AUTARQUIA ASSOCIADA À UNIVERSIDADE DE SÃO PAULO

GESTÃO DA SEGURANÇA DA INFORMAÇÃO – UMA PROPOSTA PARA POTENCIALIZAR A EFETIVIDADE DA SEGURANÇA DA INFORMAÇÃO EM AMBIENTE DE PESQUISA CIENTÍFICA

JOÃO CARLOS SOARES DE ALEXANDRIA

Tese apresentada como parte dos requisitos para a obtenção do Grau de Doutor em Ciências na Área de Tecnologia Nuclear – Aplicações.

São Paulo
2009

INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES
Autarquia associada à Universidade de São Paulo

GESTÃO DA SEGURANÇA DA INFORMAÇÃO – UMA PROPOSTA PARA POTENCIALIZAR A EFETIVIDADE DA SEGURANÇA DA INFORMAÇÃO EM AMBIENTE DE PESQUISA CIENTÍFICA

JOÃO CARLOS SOARES DE ALEXANDRIA

Tese apresentada como parte dos requisitos para a obtenção do Grau de Doutor em Ciências na Área de Tecnologia Nuclear – Aplicações.

Orientador:
Prof. Dr. Luc Marie Quoniam

Co-orientador:
Prof. Dr. Edson Luiz Riccio

São Paulo
2009

Aos meus pais pelo empenho na educação dos filhos.

A minha mulher Márcia e ao meu filho Gabriel pela paciência e compreensão durante as longas horas de estudo.

Agradecimentos

Agradeço ao Instituto de Pesquisas Energéticas e Nucleares – IPEN pela oportunidade da realização deste trabalho de pesquisa.

O desenvolvimento da presente pesquisa contou com apoio de inúmeras pessoas desta conceituada instituição, dentre as quais destaca-se:

Mariliana Santos Abi-eçab, chefe da Gerência de Redes e Suporte Técnico (GRS), pela valiosa colaboração na disponibilização de recursos utilizados e pelas informações prestadas.

Aos demais colegas da GRS meus sinceros agradecimentos.

Sou grato a todos os colegas do IPEN que, de alguma forma, contribuíram com este trabalho, seja respondendo questionário ou participando da entrevista. Muito obrigado a todos que colaboraram doando seu tempo e conhecimentos.

Agradeço aos examinadores que participaram das três sessões de avaliação (qualificação, seminário de área e defesa de tese), Professora Dra. Desirée Moraes Zouain, Prof. Dr. Wilson Aparecido Parejo Calvo, Prof. Dr. Rodolfo Politano, Prof. Dr. Leandro Ninnocentini Lopes de Faria e Prof. Dr. Ailton Fernando Dias, pelas importantes contribuições fornecidas.

Ao Prof. Dr. Edson Luiz Riccio, co-orientador, meu muito obrigado.

Quero expressar meu profundo agradecimento ao Prof. Dr. Luc Marie Quoniam, orientador deste trabalho, por ter acreditado, desde nossa primeira conversa, que a realização desta pesquisa seria possível.
O Prof. Luc foi mais que um orientador, foi um amigo, que esteve sempre presente com um gesto de confiança e de incentivo.

GESTÃO DA SEGURANÇA DA INFORMAÇÃO – UMA PROPOSTA PARA POTENCIALIZAR A EFETIVIDADE DA SEGURANÇA DA INFORMAÇÃO EM AMBIENTE DE PESQUISA CIENTÍFICA

João Carlos Soares de Alexandria

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. A segurança da informação tem o objetivo de salvaguardar a efetividade das transações e, por conseguinte, a própria continuidade do negócio. As ameaças à informação vão desde ataques *hackers*, fraudes eletrônicas, espionagem e vandalismo; a incêndio, interrupção de energia elétrica e falhas humanas. Segurança da informação é obtida a partir da implementação de um conjunto de controles, incluindo-se dentre outros, políticas, processos, procedimentos, estruturas organizacionais, *software* e *hardware*, o que exige uma gestão contínua e uma estrutura administrativa bem estabelecida para fazer frente aos seus desafios. O presente trabalho procurou investigar as razões relacionadas às dificuldades que muitas organizações enfrentam para a estruturação da segurança da informação. Muitas delas se limitam a adotarem medidas pontuais e inconsistentes com a realidade em que vivem. O mercado conta com um arcabouço legal e normativo para a implementação da segurança da informação – NBR ISO/IEC 27002, Lei Americana *Sarbanes-Oxley,* acordo de capital da Basiléia, regulamentações das agências regulatórias (ANATEL, ANVISA e CVM). As 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 sistema de informação nos seus processos de trabalho, independentemente do porte ou do setor econômico de atuação. A situação da segurança da informação no setor governamental do Brasil, e dentro deste, nas instituições de pesquisas científicas é considerada preocupante, de acordo com o Tribunal de Contas da União. Este trabalho apresenta um método de diagnóstico e avaliação da segurança da informação, aplicado na forma de levantamento de dados, que tem a intenção de servir de ponto de partida para fomentar uma discussão interna visando à estruturação da segurança da informação na organização. O referido método é destinado em especial àquelas organizações que não se enquadram no perfil das empresas atingidas pelas leis e regulamentos existentes, mas que necessitam igualmente protegerem seus ativos de informação para o bom e fiel cumprimento de seus objetivos e metas de negócio.

