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

IMPACTO DA UTILIZAÇÃO DE TÉCNICAS DE ENDOMARKETING NA EFETIVIDADE DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Dissertação de Mestrado

Cristiane Ellwanger

Santa Maria, RS, Brasil

2009

IMPACTO DA UTILIZAÇÃO DE TÉCNICAS DE ENDOMARKETING NA EFETIVIDADE DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

por

Cristiane Ellwanger

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-Graduação em Engenharia de Produção, Área de Concentração 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 Antunes Ribas. Edifício Primavera, n.º 722, Apto. 402, Centro, Santo Ângelo RS, 98.801-63
Fone: (0xx) 55 99152183; Endereço eletrônico: cristianeellwanger@yahoo.com.br

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

IMPACTO DA UTILIZAÇÃO DE TÉCNICAS DE ENDOMARKETING NA EFETIVIDADE DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

elaborada por
Cristiane Ellwanger

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

COMISSÃO EXAMINADORA:

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

_____
Dr. Rudimar Antunes da Rocha - UFSC

_____
Dr. Sergio Nunes Pereira - UFSM

Santa Maria, 2009.

Agradecimentos

Ao **meu esposo e meu filho**, por me entenderem e me incentivarem a perseguir aquilo em que acredito, por mais que isso trouxesse sacrifícios e restrições ao nosso convívio e aos demais familiares, pelo apoio recebido e pela compreensão dos momentos em que abdiquei dos meus para atingir meu objetivo.

Ao meu orientador, **Prof. Dr. Raul Ceretta Nunes**, pelo seu profissionalismo, disponibilidade, auxílio e apoio a mim direcionado.

Ao **Prof. Dr. Rudimar Antunes da Rocha** que, mesmo distante, disponibilizou seu tempo, suas sugestões, seu incentivo, sua colaboração e sua paciência.

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, em especial a minha querida amiga e colega **Maria Angélica de Oliveira Figueiredo**, por contribuir para a concretização deste trabalho ao proporcionar debates e trocas de experiências e por compartilhar comigo todos os momentos, todas as dúvidas e todas as conquistas relacionadas a este trabalho e **demais colegas** que embora não tenham participado diretamente da realização deste trabalho me beneficiaram com sua simples presença.

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

Enfim, a todas as pessoas que direta ou indiretamente contribuição para a realização deste trabalho.

“A alegria não chega apenas no encontro do achado, mas faz parte do processo de busca. (Paulo Freire)”

RESUMO

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

O IMPACTO DA UTILIZAÇÃO DE TÉCNICAS DE ENDOMARKETING NA EFETIVIDADE DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

AUTOR: CRISTIANE ELLWANGER
ORIENTADOR: PROF. DR. RAUL CERETTA NUNES
Data e Local da Defesa: 12 de junho de 2009, Santa Maria

Proteger os recursos de informação tem sido um grande desafio às organizações. O estabelecimento de uma Política de Segurança da Informação (PSI) pode resolver parte dos problemas relacionados à segurança, mas não pode resolvê-los integralmente, pois os recursos humanos, presentes no ambiente interno das organizações, podem comprometer seriamente a efetividade de uma PSI. O endomarketig (marketing interno) é um instrumento que pode contribuir para se obter ou até mesmo resgatar o comprometimento dos usuários para com a PSI. A presente dissertação investiga o impacto da utilização de técnicas de endomarketing na efetividade da PSI, utilizando-se para tanto da pesquisa experimental. Realizado junto às Unidades de Cardiologia Intensiva (UCI) e Terapia Intensiva-Adulto (UTI) do Hospital Universitário de Santa Maria – HUSM, o experimento foi constituído de um grupo de experimentação (UCI), sob o qual foram aplicadas diferentes técnicas de endomarketing e um grupo de controle (UTI), o qual recebeu apenas um nivelamento inicial. Para constatar a efetividade da PSI foram realizadas auditorias internas, nas quais os procedimentos definidos na PSI foram testados e classificados como: Procedimentos Não-Executados (PNEs); Procedimentos Parcialmente Executados (PPEs) e Procedimentos Totalmente Executados (PTEs). Os resultados do experimento demonstram que tanto o grupo de controle (UTI) quanto o grupo de experimentação (UCI) aderiram à PSI após a aplicação inicial de técnicas de endomarketing (nivelamento). Entretanto, após descontinuar a aplicação dessas técnicas no grupo de controle, observou-se uma diminuição gradativa dos percentuais de PTE pelos componentes deste grupo, que caiu de 14,6% para 4,1%, o que demonstra uma queda de 71,92% na adesão à PSI neste grupo, se considerado os PTE. Já a aplicação continuada de técnicas de endomarketing no grupo de experimentação fez com que os procedimentos descritos na PSI estivessem sempre presentes na mente dos usuários, o que gerou um aumento gradativo nos percentuais de PTEs. O percentual subiu de 8,3% para 41,7%, o que reflete uma melhora de 402,4% na adesão à PSI neste grupo, se considerado os PTEs. Se considerado os procedimentos PNEs, a aplicação contínuada de técnicas de endomarketing no grupo de experimentação possibilitou uma redução de 88%, contra um aumento de 12,6% no grupo de controle, e uma alta concentração de percentuais nos procedimentos parcialmente ou totalmente executados, que somados chegam a 93,7% na avaliação final. Conclui-se então que a aplicação contínua de técnicas de endomarketing melhora a efetividade da PSI.

Palavras-chave: Política de Segurança da Informação, Endomarketing, Recursos Humanos, Segurança.

ABSTRACT

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

THE IMPACT OF THE INTERNAL MARKETING ON INFORMATION SECURITY POLICY EFECTIVENESS

AUTHOR: CRISTIANE ELLWANGER
ADVISOR: PROF. DR. RAUL CERETTA NUNES
Date and Local: June 12, 2009, Santa Maria

Protecting the information resources has been a big challenge to organizations. The constitution of an information security policy – PSI can solve part of problems related to security but it can't solve them completely, because of the human resources, present in the internal environment of organizations, they can seriously compromise the effectiveness of an PSI. Since the endomarketing (internal marketing) is an instrument that can contribute to obtain or even to rescue the users commitment with the PSI, this present dissertation shows impact of endomarketing techniques in the policy effectiveness using the experimental research. Performed in the Intensive Cardiology Unit (UCI) and Intensive Care Adult (UTI) at Santa Maria University Hospital – (HUSM), the experiment was constituted in an experimentation group (UCI), under the endomarketing directed different techniques and a control group (UTI) which it served as a basis to observation. In order to find the effectiveness of PSI on the referred units it was performed internal audits where the procedures, defined by the PSI were classified under the percentage way following the criteria: Non-Run Procedures (PNEs), Partially Implemented Procedures (PPEs) and Fully Implemented Procedures (PTEs).The experiment results show that both the control group as the experimentation group after the initial application of endomarketing techniques joined to implanted PSI on the respective units. However, after discontinuing the application of these techniques on the control group, it was observed a gradual decrease of percentages of PTEs by the components of this group that it decreased from 14,6% to 4,1% which it shows a decrease of 71,92% in the support to PSI in this group, if considered the PTEs. Already the continuous application of endomarketing techniques in the experimentation group did with that the procedures described in PSI were always presents in the users' mind, what generated a gradual increase in the percentage of PTEs. The percentage increased from 8,3% to 41,7% what reflects an improvement of 402,4% in the support to PSI in this group, if considered to PTEs. If considered the PNEs procedures, the continued application of endomarketing techniques in the experimentation group enabled a decrease of 88% against a increase of 12,6% in the control group and a high concentration of percentages on the partially or totally run procedures that added they reach 93,7% in the final evaluation. It is concluded then that the continuous application of endomarketing techniques improves the PSI effectiveness.

Key-Words: Information Security Policy, Endomarketing, Human Resources, Security

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE SIGLAS

HUSM – Hospital Universitário de Santa Maria
IEC – *International Electrotechnical Commission*
IS – Sistemas de Informação
ISO – *International Organization for Standardization*
NBR – Norma Brasileira Reguladora
PSI – Política de Segurança da Informação
PCSI – Programa de Conscientização em Segurança da Informação
SUS – Sistema Único de Saúde
UCI – Unidade de Cardiologia Intensiva
UFSM – Universidade Federal de Santa Maria
UTI – Unidade de Terapia Intensiva - Adulto

LISTA DE APÊNDICES

SUMÁRIO

CAPÍTULO 1

INTRODUÇÃO

De uma forma ou de outra, as organizações sempre se demonstraram preocupadas com a segurança das informações existentes no ambiente organizacional, porém esta preocupação nunca se tornou tão evidente quanto nos dias atuais devido ao avanço dinâmico das tecnologias de informação e de comunicação (TICs), a integração entre essas tecnologias e a quantidade expressiva de dados que trafegam em meio a redes de comunicação. Todo este avanço em termos de tecnologias vem de um lado acelerando a administração organizacional ao proporcionar formas mais fáceis e ágeis de acesso às informações, mas sob outro ângulo gerando problemas com relação ao estabelecimento de políticas internas destinadas ao correto gerenciamento das informações organizacionais. Esta dicotomia tem sido apontada como a principal fragilidade da tríade usuário-sistema-informação (MARCIANO; LIMA-MARQUES, 2006).

O estabelecimento de uma política de segurança da informação (PSI) pode resolver parte dos problemas relacionados à segurança, por atribuir regras e procedimentos direcionados a garantir a segurança das informações organizacionais. Entretanto, ela não é capaz de resolver estes problemas integralmente, pois funcionários despreparados, não conscientes da importância da segurança da informação e que desconhecem os procedimentos necessários para garantí-la, podem comprometer significativamente a efetividade da mesma.

Além disso, segundo Wood (2000) as PSIs são, vias de regra, apresentadas aos usuários como códigos de conduta aos quais eles devem se adequar integralmente, mesmo sem haver uma discussão adequada sobre o grau de receptividade dos usuários a estas políticas. Como resultado, a implantação das PSIs pode gerar resistências por parte dos usuários no que tange aos cuidados que devem ser direcionados à manipulação segura e controlada das informações.

Desta forma, a busca constante pela efetividade da PSI tem sido um grande desafio aos

profissionais responsáveis pela gestão de segurança da informação. Na esfera técnica a PSI já é uma realidade indiscutível, mas ela ainda apresenta fracassos do ponto de vista da manipulação humana das informações geradas e mantidas pelos sistemas computacionais. Este tem sido o motivo central apontado por especialistas para os incidentes relacionados à segurança das informações empresariais (HÖNE; ELOFF, 2002; ERNEST & YOUNG, 2004; ISACA, 2005; CERT, 2007; MODULO SECURITY SOLUTIONS, 2007a; MODULO SECURITY SOLUTIONS, 2007b).

O grande desafio à segurança da informação é fazer com que o quadro funcional se conscientize da importância dos procedimentos descritos na PSI no intuito de se reduzir falhas causadas por erros intencionais ou não, advindas da falta de conhecimento ou de esclarecimentos relacionados à segurança da informação. Segundo Höne e Eloff (2002) a baixa adesão às políticas de segurança da informação decorre muitas vezes do desconhecimento dos usuários sobre a existência da política de segurança, do não entendimento deste documento por parte dos usuários ou porque os usuários não conseguem perceber um relacionamento entre a política e suas atividades diárias. Por isto, de modo equivocado, alguns dirigentes empresariais adquirem novas tecnologias, achando que assim suprirão as falhas de segurança da informação. Porém, em muitos casos, estas falhas originam-se de pessoas que desconhecem a maneira correta de manipular e proteger as informações organizacionais, comprometendo inclusive os resultados apresentados por tecnologias desenvolvidas para resguardar as informações de forma controlada e segura, como: firewalls, programas antivírus, sistemas de detecção e intrusão e biometria (JOHNSON, 2006).

Dada a relevância dos aspectos humanos no contexto da segurança da informação, muitos autores dessa área têm se empenhado em citar e descrever técnicas capazes de aumentar o nível de conscientização dos usuários para com o tema segurança da informação, como por exemplo, o Endomarketing (PAYNE, 2003; MCCOY; FOWLER, 2004; PELTIER, 2005; JOHNSON, 2006). Neste contexto, o endomarketing apresenta-se como uma estratégia de gestão voltada à aplicação de técnicas capazes de resgatar o comprometimento dos usuários para que os pressupostos, definidos na PSI, sejam realmente executados. Embora os trabalhos desenvolvidos na área de segurança, anteriormente mencionados, sejam relevantes para a comunidade acadêmica, os autores não referenciam as técnicas utilizadas em seus trabalhos como sendo técnicas de endomarketing, o que torna questionável o caráter científico da aplicação destas técnicas no ambiente organizacional, pois segundo Bekin (2005) a maioria

das organizações tem praticado ações de endomarketing algumas vezes de forma consciente e outras de forma puramente intuitiva sem sequer conhecerem a nomenclatura endomarketing.

Assim, o diferencial deste trabalho é não somente citar e descrever técnicas de endomarketing, mas abordar a sua utilização de forma não intuitiva com base em autores da área específica de marketing, bem como demonstrar o impacto que a utilização destas técnicas pode causar à efetividade da PSI.

1.1 Problema de Pesquisa

O problema de pesquisa fundamenta-se em verificar se a utilização de técnicas de endomarketing é relevante para a segurança das informações organizacionais a ponto de proporcionar melhorias na efetividade das políticas de segurança da informação no que tange a execução dos procedimentos nela definidos. Portanto o que se questiona é: **Qual o impacto causado pela utilização de técnicas de endomarketing na efetividade das políticas de segurança da informação?** Para responder a este questionamento foram estabelecidos os objetivos descritos nas seções 1.2 e 1.3 a seguir.

1.2 Objetivo Geral

Analisar e comparar, através de uma pesquisa experimental, o impacto da utilização de técnicas de endomarketing na efetividade de uma Política de Segurança da Informação implantada nas Unidades de Cardiologia Intensiva (UCI) Terapia Intensiva – Adulto (UTI) do Hospital Universitário de Santa Maria – HUSM.

1.3 Objetivos Específicos

Os objetivos específicos que norteiam este trabalho relacionam-se a seguir:

- Analisar e avaliar o ambiente interno das unidades hospitalares supramencionadas;
- Detectar o nível de conscientização dos clientes internos para com o tema Segurança da Informação;
- Aplicar técnicas de endomarketing para a obtenção do comprometimento dos usuários para com a PSI;
- Comparar o impacto da utilização destas técnicas na UCI/UTI do Hospital Universitário de Santa Maria - HUSM.

1.4 Estrutura da dissertação

A presente dissertação está estruturada em 7 capítulos. O capítulo 1 exibe uma introdução ao tema pesquisado, contextualizando uma visão geral do trabalho, sua importância, seus objetivos e sua estrutura. O Capítulo 2, apresenta um embasamento teórico sobre a Política de Segurança da Informação - PSI, iniciando-se com a descrição de conceitos e definições relacionados à Política de Segurança da informação – PSI. O capítulo também demonstra o impacto da PSI no contexto organizacional discorrendo sobre os pontos relevantes para a efetividade de uma PSI e finaliza demonstrando o papel da conscientização no processo de implantação da PSI. O capítulo 3 apresenta um aprofundamento teórico sobre endomarketing, desde a evolução histórica do marketing até a importância do endomarketing na implantação de uma PSI e como o marketing pode ser aplicado à área de segurança da informação. O capítulo finaliza com a apresentação de diferentes técnicas utilizadas para a conscientização dos usuários em segurança da informação. O capítulo 4 são descritas as características do ambiente de aplicação do presente estudo, bem como a metodologia, a forma de coleta e análise de dados e as limitações da dissertação. O capítulo 5 descreve detalhadamente todos os procedimentos executados para a realização da pesquisa. O capítulo 6 apresenta os resultados das pesquisas aplicadas nas Unidades de Cardiologia Intensiva (UCI) e Terapia Intensiva – Adulto (UTI) do Hospital Universitário de Santa Maria – HUSM. Por fim, o capítulo 7 apresenta as conclusões advindas da realização deste trabalho, bem como as sugestões para trabalhos futuros.

CAPÍTULO 2

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

Este capítulo fornece um embasamento teórico sobre a Política de Segurança da Informação – PSI, apresentando suas definições e objetivos; apresenta o impacto da PSI no contexto organizacional; discorre sobre os pontos relevantes para a efetividade de uma PSI, segundo as abordagens de Höne e Eloff (2002), Solms e Solms (2004) e Kruger e Kearney (2006); e, finaliza-se demonstrando o papel da conscientização no processo de implantação da PSI.

2.1 Definições e objetivos de uma PSI

Uma política de segurança da informação pode ser definida como a manifestação formal, através da qual a alta administração demonstra os interesses da organização em proteger os seus recursos de informação, evidenciando seu comprometimento e apoio para com a segurança da informação (TUDOR, 2006).

Na concepção de Wood (2000) uma política de segurança da informação é um conjunto de instruções gerenciais que indicam um curso de ação, um guia de princípios ou procedimentos que proporcionam praticidade, uma forma de precaução ou algum tipo de vantagem às organizações.

Whitmann (2004) salienta que devido a PSI ser o ponto de partida para a segurança da informação, ela define a postura de gerenciamento desejado para ajustar todo o perfil de segurança de uma organização. Sua criação e implantação é necessária para que haja o gerenciamento da segurança da informação nas organizações. Além disso, ela é responsável por definir o papel da segurança da informação no apoio e suporte à visão e à missão

organizacional e deve complementar os objetivos de negócio, refletindo a vontade da organização em operar de maneira controlada e segura.

Na concepção de Nosworthy (2000) os objetivos de uma PSI podem ser resumidamente descritos em:

- Demonstrar o comprometimento da alta administração para com a segurança da informação;
- Direcionar a segurança da informação nas organizações, enfatizando sua importância nas operações diárias da organização; e
- Proteger os recursos de informação pertencentes à organização.

Além destes objetivos uma PSI possui quatro importantes funções (OSBORN, 1998):

- Expor a necessidade de segurança da informação aos usuários;
- Descrever as funções e responsabilidades da organização para com a segurança da informação;
- Guiar a organização na seleção, uso apropriado de equipamentos ou produtos voltados a garantir a segurança das informações, bem como procedimentos e padrões; e
- Explicar os conceitos relacionados à segurança da informação e métodos necessários para se garantí-la na organização.

Como os objetivos e as funções de uma PSI estão diretamente relacionados aos recursos humanos, presentes no ambiente interno das organizações, é importante que ela explique a necessidade e os conceitos de segurança da informação. Oliveira (2001) ressalta a relevância destes pontos, pois faz parte da natureza humana se utilizar de meios mais rápidos para a realização de tarefas, burlando regras e regulamentos, quando não estiverem de acordo com suas necessidades. Porém, na concepção de Oliveira, a alta administração deve ser capaz de responder a estas situações de maneira consistente e apropriada, garantindo que estas ações não sejam legitimas e demonstrando a necessidade de uma política de segurança da informação.

Para Whitmann (2004) a principal função de uma PSI é explicitar aos usuários a posição da organização com relação à segurança da informação e o que é esperado deles para se garantir a manipulação segura dos recursos de informação. O autor reforça que os usuários precisam saber os requisitos necessários para a proteção de recursos, como eles devem utilizá-los e o comportamento aceitável em sua manipulação.

A implantação de uma PSI é necessária para o alcance e manutenção de um nível adequado e consistente de segurança em toda a organização. Como a segurança da informação

é uma responsabilidade que deve ser compartilhada por todos os usuários, ela precisa ser disciplinada através de uma clara e visível PSI, pois sem esta, os usuários não saberão como manipular os recursos de informação de forma segura, por não saberem ou não entenderem o que se espera deles em termos de segurança da informação. A PSI deve, primeiramente, descrever o que significa segurança para a organização e como os recursos de informação podem estar de fato seguros (GARTNER, 2003). Ela deve também direcionar a organização em seus diversos processos de negócio e tecnologias, mantendo os requisitos de segurança, controle e privacidade na mente das pessoas (MCARTHY; CAMPBELL, 2001). Isto é muito importante para que a política tenha o apoio de todos os níveis da organização e não somente do pessoal responsável pela área de segurança da informação.

2.2 A PSI e seu impacto na cultura organizacional

A implantação de uma PSI gera impactos na cultura organizacional, pois pode interferir na linha de poder e *status quo* dos envolvidos. Por esta razão é necessário estabelecer um ambiente propício à sua implementação, pois o sucesso de sua implementação depende da participação de todos, ou seja, da alta administração em apoiar a cultura voltada à segurança da informação e dos demais membros em se comprometer para com a mesma.

Dentro desse raciocínio Fávero (2006) destaca que é através de uma política de segurança eficaz que a alta administração comunica aos seus colaboradores sua motivação e como será disciplinada a segurança da informação, complementando ainda que a política rege os detalhes a serem observados, o que é esperado de cada participante da organização e às sansões em caso de não aplicação ou não seguimento das normas estipuladas na política de segurança da informação organizacional (FÁVERO, 2006).

A PSI não só define procedimentos relacionados à manipulação e proteção da informação como também atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação. Além disso, ela é um instrumento importante para proteger as organizações contra ameaças às informações a ela pertencentes ou que estão sob sua responsabilidade. Neste contexto, entende-se por ameaça a quebra de uma ou mais das três propriedades fundamentais relacionadas à segurança (confidencialidade, integridade e disponibilidade) (CERT, 2003).

Conforme a NBR/ISO IEC 17799:2005 a confidencialidade garante que somente as pessoas explicitamente autorizadas podem ter acesso à informação. Já a integridade garante que a informação deve ser encontrada em sua forma original deste o momento em que foi armazenada, mantendo desta forma a proteção dos dados ou informações contra modificações intencionais ou acidentais não autorizadas. Por sua vez a disponibilidade é garantida quando a informação está acessível, por pessoas autorizadas, sempre que necessário.

Manter boas práticas de segurança suportadas por uma política de segurança da informação é a primeira etapa para aumentar o nível de confiança dos clientes. O estabelecimento de regras claras de segurança permite que as organizações estabeleçam níveis de controle mínimos, e dimensionem as ações administrativas necessárias para o uso inadequado de recursos de TI (NEVES, 2007).

Vale destacar que na 9ª Pesquisa Nacional de Segurança da Informação realizada pela Modulo Security Solutions com cerca de 50% das 1000 maiores empresas brasileiras, atuantes em diversos segmentos de mercado foi verificada uma preocupação das empresas com relação à implementação de políticas de segurança nas suas organizações. A referida pesquisa revelou ainda que as demais 50% das empresas denunciaram equívocos sobre a política de segurança de informação (Figura 1).

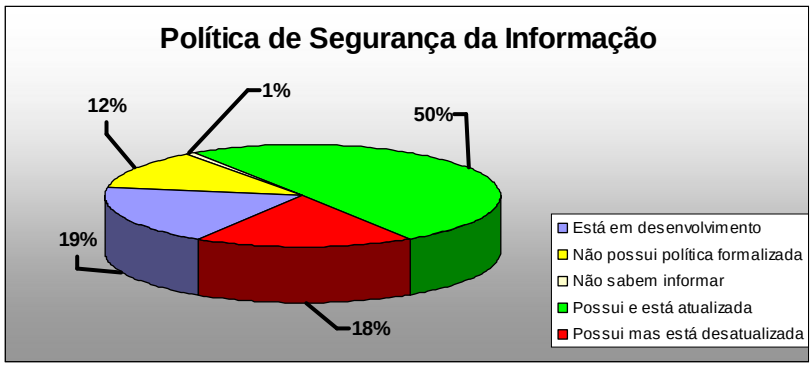


Figura 1 – Pesquisa sobre Política de Segurança
Fonte: Adaptado de Modulo Security Solutions (2003)

Embora a pesquisa demonstre um empenho das organizações em implantar uma política de segurança (50%+18%+19% = 87%) pode-se verificar que em 31% (12%+18% +1%) das empresas esta política não é formalizada ou está desatualizada. O que comprova que não existe um comprometimento das pessoas com relação à mesma. Além disso, observa-

se que o fato de 50% das empresas possuírem uma política de segurança e a mesma estar atualizada não garante que os funcionários estejam comprometidos para com ela.

Diante disso percebe-se que a implementação de uma política de segurança da informação pode gerar resistência por parte dos funcionários, especialmente, quando as regras e procedimentos nela descritos afetam diretamente as atividades diárias de todo um grupo de pessoas. Assim, na acepção de Neves (2007) para que sua implementação seja eficiente é de fundamental importância que cada mudança seja avaliada e colocada em prática juntamente com uma ação de conscientização e comunicação maciça. Complementa seu raciocínio dizendo que o processo de conscientização varia de acordo com a cultura corporativa de cada organização e que a implementação de diversas mudanças de forma abrupta gera barreiras e antipatia das pessoas.

Administrar a mudança de forma gradual, de acordo com a capacidade de absorção da comunidade envolvida é a melhor opção, não sendo necessários grandes investimentos e transformando pessoas irritadas em aliados para o processo, pois elas serão capazes de aderir a idéia com mais facilidade se compreenderem porque isto esta sendo feito, sem imposição. Ramos (2003) reforça inclusive que não se conquista aliados através da coação. Dizer que todos os funcionários serão monitorados e que o comportamento inadequado será punido, pode não ser uma boa escolha. A prática demonstra que ao invés de amedrontá-los o melhor a se fazer é encorajá-los a participar como agentes no controle da informação (RAMOS, 2003).

Com relação a quebras de segurança o ativo humano é um dos mais críticos, pois seres humanos cometem erros, têm personalidade ímpar, características dinâmicas de relacionamento interpessoal e apresentam comportamentos variados e imprevisíveis, colocando em risco, intencionalmente ou não, a confidencialidade, integridade e disponibilidade das informações a que têm acesso (SEMOLA, 2003).

O fator humano é tão importante que a 10ª Pesquisa Nacional de Segurança da Informação realizada pela empresa Módulo Security Solutions, publicada no ano de 2007, abordou pela primeira vez temas como a capacitação de equipes e a conscientização de funcionários. A pesquisa contou com a resposta de cerca de 600 profissionais atuantes nas áreas de Segurança e Tecnologia da Informação de organizações privadas, públicas e de economia mista, em diferentes áreas (MODULO SECURITY SOLUTIONS, 2007). A pesquisa revelou que quando conseguem identificar os responsáveis, as empresas descobrem que a maioria das falhas de segurança é causada por funcionários (24%) seguida de hackers (20%), problemas vírus (15%), spam (10%) e fraudes (8%) (MODULO SECURITY SOLUTIONS, 2007). Outra informação significativa desta pesquisa é que a maioria das

empresas considera a falta de conscientização dos executivos e usuários o principal obstáculo para a implementação da segurança na empresa. A Figura 2 permite verificar os percentuais obtidos na referida pesquisa.

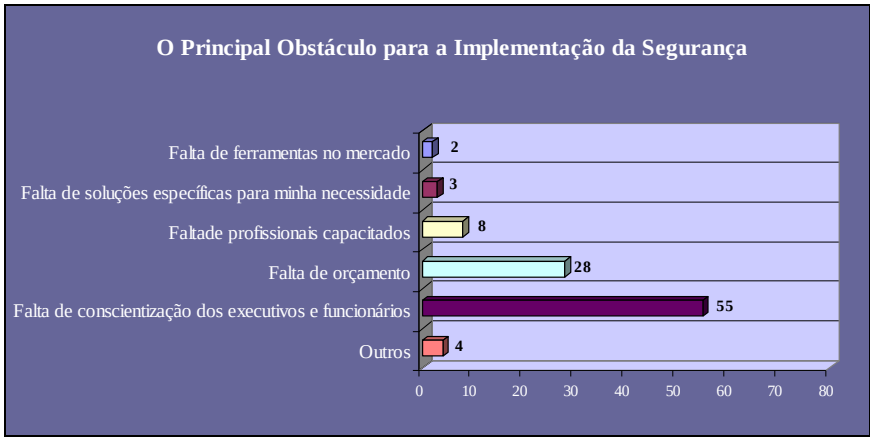


Figura 2 – Principal Obstáculo para a Implementação da Segurança
Fonte: Adaptado de MODULO SECURITY SOLUTIONS (2007)

Diante do exposto, pode-se verificar que a inexistência de um apontamento de Segurança da Informação, formal e documentado, aumenta consideravelmente os riscos provenientes de ameaças relacionadas à segurança. Uma organização moderna é resultado da interação entre máquinas e profissionais capacitados, orientados por uma política de segurança da informação sintonizada com a cultura e o ambiente tecnológico existente (AXUR, 2002).

2.3 A efetividade de uma PSI

O principal objetivo de qualquer PSI é influenciar e determinar as decisões, as ações e os comportamentos dos empregados, especificando os comportamentos aceitáveis e inaceitáveis (WHITMANN, 2004).

Na concepção de Höne e Elloff (2002), uma PSI efetiva ajuda as organizações a alcançarem os seus objetivos em termos de segurança da informação, fazendo com que os usuários compreendam o comportamento responsável e aceitável na manipulação dos recursos

de informação com vistas a garantir a proteção destes recursos. Ela também deve ajudar as organizações na priorização de recursos e atividades a fim de garantir que as estratégias de gerenciamento em segurança da informação possam ser realmente executadas, fornecendo suporte para que as estratégias de negócio sejam alcançadas. Portanto, uma PSI deve agregar as necessidades dos usuários por informações seguras e precisas, bem como as necessidades do negócio pela a obtenção de objetivos estratégicos. Assim, os usuários devem estar convencidos de que a segurança da informação não é um mal necessário, mas ao contrário, ela visa garantir que a informação correta esteja disponível no tempo certo para que decisões corretas sejam tomadas, proporcionando lucro e sucesso às organizações.

Fazer com que uma PSI seja realmente efetiva não é uma tarefa fácil. Cada organização tem suas particularidades e seus domínios de atuação e a PSI deve ser adequada a estas características. Este é um dos motivos pelos quais diversos estudiosos, da área de segurança da informação, têm se empenhado em demonstrar às organizações como obter a tão almejada efetividade de uma PSI.

Na seqüência são apresentadas as abordagens de três diferentes autores sobre o que as organizações podem fazer para garantir a efetividade de suas políticas de segurança da informação.

2.3.1 Abordagem de Höne e Ellof

A efetividade de uma PSI pode ser obtida desenvolvendo-se um conjunto de atividades relacionadas à política, as quais devem dar enfoque aos usuários e ao tipo de negócio praticado pela organização. Höne e Ellof (2002) destacam que uma política de segurança torna-se mais efetiva se os usuários tiverem a possibilidade de perceber claramente o que é esperado deles em termos de manipulação dos recursos de informação. Na concepção destes autores, seis componentes servem de apoio a efetividade de uma PSI (Figura 3): Estilo, Desenvolvimento, Apresentação, Disseminação, Manutenção e Comprometimento.

