2066-PS

PROPOSAL TO STRUCTURE THE INFORMATION SECURITY MANAGEMENT IN A SCIENTIFIC RESEARCH ENVIRONMENT

João Carlos Soares de Alexandria (IPEN - Instituto de Pesquisas Energéticas e Nucleares, São Paulo, Brasil) - jcsalex@ipen.br
Luc Marie Quoniam (Université du Sud Toulon Var, France) - quoniam@univ-tln.fr

Abstract
The increase of the connectivity in the business environment, combined with the growing dependency of information systems, has become the information security management an important governance tool. Market researches have showed that the information security implementation is concentrated on a well-defined group of organizations mainly formed by large companies and from specifics sectors of economy, for example, financial and telecommunication. However, information security must be done by all organizations that use information systems to carry out their activities, independently of its size or economic area that it belongs. Many organizations have difficulties to make a practice of information security management, among these are the public scientific research institutions. Many of them just adopt points measures, sometimes they are not consistent with their realities.

Keywords: Information security, ABNT NBR ISO/IEC 27002:2005, Information technology (IT).

PROPOSTA PARA A ESTRUTURAÇÃO DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE DE PESQUISA CIENTÍFICA

Resumo
O aumento crescente da interconectividade no ambiente de negócio, aliado à dependência cada vez maior dos sistemas de informação nas organizações, faz da gestão da segurança da informação uma importante ferramenta de governança corporativa. Pesquisas de mercado mostram que a implementação da segurança da informação está concentrada em instituições de grande porte e de segmentos específicos da economia como, por exemplo, bancário-financeiro e telecomunicação. Entretanto, a segurança da informação faz-se necessária em qualquer organização que utilize sistemas de informação nos seus processos de trabalho, independentemente do porte ou do setor econômico de atuação. Grande parte das organizações tem dificuldades para a estruturação da segurança da informação, entre as quais se encontram as instituições públicas de pesquisas científicas. Muitas delas se limitam a adotarem medidas pontuais e, muitas vezes, inconsistentes com a realidade em que vivem.

Palavras-chave: Segurança da informação, ABNT NBR ISO/IEC 27002:2005, Tecnologia da informação (TI)

1. Introdução

A informação é um bem de suma importância em todas as áreas da atividade econômica, e não poderia ser diferente em uma instituição pública de pesquisa científica.

A revolução da tecnologia da informação, mais especificamente com o desenvolvimento da *Internet*, provocou o surgimento de uma nova economia informacional, global e em rede (CASTELLS, 2005; p. 119).

Se por um lado, as organizações ganharam em facilidades no acesso e na troca de informações nunca antes visto, por outro, ficaram expostas à ação de novas e perigosas ameaças que, das mais diversas formas e motivações, podem inviabilizar ou dificultar o cumprimento dos objetivos almejados.

A segurança, ou mais apropriadamente falando a proteção, da informação é hoje um importante mecanismo de gestão que as organizações devem incorporar às suas práticas gerenciais por inúmeras razões, entre elas garantir a continuidade do negócio e maximizar o retorno sobre os investimentos (ABNT, 2005; p. ix). Além de atender a legislação em vigor e as regulamentações impostas por órgãos regulatórios.

No âmbito de pesquisa científica há ainda uma particularidade a mais, pois além da informação é necessário proteger o conhecimento produzido. Exemplo disto são os segredos industriais e a propriedade intelectual que precisam ser preservados contra utilizações indevidas.

Segurança da informação ganhou um grande impulso no mercado mundial com a publicação da Norma ISO 17799 em 2000. A partir daí muitas empresas passaram a implementar medidas de segurança com base nas práticas estabelecidas na referida Norma.

Vieram em seguida diversas regulamentações impostas a determinados setores da economia, como por exemplo, as leis Americanas *Sarbanes-Oxley Act (SOX) e a Federal Information Security Management Act (FISMA)*, ambas de 2002, para o mercado de capitais e para a segurança das operações eletrônicas das agências federais americanas, respectivamente. O Acordo de Capital da Basiléia estabelecido pelo Comitê de Supervisão Bancária da Basiléia (CSBB), em 2004, veio regulamentar o setor bancário / financeiro. A proteção dos registros médicos teve sua regulamentação estabelecida em 1996 através da *Health Insurance Portability and Accountability Act (HIPAA)* (USA, 2002a; USA, 2002b; BCB, 2000; PEREIRA, 2008; MARCIANO, 2006; p.91; BYRUM, 2004).

Embora estas leis e regulamentações sejam internacionais, elas acabaram influenciando o mundo inteiro, e a sua aplicabilidade ultrapassou os limites dos setores da economia a que foram endereçadas. Além do mais, elas exercem forte pressão sobre a proteção de dados e de sistemas de informação, mesmo que este não tenha sido o enfoque, quando da sua concepção.

Para PEIXOTO (2004) ao regular a atividade de contabilidade e auditoria das empresas de capital aberto, a *Sarbanes-Oxley* reflete diretamente seus dispositivos nos sistemas de tecnologia da informação. Para o supracitado autor é impossível separar-se processos de negócios e tecnologia no panorama corporativo atual.

Seja pela obrigatoriedade regulatória, seja para buscar uma certificação em segurança da informação que lhe confira um diferencial competitivo, ou pela necessidade pura e simples de proteger seus sistemas de informação; a gestão

da segurança da informação é um mecanismo cada vez mais presente no atual processo de governança corporativa das organizações.

2. Referencial Teórico

2.1. Segurança da Informação

A segurança da informação atualmente está polarizada em um grupo de companhias caracterizado, principalmente, por empresas com alta dependência de TI, pertencentes a setores da economia com forte ação regulatória, ou que atuam sob alta pressão competitiva, e que neste caso utilizam segurança da informação como um diferencial. Neste grupo de companhias estão instituições financeiras, multinacionais, empresas de telecomunicações e companhias de capital aberto.

A 10ª pesquisa global de segurança da informação (ERNST & YOUNG, 2007) revelou que o principal motivo para a implementação de práticas de segurança da informação nas organizações é a conformidade com a regulamentação que as mesmas estão submetidas (64% dos respondentes).

Esta regulamentação é estabelecida pelos órgãos de fiscalização dos respectivos setores da economia. São exemplos desses órgãos, no Brasil, o Banco Central para o setor financeiro, a Comissão de Valores Mobiliários (CVM) para as empresas de capital aberto e a Agência Nacional de Telecomunicações (ANATEL) para o setor de telecomunicações, entre outros.

As empresas que não se enquadram no perfil do grupo citado acima, quase sempre não possuem um departamento de segurança estruturado, e por este motivo têm grandes dificuldades para demonstrarem aos seus executivos a importância da gestão da segurança da informação para os processos de negócio (suas atividades). As razões para esta dificuldade estão normalmente relacionadas com a falta de indicadores que justifiquem, perante o corpo executivo, os investimentos financeiros e administrativos nesta área compatíveis com as necessidades das mesmas.

Dados da 10ª pesquisa nacional de segurança da informação (MODULO, 2006) revelaram que a maioria das empresas do setor financeiro possui departamento de segurança estruturado (56% das empresas pesquisadas do setor), em seguida vem o setor de telecomunicações com 50%, comércio com 39%, serviço com 35%, indústria com 31% e governo com 23%.

Apesar de muitas corporações adotarem alguns controles de segurança baseados nas melhores práticas, como por exemplo, ABNT NBR ISO/IEC 27002 ou Cobit *(Control Objectives for Information and Related Technology),* grande parte delas ainda não acredita que corre risco de perder a confidencialidade de suas informações e de comprometer a integridade dos serviços críticos dos seus negócios (GIURLANI, 2005).

A Norma ABNT NBR ISO/IEC 27002:2005 coloca a análise, avaliação e tratamento de riscos, a legislação vigente e a política de segurança da informação como as três principais fontes de requisitos de segurança da informação de uma organização.

