Revista Eletrônica de Sistemas de Informação
ISSN 1677-3071

Vol. 9, No 2

2010

doi:10.5329/RESI.2010.0902

Sumário

Revista hospedada em: http://revistas.facecla.com.br/index.php/reinfo
Forma de avaliação: *double blind review*

Esta revista é (e sempre foi) eletrônica para ajudar a proteger o meio ambiente. Ela voltou a ser diagramada em uma única coluna para facilitar a leitura na tela do computador. Mas, caso deseje imprimir esse artigo, saiba que ele foi editorado com uma fonte mais ecológica, a *Eco Sans*, que gasta menos tinta.

(mapa de palavras com os termos mais frequentes nos artigos desta edição)

PROPOSIÇÃO DE UM MODELO DINÂMICO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO PARA AMBIENTES INDUSTRIAIS

PROPOSITION OF A DYNAMIC MODEL FOR MANAGING SECURITY INFORMATION ON INDUSTRIAL ENVIRONMENTS

(artigo submetido em junho de 2010)

Alexandre dos Santos Roque
Programa de Pós-Graduação em Engenharia de Produção
Universidade Federal de Santa Maria (UFSM)
ale.roque@gmail.com

Raul Ceretta Nunes
Programa de Pós-Graduação em Engenharia de Produção
Universidade Federal de Santa Maria (UFSM)
ceretta@inf.ufsm.br

Alexandre Dias da Silva
Programa de Pós-Graduação em Engenharia de Produção
Universidade Federal de Santa Maria (UFSM)
adiass@gmail.com

ABSTRACT

The security information exchanged in industrial environment is a key factor for the success of modern organizations, because it refers to characteristics of the product and its manufacturing process. Such information is very sensitive and cannot be disclosed to competitors, under penalty of incurrence in competitiveness loss. The ongoing computerization brings benefits to the industry as it increases cooperation between people, but it also increases the vulnerability of information security. As a consequence, information security management models also need to change. This paper presents a bibliographic review about security issues concerning information management and proposes a dynamic management model in which people interaction, cooperation and motivation (senior management, sector managers and employees) are prioritized to achieve the new information security management requirements: responsibility, trust and ethics.

Key-words: security information; culture of security; industrial environment.

RESUMO

A segurança da informação que circula em ambiente de trabalho industrial é um fator fundamental para o sucesso das organizações modernas, pois, em geral, se refere a características do produto e de seu processo de fabricação, que são bastante sensíveis e não podem ser divulgadas para concorrentes, sob pena de perda de competitividade. A constante informatização traz benefícios às indústrias, pois aumenta a cooperação entre as pessoas, porém incrementa as vulnerabilidades da segurança da informação. Este incremento no nível de informatização é um fator que tem provocado mudança nos modelos de gestão de segurança da informação. Este artigo parte de uma pesquisa bibliográfica sobre os problemas relacionados à segurança da informação para, em seguida, propor um modelo dinâmico de gestão da segurança da informação em que a interação, a cooperação e a motivação das pessoas (alta-gerência, chefes e funcionários) são priorizadas para atender aos novos requisitos da gestão da segurança da informação: responsabilidade, confiança e ética.

Palavras-chave: segurança da informação; cultura de segurança; ambiente industrial.

1 INTRODUÇÃO

A tecnologia de informação e comunicação, bem como a de sistemas de informação baseados em computador, têm avançado rapidamente e possibilitado a informatização e transformação do ambiente industrial, resultando em novas estruturas organizacionais caracterizadas pela cooperação. A cooperação potencializa o compartilhamento da informação e as relações interpessoais e interorganizacionais (COSTA E FERREIRA, 2000). Desta forma, assim como no setor comercial, no setor industrial o ativo organizacional, que era basicamente composto por ativos físicos, passa a incorporar também a informação como um dos principais ativos. Sendo a informação um insumo essencial para o desenvolvimento de diversas atividades da empresa (VALENTIM *et al.*, 2008), mecanismos eficientes de gestão de segurança da informação são requeridos.