Palavras-chaves: Segurança da informação, ABNT NBR ISO/IEC 27002:2005, risco, fator humano

INFORMATION SECURITY MANAGEMENT – A PROPOSAL TO IMPROVE THE EFFECTIVENESS OF INFORMATION SECURITY IN THE SCIENTIFIC RESEARCH ENVIRONMENT

João Carlos Soares de Alexandria

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. Information security has as main goal to protect the business transactions in order to work normally. In this way, It will be safeguarding the business continuity. The threats of information come from hackers' attacks, electronic frauds and spying, as well as fire, electrical energy interruption and humans fault. Information security is made by implementation of a set of controls, including of the others politics, processes, procedures, organizational structures, software and hardware, which require a continuous management and a well established structure to be able to face such challenges. This work tried to search the reasons why the organizations have difficulties to make a practice of information security management. Many of them just limit to adopt points measures, sometimes they are not consistent with their realities. The market counts on enough quantity of standards and regulations related to information security issues, for example, ISO/IEC 27002, American Sarbanes-Oxley act, Basel capital accord, regulations from regulatory agency (such as the Brazilians ones ANATEL, ANVISA and CVM). The market researches have showed that the information security implementation is concentrated on a well-defined group of organization 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. The situation of information security in the governmental sector of Brazil, and inside its research institutions, is considered worrying by the Brazilian Court of Accounts (TCU). This research work presents an assessment and diagnostic proposal of information security, applied in the form of a data survey, which intend to be a tool that can be used as a starting point to foment debates about information security concerns into organization. This can lead them to a well-structured information security implementation. The referred proposal is specially addressed to those organizations that do not have the profile that put them among those companies which are forced to follow some law or regulation. But in the same way they need to protect their information assets to reach their goals and their business objectives.

SUMÁRIO

Página

TABELAS

Página

FIGURAS

Página

SIGLAS E ABREVIATURAS

ABES	Associação Brasileira das Empresas de *Software*
ABNT	Associação Brasileira de Normas Técnicas
AIEA	Agência Internacional de Energia Atômica
ANATEL	Agência Nacional de Telecomunicações
ANSP	*Academic Network at São Paulo*
ANVISA	Agência Nacional de Vigilância Sanitária
ARBIL	*Asset and Risk Based INFOSEC lifecycle*
ARPANET	*Advanced Research Projects Agency Network*
BCB	Banco Central do Brasil
CAIS	Centro de Atendimento a Incidentes de Segurança
CCSC	*Commercial Computer Security Centre*
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CERTA	Comprometimento, Estrutura, Regulamentação, Treinamento e Acompanhamento
CIA	*Confidentiality, Integrity and Availability*
CIO	*Chief Information Officer*
CISO	*Chief Information Security Officer*
CNEN	Comissão Nacional de Energia Nuclear
CobiT	*Control Objectives for Information and related Technology*
CPD	Centro de Processamento de Dados
CQAS	Coordenação da Qualidade Meio Ambiente e Segurança
CRM	*Customer Relationship Management*
CSBB	Comitê de Supervisão Bancária da Basiléia
CSIRT	*Computer Security Incident Response Team*
CSO	*Chief Security Officer*
CTA	Conselho Técnico Administrativo
CTO	*Chief Technical Officer* ou *Chief Technology Officer*
CVM	Comissão de Valores Mobiliários
DDOS	*Distributed Denial of Service*
DMZ	*DeMilitarized Zone* (zona desmilitarizada)
DOD	Departamento de Defesa dos Estados Unidos
DOU	Diário Oficial da União
DSIC	Departamento de Segurança da Informação e Comunicações do GSI
ERP	*Enterprise Resource Planning*