Entretanto, as organizações pertencentes aos setores da economia com fraca regulamentação têm grandes dificuldades para implementarem uma segurança da informação estruturada e compatível com as suas reais necessidades. Isto porque a aplicação de uma metodologia / ferramenta de análise e avaliação de riscos, e mesmo a definição de uma política corporativa de

segurança da informação é um processo oneroso e de razoável complexidade administrativa, que demanda o envolvimento de muitas pessoas e setores da organização. O que, paradoxalmente, pressupõe a existência de uma estrutura de segurança em estágio avançado na organização, ou um elevado nível de conscientização dos seus executivos com relação ao tema.

Esta situação cria um abismo quase intransponível a que muitas corporações têm que superar para conseguir implementar um programa de segurança que atenda as suas necessidades de negócio.

De acordo com a pesquisa nacional de segurança da informação (MODULO, 2006) o maior motivador para a tomada de decisões visando à segurança é o nível de consciência dos executivos e usuários (31%), segundo os pesquisados. Ainda segundo a referida pesquisa a imagem da empresa no mercado (23%) e o valor agregado aos produtos e negócios (19%) também influenciam.

Paul Van Kessel, comentando os dados da 10ª Pesquisa Global sobre segurança da informação (ERNST & YOUNG, 2007), diz existir evidência de que as organizações estão começando a reconhecer que segurança da informação pode dar mais do que apenas proteção para a informação. E conclui: "*melhorias significativas na performance estão sendo percebidas que impactam o resultado financeiro final, e elevam a segurança da informação de uma solução tática para uma importância estratégica"*.

Na área governamental a situação brasileira não é diferente. Um levantamento realizado pela Secretaria de Fiscalização de Tecnologia da Informação (SEFTI), do Tribunal de Contas da União (TCU) mostrou que a situação da governança de tecnologia da informação (TI) na administração pública federal é preocupante. O aspecto em que a situação da governança de TI está mais crítica é a gestão da segurança da informação (TCU, 2008; p. 38).

A auditoria da SEFTI revelou que 64% dos 255 órgãos públicos pesquisados não têm política de segurança da informação. Na análise do TCU, existe um campo vasto para atuação na área de governança de TI na Administração Pública Federal; e diz mais:

> *"Se essa atuação for realizada de forma consistente e constante, os resultados serão promissores tendo em vista que poderá haver melhoria generalizada em todos os aspectos da governança de TI. Esse fato repercutirá na gestão pública como um todo e trará benefícios para o País e os cidadãos"* (TCU, 2008; p.8).

Quando se observa o setor da pesquisa científica e tecnológica do Brasil, e em particular as instituições da área nuclear, onde esta pesquisa foi realizada, verifica-se poucos avanços na implementação de segurança da informação, como prática gerencial estruturada e formalmente estabelecida.

Para HORTON & MUGGE (2004; p. 7) a segurança da informação é influenciada pela medição coletiva dos três principais objetivos: confidencialidade, integridade e disponibilidade, conhecidos como modelo CIA (*Confidentiality, Integrity and Availability*).

Para os referidos autores, confidencialidade é fator determinante na proteção de dados que fornecem uma vantagem competitiva na produção, no tempo de comercialização ou na confiança do cliente. A integridade é fato crítico, quando dados são usados para realizar transações, análises estatísticas ou

cálculos matemáticos. A disponibilidade é fundamental quando dados ou aplicações precisam ser acessados em tempo real.

2.2. Segurança da Informação em Ambiente de Pesquisa Científica

Quando se fala em segurança da informação em instituições de pesquisa cientifica e tecnológica, à primeira vista pode parecer um contra senso já que a disseminação de informação e de conhecimento é requisito importante para o desenvolvimento da pesquisa.

Olhando-se desta forma estar-se-ia presumindo que segurança da informação é um instrumento utilizado unicamente para restringir ou para dificultar o acesso e o compartilhamento da informação. Porém, esta não é a realidade nem a finalidade da segurança da informação.

A segurança da informação é usada para auxiliar a organização a definir, de forma inequívoca, qual é o grau de sensibilidade das informações que devem ser compartilhadas. Caso esta informação tenha algum grau de sensibilidade, ou seja, se de alguma forma a instituição poderá vir a ser penalizada por uma revelação indevida desta informação, então, aí haverá a necessidade da utilização de controles de segurança para salvaguardar a sua confidencialidade.

Mesmo que a confidencialidade não seja um requisito de segurança exigido pela informação é possível afirmar que, na maioria dos casos, a disponibilidade e a integridade o serão.

Entende-se informação como todo e qualquer ativo utilizado no seu manuseio, processamento, armazenamento, transmissão e compartilhamento.

Analisando-se melhor a questão poder-se-ia indagar quais seriam os principais sistemas de informação e comunicação que uma instituição de pesquisa científica utiliza para disseminar informação e conhecimento. A resposta a esta pergunta deverá incluir alguns dos seguintes sistemas: *Homepage* institucional, serviço de correio eletrônico (E-mail), serviço de transferência de arquivos (FTP), participação em congressos, publicação de artigos, intercâmbios e visitas técnicas e científicas.

É possível ainda que algumas informações que estejam sendo compartilhadas através desses sistemas (ou canais de comunicação) sejam de caráter confidencial ou reservado. Isto pode acontecer mesmo quando existe algum método de classificação da informação já implementado.

Partindo-se da premissa que estas informações sejam públicas, qualquer pessoa possa acessá-las e utilizá-las sem que isto signifique prejuízo para a organização. Ainda assim, a integridade e a disponibilidade desses sistemas devem ser preservadas para o bom funcionamento e cumprimento dos objetivos da instituição.

Integridade significa garantir que a informação estará correta e íntegra quando um usuário ou pessoa interessada, requerer tal informação do sistema. Já a disponibilidade é a garantia de que um arquivo ou um sistema de informação estará disponível, e em perfeita condição de uso, no momento em que um usuário legítimo precisar acessá-lo (PELTIER et al., 2005; p. 22).

Garantir a integridade e a disponibilidade de um sistema de informação pode parecer uma tarefa simples, porém existem muitos fatores que podem comprometer a sua segurança. Estes fatores incluem falhas de *hardware*, desastres naturais, usuários mal intencionados e atacantes externos.

Tomando-se como exemplo a *homepage* institucional de uma organização, e supondo-se que todas as informações publicadas no *Website* corporativo sejam de caráter público, ainda assim será necessário implementar uma série de controles de segurança para preservar a sua integridade e disponibilidade. Nenhuma organização vai querer que as suas informações disponibilizadas na *Internet* sejam alteradas ou corrompidas indevidamente por pessoa não autorizada.

Desta forma, a gestão da segurança da informação vai agir para tentar impedir ou evitar que potenciais ameaças venham comprometer a integridade e a disponibilidade das informações publicadas na *homepage* da organização.

Para garantir a segurança da *homepage* institucional, ou de aplicações *Web* em geral, é necessário, entre outras, a adoção das seguintes medidas:

- hospedar a *Website* em um servidor robusto e confiável para operar 24 horas por dia, sete dias por semana (características desejadas deste equipamento: fontes redundantes, discos *Hot Swap, RAID 5,* entre outras);
- controlar o acesso físico à sala de servidores (*datacenter*);
- prover fornecimento ininterrupto de energia (instalação de gerador e *no-breaks*);
- instalar equipamento de ar condicionado compatível com a demanda do ambiente;
- utilizar *softwares* homologados e atualizados (sistema operacional, servidor *Web* e pacote de desenvolvimento);
- aplicação periódica de correções de *softwares (patches*);
- segmentação da rede em perímetros de segurança (*Firewall* e *DMZ*);
- sistema de autenticação para identificar os usuários que estão autorizados a realizarem manutenções no *site*;
- sistema de *backup*;
- antivírus; e
- prevenção contra *Hacking* (métodos e técnicas utilizadas pelos *hackers*).

As aplicações *Web* podem ser consideradas como sendo várias tecnologias que normalmente são executadas em servidores *Web* para fornecer uma função *Web*.

Em função da sua natureza, as aplicações *Web* permitem o acesso de qualquer usuário por meio de um navegador. Desta forma, será necessária a utilização de outros controles de proteção, além daqueles tradicionais de perímetro de rede que a empresa possa estar usando para restringir o acesso de usuários mal-intencionados.

