Uma Metodologia Seis Sigma para Implantação de uma Gestão de Segurança da Informação Centrada na Percepção dos Usuários

Maria Angélica Figueiredo Oliveira[1], Raul Ceretta Nunes[1], Cristiane Ellwanger[1]

[1] Grupo de Gestão e Tecnologia em Segurança da Informação
Universidade Federal de Santa Maria (UFSM)
Av. Roraima n° 1000 – Camobi – Santa Maria/RS – Brasil – CEP:97105-900
mariaangelicafo@gmail.com,cereta@inf.ufsm.br,cristianeellwanger@yahoo.com.br

Abstract. *Currently, one can found a number of methodologies, models and frameworks to implement an information security management. However, they do not address the users' critical features in the implementation. This paper proposes a Six Sigma based methodology for manage the information security, where the management is based on data and evidences generated by users. The proposed methodology was applied in a case study involving two hospital units and the results demonstrate the effectiveness of the methodology: an improvement of 43,8% on information security quality perceived by users and an increasing of 47,3% on subject understanding. Its application contributes to achieving a systemic security management.*

Resumo. *Atualmente, existe uma série de metodologias, modelos e frameworks para a implantação da gestão da segurança da informação. No entanto elas não direcionam a implantação para as características críticas do usuário. Este artigo propõe uma metodologia de gestão da segurança da informação baseada na abordagem Seis Sigma, a qual é fundamentada em dados e evidências gerados pelos usuários. A metodologia proposta foi aplicada em um estudo de caso envolvendo duas unidades hospitalares e os resultados demonstram a efetividade da metodologia: uma melhora de 43,8% na qualidade da segurança da informação percebida pelos usuários e um aumento de 47,3% no nível de entendimento sobre o tema. Sua aplicação contribui para o gerenciamento sustentável da segurança da informação.*

1. Introdução

O interesse pela gestão da segurança da informação vem aumentando no mesmo limiar do surgimento de novas ameaças advindas de diferentes meios, sejam elas humanas ou tecnológicas. Este interesse pode ser observado através de mudanças visíveis no cenário organizacional, onde há um maior amadurecimento sobre a necessidade de investir em segurança da informação. A disseminação de normas e padrões de segurança, bem como a união das principais normas e padrões de segurança numa única série de normas (série ISO/IEC 27000) que visa a certificação, também contribui neste sentido. No entanto,

mesmo havendo essa maturação, ainda continua presente a cultura do somente tratar os problemas quando estes acontecem, agindo de forma reativa, provocando uma ilusão de que atuando desta maneira as soluções são encontradas mais rapidamente, o que acaba se transformando em um "círculo vicioso" dentro da organização (Sveen et al. 2008).

Para evitar o "circulo vicioso" gerado pela gestão de segurança de forma reativa, a adoção de uma metodologia baseada num ciclo de melhoria contínua para guiar o processo de Gestão de Segurança da Informação é inevitável. Vermeulen e Solms (2002) apresentam uma metodologia na forma de *framework* para guiar o processo de implantação da gestão de segurança da informação. O framework é baseado numa ferramenta denominada ISMTB (*Information Security Management ToolBox*), que consiste em uma série de questionários baseados nos controles da norma BS 7799-1 (1999). Os questionários auxiliam no processo de conhecimento e caracterização da organização, identificando o nível de segurança atual e servindo para determinar que medidas de segurança devem ser tomadas a partir deste diagnóstico. Porém, a metodologia de Vermeulen e Solms está direcionada ao sucesso da fase de implantação e não inclui de maneira clara um ciclo de melhoria contínua. Por outro lado, Martins e Santos (2005) apresentam uma metodologia baseada no ciclo de melhoria continua PDCA (*Plan, Do, Check, Act*) onde a padronização e documentação dos procedimentos, ferramentas e técnicas são tidas como elemento central. Neste sentido apontam como fundamental a criação de indicadores e registros, bem como a definição de um processo educacional contínuo de conscientização dentro da organização e seus parceiros. Observa-se que o enfoque desta metodologia é na documentação e conscientização. Procurando enfocar mais o contexto ambiental da organização, Brooks e Warren (2006) apresentaram uma metodologia de evolução de segurança da informação baseada na modelagem UML (*Unified Modelling Language*). A intenção é representar o cenário de aplicação usando UML para mapear a interação das atividades com o sistema, a fim de permitir análises que obtenham dados que revelem o nível de segurança ideal para aquele ambiente.

Com a padronização de uma metodologia com ciclo de melhoria contínuo, tal como orienta a norma NBR ISO/IEC 27001 (2006), o problema não está mais no "como fazer", pois a maior parte das metodologias auxilia nesta tarefa, mas sim no "como manter" todas as mudanças geradas pelas melhorias empregadas com a implantação da gestão. Neste sentido, a fragilidade das metodologias normalmente está no tratamento ao componente humano [Silva e Stein 2007], essencial para obter a sustentação da segurança da informação [Kiely e Benzel 2005], a nova preocupação em gestão de segurança da informação [Saleh et al. 2007][Sveen et al. 2008].

Pessoas são consideradas o grande pilar de sustentação de qualquer mudança organizacional [Snee 2007]. Desta forma não basta ter uma metodologia de gestão de segurança da informação que apenas guie o processo de implantação de segurança, mas é necessário que ela seja também centrada nas características críticas das pessoas ou dos usuários, pois são elas que vão manter toda e qualquer melhoria que for implantada. Por essa razão a necessidade de uma metodologia que atenda esse princípio é fundamental. Sveen et al. (2008) apontam para uma filosofia de gestão que reúne princípios derivados da gestão da qualidade total, sendo a abordagem Seis Sigma [Pyzdek 2003] apontada como uma solução para garantir esse principio [Aazadnia e Fasanghari 2008]. O Seis Sigma segue uma filosofia que direciona todas as ações de melhorias aos dados gerados pelas pessoas, ou seja, seu foco é nas características críticas observadas pelos usuários.