FAPESP	Fundação de Amparo à Pesquisa do Estado de São Paulo
FIESP	Federação da Indústria do Estado de São Paulo
FISMA	*Federal Information Security Management Act*
FUCAPI	Fundação Centro de Análise, Pesquisa e Inovação Tecnológica
GDP	Gerência de Desenvolvimento de Pessoas
GMITS	*Guidelines to the Management of Information Technology Security*
GRS	Gerência de Redes e Suporte Técnico
GSI	Gabinete de Segurança Institucional
HIPAA	*Health Insurance Portability and Accountability Act*
ICP-Brasil	Infra-Estrutura de Chaves Públicas Brasileira
ICT	Instituições de Ciência e Tecnologia
IEC	*International Electrotechnical Comission*
IEEE	*Institute of Electrical and Electronics Engineers* (Instituto de Engenheiros Eletricistas e Eletrônicos)
IFAC	*International Federation of Accountants*
INB	Indústrias Nucleares do Brasil
INFOSEC	*Information Security*
IPEN	Instituto de Pesquisas Energéticas e Nucleares
IRC	*Internet Relay Chat*
IRM	*Institute of Risk Management*
ISACA	*Information Systems Audit and Control Association*
ISG-HE	*Information Security Governance Assessment Tool for Higher Education*
ISO	*International Organization for Standardization*
ITGI	*IT Governance Institute*
LAN	*Local Area Network* (redes locais de computadores)
LNCC	Laboratório Nacional de Computação Científica
NBR	Norma Brasileira
NCSSTF	*National Cyber Security Summit Task Force*
NIPC	*National Infrastructure Protection Center*
NIST	*National Institute of Standards and Technology*
NSW	*New South Wales* (Estado da Austrália)
OCDE	Organização para a Cooperação e Desenvolvimento Econômico *(OECD - Organisation for Economic Co-operation and Development)*
OCTAVE	*Operationally Critical Threat, Asset, and Vulnerability Evaluation*
P&D	Pesquisas e Desenvolvimento

PARC	*Palo Alto Research Center*
PDAs	*Personal Digital Assistants* (Assistente Pessoal Digital)
PME	pequenas e médias empresas
PRODESP	Companhia de Processamento de Dados do Estado de São Paulo
SCI	Serviço de Comunicação Institucional
SDLC	*System Development Life Cycle*
SEFTI	Secretaria de Fiscalização de Tecnologia da Informação
SEI	*Software Engineering Institute*
SERPRO	Serviço Federal de Processamento de Dados
SGI	Sistema de Gestão Integrada
SIAFI	Sistema Integrado de Administração Financeira
SIAPE	Sistema Integrado de Administração de Recursos Humanos
SIASG	Sistema Integrado de Administração de Serviços Gerais
SICAF	Sistema de Cadastramento Unificado de Fornecedores
SIGEPI	Sistema de Informação Gerencial e de Planejamento do IPEN
SOX	*Sarbanes-Oxley Act*
SRI	*Stanford Research Institute*
STJ	Superior Tribunal de Justiça
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TNCMC	Tratamento de não conformidade e melhoria contínua
UCLA	Universidade da Califórnia - Los Angeles
UCSB	Universidade da Califórnia - Santa Barbara
UFRJ	Universidade Federal do Rio de Janeiro
USA	*United States of America*
USP	Universidade de São Paulo
WWW	*World Wide Web*

1. INTRODUÇÃO

A informação é hoje um bem de suma importância em todas as áreas da atividade econômica, e não poderia ser diferente em uma instituição de pesquisa que atua no campo da energia nuclear, setor estratégico para o crescimento econômico e social de uma nação; além disso, trata-se de uma tecnologia dominada por um grupo seleto de países em todo o mundo.

A sociedade moderna vive a chamada era da informação ou informacional. 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 empresas 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.

Um caso que ganhou destaque nos jornais foi o das ultracentrífugas brasileiras utilizadas no processo de enriquecimento de urânio, desenvolvidas com tecnologia nacional pela Marinha, quatro vezes mais econômicas e produtivas que as tradicionais utilizadas nos Estados Unidos e na Europa.

A polêmica gerada em torno dessas máquinas envolveu a Agência Internacional de Energia Atômica (AIEA) que, em visita as Indústrias Nucleares do Brasil (INB), exigia visualização total dos equipamentos, a fim de garantir que eles não seriam usados para a produção de armas nucleares. O governo brasileiro

permitiu maior visualização dos mesmos, porém, sem que seu segredo industrial fosse comprometido (THOMÉ, 2006).

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.

1.1. Objetivos

O objetivo do presente estudo é a formulação de proposições que possam melhorar a efetividade das normas e procedimentos de segurança da informação em instituições públicas de pesquisa científica do setor nuclear brasileiro.

1.1.1. Objetivo Geral

A segurança da informação no IPEN (Instituto de Pesquisas Energéticas e Nucleares), e possivelmente em outras instituições de pesquisa científica, tem se pautado invariavelmente em controles tecnológicos (*Firewall* e antivírus, entre outros.). O presente trabalho tem a intenção de promover uma visão mais holística da segurança da informação no âmbito das instituições de pesquisa científica, que leve em consideração as particularidades das suas atividades e contemple outras práticas de gestão da segurança da informação, com base na Norma ABNT NBR ISO/IEC 27002:2005.