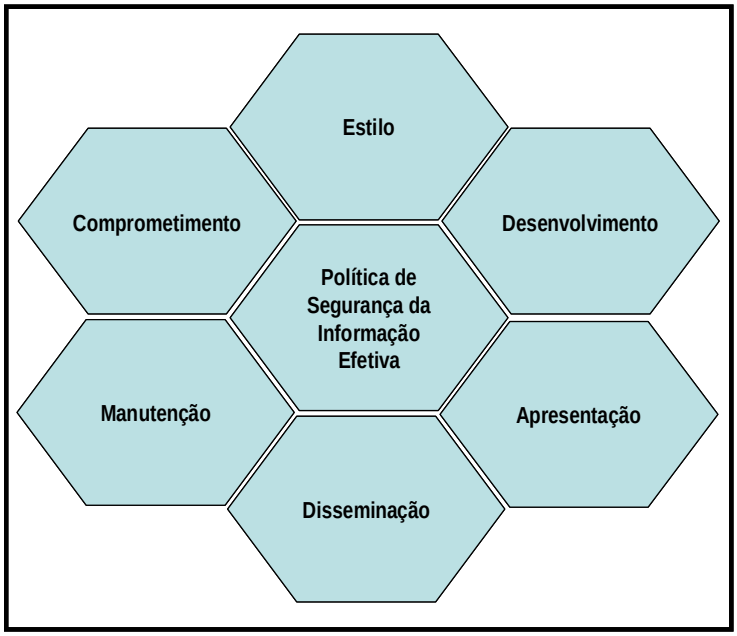


Figura 3 – Componentes de apoio à efetividade da PSI
Fonte: Adaptado de Höne e Eloff (2002)

O estilo descreve a maneira de escrita do documento. A PSI deve estar de acordo com a cultura organizacional e obedecer aos padrões de escrita dos demais documentos emitidos pela organização. Atualmente, a *WEB* disponibiliza uma grande variedade de PSIs e muitas organizações acreditam que um simples "copiar/colar" resolverá seus problemas de segurança da informação. Entretanto, a efetividade da PSI pode ser comprometida por esta ação, pois cada organização possui suas particularidades, seus segmentos de atuação e seus objetivos de negócio e estas características variam de organização para organização.

O desenvolvimento da PSI refere-se aos procedimentos executados para sua criação. Seu desenvolvimento deve ser realizado por todos os *stakeholders*, direta ou indiretamente, envolvido com a segurança da informação. Além disso, o desenvolvimento da PSI deve incluir a participação de profissionais de diversas áreas e com diferentes percepções sobre como determinados riscos podem comprometer a segurança das informações. Isso faz com que a PSI não seja um documento muito longo ou muito técnico, desenvolvido por profissionais de uma área específica.

A apresentação é o momento em que a PSI é apresentada a todos os profissionais da organização. Este momento deve permitir uma comunicação interativa, na qual todos compreendem os pressupostos definidos na política. As dúvidas existentes, quanto a um

determinado tópico, são imediatamente esclarecidas, fazendo com que os usuários sempre tenham uma resposta adequada a seus questionamentos.

A disseminação refere-se à divulgação da PSI no ambiente organizacional. Na concepção de Höne e Ellof (2002) a disseminação de uma PSI é de vital importância para sua efetividade, pois ela não terá utilidade se os usuários dos recursos de informação não estiverem cientes de sua existência e o que ela representa em termos de comportamento. Os autores reforçam ainda argumentando que se os usuários desconhecem a PSI, não se pode esperar a adesão e a observância de seus pressupostos. Se os usuários não souberem onde encontrar uma cópia dela, não se pode esperar que eles a leiam. Se os usuários não perceberem um relacionamento entre a política e suas atividades diárias não se pode esperar que eles a tratem com seriedade, nem tão pouco, que eles se responsabilizem para com ela. Por estes motivos os autores consideram a disseminação tão importante para a PSI, pois ela não está somente associada à forma de sua distribuição, mas também ao seu armazenamento e as campanhas de conscientização associadas à sua distribuição.

O comprometimento envolve a colaboração de todos, indistintamente, para com os controles definidos na PSI, desde a alta administração até os profissionais da base organizacional. Segundo Höne e Ellof (2002) os profissionais da linha de base não se comprometerão em agir de acordo com o que é determinado na PSI se os seus líderes não o fizerem.

A manutenção se refere às atualizações necessárias em uma PSI, advindas de mudanças na estrutura organizacional e/ou da aquisição de novos recursos tecnológicos. O ideal é que estas atualizações sejam realizadas em épocas apropriadas a fim de não entrarem em conflito com outras atividades realizadas pela organização, por exemplo, no final do ano geralmente os profissionais dedicam-se a realização de balancetes anuais, portanto, esta pode não ser uma boa época para se fazer atualizações da PSI.

Todos os componentes, acima descritos, são inter-relacionados. Devem ter o foco no usuário e não devem ser considerados em isolado no processo de criação de uma PSI. Na concepção de Höne e Ellof (2002) a efetividade de uma política de segurança não é somente abordar o conteúdo de forma correta, mas também a maneira como este conteúdo é direcionado e comunicado aos usuários. A apresentação deste documento deve permitir uma comunicação interativa na qual os usuários possam perceber as mensagens que a política transmite.

2.3.2 Abordagem de Solms e Solms

A definição de um processo adequado que envolva política, educação e cultura organizacional também pode servir de amparo às organizações para que sua PSI seja realmente efetiva. Solms e Solms (2004) destacam que a definição de uma política de segurança não garante que todos os funcionários irão, necessariamente, obedecê-la. O ideal é que ela expresse a cultura da organização como forma de garantir o comportamento adequado que se espera dos profissionais, o que só pode ser alcançado através de um processo adequado de educação. Para estes autores a adesão as políticas de segurança da informação depende de um processo que integre política, educação e cultura. Para tanto, é necessário que a definição da PSI origine-se da alta administração, demonstrando que garantir a segurança da informação faz parte da missão e da visão organizacional. Assim, os profissionais, que cumprirem os pressupostos definidos na PSI conseqüentemente estarão agindo de acordo com a cultura organizacional, pois a PSI é reflexo da mesma. Assim, a criação de uma PSI é função da governança corporativa e da alta administração, as quais inicializam a formação de uma cultura corporativa que inclui a segurança da informação.

Os resultados advindos da fusão entre cultura corporativa, segurança da informação e governança corporativa são denominados obediência em segurança da informação (THOMSON; SOLMS; LOUW, 2006). Thomson e Solms (2005) definem obediência em segurança da informação como o fato de os usuários se comportarem em conformidade com a visão organizacional, determinada pela alta administração, a qual é definida na Política de Segurança da Informação Corporativa.

Com base neste raciocínio Thomson, Solms e Louw (2006) propuseram um modelo para orientar as organizações a obter a obediência em segurança da informação, agregando política, educação e cultura. Este modelo (Figura 4) denomina-se MISSTEV (*Model for Information Security Shared Tacit Espoused Values*) e foi desenvolvido com a finalidade de se permitir o compartilhamento de conhecimentos sobre segurança da informação entre os profissionais, através da exposição tácita de valores. Ele é formado por dois componentes: um modelo de aprendizagem e por formas de criação do conhecimento, incluindo abordagens teóricas e a resolução de problemas.

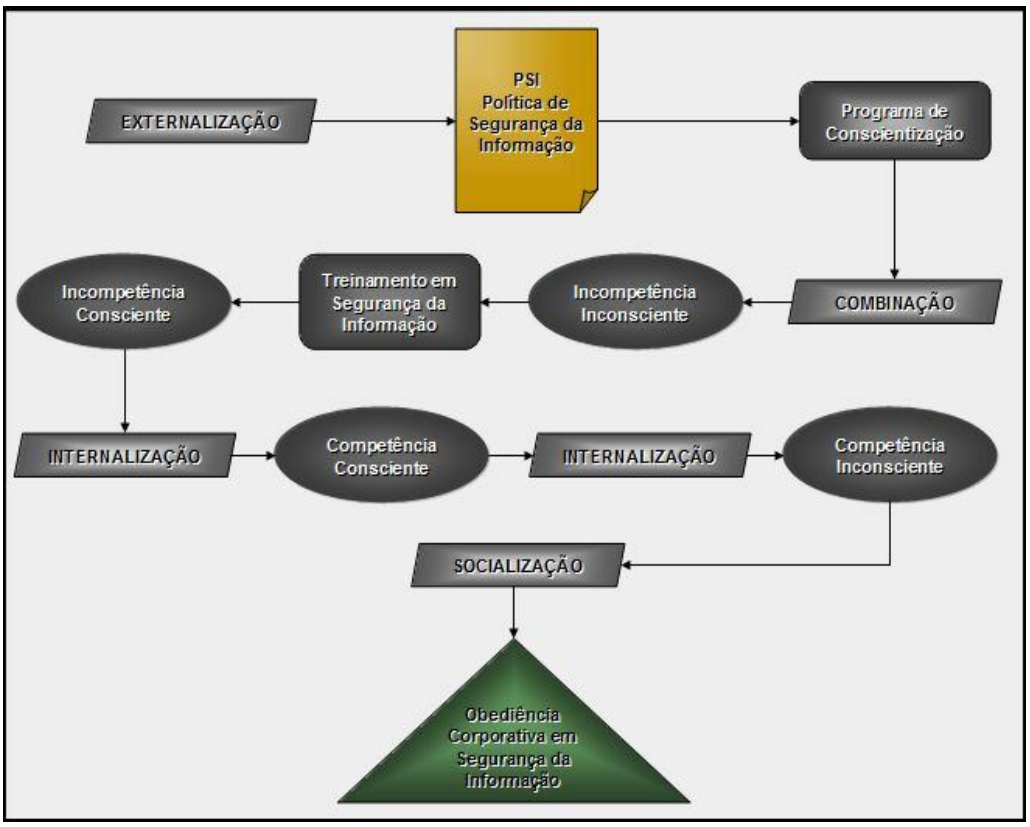


Figura 4 – Modelo MISSTEV
Fonte: Adaptado de Thonsom, Solms e Louw (2006)

O primeiro componente do modelo MISSTEV (modelo de aprendizagem) é formado por quatro estágios denominados: incompetência inconsciente, incompetência consciente, competência consciente e competência inconsciente. Eles descrevem os estágios de aprendizagem necessários para a aquisição de novas habilidades ou comportamentos. O segundo componente do modelo MISSTEV é baseado nos modos de criação do conhecimento de Nonaka (1994), o qual abrange tanto o conhecimento tácito quanto o conhecimento explícito, bem como as etapas que compreendem a criação do conhecimento, as quais devem ocorrer para que haja a transferência de conhecimentos entre as pessoas. O propósito dos modos de criação do conhecimento de Nonaka (1994) é identificar a existência de conhecimento e convertê-lo em um novo conhecimento. Essa identificação é feita por meio de quatro processos: externalização, combinação, internalização e socialização. Estes processos serão explicados, com maiores detalhes, no seguimento desta seção.

Na concepção de Thomson, Solms e Louw (2006) as organizações detêm conhecimentos tácitos, sobre segurança da informação, através de seu representante oficial. O conhecimento tácito envolve crenças, atitudes e habilidades técnicas, formando a visão da

organização sobre o que ela considera importante, em termos de segurança da informação, para que os objetivos organizacionais sejam alcançados. Entretanto o conhecimento tácito é um conhecimento subjetivo, baseado na experiência das pessoas, sendo difícil de ser formalizado e comunicado. O conhecimento na forma tácita somente pode ser praticado ou utilizado por quem o detém, havendo, portanto a necessidade de que ele seja transformado em um novo tipo de conhecimento denominado conhecimento explícito. O conhecimento explícito é um conhecimento objetivo e racional. Pode ser comunicado através de palavras e sentenças.

No contexto de segurança da informação, o conhecimento tácito do representante da alta administração é transformado em conhecimento explícito no momento em que as organizações implementam sua PSI. A PSI é a base do modelo MISSTEV, pois é a partir deste documento, formalizado, que as organizações manifestam como elas gostariam que as informações fossem tratadas em seu ambiente interno.

Esta manifestação pública, dos interesses da organização, é denominada por Thomson, Solms e Louw (2006) de externalização, que na concepção dos autores nada mais é do que a transformação do conhecimento tácito da alta administração (visão organizacional) em conhecimento explícito (desenvolvimento da PSI), de forma entendível e compreensível, capaz de demonstrar a visão da organização às pessoas que a integram.

Uma vez externalizada a visão organizacional, deve haver a apresentação da PSI aos funcionários, os quais em termos de segurança da informação encontram-se em um estágio de aprendizagem denominado “incompetência inconsciente”. Neste estágio as pessoas estão inconscientes ou desconhecem as habilidades particulares ou formas de comportamento que são esperados delas. Isso faz com que as mesmas se neguem a praticar o comportamento esperado, em termos de segurança da informação, e não vejam utilidade na aquisição de novas habilidades para agir em conformidade para com a mesma. Para que as pessoas adquiram novas habilidades é vital que elas se tornem conscientes da necessidade de se aprender alguma coisa nova (THONSOM, SOLMS; LOUW, 2006).

Os programas de conscientização em segurança da informação fazem com que os funcionários se direcionem a um novo estágio de aprendizagem, denominado “incompetência consciente”. Neste estágio as pessoas tornam-se conscientes da relevância das habilidades que elas devem possuir. Elas conseguem perceber o que é inadequado e são capazes de avaliar o nível de habilidades requeridas para obter sua própria competência com relação à segurança da informação. O propósito destes programas e focar a atenção em segurança e tornar os empregados conscientes das habilidades necessárias para proteger adequadamente os ativos

de informação. Neste estágio é vital que os empregados percebam o que é esperado deles e o motivo pelo qual proteger as informações é tão vital para a organização (THONSOM, SOLMS; LOUW, 2006).

A passagem do estágio “incompetência inconsciente” para o estágio de “incompetência consciente” é feito por meio de um processo chamado combinação. Este processo permite a transferência de conhecimento explícito da organização para os indivíduos que a compõem, fazendo-se uso de documentos, e-mails, encontros ou treinamentos. A coleta e a disseminação de informações relevantes são muito importantes para este processo, pois envolvem a transferência de conhecimento entre a organização e um grupo de pessoas.

O treinamento em segurança da informação, disponibilizado pela organização aos seus funcionários, faz com que eles compreendam as questões práticas necessárias para proteger as informações. O treinamento faz com que os empregados desenvolvam a prática necessária para proteger as informações e entendam os conceitos e procedimentos básicos de segurança, fazendo com que os funcionários progridam para o estágio de “competência consciente” do modelo MISSTEV. Neste estágio as pessoas detêm novas habilidades, necessárias para agir em prol da segurança da informação. Entretanto elas ainda precisam se concentrar na realização destas habilidades, pois elas não são praticadas de forma natural, ou seja, as pessoas não conseguem utilizar suas habilidades sem pensar nelas, pois elas não fazem parte de seu comportamento diário (THONSOM, SOLMS; LOUW, 2006).

No processo de internalização os profissionais devem entender e apoiar a visão organizacional, relacionada à segurança, determinada pela alta administração. Através deste processo os funcionários praticam os procedimentos descritos na PSI e o conhecimento explícito recebido no treinamento, fazendo uso das habilidades obtidas para a realização de suas tarefas ou se utilizando de simulações. A internalização guia os profissionais ao estágio de aprendizagem denominado competência inconsciente. Neste estágio as habilidades desenvolvidas no estágio anterior são praticadas constantemente, fazendo com que as pessoas não precisem pensar nelas para sua realização. As habilidades são praticadas tão naturalmente ou fazem parte das ações e comportamentos das pessoas que neste estágio elas se tornam totalmente instintivas. Somente quando os funcionários encontrarem-se neste estágio eles serão capazes de socializar o conhecimento adquirido (THONSOM, SOLMS; LOUW, 2006).

A socialização é o processo no qual uma pessoa, detentora do conhecimento tácito, o transfere tacitamente a outra pessoa. A socialização envolve a captura de conhecimento através da interação direta entre indivíduos, internos ou externos à organização. Ela depende do compartilhamento de experiências entre os indivíduos e resulta na aquisição de habilidades

e modelos mentais comuns entre as pessoas. Para que haja a evolução do estágio "competência inconsciente", o conhecimento que os profissionais detêm deve ser transferido tacitamente a outros profissionais através do processo de socialização. A evolução dos funcionários ao estágio de competência inconsciente direciona-os à obediência corporativa em segurança da informação e garante o sucesso da organização em termos de segurança da informação.

Na acepção de Thonsom, Solms e Louw (2006) através do modelo MISSTEV os funcionários se mantêm informados da visão organizacional, em termos de segurança da informação, conhecendo suas funções e responsabilidades para com a mesma. Além disso, o modelo facilita a transmissão do conhecimento, fazendo com que funcionários se tornem conscientes e desenvolvam novas habilidades para proteger os ativos de informação.

2.3.3 Abordagem de Kruger e Kearney

Métodos de controle também são apresentados na literatura como facilitadores para que a efetividade de uma PSI possa ser obtida pelas organizações. Kruger e Kearney (2006) destacam que a implementação de controles efetivos de segurança depende da criação de um ambiente positivo no qual todos os usuários entendem e se engajam para comportar-se de acordo com o que se espera deles. Este ambiente positivo advém de uma cultura organizacional voltada à segurança da informação e do entendimento, por parte dos profissionais, do que se deve fazer para proteger os recursos de informação existentes no meio organizacional. Para Kruger e Kearney (2006) o entendimento das práticas necessárias a segurança da informação acarreta um aumento na conscientização dos funcionários, fazendo com que eles pratiquem mais facilmente os pressupostos descritos nas políticas de segurança da informação. Este é o principal motivo pelo qual os autores salientam a importância de se avaliar os níveis de conscientização dos usuários, pois esta avaliação permite que esforços possam ser direcionados a soluções de questões problemáticas relacionadas à PSI.

Seguindo este raciocínio, Kruger e Kearney (2006) desenvolveram um protótipo para mensurar quantitativamente os níveis de conscientização dos usuários. O modelo tem por base três dimensões: conhecimento, comportamento e opinião. O conhecimento diz respeito ao que a pessoa sabe ou o quanto ele conhece sobre um determinado assunto, o comportamento

refere-se a como ela se comporta em uma dada situação e a opinião refere-se a o que ela pensa ou quais são suas opiniões sobre um determinado tópico ou questão.

Utilizando-se de uma estrutura em forma de árvore, conforme demonstra a Figura 5, cada dimensão do modelo é avaliada.

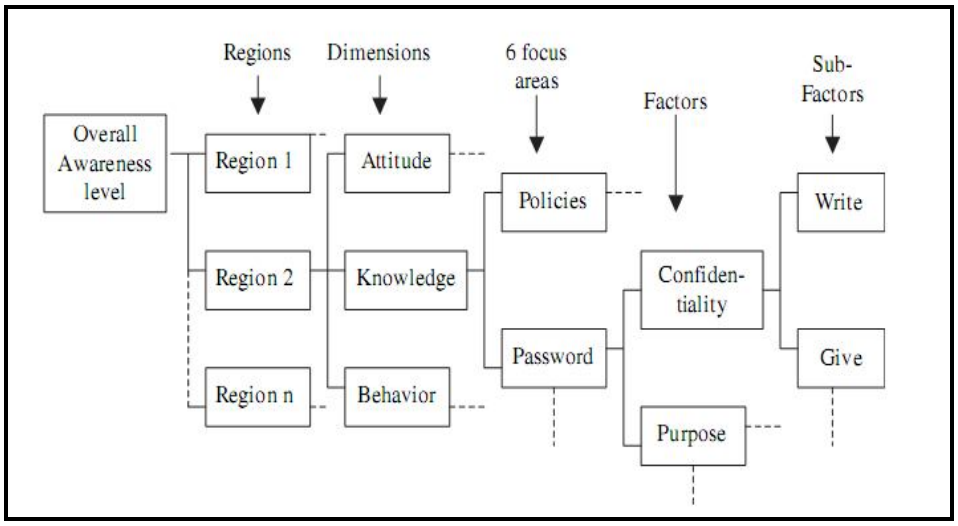


Figura 5 – Protótipo para Avaliação da Conscientização em Segurança da Informação
Fonte: Kruger e Kearney (2006, p. 292)

Esta estrutura permite organizar pontos problemáticos de acordo com critérios hierárquicos e, através de uma representação simples, captura a essência de um determinado problema por meio da descrição de um problema complexo.

Fazendo uso de uma abordagem de cima para baixo (*top down*) os autores apresentaram áreas específicas a serem tratadas, com relação à segurança da informação, expandindo-as em fatores e subfatores carentes de atenção. Após o desenvolvimento dessa estrutura, um questionário é formulado com questões direcionadas a cada fator ou subfator a ela pertencente. Cada dimensão do protótipo apresenta um peso, conforme sua relevância. Neste caso os autores atribuíram os seguintes pesos: conhecimento (30), comportamento (50) e opinião (20). A soma da média ponderada das questões, pertencentes a cada dimensão, equivale ao percentual de conscientização dos usuários, sendo este percentual comparado aos valores de referência definidos na Tabela 1 (KRUGER; KEARNEY, 2006).

Tabela 1 – Valores de referência para Conscientização em Segurança da Informação

Conscientização	Medida (%)
Boa	80 – 100
Média	60 – 79
Ruim	59 ou menos

Fonte: Adaptado de Kruger e Kearney (2006)

O nível de conscientização obtido permite verificar se a conscientização dos usuários está ou não de acordo com o esperado e fornece indicações de pontos carentes de melhoria, favorecendo a realização de *feedbacks* entre os funcionários e a alta administração. Também auxilia as organizações no controle e no direcionamento de objetivos estratégicos voltados a garantir a segurança da informação. Fazendo uso de um processo simples de coleta de dados com atribuição de valores e combinando técnicas multi-critérios para a resolução de problemas, o modelo permite mensurar quantitativamente o nível de conscientização dos usuários em segurança da informação. Além disso, devido à importância da conscientização no contexto da segurança da informação, o modelo é baseado nos princípios de sustentabilidade, sofisticação e validade científica, o que o torna um modelo base para outros sistemas de medições mais complexos ou mais sofisticados (KRUGER; KEARNEY, 2006).

2.4 O papel da conscientização na efetividade da PSI

O termo conscientização em segurança da informação é utilizado para se referir ao estado no qual os usuários de uma organização estão conscientes ou idealmente comprometidos para com sua missão de manter ou preservar a segurança da informação, sendo esta missão geralmente expressa em guias ou políticas direcionadas ao usuário final.

Apesar de a PSI expressar as intenções da alta administração sobre os quais muitos esforços de segurança da informação são construídos, elas não constituem, por si só, um esforço suficiente de conscientização. Muitos gerentes se enganam em acreditar que tudo o que eles precisam é escrever e publicar uma série de políticas para que o uso consciente da informação aconteça de forma controlada e segura (WOOD, 1997).

Entretanto, assim como as políticas de segurança, por si só, não são suficientes para se garantir a confidencialidade, integridade e a disponibilidade das informações, somente a

aquisição de tecnologias de segurança ou o desenvolvimento isolado de programas de conscientização também não são. O ideal é que as tecnologias de segurança de informação e o controle dos processos organizacionais se complementem um ao outro (YANUS; SHIN, 2007).

Através de Programas de Conscientização em Segurança da Informação – PCSIs, a conscientização visa salientar a relevância de se ter procedimentos adequados nos processos organizacionais e destacar os motivos pelos quais estes procedimentos são tão importantes para a organização (SOLMS; SOLMS, 2004; YANUS; SHIN, 2007). O desenvolvimento destes programas é de fundamental importância para que a segurança da informação seja aplicada de forma eficaz, pois os impactos das falhas causados por profissionais, presentes no ambiente interno das organizações, é maior do que todas as outras fontes de recursos combinadas tais como vírus, hackers, falhas de hardware dentre outras (JOHNSON, 2006).

Muitas das falhas de segurança podem advir do descontentamento de funcionários para com a organização. Entretanto, estas falhas também podem ocorrer porque as pessoas estão inconscientes das ameaças que podem comprometer a segurança das informações; porque contam com mais alguém para a obtenção de seus objetivos; porque não têm as habilidades necessárias para direcioná-los em prol da segurança, ou simplesmente, porque elas acreditam que tem coisas mais importantes para fazer (PAYNE, 2003).

Yanus e Shin (2007) salientam que os PCSIs envolvem educação, treinamento e comunicação e são criados a partir da Política de Segurança da Informação que, por sua vez, é desenvolvida a partir de normas, leis, regulamentos ou padrões, vigentes nas organizações, conforme demonstra a Figura 6.

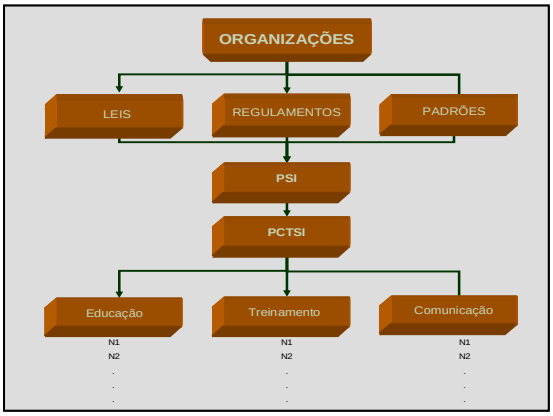


Figura 6 – Criação dos Programas de Conscientização em Segurança da Informação
Fonte: Elaborado pela autora

Siponem (2000) destaca que a educação deve se deter em aumentar a percepção das pessoas com relação a segurança da informação e responder ao questionamento “porque”, enquanto o treinamento deve aumentar as habilidades e a competência das pessoas determinando os procedimentos requeridos para se obter e preservar a segurança e respondendo a questão “como”. Na concepção do autor os usuários não ficarão satisfeitos com respostas do tipo “você deve fazer isto”, “estas são as regras” ou “esta é nossa política” se o questionamento “porque” não for respondido de forma, extremamente relevante.

A comunicação envolve a disseminação do quão relevante é a segurança da informação e as formas de se obtê-la. Deve abranger todos os níveis hierárquicos da organização, sem exceções (HÖNE; ELOFF, 2002). O importante é que as mensagens que a PSI transmite sejam comunicadas de forma que os conceitos, relacionados à segurança da informação, estejam na mente dos usuários e possam ser lembrados sempre que eles se depararem com procedimentos operacionais que exigem sua atenção (JOHNSON, 2006).

2.5 Considerações Complementares

A criação e a implantação de uma PSI são de suma importância para que as organizações manifestem aos funcionários seu interesse em preservar a integridade, a disponibilidade e a confidencialidade das informações a elas pertencentes ou que estão sob sua responsabilidade. Normas e guias de boas práticas salientam a relevância da implantação de uma PSI no ambiente interno das organizações e a apontam como um componente indispensável para que a segurança seja disciplinada adequadamente e os objetivos de negócio possam ser alcançados. Entretanto, a efetividade de uma PSI depende de uma série de fatores: deve estar atrelada ao contexto organizacional e expressar a visão da organização para que se obtenha uma cultura direcionada à segurança da informação.

Conforme demonstram as abordagens de Höne e Eloff (2002), Solms e Solms (2004) e Kruger e Kearney (2006), o simples fato de se implantar uma política de segurança da informação não garante sua efetividade. Atividades, processos ou métodos complementares são necessários à efetividade de uma PSI, seja por atividades que visam dar apoio a sua criação, seja por processos direcionados a cultivar uma cultura organizacional, envolvendo política, educação e cultura. É necessário fazer com que os usuários pratiquem os pressupostos definidos na PSI e socializem-se como forma de se garantir a proteção não

somente das informações, mas também das pessoas que as manipulam. O que se verifica, frente às diferentes concepções, é que as abordagens se complementam ao demonstrarem que a PSI deve estar atrelada a cultura organizacional. Todos os autores são unânimes em apontar a conscientização dos usuários como um fator chave e em salientar a sua relevância para que os controles definidos na PSI possam ser realmente executados, contribuindo para sua efetividade e garantindo o sucesso de uma gestão voltada à segurança da informação.

Neste contexto, a conscientização dos usuários apresenta-se como um fator determinante à efetividade da PSI e está diretamente relacionada à forma com que ela é disseminada no ambiente organizacional, aliada a exposição clara dos motivos que levam a organização a sua criação e posterior implantação. A disseminação de uma PSI, aos diversos níveis da organização, não somente contribui para o aumento da conscientização dos usuários, mas torna-os cientes dos motivos pelos quais é tão importante proteger as informações organizacionais e o que deve ser feito para que isso realmente aconteça.

Para que a PSI seja disseminada, eficientemente, muitas estratégias de marketing têm sido utilizadas. Estas estratégias são aplicadas no ambiente interno das organizações e se direcionam a obtenção da conscientização dos usuários para a conseqüente efetividade da PSI. Portanto, no próximo capítulo abordar-se-ão os pontos relevantes do Marketing Interno, também conhecido como Endomarketing, e as estratégias utilizadas para a obtenção do apoio e colaboração dos usuários na implantação de mudanças organizacionais, como acontece no caso da implantação de uma PSI.

CAPÍTULO 3

ENDOMARKETING

No intuito de se obter um conhecimento mais aprofundado sobre endomarketing, este capítulo apresenta um breve descritivo da evolução histórica do marketing, demonstrando como os preceitos do marketing podem ser aplicados ao ambiente interno das organizações. O capítulo salienta também a importância do endomarketing na implantação de uma PSI, descreve como o marketing pode ser aplicado à área de segurança da informação, segundo a concepção de McLean (1995), e finaliza-se com a apresentação de diferentes técnicas de endomarketing, aplicadas por vários autores da área de segurança.

3.1 Histórico do marketing

Ao longo do tempo as bases que sustentam o marketing passaram por um processo gradual de reestruturação, impostos pelas mudanças decorrentes do avanço da tecnologia e da própria globalização. Devido a esta reestruturação o marketing evoluiu passando de uma prática dedicada exclusivamente ao comércio para uma prática voltada à elaboração de estratégias, capazes de gerar soluções que agreguem valor e que, acima de tudo, mantenham uma postura de relacionamento com o cliente.

Em decorrência das inovações, trazidas pela tecnologia e pela valorização das informações existentes no meio organizacional, o século XX marca o direcionamento do marketing à construção e manutenção de um relacionamento entre empresas e clientes. Na acepção de Mckenna (1999) as empresas adquirem experiências para investir no seu desenvolvimento promovendo “encontros”, seja com clientes, com concorrentes ou com parceiros fornecedores de tecnologia. Estes “encontros” proporcionam a obtenção de

informações através de um monitoramento constante, da análise dos *feedbacks* e da avaliação de suas capacidades internas.