Este artigo propõe uma metodologia de implantação de uma gestão de segurança da informação baseada na abordagem Seis Sigma, na qual é explicitado ferramentas da qualidade que podem ser utilizadas em cada fase da metodologia. O intuito da metodologia é garantir uma gestão sustentável da segurança da informação com qualidade, mantendo os usuários motivados. Para atender seu objetivo, a metodologia proposta é conduzida pelo ciclo de melhoria contínua do método DMAIC (Definir, Medir, Analisar, Implementar e Controlar), base operacional do Seis Sigma, e produz uma gestão fundamentada em dados e evidências gerados através das ferramentas da qualidade selecionadas. Desta forma ao invés de indicar o "como fazer" a metodologia aponta o "como manter", possibilitando o aumento na qualidade dos processos, a efetividade e a sustentação da gestão da segurança da informação.

O artigo está organizado como segue. A seção 2 apresenta os principais conceitos de gestão da segurança da informação e a seção 3 apresenta a abordagem Seis Sigma e o método DMAIC. A seção 4 apresenta e detalha a metodologia proposta e a seção 5 descreve resultados de sua aplicação. Finalmente, a seção 6 apresenta as conclusões.

2. Gestão de Segurança da Informação

Existem muitas definições de segurança da informação presentes na literatura sob várias óticas sejam elas humanos, tecnológicas ou gerenciais, onde na área tecnológica uma das mais tradicionais diz respeito à proteção da integridade, disponibilidade e confidencialidade. Porém, segurança da informação deve ser entendida como uma postura gerencial que ultrapassa a tradicional abordagem tecnológica e que promove uma visão embasada em conceitos sociais para sua correta cobertura [Marciano e Marques 2006]. Neste sentido, o que se percebe é que para obter sustentabilidade no processo de gestão da segurança da informação é necessário envolver aspectos humanos, tecnológicos e gerenciais [Kiely e Benzel 2005].

Esta discussão a cerca dos aspectos norteadores da segurança da informação são fortemente destacados nas normas de Gestão de Segurança da Informação que promovem amplamente os seus conceitos dentro das organizações através da orientação sobre controles, processos, políticas e procedimentos, que juntos fortalecem os objetivos do negócio com a minimização dos seus riscos.

Embora existam diversas normas que auxiliam a organização a prover a segurança da informação, a NBR ISO/IEC 17799 (2005) é umas das melhores práticas da área [Tashi e Ghernaouti-Hélie 2007], tendo sido incorporada na série de normas ISO/IEC 27000 como ISO/IEC 27002. É difícil falar de segurança sem referenciar esta norma, já que os benefícios de sua aplicação são vastos como: proteção da informação, continuidade dos negócios, aumento da competitividade, atendimento aos requisitos legais, manutenção e aumento da reputação e imagem da instituição. Assegurar a proteção da informação é um princípio base para que qualquer organização forneça um serviço de credibilidade, organizado e controlado independentemente do meio de armazenamento da informação seja ela eletrônica ou em papel. A certeza de se ter um dado confiável precisa estar alinhada de tal forma a proporcionar: confidencialidade, integridade e disponibilidade.

A NBR ISO/IEC 27001 (2006) é uma norma que orienta a segurança sugerindo um Sistema de Gestão de Segurança da Informação (SGSI) dentro da organização, ao

contrário da NBR/ISO IEC 17799 que é apenas um guia que recomenda as melhores práticas no que tange à segurança da informação. A NBR ISO/IEC 27001 promove a adoção de uma abordagem de processo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI. Mantendo o SGSI relacionado ao plano de negócios estratégico a norma visa um aumento no nível de credibilidade da segurança presente na organização. A norma propõe 134 controles divididos em 11 tópicos todos alinhados com a NBR ISO/IEC 17799, sendo eles: 1 - Política de segurança; 2 - Segurança Organizacional; 3 - Classificação e controle de ativos de informação; 4- Segurança em pessoas; 5 - Segurança ambiental e física; 6 - Gerenciamento das operações e comunicações; 7 - Controle de acesso; 8 - Desenvolvimento e manutenção de sistemas; 9 - Gestão de incidentes de segurança; 10 - Gestão da continuidade do negócio; e, 11 – Conformidade.

O desenvolvimento do SGSI preconizado pela NBR ISO/IEC 27001 segue a abordagem de processo de melhoria contínua para condução de toda a gestão de segurança, e para isto utiliza o método PDCA (*Plan, Do, Check, Act*), que parte do princípio que para gerenciar adequadamente um processo é necessário (P) planejar, (D)executar, (C) verificar e (A) agir [Fenz et al. 2007].

Ainda que a NBR ISO/IEC 27001 tenha evoluído em comparação com NBR/ISO IEC 17799, onde se recomenda o método PDCA que prevê a continuidade da gestão a partir da melhoria contínua, existe pouco apoio na implementação da prática destas normas, ou seja, a norma dá ciência de "o que" precisa ser feito, mas não esclarece "o como" deve ser feito. Para cobrir esta lacuna diferentes abordagens e metodologias podem ser adotadas, assim como a proposta neste artigo. Porém é importante salientar que o uso do DMAIC não descaracteriza a padronização da norma, pois o que a norma recomenda de fato é a adoção de um ciclo de melhoria contínua.