As aplicações *Web* desprotegidas podem levar não apenas ao comprometimento do servidor *Web* propriamente dito, mas também a de qualquer banco de dados que contenha dados confidenciais para o serviço *Web*, o que provavelmente afetaria toda a organização de uma maneira muito mais séria.

De acordo com HORTON & MUGGE (2004; p. 150):

> *"para proteger uma aplicação Web, é necessário que o administrador do servidor Web e os desenvolvedores das aplicações trabalhem em conjunto, para identificar e proteger cada brecha de segurança possível. Um hacker precisa apenas de uma única 'porta destrancada' para concretizar o comprometimento da segurança do servidor Web ou de suas aplicações residentes"*.

O governo brasileiro, através do Comitê Executivo do Governo Eletrônico publicou a Resolução nº 7, de 29 de junho de 2002 (BRASIL, 2002), onde estabelece um conjunto de regras e diretrizes para a segurança dos *sítios* na *internet* da Administração Pública Federal.

3. Metodologia

3.1. Tipo de Pesquisa

Pesquisa exploratória com delineamento de levantamento

Com base nos objetivos, a presente pesquisa é do tipo exploratória, pois buscou proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses (GIL, 2008; p. 41).

De acordo com o referido autor, "*Na maioria dos casos, essas pesquisas envolvem: (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; e (c) análise de exemplos que estimulem a compreensão*".

Segundo GIL (2008; p. 43) o elemento mais importante para a identificação do delineamento é o procedimento adotado para a coleta de dados.

As pesquisas do tipo levantamento caracterizam-se pela interrogação direta das pessoas, cujo comportamento se deseja conhecer (GIL, 2008; p. 50).

Para YIN (2005, p. 24) a pesquisa exploratória é empregada quando as questões de pesquisa são principalmente do tipo "o que". Segundo o autor *"Esse tipo de questão é um fundamento lógico justificável para conduzir um estudo exploratório, tendo como objetivo o desenvolvimento de hipóteses e proposições pertinentes a inquirições adicionais"*.

3.2. O Problema

Este trabalho foi definido com o seguinte problema de pesquisa:
"O que pode ser feito para potencializar a efetividade das normas e procedimentos de segurança da informação em uma instituição pública de pesquisa cientifica da área nuclear no Brasil"

A efetividade de uma lei corresponde à concretização de sua "eficácia" na realidade social que regula. Ou seja, a lei, depois de vigente e capaz de gerar efeitos (com eficácia), só se torna efetiva quando se concretiza no grupo social em que deve ser aplicada (SOUSA, 2007).

3.3. Hipóteses

Este estudo foi elaborado para avaliar as seguintes hipóteses, relacionadas com a segurança da informação no Instituto de Pesquisas Energéticas e Nucleares – IPEN:

1. desconhecimento das normas e procedimentos de segurança por parte da comunidade de usuários;
2. falta de conscientização do usuário quanto aos riscos e danos, associados ao uso inseguro de TI (Tecnologia de informação) e da informação de modo geral, que pode causar impactos negativos às atividades desenvolvidas na organização;
3. as políticas adotadas estão desalinhadas dos requerimentos de segurança da organização, que tem requisitos específicos por se tratar de uma instituição pública de pesquisas científicas; e
4. gestão inadequada da segurança da informação.

3.4. Coleta de dados

Foram utilizados três instrumentos de coleta de dados, abrangendo os três níveis hierárquicos organizacionais (estratégico, tático e operacional).

No nível estratégico o instrumento utilizado foi o "*Information Security Governance Assessment Tool for Higher Education - ISG-HE*" (EDUCAUSE, 2008). Esta é uma ferramenta de avaliação da governança da segurança da informação para instituições de ensino superior, cujo objetivo é avaliar o grau de maturidade das práticas de segurança vigentes.

O ISG-HE é uma adaptação feita pelo EDUCAUSE, dos Estados Unidos, para instituições de ensino superior, da ferramenta originalmente desenvolvida pelo "National Cyber Security Summit Task Force". Esta ferramenta é usada para ajudar o alto escalão da organização a identificar áreas vulneráveis, que precisam ser examinadas para determinar seus riscos (NCSSTF, 2004; ISG, 2004).

No plano tático foram realizadas entrevistas semi-estruturadas com os gerentes das unidades de negócio (Centros de pesquisas). A entrevista foi composta por questões relativas às normas de segurança em vigor na organização, e outras de interesses específicos.

O objetivo desta entrevista foi captar junto aos gerentes seus conhecimentos, percepções e opiniões a respeito da segurança da informação na instituição.

No nível operacional utilizou-se um questionário para avaliar a aderência das normas e procedimentos de segurança da informação junto aos usuários finais.

O questionário foi composto por 20 questões fechadas, formatadas a partir dos dados levantados em uma pesquisa documental sobre as normas e procedimentos de segurança formalmente estabelecidos na organização.

Esses três instrumentos de coleta de dados se constituem, na verdade, em um método de diagnóstico e avaliação do grau de maturidade da segurança da informação em uma organização

A coleta de dados no IPEN aconteceu no período de julho a dezembro de 2008, e contou com a participação total de 169 pessoas, assim distribuídas:

1º) ISG-HE – Diretor-Presidente da instituição e Gerente de TI (2 pessoas);
2º) Entrevista – oito Gerentes de Centro de Pesquisa e dois pesquisadores de áreas chaves - inovação tecnológica e qualidade (10 pessoas);
3º) Questionário – 157 funcionários.

O ISG-HE foi concebido originalmente na forma de planilha Excel, onde os dados são totalizados e analisados dinamicamente.

A análise estatística dos dados coletados, tanto na aplicação do questionário quanto nas entrevistas, foi feita utilizando-se tabelas dinâmicas do "Excel" (Microsoft Office profissional, edição 2003).

As entrevistas foram realizadas com o auxilio de um equipamento portátil (*notebook*), e gravadas com o *software* "*Audacity*", programa livre e gratuito, de código fonte aberto, para edição de áudio digital (AUDACITY, 2008).

A análise qualitativa dos discursos das entrevistas foi realizada transcrevendo-as para o "Word" (Microsoft Office profissional, edição 2003).

4. Análises dos Resultados

4.1. ISG-HE

Na TAB.1 mostra-se a consolidação dos dados obtidos na aplicação do "ISG Assessment Tool for Higher Education".

No IPEN o ISG-HE foi aplicado junto ao Diretor-Presidente da instituição e também ao Gerente de TI, a quem compete à gestão da segurança da informação.

A consolidação dos dados das duas avaliações foi realizada da seguinte forma:

a. utilizando-se a seção 1 (Dependência de TI) da avaliação feita pelo Diretor-Presidente; e
b. utilizando-se as seções de 2 a 5 (Gestão de risco, Pessoas, Processos e Tecnologia) da avaliação feita pelo responsável pela segurança (gerência de TI).

TABELA 1 - Consolidação dos dados do ISG-HE

TOTAL DA DEPENDÊNCIA DE TI	**34**
TOTAL DE PONTOS DA GESTÃO DE RISCO	**0**
TOTAL DE PONTO DE PESSOAS	**5**
TOTAL DE PONTOS DE PROCESSOS	**36**
TOTAL DE PONTOS DE TECNOLOGIA	**25**
TOTAL DE PONTOS DA AVALIAÇÃO DA SEGURANÇA (Soma de Gestão de risco, Pessoas, Processos e Tecnologia)	**66**

Analisando-se os dados relativos à aplicação do ISG-HE no IPEN verificou-se que o grau de dependência da instituição com relação à tecnologia da informação obteve 34 pontos. Esta pontuação corresponde a uma dependência de TI **alta**.

Ter uma dependência de TI alta significa que a instituição (seus processos de negócio) tem um alto grau de dependência da tecnologia da informação e, portanto, precisa confiar que esta funcione adequadamente para dar o suporte necessário as suas operações.

Por outro lado, a avaliação geral (seções 2 a 5) contabilizou um total de 66 pontos, o que colocou a instituição numa situação "**pobre**" no que se refere à gestão da segurança da informação.

