Modalidade do trabalho: Ensaio teórico
Evento: IV Seminário de Inovação e Tecnologia

GESTÃO DE SEGURANÇA DE INFORMAÇÕES NAS EMPRESAS[1]

Guilherme Ströher Renz[2], Daniel Knebel Baggio[3], Matheus Feigel Grison[4], Bruna Faccin Camargo[5], Renato Przyczynski[6].

[1] Artigo utilizado na Especialização em Gestão Estratégica e adaptado para o Salão do Conhecimento
[2] Professor do Instituto Federal Farroupilha no Curso de Administração e Mestrando em Desenvolvimento na Unijuí, guilherme@conectait.com
[3] Professor do Programa de Mestrado em Desenvolvimento da Unijuí, Mestre em Contabilidade e Finanças e Doutor em Contabilidade e Finanças, danibaggio@gmail.com
[4] Administrador de Empresas, Mestrando em Desenvolvimento na Unijuí, matheusgrison@hotmail.com
[5] Contadora, Mestranda em Desenvolvimento pela Unijuí, Analista de Implementação de Sistemas, brunafaccinflor@hotmail.com
[6] Professor de Administração do Instituto Cenecista de Ensino Superior de Santo Ângelo, Mestre em Desenvolvimento, Doutor em Administração, renatoprzy@gmail.com

1 INTRODUÇÃO

A ascensão econômica constante das organizações no cenário econômico atual ocasionado pelo escalonamento da globalização provoca uma ruptura no processo de gestão das empresas até que elas se adaptem as novas exigências. Como parte desse processo evolutivo é necessária uma adaptação de todos os colaboradores, sobretudo, dos gestores que respondem pelo nível estratégico. Devido à massificação do uso da internet e da utilização de softwares que alimentam bases de dados cada vez mais robustas, as informações das empresas passam a correr risco em relação à sua segurança por serem abrangentes e por estarem disponibilizadas em ambientes tecnológicos facilmente acessáveis através de interfaces simples de operar como, por exemplo, a rede mundial de computadores.

É indiscutível o papel da Tecnologia da Informação no cenário econômico, onde essas empresas estão inseridas. Entende-se que as empresas devem monitorar constantemente situações que possam ameaçar os seus negócios. O cuidado em identificar pontos críticos no acompanhamento das ameaças faz parte de um processo de gerenciamento da Tecnologia de Informação (TI) que a empresa deve utilizar, porém, muitas delas falham neste aspecto por desconhecimento, falta de capital humano qualificado e ausência de motivação. Sendo assim, o objetivo principal desse artigo é buscar na literatura estudos na área de Gestão da Informação que revelam a existência ou inexistência de políticas de Gestão da Segurança da Informação (GSI) adotada nas empresas.

Modalidade do trabalho: Ensaio teórico
Evento: IV Seminário de Inovação e Tecnologia

O volume diário de dados gerados pelas organizações tem um valor relevante para os seus negócios. Informações sobre processos produtivos, fornecedores, projetos de produtos, custos, enfim, informações que são consideradas estratégicas diante do mercado, são a todos os momentos armazenadas e trabalhadas em computadores e dispositivos digitais. A informação é inserida em mídias de armazenamento, podendo ser um servidor de dados, um ambiente virtual ou até mesmo um disco removível como pendrive. É relevante também ressaltar que a crescente utilização de meios digitais está possibilitada pela transmissão de dados em redes de comunicação. Sendo assim, o que importa é verificar a maneira que os gestores pensam a segurança desses dispositivos e redes de comunicação que, por inúmeras razões tecnológicas, não são à prova de falhas.

Partindo dessa afirmação, este estudo tem como objetivo fundamental investigar a existência de políticas de GSI nas organizações.

2 ESTUDOS RELACIONADOS À GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Para tratar do assunto da gestão da segurança da informação das empresas, é inevitável conhecer alguns conceitos que permeiam esse assunto. Indiscutivelmente, as PSI – Políticas de Segurança da Informação – fazem frente a esse assunto. Alguns autores, Nosworthy (2000), por exemplo, definem a PSI como uma forma de demonstração de comprometimento da alta administração para com a segurança da informação.