3 Seis Sigma

Seis sigma [Perez-Wilson 1999] é uma filosofia de gestão (derivada da gestão para qualidade total) que visa promover ações para melhoria contínua e sustentabilidade com foco no usuário (interno ou externo). O termo Seis Sigma corresponde a variação mínima desejada dos processos que tem impacto para o cliente, tendo como meta a redução de defeitos em produtos ou serviços em 3.4 defeitos (equivalente aos 6σ desejados, onde σ é o grau de variabilidade) por milhão de oportunidades [Blauth 2003]. Esta seção apresenta como o Seis Sigma e seu método DMAIC se estruturam para alcançar seu objetivo.

3.1 A Abordagem Seis Sigma

O conceito do Seis Sigma está apoiado em dois pilares [Rotondaro et al. 2006] (vide Figura 1): o primeiro pilar representa os dados gerados pelas características críticas definidas pelo cliente interno e externo, onde observa-se que as pessoas são essenciais; o segundo representa a gestão realizada por processos guiados por um método robusto de trabalho. Estes pilares caracterizam a abordagem como não somente um esforço em busca da qualidade, mas também um processo para melhoria de toda organização envolvendo diretamente as pessoas.

Na prática, o Seis Sigma pode ser considerado um conjunto de ferramentas que possibilitam mudar o modo de trabalho enfatizando dados observados e evitando

decisões baseadas apenas em intuição [Motwani e Kumar 2004]. Para conseguir isto o Seis Sigma sugere a formação de um time de trabalho efetivo para que sua implementação seja bem sucedida [Pyzdek 1999], pois as pessoas são consideradas como pilar de sustentação para o alcance de resultados num processo de mudança organizacional.

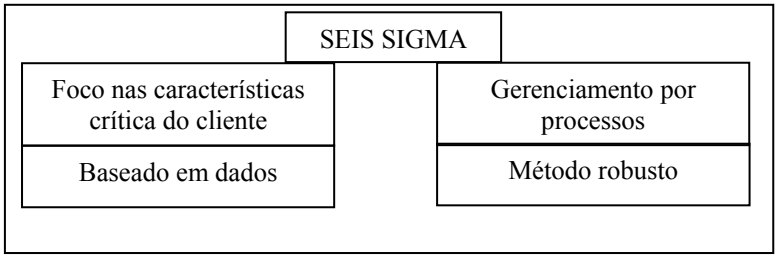

Figura 1 - Pilares da abordagem Seis Sigma. Fonte: [Rotondaro et al. 2006]

O mesmo princípio de equipe encontrado no Seis Sigma também é considerado em uma gestão de segurança da informação, onde equipe similar é denominada comitê de segurança. A Tabela 1 ilustra a relação da equipe de trabalho Seis Sigma com a equipe de trabalho relacionada ao comitê de segurança [Oliveira et al. 2008], onde observa-se a similaridade entre os papeis, mas o melhor detalhamento de papeis nas definições do Seis Sigma. Quando aplicadas a segurança da informação, ambas equipes tem como principal responsabilidade o desenvolvimento e o incentivo da segurança da informação através de ações que a promovam.

Tabela 1. Relação da equipe de trabalho Seis Sigma com o Comitê de Segurança. Fonte: [Oliveira et al. 2008]

Equipe de Trabalho Seis Sigma	Equipe de Trabalho da Gestão de Segurança da Informação	Função
Executivo líder	Comitê de Segurança da Informação-Membros da Diretoria da Organização	Incentivar e supervisionar a aplicação da metodologia na organização.
Campeão	Chefes de Setores ou divisões	Prover aproximação da equipe e o desdobramento da implementação do Seis Sigma por toda a organização
Master Black Belt	Implementadores da Segurança da Informação	Auxiliar os chefes de setores na escolha e treinamento de novos projetos de melhoria, treinar e instruir os Black Belts e Green Belts
Black Belt	Implementadores da Segurança da Informação	Implantar a Segurança da Informação
Green Belt	Implementadores da Segurança da Informação	Implantar a Segurança da informação e auxiliar os Black Belts

3.2 O Método DMAIC

Existem muitas referências na literatura sobre o DMAIC, acrônimo para as fases Definir-Medir-Analisar-Implementar-Controlar, sendo que é muito comum encontrar denominações caracterizando-o como uma metodologia de solução de problemas [Aguiar 2006]. Porém, o DMAIC também pode ser entendido como um modelo [Blauth 2003][Pyzdek 2003] ou como um método [Snee 2007] sistematizado de melhoria contínua de processos. Neste artigo o DMAIC é referenciado como método, pois a abordagem Seis Sigma o adota como seu método de melhoria contínua.

O Seis Sigma adota o método DMAIC porque ele define uma estrutura disciplinada e rigorosa para alcançar a qualidade, a qual assume-se prover menos desperdícios por trabalhar em função dos fatores chaves para o processo, resultando em uma maior eficiência no alcance das metas [Snee 2007]. Como a norma NBR ISO/IEC 27001 (2006) sugere o uso do método PDCA, também muito utilizado em sistemas de gestão, é importante frisar suas similaridades. De fato, conforme ilustra a Figura 2, o que se verifica é que há apenas variações nas atividades das fases, as quais dão maior ênfase em uma ou outra etapa da cada método. Por exemplo, enquanto a fase Planejar do PDCA é extremamente abrangente, o DMAIC detalha ações equivalentes em quatro de suas cinco fases, alcançando mais especificidade. Por outro lado, o PDCA detalha mais as ações correspondentes as fases Implementar e Controlar do DMAIC. Enfim, salienta-se o fato de ambos os métodos serem equivalentes [Aguiar 2006]. Deste modo, mesmo resolvendo adotar a abordagem Seis Sigma, se a organização já faz uso do PDCA, pode-se mantê-lo, pois a organização já está familiarizada com ele. Pelo mesmo motivo, mesmo a norma NBR ISO/IEC 27001 indicando o PDCA, uma certificação por essa norma não será afetada se a organização adotar o método DMAIC.