A gestão da segurança da informação pode ser encarada como um processo (NBR ISO/IEC 17799, 2005; NBR ISO/IEC 27001, 2006), mas um processo de gestão e não um processo tecnológico (SANTOS, 2008). É obtida por meio da implementação de controles, políticas e procedimentos que, juntos, fortalecem os objetivos de negócio com a minimização dos seus riscos e a promoção da segurança da organização. O processo de gestão deve estar em constante melhoria e em sintonia com aspectos sociais (MARCIANO E LIMA-MARQUES, 2006). O incremento da cooperação é um fator que tem provocado mudança nos modelos de gestão de segurança da informação. Tradicionalmente os modelos visam a garantir confidencialidade, integridade e disponibilidade. Porém, a chave para os novos modelos é garantir também a responsabilidade (conhecimento e obediência às regras), a confiança (autocontrole e reciprocidade com responsabilidade) e a ética (comportamento ético mesmo na ausência de normas), conforme ressaltam Dhillon e Backhouse (2000), o que em outras palavras implica em considerar os recursos humanos como elemento fundamental da gestão de segurança (MARTINEZ *et al.*, 2008). Pesquisas recentes apontam metodologias de gestão baseadas em abordagens direcionadas a dados (estatísticas obtidas do próprio processo) e pessoas (OLIVEIRA *et al.*, 2008; OLIVEIRA *et al.*, 2009), em que se observa que os funcionários devem participar ativamente e estar cientes das políticas de segurança existentes. Para tanto, esforços são necessários para que a organização estabeleça um nível de “cultura de segurança” satisfatório.

Este artigo contribui com a proposição de um dinâmico modelo de gestão de segurança da informação onde a interação, cooperação e motivação das pessoas (alta-gerência, chefes e funcionários) são priorizadas para atender aos novos requisitos da gestão de segurança da informação (responsabilidade, confiança e ética). O artigo está organizado como segue. Na seção 2 é apresentado um retrospecto sobre segurança em ambientes industriais, bem como aspectos culturais sobre segurança da informação. Na seção 3 são abordadas questões sobre impacto de falhas e investimentos em segurança da informação. Em seguida, a seção 4 apresenta a metodologia de pesquisa usada. Na seção 5 é apresentado e des-

doi:10.5329/RESI.2010.0902007

crito o modelo proposto. A seção 6 finaliza o artigo apresentando as principais conclusões e perspectivas futuras.

2 SEGURANÇA DA INFORMAÇÃO EM AMBIENTES INDUSTRIAIS

Tradicionalmente o ambiente industrial apresenta particularidades que podem ser identificadas quando enfocamos a segurança da informação: trata-se de um ambiente de projeto, transformação, criação e inovação que resulta em produtos finais ou matéria-prima para outras indústrias. Estes produtos são a fonte de vida de muitas organizações, e por tal importância, toda a informação que circula dentro da indústria, de acordo com as mais variadas funções e atribuições de seus empregados, deve ser constantemente protegida. Atualmente, mesmo sistemas industriais críticos, como usinas de energia elétrica, fornecedoras de gás e água, refinarias de petróleo e indústrias químicas, fazem uso de tecnologias Internet em seus sistemas de controle e suas informações estão cada vez mais vulneráveis a problemas de segurança (interna e externa), tal como, roubo de informações e ataques cibernéticos (NAEDELE, 2007). Como conseqüência, toda informação referente ao processo industrial é um ativo importante para a indústria, podendo ser de especial interesse para os concorrentes e até mesmo para terroristas. Deste modo, a proteção da informação tem que ser enfatizada internamente visando a diminuir as possibilidades de ataques externos. De 1982 até o ano 2000 os ataques externos que afetavam o setor industrial representavam 31% dos casos. Esse número aumentou em 2004 para mais de 70% (BYRES e LOWE, 2004).

Apesar do crescimento constante dos ataques externos à organização, é importante salientar que o impacto de vulnerabilidades internas pode ser tão prejudicial quanto os ataques externos. Estudos atuais mostram que 70% dos problemas de segurança corporativos acontecem internamente, não sendo consequência de ataques externos, como muitas pessoas podem acreditar. Conforme alertam Yulin, Shiying e Yi (2006), os problemas de segurança que acontecem internamente são capazes de causar mais danos.

Observando as questões de vulnerabilidades internas e ataques externos, percebe-se a importância da *cultura de segurança* dentro da organização como ponto fundamental para se atingir um nível de segurança satisfatório. Esta cultura de segurança atua como reforço de sistemas e infra-estruturas tecnológicas para a proteção da informação de ataques externos ou de vulnerabilidades internas a organização (YULIN, SHIYING e YI, 2006).

Para a diminuição e tratamento das falhas na segurança da organização, políticas de segurança devem ser criadas e implantadas fazendo parte do cotidiano de trabalho dos funcionários, visando a assegurar que os sistemas de informação, juntamente com informações do processo produtivo ao qual o funcionário tem acesso, fiquem restritos ao ambiente

interno de trabalho. Desta forma, com este tratamento, a segurança da informação é essencial para manter a vantagem competitiva, o fluxo de caixa, a rentabilidade, a conformidade legal e a imagem comercial da organização (JOHANSSON e JOHNSON, 2005).

