ArcSight, Inc., "**Building a Successful Security Operations Center**", http://www.arcsight.com/library/download/building-a-successful-soc, (Acesso em 1 Outubro de 2010).

[4] PMBOK®: Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos, Terceira edição, 2004. 405p.Uma Norma Nacional Americana ANSI/PMI 99-001-2004.

BIDOU, Renaud, "**Security Operation Center Concepts & Implementation",** http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.93.8577&rep=rep1&type=pdf (Acesso em 5 de Outubro de 2010).

WIKIPIDIA, "security operations center", http://en.wikipedia.org/wiki/Security_Operations_Center, (Acesso em 1 Outubro de 2010).