Whitmann (2004) salienta que a PSI é um ponto de partida para a segurança da informação. Ele ainda enfatiza que é a partir dela que a organização cria todo um perfil que irá regulamentar as atitudes relacionadas à segurança. O autor também relata que a PSI é responsável pela definição do papel da segurança da informação no apoio e no suporte à visão e missão organizacional e que estas devem propiciar uma complementação do objetivo de negócio principal da organização, permitindo que a empresa trabalhe de maneira correta, controlada e segura.

De acordo com Höne e Eloff (2002), as políticas de segurança da informação (PSI) têm uma grande importância na esfera técnica. Porém, segundo eles, a sua efetividade vem sendo o maior desafio aos profissionais responsáveis por ela em virtude da manipulação humana. Ainda segundo os autores referenciados, o fator humano tem sido o principal responsável pelos incidentes relacionados à segurança de dados empresariais e corporativos.

Neste âmbito a valorização das políticas de segurança da informação de maneira subjetiva por parte de todos os colaboradores, aponta para uma melhoria da sua efetividade, ocasionando assim uma alavancagem do ponto de vista estratégico das empresas, visto que política de gestão da segurança da informação pode se tornar um fator competitivo no cenário dos negócios.

Modalidade do trabalho: Ensaio teórico
Evento: IV Seminário de Inovação e Tecnologia

Segundo relatam Ernest e Young (2004), o grande desafio das empresas é conscientizar o capital humano das importâncias que uma PSI tem para a empresa e seus clientes e não só para ela como também para seus colaboradores, visto que informações sobre eles também estão dentro desse contexto. Estudando os riscos da falta de políticas de Gestão de Segurança da Informação (GSI), percebe-se a importância da adesão dos diretores à gestão da segurança, pois são eles os responsáveis por organizar estrategicamente uma política que universalize as ideias da organização e representa um quesito relevante no posicionamento estratégico da empresa diante do mercado global.

Outro conceito do CERT (Comitê Brasileiro de Resposta a Tratamento de Incidentes) que se deve ter em mente é com relação a ameaças. Segundo o CERT, ameaça é a quebra de uma ou mais das três propriedades fundamentais relacionadas à segurança, que seriam elas: confidencialidade, integridade e disponibilidade (CERT, 2003).

A NBR ISO/IEC 27001:2006 ainda apresenta alguns cenários que podem e já fizeram parte de muitas organizações. A norma ilustra um possível ataque a site de comércio eletrônico da empresa. Segundo a norma, deveria haver uma pessoa com treinamento suficiente nos procedimentos apropriados para minimizar os impactos a clientes, fornecedores e a rotina organizacional.

Relevante salientar o conceito trazido por Cavalcante apud in Wilson, Turban & Zviran (1992). Os autores elencam a segurança da informação como uma preocupação constante quanto à proteção do ambiente computacional de ameaças deliberadas ou acidentais as quais exploram as vulnerabilidades e comprometam o uso de dados e dos sistemas de informações.

5 METODOLOGIA

Este trabalho se caracteriza como um estudo teórico, qualitativo, bibliográfico com o objetivo de buscar na literatura estudos teóricos e bases conceituais na área de Gestão da Informação que revelam a existência ou inexistência de políticas de Gestão da Segurança da Informação (GSI) adotada nas empresas.

3 RESULTADOS

Conforme a 9ª Pesquisa Nacional de Segurança da Informação realizada pela Modulo Security Solutions com cerca de 50% das 1000 maiores empresas brasileiras, foi verificado que existe a preocupação com segurança da informação, porém os números são preocupantes, veja o Gráfico 1 abaixo:

Modalidade do trabalho: Ensaio teórico
Evento: IV Seminário de Inovação e Tecnologia

Gráfico 1 – Empresas e Políticas de GSI
[gráfico 1.jpg]
Fonte: Adaptado de Modulo Security Solutions (2003) pelos autores

Como é possível perceber no Gráfico 1, 43% das empresas (9% Não sabem Informar, 17% Está em Desenvolvimento e 17% Não Possui Política Formalizada) a política não é formalizada ou está desatualizada, o que pode nos demonstrar uma imagem de falta de comprometimento da gestão dessas empresas com relação a GSI.