Para guiar o desenvolvimento e aplicação de políticas de segurança existem normas que servem de base para todo projeto, como por exemplo, as normas ISO/IEC-17799 e ISO/IEC 27001, já mencionadas. O objetivo destas normas é fornecer recomendações para uma gestão de segurança da informação, suportando aqueles que são responsáveis pela introdução, implementação ou manutenção da gestão dentro das empresas (MARTINS E SANTOS, 2005). Porém a criação de uma política de segurança, mesmo que baseada em normas, não garante a sustentação da cultura de segurança. Para tal a ética das pessoas envolvidas necessita ser trabalhada no contexto das políticas e práticas da organização (DESAI e EMBSE, 2008).

A gestão de segurança da informação deve não somente proteger determinada informação, como, principalmente, elevar a chamada *consciência de segurança da informação,* visando a assegurar que todos os empregados da organização estejam cientes de seus papéis e responsabilidades (SVEEN, RICH e JAGER, 2007). Com empregados conscientizados, relatando e identificando incidentes de segurança, pode-se assegurar que as políticas serão constantemente utilizadas e não serão incômodas ou intrusivas (KRITZINGER e SMITH, 2008).

Um departamento de segurança da informação dentro da organização é de fundamental importância para o sucesso das políticas de segurança. Segundo Martins e Santos (2005), este departamento personifica o esforço e a capacidade de tomada de decisão na aplicação da segurança da informação. Incluí-se também o departamento de tecnologia da informação entre outros departamentos que monitoram as tarefas de segurança da informação e as responsabilidades dos colaboradores em assegurar que a infraestrutura de informação seja segura.

Tratando de pontos fundamentais como a cultura e a consciência de segurança da informação, podem-se utilizar incentivos e também pequenas sanções dentro da organização, fazendo com que os funcionários participem ativamente das políticas e se sintam confortáveis ao identificar problemas, objetivando aumentar a segurança da informação que circula dentro da indústria, sem influenciar na produtividade. Desta forma, busca-se o adequado equilíbrio dos fatores humanos e técnicos de segurança da informação, em contraposição aos modelos de políticas que são extremamente voltados a questões tecnológicas (MARCIANO e LIMA-MARQUES, 2006).

Enfim, observa-se que para tratar de segurança da informação em ambientes industriais de maneira eficiente, três elementos são importantes: a definição e adoção de uma gestão de segurança da informação que prime pelo incremento da cultura de segurança no interior da organização; um investimento da organização em recursos humanos especiali-

zados em segurança da informação, alocados preferencialmente em departamento específico; e incentivos constantes para incremento da cultura e consciência sobre a segurança da informação (NETTO e SILVEIRA, 2007).

3 RETORNO DE INVESTIMENTO EM SEGURANÇA DA INFORMAÇÃO

O tempo relacionado à sua aplicação, os recursos humanos necessários e o investimento financeiro em sistemas e infraestrutura tecnológica são exemplos de custos derivados da implantação de uma política de segurança (SONNENREICH, ALBANESE E STOUT, 2006). Neste sentido, a segurança da informação requer esforços da gestão organizacional para assegurar que a política de segurança criada seja executada com o menor custo. Porém, assegurar confidencialidade, integridade e disponibilidade da informação dentro da organização continua sendo responsabilidade da gestão de segurança da informação (ANDERSON e MOORE, 2006).

Na prática, com vistas à redução de custos, o modelo de gestão costuma possibilitar o uso das informações "sensíveis" a organização, aplicando regras que restringem as atividades cotidianas dos funcionários às suas funções de trabalho específicas (NETTO e SILVEIRA, 2007). Não contentes com a sua condição, ou motivados por interesses externos, funcionários podem quebrar estas regras. Estudos recentes apontam que 90% das organizações já sofreram com vulnerabilidades de segurança, e 75 % tiveram dificuldades no seu negócio devido a elas, resultando consequentemente em perdas financeiras (YEH E CHANG, 2007).

As perdas financeiras da organização relacionadas a incidentes de segurança podem ser estimadas, mas em muitos casos podem significar mais que números da produção. Para a maioria das organizações o impacto sobre a reputação ou sua imagem é muito mais significativo que perdas na produção. O impacto em saúde, segurança e incidentes ambientais podem ser altamente prejudiciais para a imagem da organização, podendo até afetar a sua licença de operação (BYRES e LOWE, 2004).