Quando se analisa, individualmente, a pontuação obtida em cada uma das seções da ferramenta ISG-HE, verifica-se que a seção 5 (tecnologia) apresenta a melhor situação, em termos proporcionais.

Os 25 pontos obtidos na seção 5 (tecnologia) correspondem a 34,7% dos 72 pontos possíveis. A seção 4 (processos) com 36 pontos atingiu 20,4% de um total de 176 pontos que poder-se-ia atingir; e os 5 pontos da seção 3 (pessoas) equivalem a 9,6% de um total de 52 pontos da referida seção.

Diante desses dados, conclui-se que as medidas de segurança, atualmente implementadas na instituição, estão pautadas em controles tecnológicos.

4.2. Entrevistas

As questões abordadas na entrevista giraram em torno de seis domínios de segurança: Senhas, Vírus, Recursos computacionais, E-mail, Backup e Propriedade intelectual.

Na TAB.2 sumariza-se, em termos percentuais, as respostas obtidas dos dez entrevistados relativas à Pergunta 1: *"Senhor (a) Gerente, os funcionários deste Centro de Pesquisa têm conhecimento da política do IPEN para o referido domínio de segurança?"*.

TABELA 2 - Percentuais de conhecimento das normas de segurança

	Senhas	Vírus	Recursos Computacionais	E-mail	Backup	Prop. Intelectual
SIM	40%	70%	90%	60%	50%	70%
NÃO	60%	30%	10%	40%	50%	30%

Na FIG.1 é mostrado o número total de "SIM" e "NÃO" relativos à TAB.2 e o percentual que cada um representa. A referida FIGURA mostra que na avaliação geral as políticas de segurança do IPEN são conhecidas por 63,33% dos funcionários.

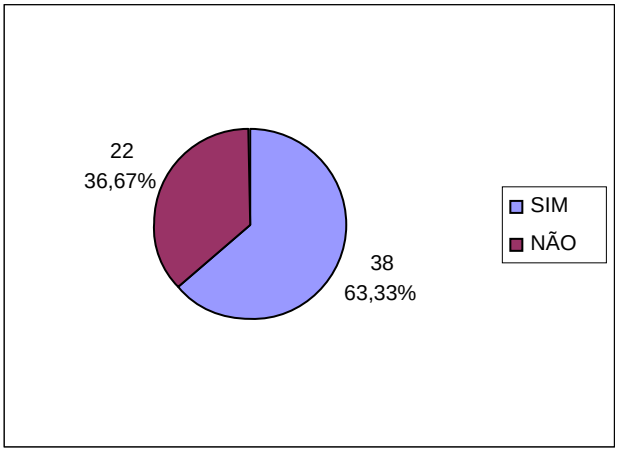

FIGURA 1 - Conhecimento das políticas

Por outro lado, analisando-se os seis domínios de segurança da TAB.2, separadamente, verifica-se, por exemplo, que na opinião dos gerentes, 60% dos funcionários do IPEN não conhecem a política de criação e uso seguro de senhas, e 50% deles não têm conhecimento da política de *backup* da instituição.

A pontuação relativa às perguntas 2, 3, 4 e 5 está sumarizada na TAB.3.

Pergunta 2: *"Em sua opinião, é importante que o IPEN tenha uma política (para o referido domínio de segurança) para o bom desempenho das atividades e cumprimento da missão da instituição? Por favor, quantifique sua resposta!"*

Pergunta 3: *"Os funcionários deste Centro de Pesquisa têm um nível adequado de conscientização e treinamento em procedimentos de segurança do (domínio x)? Por favor, quantifique sua resposta!"*

Pergunta 4: *"O Senhor (a) acha importante que o IPEN promova uma ação mais efetiva junto aos usuários sobre a sua política (para este domínio de segurança)? Por favor, quantifique sua resposta!"*

Pergunta 5: *"De uma forma geral, como o Senhor avalia a gestão do IPEN no que se refere à segurança da informação da instituição? O Senhor acha que ela é adequada? Por favor, quantifique sua resposta!"*

As respostas contidas na TAB. 3 foram quantificadas, pelos entrevistados, utilizando-se a escala de 1 a 4 do quadro abaixo, com significados variando de acordo com o contexto da pergunta formulada.

1	2	3	4
Nada Importante	Pouco Importante	Muito Importante	Extremamente importante
Nenhum	Pouco	Bom	Ótimo

TABELA 3 - Pontuação obtida na avaliação dos entrevistados

	Senhas	Vírus	Recursos Computac.	E-mail	Backup	Prop. Intelectual	Média Geral
Importância da política	35	39	37	37	36	39	**3,72**
Nível de Conscientização	24	27	26	25	25	24	**2,52**
Necessidade de ações adicionais	27	32	30	32	32	32	**3,08**
Gestão de SI							**2,90**

Os dados apresentados na TAB.3 revelaram que:

a) a importância para o IPEN das medidas de segurança, contidas nos seis domínios avaliados, obtive média de **3,72**, sendo considerada ótima de acordo com a escala de referência (TAB.4). Isto mostra que as medidas de segurança são importantes para a instituição alcançar seus objetivos (cumprimento da sua missão);
b) o nível de conscientização dos funcionários, com relação aos procedimentos de segurança, obteve média **2,52** (considerada regular pela escala de referência - TAB.4);
c) na opinião dos entrevistados o IPEN deve promover ações mais efetivas, junto aos seus usuários, sobre segurança da informação. Este item obteve média de **3,08** em uma escala de 1 a 4;
d) a avaliação da gestão da segurança da informação do IPEN teve **2,90** de média, sendo considerada regular.

TABELA 4 - Escala de referência

Fraco	Regular	Bom	Ótimo
1 a 1,99	**2 a 2,99**	**3 a 3,49**	**3,50 a 4**

Fonte: elaborada pelo autor

4.3. Questionário

Na análise geral das questões do questionário, constatou-se que as práticas de segurança menos incorporadas ao dia-a-dia dos usuários de TI (com menor aderência) correspondiam às questões 15 e 1 (backup e senhas), com

médias de **2,59** e **2,62,** respectivamente, conforme mostrado na FIG.2 e na TAB.5.

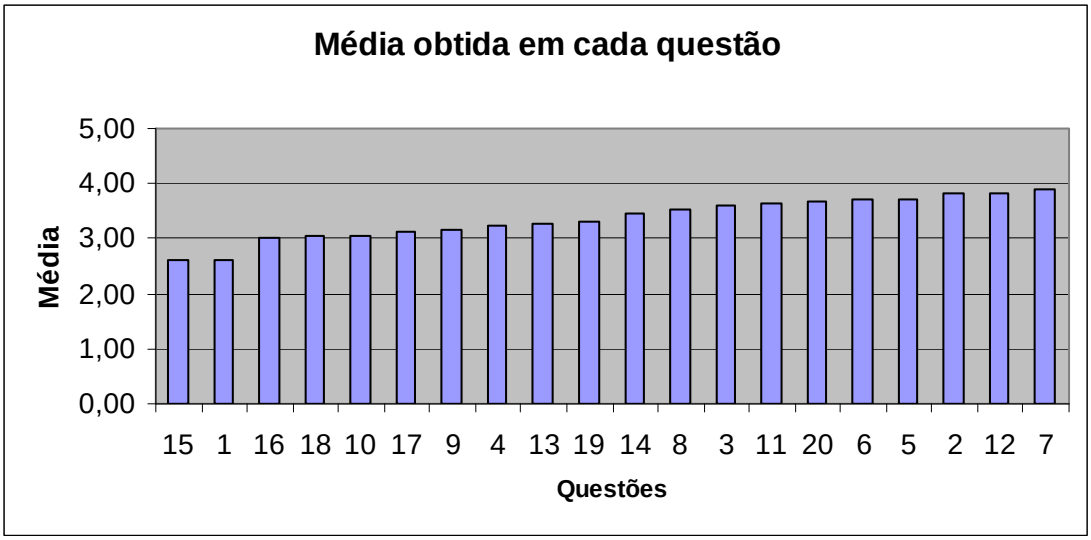

FIGURA 2 – Avaliação das questões do questionário

TABELA 5 - Médias obtidas em cada questão

Q	15	1	16	18	10	17	9	4	13	19	14	8	3	11	20	6	5	2	12	7
M	2,59	2,62	3,03	3,04	3,06	3,13	3,16	3,24	3,27	3,32	3,46	3,55	3,6	3,63	3,69	3,7	3,73	3,82	3,83	3,9
	Media geral: 3,37																			

Na FIG.3 mostra-se que a questão 15 *"Realizo cópia de segurança (backup) dos dados e informações que se encontram sob a minha guarda (no meu computador)",* obteve resposta "sempre" ou "freqüentemente" em 59,24% dos participantes. Por outro lado, 40,77% deles disseram que realizam cópia de segurança "raramente" ou "nunca".