Constata-se que as empresas não têm a noção do quanto suas atitudes podem impactar no negócio ou não possuem condições de reverter esta situação. Segundo Höne e Eloff (2002):
(...) funcionários despreparados, não conscientes da importância da segurança da informação e que desconhecem os procedimentos necessários para garanti-la, podem comprometer significativamente a efetividade da mesma. (ELWANGLER 2009, p. 16 apud HÖNE & ELOFF, 2002).

A partir dessa citação e afirmação, pode-se elencar alguns métodos que possam facilitar a implementação de PSI dentro das empresas.

De acordo com Payne (2003), o endomarketing apresenta-se como uma estratégia de gestão voltada a um conjunto de aplicações de técnicas que teoricamente, tecnicamente e praticamente seriam capazes de resgatar um comprometimento dos usuários para que se engajem em utilizar as PSI adotadas pela gestão da empresa. Neste sentido, uma possível complexidade das PSI implantadas faz parte de um processo de gerenciamento das regras de conduta normativas o que provocaria um processo de resistência natural do ser humano.

O famoso dramaturgo Bernard Shaw já frisou certa vez: “Se ensinardes alguma coisa a um homem, ele nunca aprenderá.” Quando se fala em políticas de gestão da segurança da informação, se tem plena convicção que Shaw estava certo. O aprender, segundo ele, é um processo ativo. As pessoas aprendem fazendo. Por isso, se é objetivo da organização que os funcionários, colaboradores, diretores e presidentes se envolvam no processo de gestão da segurança da informação, é preciso que se ensine a eles a perceber a real importância desse processo na prática.

Como citado anteriormente, o endomarketing, uma das diversas áreas do marketing acaba sendo uma alternativa para motivar as empresas a adotarem uma política de Gestão de Segurança da Informação. Esta área do marketing pode nos possibilitar resultados satisfatórios no processo de colaboração coletiva e articulada da implementação das políticas de gestão da segurança da informação.

Modalidade do trabalho: Ensaio teórico
Evento: IV Seminário de Inovação e Tecnologia

Segundo Bekin (2005), o marketing é uma técnica que direciona suas ações para a satisfação dos seus clientes. Sendo assim, endomarketing ou marketing interno, estaria voltando suas ações aos clientes internos da empresa, ou seja, seus colaboradores.

Elwanger (2009) atribui muito bem esta ideia do endomarketing no conceito de organização moderna que se vivencia hoje. Segundo ela, a importância dada pelo endomarketing é a satisfação dos clientes internos sendo que esta acarreta o aumento da capacidade organizacional para satisfazer os clientes externos. Ao fazer uso da estratégia do endomarketing nas empresas, segundo ela, 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. Bekin (2005) enfatiza que esse processo garante a melhor qualidade de bens, serviços e produtividade de pessoas, visando à satisfação de seus clientes.

Cerqueira (2002), diz que o comprometimento das pessoas é obtido não somente com uma adesão externa e superficial, mas também como uma adesão interna. Essa reação interna segundo Cerqueira seria uma reação positiva ao que é proposto, esta reação sendo uma adesão voluntária a uma ideia, a uma nova ordem ou mudança futura.

No contexto da GSI, seria dos colaboradores aderirem de maneira voluntária à ideia de que eles são responsáveis pela segurança da informação através de atitudes comprometidas com a política de GSI.

A tabela 1 a seguir, apresenta os principais autores consultados para a realização do presente estudo a partir das contribuições para a teoria e para a prática organizacional.