De acordo com Sveen, Rich e Jager (2007), aspectos econômicos, sociais, pressões estratégicas e culturais afetam o sucesso da gestão de segurança da informação. Estas questões não técnicas podem ser fundamentais para o sucesso da política de segurança (MARCIANO e LIMA-MARQUES, 2006). Como resultado do aspecto social da segurança, muitas organizações seguem políticas econômicas em que, cada vez mais, o investimento em segurança está sendo priorizado, pois o incremento na consciência de segurança da informação possibilita um bom retorno sobre o investimento (ANDERSON e MOORE, 2006; CANONGIA e MANDARINO JUNIOR, 2009).

4 METODOLOGIA

As pesquisas são comumente classificadas de acordo com a sua natureza e os seus objetivos. Do ponto de vista da natureza a pesquisa pode ser quantitativa ou qualitativa. De acordo com os seus objetivos a pesquisa pode ser classificada como, exploratória, descritiva ou explicativa.

As pesquisas exploratórias têm como principal finalidade desenvolver conceitos e idéias sobre determinado problema, visando à formulação de problemas mais precisos ou hipóteses pesquisáveis em estudos posteriores. As pesquisas descritivas descrevem as características de determinado fato, população ou fenômeno, visando a verificar relações entre variáveis associadas. Já as pesquisas que se preocupam em identificar os fatores que determinam, contribuem ou influenciam a ocorrência de fatos ou fenômenos são definidas como explicativas (GIL, 1999).

As variáveis qualitativas são caracterizadas pelos seus atributos; estes correspondem àqueles aspectos que não são mensuráveis, não numéricos, das hipóteses de pesquisa ou do problema de pesquisa. Sendo assim, as variáveis qualitativas são apenas descritas. Já as variáveis quantitativas são dados numéricos, quantitativos, definidos não apenas em termos de dados ou números, mas também exigindo um sistema lógico que permite a manipulação dos números, fazendo com que os resultados sejam úteis e confiáveis (TRUJILLO, 1982).

Desta forma, a metodologia utilizada nesta pesquisa classifica-se como de natureza *qualitativa com objetivo descritivo e explicativo*, tomando como base aspectos teóricos da literatura, para formular um modelo de gestão que relacione fatores humanos e técnicos de segurança da informação. A pesquisa é *qualitativa* porque verifica relações entre variáveis associadas a modelos de gestão de segurança, analisando-as indutivamente. *Descritiva e explicativa* porque foram relacionados os principais conceitos de segurança atuais, identificando o problema dos fatores humanos e financeiros que influenciam os resultados de políticas de gestão de segurança, dando ênfase à dificuldade de se ter um modelo dinâmico de gestão, que contemple adequadamente os aspectos sociais dos ambientes industriais, possibilitando elevar a cultura e a conscientização de segurança dentro da organização.

O resultado da pesquisa bibliográfica realizada para compreender as relações entre as variáveis associadas, foi descrito nas seções 1, 2 e 3, a partir do qual compreende-se que os modelos de segurança precisam englobar aspectos motivacionais, confiança e ética nas organizações para obterem sucesso. Estes aspectos foram discutidos por meio de debates realizados durante a disciplina de Gestão de Segurança da Informação, do *Programa de Pós-Graduação em Engenharia de Produção, da Universidade Federal de Santa Maria – PPGEP/UFSM,* no segundo semestre de 2009. Durante a pesquisa bibliográfica foram levantados os principais requisitos

doi:10.5329/RESI.2010.0902007

relativos aos modelos de segurança aplicados em ambiente industrial (técnicos e relacionados ao agente humano).

Considerando os requisitos identificados durante a pesquisa, foi desenvolvido um *modelo dinâmico 2D*, tendo como base a modelagem apresentada em Fishwick (2007), o qual destaca a utilização de atributos, com o apoio de formas geométricas, que refletem características comportamentais para representar dinamicamente um sistema. Estas características foram organizadas mostrando como as informações tramitam em várias direções e definindo os atores/agentes principais no contexto da gestão organizacional. Destarte, o modelo de gestão de segurança da informação proposto, contempla tais requisitos de modelagem agregando os fundamentos de segurança da informação e propondo um fluxo de informações dentro da organização, o envolvimento dos principais agentes, e também as responsabilidades de cada agente dentro do modelo. O modelo é detalhado na próxima seção.

