UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

IMPLANTAÇÃO DE UMA GESTÃO DA SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA ABORDAGEM SEIS SIGMA

Dissertação de Mestrado

Maria Angélica Figueiredo Oliveira

Santa Maria, RS, Brasil

2009

IMPLANTAÇÃO DE UMA GESTÃO DA SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA ABORDAGEM SEIS SIGMA

por

Maria Angélica Figueiredo Oliveira

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-Graduação em Engenharia de Produção, Área de Concentração em Qualidade e Produtividade, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Mestre em Engenharia de Produção**.

Orientador Prof. Dr. Raul Ceretta Nunes

Santa Maria, RS, Brasil
2009

Endereço: Rua Cândido Portinari, 250, apto 02, Camobi, Santa Maria-RS
Fone: (55) 99111202; Endereço eletrônico: mariaangelicafo@gmail.com

Universidade Federal de Santa Maria
Centro de Tecnologia
Programa de Pós-Graduação em Engenharia de Produção

A Comissão Examinadora, abaixo assinada,
aprova a Dissertação de Mestrado

IMPLANTAÇÃO DE UMA GESTÃO DA SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA ABORDAGEM SEIS SIGMA

elaborada por
Maria Angélica Figueiredo Oliveira

como requisito parcial para obtenção do grau de
Mestre em Engenharia de Produção

COMISSÃO EXAMINADORA:

_____
Dr. Raul Ceretta Nunes - UFSM
(Presidente/Orientador)

_____
Dr. José Eduardo Malta de Sá Brandão - IPEA

_____
Dr. Marcos Cordeiro d'Ornellas - UFSM

Santa Maria, 2009.

*Aos meus pais **Gui** e **Claudi**,*
pelo apoio incondicional em todas as horas.

Agradecimentos

Primeiramente a Deus, que sempre esteve presente, dando a força necessária para seguir em frente.

Ao meu orientador, Dr. Raul Ceretta Nunes, pela amizade, compreensão, dedicação e incentivo em todos os momentos.

Aos professores e colegas do Curso de Pós-Graduação em Engenharia de Produção e ao Grupo de Pesquisa de Gestão e Tecnologia em Segurança da Informação da UFSM. Meu agradecimento especial a colega e amiga Cristiane Ellwanger por toda ajuda, empenho e incentivo dado em todos os momentos e ao colega Érico Hoff do Amaral pelo auxílio dado na concepção e condução do trabalho.

Aos Funcionários e Diretores do Hospital Universitário de Santa Maria - HUSM, pelo apoio durante a realização do trabalho.

Aos meus pais Claudi e Guiomar, pelo apoio incondicional em todos os momentos.

Enfim, agradeço a todos os demais que, de uma forma ou de outra, contribuíram para a conclusão deste trabalho.

SUMÁRIO

CAPÍTULO 1 - INTRODUÇÃO 16

1.1 Motivação 17

1.2 Problema de Pesquisa 18

1.3 Objetivo Geral 18

1.4 Objetivos Específicos 19

1.5 Organização da Dissertação 19

CAPÍTULO 2 - REFERENCIAL TEÓRICO: FUNDAMENTAÇÃO CONCEITUAL SOBRE GESTÃO DA SEGURANÇA DA INFORMAÇÃO 20

2.1 Segurança da Informação 20

2.1.1 Ativos da Informação 22

2.1.2 Ameaças 23

2.1.3 Vulnerabilidades 23

2.1.4 Incidentes 23

2.1.5 Riscos 24

2.1.6 Escopo da Segurança 28

2.1.7 Política de Segurança da Informação 30

2.1.8 Conscientização em Segurança da Informação 31

2.1.9 Comitê Gestor de Segurança da Informação 33

2.2 NBR/ISO IEC 17799:2005 e NBR ISO/IEC 27001 33

2.3 Metodologias de Gestão da Segurança da Informação 36

2.4 Conclusões Parciais 40

CAPITULO 3 - REFERENCIAL TEÓRICO: FUNDAMENTAÇÃO CONCEITUAL SOBRE SEIS SIGMA 42

3.1 Seis Sigma 42

3.1.1 Seis Sigma como abordagem estatística 44
3.1.2 Seis Sigma como abordagem estratégica 45
3.2 Método DMAIC 47
3.2.1 Fase Definir 49
3.2.1.1 Equipe de Trabalho 50
3.2.1.2 Brainstorming 51
3.2.1.3 Entrevistas 52
3.2.1.4 Fluxograma 53
3.2.1.5 Diagrama de Causa e Efeito 53
3.2.1.6 Lacuna de Desempenho (*gaps*) 54
3.2.2 Fase Medir 56
3.2.2.1 FMEA (Failure Mode and Effect Analyses) 57
3.2.2.2 Diagrama de Pareto 60
3.2.2.3 Box-Plot 61
3.2.3 Fase Analisar 62
3.2.3.2 Histogramas 62
3.2.3.3 *Fault Tree Analysis* (FTA) 63
3.2.4 Fase Implementar 64
3.2.4.1 Plano de Ação - 5W1H 64
3.2.5 Fase Controlar 65
3.3 Conclusões Parciais 67
CAPITULO 4 - PROPOSTA DE IMPLANTAÇÃO DE UMA GESTÃO DA SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA ABORDAGEM SEIS SIGMA 68
4.2 Planejamento das Fases 69
4.2.1 Fase Definir 70
4.2.2 Fase Medir 71
4.2.3 Fase Analisar 72
4.2.4 Fase Implementar 73
4.2.5 Fase Controlar 73
4.3 Condução das Fases do Projeto - Cronograma 74
4.4 Conclusões Parciais 74
CAPITULO 5 - IMPLANTAÇÃO DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA ABORDAGEM SEIS SIGMA 76
5.1 Caracterização da Organização 76

5.3.1 Equipe de Trabalho 78
5.3.2 Definição do Escopo 79
5.3.2.1 Divulgação da Gestão da Segurança da Informação 79
5.3.3 Percepção Inicial 80
5.3.4 Fluxograma 83
5.3.5 Brainstorming 86
5.3.6 Entrevistas 90
5.3.7 Diagrama de Causa e efeito 93
5.3.8 Lacunas de desempenho (*Gap*) 95
5.3.9 Aspectos Gerais da fase Definir 100
5.4 Fase Medir 102
5.3.1 Mensuração do Nível de Qualidade e Entendimento em SI 103
5.3.2 FMEA (*Failure Model and Effect Analysis*) 105
5.3.3 Aspectos Gerais da Fase Medir 108
5.4 Fase Analisar 108
5.4.1 Aspectos Gerais da Fase Analisar 111
5.5 Fase Implementar 111
5.5.1 5W1H – Plano de Ação 112
5.5.2 Primeira Meta implantada - Comitê Gestor de Segurança da formação 115
5.5.3 Segunda Meta implantada - Programa de Conscientização em Segurança da Informação 115
5.5.4 Terceira Meta implantada - Política de Segurança da Informação 116
5.5.5 Aspectos Gerais da Fase Implementar 117
5.6 Fase Controlar 117
5.6.1 Desempenho Comitê Gestor de Segurança da Informação 118

5.6.2 Desempenho do Programa de Conscientização em Segurança da Informação 118
5.6.3 Desempenho da Política de Segurança da Informação 119
5.6.4 Avaliação dos Níveis de Qualidade 121
5.6.5 Avaliação dos Riscos 123
5.6.6 Divulgação dos Resultados 124
5.6.7 Aspectos Gerais da Fase Controlar 125

5.7 Cronograma 125

5.8 Conclusões Parciais 127

CAPITULO 6 - CONCLUSÕES 130
TRABALHOS FUTUROS 133

REFERÊNCIAS BIBLIOGRÁFICAS 134

APÊNDICE A 142
APÊNDICE B 144
APÊNDICE C 146
APÊNDICE D 149
APÊNDICE E 151
APÊNDICE F 155
APÊNDICE G 161
APÊNDICE H 163
APÊNDICE I 165
APÊNDICE J 172
APÊNDICE L 174
APÊNDICE M 180
APÊNDICE N 182
APÊNDICE O 189

LISTA DE TABELAS

Tabela 1- Integração STOPE com a ISO/IEC 17799:2005 29
Tabela 2- Controles NBR ISO/IEC 27001:2006 34
Tabela 3- Relação da Equipe de trabalho com a GSI 51
Tabela 4- Índice de Severidade 59
Tabela 5- Índice de Ocorrência 59
Tabela 6- Índice de Detecção 59
Tabela 7- Cronograma de Previsão do Projeto 74
Tabela 8- Composição da equipe Seis Sigma 79
Tabela 9- Pesquisa de comprometimento com as mudanças 82
Tabela 10- Resultado Brainstorming 87
Tabela 11- Obtenção dos Gaps 98
Tabela 12- Relação dos Problemas 102
Tabela 13- FMEA - Estratégias e ações recomendadas 109
Tabela 14- Plano de Ação 113
Tabela 15- Cronograma de Previsão e Realização do Proejeto Seis Sigma 126

LISTA DE FIGURAS

Figura 1 - Gerenciamento de Riscos 26
Figura 2 - Risco Residual 27
Figura 3 - Abordagem Stope 29
Figura 4 - Proposta de Metodologia da SGSI 37
Figura 5 – Framework de Gestão da Segurança da Informação 39
Figura 6 - As bases da Abordagem Seis Sigma 43
Figura 7 - Definições Seis Sigma 46
Figura 8 - Método DMAIC de Controle de Processos 48
Figura 9 - Relação do DMAIC com PDCA 49
Figura 10 - Diagrama de Causa e Efeito 54
Figura 11 - Formulário FMEA 58
Figura 12 - Box Plot 61
Figura 13 - Histograma 63
Figura 14 - Plano de Ação - 5W1H 65
Figura 15 - Síntese da proposta de implantação da Gestão da Segurança da Informação 70
Figura 16 - Índice de importância dos Controles de Segurança 81
Figura 17 - Comprometimento com as mudanças 82
Figura 18 - Fluxograma Unidade de Cardiologia Intensiva - UCI (HUSM) 84
Figura 19 - Fluxograma Unidade de Terapia Intensiva - UTI (HUSM) 85
Figura 20 - Sessões de Brainstorming 87
Figura 21 - Diagrama de Causa e Efeito 94
Figura 22 - Exemplo deQuestionário de Percepção de Segurança da Informação 97
Figura 23 - Gráfico de dispersão da Dimensão Funcionários 99
Figura 24 - Gráfico de dispersão da Dimensão Diretores 99
Figura 25 - Gráfico de dispersão da Dimensão Implementadores 100
Figura 26 – Maiores Gaps 100
Figura 27 - Nível da Qualidade da Segurança da Informação 104
Figura 28 - Nível de Entendimento em Segurança da Informação 104
Figura 29 - Formulário FMEA 106
Figura 30 - Gráfico de Pareto 106
Figura 31 - Avaliação da Conscientização em Segurança da Informação 119
Figura 32 - Avaliação Ambiente Convencional 120

Figura 33 - Avaliação Ambiente Computacional 121
Figura 34 - Relação da qualidade antes e depois das melhorias..... 122
Figura 35 - Relação do Entendimento em SI antes e depois das melhorias..... 123
Figura 36 - Relação dos NPRs 1º e 2º Avaliação 124

LISTA DE SIGLAS

SI – Segurança da Informação
GSI – Gestão da Segurança da Informação
DMAIC – Definir-Medir- Implementar- Controlar
TI – Tecnologia da Informação
CFM – Conselho Federal de Medicina
HUSM – Hospital Universitário de Santa Maria
IEC – *International Electrotechnical Commission*
ISO – *International Organization for Standardization*
NBR – Norma Brasileira Reguladora
SAME – Serviço de Arquivo Médico e Estatística
SUS – Sistema Único de Saúde
UCI – Unidade de Cardiologia Intensiva
UTI – Unidade de Terapia Intensiva
FMEA – *Failure Model and Effect Analysis*
CGSI – Comitê Gestor de Segurança da Informação

RESUMO

Dissertação de Mestrado
Programa de Pós-Graduação em Engenharia de Produção
Universidade Federal de Santa Maria

IMPLANTAÇÃO DE UMA GESTÃO DA SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA ABORDAGEM SEIS SIGMA

AUTOR: MARIA ANGÉLICA FIGUEIERDO OLIVEIRA
ORIENTADOR: DR. RAUL CERETTA NUNES
Data e Local da Defesa: 03 de Março de 2009, Santa Maria

A segurança, atualmente, é o elemento chave para garantir um dado confiável, integro e disponível, no entanto ela precisa ser vista de forma abrangente na organização e não somente um problema que se refere a área de TI. Pesquisas atuais apontam para uma nova preocupação, o da sustentação da segurança da informação, principalmente por que para minimizar os riscos e controlar as melhorias é necessário que a organização esteja apoiada em uma base sólida que gere esta sustentação. O Seis Sigma é visto como uma das soluções que direcionam a essa sustentação por ser considerado uma abordagem que promove a qualidade através do princípio de melhoria contínua, sendo as pessoas o principal agente para esta promoção. Embora haja estudos que recomendem o Seis Sigma, nenhum deles define como a abordagem poderia ser utilizada ou de que forma as ferramentas da qualidade poderiam ser aplicadas no contexto da segurança. Deste modo, atendendo a esta lacuna, a proposta de implantação apresentada nesta dissertação traz o planejamento de todas as fases de implantação de uma gestão de segurança da informação, estruturadas através do método DMAIC, base operacional do Seis Sigma, conjuntamente com a definição de ferramentas da qualidade e procedimentos que podem ser utilizados em cada uma das fases. O Planejamento de todas as fazes detiveram o foco no cliente interno ou usuário, portanto, as ferramentas e procedimentos propostos tiveram como intento atender a este objetivo, gerando uma gestão baseada em dados, imprimindo com mais veracidade, a realidade e os anseios da organização. A implantação da proposta teve como cenário de aplicação as Unidades de Cardiologia Intensiva e Terapia Intensiva do Hospital Universitário de Santa Maria - HUSM. O resultado da implantação contribuiu para o aumento de 43,8% da qualidade da segurança da informação percebida pelos usuários, o que refletiu também no entendimento sobre o tema, onde atingiu um aumento de 47,3%. Este aumento obtido no entendimento é de vital importância, pois favorece a disseminação do tema nas unidades, proporcionando a formação de uma cultura voltada a segurança da informação, visando a sustentabilidade desejada.

Palavras-chave: Gestão da Segurança da Informação, Seis Sigma, DMAIC.

ABSTRACT

Master Dissertation
Graduation Program of Production Engineering
Federal University of Santa Maria

DEPLOYMENT OF INFORMATION SECURITY MANAGEMENT THROUGH SIX SIGMA APPROACH

AUTHOR: MARIA ANGÉLICA FIGUEIREDO OLIVEIRA
ADVISER: RAUL CERETTA NUNES, DR.
Date and Local: March 03 2009, Santa Maria

Today, Information Security is the key to ensuring data reliability, integrity and availability, however it must be seen in a comprehensive manner in the organization and not just as problem that concerns the Information Technologic area. Current researches have indicated a new concern to reduce risks and improve the management of security, the information security maintenance, that it requests a solid security management methodology on the organization. The Six Sigma is seen as one solution to address this maintenance because it is considered an approach that promotes quality through the principle of continuous improvement and that people are the main agent for this promotion. Although there are studies that recommend Six Sigma, none of them shows how it could be used or how the quality tools could be applied in the security context. Thus, to fill this gap, the deployment proposed in this dissertation brings us with a Six Sigma based security management methodology, structured through the DMAIC method, where the quality tools and procedures to be used at each stage are suggested. To recover the organization context closed to its business, all proposed steps take into account the internal customer or users. The methodology was applied on the Cardiac Intensive Care Unit and General Intensive Care Unit of Santa Maria University Hospital. As the main result we observe that Six Sigma could be used on security management from traditionally set of quality tools. The experimental results have contributed to the improvement of 43.8% in the information security quality perceived by users and 47.3% in the user security understanding. This increase in understanding is vital to information security maintenance because to get it the organization need to improve the security culture.

***Keywords**: Information Security Management, Six Sigma, DMAIC.*

CAPÍTULO 1

INTRODUÇÃO

Atualmente, é inegável admitir a grande dependência das organizações para com a informação a fim de garantir sua sobrevivência. Desta forma, o interesse com a segurança destas informações vem aumentando no mesmo limiar do surgimento de novas ameaças advindas de diferentes meios, sejam elas humanas ou tecnológicas. Diante dessa realidade, de crescente interesse, vêm de fato sendo comprovada através de mudanças visíveis no cenário organizacional onde é mostrado um maior amadurecimento sobre a necessidade de investir em segurança da informação, sendo esta constatação apresentada na 10° Pesquisa Nacional de Segurança da Informação realizada em 2007 (PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO, 2007). 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, Torres & Sarriegi, 2008). Embora, essa realidade continue, muitas pesquisas vêm sendo realizadas como Vermeulen & Solms (2002), Martins & Santos (2005), Brooks & Warren (2006), Rich, Sveen & Jager (2006) e com elas novas visões estão sendo renovadas, onde aos poucos o mercado vêm se adaptando as essas mudanças. Para Sveen, Torres, & Sarriegi (2008) reagir às novas ameaças e mudanças no mercado com antecipação, antes que seja tarde demais, é uma forma inteligente que está sendo encarada como um desafio a ser vencido pelas organizações, e que precisa ser considerada, haja vista que a frase "segurança, apenas hoje, amanhã pode significar desastre" já tem provocado de forma progressiva suas vítimas (Abagnale *et al*. 2005).

A segurança da informação, até poucos anos atrás, era tradicionalmente conhecida como um problema que só dizia respeito ao pessoal de Tecnologia da Informação (TI), sendo que muitas vezes tudo se aplicava somente no âmbito tecnológico. Felizmente segundo Campbell (2006), essa compreensão errônea vem perdendo espaço. A segurança da informação é um problema sistêmico que necessita de uma solução sistêmica, precisando ser ampla e multidisciplinar com envolvimento de várias áreas da organização.

A NBR/ISO IEC 17799:2005 é um exemplo dessa visão ampla que a organização precisa ter, esta norma de segurança da informação prevê controles que envolvem desde

processos, pessoas, tecnologia até ambientes internos e externos, onde são recomendadas ações que visem assegurar a proteção das informações inerentes a estes aspectos e que se faz presente em qualquer cenário organizacional. Contudo, já existem muitas discussões em torno das normas e padrões de segurança e os benefícios que elas indiscutivelmente produzem em uma organização. Pesquisas atuais demonstradas em (Kiely & Benzel, 2005; Saleh, Alrabiah, Bakry, 2007; Sveen, Torres, & Sarriegi, 2008; Aazadnia & Fasanghari , 2008) apontam para uma nova preocupação, o da sustentação da segurança da informação, haja vista, que a perpetuação de todos os controles e estratégias que visem minimizar o risco ou até mesmo saná-los necessitam estar envoltos e apoiados em uma base sólida que gere essa transformação. Estas mesmas pesquisas que discutem este apontamento também indicam uma solução que pode ser a chave que venha garantir esta sustentabilidade tão ambicionada na segurança da informação. Estas soluções são direcionadas para uma abordagem que promove a qualidade através do princípio de promoção de melhoria contínua, o Seis Sigma. Embora os Seis Sigma seja uma abordagem amplamente difundida tanto estratégico quanto estatisticamente, na área da segurança da informação, não existe muitos resultados de sua aplicação. Isto é evidenciado nas mesmas pesquisas citados anteriormente em que apontam a sua adoção, mas, no entanto, não são apresentadas experimentações, definições de ferramentas que poderiam ser utilizadas e nem resultados que comprovem tais indagações.

Diante destas constatações, este trabalho visa atender a esta lacuna, apresentando uma proposta de implantação da gestão da segurança da informação através da abordagem Seis Sigma. A proposta provê a definição de ferramentas e procedimentos em cada uma das fases do método DMAIC, base operacional da abordagem, com o foco direcionado nas percepções e expectativas do cliente interno ou usuário. O propósito é gerar uma gestão baseada em dados, que expresse a realidade e os desejos da organização, visando a melhoria da segurança das informações e a sustentação da gestão.

1.1 Motivação

Ao se estudar a literatura sobre segurança da informação e sua implantação compreendidas nos mais diversos meios que abrangem normas, padrões, metodologias e modelos, percebe-se que ainda há certa carência de estudos aplicados que comprovem a efetivação destes meios. Esta comprovação é evidenciada por Sveen, Torres & Sarriegi (2008) que recomenda que as novas pesquisas direcionem o foco a implantação, uma vez que se discute muito “O que fazer?” para alcançar a segurança, no entanto pouco se mostra o “como

fazer?" ou "como foi feito?". Esta constatação também pode ser vista na preposição do Seis Sigma para a implantação da gestão de segurança da informação, onde é estabelecido que esta abordagem pode ser de fato efetiva para obtenção da melhoria da segurança da informação, porém não se tem dados que atestem a efetividade desta afirmativa.

Assim, para que o assunto possa ser tratado com a relevância de uma pesquisa científica, entende-se que seja necessário tentar suprir, mesmo que parcialmente, essa carência. Deste modo, esta pesquisa propõe e relata a implantação da gestão da segurança da informação através da abordagem Seis Sigma com o objetivo de verificar sua efetividade na busca pela melhoria, visando a sustentabilidade da segurança da informação.

1.2 Problema de Pesquisa

Segundo Cervo & Bervian (1996) a pesquisa é uma atividade que parte de uma dúvida e que através do emprego de processos científicos busca-se uma resposta ou solução. Desta forma, fatores resultantes da aplicação da gestão da segurança da informação, seguindo os princípios da abordagem Seis Sigma, ainda foram pouco explorados, havendo comprovadamente poucos relatos de sua utilização que atestem de fato sua efetividade. A sustentabilidade é outra questão muita discutida nas atuais pesquisas no tocante da segurança da informação, sendo reconhecida como uma qualidade perseguida, que requer muita disciplina, precisando estar apoiada numa base operacional sólida que promova esta transformação. Mas de que forma garantir a sustentabilidade em segurança da informação? De fato não existem respostas concretas que evidencie uma afirmativa ou negativa acerca dessa problemática, existindo realmente uma lacuna a ser pesquisada e explorada. Neste sentido, esta dissertação procura responder as questões levantadas, demandando uma visão teórica e prática acerca da aplicabilidade da abordagem Seis Sigma na busca pela melhoria e sustentabilidade da segurança da informação.

1.3 Objetivo Geral

O objetivo principal deste trabalho é a implantação de uma gestão de segurança da informação através da abordagem Seis Sigma com o foco direcionado nas percepções e expectativas dos clientes internos ou usuários da organização, a fim de produzir uma gestão

baseada em dados concretos, promovendo a melhoria e a qualidade da segurança das informações.

1.4 Objetivos Específicos

Foram definidos alguns objetivos específicos, que servem de caminhos para alcançar o objetivo principal deste trabalho, quais sejam:

- Apresentar uma proposta de implantação da gestão da segurança da informação através da abordagem Seis Sigma;
- Validar a proposta de implantação da gestão segurança da informação;
- Avaliar a utilização da abordagem Seis Sigma e o método DMAIC;
- Identificar a melhora do nível de qualidade da segurança da informação e a minimização dos riscos identificados.

1.5 Organização da Dissertação

Este trabalho está organizado da seguinte forma: no Capítulo 2 encontra-se a revisão da literatura relacionada a gestão da segurança da informação; o Capítulo 3 aborda a revisão da literatura sobre a abordagem Seis Sigma para o desenvolvimento do presente trabalho; o Capítulo 4 apresenta a proposta de implantação da gestão da segurança da informação através da abordagem Seis Sigma; o Capítulo 5 apresenta o relato da implantação da gestão da segurança da informação, através da abordagem Seis Sigma detalhando todas as suas fases, bem como os resultados; e, finalmente, o Capítulo 6 descreve as Conclusões e Trabalhos Futuros.

CAPÍTULO 2

REFERENCIAL TEÓRICO: FUNDAMENTAÇÃO CONCEITUAL SOBRE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Com objetivo de melhor elucidar o tema segurança da informação sob os diferentes aspectos dentro de uma organização, este capítulo realiza uma revisão da literatura dos principais conceitos que abrangem a segurança da informação e algumas metodologias de gestão da segurança de informação (seção 2.3).

2.1 Segurança da Informação

Vivemos em uma sociedade que se baseia inteiramente em informações, portanto, é inegável admitir a crescente preocupação com relação à ela por ser considerada um dos maiores ativos de uma organização. Esta constatação deve-se muito ao fato da rápida evolução no processamento distribuído, por exemplo, a internet e o comércio eletrônico. O resultado disso é que as organizações necessitam garantir que suas informações sejam adequadamente protegidas mantendo um nível elevado de segurança da informação (SOLMS, 1998).

Existem muitas definições de segurança da informação presentes na literatura sob várias óticas sejam elas humanas, tecnológicas ou gerenciais. Por exemplo, Caruso & Steffen (1999) definem segurança da informação como sendo mais que uma estrutura hierárquica envolvendo pessoas e equipamentos, mas uma postura gerencial, ultrapassando abordagem tradicional que é vista na maioria das empresas.

Beal (2005) ressalta que o papel da segurança da informação é o de garantir que as ameaças não violem os três princípios básicos que a norteia: integridade, disponibilidade e confidencialidade.

Marciano & Marques (2006) defendem que o conceito de segurança da informação precisa ser visto a partir de uma ótica social (comportamento humano) além dos tecnológicos para sua correta cobertura.

Através destas definições o que se percebe é que a segurança da informação para ser completa precisa estar entendida nessas três óticas: humanas, tecnológicas e gerenciais, o que

também é defendido por Kiely & Benzel (2005) que determinam que esses três aspectos são os elementos chaves para uma organização que busca uma segurança da informação mais efetiva. Esta discussão a cerca dos aspectos norteadores para atuação da segurança da informação são fortemente destacados nas normas de gestão de segurança da informação que promove amplamente os seus conceitos dentro da organização através da implementação de controles, processos, políticas e procedimentos, que juntos fortalecem os objetivos do negócio com a minimização dos seus riscos.

De fato, existem enumeras normas que auxiliam as organizações a prover a segurança da informação. Reconhecidamente a ISO/IEC 17799 é umas das melhores práticas da área (SOLMS & SOLMS, 2004a). Segundo Duarte (2006) o Brasil foi o primeiro país do mundo a traduzir a ISO/IEC 17799, sendo adotada como norma nacional em setembro de 2005 denominada na versão brasileira como NBR/ISO IEC 17799:2005. É impossível 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 a organização forneça um serviço de credibilidade, organizado e controlado, independentemente do meio de armazenamento seja ela eletrônica ou em papel. A certeza de se ter um dado confiável precisa estar alinhada de tal forma a proporcionar:

- Confidencialidade: a informação deve ser acessada por pessoas explicitamente autorizadas;
- Integridade: a informação deve ser encontrada em sua forma original, sendo mantida a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas;
- Disponibilidade: toda informação deve estar disponível a qualquer momento que for necessário.

Estes conceitos são conforme NBR/ISO IEC 17799:2005 os princípios básicos para garantir a segurança da informação em uma organização.

Mas para compreender a Gestão de Segurança da informação e executá-la na prática é necessária a introdução e a definição dos seus conceitos básicos, nos quais compreendem os ativos da informação, ameaças, vulnerabilidades, riscos, escopo da segurança, política de segurança da informação, conscientização em segurança da informação e comitê de segurança.

2.1.1 Ativos da Informação

O conceito de ativos da informação pode ser compreendido como o conjunto que envolve as pessoas, tecnologia e processos, sendo estes responsáveis por alguma etapa do ciclo de vida da informação (FERREIRA & ARAUJO, 2006). Na concepção de Alves (2006) ativo é tudo que representa valor para o negócio da organização sejam eles humanos, tecnológicos ou físicos.

Existe uma grande preocupação por parte das organizações em dar mais atenção a ativos específicos, como os mais caros ou os menos comuns, entretanto é importante identificar a participação desse ativo no ciclo de vida da informação, quanto maior for essa participação, maior também será a prioridade com que ele deve ser considerado no que tange à segurança da informação (Marciano & Marques, 2006).

Os ativos de diferentes meios precisam ser mapeados durante o planejamento da segurança da informação, sendo de extrema relevância a realização da sua classificação que irá determinar o grau de sigilo às informações neles contidas. A NBR ISO/IEC 17799:2005 recomenda que a classificação seja feita para assegurar que a informação receba um nível adequado de proteção. Desta forma, convém que a informação seja classificada para indicar a necessidade, prioridade e o nível esperado de proteção quanto ao tratamento da informação. Campos (2007) relaciona a classificação dos ativos quanto ao grau de importância, sendo possível criar classificações do tipo “muito importante”, “pouco importante”, e similares. Também é muito comum a classificação pelo grau de prioridade que podem ser **pública** - informação que pode vir a público sem maiores conseqüências; **interna** - informação que diz respeito a determinados setores ou unidades; e, **confidencial** - informação restrita, onde somente pessoas autorizadas possam acessar. Como discutido os ativos se não forem protegidos, independente do grau de importância, podem gerar danos a organização, derivados de ameaças dos mais diversos meios, sendo tratada a seguir.

2.1.2 Ameaças

Quando se discute sobre ameaça, naturalmente se pergunta, “que tipo de ameaça?” As ameaças podem advir de diferentes formas, sejam elas naturais ou tecnológicas. Dias (2000) define ameaça como sendo um “evento ou atitude indesejável (roubo, incêndio, vírus, etc.) que pode ocasionar a remoção, desabilitação, danificação ou destruição de um recurso.” Schneider (2001) afirma que as ameaças do mundo físico refletem no mundo digital: “Se os bancos físicos são roubados, então os bancos digitais serão roubados”.

Uma das ameaças mais discutidas atualmente são as ameaças advindas do recurso humano ou a chamada Engenharia Social que é um método de ataque onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações sigilosas (PEIXOTO, 2006). No entanto, com a quantidade de ameaças existentes vindas das mais diversas origens, o reconhecimento de que a segurança da informação é importante, nem sempre é realizado, o que acaba dificultando mais o cenário, deixando a informação mais exposta e consequentemente tornando-a vulnerável.

2.1.3 Vulnerabilidades

Segundo NBR ISO/IEC 17799:2005, vulnerabilidade é uma fragilidade de um ativo ou um grupo de ativos que pode ser explorada por uma ou mais ameaças, o que permite a ocorrência de incidentes. A representação de um ponto potencial de falha (vulnerabilidade) ou um elemento relacionado a informação que é passível de ser explorado é considerada uma ameaça (MARCIANO & MARQUES, 2006). As ameaças não podem ser eliminadas, ou seja, não se pode impedir que um raio caia em um determinado lugar, mas é possível tratar a vulnerabilidade de um determinado lugar que possa ser atingido por um raio ou uma descarga elétrica. Esta medida de tratamento resulta na redução de incidentes.

2.1.4 Incidentes

Incidentes são conceituados como sendo um evento que ocorre em decorrência da ação de uma ameaça que explora uma ou mais vulnerabilidades (RICH, SVEEN & JAGER, 2006). Para a NBR ISO/IEC 17799:2005, um incidente de segurança da informação é reconhecido como sendo um ou mais eventos indesejados ou inesperados, que tenham alguma probabilidade de comprometer as operações ou os processos do negócio e ameaçar a

segurança da informação. Na concepção de Ferreira & Araujo (2006) um incidente é identificado pela ocorrência de qualquer ação adversa, confirmado ou sob-suspeita. Os autores definem uma série de tipos de incidentes presentes em grande parte das organizações.

- Roubo e extravio de informações;
- Perda de informações ou equipamento que armazenam dados críticos;
- Propagação de vírus ou outros códigos maliciosos;
- Ataques de negação de serviço e engenharia social;
- Uso ou acesso não autorizado a um sistema, sem o conhecimento, instruções ou consentimento prévio de seu proprietário; e
- Desrespeito a Política de Segurança da Informação.

O reporte de incidentes de segurança da informação é visto como uma das questões centrais para que haja a sua redução. Uma das medidas para se obter essa redução é a criação de canais formais de comunicação como sistemas de informação, e-mail e telefone. Rich, Sveen & Jager (2006) destacam que uma das formas de alcançar sucesso no reporte de incidentes é o incentivo a usuários para a notificação de todo e qualquer incidente que seja identificado. Estes incentivos podem variar desde brindes mais simples como canetas até bônus salarial, o que resulta em uma mobilização e conseqüentemente um aumento na conscientização para que as devidas ações sejam tomadas, refletindo também na redução dos riscos.

2.1.5 Riscos

A NBR ISO/IEC 17799:2005, define o risco como sendo a combinação da probabilidade de um evento e de suas conseqüências. É fato, de que a eliminação integral do risco dificilmente possa ser obtido (GUAN et al. 2003). No entanto, é necessário avaliá-los e tratá-los para que ocorra sua mitigação, e isto somente será possível se a organização adotar a prática preconizada pela NBR ISO/IEC 17799:2005, a gestão de riscos.

No processo de implantação de Gestão de Segurança da Informação a gestão de riscos é fundamental para o processo de decisão, sendo nesta fase definida ações que serão implantadas para a mitigação dos riscos levantados (LICHTENSTEIN, 1996). Segundo Baccarini, Geoff & Love (2004) muitos projetos da área de Tecnologia da Informação pecam pela ineficácia e acabam falhando por não priorizarem a etapa de gerenciamento dos riscos,

fazendo com que o fracasso de muitos projetos de Gestão de Segurança da Informação esteja fortemente relacionado ao gerenciamento de riscos.

A prática de análise de riscos consiste em verificar a probabilidade de perda causadas por uma ameaça contra um bem específico. No âmbito da segurança da informação, ela está associada à possibilidade de perda de algum dos seus princípios, seja a disponibilidade, a integridade ou a confidencialidade (MARTINS, 2003). Para Scudere (2006) a condução de uma análise de riscos pode ser dividida em seis etapas distintas:

1) Planejamento e estratégia: caracteriza-se pelo planejamento de ações e criações de estratégias de avaliação;

2) Identificação**:** criação de procedimentos que vise uma correta identificação dos riscos;

3) Qualificação**:** introduzir da qualificação decorrente de uma vulnerabilidade;

4) Quantificação**:** pontuação do nível de risco;

5) Impactos e respostas**:** criação de procedimentos que determine o impacto de um determinado risco e a resposta que deverá ser utilizada; e

6) Monitoramento e Controle**:** definição de procedimentos para um constante acompanhamento dos riscos e ações realizadas para minimizá-los.

A Análise de riscos é parte integrante do processo de gerenciamento de risco. Segundo Gerber & Solms (2005) o processo de gerenciamento de riscos se refere ao planejamento, monitoramento e controle, baseado nas informações produzidas pela atividade de análise de riscos (vide figura 1).

Analisando as duas abordagens discutidas por Scudere (2006) e Gerber & Solms (2005) pode ser considerada na maior parte semelhantes, principalmente nos pontos básicos que são a identificação, estimação (qualificação e quantificação) e controle dos riscos. No entanto, as duas abordagens diferem em como estes pontos básicos são estabelecidos. Por exemplo, Scudere (2006) define o planejamento como sendo a primeira ação no processo de análise de riscos. Por outro lado, Gerber & Solms (2005) estabelece o planejamento após o resultado da análise de riscos. De todo modo, é importante salientar que não existe a definição de uma metodologia ou abordagem ideal, essa determinação vai depender muito do contexto da organização, natureza do problema, custo e tempo. Muitas vezes a abordagem escolhida por uma organização pode sofrer algumas modificações para estar em sincronia e adaptada ao cenário de aplicação, sendo estes ajustes responsáveis para a obtenção de bons resultados (ELOFF, 2005).

Figura 1 – Gerenciamento de Riscos.
Fonte: Adaptado de GERBER & SOLMS (2005).

Para Lichtenstein (1996) um dos fatores que são decisivos na escolha de uma abordagem ou metodologia para o gerenciamento de riscos é o conceito de usabilidade, que está ligado exatamente à facilidade de uso com que a metodologia proporciona em todo processo de realização do gerenciamento de riscos, sendo que quanto mais usual e fácil ela for menos tempo se gasta e consequentemente menos custo se despende para sua aprendizagem.

Uma das partes principais no processo de gerenciamento dos riscos, segundo Jacobson (2002) e Alberts & Dorofee (2004) são as estratégias ou respostas que serão dadas aos riscos que forem identificados. Steinberg et al. (2004) define 4 categorias nas quais podem se enquadrar respostas aos riscos:

- Evitar: não se adota tecnologia ou processos que ofereçam riscos ao negócio. A forma de tratar estes riscos pode gerar um novo risco maior do que o benefício que ele pode vir a trazer, desta forma opta-se por evitar;
- Transferir: é transferido o tratamento desses riscos a terceiros ou a outro setor sendo uma alternativa viável quando o seu tratamento onera o custo de implantação do projeto;
- Reduzir: são adotados mecanismos ou controles que tenham a ação de mitigar o risco encontrado;
- Aceitar: consiste em não se tomar nenhuma ação para reduzir probabilidade de ocorrência ou impacto.

As ações ou conjunto de ações que serão escolhidos em resposta ao risco irá depender da natureza do negócio e os seus objetivos. Dentre estas estratégias que foram relacionadas para responder aos riscos (evitar, transferir, reduzir e aceitar) a opção por redução do risco implicará na determinação de um conjunto de medidas a serem implantadas a partir de um

nível de prioridade que é definido pela própria organização. Este nível de prioridade pode variar, como por exemplo, riscos que possuem um maior impacto serão tratados primeiro. Muitas vezes o tratamento de determinado risco pode vir a desencadear outros, sendo, portanto uma decisão que necessita de avaliação, pesando os pós e contra (CAMPOS, 2007).

Observa-se que a definição de medidas precisa ser compreendida como um processo dinâmico, adaptando-se as mudanças geradas na organização e real, sendo concretizável seja pelo lado financeiro ou temporal.

Apesar de tudo, a aplicação de medidas não resolverá integralmente o problema, mesmo após aplicar as medidas, existe sempre um risco residual, tal como é ilustrado na figura 2 (GERBER & SOLMS, 2005).

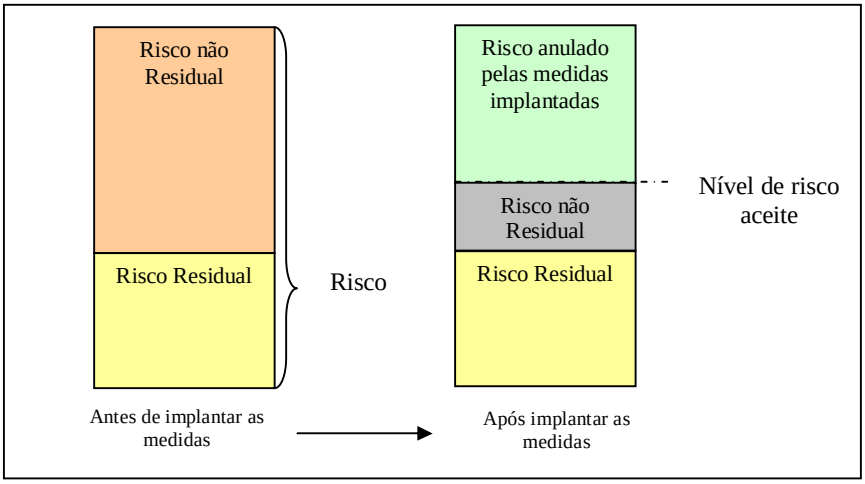


Figura 2 - Risco Residual.

Fonte: Adaptado de GERBER & SOLMS (2005).

O gerenciamento dos riscos só será eficiente se a cobertura da Gestão da Segurança da informação estiver claramente definida. Historicamente a segurança da informação era vista como um problema que somente dizia a respeito à área de Tecnologia da Informação (TI), felizmente este cenário tem sido mudado pelas próprias pesquisas em torno da segurança da informação, onde cada vez mais se discute a necessidade dela ser trabalhada e ser vista como uma gestão sistêmica, ou seja, ter o conhecimento do todo (KIELY & BENZEL, 2005; SVEEN, TORRES & SARRIEGI, 2008). Porém para que a Gestão da Segurança da Informação tenha esta característica sistêmica através de uma abordagem ampla, é necessário a definição de um escopo, tratado na próxima sessão.

2.1.6 Escopo da Segurança

A NBR ISO/IEC 17799:2005 determina que a gestão de segurança da informação precisa ter um escopo claramente definido para ser eficaz. O escopo pode abranger toda a organização como partes dela, por exemplo, somente área tecnológica, ou somente processos. O que irá determinar esta definição é o objetivo da organização e a prioridade com que alguns aspectos precisam ser tratados. No entanto, para que a gestão tenha uma visão ampla e sistêmica ela precisa estar envolta ao contexto organizacional. Para Bakry & Bakry (2001) existem 5 domínios que precisam ser tratados quando se trata de gestão: estratégia, tecnologia, organização, pessoas, e ambiente. Estas palavras formam a sigla STOPE "*strategy, technology, organization, people, and environment*" (vide figura 3), abordagem a qual foi desenvolvida para ser um meio de integração com questões relacionadas à tecnologia. A abordagem ou a visão STOPE tem sido utilizada para resolução de diversos problemas em diferentes domínios como planejamento de governo eletrônico, redes de segurança e gestão de segurança da informação. As siglas da abordagem definem sua base para o desenvolvimento e evolução de propostas (Saleh, Alrabiah, Bakry, 2007).

- Estratégia - "strategy": está associado com a liderança ou alta direção em traçar os objetivos e diretrizes para o desenvolvimento de melhorias na empresa. Conforme (Saleh, Alrabiah, Bakry, 2007) o conceito de estratégia alinhada a segurança da informação está ligado ao seu gerenciamento e apoio da organização de acordo com os requisitos do negócio e conformidade com leis e normas relevantes.
- Tecnologia - "technology": está associada com toda a infra-estrutura tecnológica que a organização dispõe seja ela internet, intranet, extranet, aplicações, sistemas de informação e canais de comunicação.
- Organização - "organization": está associada com a manipulação dos recursos que a organização mantém, como gerenciamento de todos os ativos, gestão de incidentes e plano de continuidade do negócio.
- Pessoas – "people": está associado com todos os recursos humanos que fazem parte da organização: funcionários, clientes, fornecedores.
- Ambiente – "environment": está associado com as condições tanto internas quanto externas para uma melhor operacionalização da organização.

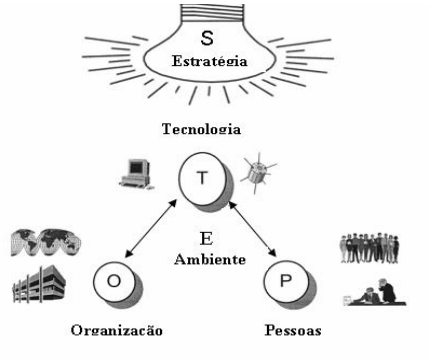


Figura 3 - Abordagem STOPE.
Fonte: Adaptado de BAKRY (2001)

Saad, Alrabiah & Bakry (2005) proporam a utilização do STOPE em seu trabalho para facilitar o entendimento e a implantação da norma ISO/IEC 17799:2005. O trabalho faz o alinhamento dos domínios abordados pelo STOPE, integrando-o com os principais controles recomendados pela norma. Na Tabela 1 pode ser vista esta integração com cada controle da norma que se refere aquele domínio. Por exemplo, o controle da Política de Segurança da Informação faz parte do domínio estratégia, pois está associado a objetivos e diretrizes da organização. Esta visão integrada da norma através dos domínios "(S) - estratégia", "(T) - tecnologia", "(E) - ambiente", "(O) -organização" e "(P) - pessoas", proporcionam uma forma mais abrangente de compreensão da ISO/IEC 17799:2005 e conseqüentemente para sua aplicação, o que segundo os próprios autores pode ser base para o desenvolvimento de indicadores de segurança.

Tabela 1 - Integração STOPE com a ISO/IEC 17799:2005.
Fonte: SAAD, ALRABIAH & BAKRY (2005).

STOPE		ISO/IEC 17799:2005			
		Part e nº	Controles	Nº de Obj.	Nº de Contr.
S	Estratégia	5	Política de Segurança da Informação	1	2
T	Tecnologia	10	Gerenciamento das operações e comunicações	10	32
		11	Controle de acesso	7	25
		12	Desenvolvimento e manutenção de sistemas	6	16
O	Organização	6	Organizando a Segurança da Informação	2	11
		13	Classificação e controle de ativos de informação	2	5
		14	Gestão de incidentes de segurança	2	5
			Gestão da continuidade do negócio.	1	5
P	Pessoas	8	Segurança em pessoas	3	9
E	Ambiente	9	Segurança ambiental e física	2	13
		15	Conformidade	3	10

2.1.7 Política de Segurança da Informação

A política de segurança da informação é considerado um dos principais instrumentos para se obter a Gestão da Segurança da Informação dentro de uma organização (Ferreira & Araújo, 2006). Ela é composta por um conjunto de regras e padrões para que seja assegurada a proteção das informações e serviços que são importantes, visando garantir a sua confidencialidade, integridade e disponibilidade (Ferreira & Araújo, 2006; Martins & Santos, 2005; Campos, 2007). A política de segurança da informação é o documento que melhor define a normativa e as melhores práticas para que ocorra a prevenção e a proteção da informação.