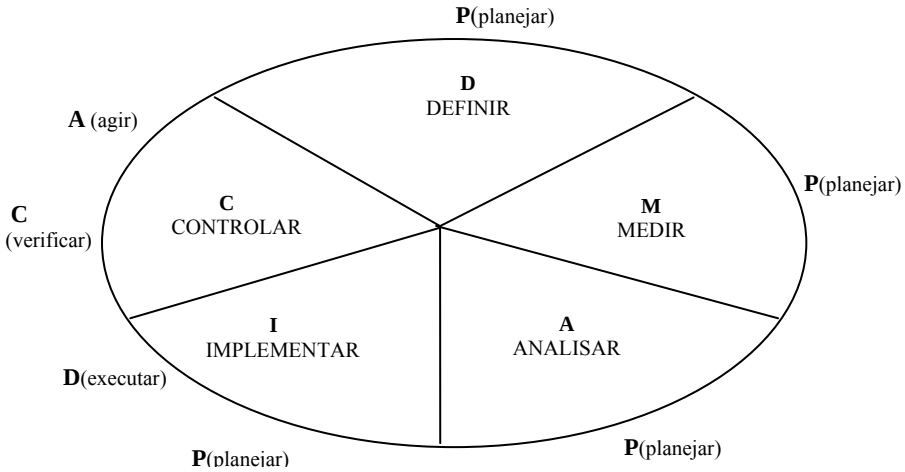

Figura 2 – Relação do DMAIC com o PDCA. Adaptado de [Aguiar 2006].

4 Metodologia de Implantação da Gestão da Segurança da Informação

A metodologia proposta nesta seção segue a filosofia da abordagem Seis Sigma, tendo como base de implementação o método DMAIC. Por seguir os princípios do Seis Sigma

a metodologia é centrada nas expectativas dos clientes (dados), neste artigo referenciado como usuários. Os dados são gerados a partir do uso de ferramentas da qualidade consolidadas, fazendo com que toda a gestão seja direcionada para o que realmente é necessário. A Figura 3 apresenta uma síntese da proposta de implantação através de uma seqüência de passos com objetivos, a metodologia que consiste nas ferramentas, técnicas e procedimentos que serão empregados, e os resultados esperados. O detalhamento correspondente a cada uma das fases DMAIC é apresentado a seguir.