5 MODELO DINÂMICO PARA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A definição de um modelo de gestão de segurança da informação está fortemente relacionada aos requisitos atuais na área de segurança da informação. Conforme abordado na seção 2, observa-se que o incremento da cultura de segurança é um elemento importante em ambientes industriais, o que requer responsabilidade, confiança e ética por parte dos funcionários. Esta seção propõe um modelo dinâmico para gestão de segurança da informação que valoriza os recursos humanos, promovendo a interação, cooperação e motivação das pessoas (alta-gerência, chefes e funcionários).

Para representar o modelo, foi desenvolvido um diagrama representativo em forma de modelo dinâmico 2D (FISHWICK, 2007) que representa o fluxo de informações entre as partes envolvidas na organização. O modelo proposto está dividido em quatro regiões fundamentais, conforme mostra a figura 1:

- os recursos humanos ou funcionários envolvidos na organização (presidência, comitê gestor de ti, chefes de setor e funcionários);
- os dados sobre segurança da informação (os documentos de segurança, a base de conhecimento e o sistema de relatórios sobre incidentes de segurança);
- as responsabilidades dos profissionais de TI (documentos e política de segurança); e
- as responsabilidades da gerência da organização (modelo econômico para investimento em segurança da informação e sistema motivacional).

Estas regiões são descritas utilizando perspectivas de segurança da informação que abordam a relação de variáveis humanas (responsabilidade, confiança e ética) e técnicas (políticas de segurança), dando ênfase

aos pontos críticos dentro de uma organização, como o investimento em segurança e a motivação dos funcionários. Estes pontos representam o sucesso ou o fracasso da gestão de segurança da informação (KIELY e BENZEL, 2005; ANDERSON e MOORE, 2006; MARTINEZ, 2008).

A ***primeira região*** (representada pela cor branca na figura 1) trata de uma estrutura de recursos humanos típica do setor industrial, envolvendo funcionários, chefes de setor e alta gerência. No modelo é previsto um comitê gestor de segurança da informação (CGSI) que deve fazer papel de mediador, a respeito de todos os problemas e soluções sobre segurança da informação, entre a alta gerência e os chefes de setor. A dinâmica nesta região, representada na figura pelo envio e recebimento de informações entre os blocos do modelo, é apresentada a seguir.

Os funcionários relatam um incidente de segurança ou um evento de segurança (algo que pode vir a tornar-se um incidente) para seu respectivo chefe de setor. Este encaminha dados sobre o funcionário a um programa motivacional, onde o funcionário pode receber um prêmio pela sua atitude. O chefe de setor (designado dentro da estrutura organizacional) encaminha as informações sobre o incidente de segurança para o CGSI, que faz a análise sobre o incidente, verificando sua veracidade e consultando a base de conhecimento sobre incidentes de segurança (BCIS). Caso o incidente seja novo, a BCIS é atualizada. Caso contrário, verificam-se as soluções tomadas para este incidente.

Independente de um incidente ser novo ou não, o sistema de relatório de incidentes é atualizado. Se um incidente novo ocasionar custos ou mudança na política de segurança existente, um relatório deve ser enviado à alta gerência para que esta tome a decisão mais apropriada dentro da realidade da organização. A alta gerência (por exemplo, presidência, diretores e/ou sócios) é responsável por efetivar a política de segurança da informação de acordo com os interesses da organização.

Para que a cooperação entre os componentes humanos aconteça adequadamente, um cuidado especial com a documentação sobre segurança da informação é necessário. Esta relação é representada no modelo proposto pela ***segunda região*** (representada pela cor cinza na figura 1). Após a definição dos interesses e recursos financeiros para investimento em segurança da informação, feito pela alta gerência, o CGSI é responsável pelo desenvolvimento e manutenção da política de segurança da informação, a qual deve ser fundamentada nos documentos e normas de segurança internacionalmente reconhecidas. Esta política de segurança vai auxiliar na criação e alimentação de uma base de conhecimento sobre eventos e incidentes de segurança (BCIS), que por sua vez, será responsável pela geração de relatórios e dados estatísticos consistentes sobre os eventos e incidentes ocorridos. Os relatórios serão enviados e também podem ser solicitados periodicamente pela alta gerência, pelos chefes de setor e principalmente pelo CGSI, o qual é responsável por manter um sistema de relatório de incidentes em operação.