A política de segurança da informação precisa estabelecer princípios institucionais de como a organização irá proteger, controlar e monitorar seus recursos e, conseqüentemente, as informações por eles manipuladas. É importante descrever na política de quem e quais são as responsabilidades e que, principalmente, seja orientada a riscos e a impactos que envolvam o processo (Ferreira & Araújo, 2006). É muito comum encontrar na literatura recomendações de que a política deva ser a primeira ação de uma gestão de segurança da informação (Martins & Santos, 2005; Vermeulen & Solms, 2002). Esta realidade se justifica pela rapidez com o que o documento é gerado, onde muitas vezes a organização opta por essa ação imediata a fim de obter algum resultado. Mas, por outro lado se está ação ganha em praticidade, peca em eficiência, uma vez que a política não estará direcionada para os riscos ou para o que realmente a organização necessita, gerando muitas vezes perdas e falta de efetividade.

É comum encontrar disparidades entre a situação real e a situação prevista no ambiente organizacional, devendo o documento da política de segurança estar preparado para as constantes mudanças no ambiente organizacional como um todo, uma vez que é reconhecida a sua adaptabilidade (MARCIANO, 2006).

Muitas vezes a padronização e normatização das ações voltadas à segurança da informação são mal interpretadas, sendo utilizadas fora de seu devido contexto. Deste modo, para uniformizar esta discussão, Marciano (2006) esclarece algumas das questões corriqueiras que fazem parte do cenário organizacional. A primeira delas se refere nas diferenças existentes entre os componentes das políticas de segurança da informação de acordo com o nível organizacional, gerando muitas vezes documentos formais que não atendem em termos práticos o que a organização realmente necessita, tornado a política como mais um documento que fica engavetado. Outro ponto que o autor enfatiza é quanto à sua formulação, as políticas

são categorizadas segundo dois tipos: política restritiva os usuários terão acesso as informações que forem expressamente permitidas. E uma política permissiva, são concedidas aos usuários todas as informações em que o acesso não seja expressamente vedado. Ainda segundo o autor, a escolha por políticas restritivas é mais comum, mas de fato o que vai definir esta escolha irá depender da filosofia da organização e o objetivo que ela almeja com esse documento. Outra questão que é relevante nesta escolha e que também é muito discutida no que tange as políticas, está no aspecto comportamental relacionados a sua efetivação (MARCINCOWSKI & STANTON, 2003). O fato de existir um documento escrito e formalizado independente de ser permissiva ou restritiva não significa que ela será seguida ou respeitada, por essa razão é preciso estabelecer medidas que acompanhem a implementação das políticas.

Solms e Solms (2004a) destaca que o ideal é que uma política expresse a cultura da organização como forma de garantir o comportamento adequado que se espera dos profissionais. Esta afirmação pode ser alcançada através de um processo adequado que reuna e integre três preceitos importantes: educação, cultura e políticas. Kruger e Kearney (2006) também ressaltam que a efetividade da política irá depender de uma ambiente positivo no qual todos os usuários entendam e se engajam em comportar-se de acordo com o que se espera deles. Para que este cenário se consolide e se torne uma realidade na organização são realizados programas de conscientização que visam está interação com os usuários, buscando a promoção da cultura da segurança e principalmente da efetividade da política.

2.1.8 Conscientização em Segurança da Informação

Implementar a gestão de segurança da informação e não trabalhar as pessoas é promover o risco. As pessoas são um dos elementos principais para que a segurança da informação de fato aconteça na organização, sendo considerado um dos fatores que podem determinar ou não a sua efetividade (Chang & Ho, 2006).

A NBR/ISO IEC 17799:2005, estabelece a conscientização e treinamento como um dos controles de segurança da informação, desta forma a organização que deseja uma gestão de segurança harmoniosa e principalmente que a política seja aderida e entendida por todos é preciso o envolvimento das pessoas. Alves (2006) afirma que um dos pontos considerados mais críticos durante o processo de implantação da gestão de segurança da informação é a conscientização quanto à segurança. Isto porque com o apoio e comprometimento das pessoas

que acessam e manipulam as informações, ficará mais fácil implantar a segurança da informação e com isso aprimorá-las no decorrer do tempo com medidas mais rígidas. Neto & Silveira (2007) constatam em sua pesquisa que as questões humanas possuem maior carência de cuidados por parte dos administradores e diretores de organização, o que pode vir a influenciar de forma negativa a efetividade da gestão da segurança da informação.

Nakamura & Geus (2007) atesta que um dos instrumentos principais da gestão da segurança da informação, a política, precisa estar amparada por um programa de conscientização. Os autores apontam ainda algumas maneiras de aumentar à adesão a política e consequentemente elevar a conscientização:

- Comunicação interna.
- Reuniões de divulgação e conscientização.
- Treinamento específico ou inclusão em programa vigentes.
- Dramatização de exemplos práticos em peças teatrais.
- Incorporação ao programa de recepção a novos funcionários
- Pôsteres, protetores de tela e *mouse pads* podem ser um instrumento eficiente para oferecer dicas, lembrando da importância da segurança da informação.

Everet (2006) também propõe algumas medidas para promover a conscientização em segurança da informação. Este autor divide essas medidas em 4 categorias ou métodos:

- Métodos promocionais – *banners*, camisetas, páginas internas, pôster, *mouse pads*, protetores de tela, canecas e copos.
- Métodos de reforço – acordos de confidencialidade, testes ou exames de conscientização, ações disciplinares e mecanismos de recompensa.
- Métodos Interativos ou Educacionais – *slides* de apresentação, treinamento, rápidas sessões dirigidas, módulos de aprendizagem *on-line*, demonstrações, vídeos e *workshops*.
- Métodos Informacionais – folhetos, histórias ou contos curtos, *web sites*, alertas por e-mail, dicas do mês e notícias.

Os métodos interativos ou educacionais são projetados para criar um entendimento acerca dos fundamentos principais em segurança da informação. Por outro lado os demais métodos são mais indicados para forçar e reforçar a comunicação e a atenção direcionada para objetivos específicos.

2.1.9 Comitê Gestor de Segurança da Informação

O Comitê Gestor de Segurança da Informação é uma iniciativa necessária para se obter sucesso na implantação da Gestão Segurança da Informação, sendo essa idéia reforçada pela NBR ISO/IEC 17799:2005. Ainda de acordo com a norma, o comitê deve ser composto por uma equipe com perfis multidisciplinares envolvendo pessoal da área da tecnologia, jurídica, direção, entre outras. Solms & Solms (2004b) explica que a segurança da informação precisa ser tratada como um negócio e não como algo simplesmente técnico. Por essa razão é que a composição do comitê precisa ter um caráter amplo com envolvimento de diversas especialidades que tenham ou não mandato definido.

Um dos itens mais importantes neste comitê é o nome de algum executivo principal da organização, atestando a divulgação do documento da política e exigindo o cumprimento de sua utilização e as ações que serão implantadas no decorrer da Gestão de Segurança da Informação. Está estratégia demonstra aos funcionários que este executivo principal está de acordo com as regras, mostrando-se também comprometido para que elas sejam adequadamente cumpridas (FERREIRA & ARAÚJO, 2006).

Algumas responsabilidades do Comitê Gestor de Segurança da Informação são:

- aprovação das políticas, normas e procedimentos de segurança da informação;
- designar, alterar ou definir responsabilidades da área de segurança da informação;
- aprovação de novos controles de segurança a serem criados com o objetivo de melhoria contínua das medidas de proteção;
- prover suporte às iniciativas da área da segurança da informação; e,
- apoiar à implantação de soluções para minimizar os riscos como também a programas de conscientização, promovendo uma cultura organizacional voltada a segurança.

2.2 NBR/ISO IEC 17799:2005 e NBR ISO/IEC 27001

Até este momento, muito se referenciou e citou sobre as normas, principalmente a NBR/ISO IEC 17799:2005, o que denota a relevância deste documento no contexto de segurança da informação. A inserção deste tema nesta seção foi estrategicamente planejado,

justamente para ressaltar a sua importância e demonstrar que é impossível falar de segurança da informação sem deixar de mencioná-la.

Foi a partir do ano de 2000 que a Associação Brasileira de Normas Técnicas (ABNT) homologou como padrão brasileiro a versão brasileira de normas britânica ISO/IEC 17799, denominada NBR ISO/IEC 17799:2001 – Código de Prática para a Gestão da Segurança da Informação, tendo sido incluída na série 27000 como NBR/ISO IEC 27002. Esta norma cobre os mais diversos tópicos, recomendando as melhores práticas no que tange à segurança da informação (TASHI & GHERNAOUTI-HÉLIE, 2007). Um grande número de controles está contido na norma com seus respectivos objetivos que devem ser atendidos para garantir a segurança das informações de uma empresa, como pode ser visualizado na tabela 2.

Tabela 2 – Controles NBR ISO/IEC 17799:2005

Fonte: NBR ISO/IEC 17799:2005

NBR ISO/IEC 17799:2001	
Controles	**Objetivos**
1- Política de segurança	descreve a importância e relaciona os principais assuntos que devem ser abordados numa política de segurança.
2- Segurança Organizacional	aborda a estrutura de uma gerência para a segurança de informação, assim como aborda o estabelecimento de responsabilidades incluindo terceiros e fornecedores de serviços.
3-Classificação e controle de ativos de informação	trabalha a classificação, o registro e o controle dos ativos da organização.
4- Segurança em pessoas	tem como foco o risco decorrente de atos intencionais ou acidentais feitos por pessoas. Também é abordada a inclusão de responsabilidades relativas à segurança na descrição dos cargos, a forma de contratação e o treinamento em assuntos relacionados à segurança.
5- Segurança ambiental e física	aborda a necessidade de se definir áreas de circulação restrita e a necessidade de proteger equipamentos e a infra-estrutura de tecnologia de Informação.
6- Gerenciamento das operações e comunicações	aborda as principais áreas que devem ser objeto de especial atenção da segurança. Dentre estas áreas destacam-se as questões relativas a procedimentos operacionais, responsabilidades, homologação e implantação de sistemas, gerência de redes, controle e prevenção de vírus, controle de mudanças, execução e guarda de backup, controle de documentação, segurança de correio eletrônico, entre outras.
7- Controle de acesso	aborda o controle de acesso a sistemas, a definição de competências, o sistema de monitoração de acesso e uso, a utilização de senhas, dentre outros assuntos.
8- Desenvolvimento e manutenção de sistemas	são abordados os requisitos de segurança dos sistemas, controles de criptografia, controle de arquivos e segurança do desenvolvimento e suporte de sistemas.
9-Gestão de incidentes de segurança	apresenta dois itens: Notificação de fragilidades e eventos de segurança da informação e gestão de incidentes de segurança da informação e melhorias.
10-Gestão da continuidade do negócio	reforça a necessidade de se ter um plano de continuidade e contingência desenvolvido, implementado, testado e atualizado.

NBR ISO/IEC 17799:2001	
Controles	**Objetivos**
11- Conformidade	aborda a necessidade de observar os requisitos legais, tais como a propriedade intelectual e a proteção das informações de clientes.

Convêm observar que os controles listados na tabela 2 devem ser considerados para atender as necessidades de qualquer organização. Entretanto, alguns desses controles podem não ser aplicáveis a todos os ambientes organizacionais, como por exemplo, o controle 10 que reforça a necessidade de se trabalhar a Gestão da Continuidade do Negócio, o que pode não ser possível de ser trabalhado em pequenas organizações, indagação está enfatizada pela norma. Desta forma, esses controles serão um referencial, que servirá como base para o início de uma gestão, respeitando sem dúvida a natureza da organização e as prioridades sinalizadas por ela.

Em 2005 surgiu a norma ISO 27001, onde no Brasil foi traduzida e homologada no final do ano de 2005 tornando-se NBR ISO/IEC 27001:2006. Esta norma estabelece-se com um guia, produzindo um Sistema de Gestão de Segurança da Informação (SGSI) dentro da organização. Ela contém os mesmos direcionamentos e controles presentes na NBR/ISO IEC 17799:2005, a diferença está na certificação que uma organização pode receber e que a NBR ISO/IEC 27001 prevê.

Outro diferencial desta norma está na promoção de uma abordagem de processo utilizada para estabelecer, implementar, operar, monitorar, analisar, manter e melhorar o SGSI. Estas etapas estão relacionadas ao plano de negócios estratégico em um ambiente operacional e com isso auxiliando a organização a obter um aumento no nível de credibilidade da segurança presente. Para que isto seja possível a norma utilizada 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). Para cada estágio são recomendadas algumas práticas:

Primeiro estágio: é realizado o planejamento, onde são estabelecidas o SGSI, a política de segurança da informação, traçados objetivos, processos e procedimentos.

Segundo estágio: é realizada a implantação da política, controles, processos e procedimentos, implementação e operação de controles para gerenciar os riscos no contexto de negócio da organização.

Terceiro estágio: é realizada a verificação e avaliação das medidas implantadas na fase anterior, bem como a mensuração do desempenho dos processos frente a política.

Quarto estágio: é realizada as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e na análise crítica pela direção.

Ainda que a NBR ISO/IEC 27001 tenha evoluído em comparação com NBR/ISO IEC 17799:2005, recomendando o PDCA para manter a continuidade da gestão a partir da melhoria contínua, as normas dão pouco apoio na implementação prática, ou seja, elas dizem "o que" precisa ser feito, mas o "como" é deixado a cargo da organização.

Deste modo, há uma diversidade de metodologias de implantação da gestão da segurança da informação, que servem de auxilio e referência para o desenvolvimento de medidas no intuito de atingir um nível desejável de segurança dentro da organização. Na próxima seção, são discutidos alguns desse tema.

2.3 Metodologias de Gestão da Segurança da Informação

Com a disseminação das normas e padrões de segurança, o interesse das organizações preocupadas em proteger o seu maior ativo, a informação, é cada dia maior. Muitos estudos vêm sendo publicados, e com eles são apresentados novas *metodologias, frameworks* e recomendações para implementação de uma gestão de segurança da informação.

A metodologia de Martins & Santos (2005) propõe um processo de implantação de um Sistema de Gestão da Segurança da Informação (SGSI) o qual resulta a padronização e documentação dos procedimentos, ferramentas e técnicas utilizadas, além da criação de indicadores dos quais serão definitivos para um processo educacional de conscientização dentro da organização. Por esta razão os autores propõem uma metodologia baseada nos principais padrões e normas de segurança, definindo um conjunto de diretrizes para garantir a segurança. A metodologia adota o ciclo de melhoria continua, PDCA, para auxiliar na concepção e elaboração de um SGSI.

O grande diferencial desta metodologia é evidenciada nas suas etapas de implantação que pode ser visualizada na figura 4. As etapas são baseadas cada qual em normas internacionais (TECSEC, 1985; ISO 15408:1999; B7799-2:2001) apresentando aspectos gerenciais na sua condução.

A metodologia prevê como primeira tarefa a criação da política de segurança da informação e em seguida a definição do escopo e análise de riscos para somente depois selecionar e implementar os controles da gestão.

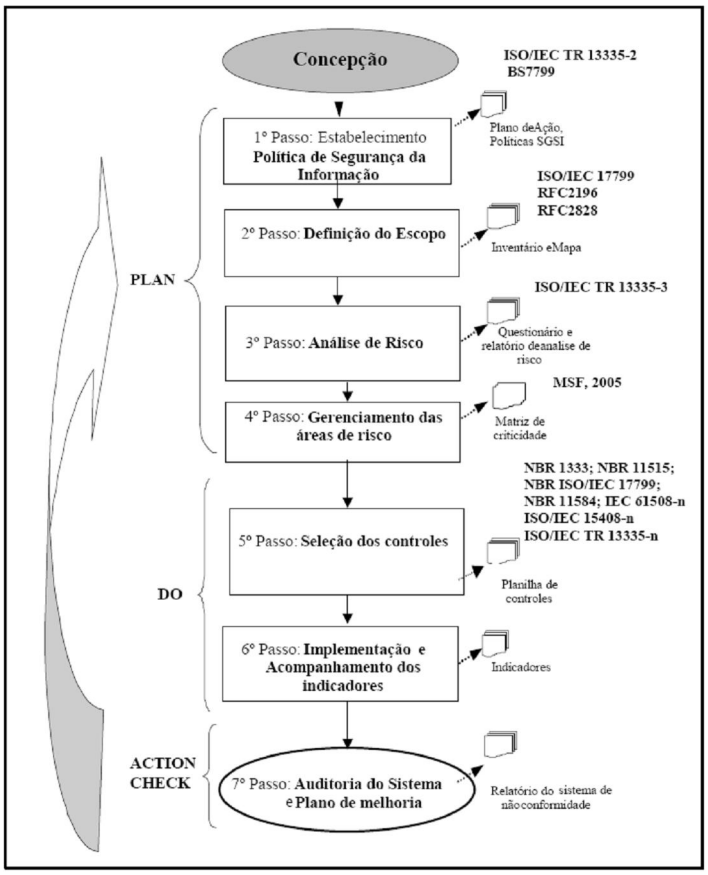


Figura 4 – Proposta de Metodologia de implantação da SGSI

Fonte: Martins & Santos (2005)

Brooks & Warren (2006) apresentam em sua pesquisa uma metodologia de evolução de segurança da informação em saúde baseadas nas técnicas *Unified Modelling Language* (UML). Neste modelo são estabelecidos quatro passos para sua implantação. O primeiro deles e o mais importante é a modelagem e a construção do cenário na qual será aplicada a metodologia. Está etapa é caracterizada pelo uso das técnicas de UML para mapear a interação das atividades com o sistema. O segundo passo é realizar a análise das ações de segurança que serão aplicadas, baseando-se em um *checklist* proposto pela Norma Australiana de Gestão de Segurança da Informação (HB 174-2003). O terceiro e quarto passo se resumem na comparação da segunda fase com o nível de segurança ideal, concluindo com implantação dos resultados das análises e em seqüência sua verificação pós implantação. Um aspecto positivo deste trabalho é a percepção que se tem na fase inicial, onde busca-se através da técnica UML mapear todo o contexto ambiental, esta fase caracteriza-se como determinante para o conhecimento do cenário organizacional e necessária para obtenção do nível ideal de segurança.

Vermeulen & Solms (2002) discutem o desenvolvimento de um *framework* para guiar a implantação da gestão de segurança da informação. Para auxiliar neste processo, os autores propõem a automatização de alguns passos ao qual resultou a criação de uma ferramenta denominada de ISMTB (*Information Security management toolbox*). Esta ferramenta foi implementada com intuito de auxiliar no processo de conhecimento e caracterização da organização para identificar o nível de segurança atual como também, servindo de base para determinar quais medidas de segurança que serão executadas. A ISMTB é composta por questionários que avaliam 5 aspectos importantes em uma organização baseados na BS 7799-1(1999) que são: confidencialidade; integridade; disponibilidade; autenticidade e auditabilidade. Os resultados desta análise determinará a extensão da aplicabilidade destes 5 aspectos e definirá quais requisitos serão escolhidos para iniciar a implantação dentro da organização.

O Framework de gestão da segurança da informação proposto pelos autores (vide figura 5) é formado por quatro domínios, que segundo eles norteiam a gestão dentro de uma organização: comprometimento da gerência, visão e estratégia da segurança, aspectos organizacionais e padrões de segurança da informação. O Framework segue três passos principais: os requisitos de segurança, onde é utilizada a ferramenta ISMTB, construção e implantação da política de segurança da informação e gestão de riscos.

Kiely & Benzel (2005) retratam em sua pesquisa, que para atingir uma proteção efetiva, a infra-estrutura de informação de uma empresa deve ter uma abordagem de gestão de segurança sistêmica, tendo como objetivo assegurar que a organização não somente pague pela segurança, mas, tenha a preocupação de sustentá-la. Como meio de seguir essa filosofia os autores recomendam a adoção da abordagem Seis Sigma, sendo que a prática de sustentação é similar com os princípios derivados pela Gestão da Qualidade Total (TQM - *Total Quality Management*) que tem por objetivo a melhoria continua, em outras palavras, a sustentação somente poderá ser garantida a partir de um processo contínuo e evolutivo de melhorias na segurança da informação. O trabalho também discute a composição de um framework formado por 4 domínios ou nós o qual abrangem pessoas; processos; tecnologia; e estratégia organizacional, considerados, segundo a visão dos autores como elementos chaves para uma gestão de segurança da informação. Entretanto, o ponto central deste trabalho é o reconhecimento de que o processo necessita ser mais dinâmico que linear, para estar em constante transformação a fim de manter uma eterna vigilância.

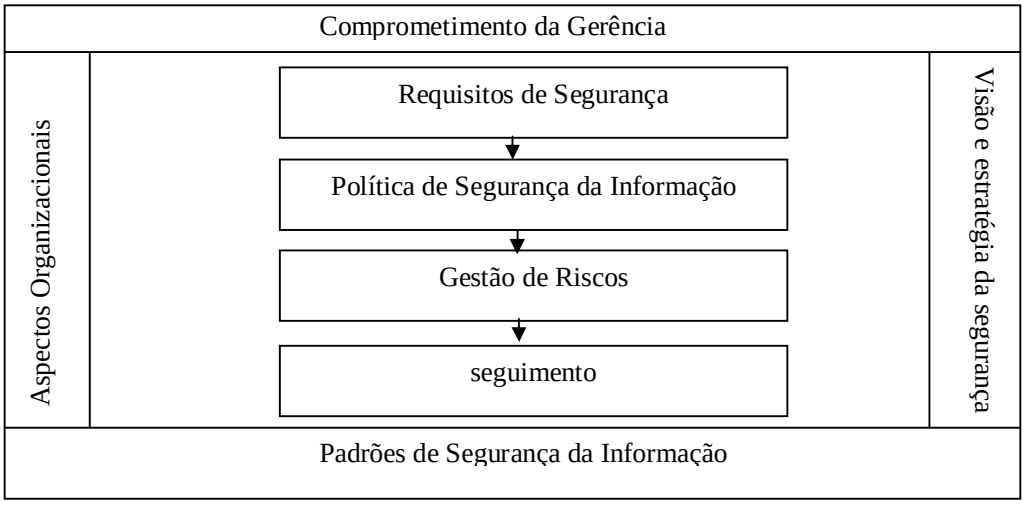


Figura 5 – Framework de Gestão de Segurança da Informação

Fonte: Adaptado de Vermeulen & Solms (2002)

Em Saleh, Alrabiah, Bakry (2007) a proposição da abordagem Seis Sigma vai mais além, nesta pesquisa os autores propõem a implementação da gestão da segurança da informação a partir da norma ISO/IEC 17799:2005, integrando suas principais partes e controles dentro dos domínios de "estratégia, tecnologia, organização, pessoas e meio ambiente" denominado como STOPE. Para a condução de todo processo de implantação é proposto a aplicação da abordagem Seis Sigma que tem com o objetivo promover um ambiente que preserve sempre o pensamento de melhoria e transformação continua. Segundo os autores, para atingir efetivamente o sucesso da gestão salienta-se a criação de uma equipe alinhada com a filosofia Seis Sigma que preveja um time de trabalho com atribuições específicas durante a execução de todo o processo de implantação. Os autores não chegam a validar de fato todas as idéias, portanto não são demonstrados resultados que evidencie sua efetividade, entretanto são recomendados que sejam feitas experiências práticas das propostas apresentadas nos mais diversos campos, bem como a divulgação dos resultados.

Para Sveen, Torres, & Sarriegi (2008) alcançar o sucesso com a implantação da gestão de segurança da segurança da informação é uma tarefa árdua e depende principalmente da reunião e entendimento de alguns elementos chaves que poderiam ser úteis na obtenção deste êxito. Os autores apresentam 10 lições para uma efetiva gestão de segurança da informação, evidenciando claramente que a gestão de segurança da informação precisa ser entendida, iniciada, executada e mantida através de uma abordagem de melhoria contínua. Não é preciso reinventar a roda, ou seja, desenvolver um outro método, isso só gera perda de tempo e de

dinheiro. Existem modelos eficientes e eficazes como o Seis Sigma para trabalhar a segurança da informação, promovendo assim a participação colaborativa da organização.

A partir das metodologias, framework e recomendações apresentadas observa-se que a gestão da segurança da informação para ser considerada "ideal" precisa ser baseada em dados, ou seja, de fato e reconhecidamente as normas indicam o que precisa ser feito para se obter um nível completo de segurança da informação em um ambiente organizacional independente do seu domínio. Entretanto, a cerca das enumeras recomendações expostas por esses documentos, alguns questionamentos surgem como, por exemplo: por onde se deve começar? Quais controles serão implantados primeiro? O que é prioridade? As respostas para essas e outras perguntas que permeiam a construção de uma gestão da segurança da informação pode ser resumidas a partir de um entendimento que centra-se como ponto em comum entre os estudos, onde a segurança da informação vai depender da importância dada pela organização a determinados ativos de informação. Esta idéia é reforçada por Silva e Stein (2007) o qual salienta que "o nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio da mesma" (SILVA E STEIN, 2007).

A gestão da segurança da informação para ser eficaz e eficiente necessita ser baseada em dados concretos, ou seja, na realidade da organização, enfatizando o que ela realmente necessita que seja solucionado. Contudo, a partir das conclusões realizadas por (Kiely & Benzel, 2005; Saleh, Alrabiah, Bakry, 2007; Sveen, Torres, & Sarriegi, 2008) apontam para uma filosofia de gestão que reúne princípios derivados da Gestão da Qualidade Total (TQM) ao qual tem o foco no cliente e destina-se a promover ações que visem à melhoria contínua, e a sua sustentabilidade, denominada de Seis Sigma. Os autores não definem uma metodologia de aplicação padrão para a abordagem Seis Sigma e nem relatam, que ferramentas da qualidade poderiam ser utilizadas com a aplicação desta prática. No entanto, eles defendem a adoção da abordagem como meio de alcançar um nível de qualidade que garanta um processo bem definido com resultados satisfatórios a fim de promover a sustentação das melhorias.

2.4 Conclusões Parciais

Existe uma grande necessidade de fornecer mecanismos mais eficientes para gerenciar as informações. A segurança, decididamente é o ponto chave para garantir um dado confiável, integro e disponível visto que a informação está a mercê de ameaças advindas de muitas formas, gerando riscos, que se não forem tratados podem ocasionar incidentes para a

organização. Entretanto a segurança da informação precisa ser tratada de forma abrangente, ela não é um problema apenas da área de tecnologia, mas é algo que diz respeito a todas as áreas, uma vez que a informação esta em todo lugar, idéia esta que é amplamente difundida pela norma NBR ISO/IEC 17799.

Contudo, para a segurança da informação ser considerada efetiva, ela necessita estar envolta a um processo bem delineado com etapas bem definidas e metas traçadas através de uma base gerencial consistente como mostradas e evidenciadas nas metodologias de gestão de segurança da informação investigadas. Desta forma, a gestão da segurança precisa ser considerada como uma transformação, que somente pode ser garantida com planejamento de ações, baseadas em dados concretos amparadas por normas de segurança, que direcionem a uma reflexão para o que de fato a organização necessita e prioriza. O conceito de gestão da qualidade total e mais especificamente o Seis Sigma está atrelada a esta filosofia proporcionando soluções que são centradas em dados direcionadas ao cliente ou no usuário, primando pela qualidade e visando a sustentação das ações.

CAPITULO 3

REFERENCIAL TEÓRICO: FUNDAMENTAÇÃO CONCEITUAL SOBRE A ABORDAGEM SEIS SIGMA

Até o presente momento, se constatou que a abordagem Seis Sigma é apontada como uma solução para gestão da segurança da informação, por primar pela qualidade, direcionamento ao cliente ou usuário e a sustentação das ações da organização. Deste modo, a fim de apresentar um maior esclarecimento sobre a abordagem, este capítulo aborda o Seis Sigma sob os diferentes aspectos em torno de sua aplicação, realizando uma revisão da literatura dos principais conceitos, ferramentas, métodos e procedimentos que são necessários para a uma efetiva implantação desta abordagem.

3.1 Seis Sigma

Os Seis Sigma (Rotondaro, 2006) teve seu início na década de oitenta, quando enumeras empresas norte-americanas procuravam alguma abordagem que às levasse a um padrão de competitividade compatível com que era praticado pelas empresas japonesas. As aplicações iniciais do Seis Sigma foram realizadas na empresa Motorola. Porém sua implantação, de fato, ocorreu no início de 1987, quando as suas filiais ao redor do mundo foram informadas sobre o que consistia tal conceito e as obrigações que as competia para alcançar as metas desejadas (PEREZ-WILSON, 1999).

Os resultados positivos com a implantação do Seis Sigma começaram aparecer no início da década de noventa. Estes resultados levantaram o interesse de outras organizações em implantar o Seis Sigma, as quais também foram beneficiadas com resultados satisfatórios, com destaque para a empresa General Electric (PANDE et al. 2001). O conceito se tornou popular após a repercussão destes resultados, onde a partir de então, começou a ser empregada em outras empresas de diversos países, inclusive no Brasil (PEARSON, 2001).

Pande et al. (2001) relaciona seis princípios que norteiam a concepção do Seis Sigma:

1. Foco genuíno no cliente: o cliente é o ponto de partida para qualquer processo de melhoria. O que diferencia o Seis Sigma é que o cliente interno ou externo que define o que é defeito ou problema.

2. Gerenciamento baseado em dados e fatos: O Seis Sigma norteia as decisões sem influência de opiniões e crenças sem fundamentos por parte dos gestores. As decisões e análises são feitas com base em dados concretos, resultantes de medições.
3. Gerenciamento, melhoria e foco nos processos: a importância da gestão dos processos é chave para o sucesso do Seis Sigma.
4. Gerenciamento pró-ativo: transformar o comportamento da organização, formando hábitos gerenciais que sejam saudáveis com o foco na prevenção em lugar de "apagar incêndios".
5. Colaboração sem fronteiras: o Seis Sigma valoriza o trabalho em equipe e colaborativo através de uma visão ampla dos processos globais da organização.
6. Busca da perfeição com tolerância a falhas: arriscar sem medo de errar. O medo das conseqüências de uma atitude errônea leva à estagnação e ineficiência da organização.

Rotondaro et al. (2006) qualifica o Seis Sigma como sendo um conceito que está apoiado em quatro coluna básicas (vide figura 6), passando a ser visto como, não somente, um simples esforço pela busca da qualidade, mas também um processo que visa o aperfeiçoamento na melhoria, resultando em impactos percebidos por toda a organização.

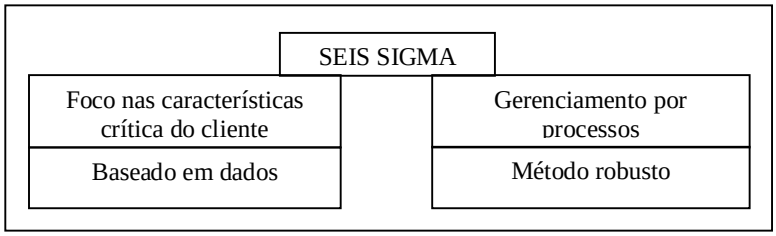


Figura 6 - As bases da abordagem Seis Sigma.
Fonte: ROTONDARO et al.(2006)

O termo Seis Sigma tem origem no nome de um parâmetro usado na Estatística para mensurar a dispersão de dados (ROTONDARO et al. 2006). Embora o seu conceito estar relacionado com a redução da dispersão quando se está tratando de controle no processo produtivo, o Seis Sigma também traz elementos que vislumbram aspectos gerenciais. Conforme (SANTOS E MARTINS, 2008) um dos aspectos fundamentais para compreender o conceito do Seis Sigma é identificar as duas abordagens presentes na literatura: a abordagem estatística e a abordagem estratégica.

3.1.1 Seis Sigma como abordagem estatística

A palavra sigma é o nome de uma letra grega, σ, usada na estatística para reconhecer um parâmetro no qual é conhecido como desvio padrão que também pode ser interpretado como o grau de variabilidade que um determinado processo sofre (PEREZ-WILSON, 1999).

Quanto se trata de um processo de produção discreta, por exemplo, pode se considerar que o número de defeitos na saída do processo é tão menor quanto a variabilidade dos fatores nas suas etapas intermediárias (RIBEIRO & CATEN, 2001; MONTGOMERY, 2001). Em um processo de produção contínua, a redução que ocorre na variabilidade existente nas características críticas permite que ela seja reduzida na saída do processo. Um dos meios para se garantir a qualidade pode estar na redução desta variabilidade que está diretamente ligada com a tomada de informações na saída do processo produtivo. Esta tomada de informações deve possuir uma variabilidade máxima para que não seja excedido uma determinada dispersão dentro de um intervalo delimitado pelos limites estipulados de variabilidade permitidos ao processo (ECKES, 2001).

Conforme Harry (1998) a obtenção dos níveis desejados de qualidade desde a época da produção em massa, era determinada pela inspeção em grande escala na saída dos processos. Porém, uma maneira diferente de obter informações sobre o processo é pelo uso da estatística, através de amostras representativas dos produtos que são produzidos, sendo esta última visão reconhecida como diferencial e decisiva para as mudanças e o avanço positivo das empresas japonesas na segunda metade do século (HARRY, 1998).

Para Perez-Wilson (1999) é errado afirmar que o nível de eficiência equivale a 3,4 falhas por milhões de oportunidades de erro quando relacionada a uma meta, o que é ainda visto em muitas das implantações que compreendem este conceito. O autor explica que o valor 3,4 provém da possibilidade de que, num longo período, o processo pode atingir variações de ±1,5σ sem indicar uma baixa na porcentagem de itens fora de especificação. Harry (1998) complementa que é possível que haja um aumento na variabilidade em longo prazo, decorrente da influência dos recursos estatísticos e também da utilização das ferramentas da qualidade.

O Seis Sigma, dentre outras definições, pode ser considerado uma estatística por tratar cada característica crítica da qualidade, avaliando sua execução em relação à especificação obtida ou à tolerância estipulada pelo cliente (WERKEMA, 2002; PEREZ-WILSON,1999).

O Seis Sigma também pode ser considerado como uma métrica quando avaliado sob o enfoque estatístico para determinar o nível de qualidade nos processos, conhecido pela diferença entre as especificações planejadas e cumpridas, quanto menor for a diferença, melhor será a qualidade no processo (WERKEMA, 2002; PEREZ-WILSON, 1999; ECKES, 2001).

Eckes (2001) também define o conceito do Seis Sigma sob o aspecto estatístico, podendo ser interpretado como um sistema de mensuração das variações que um processo sofre até chegar próximo de alcançar um ótimo desempenho.

3.1.2 Seis Sigma como abordagem estratégica

É importante salientar que é difícil de encontrar um consenso na definição sobre Seis Sigma entre os principais autores (vide figura 7), entretanto existe uma tendência de idéias e opiniões no que se refere ao uso das ferramentas estatísticas bem como o seu entendimento (FRANZ, 2003).

Observando através da abordagem estratégica, o Seis Sigma pode assumir vários enfoques diferentes. A General Eletric, considerada uma empresa diversificada na área de serviços e tecnologia, a qual opera em mais de 100 países obteve sucesso implantando o Seis Sigma (http://www.ge.com). A empresa adotou uma estratégia inteiramente disciplinada, focada no desenvolvimento e alcance de produtos e serviços próximos da perfeição, orientados através da medição do quanto de defeitos existe no processo, permitindo, desta forma, que se criasse uma sistemática eficiente para eliminá-los e tornar o zero defeito uma possibilidade real (TREICHLER et al. 2002).

Outras definições apresentam o Seis Sigma como um processo rigoroso e disciplinado no auxilio do alcance das metas, com o treinamento focado na gerência, baseado nas exigências do cliente (TREICHLER et al. 2002; NEUSCHELER-FRITSCH & NORRIS, 2001).Outra definição ressalta o Seis Sigma como um sistema abrangente, permitindo uma flexibilidade para alcançar, sustentar e maximizar o sucesso organizacional com atenção voltada à gestão e melhoria dos processos de negócios, direcionado para a compreensão das necessidades dos clientes, sejam eles internos ou externos, mediados por um conjunto de fatos, dados e análise estatística (PANDE et al. 2001).

Abordagem estatística	Abordagem estratégica
"Iniciativa chave que dá suporte à companhia no seu plano de satisfação total do cliente". (MITCHELL, 1992)	"É um processo de negócio que permite à companhia melhorar drasticamente seus limites inferiores, projetando e monitorando diariamente as atividades do negócio de uma maneira que minimizem o desperdício e os recursos enquanto aumentam a satisfação do cliente". (HARRY; SCHROEDER, 2000)
"É um modo de medir a probabilidade de produzir um produto ou criar um serviço com zero defeito." (TADIKAMALLA, 1994)	
"É uma maneira de medir a probabilidade de a companhia poder fabricar ou produzir qualquer dada unidade de um produto ou serviço com zero defeito. É a categoria que significa "best in class", com somente 3,4 DPMO". (BEHARA et al., 1995)	"É uma abordagem de melhoria de negócio que busca achar e eliminar causas de falhas e defeitos no processo de negócio, focando sobre as saídas que são de importância crítica para os clientes. É uma abordagem estratégica que trabalha através de todos os processos, produtos, funções da companhia e indústrias". (SNEE, 2000)
"Estratégia que abastece as companhias com uma série de intervenções e ferramentas estatísticas que podem levar a ganhos substanciais em lucratividade e qualidade, tanto para produtos como serviços". (HARRY, 1998)	"Um sistema abrangente e flexível para alcançar, sustentar e maximizar o sucesso empresarial. É singularmente impulsionado por uma estreita compreensão das necessidades dos clientes, pelo uso disciplinado de fatos, dados e análise estatística e a atenção diligente à gestão, melhoria e reinvenção dos processos de negócios". (PANDE et al., 2001)
"É uma abordagem quantitativa disciplinada para melhoria de métricas definidas em processos de manufatura, serviço ou financeiro". (HOERL, 1998)	
"É uma abordagem de alto desempenho, direcionada para dados para analisar as causas raízes dos problemas do negócio a fim de resolvê-los. Ela amarra os resultados de um negócio aos requisitos de mercado". (BLAKESLEE, 1999)	"Uma estratégia para melhoria de negócios usada para melhorar a lucratividade do negócio, eliminar refugo, reduzir custo da não qualidade e melhorar a eficiência e eficácia de todas as operações, assim como encontrar, ou mesmo exceder as expectativas e necessidades dos clientes". (CORONADO; ANTONY, 2002)
"É um nível otimizado de performance que se aproxima do zero defeito em um processo de confecção de um produto, serviço ou transação. Ele indica a obtenção e a manutenção de uma performance de alto nível. O Seis Sigma não é uma metodologia. É um fim, não um meio". (PEREZ-WILSON, 1999)	"Para nós, Seis Sigma é mais do que uma metodologia e um conjunto de ferramentas. É também um modo de pensar que possibilita-nos mudar o modo de trabalho para torná-lo mais dirigido aos dados. Seis sigma afasta-nos da decisão baseada na intuição". (MOTWANI et al., 2004)
"Seis Sigma é baseado nas velhas idéias de engenharia da qualidade destinadas a entender e eliminar as causas de variação e projetar a manufatura". (DALE et al., 2000)	"Hoje, Seis Sigma é uma estratégia abrangente de longo prazo para tomada de decisão mais do que um programa estritamente focado na gestão da qualidade" (ARNHEITER ; MALEIYEFF, 2005)
"Seis Sigma é uma poderosa estratégia de negócios que emprega uma abordagem disciplinada para capturar variabilidade dos processos, usando a aplicação de ferramentas e técnicas estatísticas e não estatísticas de forma rigorosa". (ANTONY, 2004)	"Seis Sigma é uma abordagem que impulsiona a melhoria do desempenho do negócio e a valorização da satisfação dos clientes, por meio do enfoque estratégico de gerenciamento; da aplicação do pensamento estatístico em todos os níveis de atividades; da medição de desempenho; da utilização de uma metodologia sistematizada que integre técnicas e métodos científicos para se avaliar e otimizar processos; e da aprendizagem decorrente da capacitação e comprometimento das pessoas". (SANTOS, 2006)

Figura 7 - Definições Seis Sigma.

Fonte: SANTOS & MARTINS (2008).

Segundo (Harry, 2000) o Seis Sigma pode ser visto como um sistema estratégico e tático se observado em um nível mais aprofundado para o gerenciamento total no desenvolvimento de negócios, sendo um ingrediente chave para o seu êxito. O autor ainda ressalta que o Seis Sigma remete a idéia de que os defeitos representam riscos, embora nem toda a forma de risco possa ser interpretada em termos de defeito. Desta forma, o Seis Sigma também se evidencia como um programa de qualidade, sendo possível alinhá-lo com a idéia de diminuição de riscos do que a de redução de defeitos.

A incorporação dos conceitos Seis Sigma pela alta direção da organização, através de uma postura de comprometimento e de reconhecimento de seus benefícios é um dos elementos chave de sucesso de implantação da abordagem, sendo complementada pela adoção de uma metodologia de solução de problemas que possa ser compreendida e empregada por todos que fazem parte da organização (PEREZ-WILSON, 1999).

O método mais utilizado na implementação do Seis Sigma é o DMAIC (Snee, 2007) e a definição das ferramentas da qualidade a ser empregado em cada uma das fases do método DMAIC irão variar de organização para organização sendo definidas de acordo com objetivos, natureza do problema, necessidades e metas traçadas no início do projeto Seis sigma.

3.2 Método DMAIC

Existem muitas referências na literatura sobre o DMAIC, sendo que é muito comum encontrar denominações caracterizando-a como uma metodologia de solução de problemas (AGUIAR, 2006). Pande et al. (2001) define o DMAIC como sendo uma ferramenta que tem como fundamentos: identificar, quantificar e minimizar as fontes de variação de um processo, assim como sustentar e melhorar o desempenho deste processo. Pyzdek (2003) e Blauth (2003) mencionam o DMAIC como um modelo sistematizado de melhoria contínua de processos. Por outro lado, Snee (2007) define o DMAIC como um método que auxilia na resolução de problemas de um modo mais rápido, produzindo uma infra-estrutura de melhoria na organização. Deste modo, havendo inúmeras denominações, para fins de padronização, neste trabalho o DMAIC será referenciado como um método.

A abordagem Seis Sigma utiliza como método de condução o D-M-A-I-C, que é o acrônimo representado por: Definir-Medir-Analisar-Implementar-Controlar (Rath & Strong, 2001) ou seja uma estrutura disciplinada e rigorosa para alcançar a melhoria do processo composta pelas 5 fases, onde cada fase é logicamente ligada com a fase anterior assim como a posterior (vide figura 8).

O método DMAIC advém do modelo MAIC (Medir-Analisar-Implementar-Controlar) o qual foi desenvolvido inicialmente na Empresa Motorola como uma evolução do ciclo PDCA (Planejar, Executar, Controlar, Agir) e logo depois adotado pela *General Electric Company* como DMAIC passando ser a base operacional do Seis Sigma para essas empresas (ROTONDARO et al. 2006).

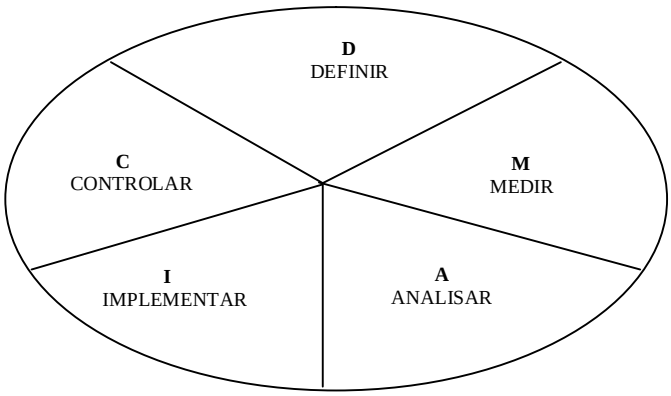


Figura 8 - Método DMAIC de controle de processos.
Fonte: Adaptado de AGUIAR (2006).

Na concepção de Snee (2007) o DMAIC é o melhor meio para alcançar a qualidade, sendo considerado um método que prevê menos desperdícios, pois trabalha em função dos fatores chaves para o processo, resultando assim em uma maior eficiência ao alcance das metas. Segundo Lynch, Bertolino & Cloutier (2003) este método é análogo a um funil, ou seja, uma grande oportunidade de uma organização ter seu escopo gradativamente estreitado, através de definições iniciais do projeto Seis Sigma e as ferramentas Seis Sigma. O resultado produzido revela um problema que pode ser entendido de forma clara com um foco bem definido, mediadas por variáveis chaves do processo, contribuindo com a obtenção das metas mais facilmente (WERKEMA, 2004).

A metodologia PDCA (Planejar-Executar-Verificar-Agir), conforme Pande et al. (2001) é muito utilizada em sistemas de gestão, sendo considerada similar ao DMAIC (AGUIAR, 2006). O que se verifica é que há apenas pequenas variações, com maior ênfase em uma ou outra etapa da cada método. Deste modo, se a empresa já faz uso de um método para solução de problemas diferente do DMAIC, então é aconselhável que permaneça usando aquele no qual a organização já esteja familiarizada (Pande et al. 2001). A Norma NBR ISO/IEC 27001:2006 que é uma norma de certificação de Sistemas de Gestão de Segurança da Informação indica a metodologia PDCA, porém, havendo de fato a equivalência entre PDCA e DMAIC (Aguiar, 2006), a intenção de uma futura certificação por essa norma não será problema, pois suas fases se relacionam. Essa relação entre ambos os modelos pode ser verificada na figura 9.