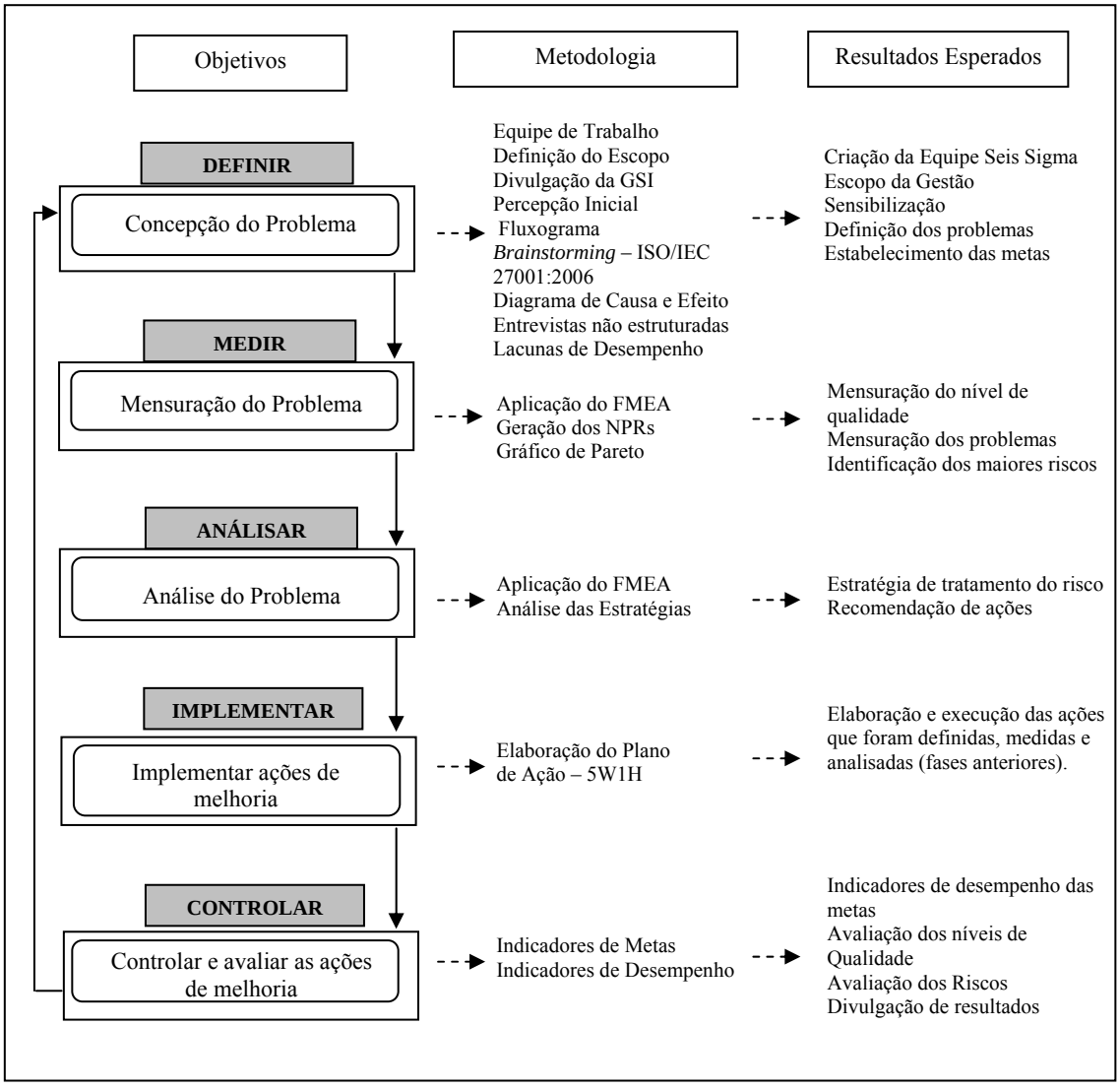

Figura 3 - Metodologia de Implantação de Gestão de Segurança da Informação.

4.1 Primeira Fase: Definição

A primeira fase da metodologia, correspondente a fase Definição do DMAIC, deve trabalhar a concepção do problema, ou seja, deve definir o escopo da gestão e do problema a ser solucionado, bem como estabelecer as metas do projeto e a equipe Seis Sigma que deverá alavancá-lo. O primeiro passo deve ser formar a equipe Seis Sigma e traçar um planejamento de cronograma que prevê o tempo necessário para cada fase do

projeto, a fim de orientar e conduzir a equipe para trabalhar dentro de um limiar de tempo.

A visão STOPE [Saleh et al. 2007] é utilizada nessa fase com o objetivo de estabelecer que a gestão tenha uma visão sistêmica, abrangendo aspectos estratégicos, tecnológicos, organizacionais, pessoas e o ambiente da organização. Esta visão também deve permear a composição da equipe Seis Sigma, tornando-a multidisciplinar com apoio de diversas áreas.

Além disso, para realizar uma gestão centrada na percepção dos usuários, a busca pela definição dos problemas e pelo estabelecimento das metas faz uso de ferramentas da qualidade. As ferramentas sugeridas para esta fase são: o *brainstorming*, o fluxograma [Aguiar 2006], o diagrama de Causa e Efeito [Rotondaro et al. 2006], as entrevistas e as Lacunas de Desempenho [Lovelock e Wright 2001]. O *brainstorming* visa a reunião de pessoas para gerar idéias ou sugestões em um menor espaço de tempo possível. O fluxograma e o diagrama de causa e efeito visam auxiliar a visualização das etapas do processo e dar suporte as análises dos problemas. As entrevistas são muito eficientes para escutar a "voz do cliente" [Rotondaro et al. 2006]. As lacunas de desempenho são um meio para capturar dos usuários os *gaps* em relação a percepção existente sobre o problema e a expectativa de solução para ele, podendo ser realizadas através de questionários.

4.2 Segunda Fase: Mensuração

A fase de mensuração tem objetivo de identificar as características críticas para a qualidade. É através da mensuração que se descobre o que de fato precisa ganhar uma atenção maior, pois é considerado crítico para a obtenção da meta desejada. Desta forma nesta fase são realizadas ações com base nas informações capturadas na fase Definir com o intuito de avaliar o quanto o processo abordado é importante e quais os pontos do processo devem ser tratados com maior ênfase.

A mensuração dos processos requerida nesta fase se confunde com a prática de gestão de riscos recomendada pela NBR/ISO 17799:2005, sendo considerada uma das partes mais importantes na implantação da gestão da segurança da informação. Por esta razão aconselha-se que a mensuração seja realizada com auxílio de ferramentas da qualidade para melhor capturar as reais necessidades das organizações. Há duas ferramentas que podem auxiliar nesta fase [Rotondaro et al. 2006]: a FMEA (*Failure Mode and Effect Analyses*), que realiza análise do modo e efeito das falhas e gera um número de prioridade de risco (NPR); e o diagrama de Pareto, o qual serve como modo de visualização dos NPRs e possibilita identificar os aspectos considerados relevantes (índices de riscos).

4.3 Terceira Fase: Análise

Identificado os maiores índices de riscos, a fase de análise visa estabelecer prioridades de ações para cada aspecto ou problema considerado relevante, priorizando o tratamento do risco através do entendimento das relações entre as causas e os efeitos. Como os dados para esta fase foram derivados da ferramenta FMEA, ela também pode auxiliar nesta fase. Salienta-se que a análise realizada nesta fase deve considerar não apenas os riscos, mas também a viabilidade para tratá-lo, ou seja, escolha dos problemas que serão

tratados irá depender não somente do risco que organização corre por estar exposto a este problema, como também a sua viabilidade de resolução.

4.4 Quarta Fase: Implementação

A quarta fase é responsável pelo planejamento e execução das ações que foram definidas, medidas e analisadas. É nesta fase que as soluções para os problemas são desenvolvidas e mudanças são realizadas para resolver tais problemas. Os resultados das mudanças no processo podem ser observados através de medições, sobre as quais a organização pode julgar se as mudanças foram realmente benéficas, ou se o projeto merece ser reavaliado [Nave 2002].