O século XXI é marcado por intensas mudanças, tanto em termos tecnológicos quanto mercadológicos e estas mudanças acarretam impacto nas atitudes e no comportamento dos clientes, fazendo com o que o marketing, praticado nas organizações, direcione-se a ações estratégicas capazes de proporcionar diferenciais competitivos. Para Kotler (2000) o mercado não é mais o mesmo. Ele está mudando radicalmente como resultado de grandes forças, tais como os avanços tecnológicos, a globalização e a desregulamentação. Isso tem criado novos comportamentos e desafios, e são os motivos pelos quais os clientes estão exigindo cada vez mais qualidade e serviços superiores, além de alguma padronização.

Aplicando os mesmos preceitos do marketing na busca pela satisfação de clientes, através do cultivo de relacionamentos benéficos para a obtenção de diferenciais competitivos, o endomarketing direciona-se ao ambiente interno das organizações, preservando os relacionamentos existentes entre as organizações e os indivíduos que as compõem, ou seja, seus próprios funcionários.

3.2 O endomarketing como estratégia de gestão

De modo geral o marketing é uma técnica que direciona suas ações para a satisfação dos seus clientes. Do ponto de vista didático, pode-se afirmar que há várias definições, ferramentas e segmentos que o marketing pode ser utilizado. O marketing interno, também denominado como endomarketing, é uma dessas técnicas (BEKIN, 2005). Ele é direcionado para atender as relações existentes dentro das organizações, isto é, a de seus empregados, independente do segmento da organização ser público, privado, com ou sem fins lucrativos.

A importância dada pelo endomarketing à satisfação dos clientes internos acarreta o aumento da capacidade organizacional para satisfazer os clientes externos. Ao fazer uso da estratégia de endomarketing as empresas passam a construir e perseguir a melhoria de seu relacionamento com os clientes internos, fortalecendo o comprometimento dos mesmos com os objetivos e valores organizacionais. Essa conquista pode garantir a melhoria da qualidade de bens, serviços e produtividade de pessoas, visando à satisfação de seus clientes (BEKIN, 1995).

Na concepção de Cerqueira (2002) endomarketing são “projetos e ações que uma empresa deve empreender para consolidar a base cultural do comprometimento dos seus funcionários com o desenvolvimento adequado das suas diversas tecnologias...”. Para o autor o comprometimento das pessoas é obtido não somente com uma adesão externa, superficial, mas também com uma adesão interna, ou seja, uma reação positiva ao que é proposto. Sendo que esta adesão deve ser feita de forma voluntária a uma idéia, a uma nova ordem ou a uma mudança futura.

O objetivo do endomarketing é manter os colaboradores informados sobre as filosofias, políticas e objetivos da empresa, integrando-os através de programas amplos e abrangentes, assistindo-lhes convenientemente em suas necessidades e aspirações e desenvolvendo esforços para que as pessoas sintam-se orgulhosas, comprometidas por pertencer e colaborarem com a organização através de dinâmicas relações de parceria (PAIXÃO, 2004). Também propõe e dissemina uma série de valores, dentre eles a eficiência, qualidade, comprometimento, cooperação, respeito e criatividade. Pode ser usado para criar e difundir uma linguagem cultural própria e homogênea para a empresa como um todo, tendo como base um conjunto de valores escolhido pelos próprios funcionários, a fim de facilitar os relacionamentos internos (CERQUEIRA, 2002).

Uma das maiores contribuição do endomarketing pode ser a ênfase dada à avaliação e aprimoramento do ambiente interno organizacional. Para tanto, apregoa Bekin (1995), para que isso aconteça o clima organizacional deve estar voltado para a motivação e a valorização do empregado.

Na concepção de Brum (1998) diversos instrumentos operacionais podem ser utilizados na aplicação de uma estratégia de endomarketing, dentre os quais se pode mencionar: vídeos; manuais técnicos e educativos; revistas com histórias em quadrinhos; jornal interno com a utilização de vários encartes; cartazes motivacionais; canais diretos; grife interna; memória; rádio interna; vídeo jornal; intranet; convenções internas etc.

As ferramentas de marketing supramencionadas podem ser empregadas de acordo com a necessidade e disponibilidade da organização, não somente de recursos financeiros, mas também de um maior envolvimento dos atores organizacionais que irão garantir o sucesso das políticas de segurança de informação.

3.3 A relevância do endomarketing na implantação da PSI

A maior dificuldade com que os empresários se deparam ao tentar implantar um modelo de gestão que privilegie a eficiência, como a gestão voltada à segurança, é a resistência dos próprios funcionários aos novos conceitos e técnicas, isto é, a mudança. E quando se fala em Política de Segurança da Informação a mudança é evidente, tendo em vista que ela influencia diretamente na chamada zona de conforto das pessoas, também conhecida como acomodação do ser humano, pois só admite lidar com aquilo que lhe é familiar. Isto faz com que a mudança signifique um grande desafio, haja vista que deverá sair de um estado emocional seguro para outro ainda desconhecido (BARDWICK, 1998).

Entretanto, fatores tecnológicos, ambientais e mercadológicos fazem com que o ambiente organizacional esteja em constante transformação e devido a estes fatores as organizações enfrentam momentos de extrema mudança e revisão de seus processos e suas estratégias de negócio.

Uma mudança organizacional pode ser conceituada como sendo qualquer transformação de natureza estrutural, estratégica, cultural, tecnológica, humana ou de outro componente, capaz de gerar impacto em partes ou no conjunto da organização (WOOD, 2000b). Na concepção de Lima, Miyasaki e Abreu (2003) a mudança pode ser entendida de acordo com seu foco, ou seja, externo ou interno à organização. No primeiro caso, a mudança é imposta de fora para dentro da organização, enquanto no outro, a mudança é causada por contingências resultantes da própria organização.

A adoção de um modelo de gestão voltado à segurança da informação pode ser visto como a manifestação clara, concisa e formalizada da organização em rever seus processos organizacionais, no intuito de se garantir a segurança das informações a ela pertencentes ou que estão sob sua responsabilidade (WOOD, 2000b).

A implantação da PSI, neste contexto, pode ser vista como sendo o estabelecimento de uma estratégia para que a gestão da segurança da informação (GSI) aconteça de forma estruturada e controlada (FONTES, 2006). O que evidencia que tanto a GSI quanto a implantação da PSI caracterizam-se como sendo uma mudança organizacional imposta tanto pelo ambiente interno quanto externo à organização.

O sucesso na adoção de estratégias de mudança envolve compreender aspectos do ambiente, dos indivíduos e da organização como um todo. A identificação de variáveis incrementais ou transformacionais, necessárias à implantação de mudanças, apresenta-se

como uma vantagem à medida que esse conhecimento permite o manejo e a implantação da mudança, o aumento da efetividade organizacional e de sua chance de sobrevivência no mercado (BRESSAN, 2001).

Apesar de todo o esforço em prol da implantação de uma mudança organizacional que preze a qualidade e a produtividade como a gestão da segurança da informação, a resistência a estas mudanças tem sido objeto de preocupação. Muitos estudos tentam identificar como e porque os membros de uma organização reagem às mudanças.

Para Robbins (2002), a resistência as mudanças pode ocorrer em âmbito individual e em âmbito organizacional. No âmbito individual ela relaciona-se às características subjetivas e pessoais dos indivíduos e envolvem aspectos como: hábitos, necessidades, características de personalidade, inseguranças, grau de conhecimento e questões econômicas. No âmbito organizacional a resistência às mudanças encontra-se direcionada a aspectos globais, envolvendo a organização como um todo, e relacionam-se à inércia estrutural e do grupo, ao foco restrito da mudança (ex. mudanças apenas em um determinado setor) e às percepções de ameaça advindas da mudança.

Na perspectiva de Eckes (2001) a resistência tem um sentido bem mais amplo. Para que os indivíduos realmente aceitem a mudança deve-se, no mínimo, demonstrar o que eles podem ganhar com isso:

> (...) um padrão bastante comum entre as pessoas é que a maioria delas associa mudanças a perdas e quando isso acontece, fica claro por que existe resistência às mudanças. Existe até um componente biológico na resistência. O que o corpo faz quando recebe um transplante de coração? Mesmo que esse coração novo e saudável signifique a diferença entre a vida e a morte, o corpo tenta rejeitá-lo (ou seja, resistir a essa mudança), optando pela manutenção do coração velho e doente. Se a mudança está associada à perda, as pessoas só a aceitarão se duas coisas forem mostradas a elas: primeiro, que haja uma necessidade de mudança (senão a organização poderá morrer); segundo, que haja um ganho para o indivíduo afetado pela mudança. Em outras palavras, deve haver um OQEGCI (o que eu ganho com isso), para que o indivíduo resolva ser apoiador da mudança (ECKES, 2001, p. 196).

Embora o raciocínio de Eckes (2001) seja bastante relevante, os indivíduos podem apresentar comportamentos diferenciados frente às mudanças que possam vir a ocorrer no ambiente organizacional. Yousef (2000) reporta que para alguns clientes internos, a mudança pode trazer satisfação, diversão e vantagens, para outros podem trazer estresse e desvantagens; e existem aqueles que nem sequer percebem as mudanças. De uma forma ou outra, mudança organizacional pode impactar no comprometimento do indivíduo para com a organização. Funcionários com alto nível de comprometimento organizacional são mais congruentes com os valores da empresa e por isso no momento de se implantar uma

determinada mudança eles tendem a aceitá-la mais facilmente sem abalar os valores e as metas de base da organização (YOUSEF, 2000).

O endomarketing, utilizado como uma estratégia de gestão propõe que o público interno esteja plenamente informado, motivado e alinhado às novas diretrizes e tecnologias empresariais que são incorporadas com a adoção de um modelo de gestão voltado à segurança, favorecendo a comunicação e os inter-relacionamentos entre os indivíduos. Neste contexto, técnicas de endomarketing como os programas de conscientização e treinamento em segurança da informação são de suma importância, pois servem para informar os funcionários dos riscos na utilização da infra-estrutura de TI da organização e os perigos que eles podem causar. E nesse sentido Solms e Solms (2004) destacam que os usuários não podem ser responsabilizados por problemas relacionados à segurança se os mesmos não sabem quais são estes problemas e o que eles podem fazer para evitá-los.

As estratégias de marketing endereçadas ao público interno da organização, através da aplicação de técnicas de endomarketing visam obter o comprometimento dos mesmos para com a política de segurança. O que se entende sobre o que foi apresentado até o momento, é que as empresas de sucesso atingem e motivam os seus funcionários de forma mais eficiente que as demais e por estarem a par das inovações impostas pela globalização e pelas tecnologias da informação (tais como políticas e normas de segurança), as pessoas estão constantemente preocupadas com o fator mudança e com as conseqüências que ela possa trazer para seus empregos. Devido à dinamicidade de suas atividades o fator comunicação é de suma importância para que elas possam entender “o que fazer” e o “porque fazer” para cultivar um ambiente organizacional voltado à segurança. Ramos (2003) ao se referir a esta questão destaca que um usuário comprometido é um grande aliado, tanto na utilização segura da informação quanto no mapeamento de riscos não identificados. Para ele os usuários são uma cadeia de conhecimento importantíssima formada a partir da conscientização e da educação. Quanto maior for o seu conhecimento maior será sua capacidade de julgamento refletindo em uma postura pró-ativa, madura e coerente (eficiente) frente às suas responsabilidades no processo de segurança.

Uma comunicação integrada com a utilização de ferramentas de endomarketing proporciona as empresas, preocupadas com a questão segurança, um ambiente colaborativo tendo por base a verdade e a transparência administrativa. Os questionamentos oriundos dos funcionários são vistos como merecedores de atenção e de uma resposta coerente. Assim, toda a organização passa a desenvolver esforços para manterem-se bem informadas e conscientes sobre as práticas que devem ser direcionadas à segurança. A comunicação clara e

compreensiva ajuda os empregados a se posicionarem criticamente em relação ao seu trabalho e à empresa como um todo, e mais importante os faz sentirem-se responsáveis pelo futuro da organização a qual pertencem.

3.4 A segurança da informação e seu respectivo marketing mix

No contexto de segurança da informação, autores como Höne e Eloff (2000), Payne (2002) e Peltier (2005) abordam a segurança como sendo um produto/serviço a ser vendido ao cliente interno, ou seja, como uma venda propriamente dita. Peltier (2005) salienta inclusive que muitos profissionais de segurança implementam um "perfeito" programa de segurança da informação e surpreendem-se ao perceberem que o programa falhou porque eles não venderam seu produto/serviço para seus clientes. Na concepção deste autor para se ter sucesso, os profissionais de segurança devem encontrar um modo ou alguma forma de vender seu produto/serviço a seus clientes.

Kevin McLean (1992) foi pioneiro, em adotar os princípios do marketing e a descrever sua aplicação no ambiente interno das organizações com vistas a proteger as informações organizacionais, proporcionando uma melhor conscientização dos usuários e seu conseqüente comprometimento para com as políticas, normas ou preceitos determinados pelas organizações. Na acepção de Siponen (2000), as ações propostas por McLean podem ser muito úteis para a educação em segurança, incentivando positivamente a segurança da informação, desde que elas sejam uma forma de manter a importância da segurança da informação sob os olhos dos funcionários.

No marketing tradicional, o *marketing mix* consiste no conjunto de ferramentas que uma determinada empresa usa para atingir seus objetivos de marketing no mercado-alvo (KOTLER, 2000). O mercado-alvo é definido como o mais homogêneo ou similar grupo de consumidores, sobre os quais uma determinada empresa deseja chamar a atenção (McCARTHY, 1978).

Neste contexto, os 4P's (**P**roduto, **P**reço, **P**osição e **P**romoção) são o conjunto inicial de variáveis que compõem o *marketing mix*. O produto se refere às variáveis determinantes de um determinado produto, tais como, qualidade, características, nome da marca, design, embalagem, tamanhos, serviços, garantias, devoluções etc.; o preço é determinado pelo preço básico, os descontos fornecidos, prazos de pagamentos, condições de crédito etc.; a praça, ou

também denominado ponto de venda, se refere aos canais de distribuição (localizações), distribuição física (estoque), transporte, armazenagem etc; e a promoção está relacionada à venda pessoal, propaganda, promoção de vendas, publicidade, relações públicas, marketing direto (mala direta, telemarketing), dentre outros (McCARTHY, 1978).

Acompanhando a evolução histórica do marketing estas variáveis foram sofrendo adaptações com o passar do tempo, visando não somente a venda de um produto/serviço, mas também a satisfação dos clientes com o estabelecimento de um vínculo capaz de unir empresas e clientes através de relacionamentos benéficos, proporcionando diferenciais competitivos às organizações.

Na acepção de McLean (1995) os pressupostos do *marketing mix* podem ser aplicados, na área de segurança da informação, conforme demonstra a Figura 7.

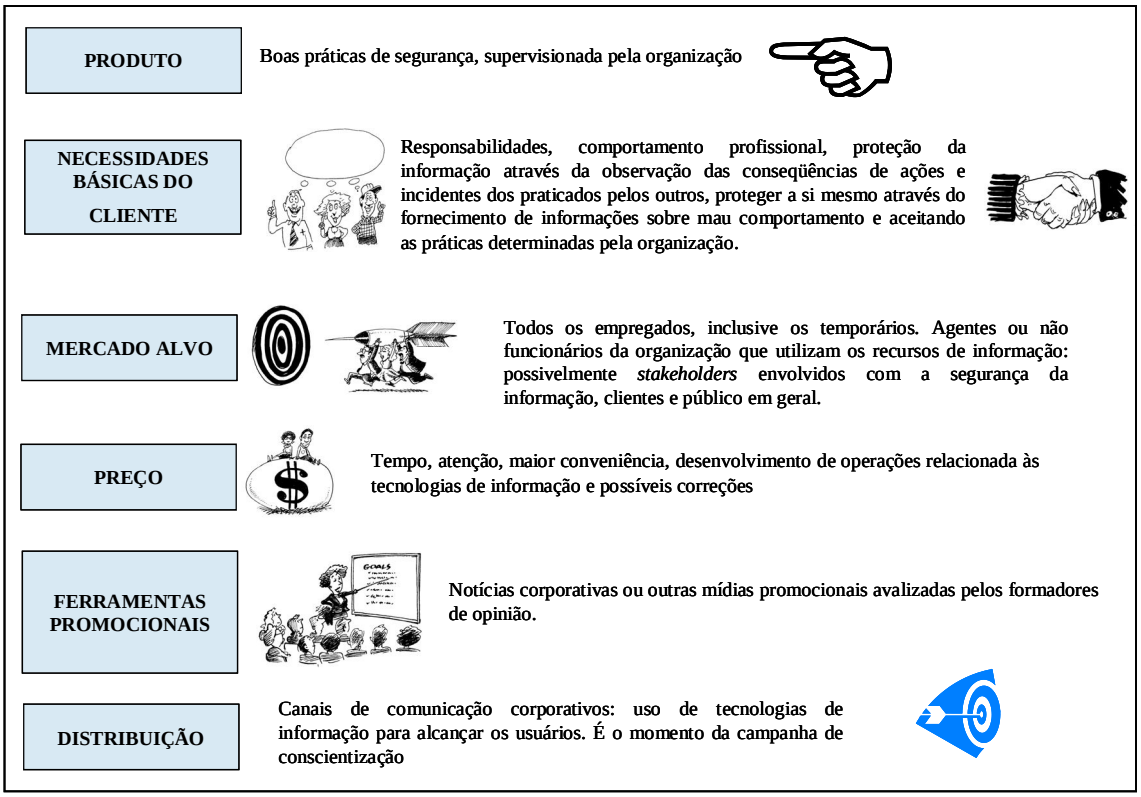


Figura 7 – Marketing Mix direcionado à Segurança da Informação
Fonte: Adaptado de McLean (1995)

O produto refere-se a uma série de objetivos, determinados pela organização, em termos de segurança da informação. A PSI norteia estes objetivos e é a base para que eles sejam alcançados.

As necessidades básicas dos clientes é o que é necessário para se garantir a segurança da informação no meio organizacional. Estas necessidades que determinam o que será "vendido" aos usuários em termos de segurança. Na maioria das organizações os funcionários desconhecem os riscos, relacionados ou não a seu comportamento, que podem comprometer a segurança da informação. Neste caso, uma campanha serve para direcionar mensagens relevantes aos usuários, demonstrando os benefícios de agir proativamente em relação à segurança da informação e alertando os usuários sobre os problemas que podem advir de seu comportamento inadequado para com os recursos de informação.

O mercado alvo envolve todas as pessoas que direta ou indiretamente estão envolvidos ou que, de alguma maneira, são atingidos pelas práticas de segurança determinadas na PSI. Nesse sentido McLean (1995) salienta a importância de dividir o mercado alvo em subgrupos a fim de explorar todo o ciclo de vida que envolve a adoção e difusão da inovação (segurança da informação). Para ele esta segmentação é relevante, pois facilita a identificação e a formação de grupos de pessoas capazes de influenciar o comportamento dos demais funcionários. A identificação destes grupos pode ser feita por meio de reuniões ou por meio de discussões em grupo.

O preço refere-se ao custo do produto/serviço. Ele deve ser claramente entendido por todos para que não haja surpresas ou rejeições aos princípios de segurança. Ele pode variar de indivíduo para indivíduo, por exemplo, com relação aos gerentes de projeto, eles podem precisar investir mais, em termos de esforços, na proteção de recursos técnicos, no controle de processos ou ainda no detalhamento e desenvolvimento de práticas de segurança da informação. No que tange aos usuários de sistemas, muitos podem ter restrições de acesso a certas informações confidenciais ou podem ter poucos recursos para preparar e disseminar informações sensíveis. Entretanto, para a maioria dos usuários, o preço é baixo e representa somente o que é necessário em termos de boas práticas de segurança.

As ferramentas promocionais e a forma de distribuição do material promocional devem ser observadas cuidadosamente. Aspectos como a natureza das mensagens, sua durabilidade, o tamanho e a natureza das audiências, o impacto das mensagens, os tópicos a serem abordados e a expectativa de resposta dos usuários são influenciadas pela escolha e uso das mídias promocionais. A forma de distribuição abrange o uso de técnicas e métodos capazes de chamar a atenção dos usuários. Os profissionais de segurança podem, por

exemplo, utilizar símbolos, humor, repetições ou drama para chamar a atenção de seu público alvo. A utilização destas técnicas pode proporcionar resultados visíveis e imediatos do comportamento dos usuários como mesas limpas e organizadas ou o uso de crachás.

Na acepção de McLean (1995) existem grandes benefícios em se utilizar os princípios de marketing nas questões relacionadas à segurança da informação. O autor salienta que a utilização destes princípios pode contribuir para mudanças comportamentais dos usuários no que tange as práticas de segurança. Segundo o autor as atitudes dos funcionários devem ser condicionadas pela necessidade de se proteger as informações organizacionais, dando espaço para se ouvir a "voz" do cliente interno (funcionário), ou seja, suas opiniões e sugestões. Além disso, deve-se proporcionar o fornecimento de repostas coerentes às suas dúvidas e questionamentos com mensagens capazes de lembrá-los ou advertí-los da importância de se proteger as informações, ou seja, as mensagens devem ser projetadas com o objetivo de conscientizar os usuários da relevância da segurança da informação para a obtenção de objetivos organizacionais.

3.5 Técnicas de endomarketing

As técnicas de endomarketing têm sido amplamente utilizadas por diversos autores, da área de segurança da informação, com vistas a se obter um aumento no nível de conscientização de usuários, contribuindo para a conseqüente efetividade da PSI. Spurling (1995) salienta a importância de métodos direcionados a promover a segurança da informação, no ambiente organizacional, no intuito de se obter o comprometimento dos usuários para com o tema em questão. Para promover a segurança da informação, o autor destaca a importância de campanhas, advertências, vídeos, posters, folders, panfletos dentre outros. No que tange ao comprometimento ele argumenta que é fácil obtê-lo se as pessoas estiverem envolvidas. Reconhecer os problemas relacionados à segurança da informação por parte da organização e o direcionamento de esforços para sua resolução é uma forma de manter os usuários envolvidos.

Para Payne (2003) a prevenção dos problemas relacionados à segurança da informação através da educação e da conscientização pode ajudar a demonstrar a seriedade da segurança da informação aos usuários. Neste contexto a autora salienta a importância da segmentação de

audiências, mencionando métodos efetivos para demonstrar a relevância do tema, tais como apresentações, discussões um-a-um, alertas de segurança, web site dentre outros.

Ferreira e Araújo (2006) corroboram o raciocínio de Payne (2003), no sentido de abranger a conscientização através de programas amplos e em constante aperfeiçoamento ao salientar a importância do treinamento, da publicação e da divulgação das políticas de segurança para que os funcionários estejam preparados para a mudança organizacional em prol da segurança utilizando-se de avisos, comunicações internas, e-mails ou intranet. Os autores salientam que desta forma será possível esclarecer os principais pontos, pertinentes às responsabilidades dos envolvidos, seja por reuniões de conscientização, elaboração de material promocional, treinamento direcionado, peças teatrais ou palestras periódicas de conscientização. Para a disseminação das políticas de segurança os autores supracitados propõem a utilização de diferentes tipos de mídias (aulas presenciais, páginas web, intranet, documentação, apostilas, jornais internos e vídeos); a diferenciação com relação ao treinamento básico, intermediário e avançado. Sublinham ainda para o fato de se orientar os novos funcionários direcionando-lhes informativos sobre as atuais tendências em incidentes de segurança.

Peltier (2005) entende que a utilização de vídeos, cartazes, folders e outras ferramentas promocionais são importantes para que as práticas de segurança, determinadas na PSI, estejam claras para os usuários, mas ressalta também a importância das apresentações, principalmente, no que diz respeito ao estilo das mesmas. O autor afirma que nas apresentações deve-se utilizar uma linguagem acessível aos usuários e de acordo com o contexto organizacional para que haja uma boa comunicação entre os usuários e o apresentador. A forma de falar e o modo de se comportar do apresentador pode comprometer, significativamente, os *feedbacks* dos usuários.

Já Johnson (2006) apresenta métodos distintos dirigidos para a conscientização dos clientes internos, ou seja, dos próprios funcionários e classifica-os em métodos educativos/interativos, informacionais, promocionais e de reforço. O Quadro 1 ilustra as técnicas utilizadas em cada um desses métodos.

MÉTODOS PROMOCIONAIS	MÉTODOS EDUCATIVOS/INTERATIVOS
▪ Eventos/Feiras ▪ Papéis de parede ▪ Banners na intranet ▪ Hiperlinks do site da intranet para o site de segurança ▪ Artigos com publicações internas ▪ Pôsteres ▪ Jogos e quebra-cabeças ▪ Bloco de notas ou adesivos ▪ Camisetas ▪ Xícaras ou copos ▪ Mouse pads	▪ Apresentação de slides ▪ Treinamento ▪ Módulos de treinamento online ▪ Sessões breves ▪ Demonstrações ▪ Vídeos ▪ Workshops
MÉTODOS DE REFORÇO	**MÉTODOS INFORMACIONAIS**
▪ Assinatura dos princípios de segurança ▪ Contrato de confidencialidade ▪ Exames ou testes de conscientização ▪ Ações disciplinares para não conformidades ▪ Avaliações anuais ou critérios de promoção ▪ Mecanismos de recompensa	▪ Folhetos ▪ Pequenos artigos ou novas histórias ▪ Postagens no site de segurança ▪ E-mails de advertência ▪ Guias de segurança da informação ▪ Cartões ▪ Notícias ▪ Dicas de segurança

Quadro 1 – Técnicas utilizadas para a conscientização dos usuários
Fonte: Adaptado de Johnson (2006)

Johnson (2006) ressalta que os métodos educativos/interativos visam criar um comprometimento dos recursos humanos a longo-prazo, no que se refere à compreensão e aplicação dos princípios fundamentais de segurança, enquanto os outros métodos são mais adequados para a execução e reforço das comunicações, ou em direcionar a atenção dos usuários para questões específicas.

Diferentes técnicas têm sido mencionadas e descritas por diversos autores, o Quadro 2 apresenta algumas técnicas utilizadas pelos autores acima mencionados (SPURLING, 1995; PAYNE, 2003; PELTIER, 2005; FERREIRA; ARAÚJO, 2006; JOHNSON, 2006).

Métodos	Spurling (1995)	Payne (2003)	Peltier (2005)	Ferreira e Araújo (2006)	Jonhson (2006)
Mensagens de advertência	X	X			X
Vídeos	X		X	X	X
Folders	X		X	X	X
Panfletos			X	X	X
Posters	X			X	X
Conscientização		X	X	X	
Treinamento		X	X	X	
Segmentação de audiências		X	X	X	
Apresentações		X	X	X	X
Discussões um-a-um		X			X
Site		X			X
E-mail				X	X
Intranet				X	X
Palestras	X	X	X	X	X
Peças teatrais				X	
Jornais internos				X	X

Quadro 2 – Métodos de conscientização utilizados por autores
Fonte: Desenvolvido pela autora

Höne e Eloff (2002) reforçam que os métodos de disseminação da PSI devem estar de acordo com os demais métodos utilizados pela organização. Entretanto, isso não significa que não haja espaço para a criatividade. Deve-se levar em consideração que existem métodos mais simples de serem implementados e mais fáceis de serem aceitos pela organização. Na acepção destes autores um marketing inteligente pode fazer com que usuários lembrem-se da PSI, entendendo-a mais facilmente e aderindo a ela.

Uma campanha interna de divulgação da PSI é um dos fatores que podem contribuir para a implementação e atualização das políticas, pois conforme Wood (2000) as políticas de segurança são, vias de regra, apresentadas como códigos de conduta aos quais os usuários devem se adequar integralmente, entretanto não se vê uma discussão adequada sobre o grau de receptividade dos usuários a estas políticas, nem se apresentam questões sobre o impacto causado por elas sobre o ambiente e sobre o comportamento daqueles que as devem seguir.

Para Payne (2000), tanto a conscientização quanto a educação em segurança da informação são, de certa forma, uma campanha de marketing, na qual certamente os princípios do marketing devem ser aplicados: conhecer as necessidades do cliente, selecionar o produto/serviço adequado para eles, elaborar métodos informacionais a cada grupo de clientes, monitorar o resultado dessas promoções e reformular o produto/serviço se necessário.

3.6 Considerações complementares

O endomarketing é uma estratégia de gestão que utiliza os preceitos do marketing tradicional para se obter o comprometimento e a colaboração dos recursos humanos para com às mudanças a serem implantadas nas organizações, proporcionando a melhoria contínua de seus processos.

Da mesma forma que o marketing tradicional busca a satisfação dos clientes externos, o endomarketing busca a satisfação dos clientes internos, procurando estabelecer com eles um relacionamento benéfico, por meio de relações de parcerias, capazes de fazer com que os objetivos estratégicos da organização sejam alcançados.

Na área de segurança da informação, a aplicação do marketing tradicional, bem como seu respectivo *marketing mix*, nada mais é do que a aplicação de Endomarketing. O Endomarketing é o marketing direcionado ao ambiente interno das organizações e colabora com a gestão de segurança da informação à medida que mantém os usuários informados das práticas necessárias para se proteger as informações organizacionais.

Portanto, o endomarketing aplicado na gestão de segurança da informação agrega qualidade aos processos organizacionais, fortalece a credibilidade das informações que trafegam tanto no ambiente organizacional quanto fora dele e permite que, de posse dessas informações, decisões acertadas e coerentes sejam tomadas de acordo com o contexto de cada organização.

CAPÍTULO 4

CARACTERIZAÇÃO DA PESQUISA

Este capítulo descreve as características do presente estudo com relação à sua natureza, seus objetivos e seus procedimentos técnicos. Descreve também o tipo de amostragem utilizada e a forma de coleta e análise de dados, finalizando-se com a descrição das limitações do presente trabalho.

4.1 Classificação

Quanto à natureza o presente estudo classifica-se como pesquisa quali-quantitativa por integrar aspectos tanto da pesquisa qualitativa quanto da pesquisa quantitativa. Silva e Menezes (2000, p. 20) destacam que a pesquisa quantitativa ”considera que tudo pode ser quantificável, o que significa traduzir em números opiniões e informações para classificá-los e analisá-los” enquanto a “pesquisa qualitativa considera que há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. A interpretação dos fenômenos e atribuição de significados são as premissas básicas no processo qualitativo. Não requer o uso de métodos e técnicas estatísticas”. O ambiente natural é a fonte direta para coleta de dados e o pesquisador é o instrumento-chave. Mattar (1993) advoga que a pesquisa qualitativa procura identificar a presença ou a ausência de algo enquanto a pesquisa quantitativa visa mensurar o quanto este algo está presente. A comunhão entre ambas as pesquisas mostra-se positiva, visto que uma serve de complemento à outra. Sob este aspecto alia-se a representatividade da pesquisa quantitativa e a validade interna da profundidade trazida pela pesquisa qualitativa (RICHARDSON, 1999). Os resultados advindos da pesquisa qualitativa servem de embasamento a uma compreensão inicial, enquanto os resultado

advindos da pesquisa quantitativa dão enfoque à recomendação de uma linha de ação. (MALHOTRA, 2006)

Quanto a seus objetivos o presente estudo classifica-se como uma pesquisa exploratória, descritiva e explicativa. Exploratória porque, a partir do levantamento bibliográfico, tem como escopo proporcionar uma maior familiaridade com o problema, de forma a explicitá-lo ou a construir hipóteses (GIL, 1996). Segundo Marconi e Lakatos (1999, p. 73) "a pesquisa bibliográfica não é mera repetição do que já foi dito ou escrito sobre certo assunto, mas propicia o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras". Descritiva porque, segundo Mattar (1999, p. 85), as pesquisas descritivas ou pesquisas conclusivas descritivas caracterizam-se por possuírem objetivos bem definidos, procedimentos formais, serem bem estruturadas e dirimidas para a solução de problemas ou avaliação de alternativas de cursos de ação e porque na acepção de Silva e Menezes (2000, p. 21) este tipo de a pesquisa "visa descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis, envolvendo o uso de técnicas padronizadas de coleta de dados tais como questionários e observações sistemáticas". Explicativa porque visa identificar os fatores que determinam ou contribuem para a ocorrência de fenômenos, utilizando-se do método experimental (GIL, 1996).