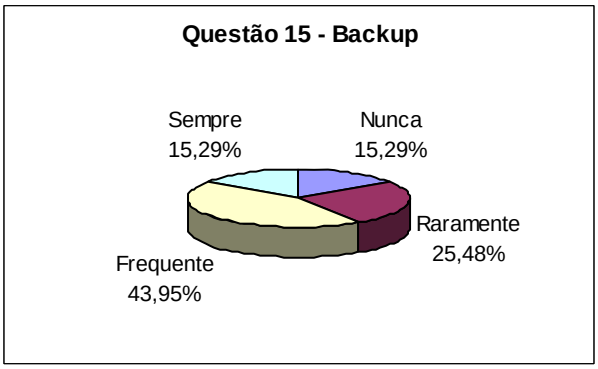

FIGURA 3 - Grau de aderência da prática de backup

A questão 1 *"Utilizou senhas fáceis de lembrar (composta por nomes ou suas iniciais, datas de aniversários, seqüência de letras e números)",* apresentou, conforme é mostrado na FIG.4, 54,77% para "nunca" e "raramente" contra 45,22% para "sempre" e "freqüentemente".

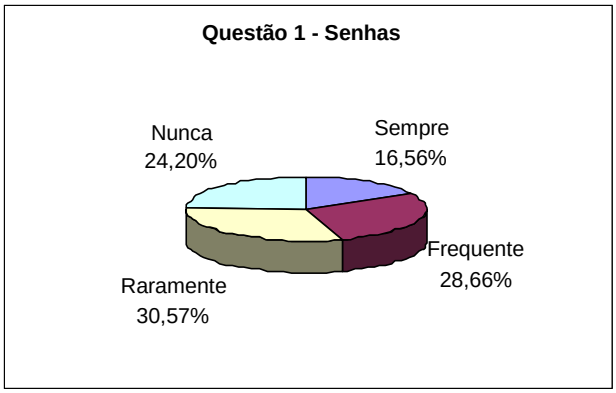

FIGURA 4 - Grau de aderência da prática de criação de senhas

Este resultado confirma uma informação levantada nas entrevistas (TAB.2), onde o domínio de segurança com menor nível de conhecimento foi o de "senhas".

Com relação às hipóteses formuladas, que serviram de base de investigação para o trabalho, conclui-se que:

Hipótese A - **Refutada**

"Desconhecimento das normas e procedimentos de segurança por parte da comunidade de usuários".

A hipótese A foi considerada refutada de acordo com os dados apresentados na FIG.1. A supracitada FIGURA mostra que, na análise geral dos seis domínios de segurança avaliados, 63,33% dos funcionários da instituição têm conhecimento das normas de segurança da informação.

Percebeu-se, entretanto, que as normas e procedimentos de segurança em vigor ainda não foram inteiramente internalizados pelos usuários de sistemas de informação. Ou seja, eles ainda não os incorporaram em seu cotidiano, da forma esperada.

Esta situação evidencia o baixo nível de conscientização e treinamento dos usuários em procedimentos de segurança.

Hipótese B - Confirmada

"Falta de conscientização do usuário quanto aos riscos e danos, associados ao uso inseguro de TI (Tecnologia de informação) e da informação de modo geral, que podem causar impactos negativos às atividades desenvolvidas na organização".

De acordo com os dados da TAB.3, o nível de conscientização dos funcionários foi considerado regular. Além disso, na mesma TABELA os dados apontaram para a necessidade do IPEN promover ações mais efetivas junto aos usuários sobre suas normas e políticas de segurança.

Os entrevistados de maneira geral foram favoráveis a esse tipo de ação. Esta questão alcançou média de 3,08 (numa escala de 1 a 4).

Associando-se as informações da hipótese B com o percentual de 63,33%, mostrado na FIG.1, correspondente aos usuários com conhecimento das políticas de segurança; conclui-se que os usuários têm conhecimento das normas, mas não as colocam em prática. Isto reforça a necessidade da instituição estabelecer um programa abrangente de conscientização e treinamento em segurança da informação.

Hipótese C - Refutada

"As políticas adotadas estão desalinhadas dos requerimentos de segurança da organização, que tem requisitos específicos por se tratar de uma instituição pública de pesquisa científica".

Quando perguntado, aos gerentes, se era importante que o IPEN tivesse uma política de segurança para os seis domínios avaliados, a média alcançada foi de 3,72 – alta (TAB.3).

Entretanto, a avaliação feita com a ferramenta ISG-HE mostrou que a instituição vive uma situação considerada "pobre" em relação a sua gestão da segurança da informação (vide TAB.1).

Concluiu-se, com isso que, as medidas de segurança vigentes estão alinhadas aos requerimentos de segurança da instituição, porém são insuficientes para garantir o nível de proteção necessário.

Pode-se dizer que as normas e procedimentos de segurança em vigor cobrem, essencialmente, questões básicas e corriqueiras ligadas à administração de sistemas de TI (senha, vírus, e-mail, backup).

Estas normas são implementadas, ao que tudo indica, por iniciativa dos próprios administradores de tais sistemas, ou seja, no plano tático / operacional da organização.

É necessário, pois, uma discussão mais ampla que eleve a gestão da segurança da informação para um patamar estratégico.

Hipótese D - Confirmada

"Gestão inadequada da segurança da informação".

Como mostrado na TAB.1, a aplicação da ferramenta ISG-HE contabilizou um total de 66 pontos na avaliação geral da segurança da informação do IPEN, o que corresponde a 19,64% dos 336 pontos possíveis. Aliado a isto, a TAB.3 apresentou a média de 2,90 para a gestão da segurança da informação do IPEN na avaliação dos entrevistados, sendo considerada regular.

Com o objetivo de potencializar a efetividade da segurança da informação, levando-se em consideração o quadro atual mostrado por meio dos dados levantados, este trabalho apresenta a seguinte uma proposta para a re-estruturação da gestão da segurança da informação na instituição.

5. Proposta para a Re-Estruturação da Gestão da Segurança da Informação

Este trabalho foi planejado com o intuito principal de traçar o panorama atual da segurança da informação em um ambiente de pesquisa científica, levantando eventuais pontos fracos (oportunidade de melhorias), para formular proposições no sentido de tornar a gestão da segurança da informação mais efetiva.

A pesquisa realizada mostrou que as normas de segurança em vigência no IPEN, instituição avaliada neste trabalho, são importantes para a execução das suas atividades e estão alinhadas com o negócio da instituição.

Contudo, algumas dessas medidas de segurança apresentaram baixo nível de aderência junto à comunidade de usuários dos sistemas de informação e comunicação. É o caso, por exemplo, da política para a realização de "*backups*", e também dos procedimentos para criação e guarda de "senhas".

Concluiu-se também que os usuários, em geral, têm conhecimento das normas existentes, mas ainda não as incorporaram em seu cotidiano.

Com base no levantamento realizado, constatou-se que as medidas de segurança em vigor são insuficientes para dar a proteção necessária que a instituição precisa. Sendo necessário, portanto, a adoção de outras práticas de segurança, tanto de cunho tecnológico, não-tecnológico e administrativo.

Desta forma, faz-se necessário que a instituição tenha uma postura mais planejada e estruturada da segurança da informação, a fim de assegurar que os ativos de informação, que dão suporte as suas atividades críticas, não venham a comprometer seus objetivos e sua imagem perante seus parceiros e a sociedade.