As informações que fluem dentro do modelo se relacionam a responsabilidades que devem ser seguidas para que ocorra a sua efetividade. A ***terceira região*** (representada pela cor azul na figura 1) enfatiza as responsabilidades dos profissionais de tecnologia da informação, acerca dos documentos de segurança que devem servir de base para a criação da política de segurança. Esta política é desenvolvida em conjunto com os interesses da organização, seguindo um modelo econômico sobre investimentos em segurança definido pela alta gerência da organização. Salienta-se que a BCIS é criada e atualizada, juntamente com um sistema de relatório de incidentes de segurança. Estes componentes do modelo são de fundamental importância, pois, servem de parâmetro para aumentar e estabelecer um nível satisfatório de consciência e cultura de segurança dentro da organização.

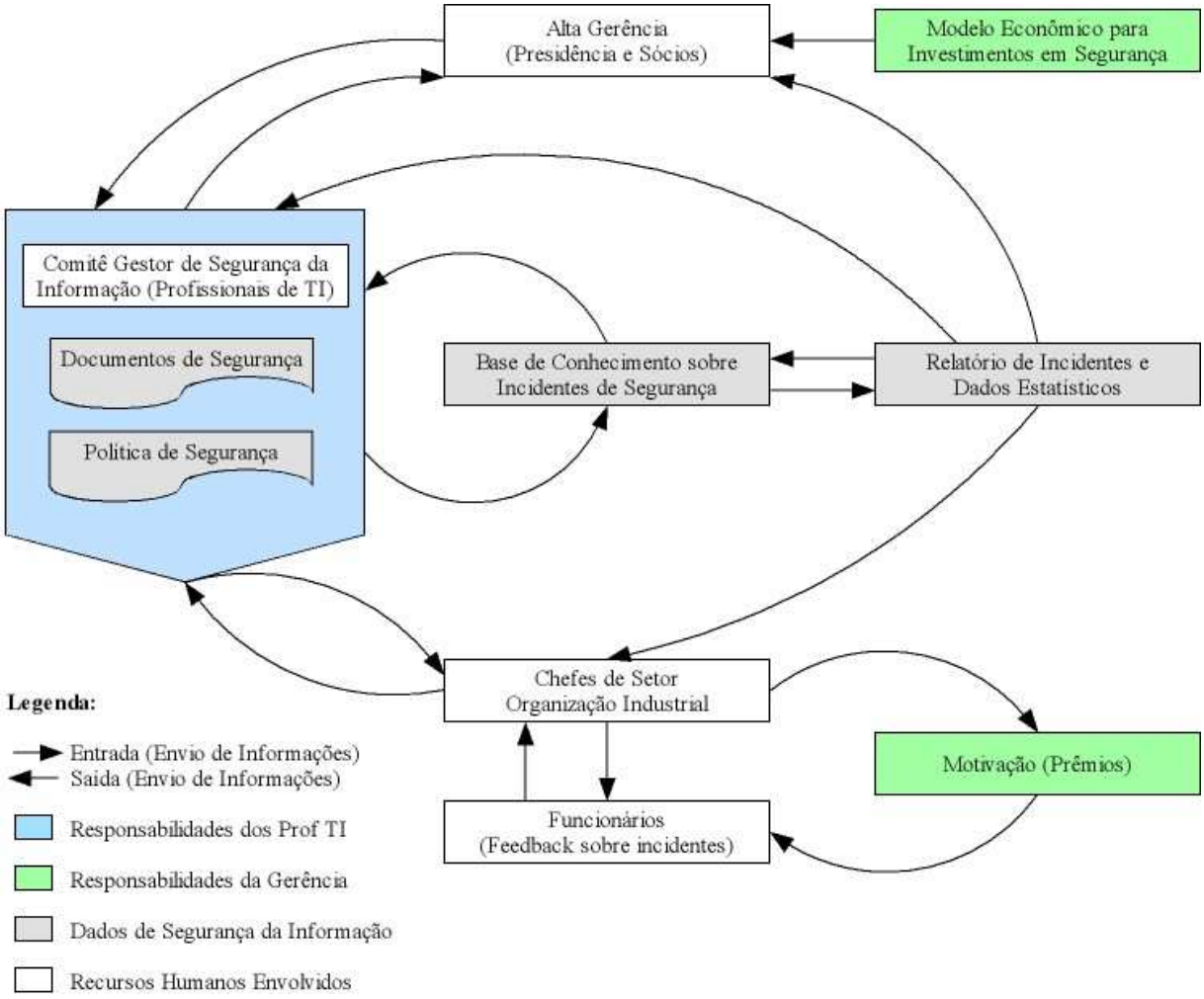

Figura 1. Modelo dinâmico para gestão de segurança da informação em ambiente industrial.