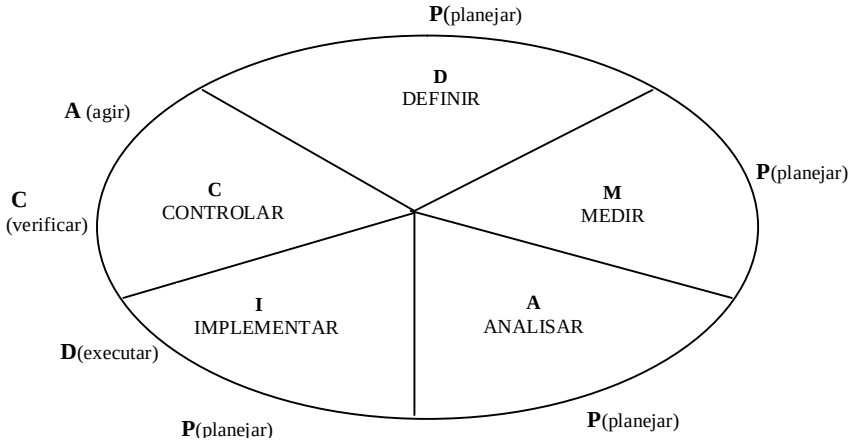


Figura 9 – Relação do DMAIC com o PDCA.
Fonte: Adaptado de AGUIAR (2006).

A seguir será detalhada cada fase do método DMAIC bem como as ferramentas da qualidade sugeridas em cada uma dessas fases. A escolha das ferramentas da qualidade a ser empregada em cada uma das fases irá depender da natureza do problema, cabendo a organização avaliar quais se adaptam melhor ao contexto (FERNANDES & ABREU, 2006).

3.2.1 Fase Definir

Na fase Definir é estabelecida a razão fundamental para o desenvolvimento de um projeto Seis Sigma (RASIS et al. 2002; WERKEMA, 2002; PANDE et al. 2001 e ROTONDARO et al. 2006). O que se sugere é que sejam feitas perguntas para definir o tema de um projeto Seis Sigma como por ex: Qual é o problema? Qual a meta a ser atingida? Quanto tempo irá levar? Sendo importante, o estabelecimento de um cronograma com a previsão de tempo de todas as fases.

Estas são perguntas que precisam ser consideradas para a definição dos requisitos iniciais de todo processo de condução do Seis Sigma. Definir quais são os requisitos do cliente, que no caso da Gestão da Segurança da Informação são os clientes internos ou os usuários que fazem parte da organização, é um outro fator importante nesta fase, sendo que na visão de Rotondaro et al. (2006) a “voz do cliente” traduz as reais necessidades do contexto organizacional em características críticas para a qualidade.

Uma das questões centrais em projetos Seis Sigma é a definição do escopo de trabalho, ou seja, qual será a cobertura do projeto, as áreas envolvidas, as esferas que serão

alvo em todo processo. A seguir na fase de definição do Projeto Seis Sigma, algumas definições de equipe e ferramentas da qualidade são aconselhadas nesta etapa do método DMAIC. Dentre estas ferramentas que podem ser utilizadas durante a implantação de um projeto Seis Sigma, são abordadas a seguir algumas práticas e ferramentas indicadas a serem utilizadas na fase Definir.

3.2.1.1 Equipe de Trabalho

Definir uma equipe de trabalho é um fator muito importante na fase Definir do DMAIC, sendo uma condição indispensável para a condução do projeto Seis Sigma e caracterizando-se como um elemento fundamental para o sucesso do projeto (PYZDEK, 2003). Segundo Snee (2001) as pessoas podem ser consideradas o pilar de sustentação para o alcance de resultados em um processo que envolve a mudança organizacional, sendo assim cada organização deve definir sua equipe ou time de trabalho da forma que melhor se adapte a sua realidade. As funções que fazem parte da equipe Seis Sigma foram propostos pela Motorola, que teve como inspiração a filosofia das artes marciais (HARRY, 1998). As funções assim denominadas (ROTONDARO et al. 2006):

- Executivo líder: normalmente é composta pela alta gerência e é responsável pela condução, incentivo e supervisão da aplicação da metodologia na organização e também por selecionar os executivos (diretores e gerentes e chefes de departamento) que irão fazer parte da equipe;
- O Campeão: essa função é mais comum em organizações de grande porte com várias divisões. As suas responsabilidades são organizar e guiar o começo e o desdobramento da implementação do seis sigma por toda a organização;
- Master Black Belt: essa função também é mais comum em empresas de grande porte. São pessoas que já tenham experiência na implantação do Sei Sigma. Suas responsabilidades são: criar mudanças na organização, oferecer ajuda aos campeões, treinar e instruir os Black Belts e Green Belts;
- Black Belts: são, juntamente com os Green Belts, elementos chaves do sistema. Suas responsabilidades são aplicar as ferramentas e os conhecimentos do Seis Sigma em projetos específicos e orientar os Green Belts na condução dos grupos;
- Green Belts: suas responsabilidades é auxiliar os Black Belts na coleta de dados e no desenvolvimento de experimentos.

Para configuração da equipe de implantação da Gestão de Segurança da Informação seguindo a abordagem de equipe Seis Sigma, Oliveira et al. (2008) realizaram um alinhamento dos dois conceitos no qual determinou-se a formação do grupo, bem como suas responsabilidades na condução de todo processo de implantação da Gestão da Segurança da Informação. Este relacionamento pode ser visto na tabela 3.

Tabela 3. Relação da equipe de trabalho Seis Sigma com a GSI.
Fonte: OLIVEIRA et al. (2008).

Seis Sigma-Equipe de Trabalho	**Gestão da Segurança da Informação- Equipe de Trabalho**	**Função**
Executivo líder	Diretores	Incentivar e supervisionar a aplicação da metodologia na organização
Campeão	Chefes de Setores ou divisões	Prover aproximação da equipe de implantadores do Seis Sigma por toda a organização
Master Black Belt	implantadores 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 e implantar a segurança da informação
Black Belt	implantadores da Segurança da Informação	Implantar a Segurança da Informação, definir ferramentas e instruir os Green Belts
Green Belt	implantadores da Segurança da Informação	Implantar a Segurança da informação e auxiliar os Black Belts

3.2.1.2 Brainstorming

O Brainstorming (Plsek & Onnias, 1989) é uma técnica muito utilizada na implantação do Seis Sigma por ser uma prática que visa a reunião de pessoas para gerar idéias, tendo como finalidade a resolução de algum tipo de problema, re-projeção de um produto ou criação de um processo, produzindo um grande número de idéias ou sugestões em um menor espaço de tempo possível.

Na fase Definir o Brainstorming é empregado para obter um melhor conhecimento da organização e conseqüentemente dos problemas vividos por ela. O objetivo principal ao usar a técnica é buscar a diversidade de opiniões e idéias, sendo por este objetivo, a técnica mais

difícil de ser utilizada, pois está mais centrada na habilidade e disposição das pessoas do que em recursos gráficos ou matemáticos (OLIVEIRA, 1995).

Segundo Plsek & Onnias (1989) os fatores chaves para o sucesso do Brainstorming são:

- Fluência - grandes quantidades de idéias independente de seu valor ou qualidade;
- Flexibilidade - idéias de diferentes categorias
- Originalidade - quando a equipe é capaz de formular idéias totalmente novas;
- Percepção - tentar ir além do óbvio na visão das pessoas sobre os problemas; e,
- Impulsividade - tentar sem medo de errar. Estimular a participação de todos, sem a preocupação se idéia é errada ou certa.

3.2.1.3 Entrevistas

A entrevista pode ser uma técnica muito eficiente para escutar a “voz do cliente” (ROTONDARO et al. 2006). A técnica é considerada uma conversa orientada para um objetivo especifico de obter, através de interrogatório, dados para a pesquisa (SERVO & BERVIAN, 2002). Porém Goldenberg (1997) assinala que, para uma entrevista ser bem sucedida é necessário criar uma atmosfera “amistosa” que passe confiança ao entrevistado, onde não se deve discordar jamais das suas opiniões, agindo com neutralidade. Segundo Gil (1999), a entrevista é diferente do questionário, sendo consideradas técnicas distintas. Se comparada com questionário à entrevista possui algumas vantagens, como a possibilidade de obtenção de um maior número de respostas, razão pela qual é mais fácil uma pessoa não querer responder a um questionário do que não querer ser entrevistado. A entrevista oferece uma interatividade que facilita entrar em particularidades de um determinado assunto que esta sendo discutido (SILVA et al. 2006). Conforme (Bauer & Gaskell, 2002) as formas de entrevistas são caracterizadas como:

- Não estruturada - nesta técnica não é obedecido um roteiro preestabelecido, é baseado apenas em uma ponto central ou questão motivadora inicial, não devendo haver a interferência do entrevistador, favorecendo para seja obtido uma grande quantidade de dados qualitativos. A pessoa entrevistada tende a participar mais, pois é dada uma maior liberdade.

- Estruturada - é realizado através de um conjunto de perguntas estruturadas de forma precisa, é muito usado na obtenção de dados qualitativos, permitindo também a obtenção e análise de dados quantitativos.
- Semi-estruturada - baseia-se em algumas questões ou guias, onde na maioria das vezes são abertas. Durante a realização da entrevista pode-se introduzir outras questões, que vão surgindo no decorrer da entrevista com o objetivo de coletar mais informações acerca do problema.

3.2.1.4 Fluxograma

É utilizado para auxiliar, obter, visualizar e apresentar as etapas do processo, indicando o fluxo de trabalho ou de informações (Aguiar, 2006). O entendimento do processo na fase Definir é fundamental para que se tenha uma visão do cenário no qual está sendo trabalhado, sendo está ferramenta um eficiente instrumento para contribuir neste entendimento. Os fluxogramas dão suporte à análise dos processos tornando-se um meio eficaz para o planejamento e solução de problemas, no entanto sua aplicabilidade só será efetiva se o processo for verdadeiramente representado (OLIVEIRA, 1995). Ainda este autor define o fluxograma como sendo “um ciclo de aprimoramento da qualidade e solução de problema”. Algumas aplicações em que o fluxograma poderia atuar:

- Definição de Projeto - identificar as oportunidades para mudanças nos processos, definir os limites de análise do estudo e desenvolver uma base de conhecimento que seja comum entre todos os membros da equipe implantadora do projeto.
- Identificação das causas primárias – elaboração de planos para determinar a coleta de dados, fornecer subsídios para geração das causas primárias, identificar caminhos dos dados e analisar o tempo requisitado para as diversas etapas pertencentes ao processo.
- Avaliação de soluções - Determinar áreas que serão atingidas pelas mudanças que forem propositadas.

3.2.1.5 Diagrama de Causa e Efeito

O diagrama de Causa e Efeito é também conhecido como "espinha de peixe" por causa do seu formato gráfico. De acordo com Rotondaro et al.(2006) esta ferramenta é um eficiente

instrumento para fornecer o relacionamento entre o problema a ser tratado e as suas causas através de uma apresentação visual (vide figura 10). No entanto, é necessário que se tenha uma abertura do campo de visão mais ampla possível, pois somente assim se garantirá o conhecimento sobre o "todo" em relação ao problema, e devendo, portanto, ser implementada com a participação de um grupo de colaboradores podendo ser realizado após as sessões de *brainstorming* (OLIVEIRA, 1995). Ainda este autor define algumas premissas para o desenvolvimento desta técnica caracterizando-se em 5 pontos principais:

1.° Definir o efeito/sintoma: a equipe deverá definir de forma clara o problema a ser tratado, sendo que nenhuma dúvida deverá permanecer sobre a natureza deste problema.

2.º Identificar as possíveis causas: caracterizar as possíveis causas que provocam um determinado efeito. Essa reposta pode advir de um *brainstorming*.

3.º Completar as espinhas: a partir do arranjo das causas sobre as "espinhas" novas sugestões serão manifestadas. A divisão das causas no diagrama deve ser fácil visualização para evitar confusão visual. Novas espinhas poderão ser inseridas conforme o nível de aprofundamento da investigação do problema.

4.° Revisar todo o diagrama: ao finalizar o diagrama é recomendado fazer uma investigação a partir da causa primária, ou seja verificar se a causa provoca realmente o efeito ao qual se esta explorando.

5.º Encontrar a causa principal: para isso é preciso se deter em características básicas da causa principal, que são: se ela é diretamente controlável; está relacionada ao efeito estudado e se sua eliminação provocará redução do efeito.

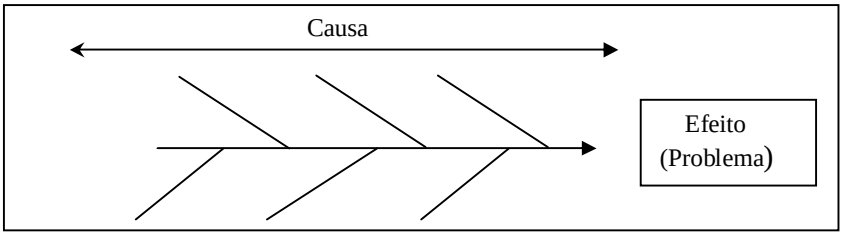


Figura 10 – Diagrama de Causa e efeito.

Fonte: Adaptado de OLIVEIRA(1995).

3.2.1.6 Lacuna de Desempenho (*gaps*)

Um dos grandes princípios sustentados pela abordagem Seis Sigma é a importância do envolvimento das pessoas em todo seu processo de execução, as quais podem ser funcionários, coordenadores, diretores. Umas das formas de se definir o problema a ser atacado é escutando a "voz do cliente", onde segundo Pande et al. (2001) é o ponto de partida para qualquer processo de melhoria, pois são realmente as pessoas que vivem o dia-a-dia da organização, que conhecem os problemas, convivem com as vulnerabilidades e são elas que podem auxiliar a definir o que é importante no serviço de segurança da informação. Deste modo, uma forma de buscar essa definição é a partir da identificação das lacunas de desempenho ou "*gaps*" (ROTONDARO, 2006).

Constata-se a existência de 7 lacunas potenciais de percepção na prestação de serviços, são elas: lacuna no conhecimento; lacuna nos padrões; lacuna na entrega ; lacuna nas comunicações internas; lacuna nas percepções; lacuna na interpretação; e lacuna no serviço LOVELOCK E WRIGHT (2001). Nesta seção apresenta-se uma aplicação do modelo de lacunas à avaliação da satisfação do cliente com relação a qualidade do serviço de segurança da informação

Parasuraman et al. (1985) propõe um modo de medir a qualidade do serviço chamado de modelo *gap*, baseado na satisfação do cliente. Dessa forma, a avaliação da qualidade de um serviço, por um cliente, é feita por meio da diferença entre a sua percepção (P) e a sua expectativa (E) de acordo com a seguinte equação

$$Q = P - E \qquad (1)$$

Onde:

P - é a medida de percepção para característica do serviço;

E - é a medida da expectativa para característica do serviço; e

Q - é a avaliação da qualidade do serviço em relação à característica do serviço ou o *gap*, podendo também ser conceituada como uma medida da qualidade do serviço em relação a uma característica específica.

O modelo proposto por Parasuraman et al. (1985) baseia-se em cinco lacunas (*gaps*), ou cinco diferenças cujas características são:

- *Gap* 1 – Lacuna entre as verdadeiras expectativas do usuário e a percepção dessas expectativas pelos gerentes.
- *Gap* 2 – Lacuna entre a percepção gerencial acerca das expectativas dos usuários e a tradução dessa percepção em normas e especificações (padrões) para atender às expectativas dos usuários.

- *Gap* 3 – Lacuna entre as normas e especificações (padrões) e o serviço efetivamente fornecido usário.
- *Gap* 4 – Lacuna entre o serviço realmente prestado e a comunicação externa.
- *Gap* 5 – Lacuna entre a percepção do serviço e a expectativa para este.

Apresentada a proposta de avaliação da qualidade do serviço, Parasuraman et al. (1985) constataram que o serviço independente do tipo, ao ser avaliado pela duas óticas de percepção e expectativa, os mesmos critérios são sempre utilizados para se chegar a uma qualidade na avaliação. Estes critérios puderam ser generalizados em 10 categorias denominadas de dimensões da qualidade. Essas dimensões representam os fatores críticos para a qualidade de um serviço, que podem causar a discrepância entre percepção e expectativa. Essas 10 dimensões são:

- Responsividade - capacidade de ajudar o usuário a fornecer o serviço prontamente;
- Confiabilidade - habilidade de cumprir com exatidão;
- Cortesia - cortesia estendida aos usuários;
- Acesso - condição de acesso aos serviços de informação;
- Comunicação - habilidade de comunicação com usuários, a forma ou meio de comunicação;
- Credibilidade- confiança no trabalho que está sendo realizado;
- Segurança - segurança no serviço prestado incluindo a confidencialidade;
- Compreensão - entendimento sobre o que está sendo feito; e,
- Tangíveis - aspectos físicos do que é fornecido pelos usuários como computadores, impressoras, instalações, entre outros.

A partir dessas dez dimensões de qualidade de serviços, foi desenvolvida um instrumento de coleta de dados chamado de escala SERVQUAL (*Service Quality*) (PARASURAMAN et al. 1988). O SERVQUAL consiste num questionário de duas declarações afirmativas, fazendo referência à expectativa do usuário e à sua percepção da qualidade do serviço. O questionário se baseia em uma escala *Lickert* de 5 ou 7 pontos, variando de “discordo totalmente” a “concordo totalmente”.

Finalizada esta fase, o próximo passo do método DMAIC é a mensuração, fase discutida na seção seguinte.

3.2.2 Fase Medir

O Seis Sigma é um método que se baseia no uso de instrumentos estatísticos para entender o comportamento de produtos e processos. Um tipo de atividade crucial no Seis Sigma é a definição e medição das variações com a intenção de descobrir as causas de problemas. Assim, podem-se desenvolver os recursos operacionais necessários para reduzir as causas destas variações e controlá-las (SANDERS & HILD, 2000). Isto demonstra a importância da fase medir durante a implantação de um projeto Seis Sigma.

Harry (1998) aconselha que nesta fase sejam selecionadas uma ou mais características Críticas à Qualidade (CTQ – Critical to Quality) através da mensuração, ou seja, o que de fato precisa ganhar uma atenção maior, pois é considerado crítico para a obtenção da meta desejada. Desta forma são realizadas ações com base nas informações capturadas na etapa definir com o intuito de avaliar o quanto o processo abordado é importante e quais os pontos a serem 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 a mensuração realizada nesta fase depende da utilização de ferramentas da qualidade que auxiliarão principalmente, na tomada de decisões como base nas reais necessidades das organizações. A seguir são apresentadas algumas das ferramentas utilizadas na fase Medir.

3.2.2.1 FMEA (Failure Mode and Effect Analyses)

Alguns autores como Werkema (2002); Rotondaro et al. (2006) mencionam o uso da ferramenta FMEA em projetos Seis Sigma e mais precisamente sugerem a sua utilização na fase medir.

A ferramenta identifica todos os possíveis modos potencias de falha, determinando o efeito de cada um sobre o desempenho do processo ou produto. Segundo Helman & Andery (1995) o FMEA é considerado um método analítico padronizado para realizar a detecção e eliminação de problemas que são potenciais ao negócio de forma sistemática e completa. Maddox (2005) reconhece o FMEA como sendo uma das ferramentas mais difundidas entre as empresas e que tem como propósito a colaboração na determinação de prioridades no processo de gerenciamento de riscos (MADDOX, 2005). Sua característica principal é ter uma dinâmica que preza pela documentação formal permitindo: padronizar documentos; fazer

registros históricos de análise que poderão auxiliar numa etapa posterior e desta forma facilitar outras revisões do processo (escopo definido) para o encaminhamento de ações corretivas; e selecionar e priorizar ações de melhoria que devem ser conduzidos.

Dependendo da fase do projeto Seis Sigma em que o FMEA está sendo utilizado, ele pode permitir diferentes resultados (ROTONDARO, 2002):

- fase Medir - pode ser usado para a identificação das características críticas para o cliente;
- fase Analisar - pode ser usado para realizar a ligação entre causas e efeitos;
- fase Melhorar, pode chegar-se a determinação de ações de melhorias a serem tomadas;
- na fase Controlar, o FMEA pode ser utilizado para o desenvolvimento de planos de controle de processo e de produto.

A realização do FMEA é feita usando-se um formulário padronizado. Um exemplo de um formulário de FMEA é apresentado na Figura 11.

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas											
Projeto:			Cliente:								
Gerente do Projeto:			Data do FMEA:								
Data início Projeto:			Data Conclusão Projeto:								
Controle	Modo de Falha	Efeito	Causa	Controles Atuais	S	O	D	RPN	Estratégia	Ações Recomendadas	Situação

Figura 11 – Formulário FMEA.

Fonte: Adaptado de ROTONDARO (2002)

O FMEA estabelece três índices para pontuar o risco podendo ser realizada com base no julgamento pessoal, por empirismo, ou com base em dados históricos ou testes. Estes índices são:

1. Índice de Severidade: dimensiona a gravidade do efeito da falha sobre o processo, ou seja, o quanto ela pode prejudicar o desempenho do processo. A tabela 4 mostra a variação destes índices.

Tabela 4 – Índice de Severidade.

Fonte: Adaptado de ROTONDARO (2002)

Índice	**Severidade**
1	Apenas perceptível
2-3	Pouca importância
4-5-6	Moderadamente grave
7-8	Grave
9-10	Extremamente Grave

2. Índice de Ocorrência: é uma estimativa das probabilidades combinadas do quanto ocorre aquela falha. As pontuações são mostradas conforme tabela 5.

Tabela 5 – Índice de Ocorrência.

Fonte: Adaptado de HELMAN, ANDERY (1995)

Índice	*Probabilidade de Ocorrência*	**Ocorrência**
1	Muita remota	Excepcional
2-3	Muito pequena	Muito poucas vezes
4-5-6	Moderada	Poucas vezes
7-8	Alta	Frequentemente
9-10	Muito Alta	Inevitável

3. Índice de Detecção: dimensiona a facilidade de detecção da falha antes que ela prejudique o funcionamento do processo, estipulado através de uma variação de índice de 1 a 10, conforme mostra a tabela 6.

Tabela 6 – Índice de Detecção.

Fonte: adaptado de Rotondaro (2002)

Índice	**Facilidade de Detecção**
1	Muita alta
2-3	Alta
4-5-6	Moderada
7-8	Pequena
9	Muito Pequena
10	Remota

Realizada a pontuação dos três índices, o próximo passo é calcular o Número de Prioridade de Risco (NPR) e definir as prioridades das ações a serem tomadas. O NPR é obtido pelo produto dos índices de severidade, probabilidade de ocorrência e facilidade de

detecção, conforme apresentado na equação (2). O valor máximo obtido pelo NPR é 1000, pois o resultado da multiplicação dos três índices (Severidade, Ocorrência, Detecção) não ultrapassa esse limite, isto supondo se os três índices recebam o valor 10.

$$NPR = S \times O \times D \qquad (2)$$

Pelos valores obtidos do NPR, serão definidas as prioridades de ações. Não existe e nem é recomendável a atribuição de um limite teórico de NPR a partir do qual devam ser tomadas as ações após a realização do FMEA. Cada processo tem sua particularidade e a predefinição de valores para tomada de decisão o que pode influenciar a atribuição dos índices pelo grupo. Os problemas sobre os quais serão tomadas ações devem ser aqueles com valores de NPR mais altos (ROTONDARO et al. 2006). Por fim, o resultado gerado com o NPR define uma maneira mais precisa de hierarquizar os riscos e com isso priorizar ações mais urgentes para saná-los ou mitigá-los. Depois de implantadas ações ou estratégias para reduzir os riscos é possível revisar a planilha do FMEA e observar se os problemas focalizados realmente tiveram seus NPR´s reduzidos.

3.2.2.2 Diagrama de Pareto

O princípio de pareto defende que as melhorias mais significativas podem ser obtidas se nos concentrarmos nos “poucos problemas vitais” e, depois, nas poucas “causas vitais” desses problemas (ROTONDARO et al. 2006). O instrumento que foi desenvolvido para a aplicação deste princípio é o Diagrama de Pareto, onde segundo Oliveira (1995) é uma abordagem estatística na qual permite, através de uma representação gráfica específica, a identificação dos aspectos considerados relevantes para a qualidade. Desta forma todo o esforço de melhoria pode ser concentrado nos pontos de maior prioridade.

O diagrama ou gráfico de Pareto pode ser utilizado após a elaboração do FMEA, sendo um excelente meio de visualização para os NPRs (Número de Prioridade do Risco) que serão gerados na fase de análise e quantificação executada com a ferramenta FMEA, pois permite a identificação dos índices mais significativos.

Rotondaro et al. (2006, pp.139) comenta uma das vantagens de utilizar o Diagrama de Pareto, afirmando que:

> Além do maior poder de comunicação de um gráfico em relação a uma tabela, o fato de qualquer pessoa, em qualquer nível hierárquico da organização, vai entender o que os dados estão mostrando e, mais que isso, vai entender da mesma forma. A objetividade da apresentação dos dados e das conclusões que podem ser tiradas é patente.

Pode-se também utilizar a comparação de dois diagramas de Pareto, um antes quando forem identificados os maiores impactos e outro após as ações de melhorias tomadas. Esse comparativo facilitaria a visualização das evoluções percebida no trabalho realizado.

3.2.2.3 Box-Plot

Box-plot é uma ferramenta da qualidade, que também é recomendada nesta fase Medir do DMAIC. *Box-plot* consiste em representar um conjunto de dados para que seja possível mostrar dispersões existentes nestes dados bem como comparações e análises (ROTONDARO et al. 1995). A Construção do *Box-plot* (vide figura 12) é simples, mas exige conhecimento de elementos estatísticos como: Primeiro Quartil (1Q) - determina o valor abaixo do qual existem 25% dos dados; Mediana - valor que divide as duas partes iguais; e, Terceiro Quartil (3Q) – determina o valor abaixo do qual existem 75% dos dados.

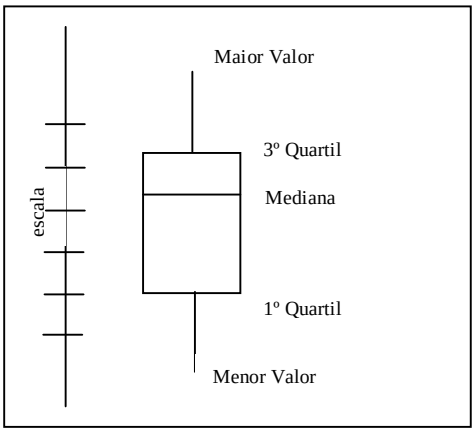


Figura 12 – *Box-Plot*
Fonte: Adaptado de ROTONDARO (2006)

Conforme Oliveira (1995) *Box-plot* é utilizado quando há interesse em visualizar características importantes de um conjunto de dados, em situações como, por exemplo:

- Monitoramento do desempenho de uma característica importante do processo;
- Comparação entre o desempenho de processos;
- Acompanhamento dos processos;

- Comparação entre o tempo dos processos.

Concluída esta etapa onde foram demonstradas algumas técnicas de mensuração que poderiam ser utilizadas na fase Medir, o próximo passo é a definição de ferramentas que venham auxiliar na análise dos resultados, identificada como a fase Analisar do método DMAIC discutido mais detalhadamente na seção seguinte.

3.2.3 Fase Analisar

Após a Medição, a fase de Análise, caracteriza-se por priorizar os processos através do entendimento das relações entre as causas e os efeitos. Normalmente segundo Chowdhury (2001) neste passo se utilizar a ferramenta de Análise do Modo e Efeito das Falhas ("Failure Mode and Effect Analysis" - FMEA), que também foi sugerida na fase anterior. É na fase Analisar que as causas fundamentais dos problemas prioritários, associados a cada uma das metas definidas durante as fases anteriores do projeto, deverão ser determinadas (WERKEMA, 2002). É claro que a escolha dos problemas que serão tratados, irá depender não somente do risco que organização corre por estar exposto a este problema como também a viabilidade da resolução daquele problema. Campos (2007) ressalta que muitas vezes ao resolver um determinado problema, a solução encontrada pode dar margens para o aparecimento de outros problemas, desta forma é muito importante pesar os pós e contras. As seguir são mostradas algumas das ferramentas que são indicadas na fase de analisar.

3.2.3.2 Histogramas

Histogramas (Paladini, 1994) são gráficos de colunas que representam a distribuição de um conjunto de dados numéricos. Na estatística, não somente a quantidade dos dados tem importância, mas a forma com que estes dados se distribuem podem contribuir decisivamente na identificação da natureza e origem dos dados (OLIVEIRA,1995). Trata-se de um gráfico formado por retângulos contíguos com base nas faixas de valores variáveis em estudo (vide figura 13). Embora se trate de um diagrama que apresente colunas dispostamente alinhadas, sendo que sua altura é a freqüência de ocorrência da classe, o histograma difere do diagrama de Pareto por justamente aplicar tipos de variáveis diferentes.

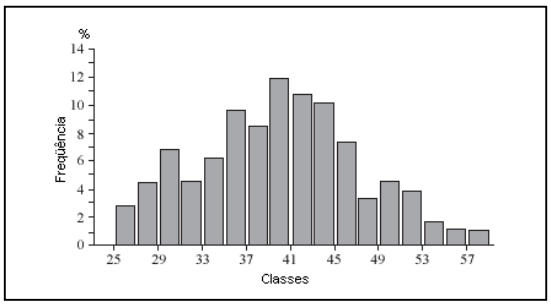


Figura 13 – Histograma

Oliveira (2005) afirma que através do histograma pode ser possível fazer inferências a respeito da natureza do problema que o originou, sendo que em alguns casos são identificadas características muito evidentes, facilitando inclusive as conclusões. Entretanto nas maioria da vezes, não é tão simples, obrigando a obtenção de informações complementares para dar mais veracidade a análise.

3.2.3.3 *Fault Tree Analysis* (FTA)

O FTA (Helman & Andery, 1995) é um método sistemático e padronizado, que tem o objetivo de fornecer bases práticas para diversas funções. Sua utilização abrange aspectos que vão desde projetos de máquinas e equipamentos até à analise de processos industriais ou administrativos.

Werkema (2002) recomenda o uso do FTA na fase de análise, sendo que seu emprego pode ser útil para:

- Auxiliar o analista a identificar de forma dedutiva as falhas do sistema.
- Assinalar os aspectos do sistema mais relevantes em relação à uma falha em particular.

Helman & Andery (1995) explicam que análise se inicia a partir de uma falha ou problema particular do sistema, motivo do estudo e prossegue com a elaboração da seqüência ou combinação de fatos que irão conduzir ao problema ou evento determinado. A árvore de falha é representada por um modelo gráfico, mostrando de maneira simples os diferentes eventos que resultam a falha.

Identificadas as medidas e técnicas que podem ser utilizada na fase Analisar, o proximo passo do método DMAIC é a fase Implementar, que determina as ações e estrategias que serão implementadas para sanar ou mimizar os problemas.

3.2.4 Fase Implementar

Esta fase também pode ser vista na literatura como “Melhorar” ou “Incorporar”, mas nesta dissertação a denominação adotada é “Implementar”. Nesta fase, 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. Com base nestas medições, a organização pode decidir se a 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 (PANDE et al. 2001; WERKEMA, 2002), como por exemplo, (*i*) Quais as ações ou idéias possíveis que podem permitir a eliminação das causas fundamentais do problema? (1) Quais dessas idéias se traduzem em soluções potenciais? (2) Que soluções permitirão o alcance da meta? (3) De que forma testar as soluções escolhidas como meio de assegurar sua eficácia e de que forma impedir a ocorrência de “efeitos colaterais”?

Pande et al.(2001) destaca, ainda, que esta fase poderá durar algum tempo já que é nesta etapa que devem ser testadas as possíveis soluções que levarão as mudanças e consequentemente ao sucesso do projeto. Algumas ferramentas podem mostrar-se particularmente úteis nesta fase, como, por exemplo: 5W2H, *Brainstorming* e FMEA (WERKEMA, 2002). A seguir é apresentada umas das principais ferramentas que pode ser usadas nesta fase a 5W1H.

3.2.4.1 Plano de Ação - 5W1H

A ferramenta 5W1H (Aguiar, 2006) é chamado plano de ação ou planejamento, sendo capaz de orientar as diversas ações que deverão ser implementadas. A sua nomenclatura advém do próprio objetivo da ferramenta sendo que, as expressões “*What, Who, When, Where, why*” somadas resulta 5W e a denominação 1H refere-se a expressão “*How*” que aparece apenas uma vez, formando a sigla 5W1H (vide figura 14).

A ferramenta serve como referência às decisões, permitindo que seja feito o acompanhamento do desenvolvimento do projeto e também servindo de documento, uma vez que a ferramenta divide de forma organizada as ações, responsabilidades e o tempo pela execução de cada tarefa (Aguiar, 2006).

Embora a 5W1H, seja considerada uma ferramenta de caráter gerencial, ela se aplica, perfeitamente, à realidade das equipes de aprimoramento no planejamento e condução de suas atividades. Tradicionalmente, na literatura é encontrada a expressão 5W2H, este acréscimo de mais um "H" deve-se ao fato de que o custo é um fator relevante (OLIVEIRA, 1995).

O que (What)?	Quem (Who?)	Quando (When)?	Onde (Where)?	Porque (Why)?	Como (How)?
Contramedidas	Responsável	Prazo	Local	Justificativa	Procedimento

Figura 14 – Plano de Ação – 5W1H.
Fonte: Adaptado de AGUIAR (2006).

Identificadas as medidas e técnicas que podem ser usadas na fase implementar, o passo seguinte do método DMAIC é a fase Controlar, considerado uma das etapas mais importantes e díficeis, pois identifica a efetividade do sucesso ou não do projeto Seis Sigma e consequentemente a possibilidade de garantia de sua sustentabilidade.

3.2.5 Fase Controlar

A fase Controlar envolve o fechamento das melhorias de um projeto Seis Sigma (RASIS et al., 2002-03). O propósito desta fase do DMAIC é assegurar que os benefícios obtidos na fase Implementar sejam de fato mantidos na organização. Para isso é importante a continuidade das medições com uso das ferramentas já mencionadas até aqui, como o FMEA. No entanto, se essas medições não confirmarem os resultados, a equipe deve retornar à etapa Medir. Uma vez que estes resultados se sustentam com o tempo, a equipe deve padronizar as alterações que foram feitas com a implantação da solução, levando em conta mecanismos de prevenção e detecção de problemas como o Poka-Yoke que foca o erro humano (FERNANDEZ & ABREU, 2006). Segundo Shingo (1996) a utilização do Poka-Yoke como uma ferramenta de redução de erros pode seguir duas abordagens: método de controle - quando o Poka-Yoke é ativado, o processo para de funcionar até que o problema identificado seja solucionado; e o método de advertência - é utilizado alertas e sinalizadores para que seja cumprida as regras. Ao relacionar esta ferramenta com a gestão da Segurança da informação e mais especificamente com a política de segurança, o Poka-Yoke pode ser uma ferramenta

útil para auxiliar na adesão as regras expostas neste documento podendo ser utilizado o método de advertência para este propósito.

Adams et al. (2003) recomendam que os resultados que foram obtidos até esta fase sejam divulgados dentro da organização e que sejam replicadas em outras áreas. Esta é uma oportunidade para que sejam relatadas experiências e novos conhecimentos para os próximos projetos da organização.

Uma forma de controlar e acompanhar as ações implantadas é através do uso de indicadores, pois segundo Sink e Tuttle (1993), a medição pode ser um impulso à melhoria do desempenho e com isso assegurando que a estratégia seja implantada. A metodologia de acompanhamento dos resultados utilizando indicadores é útil para a avaliação das melhorias, uma vez que permite a verificação das mudanças do processo ao longo do tempo. O uso de indicadores é imprescindível para compreender que o gerenciamento das ações envolvidas no programa Seis Sigma é parte do gerenciamento do desempenho, e que os indicadores podem ser usados não apenas para controlar a implementação da estratégia de negócio, mas também direcionar os projetos Seis Sigma a fim de acrescer seu potencial (HOFF, 2005; SANTOS, 2006).

Alves (2006) caracteriza dois tipos de indicadores que podem ser utilizados em projetos que visem a gestão da segurança da informação são eles:

- Indicadores de Desempenho (*Key Performance Indicator*- KPIs) - definem o quão bem está o desempenho dos processos em relação a meta desejada, devendo ser mensuráveis, exemplo, número de treinamentos da equipe, números de projetos que utilizam a gestão de riscos.
- Indicadores de Metas (*Key Goal Indicator* - KGIs) – irão mostrar se o resultado esperado no início do projeto Seis Sigma, com as definições de metas, foi alcançado.

A Fase Controlar é ultima do método DMAIC, e pode ser considerada a etapa chave para a continuidade do projeto, pois como o princípio da Filosofia Seis Sigma é a de estar sempre monitorando, é a partir deste momento que começa realmente a transformação Seis Sigma e a sustentação das melhorias.

3.3 Conclusões Parciais

Atualmente, qualquer que seja o tipo de organização em que se trabalhe seja um hospital, um banco, uma universidade, a busca incessante da competição por clientes, estudantes ou pacientes estará sempre presente. A maioria das organizações, independente do seu domínio está ciente de que a qualidade é essencial, restando poucas pessoas que precisam ser convencidas de que a qualidade é uma das armas competitivas mais importantes (OAKLAND, 1994). A abordagem Seis Sigma promove a qualidade através da busca contínua pela melhoria através de suas duas abordagens: estatística e estratégica. Sendo assim fica evidente que todo esse processo que permeia a sua implantação de fato precisa ser baseado em dados. Esta comprovação fica clara na própria filosofia adotada pela abordagem que prevê sempre o envolvimento das pessoas, tanto na definição dos problemas que irão ser solucionados como no controle das estratégias que foram implantadas para sanar estes problemas, sendo considerado "o envolvimento das pessoas" um dos fatores chaves para a obtenção de sucesso com o Seis Sigma.

Outro ponto que merece consideração no que tange a utilização da abordagem Seis Sigma é a variedade de ferramentas da qualidade que podem ser utilizadas em todo processo. Sendo que é possível adequar cada técnica com o objetivo e meta a ser atingida, independente da natureza ou magnitude do problema. Porém, o grande trunfo da abordagem Seis Sigma é o método DMAIC, que se mostra uma base operacional consistente, caracterizadas por etapas bem definidas e metas concretas aos quais se complementam para a condução de todo o processo.

A utilização de indicadores também são extremamente importantes, são eles que determinarão se as ações que foram estrategicamente implementadas, estão sendo aplicadas de forma efetiva e com isso estabelecendo-se como uma medida eficaz para a obtenção e sustentação da melhoria.

Nesta dissertação a abordagem estratégica do Seis Sigma estará mais evidente, pois este direcionamento impulsionará a melhoria do desempenho do negócio e a valorização da satisfação dos clientes internos por meio da integração de técnicas e ferramentas da qualidade, permitindo ações mais abrangentes e flexíveis afim de obter resultados mais sustentáveis.

CAPITULO 4

PROPOSTA DE IMPLANTAÇÃO DE UMA GESTÃO DA SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA ABORDAGEM SEIS SIGMA

Neste capítulo é apresentado a proposta de implantação da Gestão da Segurança da informação através da abordagem Seis Sigma. O capítulo inicia com a fundamentação da proposta (seção 4.1) e posteriormente apresenta o planejamento das fases (seção 4.2), demonstrando uma síntese da proposição que tem como base de implantação o método DMAIC. No planejamento das fases, é descrita também os seus objetivos e ferramentas que serão utilizadas no decorrer do trabalho. Ao final é apresentado um cronograma de ação (seção 4.3) e as conclusões parciais do capítulo (seção 4.4).

4.1 Fundamentação da Proposta de Implantação

A partir do referencial teórico sobre a segurança da informação e a abordagem Seis Sigma (vide capítulos 2 e 3), constata-se que para ser efetiva, a segurança precisa permear todo o contexto organizacional, atendendo tanto aspectos estratégicos e tecnológicos, como organizacionais, humanos e ambientais. Porém, considerando o que a norma NBR ISO/IEC 17799 recomenda, economicamente é inviável atender 100% de todos estes aspectos. Mesmo assim, a busca pelo conhecimento do contexto da organização pode ser identificada nas metodologias de gestão da segurança da informação (vide seção 2.3).

Quando se trata de gestão, capturar o estado atual da organização é um requisito primário. Mesmo assim, na área de segurança ainda existem propostas de metodologias onde esta atividade é realizada de maneira superficial. Por exemplo, Martins e Santos (2005) capturam o contexto da segurança da informação na organização verificando apenas se existe alguma política de segurança. Este relaxamento advém da dificuldade de descobrir o que é mais importante ou o que é mais prioritário e urgente ou o que realmente é necessário para a organização do ponto de vista da segurança da informação.

Avaliando algumas metodologias observa-se formas diferentes, e mais efetivas, para conhecer este contexto. Vermeulen e Solms (2002) aplicam um questionário fechado baseado na BS 7799-1 (1999) e Brooks e Warren (2006) realizam um *checklist* baseado na norma HB

174-2003. No entanto, questiona-se até que ponto elas funcionam realmente e propõe-se a manutenção da gestão, e conseqüentemente das melhorias, via o conceito da Gestão da Qualidade Total, sendo a abordagem Seis Sigma apontada como instrumento para obtenção desses requisitos (Kiely & Benzel, 2005; Saleh, Alrabiah, Bakry, 2007; Sveen, Torres, & Sarriegi, 2008). Porém, embora haja o questionamento de metodologias que orientam o "como fazer" e a proposição do Seis Sigma como solução, não foi constatado uma metodologia que use o Seis Sigma e explicite o "como fazer" nas etapas previstas na adoção da abordagem. Esta proposta de implantação deste trabalho visa cobrir exatamente esta lacuna.

A hipótese inicial deste trabalho, no que se refere a gestão de segurança da informação, é que independente do seu domínio, toda e qualquer transformação que seja feita requer o apoio das pessoas. Comprovadamente se tem conhecimento de que são elas que são consideradas o elemento principal para sustentação de qualquer mudança, ou seja, para a sustentação da segurança da informação.

Deste modo, a proposta de implementação nesta dissertação utiliza, através da abordagem Seis Sigma e do método DMAIC, a construção de uma gestão de segurança da informação voltada para o cliente interno ou usuário da organização, seguindo uma estratégia onde todo o planejamento das melhorias é baseado em dados concretos gerados pelas pessoas, ou seja, com o foco nas características críticas do negócio observadas por elas.

O planejamento das fases da implantação e as definições de técnicas, procedimentos e ferramentas da qualidade que serão utilizadas em todo o processo, bem como os resultados esperados em cada fase, são detalhados na próxima seção.

4.2 Planejamento das Fases

O planejamento das fases aqui apresentado segue como princípio a abordagem Seis Sigma e como base de implantação o método DMAIC, constituído de 5 fases. Toda a concepção de implantação é centrada nas percepções e expectativas dos clientes ou usuários, portanto as ferramentas e técnicas definidas têm como objetivo o vislumbramento deste propósito. A figura 15 apresenta uma síntese da proposta de implantação através de uma seqüência de passos com os objetivos, a metodologia que consiste nas ferramentas, técnicas e procedimentos que serão empregados para obter os resultados esperados. O detalhamento de cada uma das fases é apresentado a seguir.