Algumas perguntas podem ser feitas nesta fase como meio de buscar um andamento para a implantação das melhorias, como por exemplo, (1) Quais as ações ou idéias possíveis que podem permitir a eliminação das causas fundamentais do problema? (2) Quais dessas idéias se traduzem em soluções potenciais? (3) Que soluções permitirão o alcance da meta? (4) De que forma testar as soluções escolhidas como meio de assegurar sua eficácia e de que forma impedir a ocorrência de "efeitos colaterais"? Deste modo, para auxiliar nesta atividade indica-se a ferramenta 5W1H [Aguiar 2006], acrônimo de *What*, *Who*, *When*, *Where*, *why* e *How*, desenvolvida para ser utilizada como referência em todas de decisões. A ferramenta permite que seja feito o acompanhamento do desenvolvimento do projeto, bem como serve de documento que, de forma organizada, identifica as ações e as responsabilidades pela sua execução. A ferramenta também pode auxiliar no estabelecimento de um cronograma da implementação das medidas a serem executadas.

4.5 Quinta Fase: Controle

O propósito desta fase do DMAIC é assegurar que os benefícios obtidos na fase Implementar seja de fato prosseguido na organização. A manutenção das melhorias implantadas só se dá através do controle, sendo necessário verificar se as ações que foram aplicadas resultaram ou não na eliminação do problema. Para fornecer este controle, é proposto a utilização de indicadores de meta e indicadores de desempenho [Santos 2006]. Os indicadores de desempenho definem o quão bem está o desempenho dos processos em relação a meta desejada, e o indicadores de meta definem se o resultado esperado no início do projeto Seis Sigma, com as definições de metas, foi alcançado. A fase Controlar e caracterizada como a última do método DMAIC, e é considerada uma etapa chave para a continuidade do projeto, pois como o princípio da filosofia Seis Sigma é a de estar sempre monitorando, é a partir dela que começa realmente a transformação Seis Sigma e a sustentação das melhorias.

Ao chegar na fase Controlar é importante realizar a divulgação das melhorias aos usuários. Esta prática serve de elemento motivador para que as pessoas, maiores envolvidos nesta mudança e agentes no processo de gestão da segurança da informação, se tornem mais conscientes e, consequentemente, contribuam pela manutenção das melhorias e pela sustentação da segurança.

5 Aplicação da Metodologia e Análise dos Resultados

A metodologia proposta neste artigo (seção 4) foi implantada no Hospital Universitário de Santa Maria (HUSM). A instituição estabelece-se, hoje, como um Centro de Ensino,

Pesquisa e Assistência no âmbito das Ciências da Saúde no estado do Rio Grande do Sul, prestando serviços de saúde a mais de 100 municípios da região. Como o HUSM abrange muitos setores aos quais se subdividem em 28 serviços, foram selecionadas, juntamente com a direção do hospital, duas unidades que se caracterizam por serem vitais para instituição e que necessitavam de uma gestão de segurança da informação, a Unidade de Cardiologia Intensiva (UCI) e Unidade de Terapia Intensiva (UTI).

Para a implantação da gestão da segurança da informação foi composta uma equipe de trabalho Seis Sigma dividida entre funcionários lotados nas duas unidades, diretores do hospital e implementadores, sendo estes últimos especialistas em segurança da informação e sem vínculo com a instituição.

Aplicação da metodologia foi realizada num período de 12 meses e realizou dois ciclos. Como resultado, foi atingido as metas estabelecidas na primeira fase do projeto as quais resultaram no documento da Política de Segurança da Informação e na definição de um Programa de Conscientização em Segurança da Informação. Além do cumprimento dessas metas, a gestão se mostrou eficiente em termos de eliminação de problemas, já que dos 19 problemas identificados durante a fase de definição, todos tiveram ações implantadas para sua redução ou eliminação, resultando na conseqüente minimização dos riscos causados por estes problemas.

Cabe salientar que uma das razões que fez a gestão atingir suas metas foi exatamente o trabalho colaborativo que se criou entre a equipe Seis Sigma e os usuários, pois todos tiveram oportunidade de participar principalmente através da aplicação periódica da técnica de *brainstorming*. A divulgação de resultados parciais também foi um dos elementos motivadores e um ponto muito importante para a gestão, uma vez que através desses resultados os funcionários se sentiram parte integrante do processo de gestão, ficando evidente que todos contribuíram para que as mudanças acontecessem gradativamente. A figura 4 revela esta constatação, a partir do nível de qualidade percebido pelos funcionários.

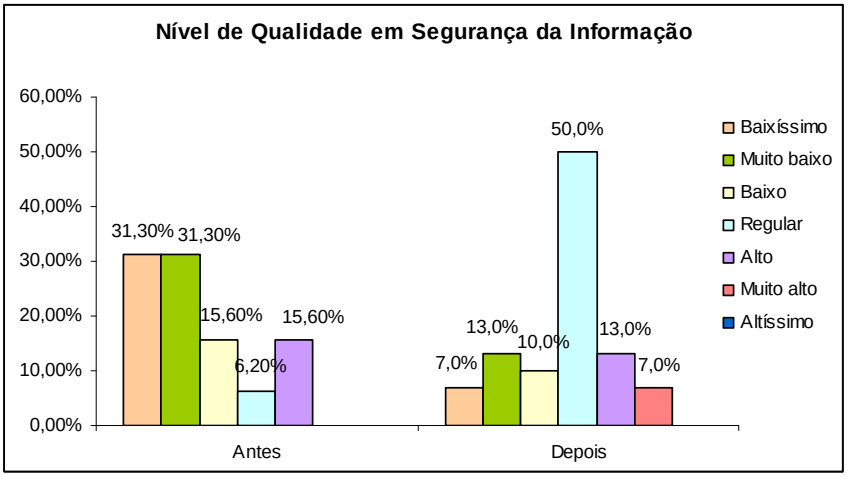

Figura 4 – Nível de Qualidade antes e após as melhorias

A avaliação ilustrada na Figura 4 foi realizada com 30 usuários, onde foi questionado sobre o nível de qualidade da segurança da informação percebido. Antes das melhorias os níveis "Baixíssimo" e "Muito baixo" correspondiam a 62,6% das