Por outro lado, deve-se salientar que para um programa corporativo de segurança da informação alcançar os objetivos desejados é necessário que este conte com o apoio incondicional da Alta Direção da organização.

Com o objetivo de potencializar a efetividade da segurança da informação na instituição, este trabalho propõe um modelo de gestão da segurança da informação baseado em cinco pontos considerados essências para o sucesso deste, os quais, durante a pesquisa realizada, se revelaram ausentes ou inexpressivos na gestão da segurança atualmente praticada.

A palavra "modelo" neste contexto significa tão somente: *dar forma ou contorno a;* ou seja, *adaptar, acomodar, conformar, harmonizar*[1]. O modelo proposto, portanto, não deve ser entendido como um método científico ou matemático.

Os cinco pilares de sustentação que compõem este modelo de gestão da segurança da informação são: comprometimento da Alta Direção, estrutura organizacional própria, regulamentação clara e objetiva, treinamento e conscientização dos usuários, e acompanhamento / monitoramento dos resultados produzidos, bem como das novas demandas.

5.1. Modelo Proposto de Gestão da Segurança da Informação

A proposta de gestão da segurança da informação aqui apresentada está fundamentada em cinco pilares de sustentação essenciais para o sucesso de um programa de segurança da informação institucional.

Na FIG.5 apresenta-se o diagrama das etapas de implementação do modelo de gestão proposto.

[1]Novo dicionário AURÉLIO. Ed. Nova Fronteira.

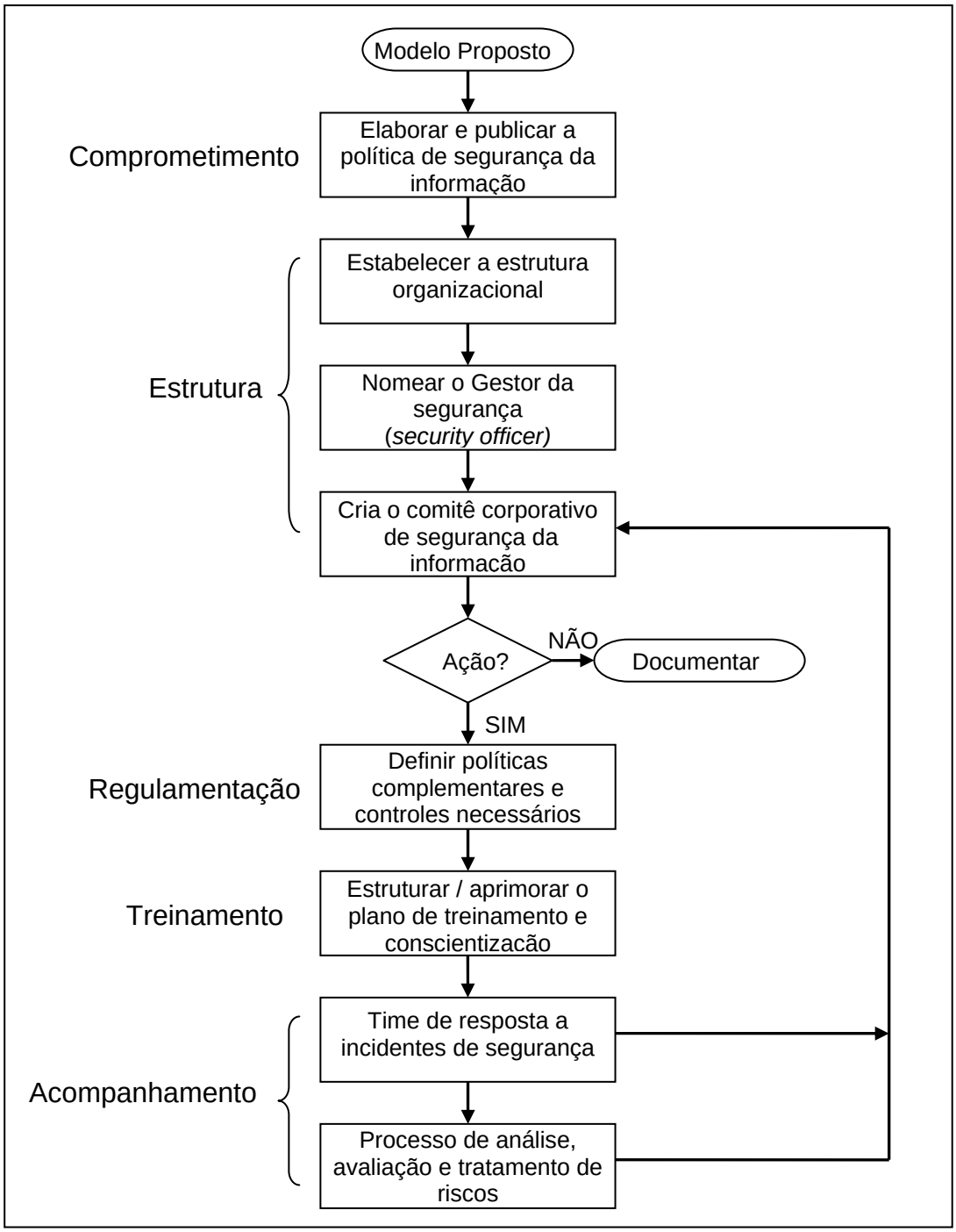

FIGURA 5 - Diagrama da implementação do modelo de gestão da segurança proposto

A seguir serão descritos os cinco elementos chaves do modelo proposto:

1) Comprometimento

O comprometimento corresponde ao engajamento da Alta Direção, que deve prover o apoio e os recursos necessários para o estabelecimento da gestão da segurança da informação na instituição. Sem o comprometimento formal e explicito da Alta Direção, sinalizando para funcionários, alunos, colaboradores, parceiros e sociedade, que a gestão da segurança da informação é um programa

de governança corporativo e de interesse estratégico da instituição, tudo o esforço empreendido ficará fragilizado.

O primeiro ato da Alta Direção para demonstrar seu comprometimento com a segurança da informação, e que, por sua vez, vai desencadear as demais ações para a sua efetividade, é a elaboração e publicação da "política corporativa de segurança da informação".

A política corporativa de segurança da informação é o documento que contém as diretrizes da instituição para o tratamento da segurança da informação. Além disso, esta deve conter suas metas globais, seu escopo, a estrutura para estabelecer os objetivos de controles e os controles, e as responsabilidades gerais e específicas da gestão da segurança da informação (TCU, 2008; ABNT, 2005).

2) Estrutura

É necessário criar uma estrutura organizacional específica e adequada para administrar a segurança da informação. É primordial, para o sucesso do programa, a nomeação de um gestor com as capacidades que a função exige, e que tenha habilidade para transitar pelas unidades de negócio e administrativas da organização.

Este profissional (conhecido no mercado como *security officer*) deve possuir os recursos humanos, financeiros e instrumentais necessários para levar a cabo sua missão. Para tanto é preciso que segurança seja sua única ocupação dentro de organização.

Para SÊMOLA (2003, p. 63) *"esse executivo deve ser multiespecialista, deve ter uma visão completa e horizontal da segurança da informação a partir de conceitos sólidos, deve possuir ricos fundamentos de gestão de projetos, coordenação de equipe e liderança. Tem de ser verdadeiramente executivo, em toda a amplitude da palavra"*.

A Instrução Normativa GSI Nº 1 (BRASIL, 2008) estabelece no seu artigo 7º o seguinte:

Ao Gestor de Segurança da Informação e Comunicações, de que trata o inciso IV do art. 5º, no âmbito de suas atribuições, incumbe:

I- promover cultura de segurança da informação e comunicações;
II- acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
III- propor recursos necessários às ações de segurança da informação e comunicações;
IV- coordenar o Comitê de Segurança da Informação e Comunicações e a equipe de tratamento e resposta a incidentes em redes computacionais;
V- realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na segurança da informação e comunicações;
VI- manter contato direto com o DSIC (Departamento de Segurança da Informação e Comunicações do GSI – Gabinete de Segurança Institucional da Presidência da República) para o trato de assuntos relativos à segurança da informação e comunicações; e
VII- propor normas relativas à segurança da informação e comunicações.