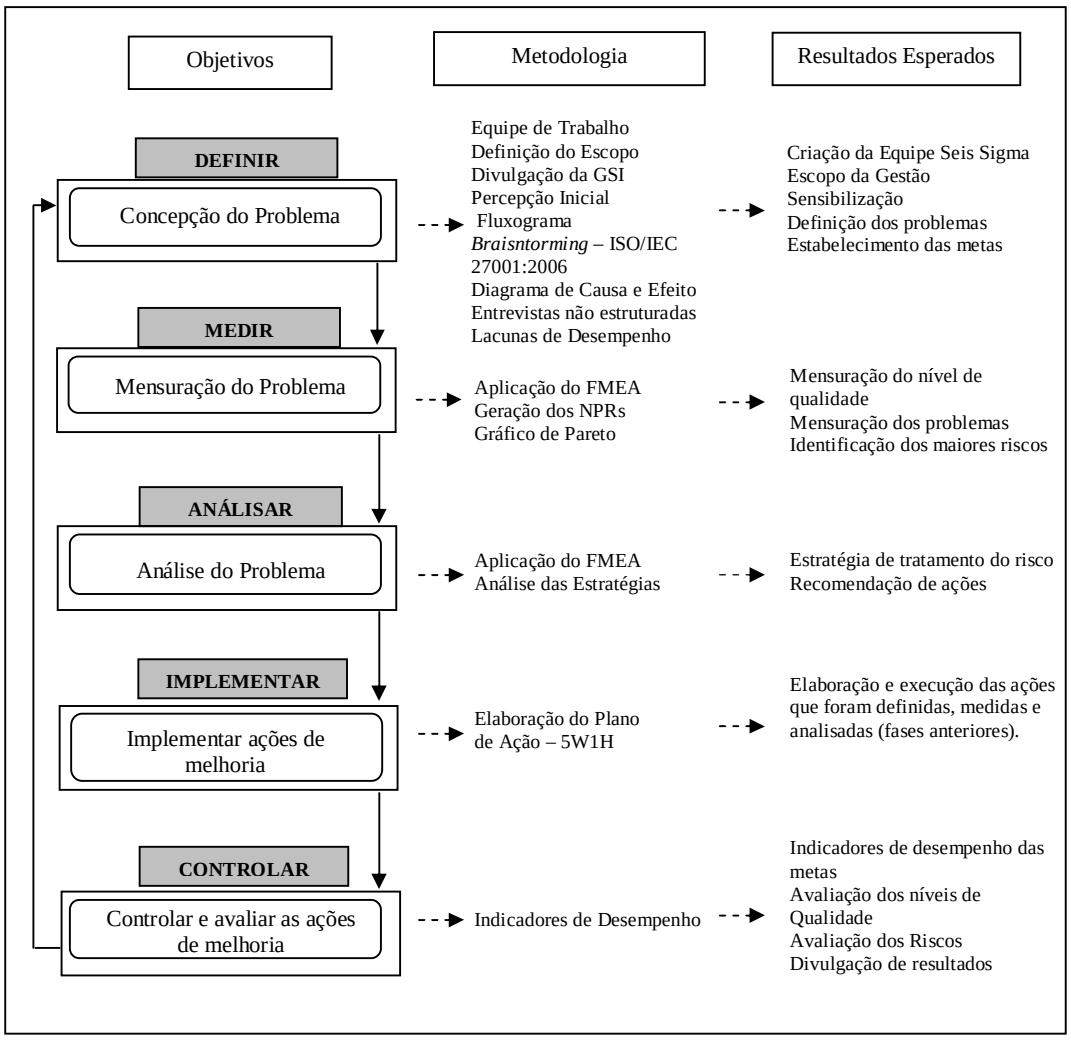


Figura 15 – Síntese da proposta de implantação da Gestão da Segurança da Informação

4.2.1 Fase Definir

Uma das primeiras tarefas desta fase é definir a equipe de trabalho Seis Sigma que irá conduzir todo o processo de gestão. Devem fazer parte desta equipe, o *BlackBelt* e os *GreenBelts*, ambos responsáveis pela implantação do Seis Sigma, o Executivo Líder, responsável pela supervisão e incentivo dos trabalhos e o Campeão, ou os Campeões, que deve estar envolvido diretamente com os *BlackBelt* e o *GreenBelts* na implantação da gestão.

Formada a equipe, deve-se preparar o marketing interno da gestão da segurança da informação na organização, tarefa importante na definição inicial dos trabalhos. O marketing interno deve promover o envolvimento das pessoas e é um dos propósitos da gestão, sendo um dos recursos indispensáveis na preparação do ambiente organizacional. As pessoas

precisam estar informadas sobre o que está acontecendo e principalmente responder as questões do "Por que?" a organização visa implantar a gestão de segurança da informação. A exposição de pôsters pode ser um bom meio para atingir essa promoção e a sensibilização com o trabalho.

A definição de um escopo é outra tarefa desta fase. Para isto propõe-se a utilização da visão STOPE (*strategy, technology, organization, people, and environment*) com o objetivo de estabelecer uma gestão que tenha uma visão sistêmica, abrangendo aspectos estratégicos, tecnológicos, organizacionais, pessoas e ambientais da organização. Deve ser obtido nesta fase a captura do diagnóstico inicial sobre a relevância do tema segurança da informação pela organização e a percepção que as pessoas tem com as mudanças que serão geradas. Essa captura pode ser obtida através da aplicação de questionários ou entrevistas não-estruturadas, contribuindo para uma maior liberdade ao entrevistado, o que pode favorecer positivamente na coleta de informações. Estas percepções iniciais poderão ser um diagnóstico importante nesta fase, pois irá determinar a importância do tema para a organização e o quanto elas estão dispostas a contribuírem para que a gestão realmente aconteça.

Para auxiliar na busca pelo problema propõe-se o emprego da técnica de *brainstorming*, utilizando como apoio a norma de segurança NBR ISO/IEC 27001:2006. O propósito de usar a norma é contribuir para o direcionamento do tema a ser desenvolvido através de reuniões com grupos de funcionários e a equipe Seis Sigma, facilitando a definição dos problemas que eles acreditam estarem presentes na organização. O fluxograma também é indicado para estabelecer o entendimento da organização como um todo, procurando identificar as vulnerabilidades e pontos críticos que poderão existir no cenário alvo. Adicionalmente, o diagrama de Causa e Efeito pode ser utilizado para descobrir e aprofundar as causas dos problemas resultantes da seção do *brainstorming* e as lacunas de desempenho podem ser utilizadas para capturar os *gaps* ou diferenças em relação a percepção existente sobre o problema e a expectativa de solução para ele.

O resultado produzido por esta etapa deverá ser a formação de uma equipe capaz de atuar em toda a implantação do projeto, a definição do escopo da gestão, a sensibilização dos usuários, a definição dos problemas juntamente com suas causas e o estabelecimento de metas a serem atingidas.

4.2.2 Fase Medir

A segunda fase tem objetivo de medir o problema que foi definido na primeira fase, procurando identificar as características críticas para a qualidade. É através da mensuração que se descobre o que de fato precisa ganhar uma atenção maior. Nesta fase é necessário medir a qualidade da segurança da informação com relação às metas que serão estabelecidas. Isto deve fazer com que se tenha o nível de qualidade, antes da implantação das ações, sendo possível ao final, na fase controlar, verificar se houve diferenças na qualidade percebida antes e após as melhorias.

A ferramenta FMEA (*Failure Mode and Effect Analyses*) pode ser utilizada nesta fase tendo como propósito, investigar a razão de determinado problema ocorrer e o efeito que este tem sobre a organização se não for combatido. O FMEA resultará o valor de cada risco, denominando o Número de Prioridade do Risco (NPR). O diagrama de Pareto pode então ser utilizado para demonstrar os resultados gerados pelo FMEA e facilitar a identificação dos maiores índices de risco.

4.2.3 Fase Analisar

A terceira fase consiste em analisar as constatações dos maiores índices de riscos, obtidas na fase medir, e estabelecer estratégias de ações para cada problema mensurado. Para isto, pode-se continuar utilizando a ferramenta FMEA, uma vez que os dados que serão analisados também são derivados da mesma ferramenta.

É nesta fase que devem ser definidas as estratégias de tratamento de risco para cada problema. Dentre as estratégias de ações para o tratamento do risco, pode-se escolher entre as seguintes opções:

- Minimizar o risco – através da aplicação de controles
- Aceitar o risco – considerar sua existência, mas não efetuar nenhuma medida
- Transferir o risco – transferir a solução do risco para terceiros, por exemplo, o administrador de rede.
- Negar o risco – ação menos recomendada, a não ser que esse risco não ofereça nenhuma preocupação para a organização.

A escolha dos problemas que serão tratados depende não somente do risco que a organização corre por estar exposta, mas também da viabilidade de resolução do problema por parte da organização.

Como resultado, esta fase deve apontar recomendações de ações para tratamento dos riscos da organização.

4.2.4 Fase Implementar

A fase Implementar é responsável pela execução das estratégias definidas na fase anterior. É na nesta fase que as soluções para os problemas devem ser desenvolvidas e mudanças são realizadas. O objetivo é agir para tentar amenizar e resolver o problema através da minimização dos seus riscos. A principal ferramenta de gestão a ser utilizada nesta fase é o Plano de Ação - 5W1H. Esta ferramenta pode servir de referência às decisões, permitindo que seja feito o acompanhamento do desenvolvimento da implementação de todas as ações. A 5W1H também ajuda na produção de um documento que, de forma organizada, realiza a identificação dos objetivos, das responsabilidades pela execução e a previsão de tempo para cada tarefa planejada, funcionando como um cronograma para o acompanhamento das melhorias.

Como resultado desta fase, através da ferramenta 5W1H é apresentado o plano de todas as ações e o controle de execução de cada uma delas.

4.2.5 Fase Controlar

A manutenção das melhorias implantadas somente será alcançada através do controle. Uma das formas de controlar as ações que são estabelecidas na fase Implementar é através da adoção de indicadores. Para isto, na fase Controlar devem ser utilizados indicadores de desempenho para avaliar se as metas foram atingidas ou não. A partir destes indicadores são realizados os primeiros ajustes e correções.

Nesta fase Controlar será possível confrontar, o nível de qualidade mensurado na fase Medir, avaliando se houve ou não mudanças com relação a qualidade do estado inicial antes das melhorias. Uma nova avaliação deverá ser realizada através do FMEA, para avaliar se as ações implantadas reduziram o risco inicial mensurado na fase Medir, sendo esta uma das tarefas da fase Controlar, gerar a avaliação das duas medidas e instruir a fase Definir para definição de novas ações.

Observa-se que a fase Controlar pode ser considerada como uma etapa chave da gestão, pois é ela quem determina a continuidade das melhorias. Uma tarefa essencial nesta fase é a divulgação dos resultados, que pode se dar através da estratégia de marketing interno,

também sugerido na primeira fase. O propósito desta estratégia é a de promover a gestão através dos seus resultados, motivando os funcionários a contribuírem para com as mudanças e a sustentação das melhorias.

4.3 Condução das Fases do Projeto - Cronograma

Um dos objetivos deste trabalho é avaliar a implementação da abordagem Seis Sigma. Deste modo, um dos fatores chaves para essa avaliação é o tempo de duração de toda a implantação da abordagem. Para que seja feito uma avaliação mais correta e apurada foi realizado um cronograma (vide tabela 7) baseado no planejamento das fases descritas anteriormente. O que se pretende com isto é chegar a fase Controlar e verificar se o tempo de previsão de cada fase foi cumprido. O cronograma também auxilia a equipe de implantação a manter o foco no trabalho com o propósito de cumprir as definições de tempo para cada fase.

No capitulo 3 foi discutido, que a definição de um cronograma deveria ser realizado na fase Definir. No entanto, acredita-se que, esta previsão deva ser feita conjuntamente com o planejamento das fases, como sendo um dos procedimentos prévios antes do início da implantação.

Tabela 7 - Cronograma de previsão para o projeto Seis Sigma

Etapas	**2008**									
	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ
DEFINIR										
MEDIR										
ANALISAR										
IMPLEMENTAR										
CONTROLAR										

4.4 Conclusões Parciais

Apesar de muitas pesquisas abordarem o Seis Sigma e o recomendarem como uma solução para a gestão de segurança da informação, observa-se que nenhuma delas define como a abordagem poderá ser utilizada ou de que forma as ferramentas da qualidade usadas

pelo Seis Sigma podem ser aplicadas no contexto de segurança da informação. Deste modo, preenchendo esta lacuna, a proposta de implantação apresentada neste capítulo traz como contribuição o alinhamento de todas as fases do método DMAIC, bem como os objetivos que se espera alcançar com cada uma delas, com as ferramentas da qualidade e procedimentos que poderão ser utilizados no decorrer de toda a implantação da gestão de segurança da informação através da abordagem Seis Sigma.

O uso do Seis Sigma possibilitou que a proposição das fases tenham o foco no cliente interno ou usuário. Portanto, as ferramentas e técnicas definidas potencializam a sustentabilidade da segurança da informação na organização. A produção de uma gestão baseada em dados e centrada nas características críticas do usuário é um dos princípios base da abordagem Seis Sigma que deverá tratar como mais veracidade a realidade e os anseios da organização.

CAPITULO 5

IMPLANTAÇÃO DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA ABORDAGEM SEIS SIGMA

Neste capítulo apresenta-se a descrição da implantação da gestão da segurança da informação, proposta no capítulo anterior, através da abordagem Seis Sigma e o método DMAIC em todas as suas fases, juntamente com as aplicações de técnicas e os resultados obtidos. O cenário para aplicação da proposta é a Unidade de Cardiologia Intensiva (UCI) o Unidade de Terapia Intensiva (UTI) do Hospital Universitário de Santa Maria - HUSM.

O capítulo descreve o contexto da organização alvo deste trabalho (seção 5.1) e relata os procedimentos realizados nas fases Definir (seção 5.2), Medir (seção 5.3), Analisar (seção 5.4), Implementar (seção 5.5) e Controlar (seção 5.6) do ciclo de melhoria DMAIC. A seção 5.7 realiza uma apuração do cronograma e a seção 5.8 apresenta as conclusões parciais.

5.1 Caracterização da Organização

A Organização alvo desta dissertação é o Hospital Universitário de Santa Maria (HUSM), a qual abrange uma totalidade de mais de 100 municípios, estabelecendo-se como campo de ensino prático aos alunos de graduação e pós-graduação da Universidade Federal de Santa Maria (UFSM) em especial aos da área da saúde.

Um fator que ressalta a importância do HUSM é o de ser o único hospital da região central do estado do Rio Grande do Sul, que atende pelo Sistema Único de Saúde (SUS), fornecendo a todos seus usuários uma diversidade de serviços especializados em 28 áreas.

O HUSM é formado por uma equipe ampla de aproximadamente 147 docentes das áreas de enfermagem, farmácia, fisioterapia, medicina e odonto-estomatologia; 1276 funcionários em nível de apoio médio e superior; 312 funcionários de serviços terceirizados, além de 876 alunos de graduação da UFSM, estagiários, residentes, mestrandos e doutorandos. Os atendimentos realizados pela a instituição, segundo as médias mensais de 2006 são em torno de:

- 914 internações;
- 549 cirurgias;
- 166 partos;

- 10.332 consultas ambulatoriais;
- 4.285 consultas no Pronto Atendimento;
- 1.144 seções de Fisioterapia;
- 63.808 exames;

Porém, até o ano de 2007, não havia um Sistema de Gestão de Segurança da Informação implantado no HUSM. Entretanto, em função das novas diretrizes (Política Nacional de Informação e Informática em saúde, 2004) expedidas pelo Ministério da Saúde e Secretaria Executiva do Departamento de Informação e Informática do SUS, as quais promulgam a Política Nacional de Informação e Informática em saúde (PNIIS), a direção do hospital demonstrou interesse em realizar a gestão da segurança da informação.

A PNIIS é composta de 19 diretrizes e aborda aspectos de tratamento das informações e pesquisa em informática na saúde. A decisão positiva da Direção do HUSM foi o primeiro passo para dar início ao processo de implantação da gestão da segurança da informação.

Como o HUSM abrange muitos setores aos quais se subdividem em 28 serviços, foram selecionadas duas unidades juntamente com a Direção que se caracterizam por serem vitais para instituição, a Unidade de Cardiologia Intensiva (UCI) e Unidade de Terapia Intensiva (UTI).

A UCI é uma unidade composta por 4 leitos, sendo responsável por todas as internações e cirurgias cardiovasculares disponibilizadas pelo HUSM. Por ser fisicamente pequena, existe uma grande rotatividade de pacientes, havendo inclusive lista de espera para internação. A equipe de funcionários que compõem a unidade contempla cerca de 20 profissionais, divididos entre médicos, enfermeiros, técnicos e auxiliares de enfermagem, nutricionistas, fisioterapeutas, administrativo e estagiário, tendo a função de cumprir às 24 horas de seu funcionamento.

A UTI é uma unidade composta por 9 leitos, sendo responsável por oferecer suporte avançado de vida a pacientes que estão intensivamente doentes e conta com cerca de 40 profissionais nas mais diversas áreas.

Apesar de serem unidades com funções específicas e diferentes em seus objetivos, fisicamente elas estão juntas, sendo que os recursos materiais e humanos são compartilhados por ambas. Desta maneira a implantação da gestão de segurança irá contemplar as duas unidades como um todo, mas respeitando suas individualidades e características.

5.2 Fase Definir

Nesta fase Definir do DMAIC inicia-se a concepção do problema e as primeiras percepções organizacionais das duas unidades. O propósito é capturar as necessidades dos usuários, associá-los aos problemas e transformá-las em metas da gestão. É nesta fase que são definidos o escopo e a equipe de implantação.

Neste trabalho o tema central é a segurança da informação, deste modo a definição dos problemas e as metas a serem atingidas visam este tema central. A seguir são apresentados os detalhes da implantação, conforme o planejamento das ações (vide seção 4.2).

5.3.1 Equipe de Trabalho

Uma das primeiras ações realizadas nesta fase Definir foi compor a equipe de trabalho, sendo esta prática uma das exigências da abordagem Seis Sigma. Deste modo, a composição da equipe foi realizada juntamente com a direção do HUSM, respeitando a configuração recomendada pela abordagem Seis Sigma, descrita no capítulo 3. A função de *Máster Black Belt* não foi nomeada nesta composição, visto que não existe um membro da equipe que tenha experiência na implantação do Seis Sigma e também por se tratar de unidades pequenas, portanto não havendo a necessidade desta função. Desta forma, a composição da equipe pode ser vista na tabela 8.

O Executivo líder e os campeões são o elo importante na implantação da gestão e peça principal para auxiliar na aproximação dos *Black Belts* e *Green Belts* com as duas unidades, uma vez que as pessoas que compõem essas funções não fazem parte do HUSM. Um outro fator considerado importante para a GSI, no que se refere as funções de Executivo líder e Campeões são a presença de pessoas da alta direção e chefia. Esta condição torna a implantação melhor vista e principalmente mais valorizada. É importante salientar que o conceito de equipe Seis Sigma é diferente do conceito de Comitê de Segurança discutido no capítulo 2. A equipe Seis Sigma é um grupo formado com a responsabilidade de implantar o Seis Sigma, o comitê é um grupo independente com responsabilidades específicas visando a sustentação da segurança.

Tabela 8 – Composição da Equipe Seis Sigma

Equipe de Implantação da Gestão da Segurança da Informação		
Função	Responsável	Responsabilidade
Executivo líder	Diretor Clínico do HUSM	Responsável por Incentivar e supervisionar a implantação da gestão da segurança da informação na UCI e UTI
Campeão	Chefe da Unidade de Cardiologia (UCI). Chefe da Unidade de Terapia Intensiva (UTI) Chefe da Informática	Prover aproximação da equipe de Implantadores com as respectivas unidades, incentivando e promovendo as mudanças nas unidades.
Black Belt	Implantador Responsável (Autora da Dissertação)	Responsável pelo planejamento das fases, definições das ferramentas da qualidade e pela implantação da gestão da segurança da informação na UCI e UTI
Green Belt	Implantadores Auxiliares (composta por três pessoas)	Responsável pela gestão da segurança da informação na UCI e UTI e auxiliar o Black Belt

5.3.2 Definição do Escopo

Após a formação da equipe, a primeira tarefa do grupo foi legitimar o escopo da GSI, ficando estabelecido e aprovado o STOPE, ou seja, a equipe irá trabalhar tendo como cobertura as esferas estratégica, tecnológica, organizacionais, pessoas e ambientais. A equipe poderia ter escolhido somente a esfera tecnológica, no entanto a GSI iria perder muito com este estreitamento. Desta maneira, todos da equipe concordaram e ratificaram essa decisão.

Outra decisão do grupo que necessitou ser feita, foi a escolha de um problema central, sendo importante tanto para equipe Seis Sigma como para os funcionários. Esta estratégia facilita o entendimento e a visão das pessoas no direcionamento ao longo do trabalho de implantação da gestão, do que simplesmente se usasse apenas o tema central Segurança da Informação. Por esta razão foi definido como problema central “Vulnerabilidades em Segurança da Informação.” Esta definição é usada principalmente nos primeiros levantamentos da fase Definir como o *brainstorming* e Diagrama de Causa e Efeito, onde a interação presencial com os funcionários é maior.

5.3.2.1 Divulgação da Gestão da Segurança da Informação

Promover o marketing interno da gestão da segurança da informação é uma tarefa necessária, uma vez que toda a gestão gera uma mudança, sendo as pessoas a principal peça nesta transformação. Desta forma, para que a UCI e a UTI entendesse a proposta da gestão de segurança da informação e principalmente não a encarasse com surpresa, o que poderia dificultar o início dos trabalhos e afetar a participação de todos na interação com as ferramentas e técnicas, a equipe desenvolveu como estratégia a distribuição de pôsters. Os pôsters, patrocinados pela direção financeira do hospital, foram fixados em pontos estratégicos, como sala de convivência, recepção das unidades e registro de ponto. O conteúdo dos pôsters aborda pontos chaves sobre o trabalho como: “o que ele vem a ser?“ e “quais os benefícios?”. Este marketing interno foi de extrema importância para o trabalho, o que contribuiu positivamente para uma maior disseminação e sensibilização da gestão, até mesmo causando interesse de outros setores. O Pôster pode ser visualizado no Apêndice A.

5.3.3 Percepção Inicial

Realizada a divulgação da GSI e composta a equipe Seis Sigma, o próximo passo foi obter a percepção inicial das unidades UCI e UTI. O propósito de realizar este entendimento foi obter um diagnóstico inicial do quão importante é o tema segurança da informação para as unidades e o quanto as pessoas estão dispostas a contribuírem para que a GSI realmente aconteça.

Para obter essa informação foi realizado um questionário (vide Apêndice B), onde a primeira pergunta foi: “Na sua opinião, qual a importância dos controles e medidas de Segurança da Informação?”.

A figura 16 demonstra que dos 38 respondentes 65,8% considera que os controles de segurança da informação são fundamentais, o que denota a preocupação que existe pelo tema. No entanto, se o resultado fosse superior para as opções “Desnecessárias e “Não sabem’, o trabalho começaria com uma conscientização a fim de atrair a adesão das pessoas para a necessidade do projeto.

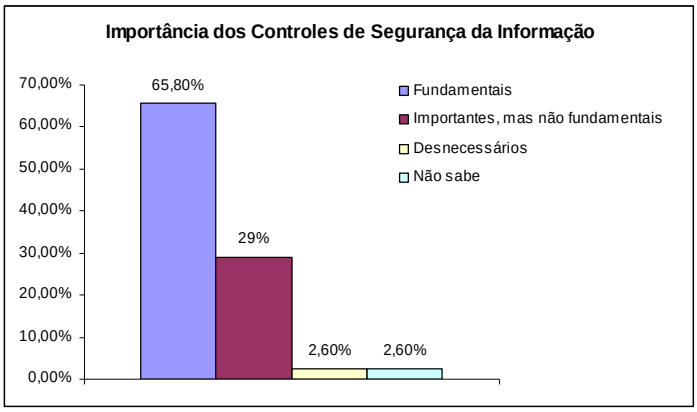


Figura 16 - Índice de importância dos Controles de Segurança

Ainda no mesmo questionário a segunda pergunta realizada aborda 6 itens referentes ao comprometimento das pessoas com as mudanças. Quando existe um cenário onde as pessoas estão imbuídas e comprometidas com qualquer trabalho, a tendência de se obter resultados positivos são maiores do que um cenário adverso. Deste modo, é muito importante realizar esta percepção, uma vez que a proposta de gestão de segurança da informação que está sendo implantada é baseada em dados oriundos dos funcionários ou usuários. Portanto, se estas pessoas não estiverem envolvidas com o trabalho e principalmente com as mudanças que serão geradas toda a gestão fica comprometida.

Os itens relacionados a segunda pergunta (vide tabela 9) foram referentes a aspectos de comunicação de informações, adaptação, comprometimento, motivação e colaboração com as mudanças. Foi utilizada uma escala *Likert* que varia de 1 a 5 para as respostas, onde 1-Muito Baixo; 2-Baixo; 3-Regular; 4-Alto e 5-Muito Alto.

Tabela 9 -Pesquisa de Motivação com comprometimento com as mudanças

Comprometimento com as mudanças.	Muito Baixo	Baixo	Regular	Alto	Muito Alto
1. Recebimento de informações sobre as mudanças que estão acontecendo na unidade.	0,00%	3,10%	28,10%	40,60%	28,20%
2. Condução das atividades pelo superior imediato da área na qual trabalha de acordo com as mudanças e as decisões corporativas tomadas pela unidade.	3,10%	21,90%	37,50%	18,80%	18,70%
3. Considerar positivas as mudanças que estão acontecendo na unidade.	0,00%	0,00%	25%	53,10%	21,90%
4. Acreditar que seu trabalho contribui para que essas mudanças tenham resultado positivo para a unidade em que trabalho.	3,10%	3,10%	37,50%	37,50%	18,80%
5. Acreditar que a unidade valoriza a segurança das suas informações (sigilo das informações estratégicas e confidenciais).	9,40%	12,50%	28,10%	40,60%	9,40%
6. Colaboração para que as mudanças adotadas na unidade tenham resultado satisfatório.	0,00%	3,10%	28,10%	40,60%	28,20%
Média	**3,12%**	**8,12%**	**31,24%**	**38,12%**	**19,40%**

O resultado obtido com as médias dos 6 itens, fornecida pelos 38 respondentes, somadas as opções “Alta” e “Muita Alta” mostram um índice de 57,52%, revelando serem pessoas comprometidas para que as mudanças aconteçam, podendo ser melhor observado na figura 17. Analisando especificamente o item 6 (“Colaboração para que as mudanças adotadas na unidade tenham resultado satisfatório.”), o resultado gerado com a soma das médias das opções “Alta” e “Muita Alta” mostram um índice de 68,80%. Conforme mostra a tabela 11, isto demonstra que as pessoas além de colaborar, também são participativas para que as mudanças tenham um resultado positivo.

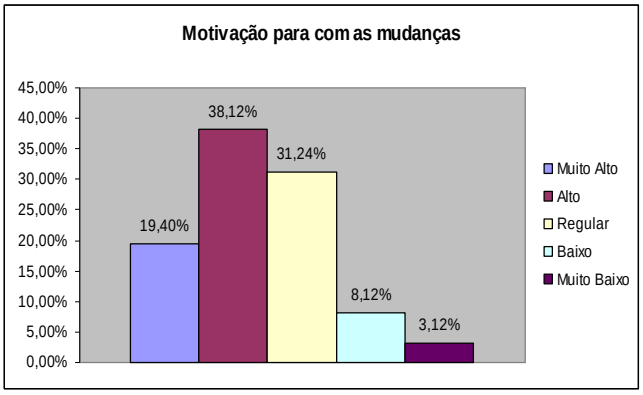


Figura 17 – Comprometimento com as mudanças.

5.3.4 Fluxograma

Após as primeiras percepções iniciais obtidas com relação às pessoas, o próximo passo foi entender as unidades. A utilização do Fluxograma nesta etapa tem como objetivo principal, mapear o contexto organizacional das duas unidades UCI e UTI, procurando conhecer o funcionamento das unidades. A equipe optou em realizar o mapeamento do fluxo de pacientes, considerando que tanto a UCI e a UTI tem como principais atividades a prestação de serviços a pacientes. A elaboração dos fluxogramas foi realizado pelos Campeões que são chefes das respectivas unidades juntamente com os seus funcionários e durou dois dias, uma vez que foi difícil reunir todos em um mesmo momento. O trabalho foi composto por dois representantes da UCI (chefe e membro da equipe (Campeão) e mais um funcionário) e dois representantes da UTI (chefe e membro da equipe (Campeão) e mais um funcionário) e o *BlackBelt*.

O fluxograma da UCI (vide figura 18) caracteriza todas as atividades no que tange o fluxo de pacientes da unidade. Seu ponto de entrada se dá através da verificação de leitos disponíveis, por se tratar de uma unidade pequena, mas com muita demanda de pacientes é necessária que haja uma checagem. Caso não tenha leito esse paciente é inserido em uma lista de espera feita manualmente. Depois de dar entrada a UCI, é verificado se o paciente já possui um registro no Serviço de Arquivo Médico e Estatística (SAME), sendo um número único que é gerado para cada paciente sempre que este der entrada em qualquer unidade clínica do hospital, todo esse processo é feito eletronicamente. Se o paciente não tem um SAME, ele é gerado, e a partir desse registro é criado um prontuário onde irá conter todo e qualquer documento (informações pessoais, notas de internação, exames, evolução médica e de enfermagem e prescrições), sendo esta uma pasta física. Caso o paciente já tenha um SAME, ele dará entrada na unidade a partir da sua internação e abertura do seu prontuário. Após a entrada na unidade, o paciente será submetido a uma verificação para saber o tipo de tratamento ou serviço que será disponibilizado de acordo o seu estado clínico. O paciente dá a saída da unidade de três formas: alta, transferência e óbito. Todas elas passam pelo procedimento de encerramento do prontuário, onde todos os documentos precisam estar organizados seguindo uma ordem cronológica. O Fluxograma da UTI (vide figura 19) segue os mesmos procedimentos iniciais caracterizados na UCI, diferindo logicamente nos serviços disponibilizados e nos leitos que são 9. A saída do paciente da unidade ocorre por transferência (que pode ser para outras unidades internas ou externas ao hospital) ou por óbito.

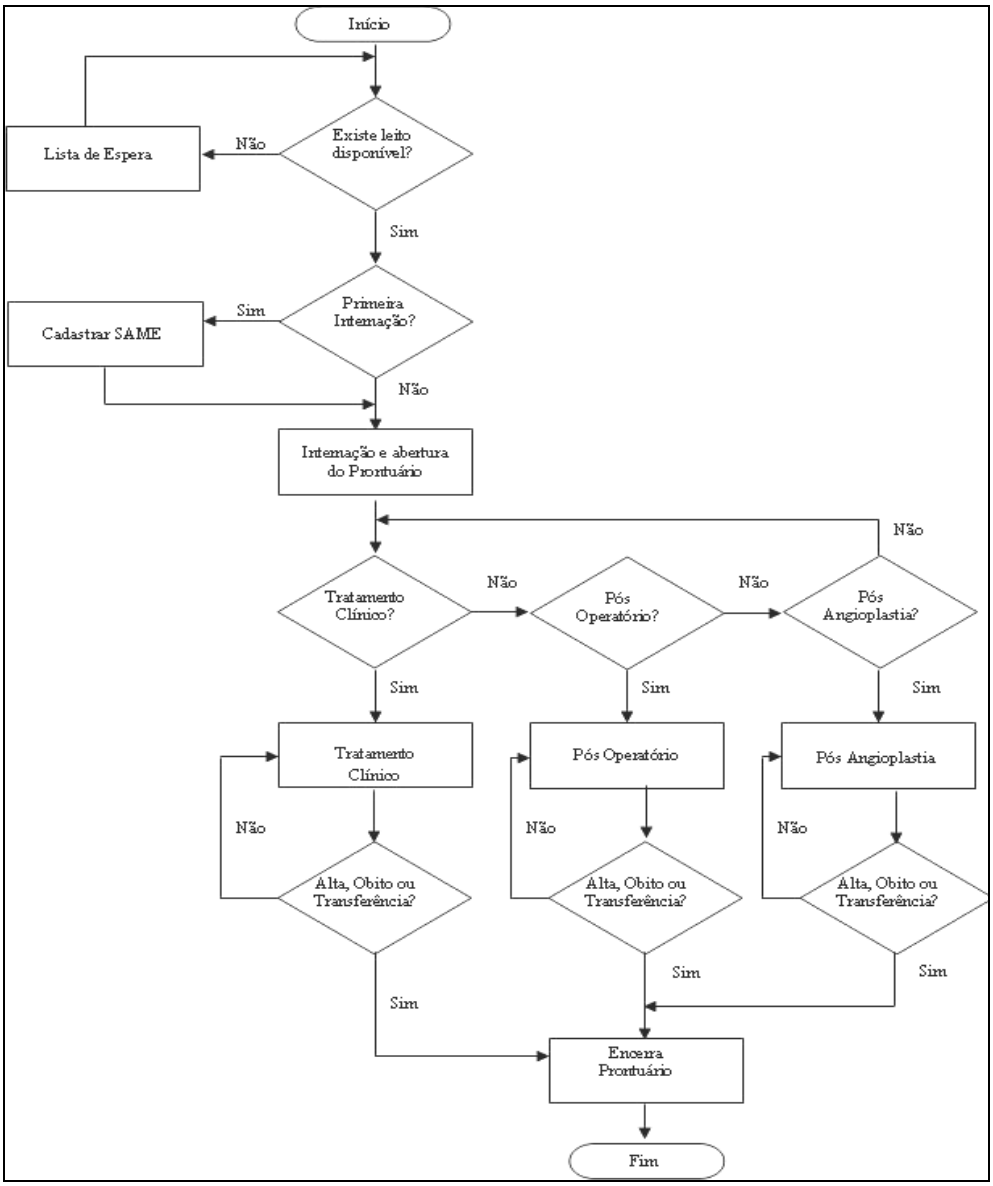


Figura 18 - Fluxograma Unidade de Cardiologia Intensiva - UCI (HUSM)

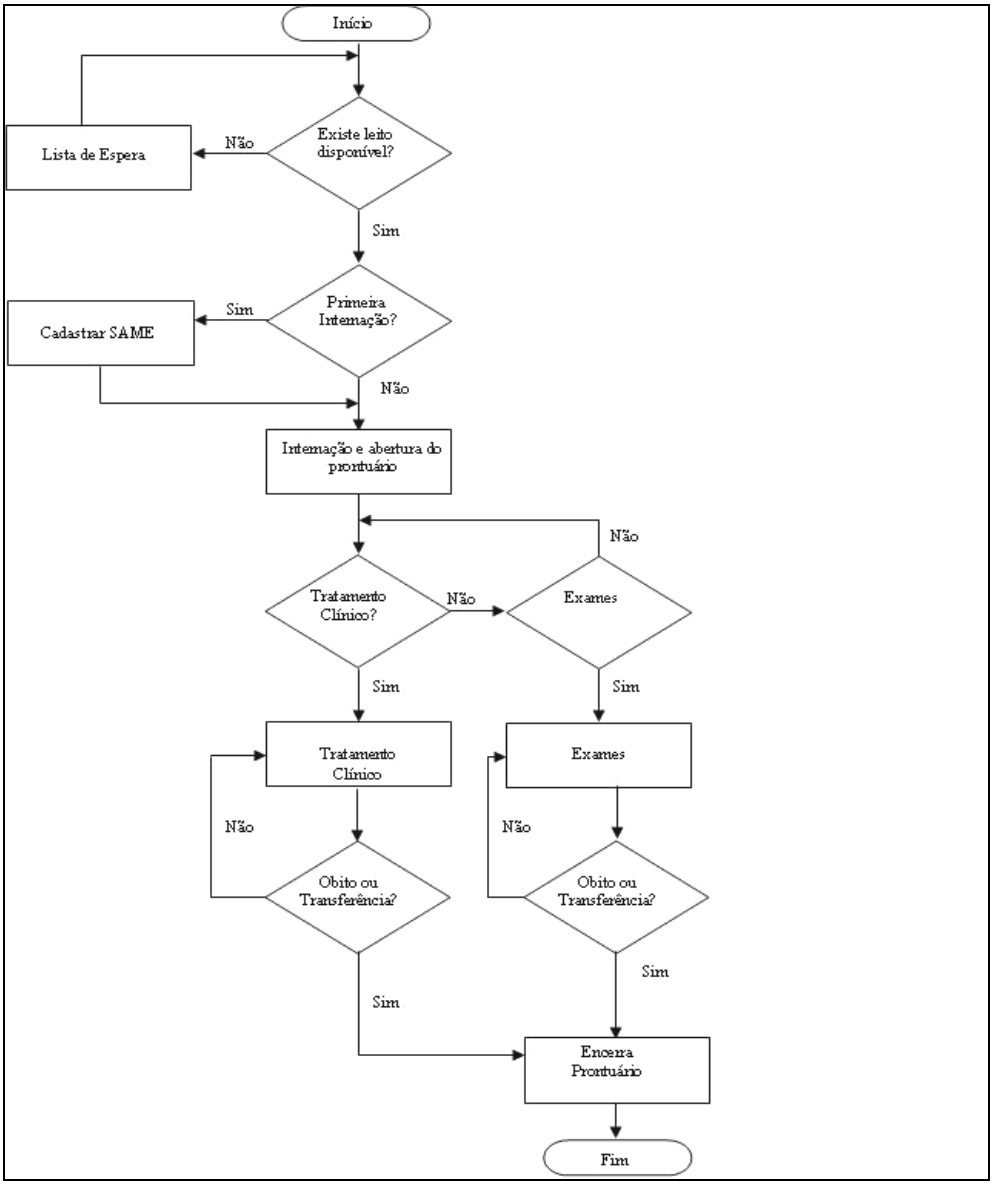


Figura 19 - Fluxograma Unidade de Terapia Intensiva - UTI (HUSM)

Ao concluir o fluxograma pode se destacar que as informações que circulam dentro das unidades são em grande parte compostas de dados de pacientes e por esta razão precisam estar seguras e protegidas. Outro ponto que merece destaque é o uso moderado do computador, uma vez que as prescrições médicas ainda são feitas manualmente. Três pontos críticos no que tange aspectos de informação pode ser observado pela equipe de elaboração do fluxograma:

1. O primeiro deles está no acesso ao SAME do paciente, que através desse número se tem acesso a todas as informações pessoais e clínicas do paciente, porém o controle de login e senha para que se tenha acesso ao SAME não é realizado pelo HUSM, sendo que é comum ocorrer o compartilhamento de logins e senhas entre os usuários, como também não é efetuada a atualização desses usuários que tem acesso as estas informações.
2. O segundo ponto crítico está na abertura do prontuário em razão de que muitos dos documentos dos pacientes são extraviados e trocados.
3. O terceiro ponto crítico esta na manutenção do prontuário dentro da unidade no período em que o paciente estiver internado, sendo que enumeras pessoas entres alunos, médicos, enfermeiros e secretários manuseiam o documento, o que acarreta o desaparecimento dos prontuários, gerando uma série de transtornos para as unidades, prejudicando principalmente a assistência ao paciente.

Diante dessas constatações resultantes do conhecimento sobre funcionamento das unidades, através do seu fluxo principal, o próximo passo foi fazer uma investigação mais detalhada a respeito deste fluxo. Identificar quais os problemas que fazem parte desta rotina retratada, procurando capturar os riscos e as vulnerabilidades existentes. Esta investigação foi feita utilizando com a técnica de *brainstorming* descrita na próxima seção.

5.3.5 Brainstorming

O objetivo do uso desta técnica no trabalho é obter através de reuniões com a equipe Seis Sigma e funcionários, a definição dos problemas que eles acreditam estarem presentes na rotina da UCI e UTI.

A técnica foi realizada em dias e horários intercalados com não mais que três pessoas de cada unidade. Isso por que as reuniões tinham que ser em grupos pequenos, uma vez que a UCI e UTI não poderiam ficar por muito tempo sem estes profissionais. Foram quatro sessões de aproximadamente 20 minutos cada, ao longo de 2 semanas, o que permitiu ter no total 12 funcionários participantes nesta técnica, estando presente em todas elas o *BlackBelt* e um *GreenBelt* como pode ser visto na figura 20 que retrata esta prática.

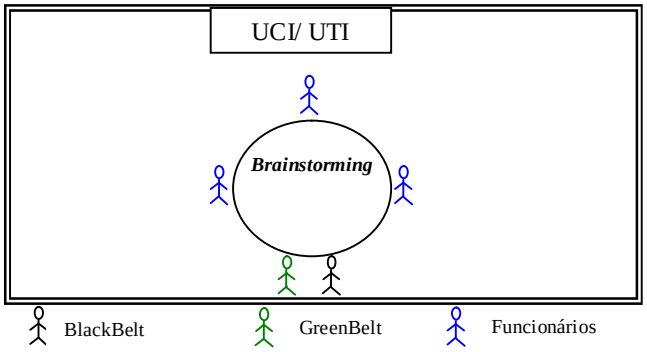


Figura 20 - Sessões de *Brainstorming*

Para que todos os participantes pudessem se interar do propósito e ficar dentro do "clima" necessário para a condução do trabalho, foi exposto claramente a proposição a ser tratada, procurando direcionar a visão de todos para o problema central definido pela equipe Seis Sigma, "Vulnerabilidades em Segurança da Informação". Usar um tema central ou problema central é fundamental na técnica de *brainstorming,* pois evita o desvio de foco nas reuniões, o que pode levar a interpretações errôneas e ineficazes.

Foi utilizado como apoio nesta técnica, a norma de segurança NBR ISO/IEC 27001:2006, o que possibilitou fornecer um panorama geral que facilitasse a relação dos controles existentes no documento com as vulnerabilidades em segurança da informação, que os participantes da técnica acreditam fazer parte das unidades, dentro das esferas estratégica, tecnológica, humana, organizacional e ambiental, e principalmente deixá-los cientes da existência da norma de segurança de informação, o que para grande maioria foi algo inovador.

As discussões começaram em torno dos problemas existentes nas unidades, os riscos que os participantes observavam, o que precisa ser feito e as ações e procedimentos diários que eram executados para que as informações estivessem em uma condição vulnerável.

Os resultados da aplicação desta técnica podem ser vistos na tabela 10, a qual enumera todos os problemas reportados durante as seções de discussões e a justificativa para estes problemas existirem.

Tabela 10 – Resultado do *Brainstorming*

Problemas	Justificativa
1. Falta treinamento em Segurança da Informação	Não existe um esclarecimento sobre a abrangência do tema, muitos acreditam que a segurança da informação seja apenas uma questão tecnológica.
2. Falta de Preocupação com a segurança das	Muitos acreditam que a segurança precisa estar presente na rotina e procedimentos diários das unidades.

Problemas	Justificativa
informações	
3. Falta de comprometimento das pessoas com a informação	Há um certo descaso quanto a manipulação da informação, ocasionada pelo descomprometimento de muitas pessoas para com os efeitos deste ato.
4. Falta de planejamento e comprometimento da direção com projetos voltados a SI	A direção não viabiliza meios ou recursos para que ações deste interesse seja aplicado nas unidades .
5. Compartilhamento de senhas	Existe um descontrole no uso de usuários e senhas sendo, muito comum a prática de ceder o acesso a outros profissionais, onde muita das vezes não pertencem a esta unidade.
6. Ausência de política de controle de acesso	Falta de uma política que controle o acesso de usuários.
7. Dificuldades de utilização dos Sistemas de Informação das unidades	Não existe um manual de ajuda para o sistema da UCI, o que acaba prejudicando a produtividade, pois muitas vezes se demora a entender alguma determinada ação ou são cometidos erros por conta dessa lacuna.
8. Falta de atualização de usuário na rede	Usuários que não pertencessem mais ao quadro de funcionários da organização, ainda continua com direto ao acesso aos sistemas.
9. Sem procedimentos para descarte de mídias	As mídias que contém informações das unidades são descartadas de forma errônea, possibilitando a recuperação facilmente destes dados.
10. Falta de políticas de Backups	Não existe um procedimento formal ou documentado sobre as rotinas de backups das unidades.
11. Inexistência de e-mail institucional	As informações que são envidadas das unidades são realizadas através do uso de e-mail pessoal dos funcionários.
12. Não são adotadas metodologias de gestão	Não se adota nenhuma metodologia ou modelo que preveja o controle e a padronização dos processos.
13. Inexistência de uma política de segurança da informação	As unidades não possuem nenhuma política de segurança que regulamente através de diretrizes e normas o uso da informação.
14. Número insuficiente de extintores de incêndio	Nos locais em que há estações de trabalho, o número de extintores são insuficientes para atender a demanda.
15. Inexistência de acordo de	Não existe nenhum termo, onde os funcionários assinem para atestar a o seu compromisso com a confidencialidade dos

Problemas	Justificativa
confidencialidade	dados que são manipulados nas unidades.
16. Ausência de conformidades com requisitos legais	A direção e conseqüentemente as unidades não seguem nenhuma norma nacional de segurança da informação.
17. Ausência de armários ou compartimento de armazenagem dos documentos confidenciais das unidades	Muitas vezes documentos confidencias, principalmente, de pacientes com dados de pacientes ficam dispostos na recepção, permitindo que qualquer pessoa possa acessá-lo.
18. Acesso facilitado nos setores	Pessoas muitas vezes sem o crachá de identificação tem acesso as unidades. No período da noite esse problema é maior, pois não tem recepcionista que bloqueie a entrada de pessoas não identificadas.
19. Inexistência de inventário de ativos e classificação da informação	Não existe um inventário com todos os ativos da informação, sendo que não há uma classificação do que é informação pública, privada e confidencial.
20. Ausência de Comitê ou grupo responsável pela segurança.	Não existe um grupo ou equipe responsável pela promoção da segurança da informação nas unidades.

Os 20 (vinte) problemas relacionados na tabela 10 são frutos das opiniões expressas pelos participantes desta técnica que revelaram estarem cientes com as vulnerabilidades presentes nas unidades.

A interação obtida com a técnica de *brainstorming* foi muito importante, apesar de terem sido poucas pessoas, apenas 12 no total, a interação foi bem recebida, uma vez que todos os participantes puderam falar e contribuir para a identificação dos problemas presentes nas unidades, como também ajudou a proporcionar um entendimento melhor sobre o tema, o que para muitos se fazia necessário, visto que muito dos problemas que foram percebidos não eram vistos como um problema, por serem corriqueiros, reforçados pela falta de conhecimento com o tema, fazendo parte da rotina das unidades como, por exemplo, o problema 17 (ausência de armários ou compartimento dos documentos confidenciais das unidades), que vêm a se relacionar com o terceiro ponto crítico relatado após o mapeamento com o fluxograma na seção 5.2.5. O problema 5 (compartilhamento de senhas) também se relaciona a seção 5.2.5, ocorrendo frequentemente nas unidades, sendo tratado por muitas

pessoas como algo normal. Esta lista parcial de problemas obtidos com a técnica serviu de base para a próxima seção descrita seguir.