Quanto aos procedimentos técnicos a pesquisa se utiliza do estudo de caso, do método experimental e da pesquisa participante. Yin (2005) destaca que um estudo de caso constitui-se de uma investigação empírica que investiga um fenômeno contemporâneo em seu contexto real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos. Deste modo, o estudo de caso foi utilizado porque os objetivos desta pesquisa concentram-se na análise de experiências empíricas e na associação destas experiências a formulações teóricas consistentemente embasadas, ou seja, a partir da teoria aplicada apresentam-se propostas e condições para a ocorrência ou não de determinadas situações.

No que tange ao método experimental, a pesquisa o utiliza por fazer parte de um tipo de pesquisa de campo que consiste em investigações empíricas cujo objetivo principal é o teste de hipóteses que dizem respeito a relações de causa e efeito (MARCONI; LAKATOS, 2003). Sua utilização justifica-se também à medida que este tipo de pesquisa oferece uma contribuição valiosa ao introduzir a clareza do pensamento científico às investigações e ao processo decisório (DIAS, 2003).

Finalmente, no que se refere à pesquisa participante, que parte da interação direta com os membros das situações investigadas e permite o estudo profundo da situação a ser

abordada (SILVA; MENEZES, 2000), a pesquisa prevê confrontar grupos de participantes para realizar um estudo profundo das questões sobre análise.

4.2 Amostragem

Para a realização da pesquisa de clima, da avaliação do nível de conscientização dos usuários para com o tema segurança da informação, bem como para a verificação do entendimento da PSI uma amostra probabilística casual simples foi utilizada, na qual, segundo Marconi e Lakatos (2003) cada elemento da população tem oportunidades iguais de ser incluído na amostra.

No que tange a realização do experimento (aplicação de técnicas de endomarketing) optou-se por utilizar uma amostra não probabilística intencional. Marconi e Lakatos (2003) relatam que este tipo de amostra envolve a escolha intencional do pesquisador. Mattar (1996) esclarece que a suposição básica de uma amostra intencional é que, com bom julgamento e estratégia adequada, podem ser escolhidos os casos a serem incluídos nas mesmas e, assim, chegar a amostras que sejam satisfatórias para os resultados da pesquisa. O experimento foi realizado com dois grupos de 8 profissionais, um recebendo estímulos de técnicas de endomarketing e outro recebendo apenas um nivelamento inicial.

4.3 Coleta e análise de dados

Com relação às técnicas de coletas de dados, para a realização do presente estudo, optou-se pela observação direta extensiva adotando as seguintes técnicas como as mais indicadas para a investigação: pesquisas de campo, bibliográficas, documentais, *checklists* e questionários estruturados. De posse dos dados, foram elaboradas tabelas, gráficos, validações, comentários e análises dos resultados, para um melhor entendimento do problema e proposição de soluções. Na acepção de Lakatos e Marconi (1991), as técnicas referem-se à parte prática da coleta de dados e apresentam duas grandes divisões: documentação indireta, a qual diz respeito à pesquisa documental e bibliográfica e a documentação direta, a qual está

relacionada à observação, a instrumentos como questionários, entrevistas e testes, considerando-se um universo delimitado.

Para a correta análise e tabulação dos dados, advindos da aplicação dos questionários e do *checklist* de auditoria, foi utilizado o software Sphinx Plus, e para o desenvolvimento dos gráficos utilizou-se o software Excel.

4.4 Limitações da dissertação

A presente pesquisa restringe-se a áreas específicas do Hospital Universitário de Santa Maria – HUSM, ou seja, às Unidades de Cardiologia Intensiva (UCI) e Terapia Intensiva-Adulto (UTI), não tendo por propósito abranger todas as unidades e setores pertencentes ao referido hospital, tendo em vista que isso comprometeria o cronograma da pesquisa, bem como aspectos relacionados a questões financeiras. A pesquisa também não pretende abordar todas as técnicas de endomarketing existentes. As técnicas utilizadas foram escolhidas de acordo com a necessidade e viabilidade econômica da instituição, além disso, as técnicas utilizadas foram viáveis por não necessitarem de um grande envolvimento dos profissionais, alocados nas unidades, o que poderia comprometer as atividades desempenhadas nas unidades e que são direcionadas aos cuidados da saúde de pacientes. Apesar de o presente trabalho caracterizar-se também como uma pesquisa descritiva, ele não tem por objetivo propor generalizações, pois diferentes organizações possuem contextualizações distintas de acordo com suas particularidades e as características dos diversos setores a elas pertencentes. As conclusões deste trabalho concentram-se nas peculiaridades pertinentes às unidades em que foi realizado o estudo.

O esclarecimento dessas limitações faz-se necessário para que os objetivos, definidos na pesquisa, pudessem ser plenamente alcançados.

CAPÍTULO 5

O CASO HUSM - UFSM

Este capítulo descreve o ambiente de aplicação do estudo e a descrição dos procedimentos metodológicos realizados para o desenvolvimento desse trabalho. Neste capitulo é apresentado detalhadamente o plano de ação desenvolvido para a realização deste estudo, a forma como foram realizadas as pesquisas de clima organizacional, de conscientização e entendimento da PSI e como foi realizado e experimento no qual foram aplicadas as técnicas de endomarketing.

5.1 O contexto do HUSM-UFSM e das Unidades foco do estudo

A organização alvo de aplicação desta dissertação é o Hospital Universitário de Santa Maria - HUSM. Esta instituição com mais de 30 anos de atuação estabelece-se, hoje, como um Centro de Ensino, Pesquisa e Assistência no âmbito das Ciências da Saúde no estado do Rio Grande do Sul, prestando serviços de excelência na área da saúde e abrangendo no total mais de 100 municípios. Caracterizando-se se como um hospital escola, o HUSM apresenta-se como um 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. Essas características permitem o desenvolvimento de atividades curriculares aliando teoria e prática, o que favorece o aprendizado especializado nas mais diversas áreas da saúde.

O HUSM é único hospital da região central do estado do Rio Grande de Sul que atende pelo Sistema Único de Saúde (SUS), fornecendo a todos seus usuários uma diversidade de serviços especializados em 28 áreas, constituindo-se de uma equipe com 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.

Em função das novas diretrizes expedidas pelo Ministério da Saúde e pela Secretaria Executiva do Departamento de Informação e Informática do SUS, os quais são responsáveis pela promulgação do documento que compõe a Política Nacional de Informação e Informática em saúde, a direção do hospital aprovou a realização deste trabalho, embora já houvesse demonstrado anteriormente motivação e interesse em trabalhar a segurança da informação, demonstrando sua preocupação para com as informações a ela pertencentes ou que estão sob sua responsabilidade e que em sua grande maioria referem-se a dados clínicos de pacientes.

A Política Nacional de Informação e Informática em saúde é composta de 19 diretrizes que se referem aos aspectos de tratamento das informações e pesquisa em informática na saúde, visto que uma de suas principais diretrizes é “Dotar a área da saúde de instrumentos jurídicos que a capacite assegurar a confidencialidade, a privacidade e a disponibilidade dos dados e das informações garantindo sua integridade” (Política Nacional de Informação e Informática em Saúde, 2004), o documento reforça ainda mais a necessidade de realizar ações em prol a segurança da informação.

Devido ao HUSM abranger muitos segmentos setoriais os quais se subdividem em 28 serviços, decidiu-se, conjuntamente com os membros da Direção, realizar a presente pesquisa junto as Unidades de Cardiologia Intensiva (UCI) e de Terapia Intensiva - Adulto (UTI), por serem consideradas unidades vitais para a organização.

A UCI é uma unidade composta por quatro leitos. É 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 composta de nove leitos. Esta unidade tem suas origens nas salas de recuperação pós-anestésica (RPA), onde pacientes submetidos a procedimentos anestésico-cirúrgicos têm suas funções vitais (respiratória, circulatória e neurológica) monitoradas e sob as quais são instituídas medidas de suporte, quando necessário, até que os efeitos residuais dos agentes anestésicos sejam controlados. A unidade é responsável por oferecer suporte

avançado à vida de pacientes que estão intensamente doentes e para isso conta com 40 profissionais das mais diversas áreas.

Apesar das duas unidades terem funções específicas e distintas em seus objetivos, uma complementa a outra, sendo os recursos materiais e humanos compartilhados por ambas. Desta maneira a implantação da PSI, bem como a aplicação de técnicas de endomarketing contempla, num primeiro momento, as duas unidades. Entretanto, durante o desenvolvimento da pesquisa, a aplicação destas técnicas é direcionada apenas à Unidade de Cardiologia Intensiva, ficando a outra unidade sem receber estímulos por meio de técnicas de endomarketing.

5.2 Descrição de procedimentos metodológicos

A Figura 8 permite visualizar os procedimentos realizados para se avaliar o impacto da utilização de técnicas de endomarketing na efetividade da PSI. Os detalhes referentes a cada um destes procedimentos são apresentados nas seções subseqüentes.

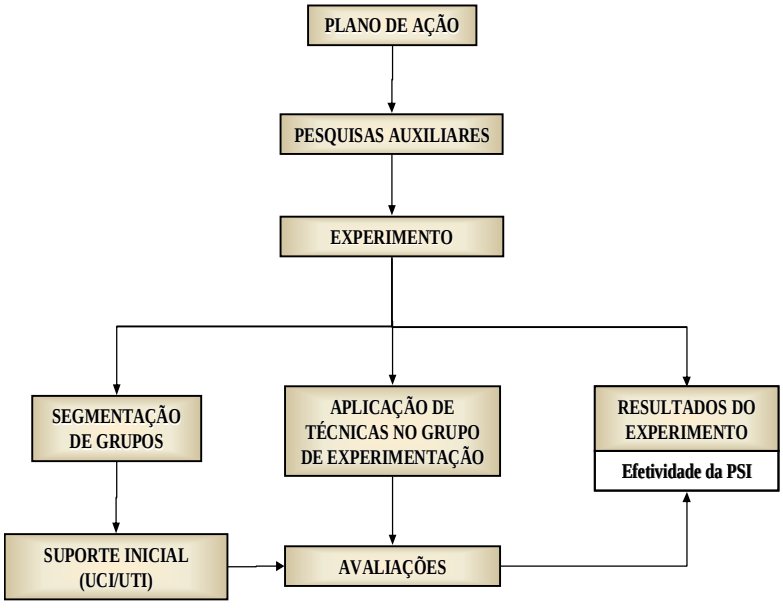


Figura 8 – Procedimentos executados para o desenvolvimento da pesquisa

5.2.1 Plano de Ação

O plano de ação foi desenvolvido para que houvesse um direcionamento das atividades que deveriam ser realizadas para a concretização do projeto como um todo. Para o desenvolvimento da estrutura do plano de ação foi utilizada a ferramenta 5W2H, que segundo Oliveira (1996) é uma das ferramentas da qualidade e serve como referência às decisões, permitindo que seja feito o acompanhamento do desenvolvimento do projeto. O plano de ação é um documento que, de forma organizada identifica as ações e responsabilidades pela sua execução. Esta ferramenta denomina-se 5W2H por fazer referência aos seguintes questionamentos: **Why** - Por que deve ser executada a tarefa ou o projeto (justificativa); **What** - O que será feito (etapas); **How** - Como deverá ser realizada cada tarefa/etapa (método); **Where** - Onde cada tarefa será executada (local); **When** - Quando cada uma das tarefas será executada (tempo); **Who** - Quem realizará as tarefas (responsabilidade); **How much** - Quanto custará cada etapa do projeto (custos) - (opcional).

Todas as atividades, descritas no plano de ação, foram definidas com o amparo teórico de autores renomados da literatura existente e podem ser visualizadas no Apêndice A.

5.2.2 Pesquisas Auxiliares

As pesquisas auxiliares foram realizadas por seus resultados servirem de subsídios para que o experimento pudesse ser realizado. Compreendem as pesquisas auxiliares: a Pesquisa de Clima Organizacional, a Pesquisa de Conscientização dos Usuários em Segurança da Informação e a Pesquisa de Entendimento da Política de Segurança da Informação.

A pesquisa de clima organizacional foi realizada com o intuito de se conhecer o ambiente interno das unidades e as necessidades e anseios dos profissionais nelas alocados. Do ponto de vista teórico Bispo (2006) advoga que a pesquisa de clima organizacional tem sido bastante utilizada por ser um instrumento valioso para o sucesso de programas voltados a melhoria da qualidade, aumento da produtividade e adoção de políticas internas. Para a realização da mesma, foi elaborado um questionário(Apêndice A), com 20 questões, no qual utilizou-se uma escala *Liket* com 5 níveis escalares variando de “muito baixo” a “muito alto”,

sendo avaliadas as seguintes variáveis, existentes no ambiente interno da organização: motivação, imagem interna, qualidade e produtividade e comunicação.

A pesquisa de conscientização dos usuários foi realizada seguindo o modelo proposto por Kruger e Kearney (2006). Este modelo permite uma avaliação em três dimensões: conhecimento, comportamento e opinião dos usuários, seguindo uma estrutura em forma de árvore, denominada estrutura analítica do processo, na qual são demonstrados os fatores relevantes a serem abordados na conscientização em segurança da informação. Esta avaliação foi realizada por proporcionar uma indicação geral do comportamento dos usuários no que tange a seu conhecimento, comportamento e opinião para com o tema segurança da informação. A figura 9 ilustra a estrutura analítica do processo da pesquisa de conscientização. Esta estrutura permite que um problema complexo (Ex. segurança da informação) seja desmembrado em problemas menores (fatores) para que problemas específicos sejam detectados (sub-fatores). Assim, fatores relevantes no que tange a segurança da informação são desmembrados em sub-fatores, os quais servem de base para a elaboração da pesquisa de conscientização (Apêndice D).

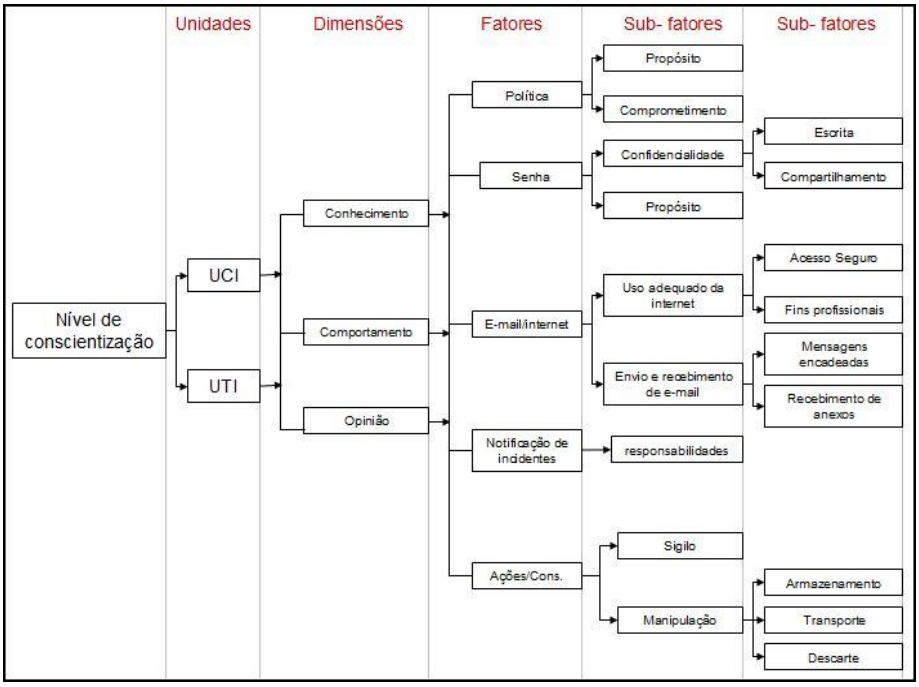


Figura 9 – Estrutura Analítica do Processo
Fonte: elaborada pela autora

No que tange à pesquisa de entendimento da PSI, ela foi realizada, seguindo as recomendações de Höne e Eloff (2002) no intuito de se verificar se os funcionários entenderam corretamente os pressupostos determinados na PSI e para que as dúvidas oriundas dos mesmos não comprometessem a efetividade da PSI. Para sua realização utilizou-se uma um questionário (Apêndice E) com a adoção de uma escala *Likert* com três níveis escalares (baixo, regular e alto), no qual os respondentes demonstram seu entendimento com relação aos procedimentos definidos na PSI para se resguardar a segurança das informações existentes no ambiente interno de ambas as unidades (UCI/UTI), respondendo também questões relacionadas ao conteúdo abordado e a clareza da PSI, bem como a forma de apresentação da mesma.

5.2.3 O Experimento

Para a realização do experimento foi constituído um grupo de experimentação e um grupo de controle. Marconi e Lakatos (2003) salientam que o grupo de experimentação é aquele sobre o qual é efetuada a manipulação das variáveis de interesse que se deseja medir, na qual o pesquisador deseja observar as suas conseqüências, sejam elas esperadas ou não. O grupo de controle por sua vez, fica isento da interferência do pesquisador, não recebendo nenhum estímulo intencional e servindo de padrão à comparação com o grupo experimental.

5.2.4 Segmentação de Grupos

Tanto o grupo de experimentação quanto o grupo de controle foram constituídos de profissionais alocados na Unidade de Cardiologia Intensiva (UCI) e na Unidade de Terapia Intensiva-Adulto (UTI) do Hospital Universitário de Santa Maria - HUSM.

Cada grupo foi formado por 8 (oito) profissionais, selecionados de tal forma que não estivessem alocados nas unidades concomitantemente e que as funções por eles desempenhadas estivessem relacionadas aos cuidados da saúde de pacientes, o que possibilitou um melhor acompanhamento dos profissionais diretamente envolvidos no estudo, caracterizando, portanto, a utilização de uma amostra não probabilística intencional.

A segmentação de grupos foi necessária para que posteriormente técnicas de endomarketing pudessem ser aplicadas sob o grupo de experimentação enquanto o grupo de controle somente foi objeto de observação, permitindo a comparação de resultados entre ambas as unidades.

Devido à proximidade existente entre as unidades foco do estudo (UCI e UTI são localizadas lado a lado no HUSM), para que houvesse um melhor isolamento da amostra optou-se por não informar os profissionais alocados nas unidades a que grupo cada um pertencia.

5.2.5 Suporte Inicial (UCI/UTI)

Tanto os profissionais da UCI quanto da UTI, receberam um suporte inicial (Quadro 3) com o direcionamento de técnicas de endomarketing a ambas as unidades para que compreendessem os pressupostos de segurança da informação adotados pela organização, pois segundo Ferreira e Araújo (2006) esses procedimentos iniciais são necessários para que haja um nivelamento de conhecimento entre os profissionais.

AVALIAÇÕES	TÉCNICAS APLICADAS
1ª Avaliação (Diagnóstico Inicial) Outubro/2008	**Técnicas aplicadas tanto no grupo de controle quanto no grupo de experimentação** ▪ Folders e cartazes de divulgação do projeto de Segurança da Informação; ▪ Conscientizaço e treinamento em Segurança da Informação ▪ Assinatura de termo de responsabilidade e Confidencialidade ▪ Oficina sobre Bioética e Privacidade ▪ Informações sobre atualizações da PSI ▪ Feedback em caso de dúvidas ▪ Disponibilização da política impressa e on-line ▪ Disponibilização de informações no site da GSI,
2ª Avaliação Novembro/2008	**Técnicas aplicadas somente no grupo de experimentação** ▪ Disponibilização de Kits contendo a PSI na forma impressa e conteúdo explicativo sobre o projeto de Segurança da Informação (folders) com logotipo e slogan do projeto; ▪ Alertas de advertência; ▪ Reuniões individuais com os componentes do grupo; ▪ Demonstração do conteúdo disponibilizado no site da Gestão de Segurança da Informação (GSI); ▪ E-mails informativos para esclarecimentos de dúvidas relacionadas a Gestão de Segurança da Informação e a Política de Segurança da Informação (PSI); ▪ Acompanhamento funcional para a realização correta dos procedimentos descritos na PSI.
3ª Avaliação Dezembro/2008	▪ Lembretes da Política de Segurança da Informação (PSI); ▪ Caixa de sugestões para o reporte de incidentes de segurança da informação e sugestões de melhorias; ▪ E-mails informativos para esclarecimentos de dúvidas relacionadas a Gestão de Segurança da Informação e a Política de Segurança da Informação (PSI); ▪ Brindes de fim de ano com lembretes de segurança da informação;

Quadro 3 - Continuação

AVALIAÇÕES	TÉCNICAS APLICADAS
4ª Avaliação Janeiro/2009	▪ Reuniões individuais com os componentes do grupo; ▪ Divulgação de atualizações realizadas no site da GSI; ▪ E-mails informativos para esclarecimentos de dúvidas relacionadas a Gestão de Segurança da Informação e a Política de Segurança da Informação (PSI); ▪ Acompanhamento funcional para a realização correta dos procedimentos descritos na PSI.
5ª Avaliação Fevereiro/2009	▪ Acompanhamento funcional para a realização correta dos procedimentos descritos na PSI. ▪ Reuniões individuais com os componentes do grupo; ▪ Divulgação dos percentuais de adesão da PSI;
6 ª Avaliação (Diagnóstico Final) Março/2009	▪ Reuniões individuais com os componentes do grupo; ▪ Alertas de advertência; ▪ Divulgação de atualizações no site da PSI; ▪ E-mails informativos para esclarecimentos de dúvidas relacionadas a Gestão de Segurança da Informação e a Política de Segurança da Informação (PSI); ▪ Acompanhamento funcional para a realização correta dos procedimentos descritos na PSI.

Quadro 3– Cronograma e técnicas aplicadas
Fonte: elaborado pela autora

Conforme demonstra o Quadro 3, foram aplicadas nas referidas unidades as seguintes técnicas de endomarketing: disponibilização de folders e cartazes sobre o projeto de segurança da informação a ser implantado nas unidades (Apêndices J, K e L); conscientização e treinamento em segurança da informação para que os profissionais tivessem um embasamento teórico no que se refere aos conceitos fundamentais sobre o tema segurança da informação (conscientização), bem como os procedimentos necessários para a manipulação de informações de forma controlada e segura (treinamento); assinatura do termo de responsabilidade e confidencialidade para que se comprometem para com a execução dos procedimentos definidos na PSI (Apêndice A); oficina de bioética e privacidade na qual os profissionais contaram com a participação de profissionais externos à organização para percebessem como a segurança da informação estava sendo tratada em outros ambientes organizacionais, informações sobre as atualizações feitas na PSI (Apêndice M); *feedback* em caso de dúvidas para que os questionamentos oriundos dos profissionais fossem imediatamente esclarecidos; disponibilização da PSI de forma impressa e online (Apêndice A e R) para que os usuários tivessem opções de acesso a mesma, bem como informações no site da gestão de segurança da informação (GSI) sobre a PSI e sobre o projeto de segurança da informação como um todo.

5.2.6 Avaliação da Efetividade da PSI

A avaliação da efetividade da PSI foi realizada por meio de auditorias internas, a fim de verificar se os procedimentos determinados na PSI estavam realmente sendo executados e demonstrar o impacto da utilização das técnicas de endomarketing para a efetividade da PSI. Kruger e Kearney (2006) advogam que as auditorias internas são fontes válidas e colaboram para a observação visto que o comportamento dos usuários pode não ser mensurado corretamente somente com o uso de questionários, pois os mesmos podem não falar a verdade quando respondem sobre seu comportamento, mas o uso de questionários é aceitável porque nem todos os respondentes mentem e porque, geralmente, eles fornecem uma indicação do comportamento dos usuários.

Assim para a realização das auditorias internas foi constituído um grupo composto por seis auditores, sendo dois membros do Comitê Gestor de Segurança da Informação, dois profissionais pertencentes ao quadro funcional do HUSM-UFSM e dois pesquisadores independentes. As auditorias foram feitas no final de cada mês, possibilitando a comparação dos períodos anterior e posterior à aplicação de técnicas de endomarketing usadas para a sensibilização do grupo de experimentação (UCI), visando à medição da efetividade do PSI. Foram objeto das auditorias internas procedimentos referentes tanto o ambiente convencional quanto ao computacional (vide Tabela 2), sendo estes procedimentos classificados pelos auditores na forma percentual seguindo-se os seguintes critérios: Procedimentos Não-Executados (PNEs); Procedimentos Parcialmente Executados (PPEs) e Procedimentos Totalmente Executados (PTEs). Classificam–se como PNEs aqueles procedimentos em que sua execução, por parte dos profissionais das unidades, não estavam em conformidade com os procedimentos referenciados na PSI. No que tange aos PPEs, classificam-se neste critério os procedimentos verificados que estavam parcialmente em conformidade com os procedimentos descritos na PSI. Finalmente, no que se refere aos PTEs, são classificados segundo este critério aqueles procedimentos totalmente em conformidade com os procedimentos definidos na política de segurança da informação.

Tabela 2 – Procedimentos verificados nas auditorias internas

AMBIENTE CONVENCIONAL	AMBIENTE COMPUTACIONAL
▪ Exposição de documentos em locais inadequados	▪ Uso de e-mail profissional
▪ Organização e armazenamento de documentos de acordo com o leito do paciente	▪ Utilização de internet para fins profissionais
▪ Exposição de documentos na impressora	▪ Não compartilhamento de senhas
▪ Descarte adequado de informações	▪ Uso de senhas fortes
▪ Sigilo de informações confidenciais	▪ Bloqueio do PC
▪ Acesso às unidades por profissionais identificados	▪ Backup de informações importantes
▪ Utilização de recursos de informação por profissionais autorizados	▪ Descarte adequado de informações
▪ Notificação de incidentes	▪ Utilização de antivírus

Para a realização das auditorias internas utilizou-se como instrumento de coleta de dados um *checklist,* o qual permitiu a verificação da conformidade do comportamento dos usuários (componentes dos grupos) à PSI. Segundo Graff e Wyck (2003) a utilização de *checklists* reduz a probabilidade de se omitir fatores chaves de segurança e, além disso, provêem uma lista de critérios quantificáveis.

5.3 Considerações Complementares

Como o endomarketing visa a ampla valorização do cliente interno (funcionário), neste caso de estudo a aplicação de técnicas de endomarketing, tanto as direcionadas ao grupo de controle (só com nivelamento inicial) quanto àquelas direcionadas exclusivamente ao grupo de experimentação, teve como base os resultados advindos das pesquisas auxiliares, as quais demonstram as opiniões e sugestões relatadas pelos próprios funcionários das unidades estudadas, valorizando-se assim o cliente interno.

A medição da efetividade da PSI e a avaliação do impacto do endomarketing nesta efetividade são realizadas pela comparação de seis avaliações. Na primeira avaliação (diagnóstico inicial),

são direcionadas técnicas de endomarketing a ambas as unidades para que as mesmas recebam estímulos iniciais para a execução correta dos procedimentos descritos na PSI. Da segunda a sexta avaliação (diagnóstico final) a continuidade dessas técnicas é direcionada exclusivamente sobre o grupo de experimentação (UCI) a fim de se verificar se os profissionais executam esses procedimentos em decorrência do recebimento ou não de um conjunto de estímulos. O comparativo entre as avaliações realizadas no grupo de experimentação (UCI) e o grupo de controle (UTI) demonstram se a aplicação de técnicas de endomarketing são realmente relevantes para a efetividade da PSI, bem como o impacto decorrente da sua aplicação.

CAPÍTULO 6

APRESENTAÇÃO E ANÁLISE DE RESULTADOS

Este capítulo foi reservado para demonstrar a análise e apresentação dos resultados advindos da realização desta pesquisa. Primeiramente, são apresentados os resultados da pesquisa de clima organizacional, partindo-se em seguida para a pesquisa de conscientização dos usuários, a pesquisa de entendimento da PSI e finalizando com a apresentação dos resultados da avaliação da efetividade da PSI, após a aplicação de técnicas de endomarketing.

6.1 Pesquisa de clima organizacional

Para a realização da Pesquisa de clima organizacional foi disponibilizado um questionário aos profissionais (apêndice C), dos quais obteve-se um retorno de 45,7% dos mesmos. Conforme mencionado no capítulo anterior, esta pesquisa abordou aspectos relacionados à motivação, imagem interna, qualidade e produtividade e comunicação, conforme explicitados no Quadro 4. Para a elaboração do questionário foi utilizada uma escala do tipo *Likert* de 5 pontos, com níveis escalares variando de "muito baixo" (1) a "muito alto" (5). A análise de cada aspecto é demonstrada nas subseções que seguem.

Motivação	Relação com o trabalho, Espírito de equipe, Padrões de liderança, Comprometimento com a mudança.
Imagem Interna	Relacionamento com o público interno, Ambiência organizacional.
Gestão de Recursos Humanos	Treinamento e desenvolvimento
Qualidade /Produtividade	Qualidade e Produtividade
Comunicação	Processo de Informação e Canais de Comunicação

Quadro 4 – Aspectos pesquisados e analisados na Pesquisa de Clima Organizacional

6.1.1 Motivação

O estudo da motivação abordou questões que envolvem a relação dos profissionais com o trabalho, o trabalho em equipe, os padrões de liderança existente nas unidades e o comprometimento com as mudanças implantadas, as quais podem ser visualizadas no Apêndice C.