Na atual estrutura do IPEN, a gestão da segurança da informação está a cargo da GRS (Gerência de Redes e Suporte Técnico), que tem como função principal administrar a rede corporativa de computadores e prestar suporte técnico aos usuários.

O organograma do IPEN mostra que a GRS está subordinada à Diretoria Administrativa, o que não confere à segurança da informação a penetrabilidade necessária nas áreas de pesquisa da instituição para efetivamente fazer valer suas ações.

Recomenda-se que a área de segurança da informação (*security office*) esteja adequadamente posicionada no organograma da organização, alinhada ao *core business* (carro-chefe da organização), e se reporte diretamente ao nível estratégico. Esta é a chamada "estrutura organizacional estratégica" (ALEXANDRIA, 2006).

Na estrutura organizacional também pode se incluir a formação do **Comitê Corporativo de Segurança da Informação**. Este comitê deve ser apoiado por uma equipe própria ou terceirizada na esfera tático-operacional e por gestores dos processos críticos em esfera estratégica (SÊMOLA, 2003; 79).

3) Regulamentação

A componente regulamentação compreende as políticas, normas e procedimentos de segurança que todos os usuários devem seguir. Este conjunto de regras vai orientar o comportamento dos usuários no uso das informações corporativas e sistemas de informação e comunicação disponibilizados para a execução das suas tarefas.

As políticas devem ser claras, objetivas, e comunicadas a todos os usuários, para que tenham ciência da sua importância e da necessidade de seu cumprimento. Esta documentação deve ser revisada e atualizada periodicamente.

O IPEN, enquanto órgão da Administração Pública Federal deve estabelecer sua política de segurança da informação em conformidade com a legislação pertinente em vigor. Destacam-se, entre outros, o decreto nº. 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, a lei nº 8.027, de 12 de abril de 1990, que dispõe sobre normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e o decreto nº. 5.563, de 11 de outubro de 2005 - Lei de Inovação.

4) Treinamento

Este item é responsável pela criação e manutenção de um plano educacional geral, que contemple ações de treinamento e conscientização dos usuários. Isto inclui aulas presenciais, palestras, campanha publicitária (cartazes e folhetos), cartilhas e alertas de segurança (E-mail e *Intranet*).

Para se conscientizar o usuário dos riscos a que as informações estão expostas é necessário manter um sistema de treinamento contínuo, para que as práticas de segurança sejam internalizadas e produzam os efeitos esperados.

5) Acompanhamento

Este elemento refere-se ao monitoramento de indicadores, que servirão para realimentar o processo de segurança, aprimorando as medidas e controles adotados.

No acompanhamento se incluem as observações realizadas pela equipe de segurança nas suas atividades diárias (visitas e conversas), incidentes ocorridos, relatórios de auditorias, dentre outros.

Um mecanismo importante de auxilio ao "acompanhamento" é a criação e manutenção de um grupo de tratamento de incidentes. Conhecido como Time de Resposta a Incidentes de Segurança, "*Computer Security Incident Response*

Team (CSIRT)", ele é responsável por receber, analisar e responder a notificações e atividades relacionadas aos incidentes de segurança da informação.

A ABNT NBR ISO/IEC 27002:2005, em sua seção 13 – Gestão de incidentes de segurança da informação, estabelece a seguinte diretriz para implementação de tratamento de incidentes:

> *"Convém que um procedimento formal seja estabelecido para relatar os eventos de segurança da informação, junto com um procedimento de resposta a incidente e escalonamento, estabelecendo a ação a ser tomada ao se receber a notificação de um evento de segurança da informação".*

Outro instrumento pertencente à componente "Acompanhamento" é o processo de análise, avaliação e tratamento de riscos.

Este é um instrumento de realimentação do ciclo da gestão da segurança, que irá fornecer subsídios para o aprimoramento geral das políticas e medidas de segurança implementadas e de novas demandas.

Outras práticas de segurança, tais como, classificação da informação e plano de continuidade de negócio, deverão ser incorporadas ao programa à medida que a segurança da informação esteja consolidada na organização.

A proposta de segurança apresentada neste trabalho tem a intenção principal de tornar efetivas as normas de segurança já estabelecidas na instituição. Desta forma, sugere-se que antes de se partir para um processo oneroso de análise e avaliação de risco, invista-se na implementação de controles de segurança que complementem e aprimorem as medidas já existentes.

O modelo de segurança proposto, o qual este autor chamou de "segurança CERTA", em razão do acrônimo formado pelos cinco componentes que lhes dão sustentação (comprometimento, estrutura, regulamentação, treinamento e acompanhamento), embora proposto para o ambiente de pesquisa científica do Instituto de Pesquisas Energéticas e Nucleares – IPEN, poderá servir de ponto de partida para a implantação da segurança da informação em outras instituições. Estas, por sua vez, deverão promover as adaptações necessárias para atender suas particularidades.

6. Conclusões

A aplicação dos três instrumentos de coleta de dados evidenciou a existência de lacunas na administração da segurança da informação na instituição avaliada.

Esta situação representa uma grave vulnerabilidade para os processos de trabalho da organização, que tem alta dependência dos sistemas de informação para a realização das suas atividades.

Exemplo disto é a ausência de procedimentos de gestão de risco revelada na aplicação do instrumento "*Information Security Governance - Higher Education".*

As entrevistas realizadas com os gerentes mostraram a falta de procedimentos para o tratamento de incidentes de segurança. O que significa dizer que os incidentes ocorridos poderão se repetir.

Por meio do questionário aplicado à comunidade de usuários de TI constatou-se que algumas práticas importantes de segurança da informação não são obedecidas da forma que deveriam.

A pesquisa também mostrou que o IPEN não possui uma política de segurança da informação formalmente definida, nos moldes estabelecidos pela Norma ABNT NBR ISO/IEC 27002:2005.

A definição da política de segurança é o primeiro passo para o reconhecimento da importância da segurança da informação para a organização e para seu tratamento.

Quando se analisa o mercado nacional como um todo, percebe-se que a gestão da segurança da informação está concentrada em um grupo de companhias que se caracteriza por empresas com alta dependência de TI, de grande porte, e pertencentes a setores da economia com forte pressão regulatória.

As instituições públicas, apesar da regulamentação existente, não sofrem maiores pressões dos órgãos superiores para proverem a proteção das suas informações.

A gestão da segurança da informação se faz necessária em qualquer organização que utilize sistemas de informação para apoiar seus processos de trabalho, independentemente da obrigação legal que lhe é imposta.

O mercado brasileiro, e em particular o setor público, tem ainda um longo caminho a percorrer para atingir este nível de maturidade em relação à segurança da informação.

Esta pesquisa revelou ainda que a idéia de segurança da informação está fortemente associada com a garantia da confidencialidade.

Neste aspecto, constatou-se que o principal requerimento de segurança da informação no ambiente de pesquisa científica estudado é a integridade, seguido pela disponibilidade.

Este fato coloca dois grandes desafios para a estruturação da segurança da informação:

a) desmistificar a idéia de que segurança da informação é aplicada quando a confidencialidade é o fator primordial da informação;
b) entender que garantir a integridade e a disponibilidade da informação é um processo complexo que exige a adoção de políticas e procedimentos bem definidos, o que só poderá ser conseguido por meio de uma de gestão bem estruturada.

Verificou-se também que impera no ambiente da pesquisa científica do IPEN o pensamento de que segurança é necessária apenas na proteção das informações institucionais. Entendendo-se como institucionais as informações pertencentes aos grandes sistemas gerenciais da organização.

Existe uma certa minimização da importância das informações que os usuários lidam no seu dia-a-dia, aquelas que estão no computador pessoal, como por exemplo, *e-mails* trocados, documentos diversos do *Word* e planilhas eletrônicas. Talvez resida aí a origem da baixa aderência à prática de *backup* entre os usuários.