5.3.6 Entrevistas

Após realizar as sessões de *brainstorming* com os funcionários, o *BlackBelt* e os *GreenBelt* tomaram a decisão de obter mais detalhes acerca dos problemas relacionados pelos funcionários das duas unidades durante o *brainstorming*. Para isto, foi realizada a técnica de entrevistas não-estruturada, a qual não utiliza um roteiro definido, apenas introduz um tema ou assunto a partir de uma motivação inicial, permitindo ao entrevistado uma maior liberdade de discursar sobre o tema proposto, contribuindo para uma investigação real do cenário vivido pelas unidades os quais podem ser determinantes para percepção do problema.

A equipe definiu que as entrevistas seriam apenas com as chefias das duas unidades e com corpo diretor do hospital motivo pelo qual se deseja confrontar se os mesmos problemas enumerados pelos funcionários que participaram do brainstorming na seção 5.2.6, também são problemas compartilhados na visão dos demais diretores.

Participaram das entrevistas, o Diretor Clínico (Executivo líder), Chefe da Informática (Campeão), Chefe UCI (Campeão) e Chefe UTI (Campeão), sendo todos estes membros da equipe Seis Sigma e por indicação do Executivo Líder a Coordenadora do Complexo Cardiológico e Acessor Jurídico, totalizando 6 pessoas.

Com exceção das entrevistas do Diretor Clínico, Acessor Jurídico e a Chefe de Informática que foram realizadas juntas com os três presentes, as demais foram realizadas separadamente, por incompatibilidade de horários, visto que algumas entrevistas tiveram que ser re-agendadas por este motivo.

As entrevistas foram executadas ao longo de 2 semanas e teve como motivação e os problemas relacionados no *brainstorming*. A entrevista seguiu um contexto muito semelhante ao de uma conversa informal, especificando apenas os problemas relatados. O resultado desta entrevista revelou algumas necessidades que foram observados de forma mais enfática pela maioria dos participantes:

1. Necessidade de conformidade com normas vigentes em segurança da informação - a adequação das unidades com normas de segurança foi colocada como algo importante e necessário para evolução gradativa das ações que forem implantadas, auxiliando principalmente na imagem das unidades como também na credibilidade do hospital.

2. Necessidade de avaliação dos riscos – avaliação dos riscos também foi outro item citado por todos entrevistados, a quantificação e o gerenciamento dos riscos são vistos muitas vezes como algo teórico, trabalhoso e secundário, deste modo uma mudança nas rotinas é necessário para que de fato essa medida seja instituída e cumprida.
3. Necessidade de classificação da informação quanto a sua relevância – a classificação é uma medida que é importante, pois muitas vezes incidentes de segurança acontecem por desconhecimento e principalmente por falta de regras que definam o acesso e o grau de proteção da informação.
4. Necessidade da política de segurança da informação - colocada pelos entrevistados como sendo o documento base para o estabelecimento da segurança da informação, mas sendo necessário um profundo esclarecimento para que se torne efetivo.
5. Necessidade de controle no acesso de usuários – essa questão é colocada por todos como "descontrole de usuários", pois não há um controle efetivo e organizado, onde muitas vezes alunos acabam tendo acesso a informações que somente médicos deveriam. A não atualização dos usuários é outro problema que gera este descontrole, sendo que funcionários afastados e demitidos continuam com acesso ao sistema e seus logins e senhas utilizados por outras pessoas. O uso de senhas fracas também é um problema recorrente, o que acaba facilitando o acesso ao sistema através de outros usuários.
6. Necessidade de treinamento e conscientização em segurança da informação – o treinamento e conscientização foi posto como algo absoluto e que seja parte do calendário de atividades do hospital como um procedimento mensal, para todo funcionário contratado na instituição.
7. Necessidade de um Comitê responsável pela segurança da informação – no hospital existem muitos comitês para diferentes fins, por exemplo, Comitê para prontuários, Comitê para prescrição médica, havendo também a necessidade de um Comitê de segurança da informação que atue ativamente no HUSM, principalmente por se tratar de uma instituição de saúde que precisa preservar e manter sigilo das informações de pacientes.

A maioria destas necessidades relacionadas reafirma os problemas resultantes da técnica de *brainstorming* (seção 5.2.6) enumerados na tabela 10, o que reforça que estes problemas são percebidos tanto pelos funcionários quanto pelo corpo diretor. As relação entre as duas técnicas observadas são:

- Necessidade 1 com o problema 15 - reforça a necessidade de normas vigentes em segurança da informação.
- Necessidade 3 com o problema 19 - reforça a necessidade de existência de classificação da informação.
- Necessidade 4 com o problema 13 - reforça a necessidade de existência de um documento que estabeleça políticas para o uso da informação.
- Necessidade 5 com o problema 5 - reforça a necessidade de existir um controle maior de usuários.
- Necessidade 6 com o problema 1 - reforça a necessidade de promover a segurança da informação através de programas de conscientização para os usuários.
- Necessidade 7 com o problema 20 - reforça a necessidade de um comitê que seja responsável pela atuação em prol da segurança da informação.

A aplicação da entrevista trouxe a tona também outras questões de ordem gerencial ao qual fora citado por todos os entrevistados, estas questões são:

- A falta de uma equipe atuante para promover iniciativas como a deste trabalho, dentro do hospital;
- A cultura reativa da instituição de só buscar a solução quando algum efeito drástico tenha ocorrido; e
- A falta de clareza sobre o quanto determinada informação agrega de valor para o hospital, valores estes que expressam o grau de importância do ativo da informação.

Esta última questão contrasta o número crescente de processos que o hospital enfrenta, onde boa parte é originado em decorrência do vazamento e descontrole na acessibilidade da informação e extravio de documentações. Estas questões citadas fazem parte do contexto geral, ou seja, do hospital como um todo, que obviamente reflete de forma significativa nas unidades foco deste trabalho.

A aplicação destas entrevistas propiciou um conhecimento a cerca dos problemas das unidades, como também a relação existente entre os problemas percebidos pelos funcionários e as necessidades percebidas pelo corpo Diretor.

O resultado obtido com o *brainstorming* que originou a lista parcial de problemas (seção 5.2.6, tabela 10), onde alguns reafirmados com a entrevista serviram de base para a próxima seção descrita seguir.

5.3.7 Diagrama de Causa e efeito

Finalizada as entrevistas a próxima ferramenta a ser utilizada na fase Definir é o Diagrama de Causa e efeito. Esta ferramenta se caracteriza por visualizar e investigar as causas, permitindo um maior aprofundamento dos problemas relatados durante a realização das entrevistas e sessões de *brainstorming*.

O Diagrama de Causa e efeito (vide figura 21) foi baseado na lista parcial de problemas obtidos na tabela 10 (seção 5.2.6) e reforçado pela entrevista (seção 5.2.7). O Diagrama (vide figura 20) foi elaborado pela equipe Seis Sigma, sendo que cada grupo de problemas similares foram classificados na espinha correspondente ao escopo da gestão, que envolvem aspectos estratégicos, tecnológicos, humanos, organizacionais e ambientais (primeiro nível, sinalizado pela flecha). Estes problemas classificados foram retratados pelos funcionários e diretores (segundo nível, sinalizado pela flecha) e aprofundados pela equipe Seis Sigma (terceiro nível, sinalizado pela flecha), os quais detalham as causas para o problema central “Vulnerabilidades em Segurança da Informação”.

No terceiro nível do diagrama é mostrado um aprofundamento das causas secundárias (segundo nível), sendo que este último nível de análise aponta para algumas causas em comum, destacando-se a ausência de política de segurança da informação, ausência de conscientização e ausência de comitê de segurança.

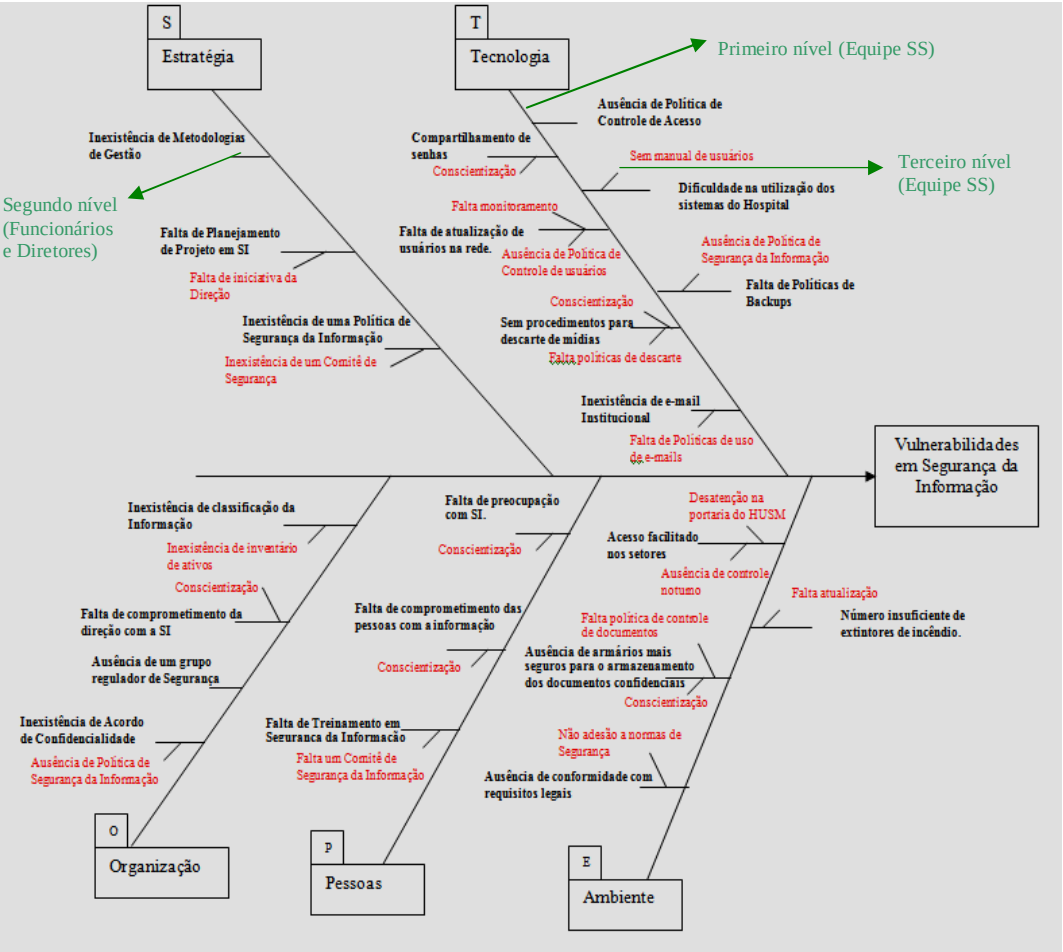


Figura 21- Diagrama de Causa e Efeito

O que observa-se com o diagrama é que grande parte dos problemas relatados desde o início até este momento da fase Definir pelos funcionários, diretores e equipe Seis Sigma e que faz da UCI e UTI vulneráveis em segurança da informação, recaem nas principais causas: a falta de um documento de política de segurança da informação que documente regras na qual controle o uso da informação; a ausência de um programa de conscientização e treinamento que oriente os usuários do uso correto e responsável da informação; e a inexistência de um comitê ou grupo que regulamente, promova e mantenha a segurança da informação no HUSM.

A partir da visualização gráfica das causas das vulnerabilidades em segurança da informação, representada pelo Diagrama de causa e efeito, o próximo passo é mapear esses dados, procurando levantar se de fato todos percebem e enxergam o problema e se a maioria quer que este seja solucionado. Para que isso fosse possível foram utilizadas as lacunas de desempenho, sendo discutida sua implementação detalhadamente na próxima sessão.

5.3.8 Lacunas de desempenho (*Gap*)

O objetivo de extrair os *gaps* após as técnicas de *brainstorming*, entrevistas e Diagrama de Causa e efeito foi realizar um afunilamento a partir dos resultados gerados por elas, agrupando os problemas chaves retratados que possuim uma causa em comum, através de perguntas disponibilizadas num questionário.

Esta estratégia visa ampliar a amostra e capturar a percepção e expectativa dos problemas relatados, a fim de convertê-las em metas. Para a elaboração do questionário foi seguido o modelo *ServQual*, que utiliza determinantes da qualidade na sua concepção.

A gestão da segurança da informação pode ser vista como um serviço, que está sendo implantado na UCI e UTI. No entanto, para que este serviço resulte em qualidade para as unidades ele precisa se enquadrar em alguns determinantes para alcançar o efeito esperado. Deste modo, foram definidos 7 determinantes que estão relacionados diretamente com as questões discutidas até o momento. Os determinantes foram definidos pela equipe Seis Sigma, seguindo a fundamentação de dois autores conforme apresentado no quadro 1.

Quadro 1 - Determinantes da Qualidade

PARASURAMAN et al.(1985)	JOHNSTON (1995, 1997)
Confiabilidade (confiança no serviço de segurança da informação, onde somente pessoas autorizadas tem acesso a informação) **Responsividade** (disposição para resolução de problemas em relação a segurança da informação) **Tangibilidade** (qualidade dos equipamentos, material de comunicação e ambiente) **Comunicação**(treinamento em segurança da informação, programas de conscientização)	**Disponibilidade** (disponibilidade das informações). **Integridade** (qualidade no serviço de segurança onde é preservado a integridade das informações).

Além dos determinantes da qualidade, o questionário ServQual faz afirmações, justamente para capturar do respondente o nível de percepção e expectativa que ele possui com relação ao que foi afirmado. Se o nível de percepção é menor ao nível de expectativa para respectiva afirmativa, significa que aquele serviço não existe ou não atende ao esperado.

Desta maneira, foram elaboradas 14 afirmações englobando os 6 determinantes da qualidade definidos, alinhando-os de acordo com as informações mais referenciadas durante a coleta obtida através das técnicas utilizadas até aqui, conforme demonstradas a seguir:

Confiabilidade:

- Existe confiabilidade nas informações geradas na unidade.
- Todos tem acesso a informação.
- O serviço de segurança da informação presente na unidade auxilia na preservação da imagem do setor.
- O acesso ao computador é feita de forma segura (existe um login e senha para cada pessoa).
- Existem procedimentos para descarte das informações em papel ou mídia.
- A unidade tem uma Política de Segurança da Informação.

Tangibilidade

- As instalações são adequadas para fornecer um controle de acesso seguro as informações da unidade

Comunicação

- Existe treinamento ou conscientização para a segurança da informação.

Integridade

- É respeitado o princípio da Integridade na unidade (somente pessoas autorizadas podem manipular as informações.)
- A informação está sempre organizada.

Responsividade

- A organização tem um comitê ou grupo responsável pela Segurança da Informação.
- A segurança da informação recebe a devida importância da unidade.
- Existe um comprometimento das pessoas com relação a segurança das informações dentro da unidade.

Disponibilidade

- A informação está sempre disponível.

Estas 14 afirmativas foram dispostas em 2 grupos, o da percepção e o da expectativa. A mesmas 14 afirmações foram aplicadas para capturar a percepção e a expectativa, apresentando mudanças somente no tempo verbal. As afirmativas do grupo da percepção expressam afirmações no presente e da expectativa foram expressas no futuro do pretérito. As repostas para cada afirmação foram dispostas numa escala *Likert* variando de 1 a 7, onde a escala menor 1 é caracterizada por discordo totalmente e escala maior 7, concordo totalmente. Um exemplo do questionário é mostrado na figura 22. O questionário completo pode ser visto no Apêndice C.

O que se percebe em relação à Segurança da Informação	Nível
1. A organização tem um comitê de Segurança da Informação.	**Discorda** 1 2 3 4 5 6 7 **Concorda**
O que se deseja em relação à Segurança da Informação	**Nível**
2. Deveria existir um comitê de Segurança da Informação na organização.	**Discorda** 1 2 3 4 5 6 7 **Concorda**

Figura 22 - Exemplo do Questionário de Percepção de Segurança da Informação

Dentre os diferentes *gaps* que podem ser obtidos através da aplicação do questionário *ServQual* como já foi mencionado no capítulo 3, para este trabalho optou-se por trabalhar com o *gap* 5 que define a lacuna ou diferença existente entre a percepção e a expectativa em relação ao serviço.

A equipe Seis Sigma decidiu aplicar o questionário para todos os funcionários da UCI e UTI como também aos Diretores do HUSM e implantadores. A aplicação se deu da seguinte maneira, denominando uma dimensão para cada grupo:

- Dimensão Funcionários (Fun) foram entregues 60 questionários e retornaram 32 preenchidos.
- Dimensão Diretores (Dir) foram entregues 6 questionários e retornaram 6 preenchidos;
- Dimensão Implantadores (Imp) foram entregues 4 questionários e retornaram 4 preenchidos;

Para que fosse possível alcançar um número satisfatório de retorno, foi estipulado um prazo de 2 (duas) semanas, que posteriormente foi prorrogado a mais 1 (uma) semana para entrega dos questionários, o que totalizou ao final 42 questionários entregues.

Os resultados podem ser visualizados na tabela 11, onde é mostrado as médias dos níveis capturados para o grupo da percepção (P) e do grupo expectativa (E) relacionada com cada dimensão. Foi utilizado o programa de estatística Sphinx Léxica (www.sphinx.com.br) para a geração das médias.

Para o calculo dos *gaps* (G) foi feita a subtração das médias resultantes da percepção e expectativa. Exemplo: Comitê Gestor de Segurança: P(1,88) - E(5,94) = G(-4,06). Este valor negativo significa que o serviço está bem abaixo do que é percebido, ou seja, se espera muito mais pelo serviço do que se percebe.

Tabela 11 - Obtenção dos *gaps*

Afirmações	Dimensões								
	FUN			DIR			IMP		
	P	E	G	P	E	G	P	E	G
1. Comitê Gestor de Segurança	1,88	6,94	-5,06	1,5	6,83	-5,33	1,75	7	-5,25
2. Confiabilidade das Informações	3	6,31	-3,31	3,83	6,83	-3	2,75	7	-4,25
3. Integridade da informação	3,31	6,25	-2,94	3,33	7	-3,67	2,75	7	-4,25
4. Disponibilidade da informação	3,59	6,22	-2,63	3	5,83	-2,83	3,25	6,75	-3,5
5. Organização da Informação	2,94	6,53	-3,59	3	7	-4	3,75	5,25	-1,5
6. Acessos a informação por todos	3,5	5,19	-1,69	4,33	3,5	0,83	5	3,25	1,75
7. Política de Segurança da Informação	1,37	6,38	-5,01	2,33	7	-4,67	1,5	7	-5,5
8. Segurança da Informação como prioridade	2,13	6,47	-4,34	2,33	7	-4,67	2,25	6,75	-4,5
9. Preservação da imagem com a segurança da informação	3,16	6,75	-3,59	3,67	6,83	-3,16	2,75	6,75	-4
10. Acesso seguro ao computador	3,16	5,97	-2,81	2,5	6,67	-4,17	2,25	7	-4,75
11. Adequação das instalações para o controle de acesso seguro	4,31	6,56	-2,25	4,67	7	-2,33	3,5	6,75	-3,25
12. Comprometimento com a segurança das informações	3,13	6,66	-3,53	3,17	6,83	-3,66	2,75	7	-4,25
13. Conscientização em Segurança	1,97	6,41	-4,44	2	7	-5	1,25	6,75	-5,5
14. Descarte da informação	2,28	6,31	-4,03	2,33	6,83	-4,5	1	6	-5

Observando a coluna com os valores dos *gaps* de cada dimensão, constata-se de forma clara, que a maioria dos valores é negativa. Isto acontece por que as médias das percepções são menores do que as de expectativa, revelando que os respondentes percebem pouco com relação as afirmações feitas e tem uma alta expectativa de que elas sejam implantadas.

Para fornecer uma idéia mais precisa da concentração dos *gaps* mais altos os dados da tabela 10 foram demonstrados em um gráfico de dispersão. A figura 23 mostra o gráfico de dispersão da dimensão Funcionários, onde observa-se que as maiores disparidades em relação aos níveis de expectativa para que ações sejam feitas são: “o Comitê Gestor de Segurança da informação” (-5,06 na afirmação 1); “a política de segurança da informação” (-5,01 na afirmação 7) e “conscientização ou treinamento” (-4,44 na afirmação 13).

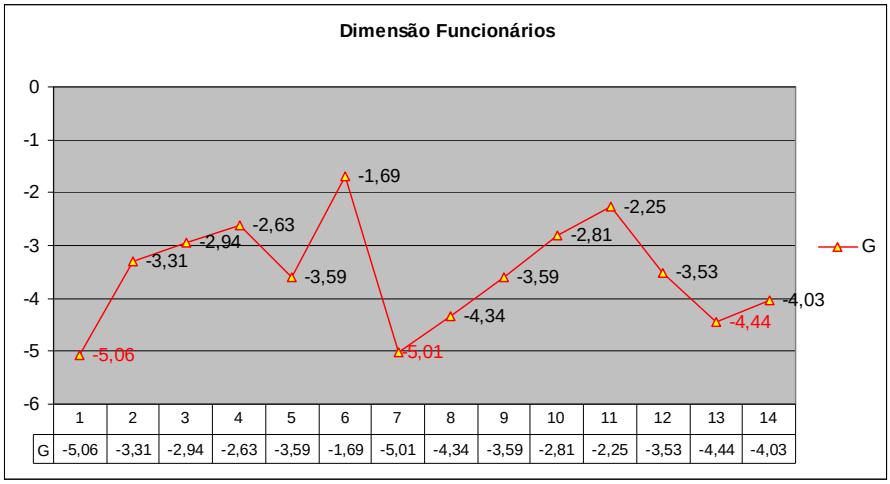


Figura 23 - Gráfico de dispersão da Dimensão Funcionários

A figura 24 apresenta o gráfico de dispersão da dimensão Diretores onde os maiores *gaps* estão concentrados em: “comitê gestor de segurança” (-5,33 na afirmação 1); “conscientização ou treinamento” (-5 na afirmação 13) e “política de segurança da informação” e “segurança da informação como prioridade” com (-4,67 na afirmação 7 e 8).

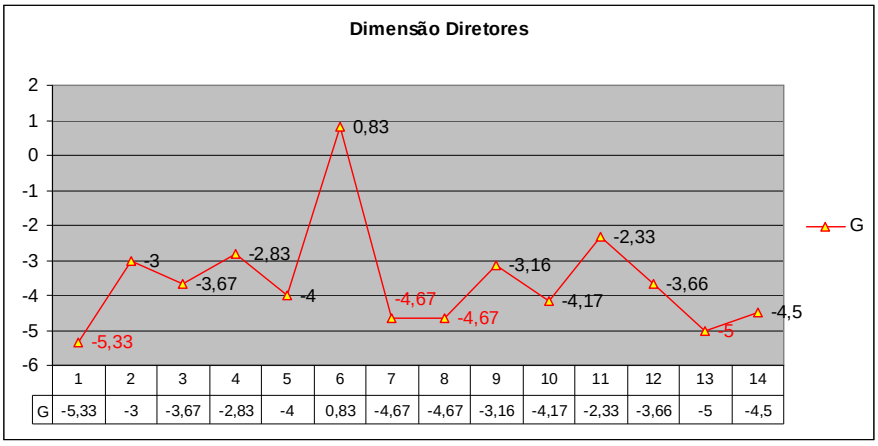


Figura 24 - Gráfico de dispersão da Dimensão Diretores

A figura 25 mostra o gráfico de dispersão da dimensão Implantadores, intensificando os mais altos *gaps* em: “conscientização ou treinamento” (-5,5 na afirmativa 13); “política de segurança da informação” (-5,5 na afirmação 7) e o comitê de segurança em (-5,25 na afirmação 1).

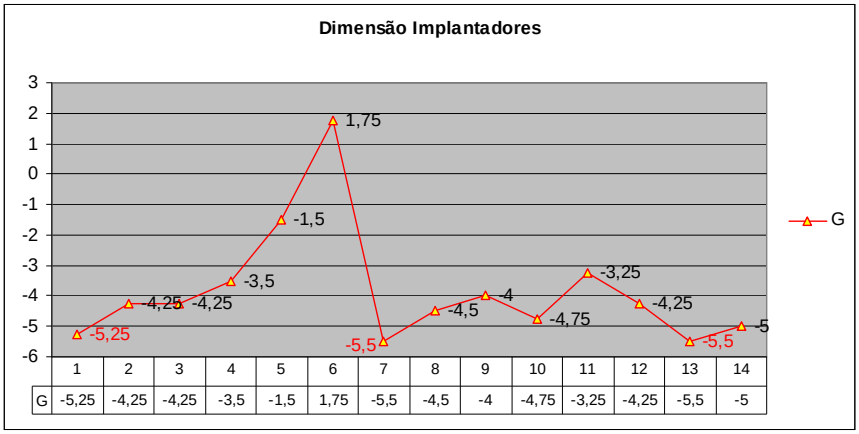


Figura 25 - Gráfico de dispersão da Dimensão Implantadores

Observa-se que algumas das disparidades são identificadas em todas as dimensões como mostra a figura 26.

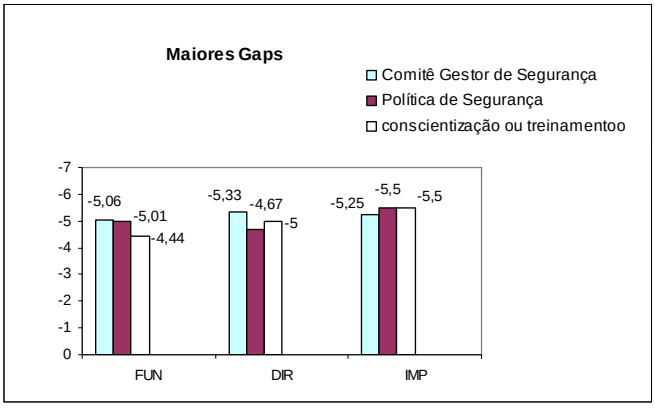


Figura 26 – Maiores Gaps

A figura 26 mostra as expectativas com relação a política de segurança da informação com valores maiores na visão dos Implantadores e Funcionários; conscientização ou treinamento em segurança com valores maiores entre Diretores e Implantadores e o comitê gestor de segurança com valores maiores entre Funcionários e Diretores. Estas igualdades resultantes entre todas as dimensões revela uma grande expectativa concreta para que essas medidas sejam implantadas, ficando de fato comprovada como sendo metas importantes as quais foram derivadas através da técnica de *brainstorming* (vide tabela 10, problemas 1, 13 e 20), reafirmados nas entrevistas (vide seção 5.2.7, necessidades 4, 6 e 7) e que vêm a ser as principais causas obtidas no Diagrama de Causa e efeito (vide seção 5.2.8).

5.3.9 Aspectos Gerais da fase Definir

Uma das principais dificuldades na fase Definir foi a reunião de todos os membros da equipe pessoalmente, realidade ocasionada por um fator principal: incompatibilidade de horários. O HUSM por ser um hospital público e funcionar 24hs, possui atendimentos em três turnos (matutino, vespertino e noturno), o que inviabilizou atividades em conjunto, visto que muitos realizam outras atividades no período em que não estão na instituição como em consultórios particulares ou em outros hospitais. Para solucionar esta adversidade a equipe decidiu criar uma lista virtual de discussões com o e-mail de todos os integrantes da equipe. O objetivo desta lista foi realizar reuniões virtuais, troca de informações, comunicar notícias, buscar a solução de problemas, unindo a equipe Seis Sigma para que todos participassem, interagissem e principalmente acompanhassem ativamente todo o processo de gestão.

A fase Definir teve duração de três meses ao todo, ultrapassando ao que estava previsto no cronograma. A causa deste acréscimo no tempo planejado deve-se ao fato de que muitas das reuniões tiveram que ser re-agendadas e conseqüentemente levando mais tempo para serem cumpridas.

O outro fator é exatamente o distanciamento da equipe Seis Sigma decorrente da incompatibilidade de horários, citado anteriormente. No entanto, este problema foi amenizado através da criação da lista virtual.

Resultados Alcançados:

- Criação da Equipe Seis Sigma: grupo responsável pela implantação da gestão da Segurança da informação (vide seção 5.2.1).
- Escopo da gestão da segurança da informação: cobrindo aspectos estratégicos, tecnológicos, organizacionais, humanos e ambientais.
- Sensibilização: através do marketing interno, onde foi realizada a divulgação da gestão da segurança da informação.
- Definição dos problemas das unidades (vide tabela 12): resultantes das técnicas de *brainstorming*, entrevistas e Diagrama de Causa e efeito.
- Estabelecimento das metas: resultantes das lacunas de desempenho, apontando as maiores expectativas como relação a implantação das políticas de segurança da informação; conscientização ou treinamento em segurança e o comitê gestor de segurança.

Tabela 12 - Relação dos problemas

Relação de Problemas definidos
1. Ausência de regras e normas em segurança da informação.
2. Uso de Senhas fracas no Sistema UCI
3. Inexistência de termo de confidencialidade nas unidades
4. Extravio de fichas de pacientes (sem estabelecimento de regras)
5. Sem monitoramento e registro da auditoria
6. As informações não são classificadas quanto as característica de proteção
7. Extravio de fichas de pacientes (locais de armazenamento)
8. Todos os profissionais compartilham o mesmo usuário e senha na unidade
9. Ausência de suporte a segurança da informação.
10. Ausência de suporte a segurança da informação- Notificação de incidentes
11. Inexistência de e-mail profissional nas unidades.
12. Falta de iniciativas que promovam a segurança da informação
13. Extravio de fichas de pacientes (falta de informação e comunicação)
14. Descontrole no compartilhamento de pastas.
15. Sem procedimentos para o descarte de mídias.
16. Compartilhamento de usuários para acesso ao sistema
17. Uso inadequado do Sistema Eletrônico de Pacientes
18. Ausência de controles que definam a situação (ativo/inativo) dos funcionários
19. Ausência de bloqueio de estação
20. Os riscos não são gerenciados
21. Má localização dos extintores
22. Acesso facilitado no setor

5.4 Fase Medir

Após a conclusão da fase Definir, esta etapa do processo é caracterizada pela avaliação dos problemas obtidos na fase anterior. A partir destes resultados, a fase medir vêm a ser um “termômetro” que indica o estado atual em relação a segurança da informação das unidades,

revelando quantitativamente os pontos em que necessitam de melhorias. Nesta fase é detalhado a mensuração do nível de qualidade e entendimento em SI (seção 5.3.1), a mensuração dos problemas e a identificação dos números de prioridade de cada risco orientadas através da ferramenta FMEA (seção 5.3.2).

5.3.1 Mensuração do Nível de Qualidade e Entendimento em SI

A equipe Seis Sigma tomou a decisão de realizar nesta fase a mensuração da qualidade atual da segurança da informação, uma vez que a abordagem Seis Sigma visa obter a qualidade do negócio através da qualidade dos processos. No caso deste trabalho, a segurança é o principal agente para a geração desta qualidade. Desta maneira foi estipulado dois quesitos para mensurar este nível:

- nível de qualidade de segurança da informação
- nível de entendimento em segurança da informação

O propósito desta medição é avaliar se houve melhorias na segurança da informação com a implantação da gestão e verificar se esta melhoria foi percebida pelas duas unidades. Esta constatação somente pode ser obtida com uma mensuração antes e outra ao final, após a implantação das melhorias.

Para isso, foi confeccionado um questionário (vide Apêndice D) simples e de rápido preenchimento, onde foi possível capturar dos usuários a qualidade percebida nas unidades, relacionado a tudo que é feito para garantir a segurança da informação, e para complementar, foi capturado o nível de entendimento dos usuários com o tema segurança da informação. A mensuração do nível de entendimento deve-se a fato de que uma das metas estabelecidas na fase Definir, comprovadas com os maiores *gaps*, foi a falta de um treinamento e conscientização em segurança da informação, demonstrando claramente que os usuários revelam uma alta expectativa para que haja um programa deste tipo.

O questionário foi entregue a 60 pessoas envolvendo as duas unidades e estipulado um prazo de 2 (duas) semanas para sua entrega, sendo retornados 38.

O resultado obtido pode ser visualizado na figura 27, revelando que o nível de segurança percebido é de 78,20 % somadas a três opções “Baixíssimo”, “Muito baixo” e “Baixo” somadas as três opções, o que veio confirmar a razão da quantidade de problemas relacionados na fase Definir (seção 5.2).

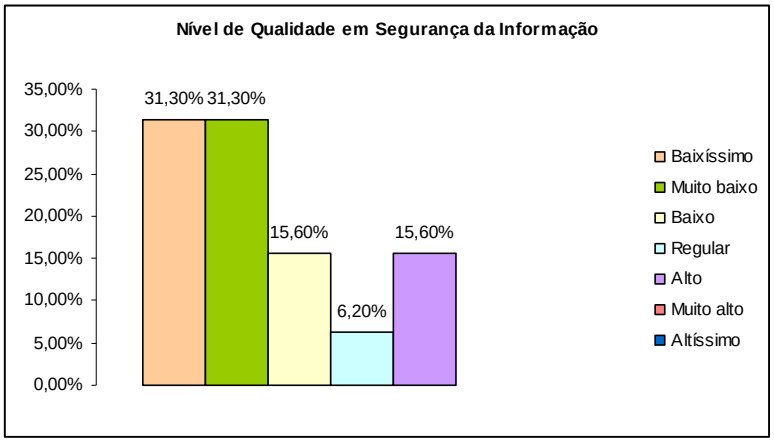


Figura 27 – Nível de Qualidade da Segurança da Informação

A figura 28 mostra o que entendimento dos respondentes para com o tema segurança da informação é de apenas 15,7 % somados os níveis “Altíssimo”, “Muito Alto” e “Alto”, considerando que o entendimento do conceito é de vital importância para a disseminação das práticas que serão produzidas pela gestão de segurança da informação. Este dado reitera o interesse sinalizado na fase Definir (seção 5.2) pela realização da conscientização em segurança da informação.

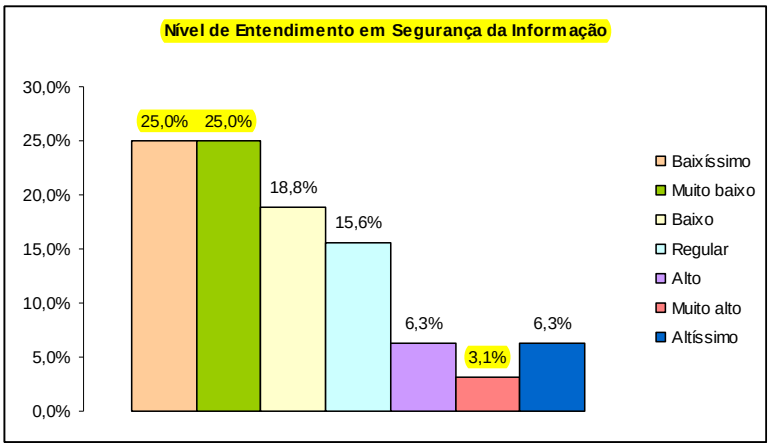


Figura 28 – Nível de Entendimento em Segurança da Informação

Após terem sido capturados os níveis atuais de qualidade e entendimento em segurança da informação percebido pelas unidades, o próximo passo é avaliar os problemas relacionados na fase Definir pelos usuários, verificando seu impacto e identificando os maiores riscos para cada problema retratado. A ferramenta utilizada nesta avaliação é o FMEA, apresentada na próxima subseção.

5.3.2 FMEA (*Failure Model and Effect Analysis*)

O objetivo da aplicação do FMEA nesta fase é avaliar as não conformidades percebidas pelo os usuários (problemas identificados na fase Definir), considerando os efeitos ou impacto que estes podem causar.

A avaliação foi realizada pela equipe Seis Sigma sob a responsabilidade do *BlackBelt*. O Formulário FMEA (vide figura 28) apresenta um cabeçalho superior com as informações gerenciais do projeto, como data de realização da medição, identificação dos clientes, data de finalização projeto. O campo “Item do Processo” é caracterizado por ser um resumo do problema principal que está identificado no campo “Modo de Falha”, originados da fase Definir. No campo “Efeito” é descrito o impacto gerado pelo problema avaliado. No campo “Causas” indica as razões que fazem o problema existir.

A avaliação de cada problema ou modo de falha determinou os seguintes índices: severidade (S) - estima o quanto de gravidade representa aquele problema ou modo de falha para as unidades; ocorrência (O) - estima a probabilidade de determinado problema vir a ocorrer (se ocorre com pouca frequência ou muita frequência); detecção (D) - indica a probabilidade que um determinado problema pode ser percebido ou detectado e o Número de Prioridade e Risco (NPR) - indica o grau de cada risco resultante da multiplicação dos três itens anteriores.

A figura 29 ilustra o formulário FMEA, podendo ser visto completo no Apêndice E. A figura 30 mostra o gráfico de Pareto ordenado pelos mais altos NPRs gerados pelo FMEA.

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas								
Projeto:	Gestão de Segurança da Informação		Cliente: UCI e UTI - Hospital Universitário de Santa Maria					
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira		Data do FMEA:	06 e 07/2008				
Data início Projeto:	03/2008		Data Conclusão Projeto:	12/2008				
Item do Processo	Modo de Falha	Efeito	Causa	Controles Atuais	S	O	D	NPR
Suporte a segurança da informação	Ausência de suporte a segurança da informação.	Os problemas de segurança da informação passam a não ser reportados ou não existe uma referência quando problemas acontecem.	-Falta um Comitê gestor de Segurança da Informação para garantir um suporte de gestão visível dentro das unidades para com a Segurança da Informação	-	8	9	7	504
Projeto em segurança da informação	Falta de iniciativas que promovam a segurança da informação	Os usuários não tem comprometimento com a segurança da informação e os riscos.	Falta programas de conscientização em segurança da informação na unidade	-	8	9	7	504
Suporte de segurança da informação	Ausência de regras e normas em segurança da informação.	Violação dos princípios de segurança da informação (confiabilidade, integridade, disponibilidade)	Não existe um processo disciplinar formal para os funcionários que tenham violado as políticas e procedimentos de segurança organizacional, tal processo pode dissuadir outros.	-	8	9	7	504
Senhas fracas	Uso de Senhas fracas no Sistema UCI.	Facilidade em ocorrer acessos indevidos por outros usuários através de interceptação ou roubo.	Inexistência de controle de verificação de segurança nas senhas.	-	8	8	6	384
Termo de confidencialidade	Inexistência de termo de confidencialidade nas unidades	Falta de Comprometimento com a informação e os dados	Não é exigido um termo de confidencialidade na contratação de um novo profissional no acesso aos sistemas da instituição	-	6	9	7	336
Fichas de pacientes	Extravio de fichas de pacientes	Demora no atendimento ao paciente	Muitos profissionais manuseando a mesma informação. Falta de regras e/ou políticas na unidade	Existem escaninhos numerados com o leito para guardar as fichas do paciente	9	9	4	324

Figura 29 - Formulário FMEA (Folha 1)

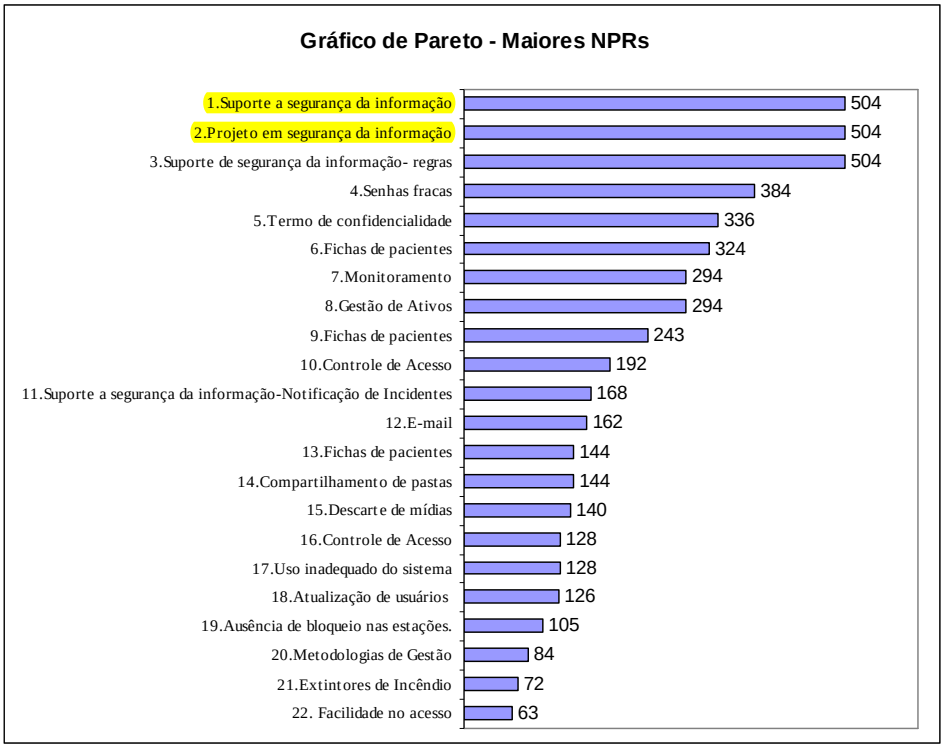


Figura 30 - Gráfico de Pareto

Como a avaliação foi realizada pela equipe Seis Sigma, sendo que metade do grupo pertence ao HUSM, representados pelo Diretor Clínico e os chefes dos respectivos setores, os NPRs que foram gerados consideraram fortemente o impacto que a instituição poderia sofrer

ao não resolver determinado problema, visando também cumprir as metas estabelecidas. Esta preocupação pode ser observada pelos mais altos NPRs obtidos na avaliação, que foram:

- "suporte de segurança da informação"- o hospital não tem um grupo ou comitê responsável pela segurança da informação, sendo que muitos dos problemas poderia ser evitado se houvesse um grupo com este caráter que fiscalizasse os problemas e irregularidades existentes, como descrito na fase Definir
- "projeto de segurança da informação" – que ressalta a importância de ter um programa de conscientização no hospital com o objetivo de propagar a idéia de que a segurança é uma responsabilidade de todos.
- "suporte de segurança da informação - regras"- causada pela inexistência de regras e de um processo disciplinar formal para quando acontecer uma violação da segurança. Alguns dos processos judiciais que o HUSM sofre são derivados pelo mau uso da informação, o que se relaciona com a ausência de regras e políticas que determine como a informação deve ser tratada.
- "senhas fracas"- o que salienta que a equipe necessita tomar alguma medida para atenuar este problema que é recorrente nas unidades como mencionado na seção 5.2.
- "termo de confidencialidade"- documento no qual o usuário se responsabiliza pela confidencialidade das informações que tem acesso.

O uso da ferramenta FMEA foi um recurso muito importante nesta fase, pois durante sua elaboração pode-se constatar que além do impacto que determinado problema ou falha pode gerar, também foi possível diagnosticar as causas que levam aquela falha ou problema acontecer. Contudo é uma ferramenta de fácil leitura e preenchimento onde toda equipe pode participar sem maiores dificuldades.

Cabe ressaltar que os NPRs obtidos com a aplicação da ferramenta interferem nas metas estabelecidas na fase Definir (seção 5.2), agregando a elas informações importantes, como, por exemplo, ficha de pacientes (problema 6 no gráfico de Pareto), que tem como causa principal a ausência de normas reguladoras que estabeleçam o seu uso correto. Este problema pode ser solucionado por meio de um controle na política de segurança da informação. O que se constata com esta avaliação realizada através do FMEA é que as estratégias de implantação devem seguir uma ordem de prioridade, obedecendo aos maiores NPRs, o que não significa que somente os maiores valores vão ser trabalhados. Cada problema precisa ser analisado e estabelecido uma estratégia de tratamento, visando a minimização ou controle dos riscos e cumprimento das metas. A implantação das estratégias

que forem estabelecidas depende da viabilidade do hospital e condições da equipe Seis Sigma para implementar cada solução. A próxima fase visa analisar cada estratégia para o tratamento dos riscos.

5.3.3 Aspectos Gerais da Fase Medir

Os objetivos propostos pela ferramenta FMEA são similares a prática de gerenciamento de riscos mencionado na norma NBR ISO/IEC 17799, principalmente, por caracterizar-se em uma etapa onde através da mensuração são gerados os maiores riscos. A aplicação do FMEA deve revelar o que precisa ganhar uma atenção maior, traduzindo em números os problemas definidos pelos usuários (funcionários e diretores).

A aplicação da ferramenta foi positiva e de fácil elaboração, levando um mês e meio para sua construção. No total a fase Medir teve um tempo de duração de 2 meses, cumprindo o estabelecido no cronograma para esta fase, salientando que esta etapa começou com um mês de atraso decorrente da ampliação de tempo da fase Definir.

Resultados Alcançados:

- Mensuração dos níveis de qualidade
  - Nível da qualidade percebida em segurança da informação - 78,20 % consideram o nível de segurança “Baixíssimo”,“Muito baixo” e “Baixo” somadas as três opções.
  - Nível de entendimento em segurança da informação - 68,8 % consideram o nível de segurança “Baixíssimo”,“Muito baixo” e “Baixo” somadas as três opções.
  - Mensuração dos problemas – através da ferramenta da qualidade FMEA pode-se quantificar cada problema através do índice de severidade, ocorrência e impacto;
- Identificação dos maiores riscos – geração do número de prioridade de cada risco NPRs, que representa a ordem de prioridade que a estratégia de solução precisa ser implantada (vide apêndice E).