Conforme demonstrado na tabela 3, a análise das questões revelou uma alta concentração nos níveis de satisfação **“alto”** e **“muito alto”**, que somados refletem os seguintes percentuais: entusiasmo dos funcionários quando comparado a quando eles ingressaram nas unidades – ENTU (40,5%); a função desempenhada pelos profissionais nas unidades – TRA (65,6%); utilização conhecimentos para a realização de tarefas – CONHEC (78,2%); empenho empregado para a realização de tarefas – EMP (90,7%); vontade dos profissionais em solicitar ou oferecer ajuda aos colegas de trabalho - OFEAJ (87,6%); cooperação para que resultados sejam atingidos – COOP (46,9%); clima de cooperação entre as unidades – CLCOOP (50,0%), relacionamento profissional ou informal com colegas de outras áreas – RELAC (78,1%); recebimento de informações do superior imediato para o bom desempenho do trabalho – IBDTR (87,6); disponibilização, pelo superior imediato, de tarefas claras a serem cumpridas – DISP (53,1%); reconhecimento de o superior imediato ser uma referência em nível profissional de forma a confiar, totalmente, nas decisões por ele tomadas – RECO (56,2%); sentir-se a vontade na presença do diretor da área - SEVOT (56,2%); recebimento de informações sobre as mudanças ocorridas nas unidades – MUDAN (43,7%); condução de atividades, pelo superior imediato da área na qual trabalha, de acordo com as mudanças e as decisões corporativas tomadas pela unidade – CONDAT (50,0%); considerar

positivas as mudanças que acontecem nas unidades - CPOMUD (56,3%); acreditar que seu trabalho contribui para que as mudanças tenham resultados positivos – STCMU (75,0%); valorização da segurança das informações, ou seja, o sigilo das informações estratégicas e confidenciais – VSINF (37,5%); colaboração para que as mudanças, implementadas nas unidades, tenham resultado satisfatório – COLMUD (68,8%).

Tabela 3: Análise do aspecto Motivação

Escala / Variável	Muito Baixo	Baixo	Regular	Alto	Muito Alto
ENTU	6,3	21,9	31,3	28,1	12,4
TRA	0,0	12,5	21,9	43,7	21,9
CONHEC	0,0	6,2	15,6	56,3	21,9
EMP	0,0	0,0	9,3	43,8	46,9
DISTR	12,5	25,0	28,1	21,9	12,5
OFEAJ	0,0	3,1	9,4	43,8	43,8
COOP	3,1	9,4	40,6	15,6	31,3
CLCOOP	6,3	18,7	25,0	34,4	15,6
RELAC	0,0	6,3	15,6	56,3	21,8
IBDTR	9,4	3,0	25,0	43,8	18,8
DISP	6,3	3,1	37,5	34,4	18,7
RECO	6,3	12,5	25,0	34,3	21,9
SEVOT	9,4	6,3	28,1	40,6	15,6
MUDAN	0,0	12,5	43,8	28,1	15,6
CONDAT	9,4	12,5	28,1	40,6	9,4
CPOMUD	3,1	3,1	37,5	37,5	18,8
STCMU	0,0	0,0	25,0	53,1	21,9
VSINF	3,1	21,9	37,5	18,8	18,7
COLMUD	0,0	3,1	28,1	40,6	28,2
Conjunto (%)	3,9	9,5	27,0	37,7	21,9

Fonte: Pesquisa da autora

A análise individual das questões apresentadas na Tabela 3 demonstra pontos de melhoria a serem estabelecidos, devido a concentração existente no nível “baixo/muito baixo” no que diz respeito à satisfação dos profissionais com relação a distribuição do trabalho entre as pessoas na área em que atuam – DISTR (37,5%) e também a alta concentração no nível “regular” de satisfação no que se refere ao recebimento de informações sobre as mudanças ocorridas nas unidades - MUDAN (43,8%) e a colaboração da equipe para que as mudanças implantadas tenham resultados satisfatórios – COLMUD (37,5%). Já a análise conjunta dos aspectos relacionados ao grupo motivação demonstrou índices positivos,

concentrando-se nos níveis de “alto” (37,7%) e “muito alto” (21,9%), apontando que 59,6 % dos profissionais encontram-se motivados

6.1.2 Imagem Interna

O foco do aspecto imagem interna foi verificar a satisfação dos funcionários para com o ambiente interno das unidades (Apêndice C). Conforme demonstra a Tabela 4, com relação a este aspecto verificou-se uma concentração nos níveis “alto/muito alto”, que somados apresentam os seguintes percentuais: 37,5% acreditam que a unidade se preocupa em estabelcer uma relação de proximidade com seus colaboradores - RELPR; 59,4 % sentem-se parte da unidade a ponto de comemorar com suas vitórias - SAVUN; 37,5 % sentem uma preocupação por parte das unidades com o bem estar de seus colaboradores - BECOL, ou seja, com a qualidade de vida dos mesmos; 53,1% sentem vontade de ir trabalhar na unidade todos os dias - VITRA e 53,1% acreditam existir um clima agradável e prazeiroso na unidade em que trabalham - CLAPR.

Tabela 4: Análise do aspecto Imagem Interna

Escala Variável	Muito Baixo	Baixo	Regular	Alto	Muito Alto
RELPR	3,1	9,4	50,0	18,8	18,7
SAVUN	0,0	0,0	40,6	37,5	21,9
BECOL	9,4	18,7	34,4	28,1	9,4
VITRA	6,3	3,1	37,5	40,6	12,5
CLAPR	9,4	6,3	31,2	34,3	18,8
Conjunto	5,6	7,5	38,8	31,9	16,3

Fonte: Pesquisa da autora

A análise individual dessas questões também demonstrou altos índices de percentuais no nível de satisfação “regular”, visto que 50% dos profissionais estão satisfeitos com a relação de proximidade existente entre a unidade e os funcionários - RELPR e 40,6% percebem uma preocupação da unidade com o bem estar de seus colaboradores - SAVUN. Os percentuais deste nível são passíveis de melhorias e o estabelecimento destas colabora para que estes percentuais migrem para um nível mais alto de satisfação. A análise conjunta dos

aspectos relacionados ao grupo imagem interna demonstrou um índice positivo. Visto que há uma concentração de 31,9% e 16,3% nos níveis “alto/muito alto” enquanto nos níveis “baixo/muito baixo” há uma concentração de 5,6% e 7,5% para com os itens pesquisados, demonstrando que 48,1% dos profissionais estão satisfeitos e tem uma boa imagem da unidade a que pertencem.

6.1.3 Gestão de Recursos Humanos

Com relação ao aspecto recursos humanos focou-se, especificamente, questões voltadas aos programas de treinamento e desenvolvimento proporcionados pela instituição às unidades (Apêncice C). Conforme demonstrado na Tabela 5, neste aspecto verificou-se uma equiparação de percentuais nos níveis “alto/muito alto” e “baixo/muito baixo” (25,0 % e 12,5% respectivamente) no que tange a satisfação dos profissionais para com os programas de treinamentos diponibilizados - PRTRE; e uma concentração de 37,5% nos níveis “alto/muito alto” no que se refere a creditação dos profissionais em a instituição oferecer oportunidades de atualização e aperfeiçoamento através de programas de treinamento tais como cursos, palestras e seminários - OPATU.

Tabela 5: Análise do aspecto Gestão de RH

Escala / Variável	Muito Baixo	Baixo	Regular	Alto	Muito Alto
PRTRE	12,5	25,0	25,0	25,0	12,5
OPATU	9,4	21,9	31,3	25,0	12,5
INAPER	12,5	28,1	25,0	28,1	6,3
PTBQU	12,5	25,0	40,6	15,6	6,3
Conjunto	11,7	25,0	30,5	23,4	9,4

Fonte: Pesquisa da autora

Além disso, a análise individual das questões demonstra uma baixa concentração existente nos níveis “alto/muito alto” (15,6% e 6,3% respectivamente) de satisfação dos profissionais no que se refere à disponibilização de incentivos por parte da instituição para a atualização e o aperfeiçoamento de seus colaboradores – INAPER, embora 40,6% dos

profissionais estejam parcialmente satisfeitos no que se refere a qualidade dos programas de treinamento disponibilizados - PTBQU. A análise conjunta dos aspectos relacionados ao grupo imagem interna demonstrou pontos de melhoria a serem estabelecidos devido à proximidade de percentuais existente entre os níveis “baixo/muito baixo” (36,7%) e “alto/muito alto” (32,8%).

6.1.4 Qualidade e Produtividade

O foco do aspecto qualidade e produtividade foi abordar questões realacionadas a qualidade dos processos realizados nas unidades e a produtividade dos profissionáis nelas alocados (vide Apêncice C). Conforme demonstrado na Tabela 6, percentuais insatisfatórios apresentaram-se neste aspecto, havendo uma alta concentração de percentuais nos níveis de satisfação “baixo” e “muito baixo”, no que diz respeito a adoção de procedimentos definidos para a obtenção da qualidade nos processos realizados nas unidades – QTPRO (37,3%); condições necessárias para uma maior e melhor produtividade – CMPROD (50,0%) e com relação a infra-estrutura necessária para o bom desempenho das atividades no local de trabalho - IENBD (43,7%).

Tabela 6: Análise do aspecto qualidade/produtividade

Escala / Variável	Muito Baixo	Baixo	Regular	Alto	Muito Alto
MCPIN	0,0	25,0	46,9	25,0	3,1
QTPRO	0,0	37,3	34,1	25,5	3,1
CMPROD	15,6	34,4	21,9	21,8	6,3
SRQPR	9,4	6,3	46,8	31,3	6,2
SRQPR	9,4	6,3	46,8	31,3	6,2
IENBD	21,8	21,9	37,5	18,8	0,0
Conjunto	9,4	25,0	37,5	24,4	3,8

Fonte: Pesquisa da autora

Verificou-se também que questões relacionadas a preocupação da unidade com a melhoria contínua de seus processos internos - MCPIN (46,9%) e a participação e responsabilidade dos profissionais pelas conquistas obtidas em relação à qualidade, segurança e a produtividade - SRQPR (46,8%) concentram-se no nível de satisfação “regular”,

demonstrando que estes pontos merecem atenção e devido a insatisfação dos funcionários com relação a procedimentos definidos para a melhoria contínua dos processos internos e com relação às condições de infra-estrutura disponibilizadas na unidade para a melhoria da produtividade.

A análise conjunta dos aspectos relacionados ao grupo imagem interna demonstrou um índice negativo de satisfação, havendo uma concentração de 34,4% nos níveis “baixo” e “muito baixo” enquanto que nos níveis “alto” e “muito alto” há uma concentração de 28,2 % de satisfação para com os itens pesquisados, conforme demonstra a tabela 6.

6.1.5 Comunicação

O foco do aspecto comunicação abordou questões relacionadas ao processo de informação e os canais de comunicação das unidades conforme demonstrado no Apêncice C.

Conforme demonstra a Tabela 7, percentuais satisfatórios apresentaram-se neste aspecto, havendo uma alta concentração de percentuais nos níveis de satisfação “alto” e “muito alto”, no que diz respeito ao conhecimento claro da missão, visão, valores, princípios e metas que a unidade se propõe a atingir – MVVUN (40,7%); na obtenção de informações sobre o que acontece nas unidades – IACUN (50,0%); acreditar que seu superior é um canal de informação sobre decisões e deliberações da unidade – IDEDI (50,8%) e em ter liberdade para falar, opinar, contribuir e sugerir LFOS (43,8%). As questões que envolviam a credibilidade sobre o conteúdo dos canais e instrumentos de comunicação cumprir com seu papel e com o repasse de um bom nível de informação para os funcionários da unidade – RBNIN (46,9%); o conhecimento dos canais e instrumentos utilizados para o repasse de informações – NCCIN (50,0%) e a satisfação para com os canais e instrumentos de comunicação, utilizados na unidade, para o repasse de informações – SCIUN (46,8%) concentram-se no nível de satisfação “regular”.

A análise individual das questões também demonstrou altos percentuais de insatisfações no nível de satisfação “regular”, no que diz respeito ao nível de repasse de informações transmitidas pelos canais de comunicação – RBNIN (46,9%), o conhecimento dos canais e instrumentos existentes para o estabelecimento da comunicação - NCCIN (50%) e na satisfação dos profissionais para com os canais e instrumentos utilizados para viabilizar a comunicação - SCIUN(46,8%)

Tabela 7: Análise do aspecto Comunicação

Escala / Variável	Muito Baixo	Baixo	Regular	Alto	Muito Alto
MVVUN	6,3	21,8	31,2	31,3	9,4
IACUN	6,3	15,6	28,1	40,6	9,4
IDEDI	9,4	9,4	34,4	43,7	3,1
LFOS	12,5	12,5	31,2	34,4	9,4
RBNIN	6,3	18,7	46,9	28,1	0,0
NCCIN	9,4	18,8	50,0	18,8	3,0
SCIUN	9,4	18,8	46,8	21,9	3,1
Conjunto	**8,5**	**16,5**	**38,4**	**31,3**	**5,4**

Fonte: Pesquisa da autora

Já a análise conjunta dos aspectos relacionados ao grupo comunicação demonstrou um índice positivo, demonstrando uma concentração de 36,7% nos níveis “alto/muito alto” (31,3% + 5,4%) enquanto que nos níveis “baixo/muito baixo” há uma concentração de 25,0% (8,5% + 16,5%) para com os itens pesquisados.

6.1.6 Considerações sobre a pesquisa de clima organizacional

A pesquisa de clima organizacional realizada neste estudo ofereceu subsídios para a identificação de pontos de insatisfação relevantes a serem observados na implantação da Gestão da Segurança da Informação e no consequente estabelecimento da PSI, os quais podem acarretar turbulências no ambiente ou incitar resistências individuais ou organizacionais. Através da análise individual e conjunta das questões, definidas na pesquisa de clima, foram identificados pontos de insatisfações de profissionais relacionadas, principalmente aos aspectos motivação, comunicação, qualidade/produtividade e gestão de RH – Treinamento/Desenvolvimento existentes nas unidades, conforme segue.

- **Motivação** - níveis regulares de satisfação no que se refere ao recebimento de informações sobre mudanças implantadas nas unidades e com a valorização da segurança das informações existentes nas unidades.

- **Comunicação** - níveis regulares de satisfação com relação ao nível de repasse de informações às unidades, ou seja, poucas informaçãoes estão sendo repassadas, e com relação ao conhecimento dos canais e instrumentos de comunicação utilizados para o repasse de informações.
- **Qualidade/produtividade** - verificou-se insatisfações dos funcionários, principalmente no que tange ao estabelecimento de procedimentos definidos para a melhoria contínua dos processos e com relação a infra-estrutura necessária para melhorar a produtividade.
- **Gestão de RH** – treinamento/desenvolvimento: insatisfações relacionadas ao incentivo direcionado aos programas de treinamento e desenvolvimento e com relação a qualidade destes programas.

A identificação destes pontos de insatisfação permite o direcinamento de medidas para melhorar o ambiente de trabalho e a qualidade de vida dos profissionais no desempenho de suas funções no intuito de se obter a contribuição dos mesmos para com a gestão de segurança da informação e no consequentente comprometimento para com a política de segurança da informação .

6.2 Pesquisa de entendimento da PSI

A realização do treinamento e conscientização em segurança da informação, no Hospital Universitário de Santa Maria – HUSM possibilitou a realização de atividades interativas, nas quais foi dado espaço para que os participantes pudessem avaliar, através de um questionário, além de seu entendimento para com os tópicos abordados na política, o conteúdo e a clareza da mesma, bem como o próprio treinamento. Para avaliar o entendimento dos funcionários para com a PSI utilizou-se uma escala *Likert* com de três níveis escalares (baixo, regular e alto) para avaliar o nível de entendimento dos participantes.

Os resultados dessa pesquisa (Figura 10) demonstram que 0,2 % dos respondentes tiveram um baixo entendimento da PSI, 13,8% tiveram um entendimento regular e 86,1% tiveram um alto entendimento da PSI. Conforme recomendado por Höne e Ellof (2002), o não

entendimento de qualquer dos controles definidos na PSI foi imediatamente esclarecido para que as possíveis dúvidas não comprometessem a efetividade da PSI.

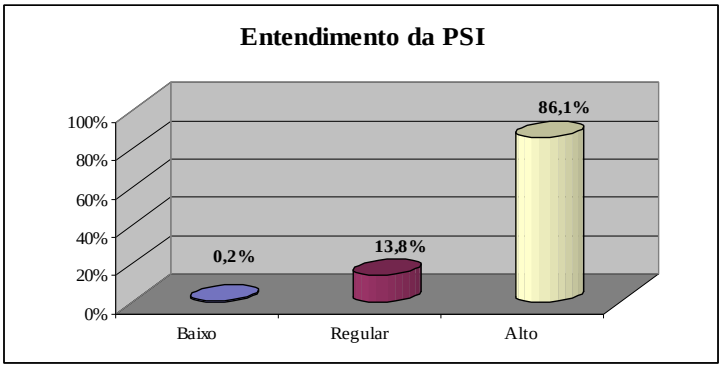


Figura 10 – Avaliação de entendimento da PSI
Fonte: Pesquisa da autora

No que se refere ao conteúdo, à clareza da PSI e ao treinamento, utilizou-se uma escala *Likert* com cinco níveis escalares, variando de “muito ruim” a “muito bom”. Os percentuais obtidos desta avaliação são demonstrados na Figura 11.

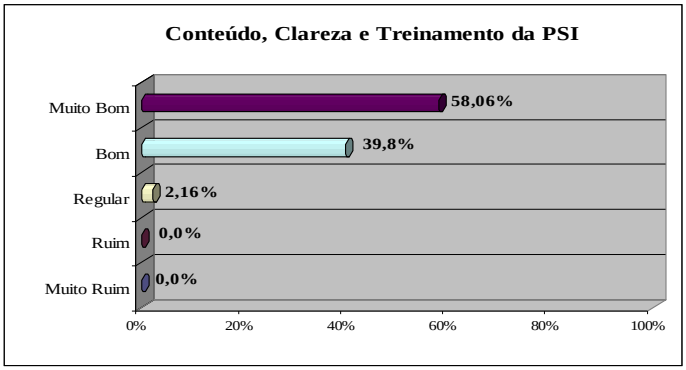


Figura 11 – Avaliação do conteúdo, da clareza e do treinamento da PSI
Fonte: Pesquisa da autora

Conforme demonstrado, 58,06% dos respondentes classificaram o conteúdo, a clareza e treinamento da PSI como “Muito Bom”, 39,8% classificaram como “Bom” e somente

2,16% classificaram como “Regular”, demonstrando um percentual significativo classificado nos níveis “Bom” e “Muito Bom”, somando um total de 97,1%.

6.3 Pesquisa de conscientização em segurança da informação

Os resultados da pesquisa de conscientização em segurança da informação demonstraram que **80%** dos respondentes possuem conhecimento sobre os pontos abordados no questionário, ou seja, sobre o propósito e o comprometimento para com a política de segurança da informação; a confidencialidade e o propósito de senhas; o uso adequado de e-mails e da internet; a responsabilidade para com a notificação de incidentes de segurança da informação e sobre as conseqüências de ações no que se refere ao sigilo e a manipulação de informações críticas. Constatou-se também que **66%** dos profissionais se comportam adequadamente com relação a estes pontos e que **61%** têm uma concepção acertada sobre os mesmos.

Entretanto, adotando-se os valores de referência propostos por Kruger e Kearney (2006), descritos na Tabela 1 da seção 2.3.3, constatou-se que o nível de conscientização total (69%) está classificado em um nível médio de conscientização, o que evidencia que os pontos abordados na pesquisa necessitam de uma monitoração para que não haja a tendência de que o nível total de conscientização diminua para níveis indesejáveis, pois a conscientização é um fator determinante à efetividade da PSI.

6.4 Efetividade da PSI

Esta seção apresenta e discute os resultados advindos da realização da pesquisa experimental, demonstrando o impacto quantitativo da utilização de técnicas de endomarketing na efetividade da PSI. A seção está dividida em seis subseções, iniciando pelo diagnóstico inicial (primeira avaliação), pelas auditorias intermediárias (da segunda a quinta avaliação) e finalizando com o diagnóstico final (sexta avaliação com análise final).

Salienta-se que anteriormente a avaliação do diagnóstico inicial foram aplicadas algumas técnicas de endomarketing (vide Quadro 3, Seção 5.2.5), entretanto estas técnicas

foram comuns tanto ao grupo de experimentação (UCI) quanto ao grupo de controle (UTI). Portanto, os dois grupos tinham subsídios suficientes para executar os procedimentos descritos na PSI. A análise e apresentação dos resultados obtidos são demonstradas nas seções subseqüentes.

6.4.1 Diagnóstico Inicial

A Figura 17 permite verificar que no diagnóstico inicial da UCI, 52,1% dos procedimentos previstos na PSI (Tabela 2, Seção 5.2.6) não foram executados (PNE). Vê-se que apenas 39,6% e 8,3% dos procedimentos da PSI foram parcialmente (PPE) ou totalmente executados (PTE), respectivamente.

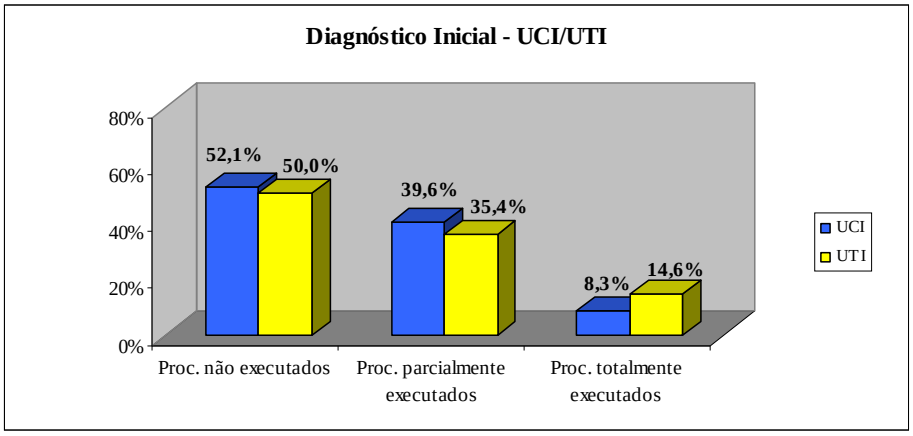


Figura 12 – Diagnóstico Inicial UCI/UTI
Fonte: Pesquisa da autora

Já em relação a UTI, o diagnóstico inicial apontou que 50,0% dos procedimentos definidos na PSI não foram executados (PNE) e que 35,4% foram parcialmente executados (PPE). Apenas 14,6% deles foram totalmente executados (PTE). Verifica-se, que mesmo com uso de técnicas de endomarketing (suporte inicial) para melhor nivelar o conhecimento sobre segurança da informação, a adesão à PSI foi pequena nos dois grupos estudados, não

ultrapassando 15 pontos percentuais de cumprimento integral dos procedimentos recomendados.

6.4.2 Segunda Avaliação

Para a realização da segunda avaliação foram aplicadas, no grupo de experimentação as seguintes técnicas de endomarketing: a) disponibilização de kits impressos (folders cuidadosamente elaborados conforme demonstrado nos Apêndices A, J e K) contendo de forma detalhada a Política de Segurança da Informação e o conteúdo explicativo sobre o projeto de segurança da informação; b) demonstração do conteúdo do site de Gestão de Segurança da Informação - GSI (Apêndice R); c) reuniões individuais com os componentes do grupo de experimentação; e) envio de e-mails para esses funcionários para esclarecimento de dúvidas; e d) alertas de advertência e acompanhamento funcional para a realização correta dos procedimentos elaborados na PSI (Apêndices N e P). Um mês após a aplicação destas técnicas foram realizadas auditorias para verificar o percentual de procedimentos que estavam sendo corretamente executados (Figura 13).

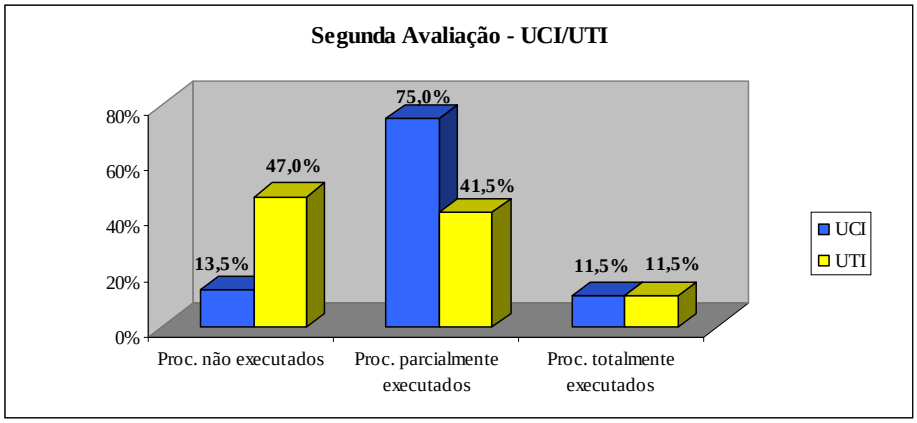


Figura 13 – Segunda Avaliação UCI/UTI
Fonte: Pesquisa da autora

Os dados revelaram que na UCI 13,5% correspondem a PNE, que 75% são de PPE e, ainda, que 11,5% foram de PTE. Verifica-se que houve um incremento de mais de 3 pontos

percentuais de cuidados com o cumprimento dos procedimentos de forma correta. Em relação a UTI os resultados apontam que 47,0% dos procedimentos não foram executados (PNE), que 41,5% dos procedimentos foram parcialmente (PTE) e que 11,5% dos procedimentos foram totalmente executados (PTE). Observa-se a pequena redução do percentual de procedimentos que não foram executados na UTI e a significativa redução na UCI. A UCI apresentou índices positivos na melhoria da execução dos procedimentos definidos na PSI.

6.4.3 Terceira Avaliação

Para a realização da terceira avaliação foram aplicadas as seguintes técnicas de endomarketing: a) lembretes sobre a PSI; b) caixa de sugestões; c) e-mails informativos; d) acompanhamento funcional para a realização correta dos procedimentos descritos na PSI; e, e) brindes de final de ano com lembretes de segurança da informação (Apêndice O). Conforme pode-se visualizar na Figura 14, a auditoria feita nesta etapa da pesquisa aponta que na UCI: 12,5% dos procedimentos definidos na PSI não foram realizados (PNE), que 63,5% foram parcialmente executados (PPE) e que, agora, 24,0% dos procedimentos foram totalmente executados (PTE). Por outro lado, na UTI, onde não foram aplicadas técnicas de endomarketing, os dados mostram 52,0 % de PNE, 40,7% de PPE e somente 7,3% de PTE.

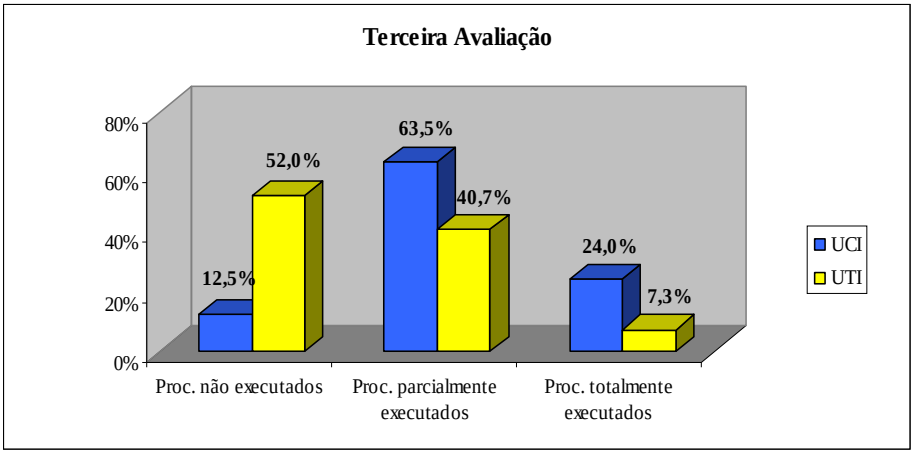


Figura 14 – Terceira Avaliação UCI/UTI
Fonte: Pesquisa da autora

Os dados mostram o aumento do percentual de procedimentos totalmente executados no grupo de experimentação (UCI) e uma elevação do percentual correspondente a não execução dos procedimentos previstos na PSI, pelo grupo de controle (UTI). Já é possível verificar nesta fase a relevância do endomarketing para a efetividade da PSI na Unidade de Cardiologia Intensiva (UCI).

6.4.4 Quarta Avaliação

Para a quarta avaliação foram aplicadas no grupo de experimentação as seguintes técnicas: a) reuniões individuais com os componentes do grupo; b) divulgação de atualizações do site da GSI; c) e-mails informativos para esclarecimentos de dúvidas relacionadas à gestão de segurança da informação e a PSI; e, d) acompanhamento funcional para a realização correta dos procedimentos descritos na PSI. Um mês após a aplicação das referidas técnicas as auditorias foi constatado (Figura 15) na Unidade de Cardiologia Intensiva (UCI) que: 11,5% dos procedimentos não foram executados, 56,2% deles foram parcialmente executados e 32,3% dos procedimentos passaram a ser totalmente executados. Na Unidade de Terapia Intensiva Adulto (UTI) esses percentuais ficaram em 58,3% de PNE, 35,4% de PPE e 6,3% de PTE, piorando ainda mais a efetividade da PSI nesta unidade.

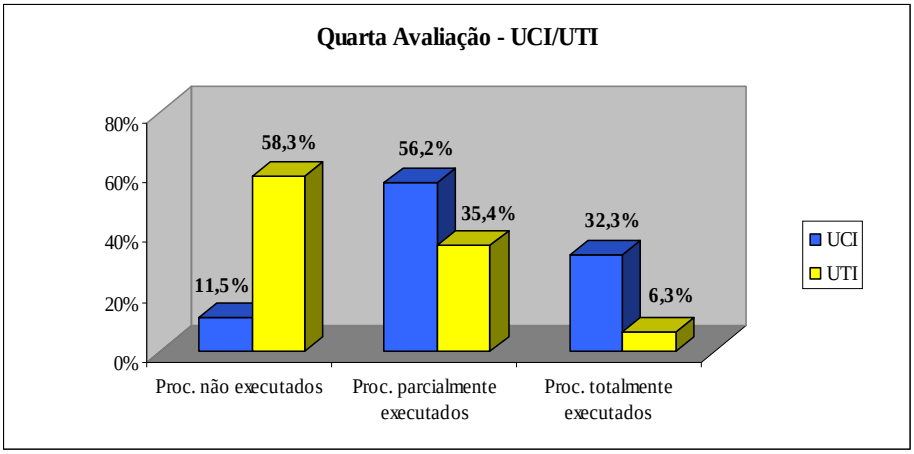


Figura 15 – Quarta Avaliação UCI/UTI
Fonte: Pesquisa da autora

Observa-se que o grupo de experimentação (UCI) apresentou um aumento percentual de 24% nos procedimentos totalmente executados em relação à primeira avaliação (seção 6.4.1), bem como uma redução de 40,6% nos procedimentos não executados. Por sua vez, pode-se perceber que no grupo de controle (UTI) houve aumento no percentual de procedimentos não executados, acarretando a diminuição de percentuais de procedimentos parcialmente e totalmente executados.