Outro efeito associado com esta constatação sugere que a salvaguarda das informações é responsabilidade exclusiva dos departamentos que administram os chamados sistemas gerenciais. O que remete ao departamento de TI total responsabilidade sobre as ações contra disseminação de vírus de computador, cuidados com a segurança das senhas, *backups*, entre outras.

A segurança da informação deve ser entendida como uma responsabilidade de todos. Afinal a informação existe porque alguém irá precisar

dela em algum momento. Portanto, este custodiante (usuário) deve assumir a sua parcela de responsabilidade na proteção da mesma, e em última análise, na segurança geral da organização.

Outro fato a ser considerado na gestão da segurança da informação, em qualquer organização, é o de garantir segurança em toda a cadeia de elementos essenciais do sistema a ser protegido.

Tomando como exemplo o correio eletrônico, considerado o sistema de informação mais importante da instituição, a segurança deste sistema vai exigir esforço e investimento não só no equipamento que o hospeda, mas também em todos os elementos necessários para o seu funcionamento.

Inclui-se aí, por exemplo, uma boa infraestrutura física do ambiente que abriga o referido sistema, condições adequadas de temperatura e umidade, fornecimento ininterrupto de energia, uma rede de comunicação de dados confiável, estações de trabalho (microcomputadores) compatíveis, e treinamento contínuo das pessoas (administradores e usuário final).

A segurança da informação não deve voltar suas atenções só para os grandes ataques *hacker* da *Internet*, vazamentos de segredos industriais, ou vírus de computador de propagação mundial, que ganham destaque na impressa.

É preciso administrar com igual empenho os incidentes comuns do dia-a-dia, antes mesmo que estes aconteçam. Tais incidentes estão propensos a ocorrerem em função de alguma vulnerabilidade existente, muitas vezes negligenciada.

As organizações de uma forma geral vivem um grande dilema: Como se estruturar para gerir a segurança da informação sem saber exatamente o que se pretende e o que se precisa? E como saber o que se precisa sem estar estruturado?

Em suma, as organizações estão cada vez mais dependentes dos sistemas de informação e comunicação, independentemente do porte ou do ramo de atividade, e por esta razão devem compreender que qualquer falha no funcionamento normal destes sistemas, ou seja, qualquer evento que comprometa a sua segurança terá impacto direto no seu negócio.

Referências Bibliográficas

1. ALEXANDRIA, J. C. S. Gestão da Segurança da Informação – Um instrumento para agregar valor aos processos de negócios e não para penalizar o usuário. In: CONGRESSO INTERNACIONAL DE GESTÃO DA TECNOLOGIA E SISTEMAS DE INFORMAÇÃO, 3º., 2006, USP, Mai. 29-Jun. 02, São Paulo, SP. **Proceedings...** São Paulo: FEA-USP, 2006. 1 CD-ROM.

2. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação - Código de práticas para a gestão da segurança da informação. Rio de Janeiro, 2005.

3. AUDACITY. Para Windows, versão 1.2.6. Disponível em: <http://audacity.sourceforge.net/?lang=pt>. Acesso em: 13 fev. 2008.

4. BANCO CENTRAL DO BRASIL. Os Princípios Essenciais da BASILÉIA. 2000. Disponível em: <http://www.bcb.gov.br/ftp/defis/basileia.pdf>. Acesso em: 13 fev. 2008.

5. BRASIL. Instrução Normativa GSI nº 1, de 13 de junho de 2008. Brasília, 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/instrucao normativa_01_cgsi.pdf>. Acesso em: 18 jun. 2009.
6. BRASIL. Resolução nº 7, de 29 de julho de 2002. Brasília, 2002. Disponível em:<http://www.planalto.gov.br/ccivil_03/Resolu%C3%A7%C3%A3o/2002/RES07-02web.htm>. acesso em: 28 abr. 2009.
7. BYRUM, S. The Impact of the Sarbanes-Oxley Act on IT Security. 2004. Disponível em: <http://www.sans.org/reading_room/whitepapers/casestudies/1344.php>. Acesso em: 13 fev. 2008.
8. CASTELLS, M. A sociedade em rede - A era da informação: economia, sociedade e cultura (volume 1). 8ª. ed. São Paulo, S.P.: Paz e Terra, 2005.
9. EDUCAUSE. Information Security Governance Assessment Tool for Higher Education. 2008. Disponível em: <http://www.educause.edu/ir/library/excel/SEC0421.xls>. Acesso em: 17 fev. 2008.
10. ERNST & YOUNG. 10th Annual Global Information Security Survey "Achieving a Balance of Risk and Performance". 2007. Disponível em: <http://www.ey.com/global/assets.nsf/Finland/Global_Information_Security_Survey_2007/$file/10th%20Annual%20GISS.pdf>. Acesso em: 04 abr. 2009.
11. GIL, A. C. Como elaborar projetos de pesquisa. 4º ed. São Paulo, S.P.: Atlas, 2008.
12. GIURLANI, S. Em busca do modelo ideal – A segurança da informação requer uma gestão única sob medida para cada organização. Security review. São Paulo, nº 3, seção Gestão, p. 38-41, ago. 2005.
13. HORTON M.; MUGGE C. Segurança em Redes – Referência rápida. Rio de Janeiro, R.J.: Elsevier Editora, 2004.
14. ISG - Information Security Governance Assessment Tool. Security Task Force. 2004. Disponível em: <http://net.educause.edu/ir/library/pdf/SEC0421.pdf>. Acesso em: 13 fev. 2008.
15. MARCIANO, J. L. P. Segurança da Informação - uma abordagem social. 2006. Tese (Doutorado) – Universidade de Brasília, Brasília.
16. MODULO. 10ª Pesquisa Nacional de Segurança da Informação. 2006. Disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf>. Acesso em: 19 mar. 2009.
17. National Cyber Security Summit Task Force. Corporate Governance Task Force Report. Information Security Governance: A call to action. 2004. Disponível em: <http://www.cyberpartnership.org/InfoSecGov4_04.pdf>. Acesso em: 03 mar. 2008.

18. PEIXOTO R. C. Implicações da Lei Sarbanes-Oxley na Tecnologia da Informação. 2004. Módulo Security Magazine de Abril / 2004. Disponível em: <http://www.correiadasilva.com.br/midia/midia_22.pdf>. Acesso em: 04 abr. 2008.

19. PELTIER, T. R.; PELTIER, J. & BLACKLEY J. Information Security Fundamentals. Boca Raton, FL.: Auerbach, 2005.

20. PEREIRA, J. M. Os Reflexos do Acordo de Basiléia II no Sistema Financeiro Mundial. 2008. Disponível em: <http://repositorio.bce.unb.br/bitstream/123456789/1010/1/ARTIGO_ReflexoAcordoBasileia.pdf>. Acesso em: 18 mar. 2009

21. SÊMOLA, M. Gestão da Segurança da Informação, uma visão executiva. Rio de Janeiro, RJ: Campus, 2003.

22. SOUSA, A. A. O problema da efetividade das leis eleitorais. ***Boletim Jurídico***. 2007. Disponível em: <http://www.boletimjuridico.com.br/doutrina/texto.asp?id=1726>. Acesso em: 25 mar. 2009.

23. TRIBUNAL DE CONTAS DA UNIÃO. Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal. Brasília, 2008. Disponível em: <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/sumarios/Sumario_Governan%C3%A7a%20em%20TI_miolo.pdf>. Acesso em 20 mar. 2009.

24. USA - UNITED STATES OF AMERICA. Federal Information Security Management Act (Title III of E-Gov). 2002. USA, 2002a. Disponível em: <http://www-08.nist.gov/drivers/documents/FISMA-final.pdf>. Acesso em: 15 out. 2007.

25. USA - UNITED STATES OF AMERICA. Sarbanes-Oxley Act. 2002. USA, 2002b. Disponível em: <http://www.law.uc.edu/CCL/SOact/soact.pdf>. Acesso em: 13 fev. 2008.

26. YIN, R. K. Estudo de caso: planejamento e métodos; trad. Daniel Grassi. 3ª. ed. Porto Alegre, R.S.: Bookman, 2005.