5.4 Fase Analisar

A fase Analisar consiste na tarefa de traçar a estratégias de tratamento do risco. Assim como na fase Medir onde se obteve os NPRs através da ferramenta FMEA, nesta fase o uso desse recurso se estende com o objetivo principal de propor ações de melhoria para cada risco. A análise de cada risco como a estratégia de tratamento, depende da viabilidade

financeira do hospital assim como seus recursos e a disponibilidade da equipe em executar cada ação recomendada. A tabela 13 mostra as estratégias de tratamento e as ações que são recomendadas para cada risco. Para melhor visualização optou-se por apresentar o item do processo, modo de falha e o NPR. A descrição dos campos são os mesmos utilizados na fase Medir com o acréscimo do campo "Estratégia" que indica a estratégia de resposta de cada risco e o campo "Ações recomendadas", que descreve a solução planejada para minimização do risco. O formulário completo pode ser visto no Apêndice F.

Tabela 13 – FMEA - Estratégias e Ações recomendadas

Item do Processo	Modo de Falha	**NPR**	Estratégia	Ações recomendadas
1. Suporte em segurança da informação	Ausência de suporte a segurança da informação.	**504**	Mitigar	Criação de um Comitê de Segurança da Informação no HUSM
2. Projeto em segurança da informação	Falta de iniciativas que promovam a segurança da informação	**504**	Mitigar	Promover encontros com os funcionários que visem a conscientização para com a segurança, instituindo como uma atividade no calendário do HUSM.
3. Suporte de segurança da informação	Ausência de processos disciplinares, regras e normas em segurança da informação.	**504**	Mitigar	Elaboração do documento da Política de Segurança da informação
4. Senhas fracas	Uso de Senhas fracas no Sistema UCI	**384**	Mitigar	Elaborar políticas de controle acesso e implementação de controle das senhas no cadastro dos usuários do sistema UCI.
5. Termo de confidencialidade	Inexistência de termo de confidencialidade nas unidades	**336**	Mitigar	Criação e o estabelecimento de termo de confidencialidade para todo o usuário novo no sistema.
6. Fichas de pacientes	Extravio de fichas de pacientes (sem estabelecimento de regras)	**324**	Mitigar	Estabelecimento de normas para o manuseio e armazenamento das fichas de pacientes
7. Monitoramento	Sem monitoramento e registro da auditoria	**294**	Mitigar	Implantar a geração de logs e gerados no sistema da UCI
8. Gestão de Ativos	As informações não são classificadas quanto as características de proteção	**294**	Mitigar	Inventário dos ativos e classificação da informação
9. Fichas de pacientes	Extravio de fichas de pacientes (locais de armazenamento)	**243**	Mitigar	Providenciar recursos como prateleiras ou armários para o armazenamento adequado, evitando que fiquem exposto ou extraviados.
10. Controle de Acesso	Todos os profissionais compartilham o mesmo usuário e senha na unidade	**192**	Mitigar	Criação de um domínio de cada unidade para fazer o gerenciamento dos usuários para o acesso ao computador.

Item do Processo	Modo de Falha	NPR	Estratégia	Ações recomendadas
11. Suporte a segurança da informação	Ausência de suporte a segurança da informação-Notificação de incidentes	**168**	Mitigar	Criação de canais de comunicação para reporte de incidentes, como site, e-mail ou telefone.
12. E-mail	Inexistência de e-mail profissional nas unidades.	**162**	Mitigar	Criação de e-mails profissionais nas unidades e criação do e-mail da unidade.
13. Fichas de pacientes	Extravio de fichas de pacientes (falta de informação e comunicação)	**144**	Mitigar	Elaborar e implantar mensagens de alerta para evitar o extravio.
14. Compartilhamento de pastas	Descontrole no compartilhamento de pastas.	**144**	Mitigar	Coibir o compartilhamento de pastas, através de controles na rede
15. Descarte de mídias	Sem procedimentos para o descarte de mídias.	**140**	Mitigar	Estabelecer políticas para descarte de mídias no documento da política
16. Controle de Acesso	Compartilhamento de usuários para acesso ao sistema	**128**	Mitigar	conscientização e mensagens de alerta para inibir o compartilhamento de login e senha com outros usuários
17. Uso inadequado do sistema	Uso inadequado do Sistema Eletrônico de Pacientes	**128**	Mitigar	Criação de Manual de ajuda para o sistema
18. Atualização de usuários	Ausência de controles que definam a situação (ativo/inativo) dos funcionários	**126**	Mitigar	Determinar através da direção do hospital o encaminhamento de todos funcionários inativos das unidades.
19. Ausência de bloqueio nas estações.	Ausência de bloqueio de estação	**105**	Mitigar	implantar bloqueios na estação quando constatada a ociosidade da máquina.
20. Metodologias de Gestão	Os riscos não são gerenciados	**84**	Mitigar	Adoção do FMEA como ferramenta de gerenciamento dos riscos, estimulando a instituição adotar uma cultura proativa
21. Extintores de Incêndio	Má localização dos extintores	**72**	Transferir	Recomendar a direção que sejam realocados alguns extintores e providenciados a compra de outros.
22. Acesso facilitado nos setores	Acesso facilitado no turno da noite	**63**	Transferir	Permitir que a porta de acesso as unidades somente seja aberto por dentro em horário noturno

Na tabela 13, pode ser observado cada problema com a sua respectiva estratégia de tratamento dos riscos juntamente com as recomendações de ações. Assim como na fase Medir a equipe Seis Sigma analisou cada problema, estabelecendo uma estratégia de resposta para o risco mensurado. As ações recomendadas foram elaboradas a partir dos recursos e das condições de tratamento disponíveis no HUSM, complementadas pelos recursos que podem ser fornecidos e implementados pelos *BlackBelts* e *GreenBelts*. É importante planejar a

execução de cada ação, levando em conta as prioridades obtidas com os NPRs. Entretanto, algumas ações podem levar mais tempo que outras, por serem mais complexas e exigir um esforço maior da equipe.

5.4.1 Aspectos Gerais da Fase Analisar

A fase Analisar pode-se resumir como a continuação integrada da fase Medir que mensurou cada problema descrito. A análise realizada foi bastante minuciosa o que contou muito com os esforços do Executivo Líder no intuito de angariar subsídios para que pudesse ser possível na próxima fase Implementar realizar o planejamento da execução das ações recomendadas. Está fase de análise de viabilidade para a definição de cada estratégia teve a duração de 28 dias, necessários para a confirmação de cada ação estabelecida, cumprido o programado no cronograma. Um dos aspectos que contribuiu para o cumprimento do tempo e conseqüentemente dos objetivos desta fase foi a utilização da lista virtual, que foi formada para atenuar o problema de incompatibilidade de horários que a equipe tinha, mas que obteve um amadurecimento gradativo da idéia de utilização deste recurso.

Resultados Alcançados:

- Estratégia de tratamento do risco – analise de cada risco, estipulando uma estratégia de resposta (campo “Estratégia” na tabela 13”).
- Recomendação de ações – recomendações de ações para cada estratégia de risco retratada (campo “Ações recomendadas” na tabela 13”).

5.5 Fase Implementar

Um dos fatores críticos para o sucesso da implantação de uma gestão Seis Sigma é estar fundamenta em dados. Ao chegar a esta fase teve-se um trabalho intenso de coleta de dados, medições e analises, justificando os princípios do Seis Sigma de ser uma abordagem que promove o alcance das melhorias baseando-se em dados concretos, capturados a partir das exigências e requisitos dos usuários.

A fase Implementar caracteriza-se pelo seu cunho prático uma vez que é a partir deste momento que as ações de melhoria são implantadas. Entretanto, para que as ações fossem realizadas de forma organizada, a principal ferramenta utilizada nesta fase é a 5W1H detalhada não próxima subseção.

5.5.1 5W1H – Plano de Ação

A ferramenta da qualidade 5W1H estabelece um plano de execução, no qual orienta as diversas ações planejadas na fase Analisar, servindo também como uma ferramenta de controle e documentação para verificar o andamento e a execução de cada ação projetada. Como foi mencionado na fase Medir, os maiores NPRs foram planejados com prioridade de execução. A tabela 14 apresenta este planejamento.

A ferramenta 5W1H é composta por 7 campos. O primeiro campo “O que” consiste em caracterizar sobre o que se refere a determinada ação. No campo “Quem” é definido o responsável pela implantação da ação, sendo indicada no trabalho pelos seguintes responsáveis: (I) Implantadores, (D) Direção, (F) Funcionários. O campo “Quando” indica a data que foi executada a ação. O campo “Onde” define o local. O campo “Porque” esclarece a razão daquela ação estar sendo planejada. O campo “Como” determina de que forma a ação será tratada. O campo “S” (Situação) informa sobre a execução da ação, sendo que (C) indica que a ação foi concluída e (A) indica que a ação permanece em andamento.

Um aspecto positivo que contribuiu para a implantação da maioria das ações foi o trabalho colaborativo, o que possibilitou a divisão de tarefas entre Diretores, Funcionários e Implantadores, como pode ser observado no campo “Quem” da tabela 14. Esta divisão provocou com que algumas ações de nível de prioridade menor fossem finalizadas antes das de nível de prioridade maior, em função de não exigir muito tempo para sua execução, sendo algumas mais fáceis de serem cumpridas como, por exemplo, o problema 13 “Elaborar e implantar mensagens de alerta para evitar o extravio das fichas de pacientes”. Esta constatação é vista como positiva, uma vez que o envolvimento das pessoas foi fundamental para garantir a obtenção das metas.

A ação planejada para o problema 10 (vide tabela 14) que tem objetivo de criar um domínio para cada unidade, visando o gerenciamento dos usuários não pode ser concluída, uma vez que envolvia severas mudanças no servidor de usuários do HUSM. Deste modo, a Direção juntamente com setor de informática estuda a possibilidade de implantação desta medida. O planejamento para o problema 21 (vide tabela 14) também não foi concluído, no entanto a Direção também estuda a viabilidade de solução do problema. A ação para o problema 22 (vide tabela 14) não foi implantada por questões administrativas, sendo ainda analisada pela Direção. Em função do adiamento temporário destas ações, o planejamento da implantação das medidas foi estendido para o mês de dezembro.

A seguir é detalhada a implantação das metas que foram estabelecidas na fase Definir.

Tabela 14 - Plano de Ação

O que	Quem	Quando	Onde	Porque	Como	S
1. Ausência de suporte a segurança da informação.	I, D, F	Inicio: 08/2008 Término: 08/2008	UCI e UTI	Criar no HUSM um grupo responsável para oferecer aos usuários suporte e manter a segurança da informação	Criação de um Comitê de Segurança da Informação	C
2. Falta de iniciativas que promovam a segurança da informação	I, D	Inicio: 08/2008 Término: 09/2008	UCI e UTI	Promover o uso consciente da informação como também subsidiar com as melhores práticas em segurança da informação.	Criação de programa de Conscientização em Segurança da Informação e divulgação do tema.	C
3. Ausência de processos disciplinares.	I, D	Inicio: 08/2008 Término: 09/2008	UCI e UTI	Estabelecer políticas que promova o uso correto da informação, sendo criadas sanções ou punições no caso de violação das regras.	Elaboração da política de Segurança da Informação	C
4. Uso de Senhas fracas no Sistema UCI	I	Inicio: 09/2008 Término: 09/2008	UCI e UTI	Controlar o uso de senhas fracas que são definidas pelos usuários	Inserir função de controle no sistema de cadastro de usuários da UCI	C
5. Inexistência de termo de confidencialidade nas unidades	D	Inicio: 08/2008 Término: 08/2008	UCI e UTI	Promover o uso consciente da informação e responsabilizando aqueles que fazem mau uso dela.	Criação do termo de confidencialidade nas unidades que deve ser assinado pelos atuais e novos funcionários	C
6. Extravio de fichas de pacientes	I, F, C	Inicio: 08/2008 Término: 09/2008	UCI e UTI	Diminuir o número de desaparecimento de prontuários e organizar a informação.	Estabelecer normas para o manuseio e armazenamento das fichas de pacientes	C
7. Sem monitoramento e registro da auditoria	I	Inicio: 09/2008 Término: 09/2008	UCI e UTI	Maior controle sobre as operações realizadas no sistema	Implantar a geração de logs no sistema da UCI	C
8. As informações não são classificadas quanto as característica de proteção	I, F	Inicio: 08/2008 Término: 09/2008	UCI e UTI	As pessoas não tem conhecimento do valor da informação.	Inventário dos ativos e classificação da informação	C
9. Extravio de fichas de pacientes	F	Inicio: 09/2008 Término: 09/2008	UCI e UTI	Organizar e manter protegidas todas as informações principalmente de pacientes.	Providenciar recursos como prateleiras ou armários para armazenar as fichas de pacientes	C
10. Controles Compartilhamento de usuários para acesso ao sistema	I	Inicio: 08/2008 Término: 09/2008	UCI e UTI	Evitar o uso compartilhado de logins e senhas	Política de controle de usuário e senhas nas unidades para acesso ao sistema	C
11. Ausência de suporte a	I, D	Inicio:	UCI e	Fornecer aos usuários meios	Criação de canais (e-	C

O que	Quem	Quando	Onde	Porque	Como	S
segurança da informação- Notificação de incidentes		09/2008 Término: 09/2008	UTI	para notificar todos os incidentes de segurança da informação que for presenciado.	mail, site) de comunicação para reporte de incidentes	
12. Inexistência de e-mail profissional nas unidades.	D	Inicio: 08/2008 Término: 08/2008	UCI e UTI	Evitar que os funcionários utilizem e-mails pessoais para assuntos profissionais	Criação de e-mails profissionais nas unidades	C
13. Extravio de fichas de pacientes	I, D	Inicio: 08/2008 Término: 08/2008	UCI e UTI	Evitar que os funcionários deixem fichas, prontuários ou qualquer informação de paciente exposta.	Elaborar e implantar mensagens de alerta para evitar o extravio das fichas	C
14. Descontrole no compartilhamento de pastas.	D	Inicio: 08/2008 Término: 08/2008	UCI e UTI	Impedir que o compartilhamento seja feito sem nenhuma razão e que outras pessoas tenham acesso, manipule ou copie a informação.	Através de bloqueio na rede, sendo permitido por meio de uma autorização.	C
15. Sem procedimentos para o descarte de mídias.	I, D	Inicio: 08/2008 Término: 09/2008	UCI e UTI	Evitar que informações em CD, disquete ou papel vão para o lixo com a possibilidade de recuperá-la	Estabelecer políticas para descarte de mídias	C
16. Controles Compartilhamento de usuários para acesso ao sistema	D	Inicio: 12/2008	UCI e UTI	Para evitar que pessoas de outros departamentos ou de fora acessem os computadores das unidades	Criação de um domínio de cada unidade para fazer o gerenciamento dos usuários.	A
17. Uso inadequado do Sistema Eletrônico de Pacientes	I	Inicio: 08/2008 Término: 08/2008	UCI	Evitar erro de cadastro, redução da produtividade e oferecer um suporte on-line	Criação de Manual de ajuda para o sistema da UCI.	C
18. Ausência de controles que definam a situação (ativo/inativo) dos funcionários	D	Inicio: 08/2008 Término: 08/2008	UCI e UTI	Impedir que funcionários demitidos, afastados e em licença tenha acesso ao sistema do HUSM, evitando também que outros se apossem desses usuários.	Atualização de todos os funcionários inativos que tenham um usuário de acesso ao sistema.	C
19. Ausência de bloqueio de estação	D	Inicio: 08/2008 Término: 08/2008	UCI e UTI	Impedir que terceiros utilize a máquina deixada com a sessão aberta por outro usuário.	Implementar bloqueios automáticos na estação de trabalho quando detectada a ociosidade da máquina.	C
20. Os riscos não são gerenciados	I, D	Inicio: 09/2008 Término: 09/2008	UCI e UTI	Estimular a instituição através da sua direção e o comitê gestor de SI a obter uma cultura proativa, gerenciando os seus riscos	Adoção do FMEA como ferramenta de gerenciamento dos riscos	C
21. Má localização dos	D	Inicio:	UCI e	A localização dos	Realocação ou	A

O que	Quem	Quando	Onde	Porque	Como	S
extintores		12/2008	UTI	extintores fica longe das estações de trabalho, o que pode dificultar o seu uso	compra de novos extintores	
22. Acesso facilitados as unidades	D	Inicio: 12/2008	UCI e UTI	Evitar que pessoas de fora tenham acesso as informações restritas ao setor	Permitir que a porta de acesso as unidades abra somente por dentro, sobretudo no horário noturno	A

5.5.2 Primeira Meta implantada – Comitê Gestor de Segurança da Informação

A criação do Comitê Gestor de Segurança da Informação (CGSI) foi uma das metas definidas por todos os participantes da pesquisa *ServQual* (lacunas de desempenho) realizado na fase Definir. Deste modo, para cumpri-la, foi necessário instituir uma comissão que assegure a continuação da gestão da segurança da informação não somente nas unidades UCI e UTI, mas que também vise sua expansão para outros setores do HUSM. A criação do comitê foi a primeira meta ser cumprida, uma vez que sua atuação tem influência sobre as outras, principalmente na política.

A equipe Seis Sigma através da sua autoridade maior, o Executivo líder, juntamente com o Diretor Geral do HUSM aprovaram a criação do Comitê Gestor de Segurança da Informação (vide Apêndice G), nomeando os respectivos representantes para a composição do primeiro grupo da instituição responsável pela segurança da informação. Fazem parte também do CGSI os membros da equipe Seis Sigma Executivo Líder e os Campeões.

Deve-se destacar que os conceitos da equipe Seis Sigma é diferente do Comitê Gestor de Segurança da Informação, sendo o primeiro um grupo responsável pela implantação do projeto Seis Sigma e o segundo um grupo independente e deliberativo do HUSM, portanto cabe a ele a decisão de aprovar, promover, monitorar e principalmente manter a gestão da segurança da informação, disseminando a cultura pelo hospital.

Os primeiros trabalhos executados pelo CGSI foram aprovar e apoiar a realização do programa de conscientização em segurança da informação e a implantação da política de segurança da informação detalhadas a seguir.

5.5.3 Segunda Meta implantada - Programa de Conscientização em Segurança da Informação

A criação do Programa de Conscientização em Segurança da Informação (PCSI) foi outra meta definida na fase inicial da gestão de segurança da informação. Após a aprovação pelo CGSI o programa foi implantado no mês de setembro de 2008 e teve a duração de três dias, sendo oferecida em três turnos diferentes com duração de 40 minutos cada apresentação. Foram abordados no programa os seguintes temas:

- Conceitos principais de segurança da informação, como confidencialidade, integridade e disponibilidade;
- Tipos de informação: públicas, privadas, íntimas e secretas;
- Quebra de Confidencialidade;
- Engenharia Social;
- Os problemas que foram relatados durante a fase Definir e como se espera tratá-los.

Este último tópico apresentado no programa serviu de base para que todos os funcionários entendessem como os problemas poderiam ser tratados. Para isto se utilizou o plano de ações, onde eles puderem perceber que através da reunião de esforços de todos é possível chegar a soluções que minimizem os problemas existentes e também que essas mesmas soluções sejam sustentadas. Durante o programa de conscientização também foram apresentados os nomes dos membros que compõem o comitê formado no HUSM, o qual irá tratar de questões específicas de segurança da informação dentro da instituição.

5.5.4 Terceira Meta implantada - Política de Segurança da Informação

O documento da Política de Segurança da Informação (PSI) foi a terceira meta a ser cumprida e é um dos principais instrumentos da gestão da segurança da informação. A política pode ser vista no Apêndice I, no entanto por medidas de segurança, somente a primeira e segunda folha foram expostas totalmente, as demais são mostrados apenas os tópicos abordados no documento.

A política foi implementada com a colaboração de toda equipe conforme as necessidades e a realidade das unidades, contando com a supervisão do comitê. O documento é composto por normas e padrões divididos em ambiente convencional e computacional, uma vez que muitas das rotinas das duas unidades são realizadas de forma manual. O ambiente convencional reúne todos os aspectos não tecnológicos que fazem parte da unidade, como os prontuários dos pacientes, exposição de documentos na impressora, acessos de profissionais as unidades e entre outros. O ambiente computacional reúne todos os aspectos tecnológicos

que são utilizados pelas unidades, como o uso de e-mails profissionais, utilização de internet para fins profissionais, uso de senhas fortes e entre outros.

A política foi implantada em setembro de 2008, após ter sido aprovada pelo Comitê Gestor de Segurança da Informação e realizada o seu treinamento sobre cada item abordado na política. O treinamento da política se deu da mesma forma que o programa de conscientização, também sendo oferecido em três turnos diferentes, tendo a duração de três dias, o que resultou a participação de 39 funcionários. Foi disponibilizada uma cópia impressa do documento para o responsável de cada turno e também para os responsáveis pelas unidades.

5.5.5 Aspectos Gerais da Fase Implementar

A fase Implementar por caracterizar-se em procedimentos mais práticos, muitas das ações já foram sendo executadas a medida que eram planejadas, o que causou o alinhamento do cronograma executado com o previsto. Todas as ações foram realizadas em cooperação com os membros da equipe e funcionários. Desta maneira foi possível implantar a maioria delas eficientemente. Das 22 ações planejadas, 19 foram concluídas, restando 3 (vide tabela 14, problema 10, 21 e 22) com execuções em andamento, sendo estendidas para o mês de dezembro.

A ferramenta 5W1H, além de ser um recurso eficiente no planejamento da execução dos trabalhos é também um meio de manter documentada todas ações previstas e executadas, auxiliando a gestão como sendo uma ferramenta de controle.

Resultados Alcançados:

- Elaboração e execução das ações que foram definidas (seção 5.2), medidas (seção 5.3) e analisadas (5.4), sendo 22 ações planejadas, 19 foram concluídas (Vide tabela 14, Situação C), resultando na obtenção das metas estabelecidas que foram a criação do comitê, programa de conscientização e a política.

5.6 Fase Controlar

A fase Controlar consiste em uma etapa de verificação em que as ações são inspecionadas, investigando se surtiram melhorias e se foram bem sucedidas,ou seja, se o problema foi eliminado ou reduzido e se as metas foram atingidas. Se o resultado for favorável, a equipe deverá impedir que o problema já resolvido ocorra novamente no futuro

ou que evolua. Deste modo, é fundamental traçar calendários de inspeções e manter uma constante vigilância das ações de melhorias. A fase Controlar finaliza um ciclo que deverá ser mantido e controlado pelo HUSM. A partir desta etapa a característica do método DMAIC fica evidente, pois ao se verificar e monitorar ações de melhorias, novos ajustes e correções devem ser feitas, demonstrando a dinamicidade do método.

A sustentação das melhorias somente poderá ser atingida se existir uma constante monitoria, promovendo assim uma qualidade gradual voltada para a segurança da informação.

Neste trabalho, para realizar o controle das ações implantadas utilizou-se os Indicadores de Desempenho (*Key Performance Indicator*- KPIs) que verificam o quão bem está o desempenho dos processos em relação à meta implantada.

5.6.1 Desempenho Comitê Gestor de Segurança da Informação

O comitê tem pouco tempo de atuação, mas realizou decisões importantes, como o estabelecimento de um programa de conscientização nas unidades e aprovação da política. O grupo tem o projeto de estender o programa, instituindo-o como uma atividade no calendário da instituição para todos os funcionários novos, fazendo parte dos cursos de humanização que já são oferecidos pelo hospital, o que foge do escopo deste trabalho. Por ser um grupo interdisciplinar, o qual envolve diferentes áreas, como informática, jurídico e pesquisa, espera-se que sua atuação auxilie na sustentação das melhorias que foram implantadas e conseqüentemente expandindo-as para os demais setores.

5.6.2 Desempenho do Programa de Conscientização em Segurança da Informação

Após a implantação do programa foi realizado uma avaliação (vide Apêndice H) para verificar o nível de satisfação dos funcionários com o programa de conscientização, tanto no que diz respeito ao conteúdo abordado quanto a apresentação realizada. A avaliação é um instrumento importante de controle na melhoria contínua da qualidade e neste caso os participantes demonstraram satisfação em participar do programa de conscientização na área de segurança da informação, como pode ser visualizado na figura 31. A figura revela que 72,70% dos participantes avaliaram como “Muito Bom” a apresentação do PCSI, e 68,20% avaliaram como “Muito Bom” o conteúdo, demonstrando satisfação em discutir e aprender sobre segurança da informação.

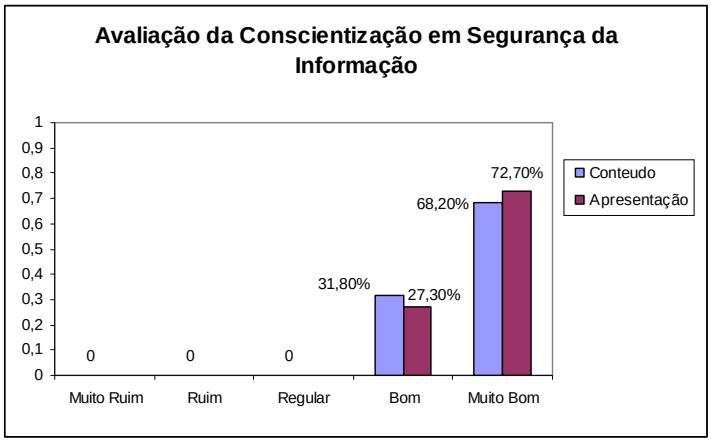


Figura 31 - Avaliação da Conscientização em Segurança da Informação

O programa de conscientização em segurança da informação, como observado nas avaliações, obteve um índice de satisfação grande entre os participantes, entretanto não alcançou a participação massiva de todos os funcionários das duas unidades, obtendo apenas 53% de participação. Deste modo, a Direção do HUSM, juntamente com o comitê planeja a promoção de mais semanas como esta para os demais funcionários que não puderam participar.

5.6.3 Desempenho da Política de Segurança da Informação

Passados 45 dias de adaptação após a implantação da política, foi realizada uma avaliação (vide Apêndice J). O objetivo desta avaliação é verificar o desempenho de cada item abordado nos dois ambientes: convencional e computacional.

A equipe definiu três critérios para avaliação do desempenho da política: Não Executado (NE); Parcialmente Executado (PE); Totalmente Executado (TE). A avaliação contou com a participação de 6 (seis) pessoas dividindo-se em 2 (dois) representantes da Direção, 2 (dois) dos Funcionários e 2 (dois) dos Implantadores. A figura 32 mostra os resultados da avaliação para o ambiente convencional, onde demonstra que 46% dos itens propostos na política não estão sendo executados no que tange o ambiente convencional. Isto denota que é necessário um novo treinamento para com a política, até mesmo para investigar a razão da pouca adesão, apenas 22 % foi totalmente executado.

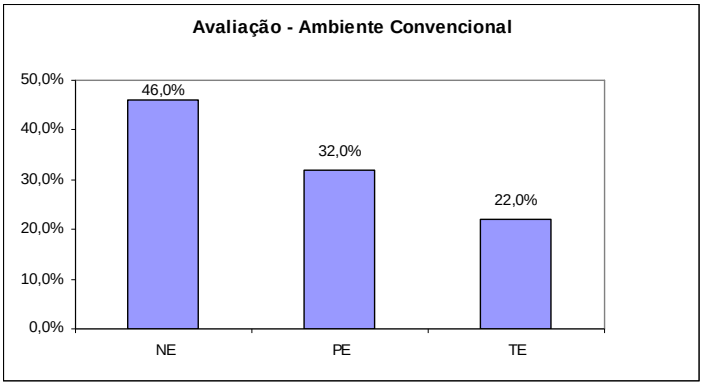


Figura 32 - Avaliação Ambiente Convencional

A figura 33 mostra os resultados da avaliação para o ambiente computacional e ilustra que 50 % das normas contidas na política estão sendo parcialmente executadas, 43% não estão sendo executadas e apenas 7% estão sendo executadas totalmente.

O índice de regras "Não Executadas (NE) continua sendo alto o que revela também a necessidade de uma investigação para saber a causa desses números. No entanto, é muito prematuro tomar alguma ação imediata, uma vez que a própria unidade está se adaptando as mudanças. Porém o controle é fundamental, pois a partir dessas evidências que são geradas as correções e os ajustes, o que pode favorecer a melhoria e auxiliar na adesão a política.

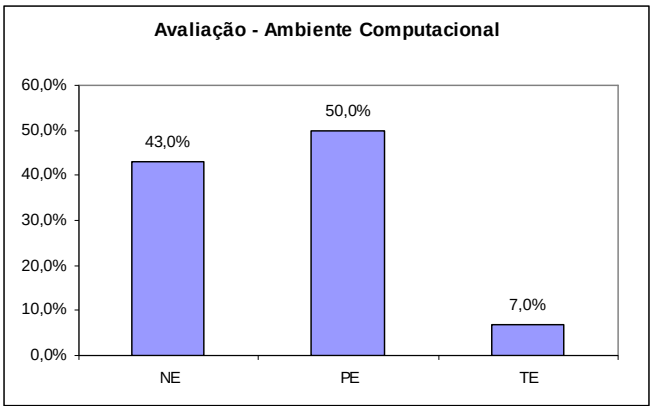


Figura 33 - Auditoria Ambiente Computacional

Após esta primeira avaliação pós-implantação da política foram feitas algumas correções a pedido dos próprios funcionários como, por exemplo:

- nova redistribuição da política: redistribuição da política separando-a por norma, o que facilita a própria leitura e a localização de algum determinado item específico

como pode ser visto na segunda versão do documento no Apêndice L. Por medidas de segurança a segunda versão da política na foi exposta totalmente, pois apresenta normas internas restritas ao hospital.

- disponibilização da política: disponibilização a política em diferentes meios como e-mail, cartilhas e site, onde foi criado um link a partir da página principal do HUSM com acesso direto a página da Gestão da Segurança da Informação (vide Apêndice M). Além da política o site também aborda alguns esclarecimentos sobre conceitos da gestão de segurança da informação, notícias da área e regulamentações vigentes, estabelecendo-se como um canal de comunicação entre a equipe de implantação da GSI, CGSI e funcionários.

A política implantada na UCI e UTI tem um prazo de revisão de no máximo 6 meses podendo este intervalo ficar maior com o tempo a medida que o próprio documento vai ficando mais completo. Entretanto, é muito importante que o seu conteúdo seja sempre atualizado e que esses prazos sejam respeitados, refletindo a dinâmica dos processos envolvidos, procurando sempre adequar o documento as mudanças que vierem acontecer nas unidades.

Novas avaliações de desempenho devem ser feitas a fim de investigar a efetividade do documento. É partir deste controle que a sustentação das melhorias e conseqüentemente da gestão pode ser alcançada.

5.6.4 Avaliação dos Níveis de Qualidade

Uma fator que contribuiu para o trabalho ter atingido suas metas, foi exatamente o trabalho colaborativo que se criou ao longo de todo o processo de gestão, favorecendo para que todas as mudanças acontecessem gradativamente. A figura 34 abaixo ilustra essa constatação, a partir do nível de qualidade percebido pelos funcionários.

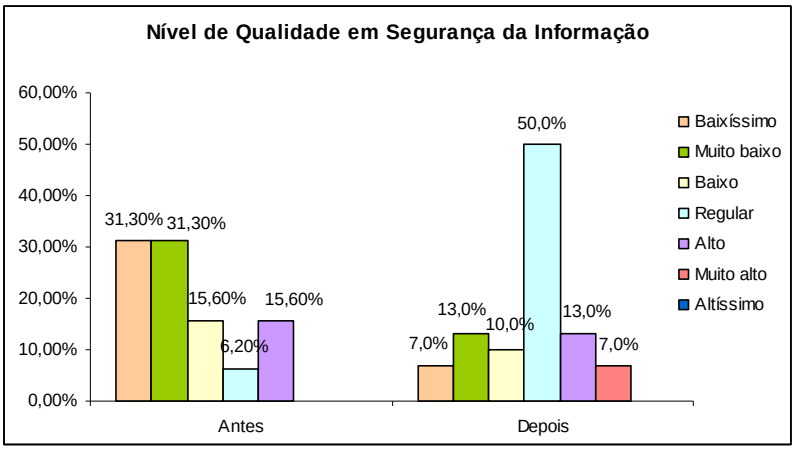


Figura 34 - Relação da qualidade antes e depois da implantação das melhorias

O mesmo questionário do apêndice D foi aplicado novamente, contando com a participação de 30 usuários. A primeira pergunta foi sobre o nível de qualidade da segurança da informação percebida. Antes das implantações das melhorias, os níveis “Baixíssimo” e “Muito baixo” e “Baixo” somavam 78,20%. Após a implantação, este índice caiu para 30%, somadas as três opções mencionadas.

O aumento mais visível ficou na opção Regular, obtendo um acréscimo de 43,8% com relação à avaliação realizada antes das implantações. A opção “Muito Alto” não havia sido mencionada na primeira avaliação antes das implantações das melhorias, representando na avaliação atual 7%.

A outra pergunta realizada foi sobre o entendimento dos usuários com o tema segurança da informação, sendo uma das questões mais citadas na fase Definir (seção 5.2). Por esta razão o programa de conscientização foi definido como uma das metas da gestão. A figura 35 mostra as duas avaliações antes e após as melhorias. Antes e depois da implantação das melhorias somadas as opções “Alto”, “Muito Alto” e “Altíssimo” representavam 15,7%, número considerado baixo para a realidade das unidades. Após as melhorias este índice teve um acréscimo satisfatório de 63%, somadas as três opções citadas anteriormente, indicando um aumento de 47,3% no nível de entendimento do tema pelos usuários.

O aumento que foi 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 funcionários que estarão gradativamente mais conscientes reforçados com o trabalho atuante do comitê gestor de segurança da informação, grupo responsável pela propagação da segurança da informação no HUSM.

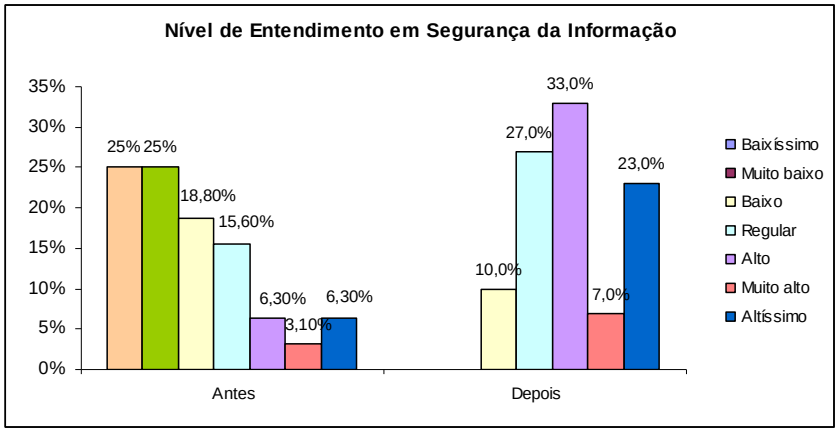


Figura 35 - Relação do Entendimento em SI antes e depois das melhorias

5.6.5 Avaliação dos Riscos

Como já foi mencionado na fase Implementar, das 22 ações que foram planejadas, 19 tiveram seus trabalhos concluídos, restando outras 3 com execuções em andamento (vide subseção 5.5.2) cumprindo as metas estabelecidas. Desta maneira, para verificar a efetividade destas ações implantadas, identificando se houve redução no NPR gerado da primeira avaliação na fase Medir, uma nova mensuração foi efetuada, a qual pode ser visualizada na integra no Apêndice N. A figura 35 faz uma comparação dos maiores NPRs da primeira avaliação com os NPRs gerados da segunda avaliação.

Observa-se na figura 36 após as implantações, os NPRs tiveram variações consideráveis, principalmente no que se refere ao índice de impacto e ocorrência (detalhado no Apêndice N) em comparação com a primeira avaliação, uma vez que os problemas ao quais estes valores se referem tiveram um controle implantado, situação que antes não existia na maioria dos problemas relacionados. Com relação ao problema 16, 21 e 22 (vide figura 36), não foi tomada nenhuma ação para solucioná-los, razão pela qual não houve alteração dos NPRs.

É importante destacar que as ações que foram implantadas não garante a solução ou a eliminação do problema, no entanto pode-se constatar que o risco causado por esses problemas foi minimizado. Por esta razão que se torna fundamental o controle de todas as ações implantadas, para que de fato elas permaneçam efetivas nas unidades. Este controle pode ser feito através do FMEA, sendo uma ferramenta de fácil elaboração e conhecida por todos da equipe Seis Sigma que fazem parte do comitê.

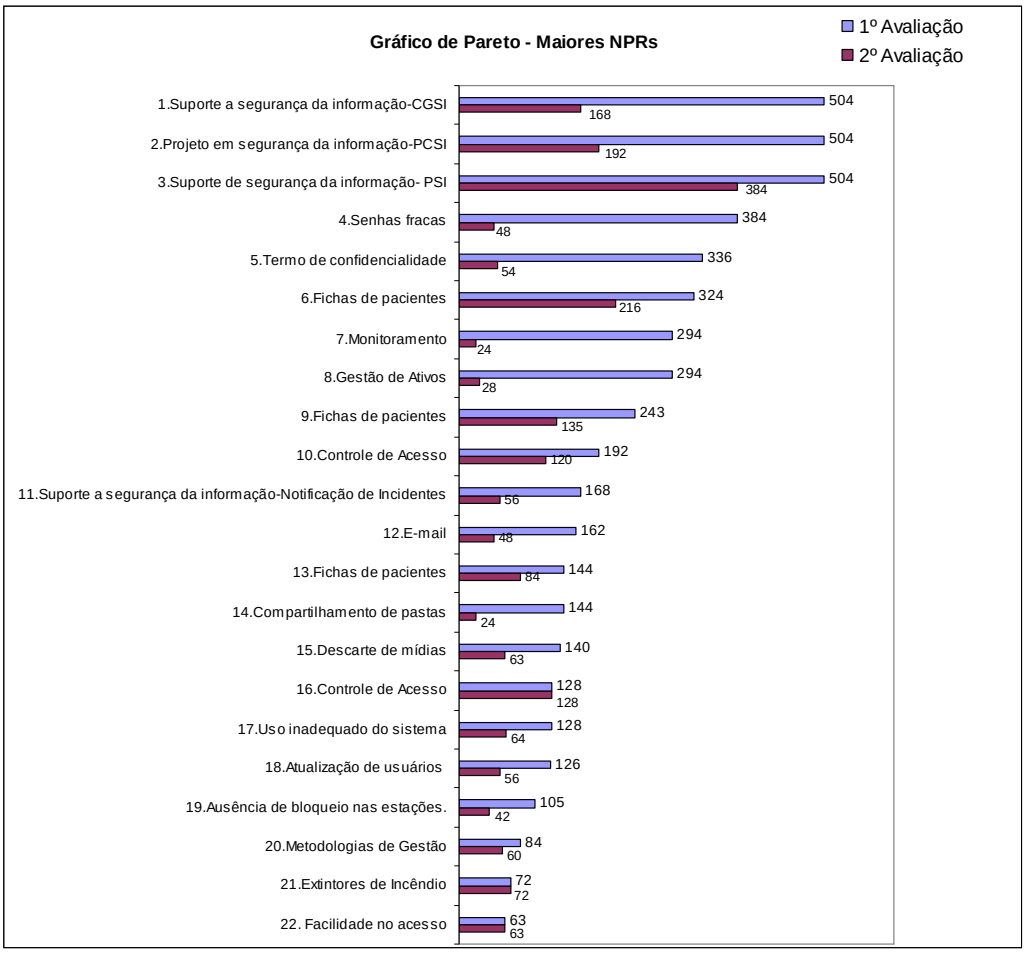


Figura 36 - Relação dos NPRs da 1º e 2º Avaliação

5.6.6 Divulgação dos Resultados

Uma tarefa importante na fase Controlar foi a divulgação dos resultados. Esta estratégia de marketing interno, que também foi realizada no início da gestão funcionou como elemento motivador, contribuindo para a sensibilização das pessoas. Por este mesmo propósito é que o makerting interno também foi utilizado ao final dos trabalhos, através da divulgação dos resultados, como forma de propagar a gestão e principalmente destacar as pessoas como peça fundamental para que as mudanças ocorressem. A divulgação dos resultados foi realizada no mês de dezembro de 2008 através da distribuição de *folders* pela UCI e UTI, mostrando as principais ações implantadas durante o processo de gestão. O folder pode ser visto no Apêndice O.

5.6.7 Aspectos Gerais da Fase Controlar

A fase Controlar teve como principal objetivo o controle das ações através dos indicadores de desempenho, avaliando a eficiência das metas que foram implantadas. Pontos significativos podem ser destacados com relação metas. O que se observou com o documento da política no que se refere ao ambiente convencional é que se obteve pouca adesão, apenas 22% dos itens foram totalmente executados, resultado que refletiu no ambiente computacional em que somente 7% dos itens foram totalmente executados. Algumas modificações e correções foram realizadas para atenuar esta baixa efetividade obtida e auxiliar na adesão ao documento como, por exemplo, a sua disponibilização na Internet. Diferente da política, o programa de conscientização obteve uma boa aceitação, constatando-se índices de 72,70% para avaliação "Muito Bom". Em relação aos níveis de qualidade e ao nível de entendimento, destacando-se o último, o qual obteve um acréscimo de 47,3%. A fase controlar teve início a partir de outubro, cumprindo o cronograma estabelecido.

Resultados Alcançados:

- Controle das metas através de indicadores de desempenho.
  - Ações executadas pelo comitê gestor de segurança da informação.
  - Índices de desempenho da política de segurança da informação.
  - Índices de desempenho do programa de conscientização em segurança da informação.
- Avaliação dos níveis de Qualidade.
  - Nível de qualidade em segurança da informação.
  - Nível de entendimento em segurança da informação.
- Divulgação dos Resultados.
  - Marketing interno através da distribuição de folders.
- Avaliação dos Riscos.
  - Relação dos NPRs da fase Medir com a fase Controlar.

5.7 Cronograma

Uma das constatações que foram feitas ao chegar ao final da fase controlar, refere-se ao cronograma de execução do projeto. O objetivo foi verificar se os prazos estabelecidos foram cumpridos. Para isso foi montado um novo cronograma que demonstra o tempo de execução de cada fase. Na tabela 15 pode ser visto o cronograma para as fases planejadas indicadas pela letra P e para as fases realizadas, indicadas pela letra R.

Tabela 15 – Cronograma de previsão e realização do projeto Seis Sigma

ETAPAS		2008									
		MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ
DEFINIR	P										
	R										
MEDIR	P										
	R										
ANALISAR	P										
	R										
IMPLEMENTAR	P										
	R										
CONTROLAR	P										
	R										

Observou-se que a fase Definir demorou um mês a mais do que foi planejado, isso por que no início do projeto pela própria exigência da abordagem em se ter dados gerados pelos usuários, as reuniões foram mais intensas, uma vez que o tema jamais havia sido trabalhado no hospital e como também não havia sido proporcionado um processo de interação tão grande como o que ocorreu neste trabalho, visto que muitas das seções de *brainstorming* tiveram que ser re-agendadas, pois o tempo delimitado, não era suficiente, sendo que eles tinham muitas dúvidas em relação ao tema e por esta razão as primeiras seções foram mais esclarecimentos do que uma coleta de problemas. Outro fator que contribuiu para elevar o tempo refere-se ao não conhecimento dos Implantadores a cerca da rotina do hospital e do funcionamento das unidades, onde foram necessárias várias reuniões e observações para obter um melhor entendimento de todo o processo.

Esse mesmo acréscimo de tempo teve efeito em cadeia na fase Medir e Analisar o que acabou também não cumprindo o planejado com a data, embora a quantidade de tempo tenha se dado dentro do previsto. O cronograma teve seu alinhamento a partir da fase Implementar, embora tenha sido estendido o plano de execução das três ações que não foram concluídas nesta fase para o mês dezembro. O início da fase Controlar não sofreu alterações, portanto estando dentro do planejado.

5.8 Conclusões Parciais

A implantação da gestão de segurança da informação através da abordagem Seis Sigma teve como foco as unidades UCI e UTI do HUSM, considerados setores vulneráveis pela própria condição e principalmente pelo fluxo grande de pessoas que circulam. A implantação foi centrada nas expectativas e percepções dos usuários com os problemas e suas soluções, o que contribuiu para uma participação intensa das pessoas em todo o processo.

Na fase Definir os resultados alcançados foram: a criação da equipe Seis Sigma, definição do escopo, sensibilização para a GSI, definição dos problemas das unidades e o estabelecimento das metas. Entretanto, foram encontradas algumas dificuldades nesta fase inicial dos trabalhos, entre elas estava à impossibilidade de reunião presencial de todos os membros da equipe e o distanciamento de alguns destes membros no processo de gestão. Estas dificuldades foram decorrentes de um fator principal: incompatibilidade de horários. Como solução foi criada uma lista virtual de discussões com o e-mail de todos os integrantes da equipe. O objetivo desta lista foi realizar reuniões virtuais, troca de informações, comunicar notícias, promovendo a união da equipe com a proposta de que todos participassem e acompanhassem ativamente todo o processo de gestão. A fase Definir teve duração de três meses ao todo, ultrapassando ao que estava previsto no cronograma. A causa principal deste prolongamento foi o re-agendamento de muitas reuniões, levando mais tempo para serem cumpridas.