respostas. Depois das melhorias esse índice caiu para 20%. A mudança mais visível ficou na opção Regular, tendo sido 43,8% maior na segunda avaliação após as melhorias. Outro ponto observado foi na opção "Muito Alto", que na primeira avaliação, antes das melhorias, não havia sido mencionada e na segunda avaliação representou 7 % das respostas. Em síntese, as avaliações demonstraram uma boa aderência à gestão de segurança e uma melhora significativa na percepção de qualidade de segurança da informação.

Outra avaliação realizada foi sobre o entendimento dos usuários com o tema segurança da informação. Por ser uma instituição da área da saúde a questão do nivelamento dos usuários foi um dos itens mais citados nas ferramentas da fase Definir. Por esta razão, o Programa de Conscientização em Segurança da Informação foi definido como uma das metas do projeto. A figura 5 mostra as duas avaliações antes e após as melhorias. Antes das melhorias as opções "Alto", "Muito Alto" e "Altíssimo" representavam 15,7%, número considerado baixo para a realidade das unidades. Após as melhorias esse índice teve um acréscimo satisfatório, somadas as três opções, saltando para 63%, indicando um aumento de 47,3% no entendimento do tema pelos usuários. Salienta-se que o aumento obtido no nível de entendimento em segurança da informação pelos usuários é muito importante para manutenção da gestão, tendo em vista que o seu entendimento reflete também no comportamento dos usuários.

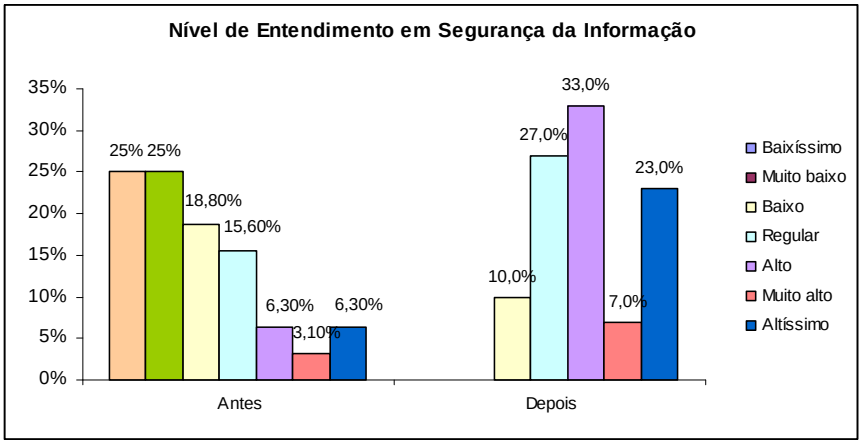

Figura 5 – Nível de Entendimento em SI antes e após a melhorias

6 Conclusões

No gerenciamento de informações, a segurança é um elemento chave para garantir a confiabilidade, integridade e disponibilidade dos dados. No entanto ela precisa ser tratada com uma visão abrangente dentro das organizações e não apenas como um problema tecnológico. Contudo, para a segurança da informação ser efetiva, ela também necessita estar envolta a um processo bem delineado com etapas bem definidas e com objetivos e metas traçados a partir de uma base gerencial organizada que possibilite a sua sustentabilidade.

Este artigo apresentou uma proposta de metodologia para implantação da gestão de segurança da informação, a qual adota uma visão sistêmica abrangendo aspectos

estratégicos, tecnológicos, organizacionais, de pessoas e de ambiente (visão STOPE) alinhada a abordagem direcionada a dados Seis Sigma. Sendo o Seis Sigma centrado nas características críticas percebidas pelos usuários, a metodologia de gestão proposta potencializa a sustentabilidade da segurança da informação comprometendo os usuários com a implantação da gestão da segurança.

A metodologia foi testada num estudo de caso envolvendo as unidades de Cardiologia Intensiva (UCI) e Terapia Intensiva (UTI) do Hospital Universitário de Santa Maria e demonstrou eficiência em seus resultados. Aplicando a metodologia, a qualidade na segurança da informação percebida pelos usuários aumentou 43,8% se comparado com uma avaliação realizada antes da aplicação da metodologia. A qualidade também aumentou 47,3%, quando considerado o nível de entendimento dos usuários sobre o papel da segurança da informação. O aumento do nível de entendimento é importante, pois reflete no comportamento das pessoas, o que contribui para formação de uma consciência coletiva e para a sustentação da gestão da segurança da informação. A metodologia apresentada está servindo como referência para especificação e desenvolvimento de um sistema computacional de apoio a gestão da segurança da informação.

Referências

Aazadnia, M., Fasanghari, M. (2008) "Improving the Information Technology Service Management with Six Sigma". *IJCSNS International Journal of Computer Science and Network Security*, v.8, n.3.