6.4.5 Quinta Avaliação

Para a quinta avaliação foram aplicadas no grupo de experimentação as seguintes técnicas: a) acompanhamento funcional para a realização correta dos procedimentos descritos na PSI; b) reuniões individuais com os componentes do grupo; e, c) divulgação dos percentuais de adesão a PSI. Um mês depois da aplicação das técnicas, a auditoria interna verificou os percentuais listados na Figura 16, onde observa-se que no grupo de experimentação (UCI) apenas 10,4% não realizaram os procedimentos recomendados pela PSI.

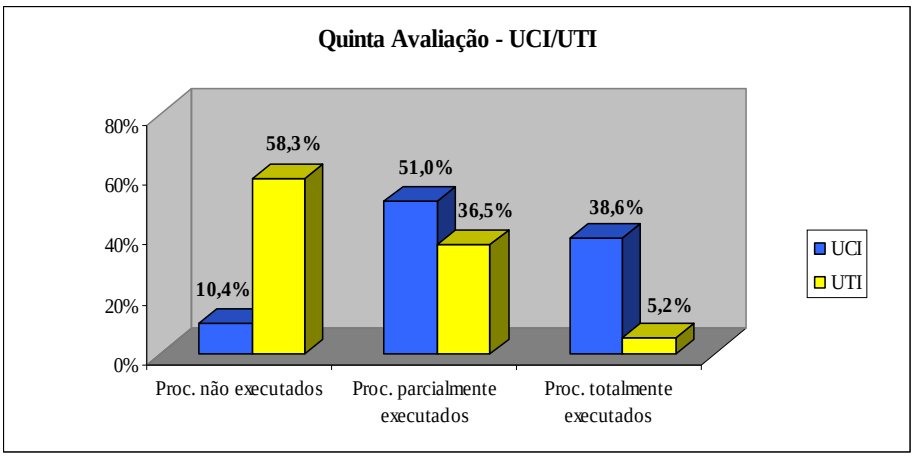


Figura 16 – Quinta Avaliação UCI/UTI
Fonte: Pesquisa da autora

Esta avaliação demonstra que o grupo de experimentação continua reduzindo os percentuais de PNE, bem como continua aumentando os percentuais de PPE e PTE. Em contrapartida, na avaliação do grupo controle verifica-se que os percentuais referentes aos PNE continuam aumentando, acarretando a diminuição dos percentuais referentes aos PPE e PTE.

6.4.6 Diagnóstico Final

Para a realização do diagnóstico final foram aplicadas as seguintes técnicas de endomarketing: a) reuniões individuais com os componentes do grupo; b) alertas de advertência sobre a PSI; c) divulgação de atualizações do site da GSI; d) e-mails informativos para esclarecimentos de dúvidas relacionadas à gestão de segurança da informação e à PSI; e) acompanhamento funcional para a realização correta dos procedimentos descritos na PSI; e, f) brindes.

O diagnóstico final (Figura 17) demonstra que após a aplicação das técnicas de endomarketing houve uma diminuição significativa nos percentuais de procedimentos não executados (PNE) e um alto índice de percentuais nos procedimentos totalmente executados (PTE) na UCI, quando comparados aos percentuais demonstrados na UTI do hospital analisado.

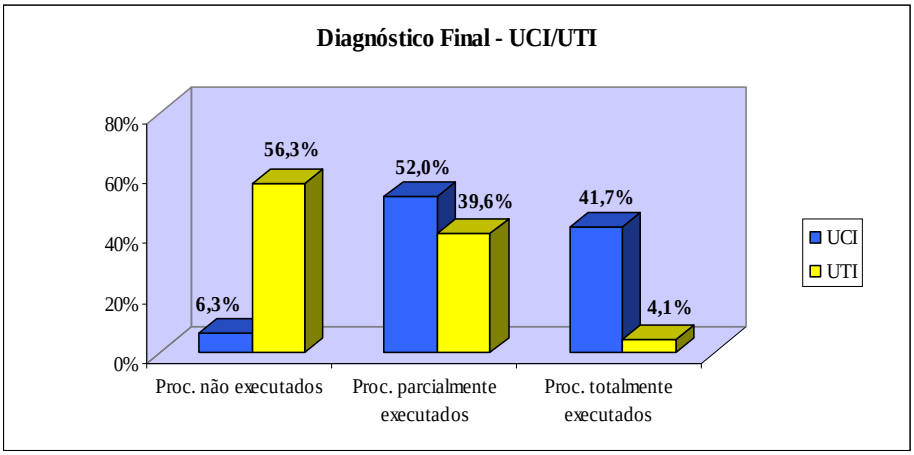
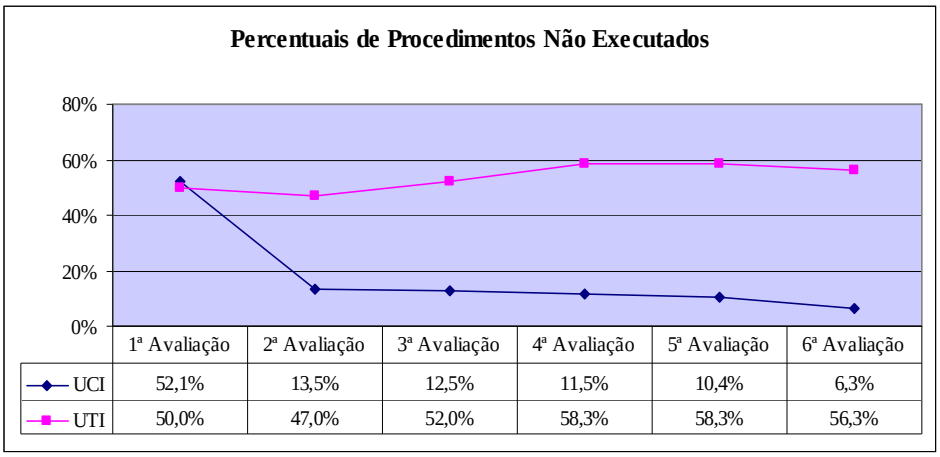


Figura 17 – Diagnóstico Final UCI/UTI
Fonte: Pesquisa da autora

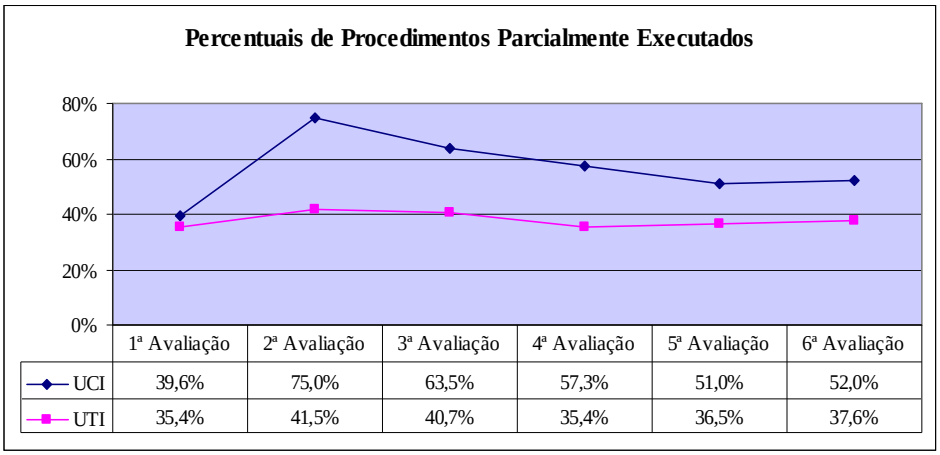
Resultados envolvendo todas as 6 avaliações também foram observados nas duas unidades (UCI/UTI). Os percentuais referentes aos procedimentos não executados – PNE podem ser visualizados na série temporal da Figura 18. A partir desta avaliação, verificou-se que a UCI apresentou uma queda nos percentuais destes procedimentos de 45,8% durante todo o período em que foram feitas as avaliações, enquanto que à UTI apresentou um aumento nos percentuais destes procedimentos de 6,3% no mesmo período. Estes resultados refletem uma diferença de 39,5% de PNE entre ambas as unidades, evidenciando uma diminuição significativa de percentuais de PNE na Unidade de Cardiologia intensiva (UCI) em decorrência da aplicação de técnicas de endomarketing.



	1ª Avaliação	2ª Avaliação	3ª Avaliação	4ª Avaliação	5ª Avaliação	6ª Avaliação
UCI	52,1%	13,5%	12,5%	11,5%	10,4%	6,3%
UTI	50,0%	47,0%	52,0%	58,3%	58,3%	56,3%

Figura 18 – Comparativo de percentuais de procedimentos não executados UCI/UTI
Fonte: Pesquisa da autora

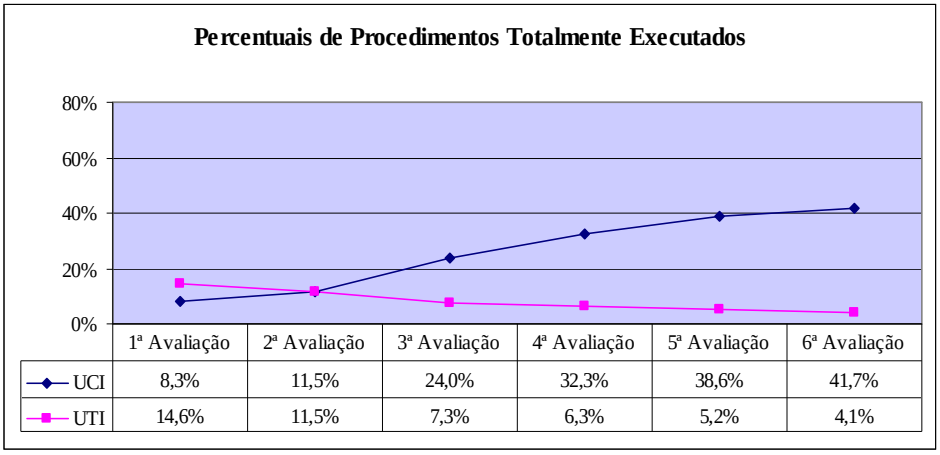
Na avaliação cumulativa referente aos procedimentos parcialmente executados – PPE (Figura 19) observa-se que a Unidade de Cardiologia Intensiva (UCI) apresentou um aumento nos percentuais destes procedimentos de 12,4%, conseqüência da diminuição de percentuais de PNE enquanto que a Unidade de Terapia intensiva – Adulto (UTI) apresentou um aumento destes percentuais de 4,2% devido à diminuição dos percentuais de PTE (Figura 20).



	1ª Avaliação	2ª Avaliação	3ª Avaliação	4ª Avaliação	5ª Avaliação	6ª Avaliação
UCI	39,6%	75,0%	63,5%	57,3%	51,0%	52,0%
UTI	35,4%	41,5%	40,7%	35,4%	36,5%	37,6%

Figura 19 – Comparativo de percentuais parcialmente executados UCI/UTI
Fonte: Pesquisa da autora

A avaliação referente aos procedimentos totalmente executados – PTE (Figura 20) demonstra que a UCI apresenta um aumento nos percentuais destes procedimentos de 33,4% enquanto que a UTI apresentou uma diminuição destes percentuais de 10,5%, evidenciando uma diferença positiva (22,9%) para a UCI frente a UTI por ela apresentar um significativo aumento nos percentuais PTE**.**



	1ª Avaliação	2ª Avaliação	3ª Avaliação	4ª Avaliação	5ª Avaliação	6ª Avaliação
UCI	8,3%	11,5%	24,0%	32,3%	38,6%	41,7%
UTI	14,6%	11,5%	7,3%	6,3%	5,2%	4,1%

Figura 20 – Comparativo de percentuais totalmente executados UCI/UTI
Fonte: Pesquisa da autora

As avaliações demonstradas nas figuras anteriores revelam que em aspectos gerais, no que se refere aos três tipos de procedimentos (PNE, PPE e PTE), o grupo de experimentação

(UCI) se destaca consideravelmente quando comparado ao grupo de controle (UTI). A diminuição dos percentuais de PNE e o aumento de PPE e PTE demonstram que membros do quadro funcional da UCI executaram de forma mais expressiva os procedimentos definidos na política de segurança da informação por terem sido estimulados com a aplicação contínua de técnicas de endomarketing.

CAPÍTULO 7

CONCLUSÕES E RECOMENDAÇÕES

O caráter formal de uma política de segurança da informação (PSI) pode gerar resistências no ambiente organizacional ao impor regras e responsabilidades aos usuários para com os recursos informacionais. A efetividade de uma PSI está diretamente relacionada à forma com que ela é direcionada e comunicada aos usuários, sendo refletida pelas ações ou tarefas que eles realmente executam. As técnicas de endomarketing são direcionadas aos inter-relacionamentos e valorização das opiniões e sugestões fornecidas pelos usuários internos, ou seja, os próprios funcionários. Tais técnicas podem minimizar o fator resistência na implantação de uma PSI, pois as regras não são auto-aplicáveis nem autoformuláveis, exigindo, muitas vezes, juízos de valores e percepções equivocadas. Estes estereótipos podem ser tanto de seus formuladores, quanto dos agentes que operacionalizam a PSI. Intuitivamente técnicas de endomarketing têm sido utilizadas para a conscientização dos usuários em segurança da informação, mas o impacto quantitativo destas técnicas para a efetividade da PSI ainda não havia sido explorado. Este trabalho realizou um experimento com duas unidades de um hospital (UCI e UTI) para avaliar esta efetividade.

Das avaliações do experimento, verificou-se que tanto o grupo de controle (UTI) quanto o grupo de experimentação (UCI), após a aplicação das técnicas de suporte inicial (nivelamento), aderiram à política de segurança da informação implantada nas respectivas unidades. Entretanto, após descontinuar a aplicação de técnicas de endomarketing no grupo de controle, observou-se uma diminuição gradativa dos percentuais de procedimentos totalmente executados pelos componentes deste grupo, que caiu de 14,6% para 4,1%, o que demonstra uma queda de 71,92% na adesão à PSI neste grupo, se considerado os procedimentos totalmente executados (PTE). Já a aplicação continuada de técnicas de endomarketing no grupo de experimentação fez com que os procedimentos descritos na PSI estivessem sempre

presentes na mente dos usuários, o que gerou um aumento gradativo nos percentuais de procedimentos totalmente executados. O percentual subiu de 8,3% para 41,7%, o que reflete uma melhora de 402,4% na adesão à PSI neste grupo, se considerado os PTEs. Se considerado os procedimentos não executados (PNEs), a aplicação contínuada de técnicas de endomarketing no grupo de experimentação possibilitou uma redução de 88%, contra um aumento de 12,6% no grupo de controle, e uma alta concentração de percentuais nos procedimentos parcialmente ou totalmente executados, que somados chegam a 93,7% na avaliação final.

Conclui-se, portanto, que a aplicação de técnicas de endomarketing faz-se relevante para se obter o comprometimento dos usuários para com a PSI, o que contribui conseqüentemente para sua efetividade.

Para trabalhos futuros sugere-se a aplicação de técnicas de endomarketing em outros contextos organizacionais a fim de se verificar se o impacto de sua utilização na efetividade da PSI apresenta variações quantitativas distintas das apresentadas neste trabalho. Além disso, como existem diversas técnicas de endomarketing, é interessante investigar qual o conjunto mínimo de técnicas de endomarketing e o período ótimo de aplicação que oferecer o melhor resultado na efetividade da PSI.

REFERÊNCIAS BIBLIOGRÁFICAS

AXUR. **White Paper: Política de Segurança da Informação. AXUR Information Security. 2002.** Disponível em: http://www.axur.com.br. Acesso: dezembro de 2007.

BARDWIK, J. M. **Perigo na Zona de Conforto.** São Paulo: Pioneira. 1998.

BEKIN, S.F. **Conversando sobre endomarketing.** São Paulo: Macron Books. 1995.

_____. **Endomarketing: Como praticá-lo com sucesso.** São Paulo. Prentice Hall. 2005

BISPO, C.A.F. **Um novo modelo de pesquisa de clima organizacional.** Revista Produção, v. 16, n. 2, p. 258-273, Maio/Ago. 2006.

BRESSAN, C. L. **Uma contribuição a contribuição do fenômeno de mudança organizacional a partir da visão gerencial,** Brasília, 2001. Dissertação (Mestrado em Psicologia). Programa de Pós-Graduação em Psicologia, Universidade de Brasília, 2001

BRUM, A. M. **Endomarketing.** Porto Alegre: L&PM, 1998.

_____. **Respirando Endomarketing**. Porto Alegre: L&PM, 2003.

CERQUEIRA, W**. Endomarketing: educação e cultura para a qualidade**. Rio de Janeiro: Qualimark, 2002.

CERT. **Práticas de Segurança para Administradores de Redes Internet**. 2003. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em http://www.nic.br/seguranca/index.htm. Acesso: outubro/2007.

DIAS, S.R. **Gestão de Marketing.** São Paulo: Saraiva, 2003

ECKES, G. **A revolução Seis Sigma: o método que levou a GE e outras empresas a transformar processos em lucro**. Tradução: Dr. Reynaldo Cavalheiro Marcondes. Rio de Janeiro: Campus, 2001.

ERNEST & YOUNG. **Global Information Security Survey**. ERNEST & YOUNG. 2004. Disponível em: http://www.ey.com. Acesso: março de 2008.

FÁVERO, A. **Política de Segurança da Informação – Guia prático para elaboração e implementação.** Prefácio. Rio de Janeiro.Ciência Moderna. 2006

FERREIRA, F.N.F.; ARAÚJO, M. T. **Política de Segurança da Informação - Guia prático para elaboração e implementação.** Rio de Janeiro.Ciência Moderna. 2006.

FONTES, E. **Segurança da Informação: o usuário faz a diferença.** São Paulo. Ed. Saraiva. 2006.

GARTNER, EXP Club. Information Security- Information security - How much is enough? Gartner, inc. 2003.

GIL, A.C. **Como elaborar projetos de pesquisa**. 3ª ed. São Paulo: Atlas. 1996

GRAFF M.; WYCK, K. V. **Secure Coding: Principles and Practices**, O'Reilly, Sebastopol, CA, 2003.

HÖNE, K.; ELOFF, J.H.P. **What makes an effective information security police?** Network Security. pp 14-16. 2002.

ISACA. **Security Awareness: Best Practices to Secure Your Enterprise**. Information Systems Audit and Control Association. 2005. Disponível em: http://www.isaca.org.br Acesso: dezembro 2007.

JOHNSON E. **Security awareness: switch to a better programme**. Computer Fraud Security. pp 15-18. 2006.

KOTLER, P. **Administração de marketing**. 10.ed.Tradução de Bazán Tecnologia e Lingüística. São Paulo: Prentice Hall, 2000.

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

LIMA, P.; MIYASAKI, M.; ABREU, Y. **Evolução das organizações**. In: SEMEAD – Seminários em Administração - FEA/USP, anais. São Paulo, 2003.

MALHOTRA, N.K. **Pesquisa de marketing: uma orientação aplicada.** Porto Alegre: Bookman, 2006.

MARCIANO, J. L.; LIMA-MARQUES, M. **Enfoque Social da Segurança da Informação**. Revista Ciência da Informação, v.35, n. 3. 2006.

MARCONI M. A, LAKATOS E.M. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MATTAR, F. N. **Pesquisa de marketing: metodologia, planejamento, execução e análise**. São Paulo: Atlas, 1993.

MCCARTHY, E. Jerome. **Basic marketing: a managerial approach**. 6th ed. Richard D. Irwin, Homewood, 1978.

MCCARTHY, M.P.; CAMPBELL S. **Security Transformation – Digital Defense Strategies to Protect Your Company's Reputation and Market Share**. McGraw-Hill. Nova York. 2001.

MCCOY, C.; FOWLER, R. T. **You Are de Key to Security: Establishing a Successful Security Awareness Program.** In Proceedings of the 32 nd annual ACM SIGUCCS Conference on User Services. pp 346-349. Baltimore, MD, USA, 2004.

McKENNA, Regis. **Marketing de relacionamento.** Rio de Janeiro.Campus, 1999.

McLEAN , K. **Control Concepts -Who's Buying?** Computer Audit Update. pp.3-13. 1995

MODULO SECURITY INFORMATION**. 9ª Pesquisa Nacional de Segurança da Informação**. Disponível em: http://www.modulo.com.br/media/9a_pesquisa_nacional.pdf. Acesso: novembro de 2007a.

_____. **"10ª Pesquisa Nacional de Segurança da Informação".** Disponível em: http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf. Acesso: novembro de 2007b.

NOSWORTHY , J.D. **Implementing Information Security in the 21st Century – Do You Have the Balancing Factors?** Computers & Security, 19(4), pp. 337 – 347. 2000.

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

NEVES, E. V. C. **Visão Geral de uma Política de Segurança: Parte III - Produzindo o Business Case**. Disponível em: http://www.camargoneves.com/Artigos/VGPS3.pdf Acesso: dezembro de 2007.

NONAKA, I. A dynamic theory of organizational Knowledge creation. Organizational Science, Vol. 5 , nº1, pp.14-37.1994.

OLIVEIRA, W.J. **Segurança da informação**. Florianópolis.Visual Books, 2001.

OLIVEIRA, S. T. **Ferramentas para o aprimoramento da qualidade**. 2.ed.. São Paulo: Pioneira, 1996.

OSBORNE, K. **Auditing the IT Security function. Computers & Security**. Vol. 17(1), pp. 34-41, 1998.

PAIXÃO, M. V. P. **Marketing interno e a Mudança Organizacional**. Convibra – Congresso Virtual Brasileiro de Administração, 2004.

PAYNE, S. **Developing Security Education and Awareness Programs**. Educause Leadership Strategies Series. Vol 8. pp. 49-53. 2003.

PELTIER, T.R. **Implementing an Information Security Awareness Program**. Security Management Practices. pp 37-49. 2005.

RAMOS, F**. Security Awareness através do método D3/AET**. AXUR Information Security. 2003. Disponível em: http://www.axur.net. Acesso: dezembro de 2007.

RICHARDSON, R.J. Pesquisa social: métodos e técnicas. São Paulo: Atlas, 1999.

ROBBINS, S.P. **Comportamento organizacional**. 9 ed. São Paulo: Pretince Hall, 2002.

SÊMOLA, M. **Gestão da Segurança da Informação – Uma Visão Executiva**. Rio de Janeiro: Campus/Elsevier, 2003.

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação.** 2a edição. Florianópolis. 2001.

SIPONEN, M.T. **A conceptual foundation for organization information security awareness**. Information Management &Computer Security. pp.31-41. 2000.

SOCIEDADE BRASILEIRA DE INFORMÁTICA NA SAÚDE**. Política Nacional de Informação e Informática em Saúde**. 2004. Acesso em 05/11/2007. Disponível em:< http://www.sbis.org.br>.

SOLMS, B. V.; SOLMS, R. V. **The 10 deadly sins for informations security management**. Computers & Security 23, pp.371-376. 2004.

SOLMS R. V., SOLMS B.V. **From policies to culture.** Computers and Security, Vol. 23, pp. 275–279. 2004

SPURLING, P. **Promoting security awareness and commitment.** Information Management & Computer Security. vol 3. pp 20-26. 1995.

THOMSON, K.L.; SOLMS, R.V. **Information security obedience: a definition.** Computers & Security, Vol.24, pp. 69-75, 2005.

THOMSON, K.L.; SOLMS, R.V; LOUW; L. **Cultivating an organizational information security culture.** Computers & Security, pp. 07-11, 2006.

TUDOR, J.K. **Information Security Architecture: An Integrated Approach to Security in the Organization.** 2ª edição, CRC Press. 2006

WHITMAN M. E. **In defence of the realm: understanding the threats to information security**. International Journal of Information Management.Vol24; pp.43-47. 2004.

WOOD, C. C. **An unnapreciated reason why information security policies fail.** Computer Fraud & Security, n. 10, p. 13–14. 2000.

_____. **Information security awareness raising methods.** Computer Fraud Security. 1995.

_____. **Policies Alone Do not Constitute a Sufficient Awareness Effort**. Computer Fraud Security. 1997.

WOOD, J.T. **Mudança Organizacional**. São Paulo: Atlas. 2000b.

YANUS, R.; SHIN, N. **Critical Success Factors for Managing an Information Security Awareness Program.** In: Proceefings of the 6th Annual ISOnEworld Conference. Las Vegas, NV. 2007.

YIN, Robert K. Estudo de Caso: planejamento e métodos, - 3. ed. – Porto Alegre: Bookman, 2005.

YOUSEF, D. A. **Organizational commitment and job satisfaction as predictors of attitudes toward organizational change in a non-western setting**. Journal: Personel Review, v. 29, p. 567-592, 2000.

APÊNDICES

APÊNDICE A – Plano de ação

AÇÃO (WHAT)	JUSTIFICATIVA (WHY)	METODOLOGIA (HOW)	RESPONSÁVEL (WHO)	LOCAL (WHERE)	PRAZOS (WHEN)	FUNDAMENTAÇÃO TEÓRICA				
						Spurling 1995	Wood 1997	McCoy 2004	Peltier 2005	Everet 2006
Definir Logomarca e/ou Slogan	Para marcar o inicio do Processo de Gestão da Segurança da Informação	Reuniões com o grupo de Segurança da informação	Pesquisadora	GMICRO	maio		X	X	X	X
Verificar canais e instrumentos existentes	Para averiguar quais os canais e instrumentos já são utilizados na UCI	Entrevistas com Comitê Gestor de Segurança da informação	Pesquisadora	UCI/UTI	maio			X	X	X
Definir instrumentos de endomarketing a serem utilizados inclusive cores.	Para a divulgação do projeto de gestão da segurança da informação e da política de segurança da informação.	Reuniões com o Comitê Gestor de Segurança da informação ou responsável e o Grupo de Segurança da Informação.	Pesquisadora	GMICRO	Jun.	X	X	X	X	X
Definir como será feita a alavancagem formal	Para informar aos funcionários a quem devem ser reportados os problemas relacionados à segurança da informação.	Reuniões com Grupo de Segurança da Informação	Pesquisadora	GMICRO	Jun.	X	X		X	
Divulgar o projeto	Para que os funcionários saibam o que é uma gestão voltada a segurança da informação e os benefícios que a mesma pode oferecer a organização	Reuniões rápidas com no máximo 3 funcionários para que não haja interrupção das atividades dos mesmos ou disponibilização de folders que demonstrem o que é a GSI e seus benefícios	Pesquisadora	UCI/UTI	Jun.	X	X	X	X	X

APÊNDICE A - Plano de Ação (continuação)

AÇÃO (WHAT)	JUSTIFICATIVA (WHY)	METODOLOGIA (HOW)	RESPONSÁVEL (WHO)	LOCAL (WHERE)	PRAZOS (WHEN)	FUNDAMENTAÇÃO TEÓRICA				
						Spurling 1995	Wood 1997	McCoy 2004	Peltier 2005	Everet 2006
Mapear o perfil dos funcionários	Para que os funcionários possam posteriormente na fase de treinamento e conscientização serem segmentados de acordo com seu perfil.	Entrevistas, questionários ou documentos existentes na organização que demonstrem o perfil dos funcionários.	Pesquisadora	UCI/UTI	Jun.	X	X	X	X	X
Mapear os riscos relacionados à segurança da informação (identificação dos problemas existentes)	Para que os funcionários possam saber na fase de conscientização e treinamento quais os problemas que estão afetando a unidade e o que pode ser feito para minimizá-los.	Questionários, entrevistas, observação	Pesquisadora	UCI/UTI	Jun.	X	X	X		
Aplicar a Pesquisa de Clima Organizacional	Para verificar os esforços que serão necessários para se obter o comprometimento dos recursos humanos presentes na UCI.	Aplicação de pesquisa de clima organizacional.	Pesquisadora	UCI/UTI	Jun.	CONTRIBUIÇÃO				
Demonstrar as informações coletas	Para que os membros do grupo de Gestão de Segurança da Informação tenha uma visão global dos problemas existentes, do perfil dos funcionários e dos esforços que serão necessários para a conscientização e treinamento	Exposição de gráficos (diagrama de pareto, diagrama de causa e efeito) e análises descritivas (estratificação).	Pesquisadora	GMICRO	Jul.	X	X	X		

APÊNDICE A - Plano de Ação (continuação)

AÇÃO (WHAT)	JUSTIFICATIVA (WHY)	METODOLOGIA (HOW)	RESPONSÁVEL (WHO)	LOCAL (WHERE)	PRAZOS (WHEN)	FUNDAMENTAÇÃO TEÓRICA				
						Spurling 1995	Wood 1997	McCoy 2004	Peltier 2005	Everet 2006
Analisar as Informações coletadas	Para se verificar quais os ajustes podem ser realizados tanto no clima organizacional quanto na própria política a ser implantada nas unidades.	Estudo dos dados sob análise com uso de ferramentas da qualidade (diagrama de pareto)	Pesquisadora	Indiferente	Jul.	X	X	X		
Desenvolver material de endomarketing	Para divulgação da política de segurança da informação	Forders, cartazes, apresentações, foldes para pesquisa de satisfação dos funcionários dos funcionários para com a conscientização/treinamento e para com a política de segurança da informação	Pesquisadora	GMICRO	Ago.	X	X	X	X	X
Conscientizar/treinar o pessoal	Para que os funcionários tenham consciência dos problemas relacionados à segurança e saibam o que fazer para evitá-los bem como conheçam a política de segurança da informação.	Reuniões, palestras ou apresentações. Com lista de presença para se verificar o número de profissionais presentes. Havendo a possibilidade de que essa atividade seja realizada em turnos diferenciados inclusive em alguns casos em finais de semana ou feridos para atingir todos os funcionários da unidade.	Pesquisadora	Sala de treinamentos da UCI	Ago.	X	X	X	X	X

APÊNDICE A - Plano de Ação (continuação)

AÇÃO (WHAT)	JUSTIFICATIVA (WHY)	METODOLOGIA (HOW)	RESPONSÁVEL (WHO)	LOCAL (WHERE)	PRAZOS (WHEN)	FUNDAMENTAÇÃO TEÓRICA				
						Spurling 1995	Wood 1997	McCoy 2004	Peltier 2005	Everet 2006
Coleta de sugestões de melhoria – conscientização /treinamento	Para se verificar onde pode se melhorar no que diz respeito à conscientização e ao treinamento	Pesquisa de satisfação dos funcionários a ser entregue momentos antes do inicio da conscientização/treinamento e recolhido no final.	Pesquisadora	UCI (sala de treinamentos. No dia em que for realizado a conscientização/ treinamento.	Ago.	X	X	X	X	X
Avaliar o conhecimento obtido na fase de conscientização e treinamento	Para se verificar se existe a necessidade de uma nova uma nova rodada de conscientização e treinamento abordando pontos que tenham deixado dúvidas.	Questionários /testes	Pesquisadora	UCI/UTI	Ago.		X			X
Avaliar o comprometimento obtido	Para se verificar se a política de segurança implantada na UCI conseguiu um número expressivo de adeptos.	Auditoria através checklist para verificar quais os controles da política de segurança da informação está realmente sendo executados	Pesquisadora	UCI/UTI	Out., Nov., Dez., Jan., Fev. e Mar./08		X			X
Coleta de sugestões de melhoria – política de segurança da informação	Para se verificar se existe a necessidade de algum ajuste na política de segurança da informação de acordo com a visão dos funcionários.	Pesquisa de satisfação dos funcionários para com a política de segurança da informação e sugestões de melhoria para com a mesma	Pesquisadora	UCI/UTI	Out./08	X	X	X	X	X

APÊNDICE A - Plano de Ação (continuação)

AÇÃO (WHAT)	JUSTIFICATIVA (WHY)	METODOLOGIA (HOW)	RESPONSÁVEL (WHO)	LOCAL (WHERE)	PRAZOS (WHEN)	FUNDAMENTAÇÃO TEÓRICA				
						Spurling 1995	Wood 1997	McCoy 2004	Peltier 2005	Everet 2006
Divulgação dos resultados parciais obtidos	Para que o grupo do projeto de gestão de segurança da informação tenha conhecimento dos resultados.	Defesa da Dissertação	Pesquisadora	GMICRO	Jan./09	X	X	X		
Divulgação dos resultados finais obtidos	Para que o grupo do projeto de gestão de segurança da informação tenha conhecimento dos resultados.	Defesa da dissertação	Pesquisadora	GMICRO	Mar./09					

APÊNDICE B – Política de segurança da informação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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/gsi_husm

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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:

Padrões:

APÊNDICE C – Pesquisa de clima organizacional

Gestão de Segurança da Informação	*Pesquisa de Clima Organizacional*	**Versão 001-02**

Prezado Colaborador

O presente questionário é um dos componentes necessários à realização de uma dissertação de mestrado voltada à segurança da informação. Como esta pesquisa se sustenta na evidência do respeito para com os colaboradores internos da organização e certos de que as pessoas são um grande diferencial competitivo, queremos saber o que você pensa sobre a organização em que você trabalha (HUSM) e sobre a unidade a que está vinculado (UCI/UTI). Por favor, assinale no quadro abaixo, sua verdadeira e sincera impressão sobre os valores descritos. Sua opinião nos orientará no caminho que deveremos percorrer. 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.