Na fase Medir, os resultados alcançados foram: a mensuração dos níveis de qualidade; mensuração dos problemas e a identificação dos maiores riscos gerados com os NPRs. A principal ferramenta utilizada nesta fase foi o FMEA, a qual foi considerada de fácil aplicabilidade. No total, a fase medir teve um tempo de duração de dois meses, cumprindo o estabelecido no cronograma para esta fase. No entanto, iniciou com um mês de atraso decorrente da ampliação de tempo da fase Definir.

Na fase Analisar, os resultados alcançados foram: análise da estratégia de tratamento do risco e a recomendação de ações de solução ao problema. Pode-se resumir que esta fase foi sucessão integrada à fase Medir, sendo utilizada como principal ferramenta o FMEA. Esta fase, incluindo a definição de cada estratégia, teve a duração de praticamente um mês e cumpriu com o estabelecido no cronograma. Um aspecto que contribuiu para o cumprimento do tempo e conseqüentemente dos objetivos desta fase foi a utilização da lista virtual criada

na fase Definir, que obteve um amadurecimento gradativo sobre seu uso por parte dos integrantes que utilizaram este recurso.

Na fase Implementar, os resultados obtidos foram: elaboração e execução das ações de melhoria. Esta fase caracterizou-se por procedimentos mais práticos, onde muitas das ações já foram sendo executadas a medida que eram planejadas. Todas as ações foram realizadas em cooperação com os membros da equipe e funcionários, o que possibilitou torná-la efetiva (ação concluída). Das 22 ações planejadas, 19 foram concluídas, garantindo a obtenção das metas estabelecidas na fase Definir que foram a política de segurança da informação, programa de conscientização e o comitê. O cronograma teve seu alinhamento a partir da fase Implementar, razão pelo qual durante a fase de Análise, as implementações foram sendo planejadas, o que resultou completar esta etapa dentro do planejado. As 3 ações que não foram implantadas tiveram seu plano de execução estendido para dezembro, aguardando a análise de viabilidade de implantação com a direção. A principal ferramenta utilizada, a 5W1H, foi um recurso eficiente não somente no planejamento da execução dos trabalhos como também por ser uma ferramenta de controle, auxiliando na gestão.

Na fase Controlar, os resultados alcançados foram: o controle das metas através de indicadores de desempenho, a avaliação dos níveis de qualidade, a divulgação dos resultados e a avaliação dos riscos. Esta fase é importante para a avaliação de eficiência das metas implantadas. Pontos significativos puderam ser observados, como o documento da política, o qual obteve pouca adesão, apenas 22 % dos itens que abrangem aspectos ambientais foram totalmente executados, refletindo também no ambiente computacional, obtendo somente 7% dos itens totalmente executados. Algumas modificações e correções foram realizadas nesta fase para atenuar esta baixa efetividade obtida e auxiliar na adesão ao documento como, por exemplo, a sua disponibilização na Internet a pedido dos próprios funcionários. Diferente da política o programa de conscientização obteve uma boa aceitação, constatando-se índices de 72,70% para avaliação “Muito Bom”, refletindo no aumento do nível de entendimento em segurança da informação, o qual obteve um acréscimo de 47,3%.

Apesar do trabalho de implantação ter durado 10 meses, com ações implantadas a partir do 6° mês, a repercussão dessas implantações foi positiva principalmente pela alta direção que planeja sua extensão a outras unidades. Deste modo, este tempo decorrente de 4 (quatro) meses entre o início e o aparecimento dos primeiros resultados são justificados pela quantidade de melhorias que foram implantadas que foram evidenciadas na fase Implementar.

A abordagem Seis Sigma tem como um dos princípios a gestão baseada em dados, o que evidencia fortemente sua relação com o método DMAIC, base operacional da abordagem,

que apresenta a primeira fase de definição de forma mais enfática, o que auxilia para que os projetos de melhoria apresentem uma possibilidade maior de sucesso, pois são centrados nas percepções e expectativas dos usuários, como pode ser constado neste trabalho.

Um ponto que merece consideração sobre a abordagem Seis Sigma é o uso das ferramentas da qualidade que mediaram todo o processo de implantação. Nesta dissertação foram utilizadas algumas ferramentas, como o *brainstorming*, Diagrama de Causa e Efeito, Fluxograma, FMEA, Gráfico de Pareto e 5W1H, sendo que foi possível adequar cada ferramenta com o objetivo que se pretendia alcançar em cada uma das fases, como proposto no planejamento das fases (vide figura 15) e observado ao longo de todo processo de implantação. Por se tratarem de ferramentas de fácil usabilidade não foi necessário realizar um treinamento com a equipe Seis Sigma, apenas uma apresentação, relacionando os conceitos e características de uso foi suficiente para que todos pudessem se interar dos objetivos de cada ferramenta.

Como o DMAIC é um método que prevê a continuação dos trabalhos, criando um ciclo evolutivo de melhorias, não significa que o recomeço do método irá demorar os mesmos 10 meses que levaram esta implantação, dos quais 3 meses foram utilizados somente na fase Definir. No início da implantação do método, detalhada neste capítulo, não se conhecia os problemas, as necessidades, os riscos presentes nas unidades, motivo que justifica o tempo despendido nesta fase. Deste modo, a continuidade do método e consequentemente da gestão será mais ágil e menos onerosa, intensificando os trabalhos na fase Controlar.

CAPITULO 6

CONCLUSÕES

É sabido da necessidade existente, hoje em dia, de fornecer mecanismos mais eficientes para gerenciar as informações. A segurança é o ponto chave para garantir um dado confiável, integro e disponível, visto que a informação está a mercê de ameaças advindas de muitas formas, gerando riscos que se não forem tratados podem acarretar incidentes para a organização. Entretanto, a segurança da informação precisa ser tratada de forma abrangente, ela não é um problema apenas da área de tecnologia, mas é algo que diz respeito a todas as áreas, uma vez que a informação esta em todo lugar.

Independente do tipo de organização em que se trabalhe seja um hospital, um banco, uma universidade, a busca incessante da competição por clientes, estará sempre presente. A maioria das organizações, independente do seu domínio, está ciente de que a qualidade é importante. A abordagem Seis Sigma promove esta qualidade através da busca contínua pela melhoria apoiada através de sua base operacional, o método DMAIC. Deste modo, fica evidente que todo este processo que permeia a sua implantação precisa ser baseado em dados. Esta comprovação fica clara na própria filosofia adotada pela abordagem que prevê sempre o envolvimento das pessoas, tanto na definição dos problemas que irão ser solucionados, como no controle da solução destes problemas. O envolvimento das pessoas é um dos fatores chaves para a obtenção de sucesso com o Seis Sigma.

Esta dissertação apresentou uma proposta de implantação de uma gestão de segurança da informação através da abordagem Seis Sigma, tendo como base de implantação o método DMAIC, composto de 5 fases: Definir, Medir, Analisar, Implementar e Controlar. A proposta teve como princípio o foco no cliente interno ou usuário, sendo ele o ponto de partida para o processo de melhoria. A proposta instrumenta cada fase de execução com as ferramentas, técnicas e procedimentos que podem ser utilizados, produzindo uma gestão baseada em evidências e na realidade da organização. A implantação da proposta teve como cenário de aplicação as unidades de Cardiologia Intensiva (UCI) e Terapia Intensiva (UTI) do Hospital Universitário de Santa Maria - HUSM.

A implantação da gestão nas unidades resultou em 22 ações planejadas para a melhoria dos problemas relacionados, 19 destas tiveram suas ações concluídas, garantindo o cumprimento das metas estabelecidas na fase Definir que foram o comitê gestor de segurança da informação, programa de conscientização e política de segurança da informação. O

trabalho colaborativo formado entre a equipe Seis Sigma e funcionários foi o impulsionador para que a maioria das ações fosse concluída nas unidades.

Entre as metas que foram implantadas, sobretudo a política de segurança da informação foi constatado uma pouca adesão ao documento, revelando que apenas 22 % dos itens, os quais abrangem aspectos ambientais foram totalmente executados, o que refletiu também no ambiente computacional, que obteve apenas 7% dos itens totalmente executados. Em função destes resultados alguns ajustes e correções foram realizados na política, como a redistribuição do documento para facilitar o seu manuseio e entendimento e a sua disponibilização em outros meios como a internet, sendo ajustes sugeridos pelos próprios usuários como forma de aumentar a adesão obtida.

Diferentemente da política, o Programa de conscientização obteve uma boa aceitação, resultando índices de 72,70% para avaliação “Muito Bom”, o que contribuiu para o aumento de 43,8% da qualidade da segurança da informação percebida pelos usuários e que refletiu também no entendimento sobre o tema, onde atingiu um aumento de 47,3% em relação à realidade que existia antes das melhorias serem implantadas. Este aumento, especialmente, no entendimento sobre o tema é de vital importância porque favorece a disseminação da segurança nas unidades e principalmente a sustentação da gestão, uma vez que as pessoas estão comprovadamente mais conscientes, o que pode influenciar positivamente no seu comportamento, auxiliando para a manutenção efetiva das melhorias que foram implantadas, propiciando a formação de uma cultura voltada a segurança da informação.

Em comparação com outras metodologias de gestão de segurança da informação, discutidas no trabalho, a proposta fundamentada através da abordagem Seis Sigma apresentada nesta dissertação se mostrou mais eficaz, pois a implantação de todas ações, em especial o estabelecimento da política de segurança da informação são realizadas após a coleta de dados, definições de problemas e avaliação dos riscos, apoiados com a utilização de ferramentas da qualidade. Diferentemente das metodologias estudadas que optam por uma análise geral a fim de obter resultados em menos tempo, mas sem garantia de eficácia e principalmente de sustentabilidade destes resultados.

A implantação da gestão da segurança da informação proposta levou 10 meses e pode ser considerada economicamente cara, principalmente por ter despendido um dos maiores intervalos de tempo na fase Definir, onde foram utilizados um maior número de interações com as pessoas, mediadas por ferramentas, técnicas e procedimentos. Entretanto, os resultados gerados desta definição inicial foram essenciais para obtenção do contexto organizacional das unidades, mostrando o que realmente é fundamental e prioritário para a

realidade do ambiente no contexto da segurança. Toda a implantação teve o apoio desde a alta diretoria até estagiários, promovendo uma participação ativa através das suas percepções e expectativas com relação aos problemas. Este envolvimento favoreceu para que as mudanças pudessem ocorrer, o que comprovou a percepção realizada no início dos trabalhos em que foi capturado o nível de comprometimento das unidades para com as mudanças, onde se mostrou ser um ambiente favorável.

A implantação descrita nesta dissertação foi aplicada pela primeira vez nas unidades UCI e UTI do HUSM. No entanto, como se utilizou o método DMAIC, que é considerado um ciclo contínuo de melhoria, os trabalhos deverão ser prosseguidos no hospital, ou seja, o DMAIC deverá ter seu ciclo continuado. Contudo, o tempo de implantação de cada fase irá ser muito mais rápido no giro do método DMAIC, podendo inclusive levar um ou dois meses, sendo que algumas mensurações serão necessárias um intervalo de tempo maior como, por exemplo, a política, que deverá atingir o seu amadurecimento com a prática, sendo indispensável este tempo em decorrência da adaptação natural das unidades. Na UCI e UTI o giro do Método DMAIC se dará ao longo do ano de 2009, através do comitê gestor de segurança da informação, grupo formado e reconhecido no HUSM responsável por garantir a sustentação e a renovação da gestão da segurança da informação que foi implantada, como também realizar a sua expansão para os demais setores do hospital.

O DMAIC é definido com um método que auxilia na solução do problema, mas também pode ser considerado como um método científico, pois permitiu que a equipe ficasse centrada na obtenção dos objetivos inerentes a cada fase, orientando todas as ações do trabalho de forma estruturada e organizada, sendo que os objetivos atingidos em cada uma das etapas complementavam a seguinte, comprovando ser um método eficaz para a implantação da gestão da segurança da informação. A utilização de um cronograma aliado ao método também auxiliou para que as etapas fossem respeitadas inclusive servindo de apoio a equipe.

Como contribuição de pesquisa esta dissertação traz a proposta de implantação da gestão da segurança da informação através da abordagem Seis Sigma. Embora, haja pesquisas que referenciam o Seis Sigma e a recomendam como uma solução para a gestão de segurança da informação, constatou-se que nenhuma delas define como esta abordagem poderia ser utilizada ou de que forma as ferramentas da qualidade usadas pelo Seis Sigma poderiam ser aplicadas no contexto da segurança. Deste modo, atendendo a esta lacuna, a proposta de implantação apresentada nesta dissertação traz o delineamento de todas as fases de implantação de uma gestão de segurança da informação estruturadas através do método

DMAIC, conjuntamente com a definição de ferramentas da qualidade e procedimentos que puderam ser utilizados em cada uma das fases relatadas neste trabalho.

A proposição da gestão deteve o foco no cliente interno ou usuário, portanto as ferramentas e procedimentos definidos e empregados tiveram como propósito atender a este objetivo, resultando em uma gestão baseada em dados, fruto de medições, imprimindo com mais veracidade a realidade e os anseios da organização. O estudo de caso apresentado neste trabalho teve como cenário uma instituição de saúde, entretanto a proposta pode ser aplicada em qualquer domínio.

TRABALHOS FUTUROS

Para manutenção das melhorias é muito importante traçar calendários de inspeções, pois através da manutenção novas ações podem ser revistas e ajustadas, fazendo com que a gestão da segurança da informação tenha um ciclo contínuo. Desta forma é fundamental assegurar que as ações se perpetuem podendo inclusive ser inseridas outras ferramentas da qualidade para avaliar a sustentabilidade da gestão da segurança da informação. Sugere-se a criação de um sistema informatizado de gestão que reúna as ferramentas que foram utilizadas neste trabalho com o objetivo de facilitar o processo de implantação.

Como foi constada no trabalho a política de segurança da informação não obteve resultados satisfatórios, sendo assim é necessário um trabalho mais intenso de promoção a adesão as regras contidas no documento. Técnicas de Endomarketing podem ser usadas para auxiliar e reforçar a esta adesão como, por exemplo, recursos áudio-visuais, incentivos, brindes, workshops, entre outros.

REFERÊNCIAS BIBLIOGRÁFICAS

_____http:// www.ge.com/

_____http://www.sphinx.com.br/

10° Pesquisa Nacional de Segurança da Informação. Disponível em: < http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf >. Acesso em 10 de Set.2008. Módulo Security. 2007.

AAZADNIA, M., FASANGHARI, M. **Improving the Information Technology Service Management with Six Sigma.** IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.3, 2008.

ABAGNALE, F., et al.: FBI 2005 **Computer Crime Survey**. Federal Bureau of Investigation, 2005.

ADAMS, Cary W. et al. **Six sigma deployment**. Butterworth Heinemann., 2003.

AGUIAR, Silvio. **Integração das Ferramentas da Qualidade ao PDCA e ao Programa Seis Sigma**. Nova Lima: INDG Tecnologia e Serviços Ltda., 2006.

ALBERTS, C; DOROFEE, A. **Managing Information Security Risks: the OCTAVE approach**, 2º ed: Pearson Educations, Inc, 2004.

ALVES, A. A. **Segurança da Informação - Uma Visão Inovadora de Gestão**. Editora Ciência Modera, Rio de Janeiro, 2006.

ALVES, R. **Filosofia da ciência: introdução ao jogo e suas regras**. 21 ed. São Paulo: Brasiliense, 1995.

BACCARINI, David; GEOFF. S.; LOVE, Peter E.D. **Management of risks in information technology projects**. Industrial Management & Data Systems. Volume 104, Number 4, pp. 286, 2004.

BAKRY S.H, BAKRY F.H. **A strategic view for the development of e-business**. International Journal of Network Management 2001; 11: 103–112.

BAUER, M. W. & GASKELL, G. **Pesquisa qualitativa com texto, imagem e som**. Tradução de Pedrinho A. Guareschi. Petrópolis: Vozes, 2002.

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

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações** – São Paulo: Atlas, 2005.

BERTO, R. M. V. S.; NAKANO, D. N. A **produção científica nos anais do encontro nacional de engenharia de produção: um levantamento dos métodos e tipos de pesquisa**. Produção, v. 9, n. 2, p. 65-75, jul. 2000.

BLAUTH , Regis. **Seis Sigma: Uma estratégia para melhorar resultados**. Revista FAE Business, n.5, abr. 2003. Disponível em: <http://www.est.ipcb.pt/psi/psi_OG/>. Acesso em 10 Abr. 2008.

BROOKS, W.; WARREN, M. **A Metodology of Health information Security Evaluation**. Health Care and Informatics Review Online. 2006.

CALDER, A; WATKINS, S. IT **Governance: a manager's guide to date security and bs7799/iso17799**, 2nd: London and Sterling, VA, 2003.

CAMPBELL, S. **How to Think About Security Failures**. Communications of the ACM 49(1), 37–39, 2006.

CAMPOS, André. **Sistema de Segurança da informação: Controlando os Riscos**. 2.ed. Florianópolis: Visual Books, 2007.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações**. São Paulo: Editora SENAC São Paulo, 1999.

CERVO, A. L.; BERVIAN, P. A. **Metodologia científica**. São Paulo: Makron Books, 1996.

CHANG, S. E. ; HO, C. B. **Organizational factors to the effectiveness of implementing information security management**. Management & Data Systems, Vol. 106 No. 3, pp. 345-361, 2006.

CHOWDHURY, S. **Working toward Six-Sigma Success**. Manufacturing Engineer, 127, pp. 14, jul. 2001.

CUPPENS, F.; SAUREL, C. **Specifying a security policy**. In: Proceedings of 9th IEEE Workshop on Computer Security Foundations. Kenmare, Kerry, Ireland: Kluwer Academic Publishers, 1996. p. 123–134. Disponível em: <http://www.rennes.enstbretagne.fr/_fcuppens/articles/csfw96.ps>. Acesso em: 30 maio 2007.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2000.

DUARTE, Carolina. **Normas Internacionais em Segurança da Informação: Grandes mudanças na versão 2005 da ISO/IEC 17799**. 10 Jan 2006. Modulo Security Magazine. Disponível em http://www.modulo.com.br Acesso em: 20 Set 2007.

ECKES, George. A Revolução Seis Sigma: **O método que levou a GE e outras empresas a transformar processos em lucro**. Rio de Janeiro: Editora Campus, 2001.

ELOFF , J. H. P. ; ELOFF, M. M. **Information security architecture**. Computer Fraud & Security, vol. 2005, pp. 10-16, 2005.

EVERET, J. **Security awareness: switch to a better programme**. Computer Fraud Security. pp 15-18. 2006.

FENZ, S.; GOLUCH G.; EKELHART A.; RIEDL, B.; WEIPPL, E. **Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard**. IEEE Computer & Society. 13th IEEE International Symposium on Pacific Rim Dependable Computing, 2007.

FERNANDES, A. A.; ABREU, V. F. **Implantando a Governança de TI da Estratégia à Gestão dos Processos e Serviços**. Rio de Janeiro: Brasport, 2006.

FERREIRA, F. N. F.; ARAÚJO, M. T. **Política de Segurança da Informação: Guia Prático para Implementação e Elaboração**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2006.

FRANZ, L. A. S. **Análise Crítica de um Projeto Seis Sigma em uma Indústria Petroquímica**. Dissertação de Mestrado submetida ao Programa de Pós-Graduação em Engenharia de Produção, Porto Alegre :UFRGS: Escola de Engenharia, 2003.

FREITAS, Marta A.; COLOSIMO, Enrico A. **Confiabilidade: análise de tempo de falha e testes de vida acelerados**. Belo Horizonte: Fundação Christiano Ottoni, Escola de Engenharia da UFMG, 1 ed., 1997.

GEORGE M.; ROWLANDS D.; KASTLE, B. **Was ist Lean Six Sigma?** Springer, 2007.

GERBER, M ; SOLMS, R. V.; **Management of risk in the information age**. Computers & Security, vol. 24, pp. 16-30, 2005.

GIL, A. C. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2002.

GOLDENBERG, Mirian. **A arte de pesquisar - como fazer pesquisa qualitativa em Ciências Sociais**. Rio de Janeiro/São Paulo: Editora Record, 1997.

HARRY, Mikel J. **Abatement of business risk is key to Six Sigma**. Quality Progress, v. 33, n.7, p. 72-76, july , 2000.

HARRY, Mikel J. **Six Sigma: a breakthrough strategy for profitability**. Quality Progress. v.31, n. 5, p. 60-64, mai. 1998.

HB 174-2003. **Information security management implementation guide for the health sector**. Australia: Standards Australia International Ltd; 2003.

HELMAN, Horacio; ANDERY, P. R. P. **Análise de Falhas (Aplicação dos métodos de FMEA – FTA)**. Fundação Christiano Ottoni, Belo Horizonte, 1995.

HOFF, C. H. Y. **Avaliação dos resultados da aplicação da estratégia Seis Sigma em um restaurante industrial**. Dissertação de Mestrado em Gestão e Desenvolvimento Regional – Economia, Contabilidade e Administração, Universidade de Taubaté, Taubaté. 2005

JACOBSON, R. V. **Risk Assessment and Risk Management in Computer Security.** Handbook, S. Bosworth and M. E. Kabay, Eds., 4º ed: John Wiley & Sons, INC, 2002.

JOHNSTON, R. **Identifying the critical determinants of service quality in retail banking: importance and effect**. International Journal of Bank Marketing, v. 15, n.4, p. 111-116, 1997.

JOHNSTON, R. **The determinants of service quality: satisfiers and dissatisfiers**. International Journal of Service Industry Management, v. 6, n. 5, p. 53-71, 1995.

KIELY, L.; BENZEL, T. V. **Systemic Security Management**. IEEE Security & Privacy, pp. 74-77, 2005.

KRUGER, H.A e KEARNEY, W. D. **A prototype for assessing information security awareness**. Computer & Security. v25. pp 289-286, 2006.

LICHTENSTEIN, Sharman. **Factors in the selection of a risk assessment method**. Information Mamagement & Security, 1996. Disponível em: <http://www.emeraldinsight.com.> Acesso em 10 de fev. 2008.

LOVELOCK, C.; WRIGHT, L. **Serviços: marketing e gestão**. Tradução de Cid Knipel Moreira. São Paulo: Saraiva, 2001.

LYNCH, D. P., BERTOLINO, S., CLOUTIER E.T., **How to Scope DMAIC Projects**. Quality Progress, 36, pp. 37-41, jan.2003.

MADDOXX, M.E. **Error apparent**. Industrial Engineer, v.37, n.5, p. 40-44, 2005.

MARCIANO, J. L. P. **Segurança da Informação: uma abordagem social**. Brasília: Tese de Doutorado do Programa de Pós-Graduação em Ciência da Informação da Universidade de Brasília. 2006.

MARCIANO, J. L. P, MARQUES, M. L. O **Enfoque Social da Segurança da Informação**. Ciência da Informação, V.35, n.3, p.89-98, set/dez 2006. Disponível em: <http://www.ibict.br>. Acesso em 10 de fev.2008.

MARCINCOWSKI, S. J.; STANTON, J. M. **Motivational aspects of information security policies**. In: IEEE International Conference on Systems, Man and Cybernetics. Oakland, California: IEEE Society, v. 3, p. 2527–2532, 2003.

MARTINS, A. B.; SANTOS. C.A.S. **Uma Metodologia para implantação de um Sistema de Gestão de Segurança da Informação.** Revista de Gestão e Tecnologia e Sistema de Informação. Vol. 2, No. 2, pp. 121-136, 2005.

MARTINS, José Carlos. **Gestão de projetos de segurança da informação**. Rio de Janeiro: Editora Brasport, 2003.

MONTGOMERY, Douglas C. **Introduction to Statistical**. Quality Control. New York: John Wiley & Sons, 4 ed., 2000.

NAKANO, D. N.; FLEURY, **A. C. C. Métodos de pesquisa na engenharia de produção**. In: Encontro Nacional de Engenharia de Produção (ENEGEP), VXI., 1996.

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

NBR ISO/IEC 17799:2005 – **Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação**. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2005.

NBR ISO/IEC 27001:2006 – **Tecnologia da Informação. Sistema de Gestão da Segurança da Informação**. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2006.

NBR ISO 9000. ABNT - **ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Sistemas de gestão da qualidade - fundamentos e vocabulário: NBR ISO 9000**. Rio de Janeiro, 2000.

NETTO, A. S.; SILVEIRA, M. A. P. **Gestão da Segurança da Informação: Fatores que influenciam sua adoção em pequenas e médias empresas.** Revista de Gestão da Tecnologia e Sistemas de Informação Vol. 4, No. 3, p. 375-397, 2007.

NEUSCHELER-FRITSCH, D.; NORRIS, R. **Capturing financial benefits from Six Sigma**. Quality Progress, v. 34, n. 5, p. 39-44, may 2001.

OAKLAND, J. S. **Gerenciamento da qualidade total**. São Paulo: Nobel, 1994.

OLIVEIRA, M. A. F; CERETTA, R. N.; AMARAL, E. H.; ZEN, E.; NUNES; S.P. **Uma Metodologia de Gestão de Segurança da Informação direcionada a riscos baseado na abordagem Seis Sigma**. XXVIII Encontro Nacional de Engenharia de Produção ENEGEP, Rio de Janeiro, 2008.

OLIVEIRA, Sidney T. de. **Ferramentas para o aprimoramento da qualidade**. São Paulo: Pioneira, 1995.

PALADINI, E. P. **Qualidade total na prática.** São Paulo: Atlas, 1994

PANDE, Peter S.; NEUMAN, Robert P.; CAVANAGH, R. R. **Estratégia Seis Sigma: como a GE, a Motorola e outras grandes empresas estão aguçando seu desempenho**. 1 ed. Rio de Janeiro: Qualitymark, 2001.

PARASURAMAN, A.; ZEITHAML, V. & BERRY, L. **A conceptual model of service quality and its implications for future research.** Journal of marketing, v.49, p. 41-50, Fall 1985.

PARASURAMAN, A.; ZEITHML, V. & BERRY, L. **SERVQUAL: A multiple-item scale for measuring consumer perceptions of service quality**. Journal of retailing, v. 64, n. 1, p. 12-40, New York University, Spring, 1988.

PEARSON, Thomas A. **Measure for Six Sigma success: Combining measuremente science with Six Sigma bilds organization wisdom, big business advantages**. Quality Progress. v. 34, n. 2, p. 35-40, feb. 2001.

PEIXOTO, M. C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

PEREZ-WILSON, Mario. **Seis Sigma: compreendendo o conceito, as implicações e os desafios**. Tradução de Bazán Tecnologia e Lingüística. Rio de Janeiro: Qualitymark, 1 ed.,1999.

PFLEEGER, C. P.; PFLEEGER, S. L. **Security in Computing**, 3nd ed ed:Prentice Hall PTR, 2002.

PLSEK P.; ONNIAS A. **Quality Improvement Tools: Brainstorming**. Juran Institute Inc., USA, pp. 1-2, 1989.

Política Nacional de Informação e Informática em Saúde. 2004. Capturado em 05/11/2007. Disponível na Internet: http://www.sbis.org.br

PYZDEK, T. **The Six Sigma HandBook**. McGraw-Hill: New York, 2003.

RASIS, Dana; GITLOW, Howard S.; POPOVICH, Edward. **Paper organizers international: a fictitious Six Sigma Green Belt case study**. I. Quality Engineering. v. 15, n. 1, p. 127-145, 2002-03.

RATH & STRONG (Org.). **Six Sigma Pocket Guide**, 2. ed. Lexington, 192 p., 2001.

RIBEIRO, José L. D.; CATEN, Carla S. **Controle Estatístico do Processo - Apostila de Curso**. Programa de Pós Graduação em Engenharia de Produção. Escola de Engenharia. PortoAlegre: UFRGS, 2001a.

RICH, E.; SVEEN, F.O.; JAGER, M. **Overcoming Organizational Challenges to Secure Knowledge Management**. Proceedings of the Second Secure Knowledge Management Workshop, 2006, Brooklyn, NY 2006.

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. **Seis Sigma. Estratégia Gerencial para a Melhoria de Processos**, **Produtos e Serviços**. Editora atlas, São Paulo, 2006.

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. **Seis Sigma. Estratégia Gerencial para a Melhoria de Processos**, **Produtos e Serviços**. Editora atlas, São Paulo, 2002.

RUIZ, J. A. **Metodologia científica: guia para eficiência nos estudos 4**. Ed. Rio de Janeiro: Atlas, 1996.

SAAD M., ALRABIAH A. and BAKRY S. **E-Business Diffusion Requirements: A STOPE View for Easing the Use of ISO 17799 Information Security Mangement Standard.** Proceedings of the King Saud University Conference on the Digital Gap, King Saud University, Saudi-Arabia. 2005

SALEH, M. S.; ALRABIAH, A.; BARKRY, S. H. **Using ISO 17799:2005 information security management: a STOPE view with six sigma approach**. International Journal of Network Management, vol.17, pp. 85–97, 2007.

SANDERS, Doug; HILD, Cheryl. **A discussion of strategies for Six Sigma implementation**.Quality Engineering. v. 12, n. 3, p. 303-309, 2000.

SANTOS, A. B.; MARTINS; F. M. **Modelo de referência para estruturar o Seis Sigma nas organizações**. Gestão e Produção. São Carlos, v. 15, n. 1, p. 43-56, jan.-abr. 2008.

SANTOS, A. B. **Modelo de Referência para estruturar o programa de qualidade seis sigma: proposta e avaliação**. São Carlos. v.1. Tese - (Doutorado em Engenharia de Produção). Universidade Federal de São Carlos. 2006.

SCHELL, R. R. **Information security: science, pseudoscience and flying pigs**. In: 17th Computer Security Applications Conference. ACSAC, p. 205–216, 2001.

SCHNEIER, Bruce. **Segredos e mentiras sobre a proteção na vida digital**. Rio de Janeiro: Campus, 2001.

SCUDERE, L. **Risco Digital**. Rio de Janeiro: Elsivier, 2006.

SEHWAIL, L.; DeYONG, C. **Six Sigma in HelthCare**. Jornal of Health Care Quality Assurance imcorporating Leadership in Health Services. Vol. 16, N° 4, pp. 1-5, 2003.

SERVO, A. L.; BERVIAN, P. A. **Metodologia Científica**, 5 ed. São Paulo: Pearson Prentice Hall, 2002.

SHINGO, S. **O Sistema Toyota de Produção do ponto de vista da Engenharia de Produção**, Bookman, Porto Alegre, 1996.

SILVA D. R. P e STEIN, L. M. **Segurança da informação: uma reflexão sobre o componente humano**. Ciências & Cognição, Vol 10, pp. 46-53, 2007.

SILVA, G. R. F.; MACÊDO, K. N. F.; REBOUÇAS, C. B. A.; SOUZA, A. M. A. **Interview as a technique of qualitative research - a literature review**. Online Brazilian Journal of Nursing. V.5, N°2, 2006.

SINK, D.S. e TUTTLE, T.C. **Planejamento e Medição para a Performance**. Rio de Janeiro, Qualitymark, 1993.

SNEE, Ronald. 3.4 Per Million: **Use DMAIC to Make Improvement Part of The Way We Work**. Quality Progress. Set. 2007 Disponível em: <http://www.asq.org/qic/display-item/index.html?item=21249>. Acesso em 10 Abr. 2008.

SNEE, R. D. **Dealing with the Achilles Heel of Six Sigma initiatives: Project selection is key to success**. Quality Progress. v. 34, n. 3, p. 66-72, 2001.

SOLMS, R. V.; SOLMS, B.V. **From policies to culture**. Computers and Security, 23(4): 275–9, 2004a.

SOLMS, R. V.; SOLMS B.V. **The 10 deadly sins of information security management.** Computers and Security. Computers & Security, 23, 371-376, 2004b.

SOLMS, R.V. **Information security management (2): guidelines to the management of information technology security (GMITS)**. Information Management & Computer Security, 6(5): 221-223. MCB, University Press.1998

STANTON, J. M. et al. **Analysis of end user security behaviors**. Computers & Security, v. 24, n. 2, p. 124–133, Mar. 2005.

STEINBERG, R. M.; EVERSON, M.E.A.; MARTENS, F.J.; NOTTINGHAM, L.E. **Enterprise Risk Management Framework (DRAFT).** Comittee of Sponsoring Organizations of the Tradeway Commission (COSO). Disponível em: http://www.erm.coso.org. Acesso em: julho 2008.

SVEEN, F. O.; TORRES, J. M.; SARRIEGI, J. M. **Learning from Your Elders: A Shortcut to Information Security Management Success**. Computer Safety, Reliability and Security. Vol. 4680, pp. 224-237, 2008.

TASHI, I.; GHERNAOUTI-HÉLIE, S. **Security metrics to improve information security management**, Proceedings of the 6th Annual Security Conference, April 11-12, Las Vegas, NV, 2007.

TREICHLER, David; CARMICHAEL, Ronald; KUSMANOFF, Antone; LEWIS, John; BERTHIEZ, Gwendolyn. **Design for Six Sigma: 15 lessons learned**. Quality Progress. v. 35, n. 1, p. 33-42, july 2002.

VERMEULEN, Clive; SOLMS, R.V. **The information security management tollbox - taking the pain out of security management**. Information Management & Computer Security.10/3, pp. 119-125, 2002.

WERKEMA, M. C. C. **Criando a Cultura Seis Sigma**. Rio de Janeiro: Qualitymark, 2002.

WERKEMA, M. C. C. **Criando a Cultura Seis Sigma**. Nova Lima, MG: Werkema, 2004.

APÊNDICE A

Divulgação - Pôster do projeto de Gestão de Segurança da Informação do HUSM

Gestão de Segurança da Informação

GSI
Hospital Universitário UFSM

O que é projeto de Gestão de Segurança da Informação (GSI)?

É um projeto que visa garantir a segurança de informação dentro da UCI e UTI bem como divulgar a melhores práticas no estabelecimento e na manutenção de controles a serem implantados nas respectivas unidades.

Benefícios

- Qualificar o hopital (HUSM) com elementos legal-jurídicos gerindo uma política de segurança da informação. Desta forma isso fortalecerá o compromisso das unidades para com o cidadão, promovendo uma consciência ética e de profundo respeito à privacidade e confiabilidade dos seus dados.
- Proporcionar aos usuários da UCI e UTI, um Sistema de Gestão de Segurança da Informação que venha assegurar a proteção da informação, através de políticas, mecanismos e medidas de e para a segurança.
- Promover os programas de conscientização a fim de que se possa incorporar uma cultura organizacional que se volta à segurança da informação, de modo que permite uma maior qualidade dos padrões de saúde em ações e pesquisas executados na instituição, compromissados com a responsabilidade social e assistência ética.

Iniciativa

HUSM

Universidade Federal de Santa Maria 1960

APÊNDICE B

Questionário de Percepção Inicial da Segurança da Informação

Prezado Colaborador

O presente questionário é um dos componentes necessários a realização de um projeto voltado à segurança da informação. Todos os dados colhidos serão mantidos em sigilo de pesquisa, além do que os (as) participantes não serão nominalmente identificados, sendo preservado seu anonimato sob qualquer circunstância.

Obrigado por sua atenção.

1. Na sua opinião, analisando a estrutura da unidade, os controles de segurança da informação são:

☐Fundamentais
☐Importantes, mas não fundamentais
☐Desnecessários
☐Não sabe

2. Responda os itens abaixo, marcando uma entre as opções disponíveis, no que se refere ao seu comprometimento com as mudanças que acontecem na unidade.

Comprometimento com as mudanças.	**Muito Baixo**	**Baixo**	**Regular**	**Alto**	**Muito Alto**
Recebimento de informações sobre as mudanças que estão acontecendo na unidade.					
Condução das atividades pelo superior imediato da área na qual trabalha de acordo com as mudanças e as decisões corporativas tomadas pela unidade.					
Considerar positivas as mudanças que estão acontecendo na unidade.					
Acreditar que seu trabalho contribui para que essas mudanças tenham resultado positivo para a unidade em que trabalho.					
Acreditar que a unidade valoriza a segurança das suas informações (sigilo das informações estratégicas e confidenciais).					
Colaboração para que as mudanças adotadas na unidade tenham resultado satisfatório.					

Sinta-se à vontade para fazer quaisquer sugestões e apresentar eventuais comentários ao questionário ou aos temas que ele aborda.

_____
_____
_____
_____

APÊNDICE C

Questionário de Percepção da Segurança da Informação

Prezado Colaborador

O presente questionário é um dos componentes necessários a realização de um projeto voltado à segurança da informação. Todos os dados colhidos serão mantidos em sigilo de pesquisa, além do que os (as) participantes não serão nominalmente identificados, sendo preservado seu anonimato sob qualquer circunstância.

Se você **concorda** fortemente com a afirmação, marque o **"7"**.

Se você **discorda** fortemente da afirmação marque o **"1"**.

Para opiniões menos extremas, marque qualquer uma das pontuações da escala.

Obrigado por sua atenção.

Unidade em que trabalha?		☐UTI ☐UCI
O que se percebe em relação à Segurança da Informação		**Nível**
1	A organização tem um comitê de Segurança da Informação.	**Discorda 1 2 3 4 5 6 7 Concorda**
2	Existe confiabilidade nas informações geradas nas unidade.	**Discorda 1 2 3 4 5 6 7 Concorda**
3	É respeitado o princípio da Integridade na unidade (somente pessoas autorizadas podem manipular as informações.)	**Discorda 1 2 3 4 5 6 7 Concorda**
4	A informação está sempre disponível.	**Discorda 1 2 3 4 5 6 7 Concorda**
5	A informação está sempre organizada.	**Discorda 1 2 3 4 5 6 7 Concorda**
6	Todos tem acesso a informação.	**Discorda 1 2 3 4 5 6 7 Concorda**
7	A unidade tem uma Política de Segurança da Informação.	**Discorda 1 2 3 4 5 6 7 Concorda**
8	È dada a devida importância a Segurança da Informação na unidade.	**Discorda 1 2 3 4 5 6 7 Concorda**
9	O serviço de Segurança da Informação presente na unidade, auxilia na preservação da imagem do setor.	**Discorda 1 2 3 4 5 6 7 Concorda**
10	O acesso ao computador é feita de forma segura.	**Discorda 1 2 3 4 5 6 7 Concorda**
11	Existe um comprometimento com relação a segurança das informações dentro da unidade.	**Discorda 1 2 3 4 5 6 7 Concorda**
12	As instalações são adequadas para fornecer um controle de acesso seguro as informações da unidade	**Discorda 1 2 3 4 5 6 7 Concorda**
13	Existe treinamento ou conscientização para	**Discorda Concorda**

	a Segurança da Informação.	**1 2 3 4 5 6 7**
14	Existem procedimentos para descarte das informações em papel ou mídia.	**Discorda** **Concorda** **1 2 3 4 5 6 7**
O que se deseja em relação à Segurança da Informação		**Nível**
15	Deveria existir um comitê de Segurança da Informação na organização.	**Discorda** **Concorda** **1 2 3 4 5 6 7**
16	Deveria ser respeitado o princípio da Confidencialidade na unidade (somente pessoas autorizadas tem acesso as informações.)	**Discorda** **Concorda** **1 2 3 4 5 6 7**
17	Deveria ser respeitado o princípio da integridade na unidade (somente pessoas autorizadas podem manipular as informações.)	**Discorda** **Concorda** **1 2 3 4 5 6 7**
18	A informação deveria estar sempre disponível.	**Discorda** **Concorda** **1 2 3 4 5 6 7**
19	A informação deveria estar sempre organizada.	**Discorda** **Concorda** **1 2 3 4 5 6 7**
20	Todos deveriam ter acesso a informação.	**Discorda** **Concorda** **1 2 3 4 5 6 7**
21	Deveria existir uma política de Segurança da Informação na unidade.	**Discorda** **Concorda** **1 2 3 4 5 6 7**
22	Deveria ser dado importância a Segurança da Informação na unidade.	**Discorda** **Concorda** **1 2 3 4 5 6 7**
23	O serviço de Segurança da Informação deveria auxiliar na preservação da imagem do setor.	**Discorda** **Concorda** **1 2 3 4 5 6 7**
24	O acesso ao computador deveria ser feita de forma mais segura.	**Discorda** **Concorda** **1 2 3 4 5 6 7**
25	Deveria existir um comprometimento com relação à segurança das informações dentro da unidade.	**Discorda** **Concorda** **1 2 3 4 5 6 7**
26	As instalações deveriam ser adequadas para fornecer um controle de acesso seguro as informações da unidade	**Discorda** **Concorda** **1 2 3 4 5 6 7**
27	Deveria existir treinamento ou conscientização para a segurança da informação.	**Discorda** **Concorda** **1 2 3 4 5 6 7**
28	Deveriam existir procedimentos para o descarte das informações em papel ou mídia.	Discorda Concorda 1 2 3 4 5 6 7

APÊNDICE D

Questionários de Percepção dos Níveis de Qualidade e Entendimento

Prezado Colaborador

O presente questionário é um dos componentes necessários a realização de um projeto voltado à segurança da informação. Todos os dados colhidos serão mantidos em sigilo de pesquisa, além do que os (as) participantes não serão nominalmente identificados, sendo preservado seu anonimato sob qualquer circunstância.

Obrigado por sua atenção.