Aguiar, Silvio. (2006) "Integração das Ferramentas da Qualidade ao PDCA e ao Programa Seis Sigma". Nova Lima: INDG Tecnologia e Serviços Ltda.

Blauth , Regis. (2003) "Seis Sigma: Uma estratégia para melhorar resultados". *Revista FAE,* Business, n.5, abril.

Boynton, B. C. (2007) "Identification of Process Improvement Methodologies with Application in Information Security". *Information Security Curriculum Development*. Conference'07, September 28-29, Kennesaw, Georgia, USA.

Brooks, W.; Warren, M. (2006) "A Metodology of Health information Security Evaluation". *Health Care and Informatics.* Review Online.

Fenz, S.; Goluch G.; Ekelhart A.; Riedl, B.; Weippl, E. (2007) "Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard". *IEEE Computer & Society*. 13th IEEE International Symposium on Pacific Rim Dependable Computing.

BS7799-1 (1999) "Information security management – code of practice", British Standard Institute, London.

BS7799-2 (2002) "Information security management – specification with guidance for use", British Standard Institute, London.

Kiely, L.; Benzel, T. V. (2005) "Systemic Security Management". *IEEE Security & Privacy*, pp. 74-77.

Lovelock, C. e Wright, L. (2001) "Serviços: marketing e gestão". São Paulo: Saraiva.

Marciano, J. L. P, Marques, M. L. (2006) "O Enfoque Social da Segurança da Informação". *Revista Ciência da Informação*, v.35, n.3, p.89-98, set/dez 2006.

Martins, A. B.; Santos. C.A.S. (2005) "Uma Metodologia para implantação de um Sistema de Gestão de Segurança da Informação". Revista de Gestão e Tecnologia e Sistema de Informação. v. 2, n. 2, pp. 121-136.

Motwani, J.; Kumar, A.J. (2004) "A business process change framework for examining the implementation of six sigma: a case study of Dow Chemicals". *The TQM Magazine*, York, England, v.16, n.4, p.273-283.

Nave, Dave. (2002) "How to compare Six Sigma, Lean and the Theory of Constraints: a framework for choosing what´s best for your organization". *Quality Engineering*. v. 35, n. 3, p. 73-78, mar.

NBR ISO/IEC 17799:2005. (2005) "Tecnologia da Informação: Código de Prática para Gestão da Segurança da Informação". ABNT. Rio de Janeiro.

NBR ISO/IEC 27001 (2006). "Tecnologia da Informação. Sistema de Gestão da Segurança da Informação". ABNT. Rio de Janeiro.

Oliveira, M. A. F.; Nunes, R. C.; Amaral, E. H.; Zen, E.; Pereira, S. N. (2008) "Uma Metodologia de Gestão de Segurança da Informação direcionada a Riscos baseado na Abordagem Seis Sigma". Encontro Nacional de Eng. de Produção, Rio de Janeiro.

Perez-Wilson, Mario. (1999) "Seis Sigma: compreendendo o conceito, as implicações e os desafios". Rio de Janeiro: Qualitymark.

Pyzdek, T. (2003) "The Six Sigma HandBook". McGraw-Hill: New York.

Rotondaro. R. G.; Ramos, A. W.; Ribeiro, C.; Myake, D. I.; Nakano, D.; Laurindo, F. J. B.; Ho, L. L.; Carvalho, M. M.; Braz, M. A.; Balestrassi, P. P. (2006) "Seis Sigma. Estratégia Gerencial para a Melhoria de Processos, Produtos e Serviços". Atlas: São Paulo.

Saleh, M. S.; Alrabiah, A.; Barkry, S. H. (2007) "Using ISO 17799:2005 information security management: a STOPE view with six sigma approach". *International Journal of Network Management*, v.17, p. 85–97.

Santos, A. B. (2006) "Modelo de Referência para estruturar o programa de qualidade seis sigma: proposta e avaliação". Tese - (Doutorado em Engenharia de Produção). Universidade Federal de São Carlos.

Silva D. R. P e Stein, L. M. (2007) "Segurança da informação: uma reflexão sobre o componente humano". Ciências & Cognição, v. 10, p. 46-53.

Snee, Ronald. 3.4 (2007) "Per Million: Use DMAIC to Make Improvement Part of The Way We Work". Quality Progress.

Snee, Ronald D. (2001) "Dealing with the Achilles Heel of Six Sigma initiatives: Project selection is key to success". Quality Progress. v. 34, n. 3, p. 66-72.

Sehwail, L. e DeYong, C. (2003) "Six Sigma in HelthCare". *Jornal of Health Care Quality Assurance imcorporating Leadership in Health Services*. v. 16, n. 4, p. 1-5.

Solms, R. V. e Solms, B. V. (2004) "From policies to culture". *Computers and Security*, 23(4): 275–9.

Sveen, F. O.; Torres, J. M.; Sarriegi, J. M. (2008) "Learning from Your Elders: A Shortcut to Information Security Management Success". *Computer Safety, Reliability and Security*. v. 4680, p. 224-237.

Tashi, I.; Ghernaouti-Hélie, S. (2007) "Security metrics to improve information security management". *Proceedings of the 6th Annual Security Conference*. Apr. 11-12, Las Vegas, NV.

TCSEC, Department of Defense. (1985) "Trusted Computer System Evaluation Criteria". December. Disponível em <http://www.radium.ncsc.mil/tpep/library/rainbow/index.html> Acesso em Jan. 2008.

Vermeulen, C.; Solms, R.V. (2002) "The information security management tollbox – taking the pain out of security management". *Information. Management & Computer Security*. 10/3, p. 119-125.