Fonte: proposição da pesquisa

Finalmente, temos uma ***quarta região*** (representada pela cor verde na figura 1) que prioriza dois aspectos fundamentais para o sucesso da gestão de segurança da informação, a existência de um modelo econômi-

co que reserve investimentos na área de segurança da informação e um programa de incentivos com prêmios para os funcionários que participam ativamente da política de segurança. Estes dois itens são responsabilidades da gerência organizacional, que dentro dos interesses e disponibilidades da organização, reserva investimentos exclusivos para a segurança da informação, concomitantemente com premiações aos funcionários que relatam incidentes de segurança.

Um dos fatores relevantes do modelo desenvolvido é a definição clara de responsabilidades dentro da organização, a respeito de segurança da informação, o que possibilita uma compreensão facilitada do modelo de gestão. O papel do comitê gestor de segurança é responder à necessidade da existência de uma equipe técnica focada no desenvolvimento e monitoramento da política de segurança da informação, estabelecendo um elo de ligação importante entre a alta gerência e os chefes dos mais variados setores dentro da indústria, o que proporciona agilidade ao modelo.

Finalmente, cabe ressaltar que nos dias atuais existe a dificuldade de justificar o investimento em segurança da informação. Com a implementação de prêmios e uma base de conhecimento sobre eventos e incidentes de segurança, o modelo proposto possibilita motivar a geração de relatórios, aumentar o conhecimento sobre incidentes e reduzir o tempo de resposta aos incidentes, para assim, maximizar o retorno ao investimento em segurança.

6 CONSIDERAÇÕES FINAIS

O incremento constante da informatização do ambiente industrial trouxe benefícios às indústrias, mas em contrapartida elevou as vulnerabilidades de segurança da informação. Hoje em dia a segurança da informação é entendida como um processo de gestão, e como tal, para ter sucesso é necessário promover a interação, cooperação e motivação das pessoas. Este artigo propôs um modelo dinâmico de gestão de segurança da informação, que valoriza as pessoas em todos os níveis visando a mostrar formas de como elevar a cultura de segurança dentro da organização, promovendo assim não só a proteção contra ataques externos, mas também contra ataques internos.

O modelo desenvolvido trata de itens fundamentais, como um programa de motivação através de premiação, um modelo econômico que reserve recursos a serem aplicados em segurança da informação e a existência de um comitê gestor de segurança da informação servindo de mediador entre os chefes de setor e a alta gerência. Desta forma o modelo possibilita que todos os funcionários dentro da organização tenham responsabilidades e papéis importantes, promovendo o trabalho em conjunto e motivado, elevando a cultura de segurança da informação dentro da organização.

O fato de o modelo proposto ser a consolidação de uma pesquisa teórica empírica pode caracterizar uma limitação, pois toda literatura

apresenta lacunas e pontos inexplorados. Em contrapartida, verificou-se com o estudo realizado que a base bibliográfica usada apresenta resultados que destacam a importância de fatores abordados no modelo proposto, como aspectos humanos (responsabilidade, confiança e ética), que objetivam estabelecer nas organizações uma cultura de segurança da informação.

A próxima etapa desta pesquisa compreende a realização de algumas atividades que são sugeridas como trabalhos futuros, as quais são: a aplicação do modelo em organizações do setor industrial e uma análise comparativa do impacto da adoção do modelo nos diferentes níveis funcionais da organização, visto que este trabalho contempla apenas a parte teórica do modelo. Esta análise será importante para validar empiricamente o modelo, alem de contribuir para o crescimento da cultura de segurança, possibilitando ainda verificar o retorno sobre o investimento em segurança da informação.

REFERÊNCIAS

ANDERSON, R; MOORE, T. The economics of information security. *AAAS - American Association for the Advancement of Science, REVIEW*, 2006.

BYRES, E.; LOWE, J. The myths and facts behind cyber security risks for industrial control systems. British Columbia Institute of Technology, PA Consulting Group. *VDE Congress*, Berlin, 2004.

CANONGIA, C; MANDARINO JUNIOR, R. Segurança cibernética: o desafio da nova sociedade da informação. *Revista Parcerias Estratégicas*, v. 14, n. 29, p. 11-46, Brasília, 2009.

COSTA, P. R. P. R. da; FERREIRA, M. A. T. A interação e a cooperação como fontes de competitividade e aprendizagem na pequena e média indústria brasileira. *Perspectiva em Ciência da Informação*, v. 5, n. 2, p. 183-203, jul./dez, 2000.

DESAI, M. S.; EMBSE, T. J. Von der. Managing electronic information: an ethics perspective. *Journal of Information Management & Computer Security*, v. 16, n. 1, p. 20-27, 2008.