Unidade e turno em que trabalha

☐ UCI **Turno** ☐ 08:00 – 12:00 ☐ 12:00 – 16:00 ☐ 16:00 – 20:00 ☐ 20:00 – 08:00

☐ UTI **Turno:** ☐ 07:00 – 13:30 ☐ 13:30 – 19:30 ☐ 19:30 – 07:30

Função que desempenha

☐ Médico ☐ Enfermeiro ☐ Fisioterapeuta ☐ Auxiliar Administrativo

☐ outra Qual ?_____

Cargo que ocupa

☐ Diretor ☐ Supervisor ☐ Funcionário ☐ Estagiário ☐ Outro. Qual? _____

Tempo de serviço

☐ até 5 anos ☐ até 10 anos ☐ até 15 anos ☐ Outro Qual? _____

Faixa etária

☐ de 18 - 25 ☐ de 26 – 35 ☐ de 36 – 45 ☐ de 46 – 55 ☐ de 56 ou mais

Sexo ☐ Feminino ☐ Masculino

Grau de Instrução

☐ Doutorado ☐ Mestrado ☐ Pós-Graduação ☐ Graduação ☐ Nível Técnico

☐ Outro. Qual? _____

Responda ao questionário abaixo assinalando com um "X" no espaço correspondente a opção que melhor represente o seu nível de satisfação para com os itens apresentados.

MUITO BAIXO	BAIXO	REGULAR	ALTO	MUITO ALTO
☹	😐	?☺!	☺	☺!!
1	2	3	4	5

Assinale somente uma das alternativas de cada um dos itens. Preencha com **sinceridade** e sem receio, pois essa **pesquisa não é identificada**. Se você não assinalar exatamente o seu nível de satisfação, o resultado será errado e teremos perdido uma ótima oportunidade de saber como vocês estão se sentindo**.**

Por favor, não assinale mais de uma alternativa.

Itens avaliados	Nível de Satisfação				
	☹	😐	?☺!	☺	☺!!
	1	2	3	4	5
Motivação - Relação com o trabalho					
Nível de entusiasmo comparado ao que possuía quando ingressou na unidade.	1	2	3	4	5
Com o trabalho que realiza na unidade	1	2	3	4	5
Utilização de todos os conhecimentos na realização do trabalho.	1	2	3	4	5
Empenho empregado na realização de suas tarefas	1	2	3	4	5
Distribuição do trabalho entre as pessoas na área em que atua.	1	2	3	4	5
Motivação - Espírito de equipe					
Vontade para solicitar ou oferecer ajuda aos meus colegas de trabalho.	1	2	3	4	5
Cooperação de todos para que os resultados sejam atingidos.	1	2	3	4	5
Clima de cooperação entre as unidades	1	2	3	4	5
Relacionamento profissionalmente ou informalmente com colegas de outras áreas.	1	2	3	4	5
Motivação - Padrões de liderança					
Recebimento do superior imediato das informações necessárias para o bom desempenho do trabalho.	1	2	3	4	5
Disponibilização clara das tarefas a serem cumpridas pelo superior imediato.	1	2	3	4	5
Reconhecimento de o superior imediato ser uma referência em nível profissional, de forma a confiar totalmente nas decisões por ele tomadas.	1	2	3	4	5
Sentir-se a vontade na presença do diretor da área.	1	2	3	4	5
Motivação - Comprometimento com a mudança					

Recebimento de informações sobre as mudanças que estão acontecendo na unidade.	1	2	3	4	5
Condução das atividades pelo superior imediato da área na qual trabalha de acordo com as mudanças e as decisões corporativas tomadas pela unidade.	1	2	3	4	5
Considerar positivas as mudanças que estão acontecendo na unidade.	1	2	3	4	5
Acreditar que seu trabalho contribui para que essas mudanças tenham resultado positivo para a unidade em que trabalho.	1	2	3	4	5
Acreditar que a unidade valoriza a segurança das suas informações (sigilo das informações estratégicas e confidenciais).	1	2	3	4	5
Colaboração para que as mudanças adotadas na unidade tenham resultado satisfatório.	1	2	3	4	5
Imagem Interna - Relacionamento com o público interno					
Acreditar que a unidade se preocupa em estabelecer uma relação de proximidade com os seus colaboradores.	1	2	3	4	5
Sentir-se parte da unidade a ponto de comemorar com as suas vitórias.	1	2	3	4	5
Imagem Interna - Ambiência organizacional					
Preocupação por parte da unidade com o bem estar dos seus colaboradores (qualidade de vida).	1	2	3	4	5
Vontade de ir à unidade todos os dias para trabalhar.	1	2	3	4	5
Existência de um clima agradável e prazeroso para se trabalhar na unidade.	1	2	3	4	5
Imagem Interna e Externa - Atendimento					
Bom atendimento quando da obtenção de informações ou serviços internos da unidade.	1	2	3	4	5
Bom atendimento da unidade para com o cliente externo (pessoas que procuram a empresa, visitantes, fornecedores, clientes, etc.).	1	2	3	4	5
Gestão de Recursos Humanos - Treinamento e desenvolvimento					
Programa de treinamento para os colaboradores da área.	1	2	3	4	5
Oportunidade de se atualizar e aperfeiçoar através de programas de treinamento como cursos, palestras e seminários.	1	2	3	4	5
Incentivo da unidade para com a atualização e o aperfeiçoamento dos seus colaboradores.	1	2	3	4	5
Programas de treinamento de boa qualidade disponibilizados aos colaboradores.	1	2	3	4	5
Gestão de Recursos Humanos - Benefícios					
Recebimento de informações sobre os benefícios a que tem direito como colaborador.	1	2	3	4	5
Qualidade e quantidade em benefícios disponibilizados pela unidade em que trabalha se comparada com outras unidades do HUSM.	1	2	3	4	5
Atendimento integral de minhas necessidades e as de minha família no que diz respeito à assistência médica.	1	2	3	4	5
Gestão de Recursos Humanos - Remuneração					
Clareza do sistema de remuneração adotado na unidade	1	2	3	4	5
Salário compatível com suas responsabilidades e com o trabalho que realiza.	1	2	3	4	5
Sistema de remuneração do HUSM quando comparado com o mercado (outros hospitais),	1	2	3	4	5
Gestão de Recursos Humanos - Reconhecimento e recompensa					
Recebimento de retorno do superior imediato sobre seu desempenho (se está positivo ou negativo).	1	2	3	4	5

Recebimento de informações sobre os critérios básicos de promoção	1	2	3	4	5
Reconhecimento e a recompensa em sua área serem baseados no resultado concreto das atividades que cada um realiza.	1	2	3	4	5
Reconhecimento e recompensa por seu esforço.	1	2	3	4	5
Busca de informações sobre seu desempenho profissional junto a seu superior imediato.	1	2	3	4	5
Qualidade e Produtividade - Qualidade					
Preocupação da unidade em que trabalha com a melhoria contínua de seus processos internos.	1	2	3	4	5
Adoção pelos profissionais da unidade de procedimentos definidos pela unidade para a obtenção da qualidade em todos os processos.	1	2	3	4	5
Qualidade e Produtividade - Produtividade					
Condições necessárias para uma maior e melhor produtividade.	1	2	3	4	5
Por sentir-se participante e responsável pelas conquistas obtidas em relação à qualidade, à segurança e à produtividade.	1	2	3	4	5
Infra-estrutura necessária para o bom desempenho das atividades no local de trabalho.	1	2	3	4	5
Comunicação - Processo da Informação					
Conhecimento claro da missão, visão, valores, princípios e metas que a unidade se propõe a atingir.	1	2	3	4	5
Informações sobre o que acontece na unidade em que trabalho.	1	2	3	4	5
Em seu superior imediato ser um canal de informação sobre as decisões e deliberações da Direção da unidade	1	2	3	4	5
Nível de liberdade para falar, opinar, contribuir e sugerir na área em que trabalha.	1	2	3	4	5
Comunicação - Canais de Comunicação					
O conteúdo dos canais e instrumentos de comunicação cumprem com o seu papel de repassar um bom nível de informação para os funcionários de sua unidade.	1	2	3	4	5
Nível de conhecimento de canais e instrumentos que repassam informações à unidade.	1	2	3	4	5
O nível de sua satisfação para com os canais e instrumentos utilizados na unidade	1	2	3	4	5

Sugestões:

_____

_____

_____

Obrigado por sua participação

APÊNDICE D – Pesquisa de conscientização

	***Pesquisa de Conscientização em Segurança da Informação***	**Versão 001**

Prezado Colaborador

O presente questionário é um dos componentes necessários a realização de uma dissertação de mestrado voltada à segurança da informação. Como esta pesquisa se sustenta na evidência do respeito para com os colaboradores internos da organização e certos de que as pessoas são um grande diferencial competitivo, queremos saber o nível de conscientização em segurança da informação existente na unidade em que você está alocado (UCI/UTI). 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.

Responda ao questionário abaixo assinalando com um "X" no espaço reservado. Assinale **somente uma** das alternativas de cada um dos itens. Preencha com **sinceridade** e sem receio, pois essa **pesquisa não é identificada**.

Por favor, não assinale mais de uma alternativa

Nas questões abaixo você tem TRÊS opções de respostas ➲	**Verdadeiro**	**Falso**	**Não sei**
O objetivo dos regulamentos (políticas, normas e regras) de segurança da informação é fazer com que o uso das informações existentes na unidade aconteça de forma estruturada, possibilitando que o serviço não seja prejudicado por um mau uso da informação: seja por erro ou acidente.			
Para que uma senha seja classificada como "senha forte" ela deve abranger caracteres numéricos, letras e símbolos e deve ser de uso individual.			
O acesso ao ambiente computacional é feito por meio da identificação (login) e da autenticação (senha). O login informa ao ambiente computacional quem eu sou e a senha garante que eu realmente sou quem eu digo ser.			
Tanto o acesso a internet na unidade quanto o e-mail profissional são recursos da organização (HUSM) e somente devem ser utilizados para propósitos profissionais.			
Todas as ações que envolvem o uso das informações existentes na unidade implicam em conseqüências para as mesmas. Devem, portanto, ser observados o sigilo das informações bem como a correta manipulação das mesmas.			
A segurança da informação é responsabilidade de todos, portanto os riscos relacionados à informação quando identificados devem ser imediatamente reportados aos profissionais responsáveis.			
Nas questões abaixo você tem DUAS opções de respostas ➲	**Verdadeiro**	**Falso**	
Ao fazer uso do e-mail procuro sempre abrir os arquivos anexados quando tenho certeza da procedência dos mesmos e da inexistência de vírus.			

Ao escolher uma senha procuro sempre escolher dados que possam ser facilmente lembrados tais como data de nascimento, seqüência de números (12345) ou seqüência de letras do teclado (QWERTYU).		
Em ambientes públicos (elevadores, corredores, ônibus etc.) procuro sempre não falar sobre assuntos da unidade a fim de manter sigilo das informações da mesma.		
Procuro não deixar informações importantes da unidade expostas ou em locais inadequados que possam comprometer a integridade e a confidencialidade das informações.		
Procuro notificar (comunicar) os responsáveis quando percebo algum risco relacionado às informações da unidade.		
Se houvesse uma política de segurança da informação na unidade com certeza procuraria alinhar meu comportamento aos controles definidos na política de segurança da informação.		
Tanto no ambiente convencional quanto digital ao descartar as informações importantes procuro inutilizá-las definitivamente a fim de preservar a confidencialidade das informações.		
Ao encaminhar informações importantes à outras pessoas. Saliento sobre a importância em se preservar a confidencialidade dos dado que estão sendo entregues.		
Ao encaminhar mensagens por e-mail não costumo observar atenciosamente os destinatários, pois geralmente não tenho tempo para isso.		
Nas questões abaixo você tem duas opções de respostas ➲	👍☺ **Verdadeiro**	👎😐 **Falso**
Na minha opinião não existe necessidade de se implantar uma política de segurança da informação na unidade pois a mesma não apresenta riscos que possam comprometer as informações existentes.		
Não vejo problema na utilização de e-mail pessoal para fins profissionais.		
Estou consciente que minha senha não deve ser disponibilizada a outras pessoas. Entretanto devido a natureza de meu trabalho é natural que eu disponibilize a minha senha para colegas de trabalho (desde que eu confie nele).		
Sei que deveria informar as pessoas responsáveis os incidentes relacionados à segurança das informações identificados por mim, mas geralmente não procedo desta forma por entender que esta não seja uma atribuição minha.		
Na minha opinião, dentre as atividades que realizo na unidade não executo nenhuma ação que possa comprometer a segurança da informação.		
TOTAL DE PONTOS		

Unidade e turno em que trabalha

☐ UCI **Turno** ☐ 08:00 – 12:00 ☐ 12:00 – 16:00 ☐ 16:00 – 20:00 ☐ 20:00 – 08:00

☐ UTI **Turno:** ☐ 07:00 – 13:30 ☐ 13:30 – 19:30 ☐ 19:30 – 07:30

Função que desempenha

☐ Médico ☐ Enfermeiro ☐ Fisioterapeuta ☐ Auxiliar Administrativo

☐ outra Qual ?_____

Cargo que ocupa

☐ Diretor ☐ Supervisor ☐ Funcionário ☐ Estagiário ☐ Outro. Qual? _____

Tempo de serviço

☐ até 5 anos ☐ até 10 anos ☐ até 15 anos ☐ Outro Qual? _____

Faixa etária

☐ de 18 - 25 ☐ de 26 – 35 ☐ de 36 – 45 ☐ de 46 – 55 ☐ de 56 ou mais

Sexo ☐ Feminino ☐ Masculino

Grau de Instrução

☐ Doutorado ☐ Mestrado ☐ Pós-Graduação ☐ Graduação ☐ Nível Técnico

☐ Outro. Qual? _____

OBRIGADO PELA SUA PARTICIPAÇÃO

APÊNDICE E – Formulário de avaliação do entendimento da PSI

BAIXO	REGULAR	ALTO
☹	😐	?☺!
1	2	3

Entendimento da PSI			
1. Conceitos Básicos			
- Conceito	1	2	3
- Objetivos	1	2	3
- Benefícios	1	2	3
- Comitê	1	2	3
2. **Responsabilidades**			
- Manter a salvaguarda	1	2	3
- Zelo e manutenção da informação	1	2	3
- Comprometimento com segurança da informação	1	2	3
- Sigilo da informação	1	2	3
- Backup	1	2	3
- Pastas compartilhadas	1	2	3
- Login e senha individual	1	2	3
- Alteração das informações	1	2	3
- Bloqueio do PC	1	2	3
- Manipulação irregular	1	2	3
- Bloqueio de login e senha por motivos de licença, férias etc.	1	2	3
- Internet (tempo e conteúdo de acesso)	1	2	3
- Manuseio de equipamentos por profissionais autorizados	1	2	3
- Descarte de informações	1	2	3
- Uso de notebook	1	2	3
- Documentos com informações de pacientes	1	2	3
- Ordem de prontuários	1	2	3
- Documentos na impressora	1	2	3
- Respeito e cumprimento da PSI	1	2	3

APÊNDICE F – Logomarca da gestão de segurança da informação

APÊNDICE G – FOLDER DO PROGRAMA DE CONSCIENTIZAÇÃO E TREINAMENTO – FACE 1

Evento

PROGRAMA DE CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

Professor Responsável:
Prof. Dr. Raul Ceretta Nunes

Equipe de execução:
Cristiane Ellwanger – PPGEP
Maria Angélica F. Oliveira – PPGEP

OBJETIVO

Promover a conscientização e treinamento em segurança da informação na Unidade de Cardiologia Intensiva (UCI) e na Unidade de Terapia Intensiva (UTI) – Adulto do HUSM.

JUSTIFICATIVA

Tanto a conscientização quanto o treinamento visam conscientizar os funcionários da importância em se adquirir uma cultura voltada à segurança da informação, e fornecer embasamentos teórico-práticos para que os mesmos possam se envolver no processo de Gestão da Segurança da Informação, colaborar para se garantir a confidencialidade, integridade e a disponibilidade das informações existentes nas unidades e se comprometer para com a política de segurança da informação.

BENEFÍCIOS

O principal benefício é contribuir para a minimização dos riscos existentes nas unidades. Outros benefícios são:

- Maior confiança dos (potenciais) clientes, fornecedores e envolvidos no processo de segurança da informação;
- Melhor proteção da confidencialidade das informações críticas;
- Maior confiabilidade e exatidão das informações internas;
- Índices menores de incidentes, erros e omissões;
- Melhor e mais rápida detecção dos riscos remanescentes de segurança;
- Melhoria de princípios éticos dos funcionários;
- Aumento da produtividade; e
- Melhor conformidade a normas e regulamentos organizacionais.

METODOLOGIA

Tanto a conscientização quanto o treinamento serão realizados em duas etapas distintas conforme segue:

1ª ETAPA - No processo de Conscientização serão expostos os conceitos fundamentais da Gestão de segurança da informação e os riscos identificados que possam comprometer a segurança das informações a fim de que os profissionais alocados nas respectivas unidades possam perceber a relevância do assunto e contribuir para que seu comportamento não entre em conflito com a política de segurança da informação bem como com as normas organizacionais vigentes.

Posteriormente no processo de treinamento será divulgada a política de segurança da informação com o esclarecimento de seus principais pontos, bem como será realizada a entrega de uma cópia da mesma a cada participante para que possam analisá-la e sugerir melhorias.

2ª ETAPA - A realização da segunda etapa visa o fortalecimento da cultura voltada à segurança da informação bem como esclarecer as possíveis dúvidas que por ventura não sejam sanadas na primeira etapa. Além disso, nessa ocasião será

APÊNDICE H – Folder do programa de conscientização e treinamento – face 2

divulgada a política de segurança definitiva a qual abrangerá se conveniente, as sugestões dos profissionais pertencentes às unidades.

As atividades serão realizadas em semanas alternadas conforme a disponibilidade de horário dos profissionais alocados nas unidades, durante o expediente normal com revezamento de profissionais para que não haja prejuízo de suas atividades normais de trabalho e em períodos não excedentes à 60 minutos por equipe de profissionais.

CRONOGRAMA

CONSCIENTIZAÇÃO			TREINAMENTO		
DATA	**TURNO**	**HORÁRIO**	**DATA**	**TURNO**	**HORÁRIO**
05/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30	19/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30
	Tarde	16:00 - 17:00 17:00 - 18:00		Tarde	16:00 - 17:00 17:00 - 18:00
	Noite	20:00 - 21:00 21:00 - 22:00		Noite	20:00 - 21:00 21:00 - 22:00
06/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30	20/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30
	Tarde	16:00 - 17:00 17:00 - 18:00		Tarde	16:00 - 17:00 17:00 - 18:00
	Noite	20:00 - 21:00 21:00 - 22:00		Noite	20:00 - 21:00 21:00 - 22:00
07/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30	21/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30
	Tarde	16:00 - 17:00 17:00 - 18:00		Tarde	16:00 - 17:00 17:00 - 18:00
	Noite	20:00 - 21:00 21:00 - 22:00		Noite	20:00 - 21:00 21:00 - 22:00
LOCAL: Sala de Reuniões da UCI					
26/08/2008	**Oficina de "Bioética e Privacidade".** Palestrante: Dra. Jennifer Braathen Salgueiro - Bióloga e membro do Comitê de Ética em Pesquisa do Hospital de Clínicas - Porto Alegre Horário: 16h as 18h Local: Auditótio Gulerpe Público-alvo: Profissionais de saúde do HUSM				

APÊNDICE I – Convite programa de conscientização e treinamento

GSI
Gestão de Segurança da Informação
Hospital Universitário
UFSM

Prezado Colaborador!

Solicitamos sua presença para a **Semana de Conscientização e Treinamento** que será realizada na sala de reuniões da UCI (Unidade Cardiológica Intensiva). As palestras terão uma hora de duração cada e serão oferecidas nos três turnos. Abaixo segue o cronograma de horários das palestras:

Conscientização			Treinamento		
Data	Turno	Horário	Data	Turno	Horário
05/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30	19/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30
	Tarde	16:00 - 17:00 17:00 - 18:00		Tarde	16:00 - 17:00 17:00 - 18:00
	Noite	20:00 - 21:00 21:00 - 22:00		Noite	20:00 - 21:00 21:00 - 22:00
06/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30	20/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30
	Tarde	16:00 - 17:00 17:00 - 18:00		Tarde	16:00 - 17:00 17:00 - 18:00
	Noite	20:00 - 21:00 21:00 - 22:00		Noite	20:00 - 21:00 21:00 - 22:00
07/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30	21/08/2008	Manhã	08:30 - 09:30 09:30 - 10:30
	Tarde	16:00 - 17:00 17:00 - 18:00		Tarde	16:00 - 17:00 17:00 - 18:00
	Noite	20:00 - 21:00 21:00 - 22:00		Noite	20:00 - 21:00 21:00 - 22:00

Contamos com sua participação neste evento.

Atenciosamente,

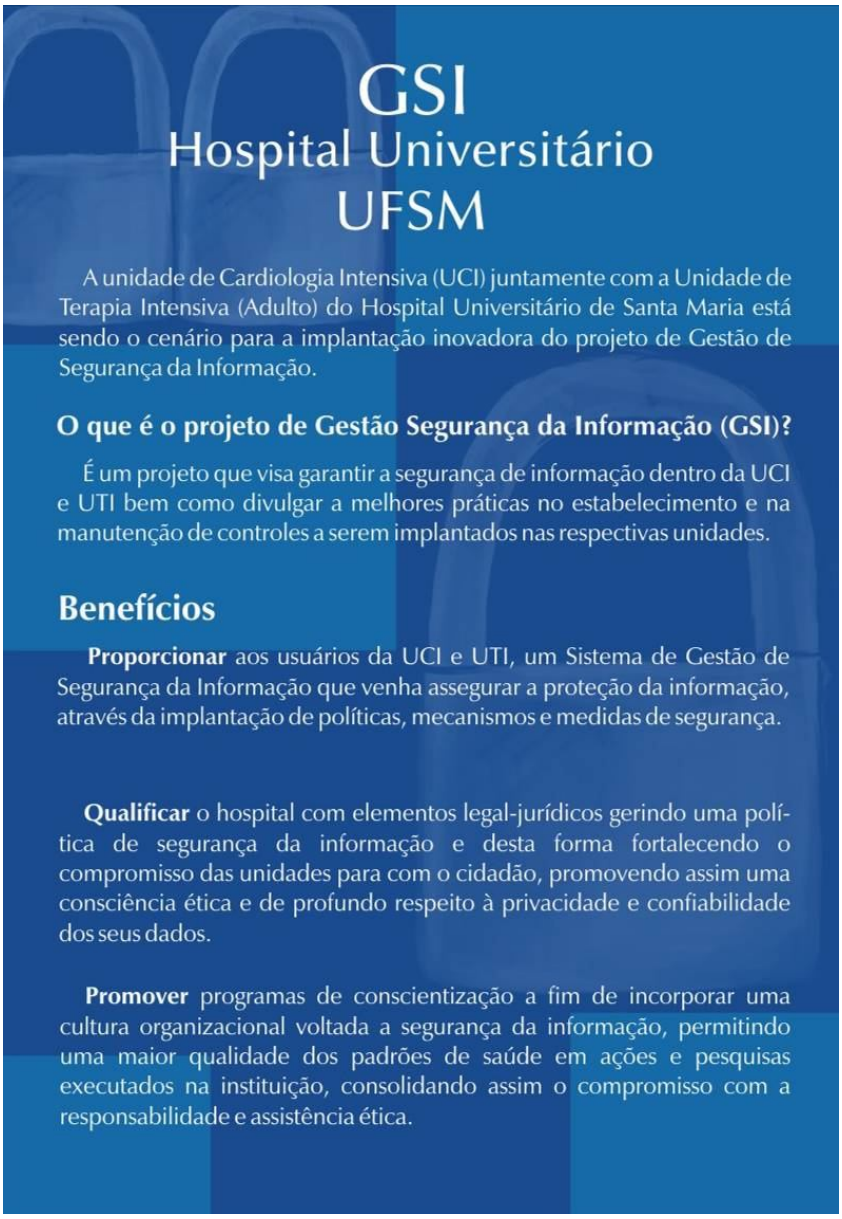
Equipe de Gestão de Segurança da Informação
Hospital Universitário de Santa Maria (HUSM)

Ramal do setor: 3220 2523-33
Contato via e-mail:

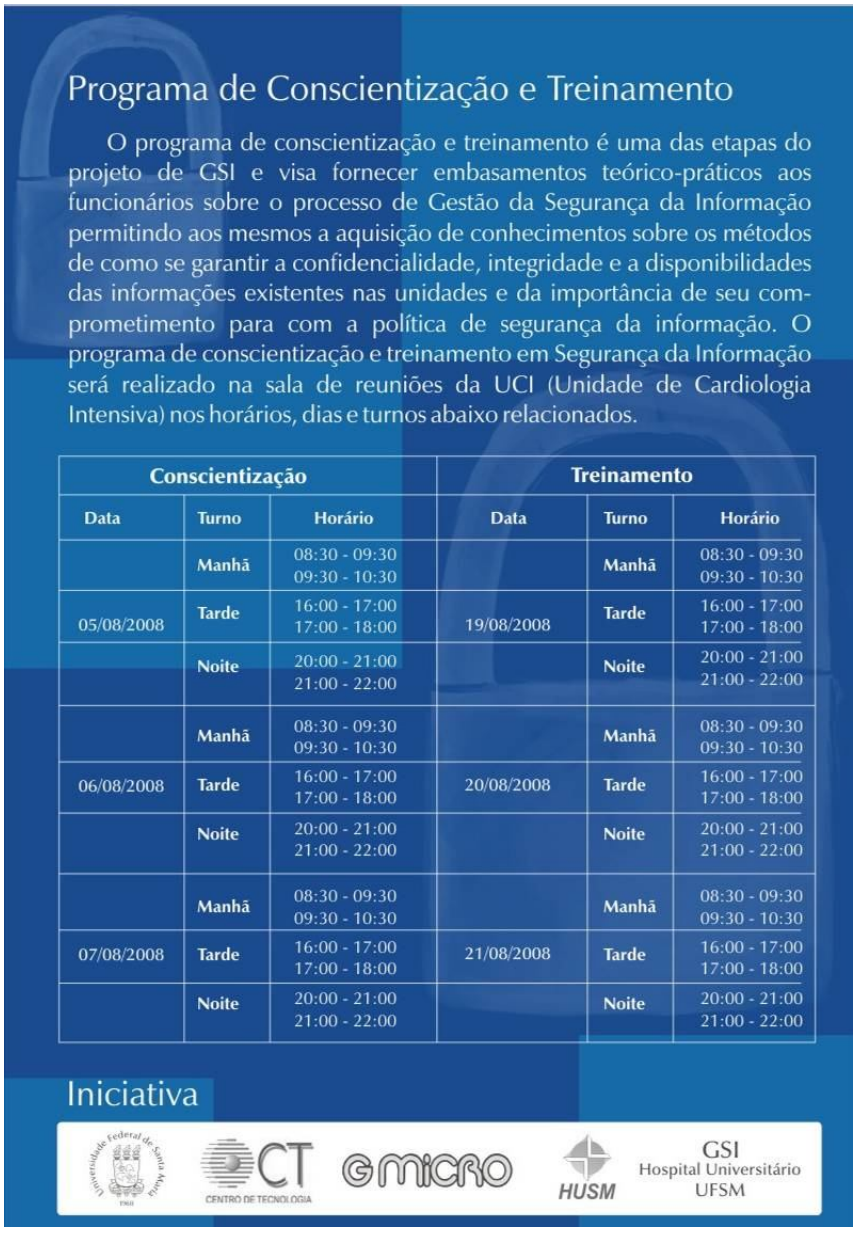
Iniciativa

CT CENTRO DE TECNOLOGIA · gmicro · HUSM · GSI Hospital Universitário UFSM

APÊNDICE J – Folder projeto de segurança da informação-face 1



APÊNDICE K – Folder projeto de segurança da informação-face 2



Programa de Conscientização e Treinamento

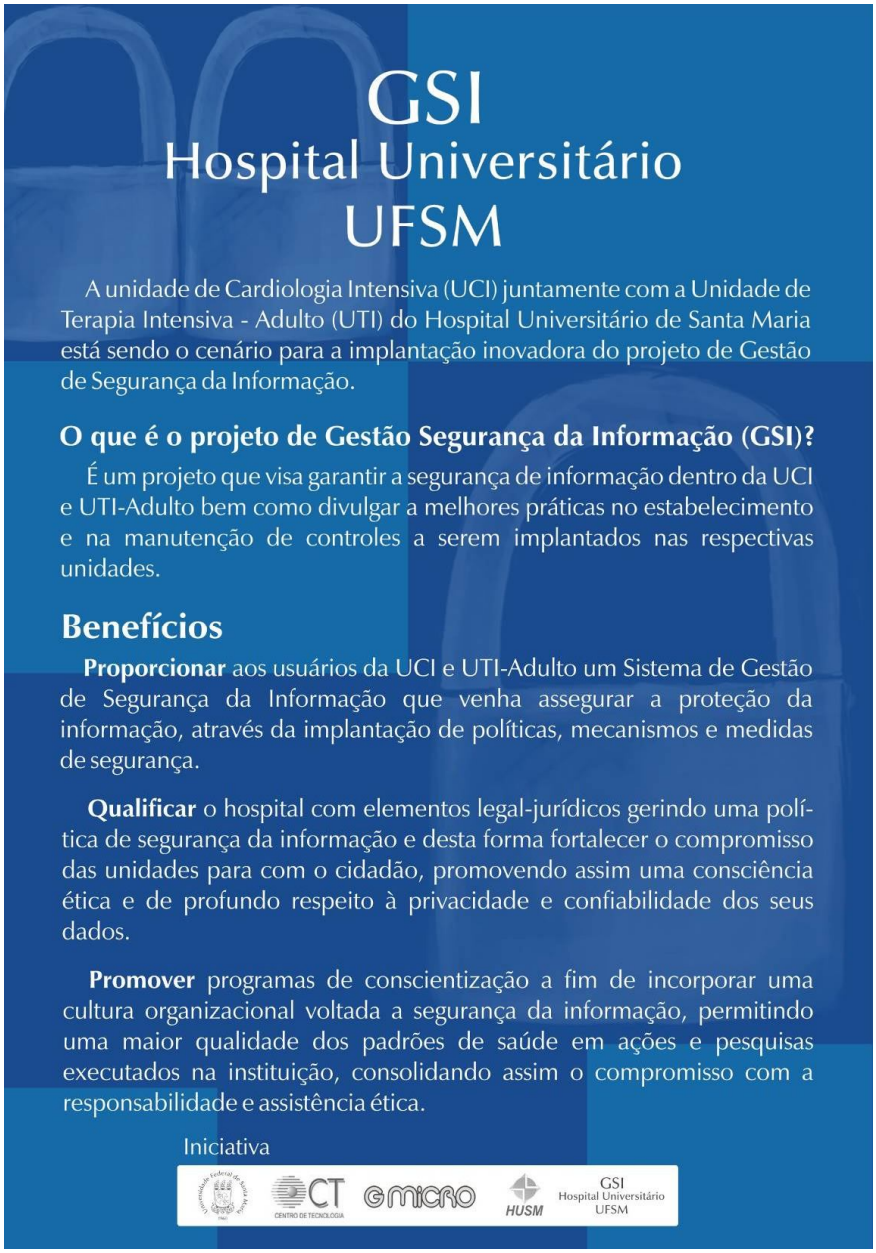
O programa de conscientização e treinamento é uma das etapas do projeto de GSI e visa fornecer embasamentos teórico-práticos aos funcionários sobre o processo de Gestão da Segurança da Informação permitindo aos mesmos a aquisição de conhecimentos sobre os métodos de como se garantir a confidencialidade, integridade e a disponibilidades das informações existentes nas unidades e da importância de seu comprometimento para com a política de segurança da informação. O programa de conscientização e treinamento em Segurança da Informação será realizado na sala de reuniões da UCI (Unidade de Cardiologia Intensiva) nos horários, dias e turnos abaixo relacionados.