Tabela 1- Autores consultados
[Tabela 1.jpg]
Fonte: Resultado da pesquisa.

A tabela apresenta um número considerável de autores, os quais investigaram os aspectos da Gestão da Informação. Dentre eles, destaca-se Whitmann (2004) que evidencia a importância das PSI dentro da organização. Essa importância é relevante visto que a PSI é o primeiro fator a ser adotado dentro de uma GSI. Ainda, Ernest e Young (2004) evidenciaram os fatores limitantes a uma política de Gestão da Informação eficiente e posteriormente Payne (2003) nos trás uma ferramenta que aborda as potencialidades de se utilizar o endomarketing para trabalhar a Gestão da Informação.

Modalidade do trabalho: Ensaio teórico
Evento: IV Seminário de Inovação e Tecnologia

CONSIDERAÇÕES FINAIS

Considerando o objetivo de buscar na literatura estudos na área de Gestão da Informação que revelam a existência ou inexistência de políticas de Gestão da Segurança da Informação (GSI) adotada nas empresas, pode-se dizer que, ao final do estudo, o objetivo foi atingido. Conforme ilustrado em gráfico da Modulo Security Informations, em 43% das empresas, as políticas de GSI não são formalizadas ou estão desatualizadas e até mesmo inexistem.

Os autores pesquisados foram relevantes por sua contribuição teórica para os estudos na área de Gestão da Informação. Dentre as principais contribuições, evidencia-se a importância de se construir e aplicar uma política de gestão da segurança da informação nas organizações. Os dados coletados foram analisados a partir dos principais conceitos e abordagens teóricas apresentadas no referencial bibliográfico da presente pesquisa.

Manter boas práticas de segurança suportadas por uma boa política de segurança da informação deve ser um os primeiros passos no sentido de reforçar o nível de confiança dos clientes em relação às organizações. Ainda, 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).

As abordagens sobre a efetividade das políticas de gestão da segurança de informação foram sustentadas nos estudos analisados neste artigo, tendo o objetivo geral como orientação principal de análise. A condição de desenvolvimento e implantação de políticas de segurança da informação está diretamente relacionada à capacidade dos colaboradores de interagir com esse as normas e procedimentos de segurança. O processo de cooperação dos colaboradores para o sucesso das políticas de segurança pode estar diretamente ligado aos valores pessoais, à cultura organizacional e ao conhecimento prévio sobre segurança da informação.

O endomarketing é uma ferramenta da Administração que possibilita escalonar a forma como se trata e como se comunica com todos os colaboradores da organização. Uma política de GSI deve ser adotada e utilizada por todos os atores organizacionais.

Ainda, tratando-se de um assunto que pode ser considerado estratégico para as organizações, considerando sua complexidade, recomenda-se que as organizações administrem seu capital intelectual a fim de construir uma política de gestão de segurança de informação qualificada, não só voltada à segurança da informação, mas também à gestão da Tecnologia da Informação (TI) como um ativo valioso.

Modalidade do trabalho: Ensaio teórico
Evento: IV Seminário de Inovação e Tecnologia

Como sugestão de estudos futuros, recomenda-se estudos empíricos voltados a analisar políticas de Gestão da Informação já implementadas, tendo como enfoque principal as ações de endomarketing como ferramenta de suporte à gestão da segurança da informação nas organizações.

REFERÊNCIAS BIBLIOGRÁFICAS

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

WHITMANN M. E. In Defence of the realm: undersatanding the threats to information security. International Journal of Information Management. Vol 24; pp. 43-47.2004.

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

ERNEST & YOUNG. Global Information Security Survey. Ernest & Young. 2004. Disponível em: http://www.ey.com Acesso: novembro 2012.

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/. Acesso em: 15 de agosto de 2011.

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.

CAVALCANTE, Sayonara de Medeiros; RAMOS, Anatália Sataiva Martins, Gestão da informação: um estudo teórico sobre a utilização do correio eletrônico dentro das políticas de segurança da informação, com base na norma ISO/IEC 17799. Anais do XXVII ENEGEP, Curitiba, 2002.