1 Como você avalia o nível da qualidade da segurança da informação dentro da unidade?

Baixo						Alto
1	2	3	4	5	6	7

2 Como você avalia o seu nível de entendimento sobre o tema segurança da informação?

Baixo						Alto
1	2	3	4	5	6	7

APÊNDICE E

Formulário FMEA gerado na fase Medir

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas			
Projeto:	Gestão de Segurança da Informação	**Cliente: UCI e UTI - Hospital Universitário de Santa Maria**	
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira	Data do FMEA:	06 e 07 /2008
Data início Projeto:	03/2008	Data Conclusão Projeto:	12/2008

Item do Processo	Modo de Falha	Efeito	Causa	Controles Atuais	S	O	D	NPR
Suporte a segurança da informação	Ausência de suporte a segurança da informação.	Os problemas de segurança da informação passam a não ser reportados por não ter uma referência quando estes acontecem.	-Falta um Comitê gestor de Segurança da Informação para garantir um suporte de gestão visível dentro das unidades para com a Segurança da Informação	-	8	9	7	**504**
Projeto em segurança da informação	Falta de iniciativas que promovam a segurança da informação	Os usuários não tem comprometimento com a segurança da informação e os riscos.	Falta programas de conscientização em segurança da informação na unidade	-	8	9	7	**504**
Suporte de segurança da informação	Ausência de regras e normas em segurança da informação.	Violação dos princípios de segurança da informação (confiabilidade, integridade, disponibilidade)	Não existe um processo disciplinar formal para os funcionários que tenham violado as políticas e procedimentos de segurança organizacional, tal processo pode dissuadir outros.	-	8	9	7	**504**
Senhas fracas	Uso de Senhas fracas no Sistema UCI.	Facilidade em ocorrer acessos indevidos por outros usuários através de interceptação ou roubo.	Inexistência de controle de verificação de segurança nas senhas.	-	8	8	6	**384**
Termo de confidencialidade	Inexistência de termo de confidencialidade nas unidades	Falta de Comprometimento com a informação e os dados	Não é exigido um termo de confidencialidade na contratação de um novo profissional no acesso aos sistemas da instituição	-	6	9	7	**336**
Fichas de pacientes	Extravio de fichas de pacientes	Demora no atendimento ao paciente	Muitos profissionais manuseando a mesma informação. Falta de regras e/ou políticas na unidade	Existem escaninhos numerados com o leito para guardar as fichas do paciente	9	9	4	**324**

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas								
Projeto:	Gestão de Segurança da Informação		**Cliente: UCI e UTI - Hospital Universitário de Santa Maria**					
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira		Data do FMEA:	06 e 07 /2008				
Data início Projeto:	03/2008		Data Conclusão Projeto:	12/2008				
Item do Processo	Modo de Falha	Efeito	Causa	Controles Atuais	S	O	D	NPR
Monitoramento	Sem monitoramento e registro da auditoria	Impossibilidade de auditar os dados acompanhar as atividades do sistemas como, falhas, erros e deleções.	Não é gerado logs das atividades realizadas no sistema	-	6	7	7	**294**
Gestão de Ativos	As informações não são classificadas quanto as característica de proteção.	Violação do principio de confidencialidade.	Falta regras de classificação das informações (pública, privada, sigilosa).	-	7	7	6	**294**
Fichas de pacientes	Extravio de fichas de pacientes	Exposição de documentos confidenciais	Ausência de compartimentos e armários para o armazenamento dos documentos	-	9	9	3	**243**
Controle de Acesso	Todos os profissionais compartilham o mesmo usuário e senha na unidade	Qualquer pessoa pode ter acesso ao computador e consequentemente os arquivos contidos nele. Possibilidade nula de monitorar a rede ou de fazer auditoria por usuário.	-Falta de um gerenciamento de usuário e senha. -Políticas de usuário e senha. - Falta de identificação única do usuário	-	8	8	3	**192**
Suporte a segurança da informação	Ausência de suporte a segurança da informação.	Sem comunicação de falhas ou incidentes de segurança da informação	Inexistência de um canal de comunicação	-	7	6	4	**168**
e-mail	Inexistência de e-mail profissional nas unidades.	Informações do setor são enviadas por e-mail pessoal, ocasionando falta de segurança, imagem da unidade fica comprometida, impossibilidade de realizar auditoria.	Falta de políticas de uso de e-mails instituicionais.		6	9	3	**162**
Fichas de pacientes	Extravio de fichas de pacientes	Demora na transcrição de eventos atuais	Fichas de pacientes são colocadas em qualquer lugar.	-	6	8	3	**144**
Compartilhamento de pastas	Descontrole no compartilhamento de pastas.	Acesso facilitado a dados e informações	compartilhamento de pastas não são desfeitos assim que a informação necessária já foi a adquirida	-	6	6	4	**144**

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas			
Projeto:	Gestão de Segurança da Informação	**Cliente: UCI e UTI - Hospital Universitário de Santa Maria**	
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira	Data do FMEA:	06 e 07 /2008
Data início Projeto:	03/2008	Data Conclusão Projeto:	12/2008

Item do Processo	Modo de Falha	Efeito	Causa	Controles Atuais	S	O	D	NPR
Descarte de mídias	Sem procedimentos para o descarte de mídias.	Vazamento de informações, quebra de sigilo.	Falta de uma política para o descarte de mídias	-	7	4	5	**140**
Controle de acesso	Todos os profissionais compartilham o mesmo usuário e senha na unidade	Engenharia Social- tentativa de descoberta das informações da organização	Falta de uma política de usuários e senhas seguindo normas estipuladas pela organização.	-	8	8	2	**128**
Uso inadequado do sistema	Uso inadequado do Sistema Eletrônico de Pacientes	Erros operacionais, demora no cadastramento, baixa produtividade.	Inexistência de treinamento falta de capacidade de quem utiliza o sistema, inexistência de manual do usuário.	-	8	8	2	**128**
Atualização de usuários	Ausência de controles que definam a situação (ativo/inativo) dos funcionários	Funcionários demitidos ou afastados continuam tendo acesso a rede e consequentemente as informações.	Inexistência de regras de comunicação física ou eletrônica entre setor de Recursos humanos e Setor de informática para cancelamento de usuários demitidos ou afastados do hospital.	-	7	6	3	**126**
Ausência de bloqueio nas estações.	Ausência de bloqueio de estação	Estação de trabalho fica vulnerável sendo acessível por qualquer pessoa	Existem estações de trabalho que não possuem controle de login e senha para facilitar o acesso	-	7	5	3	**105**
Metodologias de Gestão	Os riscos não são gerenciados	Desperdício de tempo, ineficiência dos processos.	Não são adotadas metodologias de gestão e postura pro ativa		6	7	2	**84**
Extintores de Incêndio	Má localização dos extintores	A localização do extintores fica longe das estações de trabalho, o que pode dificultar o seu uso na ocorrência de incidentes.	Número insuficiente de extintores	Extintores no corredor	9	8	1	**72**
Acesso físico	Acesso facilitado nas unidades	Possibilidade de extravio e roubo de documentações de pacientes e acesso a informações sigilosas.	Pessoas muitas vezes sem o crachá de identificação tem acesso as unidades. No período da noite esse problema é maior, pois não tem recepcionista que bloqueie a entrada de pessoas não identificadas nas unidades.	Portaria central	9	7	1	**63**

APÊNDICE F

Formulário FMEA gerado na fase Analisar

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas			
Projeto:	Gestão de Segurança da Informação	Cliente:	**UCI e UTI - Hospital Universitário de Santa Maria**
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira	Data do FMEA:	**06 e 07 /2008**
Data início Projeto:	03/2008	Data Conclusão Projeto:	**12/2008**

Item do Processo	Modo de Falha	Efeito	Causa	Controles Atuais	S	O	D	**RPN**	Estratégia	Ações Recomendadas
Suporte a segurança da informação	Ausência de suporte a segurança da informação.	Os problemas de segurança da informação passam a não ser reportados ou não existe uma referência quando problemas acontecem.	-Falta um Comitê gestor de Segurança da Informação para garantir um suporte de gestão visível dentro das unidades para com a Segurança da Informação	-	8	9	7	**504**	Mitigar	Criação de um comitê Gestor de Segurança da Informação na organização
Projeto em segurança da informação	Falta de iniciativas que promovam a segurança da informação	Os usuários não tem comprometimento com a segurança da informação e os riscos.	Falta programas de conscientização em segurança da informação na unidade	-	8	9	7	**504**	Mitigar	Promover programas de Conscientização em Segurança da Informação
Suporte de segurança da informação	Ausência de regras e normas em segurança da informação.	Violação dos princípios de segurança da informação (confiabilidade, integridade, disponibilidade)	Não existe um processo disciplinar formal para os funcionários que tenham violado as políticas e procedimentos de segurança organizacional, tal processo pode dissuadir outros.	-	8	9	7	**504**	Mitigar	Estabelecer no documento da PSI processos disciplinares para violações dos princípios da Segurança da Informação

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas			
Projeto:	Gestão de Segurança da Informação	Cliente:	**UCI e UTI - Hospital Universitário de Santa Maria**
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira	Data do FMEA:	**06 e 07 /2008**
Data início Projeto:	03/2008	Data Conclusão Projeto:	**12/2008**

Item do Processo	Modo de Falha	Efeito	Causa	Controles Atuais	S	O	D	**RPN**	Estratégia	Ações Recomendadas
Senhas fracas	Uso de Senhas fracas no Sistema UCI.	Facilidade em ocorrer acessos indevidos por outros usuários através de interceptação ou roubo.	Inexistência de controle de verificação de segurança nas senhas.	-	8	8	6	**384**	Mitigar	Estabelecer uma política de controles de senhas
Termo de confidencialidade	Inexistência de termo de confidencialidade nas unidades	Falta de Comprometimento com a informação e os dados	Não é exigido um termo de confidencialidade na contratação de um novo profissional no acesso aos sistemas da instituição	-	6	9	7	**336**	Mitigar	Criação de termo de Confidencialidade nas unidades.
Fichas de pacientes	Extravio de fichas de pacientes	Demora no atendimento ao paciente	Muitos profissionais manuseando a mesma informação. Falta de regras e/ou políticas na unidade	Existem escaninhos numerados com o leito para guardar as fichas do paciente	9	9	4	**324**	Mitigar	Criação da Política de Segurança da Informação nas Unidades que estabeleça normas de acesso as informações.
Monitoramento	Sem monitoramento e registro da auditoria	Impossibilidade de auditar os dados acompanhar as atividades do sistemas como, falhas, erros e deleções.	Não é gerado logs das atividades realizadas no sistema	-	6	7	7	**294**		Registros de logs de cada operação.
Gestão de Ativos	As informações não são classificadas quanto as característica de proteção.	Violação do principio de confidencialidade.	Falta regras de classificação das informações (pública, privada, sigilosa).	-	7	7	6	**294**	Mitigar	Estabelecer a classificação das informações nas unidades e a utilização de rótulos em relatórios gerados pelo sistema conforme a classificação da informação

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas			
Projeto:	Gestão de Segurança da Informação	Cliente:	**UCI e UTI - Hospital Universitário de Santa Maria**
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira	Data do FMEA:	**06 e 07 /2008**
Data início Projeto:	03/2008	Data Conclusão Projeto:	**12/2008**

Item do Processo	Modo de Falha	Efeito	Causa	Controles Atuais	S	O	D	**RPN**	Estratégia	Ações Recomendadas
Fichas de pacientes	Extravio de fichas de pacientes	Exposição de documentos confidenciais	Ausência de compartimentos e armários para o armazenamento dos documentos	-	9	9	3	**243**		
Controle de Acesso	Todos os profissionais compartilham o mesmo usuário e senha na unidade	Qualquer pessoa pode ter acesso ao computador e consequentemente os arquivos contidos nele. Possibilidade nula de monitorar a rede ou de fazer auditoria por usuário.	-Falta de um gerenciamento de usuário e senha. -Políticas de usuário e senha. - Falta de identificação única do usuário	-	8	8	3	**192**	Mitigar	Política de usuário e senhas nas unidades
Suporte a segurança da informação	Ausência de suporte a segurança da informação.	Sem comunicação de falhas ou incidentes de segurança da informação	Inexistência de um canal de comunicação	-	7	6	4	**168**	Mitigar	Criação de um canal de comunicação para reporte de incidentes
e-mail	Inexistência de e-mail profissional nas unidades.	Informações do setor são enviadas por e-mail pessoal, ocasionando falta de segurança, imagem da unidade fica comprometida, impossibilidade de realizar auditoria.	Falta de políticas de uso de e-mails institucionais.		6	9	3	**162**	Mitigar	Recomendar o uso de e-mails com o domínio da Instituição e estabelecer regras e políticas para o seu uso

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas			
Projeto:	Gestão de Segurança da Informação	Cliente:	**UCI e UTI - Hospital Universitário de Santa Maria**
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira	Data do FMEA:	**06 e 07 /2008**
Data início Projeto:	03/2008	Data Conclusão Projeto:	**12/2008**

Item do Processo	Modo de Falha	Efeito	Causa	Controles Atuais	S	O	D	**RPN**	Estratégia	Ações Recomendadas
Fichas de pacientes	Extravio de fichas de pacientes	Demora na transcrição de eventos atuais	Fichas de pacientes são colocadas em qualquer lugar.	-	6	8	3	**144**		Implantar políticas e mensagens de alerta
Compartilhamento de pastas	Descontrole no compartilhamento de pastas.	Acesso facilitado a dados e informações	compartilhamento de pastas não são desfeitos assim que a informação necessária já foi a adquirida	-	6	6	4	**144**	Evitar	Recomendar e monitorar todo o compartilhamento criado na rede
Descarte de mídias	Sem procedimentos para o descarte de mídias.	Vazamento de informações, quebra de sigilo.	Falta de uma política para o descarte de mídias	-	7	4	5	**140**	Mitigar	Estabelecer na Política de procedimentos para o descarte de informações
Controle de acesso	Todos os profissionais compartilham o mesmo usuário e senha na unidade	Engenharia Social- tentativa de descoberta das informações da organização	Falta de uma política de usuários e senhas seguindo normas estipuladas pela organização.	-	8	8	2	**128**	Mitigar	Política de usuário e senhas nas unidades e programas de conscientização
Uso inadequado do sistema	Uso inadequado do Sistema Eletrônico de Pacientes	Erros operacionais, demora no cadastramento, baixa produtividade.	Inexistência de treinamento falta de capacidade de quem utiliza o sistema, inexistência de manual do usuário.	-	8	8	2	**128**	Mitigar	Implementação de manual de usuário.
Atualização de usuários	Ausência de controles que definam a situação (ativo/inativo) dos funcionários	Funcionários demitidos ou afastados continuam tendo acesso a rede e consequentemente as informações.	Inexistência de regras de comunicação física ou eletrônica entre setor de Recursos humanos e Setor de informática para cancelamento de usuários demitidos ou afastados do hospital.	-	7	6	3	**126**	Transferir	Recursos Humanos do HUSM deve gerar listas atualizadas de colaboradores afastados e demitidos

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas			
Projeto:	Gestão de Segurança da Informação	Cliente:	**UCI e UTI - Hospital Universitário de Santa Maria**
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira	Data do FMEA:	**06 e 07 /2008**
Data início Projeto:	03/2008	Data Conclusão Projeto:	**12/2008**

Item do Processo	Modo de Falha	Efeito	Causa	Controles Atuais	S	O	D	**RPN**	Estratégia	Ações Recomendadas
Ausência de bloqueio nas estações.	Ausência de bloqueio de estação	Estação de trabalho fica vulnerável sendo acessível por qualquer pessoa	Existem estações de trabalho que não possuem controle de login e senha para facilitar o acesso	-	7	5	3	**105**	Transferir	Criar bloqueios em todas as estações das unidades.
Metodologias de Gestão	Os riscos não são gerenciados	Desperdício de tempo, ineficiência dos processos.	Não são adotadas metodologias de gestão e postura pro ativa		6	7	2	**84**	Transferir	Adoção do FMEA como ferramenta de gerenciamento dos riscos, estimulando para uma cultura proativa
Extintores de Incêndio	Má localização dos extintores	A localização dos extintores fica longe das estações de trabalho, o que pode dificultar o seu uso na ocorrência de incidentes.	Número insuficiente de extintores	Extintores no corredor	9	8	1	**72**	Transferir	Recomendar a direção que seja realocados alguns extintores e providenciado a compra de outros.
Acesso físico	Acesso facilitado nas unidades	Possibilidade de extravio e roubo de documentações de pacientes e acesso a informações sigilosas.	Pessoas muitas vezes sem o crachá de identificação tem acesso as unidades. No período da noite esse problema é maior, pois não tem recepcionista que bloqueie a entrada de pessoas não identificadas nas unidades.	Portaria central	9	7	1	**63**	Transferir	Porta principal de acesso a unidade ser aberta somente pelo lado interno, principalmente no turno da noite

APÊNDICE G

Criação do Comitê Gestor de Segurança da informação

Termo de Criação do Comitê Gestor de Segurança da Informação

Este termo visa estabelecer a criação do Comitê Gestor de Segurança da Informação no Hospital Universitário de Santa Maria (HUSM) dos quais seus membros irão atuar na implantação da Gestão de Segurança da Informação na Unidade de Terapia Intensiva (UTI-Adulto) e Unidade de Cardiologia Intensiva (UCI). As responsabilidades do Comitê incluem:

I. Aprovação das políticas, normas e procedimentos de segurança da informação;
II. Designar, alterar ou definir responsabilidades da área de segurança da informação;
III. Aprovação de novos controles de segurança a serem criados com o objetivo de melhoria contínua das medidas de proteção;
IV. Prover suporte às iniciativas da área da Segurança da Informação;
V. Apoiar à implantação de soluções para minimizar os riscos como também a programas de conscientização para o fortalecimento de uma cultura organizacional voltada a segurança;

E assim assinam o presente termo os respectivos componentes do Comitê de Gestão de Segurança da Informação.

Direção Clínica - HUSM

Chefe da Cardiologia - HUSM

Chefe UCI- HUSM

Secretaria Geral e Ouvidoria do HUSM

Chefe da Enfermagem UCI e UTI

Chefe do Serviço de Informática

Direção de Ensino Pesquisa e Extensão

De acordo da Direção Geral do HUSM

Santa Maria, 06 de Setembro de 2008

APÊNDICE H

Avaliação do Programa de Conscientização em Segurança da Informação realizada na fase Controlar

Avaliação – Programa de Conscientização em Segurança da Informação

Data: _____/_____/_____

Marque as opções de acordo com a sua opinião em relação ao programa.

1. Avaliação do Programa de conscientização:

☐ Muito Bom
☐ Bom
☐ Regular
☐ Ruim
☐ Muito Ruim

2. Avaliação do conteúdo e conceitos apresentados no Programa de Conscientização.

☐ Muito Bom
☐ Bom
☐ Regular
☐ Ruim
☐ Muito Ruim

Outras Considerações:

_____
_____
_____
_____
_____

APÊNDICE I

Política de Segurança da Informação
(Primeira Versão)

Instituição
Hospital Universitário de Santa Maria – HUSM
Setores
Unidade de Cardiologia Intensiva (UCI) Unidade de Terapia Intensiva - Adulto (UTI)

Apresentação
O HUSM acredita que a continuidade do seu negócio decididamente depende de uma Gestão de Segurança da Informação baseada no princípio de integração dos esforços de suas diversas áreas. O objetivo desta Política de Segurança da Informação (PSI) é fazer com que o uso da informação da instituição aconteça de forma estruturada, possibilitando que tanto a assistência a saúde quanto a pesquisa não sejam prejudicadas pelo mau uso da informação. Proteger a informação é uma responsabilidade de todos.

Autores: Equipe de Gestão de Segurança da Informação

Comitê Gestor de Segurança da Informação (CGSI)

Versão: 1.0

Efetivação: Setembro 2008

Revisão
O conteúdo desta política deve ser constantemente atualizado com intervalos máximos de 6 (seis) meses, refletindo a dinâmica dos processos envolvidos, procurando sempre se adequar as mudanças técnicas e de infra-estrutura da instituição.

Introdução

O uso da Informação nas instituições de saúde necessita estar permanentemente protegida contra acessos indevidos e alterações. Como o cenário atual demonstra uma constante tentativa de exploração maliciosa destas informações torna-se imprescindível o zelo pela segurança, evitando as vulnerabilidades que dão margem a invasões, que resultam na perda da confidencialidade, integridade e disponibilidade das informações.

Evidencia-se, portanto, a necessidade da implantação de uma Política de Segurança da Informação - PSI que defina normas, procedimentos e requisitos mínimos, nos diversos aspectos que envolvem, direta e indiretamente, o acervo de informações, salvaguardando a sua exatidão, independentemente de onde e como estejam armazenadas.

Objetivo da segurança da informação é alcançar e manter níveis adequados de:

Confidencialidade - a informação somente deve estar acessível a usuários autorizados;
Disponibilidade - informação deve disponível e acessível por usuários autorizados quando solicitadas;
Integridade – a informação deve ser correta, verdadeira e não estar corrompida.

Dentre os benefícios proporcionados pela Política de Segurança da Informação (PSI) pode se mencionar:

- Proteger a qualidade da informação, especialmente as que servem de base para tomada de decisões;
- Os custos decorrentes de eventos que possam causar perigo as informações são reduzidos através da prevenção de incidentes;
- Garantir a boa reputação da instituição sob os olhos do público interno e externo;
- Garantir a continuidade dos processos de trabalho da instituição dependentes da informação.

Comitê Gestor de Segurança da Informação

O Comitê Gestor de Segurança da Informação (CGSI) tem caráter participativo de trabalho sendo composto por membros de diversas especialidades podendo sofrer alterações em sua composição conforme a necessidade da instituição. Formam o Comitê de Segurança da informação os seguintes membros:

- Direção Clínica – HUSM
- Chefe da Cardiologia - HUSM
- Chefe da UCI - HUSM
- Chefe Secretaria Geral e Ouvidoria – HUSM
- Chefe da Enfermagem UCI e UTI - HUSM
- Chefe do Serviço de Informática - HUSM
- Direção de Ensino Pesquisa e Extensão

DEFINIÇÕES GERAIS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Da divulgação

NORMAS

De propriedade

De documentos em papeis (prontuários, fichas de pacientes, resultados de exames)

De uso de dispositivos móveis

De descarte de informações

De segurança física

De Acesso à Internet

De uso do Correio Eletrônico

De contas e senhas para usuários

RESPONSABILIDADES

Dos usuários

Comitê de Segurança da Informação

Sanções

APÊNDICE J

Avaliação da Política de Segurança da Informação realizada na fase Controlar

Avaliação – Política de Segurança da Informação

Data: _____/_____/_____ **Unidade:** ( ) UCI ( ) UTI

Avaliadores: ( ) Implementadores
( ) Diretoria
( ) Funcionários

Instruções para Avaliação:
Marque **NE** para procedimentos **Não** executados
Marque **PE** para procedimentos **Parcialmente** executados
Marque **TE** para procedimentos **Totalmente** executados

AMBIENTE CONVENCIONAL	**NE**	**PE**	**TE**
Exposição de documentos em locais inadequados			
Organização e armazenamento de documentos de acordo com o leito do paciente			
Exposição de documentos na impressora			
Descarte adequado de informações			
Sigilo de informações confidenciais			
Acesso de profissionais identificados nas unidades			
Notificação de incidentes			
AMBIENTE COMPUTACIONAL	**NE**	**PE**	**TE**
Uso de e-mail profissional			
Utilização da internet para fins profissionais			
Não compartilhamento de senhas			
Uso de senhas fortes			
Bloqueio do PC			
Descarte correto de informações			
Backup de informações importantes			
Utilização de antivírus			

Observações:
_____
_____
_____

APÊNDICE L

Política de Segurança da Informação
(Segunda Versão)

Instituição
Hospital Universitário de Santa Maria – HUSM
Setores
Unidade de Cardiologia Intensiva(UCI) Unidade de Terapia Intensiva - Adulto (UTI)

Apresentação
O HUSM acredita que a continuidade do seu negócio decididamente depende de uma Gestão de Segurança da Informação baseada no princípio de integração dos esforços de suas diversas áreas. O objetivo desta Política de Segurança da Informação (PSI) é fazer com que o uso da informação da instituição aconteça de forma estruturada, possibilitando que tanto a assistência a saúde quanto a pesquisa não sejam prejudicadas pelo mau uso da informação. Proteger a informação é uma responsabilidade de todos.

Autores: Equipe de Gestão de Segurança da Informação

Comitê Gestor de Segurança da Informação (CGSI)

Versão: 1.1

Reporte de Incidentes
Qualquer suspeita de incidência de segurança da informação deve ser reportado imediatamente ao Comitê Gestor de Segurança da Informação podendo ser feitos anonimamente para: E-mail: gsi_husm@smail.ufsm.br Página: http://www.husm.ufsm.br **Link: GSI**

Introdução

O uso da Informação nas instituições de saúde necessita estar permanentemente protegida contra acessos indevidos e alterações. Como o cenário atual demonstra uma constante tentativa de exploração maliciosa destas informações torna-se imprescindível o zelo pela segurança, evitando as vulnerabilidades que dão margem a invasões, que resultam na perda da confidencialidade, integridade e disponibilidade das informações.

Evidencia-se, portanto, a necessidade da implantação de uma Política de Segurança da Informação - PSI que defina normas, procedimentos e requisitos mínimos, nos diversos aspectos que envolvem, direta e indiretamente, o acervo de informações, salvaguardando a sua exatidão, independentemente de onde e como estejam armazenadas.

Objetivo da segurança da informação é alcançar e manter níveis adequados de:

Confidencialidade - a informação somente deve estar acessível a usuários autorizados;
Disponibilidade - informação deve disponível e acessível por usuários autorizados quando solicitadas;
Integridade – a informação deve ser correta, verdadeira e não estar corrompida.

Dentre os benefícios proporcionados pela Política de Segurança da Informação (PSI) pode se mencionar:

- Proteger a qualidade da informação, especialmente as que servem de base para tomada de decisões;
- Os custos decorrentes de eventos que possam causar perigo as informações são reduzidos através da prevenção de incidentes;
- Garantir a boa reputação da instituição sob os olhos do público interno e externo;
- Garantir a continuidade dos processos de trabalho da instituição dependentes da informação.

Comitê Gestor de Segurança da Informação

O Comitê Gestor de Segurança da Informação (CGSI) tem caráter participativo de trabalho sendo composto por membros de diversas especialidades podendo sofrer alterações em sua composição conforme a necessidade da instituição. Formam o Comitê de Segurança da informação as seguintes áreas: Direção Clínica (01), Chefe da Cardiologia (01), Chefe da UCI (01), Chefe Secretaria Geral e Ouvidoria(01), Chefe da Enfermagem UCI e UTI (01), Chefe do Serviço de Informática (01), Direção de Ensino Pesquisa e Extensão (01).

RESPONSABILIDADES

Dos usuários

1. Respeitar e cumprir as determinações desta política de segurança da informação. O não cumprimento das normas implica em sanções a ser aplicado pelo Comitê Gestor de Segurança da Informação.
2. Proteger os recursos de informação que estão sob sua responsabilidade;
3. Zelar pela manutenção das informações bem como pela preservação da confidencialidade, integridade e disponibilidade das mesmas;
4. Comprometer-se com as informações a que tem acesso devendo mantê-la segura.
5. Manter sigilo de informações críticas presentes nas unidades, dentre as quais se destacam aquelas que dizem respeito diretamente a saúde de pacientes, não as divulgando sem consentimento prévio;
6. Responsabilizar-se pela realização de backups (cópias) dos dados necessários ao desempenho de suas atividades;
7. Evitar colocar dados importantes em pastas compartilhadas, pois esta prática pode ocasionar problemas de confidencialidade à informação;
8. Manter um login e senha de acesso individual aos sistemas de informação do HUSM não sendo permitido o seu compartilhamento com outros usuários. A identificação unívoca é a prova de que todas as ações que foram feitas partiram deste usuário, e não de outros que se dizem ser ele. Podemos considerar a senha uma ferramenta que evita que, em muitos casos, um problema no sistema inteiro venha a ser causado por uma falha humana. Entre outras coisas, evita que usuários tenham acesso a informações não convenientes a eles e garante a informação certa a cada um dos mesmos.
9. Usuários não devem alterar informações que não estão sob sua responsabilidade. Em alguns casos, a boa vontade pode ser danosa, pois todos estamos sujeitos a cometer erros e alterar informações preciosas mesmo que não se tenha a intenção de fazê-lo.
10. Responsabilizar-se individualmente pelos recursos institucionais (tecnológicos ou não) disponíveis para a realização de suas atividades.
11. Ao deixar o local de trabalho em que se faça uso de computador o usuário deve fazer a ativação de proteção de tela/bloqueio do teclado como forma de proteger a entrada e saída dos dados das unidades.
12. A manipulação irregular, divulgação ou uso indevido da informação e dos recursos computacionais da UCI e UTI não é permitida.
13. Nenhum usuário pode monitorar o tráfego da rede ou simular algum dispositivo da rede, sem a devida autorização do Serviço de informática.
14. Ao encaminhar informações sigilosas para outros setores, salientar a importância da confidencialidade dos dados quanto ao seu transporte.
15. Usuários que se desligarem, entrarem em licença ou de férias das unidades e que tenham acesso aos sistemas da instituição devem solicitar o bloqueio de seu login de senha.
16. Informar a algum membro do Comitê Gestor de Segurança da Informação imediatamente qualquer violação das normas estabelecidas incluindo as não intencionais e culposas.

Gestão de Segurança da Informação
Hospital Universitário
UFSM

Termo de Confidencialidade e de Responsabilidade da Política de Segurança da Informação da Unidade de Cardiologia Intensiva (UCI) e Unidade de Terapia Intensiva (UTI)

Eu,_____declaro, nesta data, ter plena ciência e concordância com todos os termos estabelecidos por este Termo de Confidencialidade e de Responsabilidade, comprometo-me a:

1. Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança.
2. Utilizar adequadamente os equipamentos da Instituição, evitando acessos indevidos aos ambientes computacionais aos que estou habilitado, que possam comprometer a segurança das informações.
3. Não revelar fora do âmbito profissional, fato ou informações de qualquer natureza que tenha conhecimento devido a minhas atribuições, salvo em decorrência de decisão competente do superior hierárquico.
4. Acessar as informações somente por necessidade de serviço.
5. Manter cautela quando a exibição de informações sigilosas e confidenciais em meio físico, em tela, impressoras ou outras formas eletrônicas.
6. Utilizar o recurso de Correio Eletrônico somente para fins profissionais.
7. Não me ausentar do local de trabalho sem encerrar a sessão de uso do computador ou sistema, evitando assim o acesso por pessoas não autorizadas.
8. Não divulgar a minha senha de acesso aos sistemas do HUSM a outras pessoas;
9. De maneira alguma ou sobre qualquer pretexto, procurar descobrir as senhas de outras pessoas;
10. Solicitar o cancelamento de minha senha quando não for mais de minha utilização e o bloqueio ao entrar em férias e licenciar-me.
11. Somente utilizar o meu acesso para os fins designados e para os quais estiver devidamente autorizado, em razão de minhas funções;
12. Reportar imediatamente ao superior imediato ou ao Comitê de Segurança da Informação em caso de violação, acidental ou não, da minha senha, e providenciar a sua substituição.
13. Estou ciente de que todas as ações realizadas na UCI e UTI são passives de monitoração.

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação das sansões disciplinares cabíveis.

Santa Maria, _____ de _____ de 2008.

_____
Assinatura

APÊNDICE – Referências para outras políticas e padrões

As seguintes políticas e circulares devem ser lidas em conjunto com a Política de Segurança da Informação para completar a cobertura de todos os tópicos, onde podem ser aplicados:

Políticas:

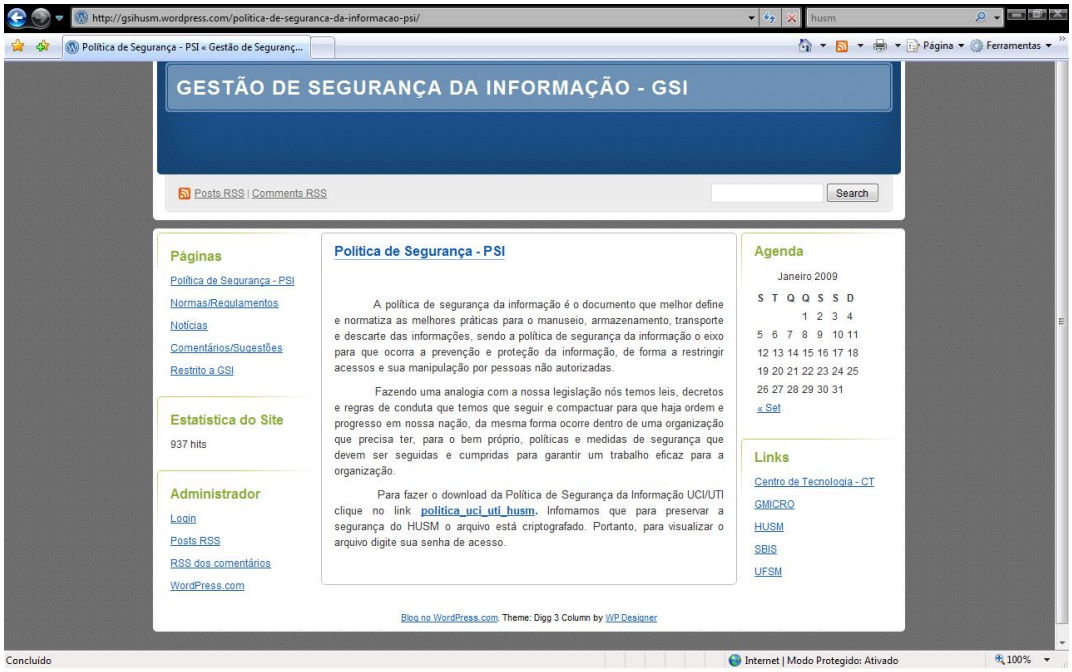
1.	Disposições Gerais	PDG (01)	Pág 06
2.	Uso Aceitável	PUA (01)	Pág 07
3.	Internet e Correio Eletrônico	PIC (01)	Pág 08
4.	Controle Lógico	PCL (01)	Pág 09
5.	Controle Físico	PCF (01)	Pág 10
6.	Classificação da Informação	PCI (01)	Pág 11

Padrões:

1.	Circular n°11-2008-DEPE/HUSM de 04 de Julho de 2008 DEPE	P01	Pág 12
2.	Ordem para a montagem de prontuários	P02	Pág 13
3.	Norma de Segurança Interna do HUSM	P03	Pág 14

APÊNDICE M

Site da Gestão da Segurança da Informação


http://gsihusm.wordpress.com/politica-de-seguranca-da-informacao-psi/
husm
Política de Segurança - PSI « Gestão de Segurança...
Página
Ferramentas
GESTÃO DE SEGURANÇA DA INFORMAÇÃO - GSI
Posts RSS | Comments RSS
Search
Páginas
Política de Segurança - PSI
Normas/Regulamentos
Notícias
Comentários/Sugestões
Restrito a GSI
Estatística do Site
937 hits
Administrador
Login
Posts RSS
RSS dos comentários
WordPress.com
Política de Segurança - PSI
A política de segurança da informação é o documento que melhor define e normatiza as melhores práticas para o manuseio, armazenamento, transporte e descarte das informações, sendo a política de segurança da informação o eixo para que ocorra a prevenção e proteção da informação, de forma a restringir acessos e sua manipulação por pessoas não autorizadas.
Fazendo uma analogia com a nossa legislação nós temos leis, decretos e regras de conduta que temos que seguir e compactuar para que haja ordem e progresso em nossa nação, da mesma forma ocorre dentro de uma organização que precisa ter, para o bem próprio, políticas e medidas de segurança que devem ser seguidas e cumpridas para garantir um trabalho eficaz para a organização.
Para fazer o download da Política de Segurança da Informação UCI/UTI clique no link política_uci_uti_husm. Informamos que para preservar a segurança do HUSM o arquivo está criptografado. Portanto, para visualizar o arquivo digite sua senha de acesso.
Agenda
Janeiro 2009
S T Q Q S S D
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31
« Set
Links
Centro de Tecnologia - CT
GMICRO
HUSM
SBIS
UFSM
Blog no WordPress.com. Theme: Digg 3 Column by WP Designer
Concluído
Internet | Modo Protegido: Ativado
100%

APÊNDICE N

Formulário FMEA gerado na fase Controlar

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas			
Projeto:	Gestão de Segurança da Informação	Cliente:	**UCI e UTI - Hospital Universitário de Santa Maria**
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira	Data do FMEA:	**06 e 07 /2008 Reavaliação - 12/2008**
	03/2008	Data Conclusão Projeto:	**12/2008**

Item do Processo	Modo de Falha	Efeito	Causa	Cont. Atuais	S	O	D	**RPN**	Estratégia	Ações Recomendadas	S	O	D	**RPN**
Suporte a segurança da informação	Ausência de suporte a segurança da informação.	Os problemas de segurança da informação passam a não ser reportados ou não existe uma referência quando problemas acontecem.	-Falta um Comitê gestor de Segurança da Informação para garantir um suporte de gestão visível dentro das unidades para com a Segurança da Informação	-	8	9	7	**504**	Mitigar	Criação de um comitê Gestor de Segurança da Informação na organização	8	7	3	**168**
Projeto em segurança da informação	Falta de iniciativas que promovam a segurança da informação	Os usuários não tem comprometimento com a segurança da informação e os riscos.	Falta programas de conscientização em segurança da informação na unidade	-	8	9	7	**504**	Mitigar	Promover programas de Conscientização em Segurança da Informação	8	8	3	**192**
Suporte de segurança da informação	Ausência de regras e normas em segurança da informação.	Violação dos princípios de segurança da informação (confiabilidade, integridade, disponibilidade)	Não existe um processo disciplinar formal para os funcionários que tenham violado as políticas e procedimentos de segurança organizacional,	-	8	9	7	**504**	Mitigar	Estabelecer no documento da PSI processos disciplinares para violações dos princípios da Segurança da Informação	8	8	6	**384**

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas														
Projeto:	Gestão de Segurança da Informação			Cliente:	**UCI e UTI - Hospital Universitário de Santa Maria**									
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira			Data do FMEA:	**06 e 07 /2008 Reavaliação - 12/2008**									
	03/2008			Data Conclusão Projeto:	**12/2008**									
Item do Processo	Modo de Falha	Efeito	Causa	Cont. Atuais	S	O	D	**RPN**	Estratégia	Ações Recomendadas	S	O	D	**RPN**
			tal processo pode dissuadir outros.											
Senhas fracas	Uso de Senhas fracas no Sistema UCI.	Facilidade em ocorrer acessos indevidos por outros usuários através de interceptação ou roubo.	Inexistência de controle de verificação de segurança nas senhas.	-	8	8	6	**384**	Mitigar	Estabelecer uma política de controles de senhas	8	6	1	**48**
Termo de confidencialidade	Inexistência de termo de confidencialidade nas unidades	Falta de Comprometimento com a informação e os dados	Não é exigido um termo de confidencialidade na contratação de um novo profissional no acesso aos sistemas da instituição	-	6	9	7	**336**	Mitigar	Criação de termo de Confidencialidade nas unidades.	6	3	3	**54**
Fichas de pacientes	Extravio de fichas de pacientes	Demora no atendimento ao paciente	Muitos profissionais manuseando a mesma informação. Falta de regras e/ou políticas na unidade	Existem escaninhos numerados com o leito para guardar as fichas do paciente	9	9	4	**324**	Mitigar	Criação da Política de Segurança da Informação nas Unidades que estabeleça normas de acesso as informações.	9	8	2	**216**
Monitoramento	Sem monitoramento e registro da auditoria	Impossibilidade de auditar os dados acompanhar as atividades do sistemas como, falhas, erros e deleções.	Não é gerado logs das atividades realizadas no sistema	-	6	7	7	**294**	Mitigar	Registros de logs de cada operação.	6	2	2	**24**

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas			
Projeto:	Gestão de Segurança da Informação	Cliente:	**UCI e UTI - Hospital Universitário de Santa Maria**
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira	Data do FMEA:	**06 e 07 /2008 Reavaliação - 12/2008**
	03/2008	Data Conclusão Projeto:	**12/2008**

Item do Processo	Modo de Falha	Efeito	Causa	Cont. Atuais	S	O	D	**RPN**	Estratégia	Ações Recomendadas	S	O	D	**RPN**
Gestão de Ativos	As informações não são classificadas quanto as característica de proteção.	Violação do principio de confidencialidade.	Falta regras de classificação das informações (pública, privada, sigilosa).	-	7	7	6	**294**	Mitigar	Estabelecer a classificação das informações nas unidades e a utilização de rótulos em relatórios gerados pelo sistema conforme a classificação da informação	7	2	2	**28**
Fichas de pacientes	Extravio de fichas de pacientes	Exposição de documentos confidenciais	Ausência de compartimentos e armários para o armazenamento dos documentos	-	9	9	3	**243**			9	5	3	**135**
Controle de Acesso	Todos os profissionais compartilham o mesmo usuário e senha na unidade	Qualquer pessoa pode ter acesso ao computador e consequentemente os arquivos contidos nele. Possibilidade nula de monitorar a rede ou de fazer auditoria por usuário.	-Falta de um gerenciamento de usuário e senha. -Políticas de usuário e senha. - Falta de identificação única do usuário	-	8	8	3	**192**	Mitigar	Política de usuário e senhas nas unidades	8	5	3	**120**
Suporte a segurança da informação	Ausência de suporte a segurança da informação.	Sem comunicação de falhas ou incidentes de segurança da informação	Inexistência de um canal de comunicação	-	7	6	4	**168**	Mitigar	Criação de um canal de comunicação para reporte de incidentes	7	4	2	**56**
e-mail	Inexistência de e-mail profissional nas unidades.	Informações do setor são enviadas por e-mail pessoal, ocasionando falta de segurança,	Falta de políticas de uso de e-mails institucionais.		6	9	3	**162**	Mitigar	Recomendar o uso de e-mails com o domínio da Instituição e	6	4	2	**48**

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas			
Projeto:	Gestão de Segurança da Informação	Cliente:	**UCI e UTI - Hospital Universitário de Santa Maria**
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira	Data do FMEA:	**06 e 07 /2008 Reavaliação - 12/2008**
	03/2008	Data Conclusão Projeto:	**12/2008**

Item do Processo	Modo de Falha	Efeito	Causa	Cont. Atuais	S	O	D	**RPN**	Estratégia	Ações Recomendadas	S	O	D	**RPN**
		imagem da unidade fica comprometida, impossibilidade de realizar auditoria.								estabelecer regras e políticas para o seu uso				
Fichas de pacientes	Extravio de fichas de pacientes	Demora na transcrição de eventos atuais	Fichas de pacientes são colocadas em qualquer lugar.	-	6	8	3	**144**		Implantar políticas e mensagens de alerta	6	7	2	**84**
Compartilhamento de pastas	Descontrole no compartilhamento de pastas.	Acesso facilitado a dados e informações	compartilhamento de pastas não são desfeitos assim que a informação necessária já foi a adquirida	-	6	6	4	**144**	Evitar	Recomendar e monitorar todo o compartilhamento criado na rede	6	2	2	**24**
Descarte de mídias	Sem procedimentos para o descarte de mídias.	Vazamento de informações, quebra de sigilo.	Falta de uma política para o descarte de mídias	-	7	4	5	**140**	Mitigar	Estabelecer na Política de procedimentos para o descarte de informações	7	3	3	**63**
Controle de acesso	Todos os profissionais compartilham o mesmo usuário e senha na unidade	Engenharia Social-tentativa de descoberta das informações da organização	Falta de uma política de usuários e senhas seguindo normas estipuladas pela organização.	-	8	8	2	**128**	Mitigar	Criação de um domínio de cada unidade para fazer o gerenciamento dos usuários.	8	8	2	**128**
Uso inadequado do sistema	Uso inadequado do Sistema Eletrônico de Pacientes	Erros operacionais, demora no cadastramento, baixa produtividade.	Inexistência de treinamento falta de capacidade de quem utiliza o sistema, inexistência de manual do usuário.	-	8	8	2	**128**	Mitigar	Implementação de manual de usuário.	8	4	2	**64**

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas			
Projeto:	Gestão de Segurança da Informação	Cliente:	**UCI e UTI - Hospital Universitário de Santa Maria**
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira	Data do FMEA:	**06 e 07 /2008 Reavaliação - 12/2008**
	03/2008	Data Conclusão Projeto:	**12/2008**

Item do Processo	Modo de Falha	Efeito	Causa	Cont. Atuais	S	O	D	**RPN**	Estratégia	Ações Recomendadas	S	O	D	**RPN**
Atualização de usuários	Ausência de controles que definam a situação (ativo/inativo) dos funcionários	Funcionários demitidos ou afastados continuam tendo acesso a rede e consequentemente as informações.	Inexistência de regras de comunicação física ou eletrônica entre setor de Recursos humanos e Setor de informática para cancelamento de usuários demitidos ou afastados do hospital.	-	7	6	3	**126**	Transferir	Recursos Humanos do HUSM deve gerar listas atualizadas de colaboradores afastados e demitidos	7	4	2	**56**
Ausência de bloqueio nas estações.	Ausência de bloqueio de estação	Estação de trabalho fica vulnerável sendo acessível por qualquer pessoa	Existem estações de trabalho que não possuem controle de login e senha.	-	7	5	3	**105**	Transferir	Criar bloqueios em todas as estações das unidades.	7	3	2	**42**
Metodologias de Gestão	Os riscos não são gerenciados	Desperdício de tempo, ineficiência dos processos.	Não são adotadas metodologias de gestão e postura pro ativa		6	7	2	**84**	Transferir	Adoção do FMEA como ferramenta de gerenciamento dos riscos, estimulando para uma cultura proativa	6	5	2	**60**
Extintores de Incêndio	Má localização dos extintores	A localização dos extintores que existem fica longe das estações de trabalho, o que pode dificultar o seu uso	Número insuficiente de extintores	Extintores no corredor	9	8	1	**72**	Transferir	Recomendar a direção que seja realocados alguns extintores e providenciado a compra de outros.	9	8	1	**72**

FMEA – Análise dos Modos de Falhas e Efeitos das Falhas														
Projeto:	Gestão de Segurança da Informação			Cliente:				**UCI e UTI - Hospital Universitário de Santa Maria**						
Gerente do Projeto:	Maria Angélica Figueiredo Oliveira			Data do FMEA:				**06 e 07 /2008 Reavaliação - 12/2008**						
	03/2008			Data Conclusão Projeto:				**12/2008**						
Item do Processo	Modo de Falha	Efeito	Causa	Cont. Atuais	S	O	D	**RPN**	Estratégia	Ações Recomendadas	S	O	D	**RPN**
Acesso físico	Acesso facilitado nas unidades	Possibilidade de extravio e roubo de documentações de pacientes e acesso a informações sigilosas.	Pessoas muitas vezes sem o crachá de identificação tem acesso as unidades. No período da noite esse problema é maior, pois não tem recepcionista que bloqueie a entrada de pessoas não identificadas nas unidades.	Portaria central	9	7	1	**63**	Transferir	Porta principal de acesso a unidade ser aberta somente pelo lado interno, principalmente no turno da noite	9	7	1	**63**

APÊNDICE O

Folder de Divulgação dos Resultados

Projeto de Gestão da Segurança da Informação

Resultados Parciais

Equipe de Gestão da Segurança da Informação

Gestão da Segurança da Informação (GSI)

E um projeto que visa garantir a segurança da informação dentro da UCI e UTI, bem como divulgar as melhores práticas no estabelecimento e manutenção de controles a serem implantados nas respectivas unidades.

Benefícios

- Proporcionar aos usuários da UCI e UTI, uma **Gestão da Segurança da Informação** que venha assegurar a proteção da informação, através da implantação de políticas, mecanismos e medidas de segurança.
- Qualificar o hospital com elementos legal-jurídicos através da **Política de Segurança da Informação (PSI)** a fim de fortalecer o compromisso das unidades para com o cidadão, promovendo assim uma consciência ética de profundo respeito à privacidade e confiabilidade dos seus dados.
- Promover **programas de conscientização** a fim de incorporar uma cultura organizacional voltada à segurança da informação.

Até o momento algumas medidas de segurança já foram implantadas, dentre as quais se destacam:

- Mapeamentos dos Riscos da informação existentes nas unidades com o propósito de sua redução.
- Criação do Comitê Gestor de Segurança da informação, responsável por supervisionar, aprovar todas as ações, normas e procedimentos de segurança da informação.
- Criação e desenvolvimento do Programa de Conscientização e Treinamento em Segurança da Informação.
- Criação e estabelecimento da Política de Segurança da Informação.
- Criação e implantação de um canal de comunicação (site, e-mail) para o reporte de incidentes e sugestões para o projeto.

PROTEGER A INFORMAÇÃO É UMA RESPONSABILIDADE DE TODOS.

E-mail: gsi_husm@smail.ufsm.br
http://www.husm.ufsm.br
link: GSI