DHILLON, G.; BACKHOUSE, J. Information system security management in the new millennium. *Communications of the ACM*, v. 43, n. 7, p. 125-128, July, 2000. doi:10.1145/341852.341877

FISHWICK, P. A. Handbook of dynamic system modeling. *CRC Press*, p. 760, 2007. doi:10.1201/9781420010855

GIL, A. C. *Métodos e técnicas de pesquisa social*. 5. ed. São Paulo: Atlas 1999.

JOHANSSON, E; JOHNSON, P. Assessment of enterprise information security – an architecture theory diagram definition. *CSER - Conference on systems engineering research*, *Department of Systems Engineering and*

Engineering Management, Stevens Institute of Technology, Hoboken, NJ, USA, 2005.

KIELY, L.; BENZEL, T. V. Systemic security management. *IEEE Security & Privacy*, p. 74-77, 2005.

KRITZINGER, E; SMITH, E. Information security management: an information security retrieval and awareness model for industry. *Computer & Security*, v. 27, n. 5-6, p. 224-231, 2008. doi:10.1016/j.cose.2008.05.006

MARCIANO, J. L. P.; LIMA-MARQUES, M. O enfoque social da segurança da informação. *Revista Ciência da Informação*, v. 35, n. 3, p. 89-98, set/dez 2006.

MARTINS, A. B.; SANTOS, C. A. S. Uma metodologia para implantação de um sistema de gestão de segurança da informação. *Journal of Information Systems and Technology Management* (Jistem), v. 2, n. 2, p. 121-136, 2005. doi:10.4301/S1807-17752005000200002

MARTINEZ, I. J.; SAMSA, M. E.; BURKE, J. F.; AKCAM, B. K. Toward a generic model of security in an organizational context: exploring insider threats to information infrastructure. In: IEEE Hawaii International Conference on System Sciences, 41, Hawaii, *Proceedings...* IEEE Computer Society, 2008.

NAEDELE, M. Addressing IT security for critical control systems. In: Hawaii International Conference on System Sciences, 40., Hawaii. *Proceedings...* IEEE Computer Society, 2007.

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

NBR ISO/IEC 17799. *Tecnologia da informação*: código de prática para gestão da segurança da informação. ABNT. Rio de Janeiro. 2005.

NBR ISO/IEC 27001. *Tecnologia da informação:* sistema de gestão da segurança da informação. ABNT. Rio de Janeiro. 2006.

OLIVEIRA, M. A .F; NUNES, R. C.; ELWANGER, C. Uma metodologia seis sigma para implantação de uma gestão de segurança da informação centrada na percepção dos usuários. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG), 9, Campinas, *Anais...* Setembro, 2009.

OLIVEIRA, M. A .F; NUNES, R. C.; AMARAL, E. M. H.; ZEN, E.; PEREIRA, S. N. Uma metodologia de gestão de segurança da informação direcionada a riscos baseado na abordagem seis sigma. In: Encontro Nacional de Engenharia de Produção (ENEGEP), 28., Rio de Janeiro, *Anais.* Outubro, 2008.

SANTOS, R. O bê-a-bá da gestão de risco e governança. *Observatório de Tecnologias de Gestão - OTG*, Brasília, fevereiro, 2008.

SVEEN, F. O.; RICH, E; JAGER, M. Overcoming organizational challenges to secure knowledge management. *Information Systems Frontiers*, v. 9, n. 5, p. 481-492, 2007. doi:10.1007/s10796-007-9052-5

SONNENREICH, W; ALBANESE, J; STOUT, B. Return on security investment (ROSI) – a practical quantitative model. *Journal of Research and Practice in Information Technology*, v. 38, n. 1, 2006.

TRUJILLO, F. A. *Metodologia científica da pesquisa*. São Paulo: McGraw Hill, 1982.

VALENTIM, M. L. P.; CARVALHO, E. L.; WOIDA, L. M.; CASSIANO, E. L. Gestão da informação utilizando o método Infomapping. *Perspectivas em Ciência da Informação*, v. 13, n. 1, p. 184-198, jan./abr., 2008.

YEH, Q; CHANG, A. J. Threats and countermeasures for information system security: a cross-industry study. *Information & Management*, v. 44, n. 5, p. 480-491, July, 2007. doi:10.1016/j.im.2007.05.003

YULIN, D; SHIYING, L; YI, L. Information relevance management model – a new strategy in information security management in the outsourcing industry. In: ICIS-COMSAR'06, p. 433-438, *Proceedings...* IEEE Computer Society, 2006.