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

MODULO SECURITY INFORMATION. 9ª Pesquisa Nacional de Segurança da Informação. Disponível em: http://www.modulo.com.br/. Acesso em 14 de novembro de 2011.

ELWANGER, Cristiane. Impacto da Utilização de Técnicas de Endomarketing na Efetividade das Políticas de Segurança da Informação. Dissertação de Mestrado, UFSM. 2009.

PAYNE, S. Developing Security Education and Awareness Programs. Educause Leadership Strategies Series. Vol 8. Pp. 49-52. 2003.

Modalidade do trabalho: Ensaio teórico
Evento: IV Seminário de Inovação e Tecnologia

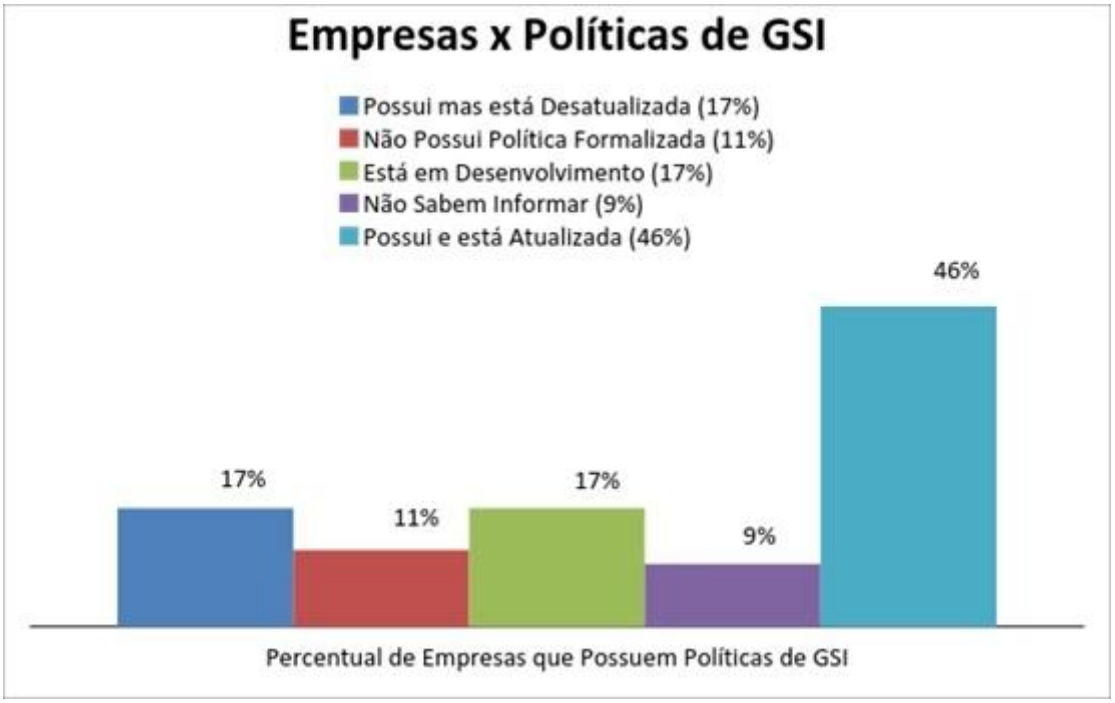

Gráfico 1 – Empresas e Políticas de GSI

Autores Consultados	Contribuições para a realização do estudo
Nosworthy (2000)	Definição de PSI
Whitmann (2004)	Importância da PSI
Höne e Eloff (2002)	Importância da GSI
Ernest e Young (2004)	Fatores limitantes a implantação de GSI
Payne (2003)	Ferramenta para a introdução dos conceitos de GSI nas empresas
Bekin (2005)	Conceitos importantes do Marketing e do Endomarketing
Cerqueira (2002)	Importância do Endomarketing para as organizações

Fonte: Resultado da pesquisa.

Tabela 1- Autores consultados