Conscientização			Treinamento		
Data	Turno	Horário	Data	Turno	Horário
	Manhã	08:30 - 09:30 09:30 - 10:30		Manhã	08:30 - 09:30 09:30 - 10:30
05/08/2008	Tarde	16:00 - 17:00 17:00 - 18:00	19/08/2008	Tarde	16:00 - 17:00 17:00 - 18:00
	Noite	20:00 - 21:00 21:00 - 22:00		Noite	20:00 - 21:00 21:00 - 22:00
	Manhã	08:30 - 09:30 09:30 - 10:30		Manhã	08:30 - 09:30 09:30 - 10:30
06/08/2008	Tarde	16:00 - 17:00 17:00 - 18:00	20/08/2008	Tarde	16:00 - 17:00 17:00 - 18:00
	Noite	20:00 - 21:00 21:00 - 22:00		Noite	20:00 - 21:00 21:00 - 22:00
	Manhã	08:30 - 09:30 09:30 - 10:30		Manhã	08:30 - 09:30 09:30 - 10:30
07/08/2008	Tarde	16:00 - 17:00 17:00 - 18:00	21/08/2008	Tarde	16:00 - 17:00 17:00 - 18:00
	Noite	20:00 - 21:00 21:00 - 22:00		Noite	20:00 - 21:00 21:00 - 22:00

Iniciativa

CT CENTRO DE TECNOLOGIA · GMICRO · HUSM · GSI Hospital Universitário UFSM

APÊNDICE L – Cartaz de segurança da informação



APÊNDICE M – Cartaz da oficina de bioética e privacidade

APÊNDICE N – Lembretes de segurança

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Fazer backup das informações importantes.

Feliz Natal e um Próspero Ano Novo!!!

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Descartar as informações corretamente.

Feliz Natal e um Próspero Ano Novo!!!

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Manter sigilo de informações confidenciais.

Feliz Natal e um Próspero Ano Novo!!!

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Manter informações organizadas.

Feliz Natal e um Próspero Ano Novo!!!

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Possuir e-mail profissional para receber e enviar informações.

Feliz Natal e um Próspero Ano Novo!!!

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Utilizar o antivírus em anexos recebidos por e-mail.

Feliz Natal e um Próspero Ano Novo!!!

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Proteger, zelar e cuidar dos recursos de informação.

Feliz Natal e um Próspero Ano Novo!!!

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Participar dos programas de conscientização e treinamento.

Feliz Natal e um Próspero Ano Novo!!!

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Comunicar os problemas de segurança da informação verificados.

Feliz Natal e um Próspero Ano Novo!!!

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Manter a confidencialidade de suas senhas.

Feliz Natal e um Próspero Ano Novo!!!

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Armazenar corretamente as informações.

Feliz Natal e um Próspero Ano Novo!!!

Gestão de Segurança da Informação

Praticar a Segurança da Informação é:

Preservar as informações da exposição inadequada.

Feliz Natal e um Próspero Ano Novo!!!

APÊNDICE O – Brindes promocionais

APÊNDICE P – Lembretes da GSI

Gestão de Segurança da Informação

10 LEMBRETES DA GSI

1. **NÃO COMPARTILHE SUA SENHA** – usuários que utilizam a mesma senha podem ser co-responsabilizados em caso de perda, extravio ou uso indevido de informações.

2. Faça o **DESCARTE CORRETO** das informações – rasgue ou triture as informações desnecessárias;

3. **ARMAZENE CORRETAMENTE** as informações a que tem acesso - informações devem ser organizadas em locais adequados. Não deixe informações confidenciais dispostas pelo local de trabalho;

4. **FAÇA BACKUP (CÓPIAS)** das informações. Isso permite a recuperação de informações importantes;

5. Seja profissional, **MANTENHA SIGILO DAS INFORMAÇÕES** confidenciais a que tem acesso. Evite o vazamento de informações em corredores, elevadores e locais onde não haja privacidade;

6. Ao sair de reuniões **NÃO DEIXE CARIMBOS SOBRE A MESA, INFORMAÇÕES EM QUADROS OU EM PAPÉIS DE RASCUNHO**. Outras pessoas podem ter acesso a estas informações;

7. A internet e o e-mail profissional são recursos da instituição. **UTILIZE-OS DE FORMA RESPONSÁVEL**;

8. **PROTEJA, ZELE, CUIDE OS EQUIPAMENTOS** que estão sob sua responsabilidade. Eles são necessários para o bom desempenho de sua função e contribuem para a sua imagem profissional;

9. **COMUNIQUE INCIDENTES**, ou seja, as situações que possam comprometer as informações. Esta ação contribui para a melhoria contínua da segurança da informação;

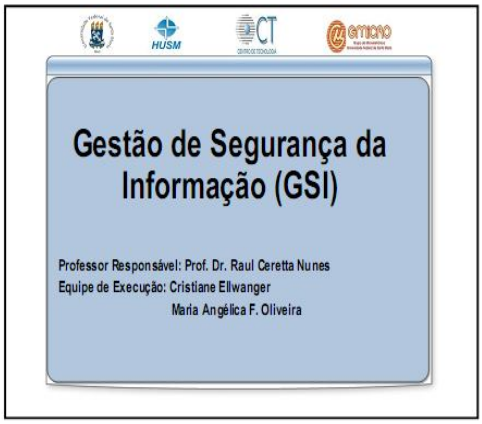
10. **PARTICIPE DOS PROGRAMAS DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO**. Eles contribuem para o seu desenvolcimento intectual e profissional.

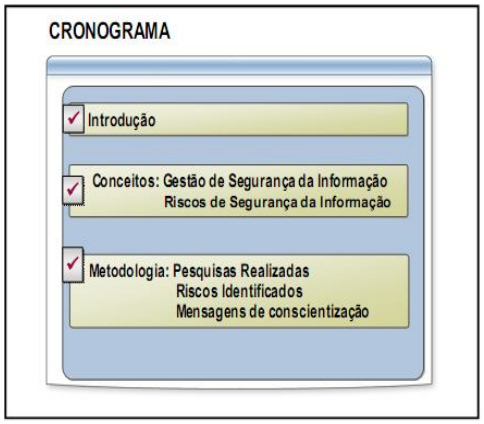
COLABORE.
Faça sua Parte !!!!

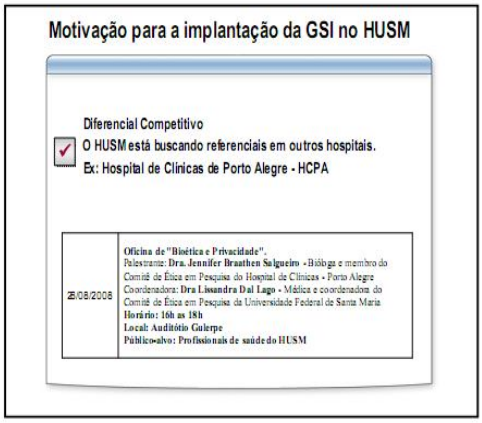
Dúvidas/Sugestões: www. husm.ufsm.br – link GSI
e-mail: gsi_husm@smail.ufsm.br

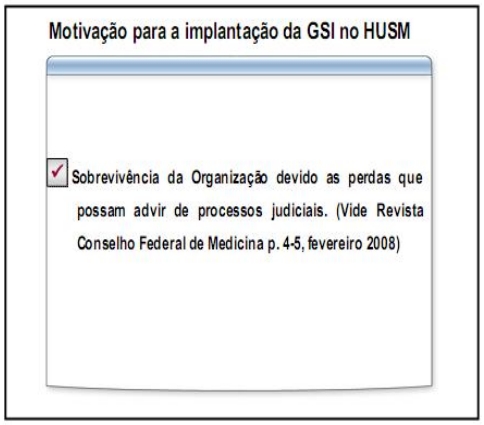
"A SEGURANÇA DA INFORMAÇÃO É RESPONSABILIDADE DE TODOS".

APÊNDICE Q – Apresentação de conscientização em segurança da informação

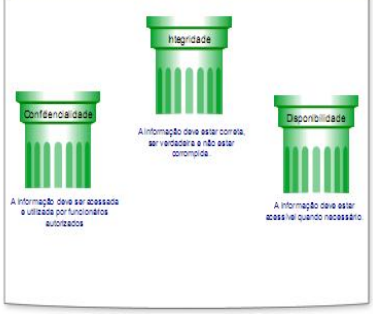








Conceitos Fundamentais da GSI – Princípios



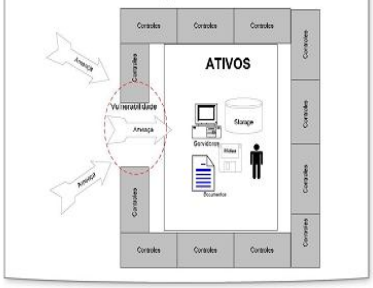
Riscos de Segurança da Informação - Conceitos

AMEAÇAS/VULNERABILIDADES:

"Ameaças são agentes externos ao ativo de informação, que se aproveitando de suas vulnerabilidades poderá quebrar a confidencialidade, integridade e disponibilidade da informação suportada ou utilizada por esse ativo."

Riscos de Segurança da Informação - Conceitos

RISCO = AMEAÇA + VULNERABILIDADE



Como o Projeto começou

Porque fazer a Pesquisa de Clima Organizacional?

Pesquisa de Clima Organizacional: tem por intuito verificar como se sente o público interno da organização

No processo de Gestão de GSI seu principal objetivo foi:

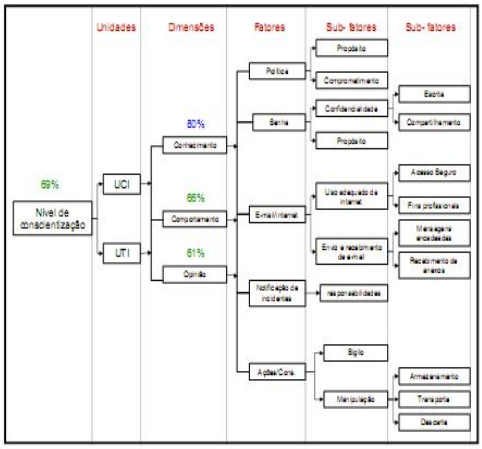
- Verificar a motivação existente
- Verificar o nível de resistência

Porque fazer a Pesquisa de Conscientização?

Pesquisa de Conscientização: tem por intuito verificar o nível de conscientização em segurança da informação existente nas unidades.

No processo de Gestão de GSI seu principal objetivo foi:

- Verificar o conhecimento
- Verificar o comportamento
- Verificar a opinião



Porque fazer a Pesquisa de Percepção?

Para medir o nível de conhecimento ou a percepção com o tema Segurança da Informação.

No processo de Gestão de GSI seu principal objetivo foi:

- Verificar o nível da percepção do que já existe.
- Verificar o nível de expectativa do que se gostaria que existisse.

Considerações finais

Nível percebido com relação a Qualidade da Segurança da informação → 75% - nível baixo

Nível de entendimento em segurança da informação → apenas 27,8% reconhecem ter um alto nível

60,8% → não estão satisfeitos com a valorização que é dada ao sigilo das informações existentes na unidade.

86,9% → se sentem participantes e responsáveis pelas conquistas obtidas.

87% → acreditam não ter a infra-estrutura necessária para o bom desempenho de suas atividades.

73,8% → Possuem um nível baixo de conhecimento dos canais de comunicação.

65,5% → acreditam que os canais repassam um baixo nível de informação.

Alguns Riscos Identificados

- Falta de conhecimento sobre o tema "segurança da informação";
- Inexistência de e-mail profissional nas unidades;
- Não há procedimentos adequados para o descarte das informações;
- As informações não são classificadas quanto as suas características de proteção;
- Inexistência de um termo de confidencialidade para as unidades;
- Engenharia Social;
- Impossibilidade de realização de autoria dos profissionais;
- Acesso não controlado aos computadores das unidades;
- Incidentes de segurança não são reportados;
- Profissionais não sabem a quem reportar os problemas de segurança.

Algumas estratégias implantadas

Comitê Gestor de Segurança da Informação

Importância da Conscientização

A maioria das falhas de Segurança da Informação são decorrentes de fatores humanos.

Fonte: 10º Pesquisa Nacional de Segurança da Informação, 2007

Mensagens de conscientização

Escolha uma senha fácil de ser lembrada e difícil de ser descoberta por outras pessoas.

Ao descartar qualquer informação em mídia impressa ou eletrônica destrua-a completamente. (reuniões)

Mensagens de conscientização

Ao ausentar-se do local onde esta o computador que você utiliza, deixe-o protegido (bloqueio).

Não forneça informações confidenciais a pessoas estranhas a unidade (telefone, elevadores, corredores).

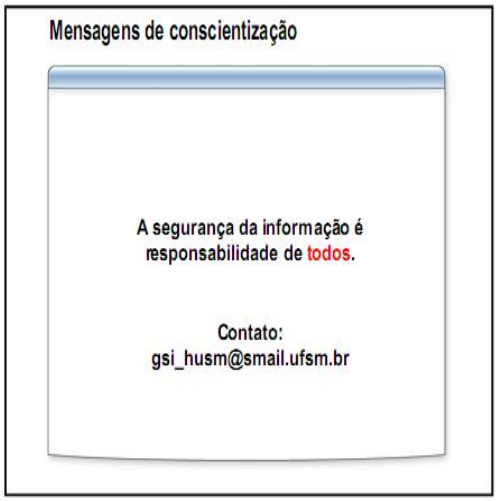
Mensagens de conscientização

Faça backups das informações críticas da unidade (disponibilidade).

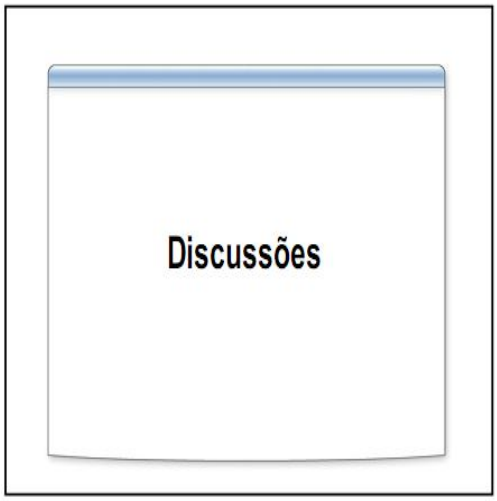
Nunca abra arquivos executáveis recebidos em anexos (.exe, .bat, .src, .lnk).
Observem os destinatários ao enviar mensagens encadeadas.

Mensagens de conscientização

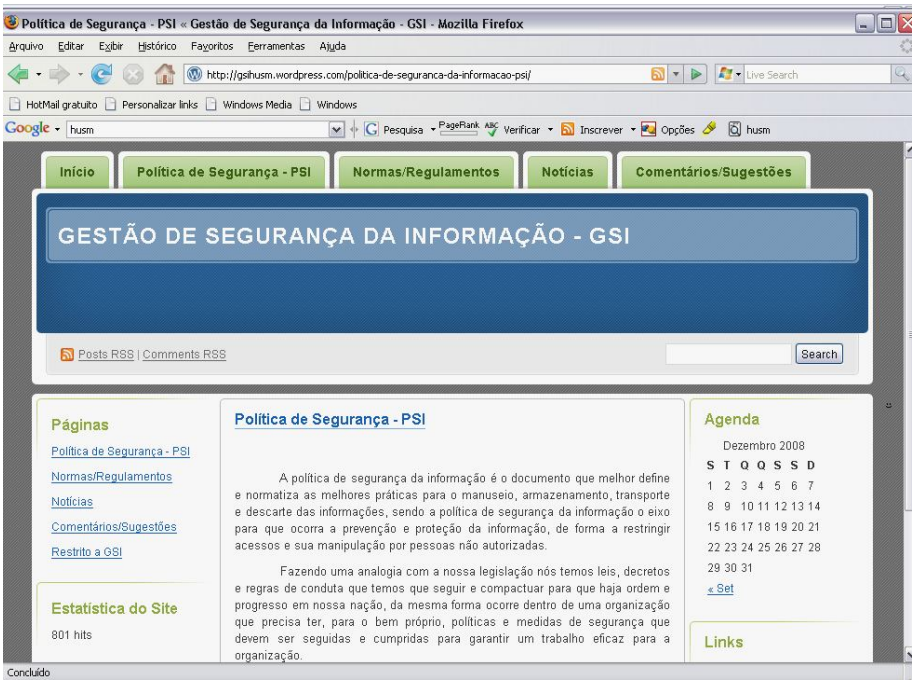
Não deixar documentos do paciente como prontuários, fichas de exames, notas de internação em lugar visível ao público externo.


Mensagens de conscientização
A segurança da informação é responsabilidade de todos.
Contato:
gsi_husm@smail.ufsm.br

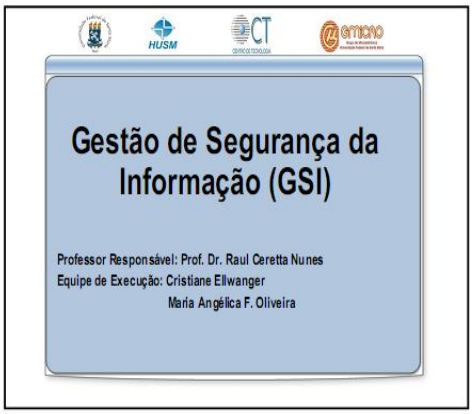

OFICINA DE "BIOÉTICA E PRIVACIDADE"
26/08/2008 16h as 18h Gulerpe
Palestrante: Drª. Jennifer Braathen Salgueiro - Bióloga e membro do Comitê de Ética em Pesquisa do Hospital de Clínicas de Porto Alegre.
Coordenadora: Drª Lissandra Dal Lago - Médica e Coordenadora do Comitê de Ética em Pesquisa da Universidade Federal de Santa Maria.
Público-alvo: Profissionais da saúde do HUSM
Promoção: Gestão de Segurança da Informação (GSI)
Apoio: Comitê de Biosegurança do HUSM
HUSM
CT

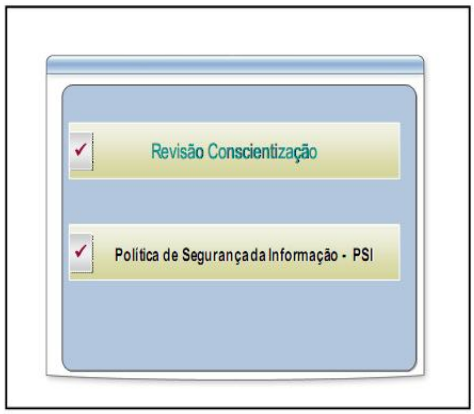

Discussões

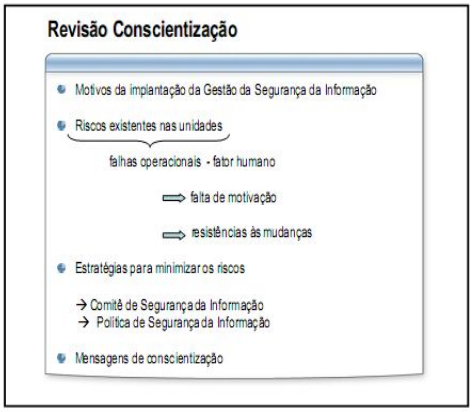
APÊNDICE R – Site desenvolvido para a gestão de segurança da informação – GSI

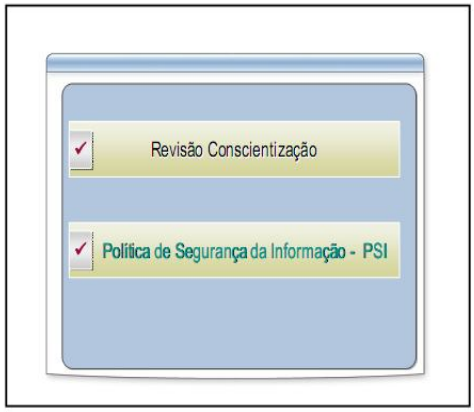


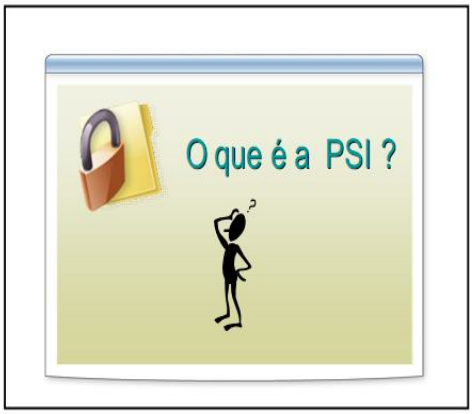
APÊNDICE S – Apresentação do treinamento em segurança da informação

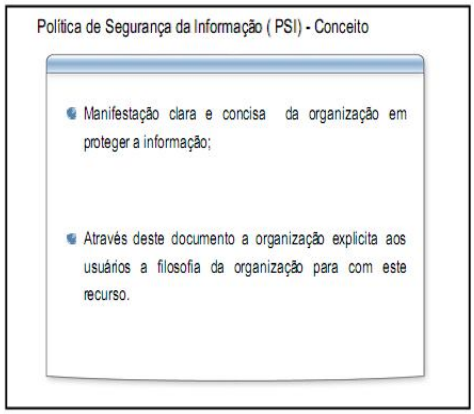




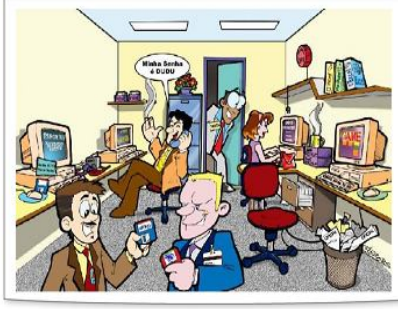








Ambiente de Trabalho sem PSI



Política de Segurança da Informação (PSI) - Objetivos

- Uso da informação aconteça de forma estruturada possibilitando que o negócio não seja prejudicado pelo mau uso da informação: seja por erro ou por acidente;

CONTROLES

Comitê Gestor de Segurança da Informação

Responsabilidades dos Usuários

- Manter a salvaguarda dos recursos de informação sob sua responsabilidade;
- Zelar pela manutenção das informações bem como pela preservação da confidencialidade, integridade e disponibilidade das mesmas;
- Comprometer-se com as informações a que tem acesso devendo mantê-la segura.
- Manter sigilo de informações críticas presentes nas unidades, dentre as quais se destacam aquelas que dizem respeito ao prontuário do paciente, não as divulgando sem consentimento prévio;

Responsabilidades dos Usuários

- Responsabilizar-se pela realização de backups (cópias) dos dados necessários ao desempenho de suas atividades;
- Evitar colocar dados importantes em pastas compartilhadas, pois esta prática pode ocasionar problemas de confidencialidade à informação;
- Manter um login e senha de acesso individual aos sistemas de informação do HUSM não sendo permitido o seu compartilhamento com outros usuários.
- Usuários não devem alterar informações que não estão sob sua responsabilidade.

Responsabilidades dos Usuários

- 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.
- A manipulação irregular, divulgação ou uso indevido da informação e dos recursos computacionais da UCI e UTI não é permitida.
- Ao encaminhar informações sigilosas para outros setores, salientar a importância da confidencialidade dos dados quanto ao seu transporte.
- Usuários que se desligarem das unidades, entrarem em licença ou de férias e que tenham acesso aos sistemas da instituição devem solicitar o bloqueio de seu login de senha.

Responsabilidades dos Usuários

- O tempo de permanência dos usuários na internet e o conteúdo acessado por eles devem ser de propósitos profissionais não sendo permitido o uso de ferramentas de conversação instantânea.
- O acesso e o manuseio dos equipamentos computacionais das unidades só podem ser realizados por usuários alocados nas unidades, do contrário somente com autorização do responsável.
- Informações consideradas importantes, em papel ou em qualquer outra mídia, que não são mais utilizadas devem ser destruídas antes de serem colocadas no lixo.

Responsabilidades dos Usuários

- Conforme regras estabelecidas pelo DEPE e Serviço de Informática do HUSM, todo o usuário que faz uso de notebook e acesse a rede de computadores da instituição, deve assinar o termo de responsabilidade e de confidencialidade.

Definição pela circular nº11-2008-DEPE/HUSM de 04 de Julho de 2008, comprometendo-se a manter sigilo sobre dados confidenciais que por ventura possa ter acesso e/ou deles não lançar mão em nenhum outro âmbito e/ou necessidade, que não seja a de prestar serviço a instituição.

Responsabilidades dos Usuários

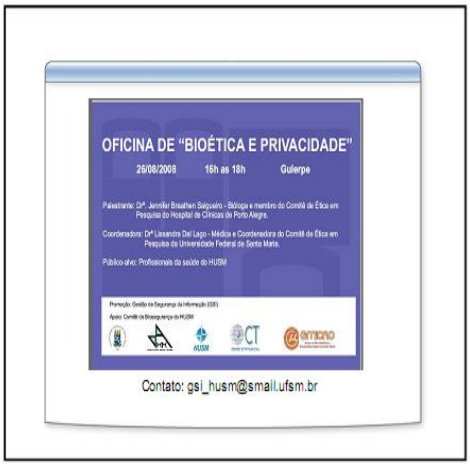
- Os documentos do paciente como prontuários, fichas de exames, notas de internação não devem ficar expostos em local visível ao público externo.
- Os prontuários devem estar organizados conforme o documento que determina a ordem para a montagem de prontuários determinada pelo serviço de Análise de Prontuários.
- Relatórios ou documentos impressos não devem ficar dispostos na impressora por longos períodos de tempo.
- Respeitar e cumprir as determinações desta política de segurança da informação. O não cumprimento das normas, implica em sanções que podem variar com o danos causados às unidades.

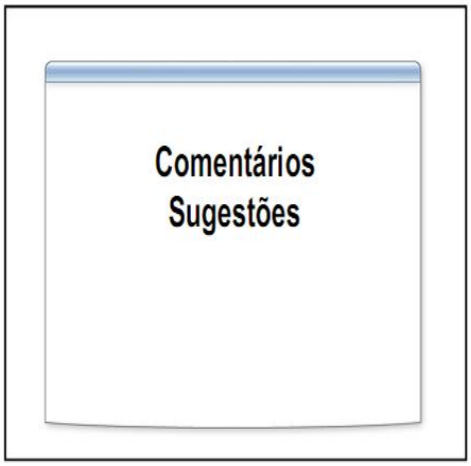
Responsabilidades dos Usuários

- Informar a algum membro do Comitê Gestor de Segurança da Informação imediatamente qualquer violação das normas estabelecidas incluindo as não intencionais e culposas.

Responsabilidades dos Usuários

A segurança da informação é responsabilidade de todos.


OFICINA DE "BIOÉTICA E PRIVACIDADE"
26/08/2009 16h as 18h Gulerpe
Palestrante: Drª. Jennifer Braathen Salgueiro - Bióloga e membro do Comitê de Ética em Pesquisa do Hospital de Clínicas de Porto Alegre.
Coordenadora: Drª Lisandra Dal Lago - Médica e Coordenadora do Comitê de Ética em Pesquisa da Universidade Federal de Santa Maria.
Público alvo: Profissionais da saúde do HUSM
HUSM
Contato: gsi_husm@smail.ufsm.br


Comentários
Sugestões