1.1.2. Objetivos Específicos

- Caracterizar a importância da segurança da informação no cenário econômico atual e em particular no ambiente de pesquisa científica;
- Realizar um levantamento das práticas de segurança da informação formalmente estabelecidas;
- Avaliar a aderência dessas políticas junto aos usuários em suas atividades cotidianas; e
- Verificar com os gestores da instituição (tomadores de decisão) as necessidades e demandas pertinentes ao assunto abordado.

1.2. Contribuição do Trabalho

1.2.1. Contribuição Original ao Conhecimento

Desenvolvimento de um método de diagnóstico e avaliação das práticas de segurança da informação para instituições públicas de pesquisa científica, visando à implementação de ações que potencializem sua efetividade.

Este trabalho pretende ser uma contribuição aos estudos acerca da segurança da informação no Brasil, e da sua implementação em organizações que por força das suas características, dentre as quais se encontram as instituições públicas de pesquisa cientifica, não se enquadram no perfil das

organizações que figuram em posição de destaque na implementação de práticas relativa ao tema abordado.

1.2.2. Contribuições Específicas

As contribuições advindas deste trabalho de pesquisa podem ser resumidas da seguinte forma:

I) levantamento das normas e procedimentos de segurança da informação formalmente adotados pela organização;

II) fornecimento de elementos para a estruturação da segurança da informação;

III) identificação dos sistemas de informação que carecem de controles de segurança mais robustos;

IV) fornecimento de subsídios para a adequação das medidas de segurança face às necessidades reais de um ambiente de pesquisa científica e tecnológica;

V) contribuição para um melhor entendimento dos benefícios obtidos por meio da gestão de segurança da informação como instrumento de governança corporativa;

VI) ampliação do escopo da segurança da informação para além dos controles de cunho tecnológicos;

VII) fortalecimento de ações de segurança que valorizem o elemento humano envolvido; e

VIII) identificação das áreas onde a situação da segurança da informação está mais crítica, e que exige uma atuação mais efetiva;

Os dados levantados nesta pesquisa constituem indicadores que podem ser usados para promover ações educativas e de conscientização, em práticas de segurança com fraca aderência junto ao usuário de TI.

1.3. Justificativa

> *"Boa parte da administração pública pode estar vulnerável à ocorrência de interrupção de serviços, perda de dados, fraudes e paralisação das funções essenciais"* - Ministro Guilherme Palmeira (TCU, 2008).

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 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 motivação para o desenvolvimento de um método de diagnóstico e avaliação das práticas de segurança da informação vem da necessidade de se promover um maior engajamento e conscientização do corpo executivo e dos

tomadores de decisão (nível estratégico / tático) com respeito à importância da segurança da informação em qualquer tipo de organização.

Esta conscientização da alta direção da organização elevará a segurança da informação, de uma condição pontual e esporádica, para o patamar estratégico, como prática gerencial estruturada de governança corporativa.

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. É nesta lacuna que o instrumento de diagnóstico e avaliação, aqui apresentado, deve se situar.

Este instrumento de diagnóstico não exige a formalidade nem o custo financeiro e operacional que se teria na aplicação de uma metodologia de análise e avaliação de risco. O instrumento de diagnóstico proposto neste trabalho pode ser conduzido por uma única pessoa, na forma de um levantamento de dados.

Já a aplicação de uma metodologia de análise e avaliação de risco requer um nível de especialização que normalmente essas organizações não possuem. De qualquer forma deverá sempre existir a figura de um tutor (patrocinador), gerente ou diretor, que se interesse pelo projeto e que sirva de porta voz, em sua defesa, dentro da organização.

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.

Pesquisas mostram que 40% do acesso à *Internet* nas empresas não estão relacionados aos negócios, o que resulta em perda de produtividade e abertura para a entrada de *spywares* e vírus (CADERNO DIGITAL, 2008).

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 lucro final (bottom line) e elevam a segurança da informação de uma solução tática para uma importância estratégica"*.

Não obstante, muitas organizações ainda relutam em investir na área de segurança da informação. Dados da 10ª Pesquisa Nacional de Segurança da Informação (MODULO, 2006) revelam que 33% das companhias pesquisadas não sabem quantificar as perdas provenientes das falhas de segurança, 21% delas sequer conseguem identificar os responsáveis pelo problema. Ainda de acordo com a referida pesquisa o motivo para este percentual elevado pode ser a falta de um planejamento formal de segurança, que muitas dessas empresas não possuem (35%).

Entre as pequenas e médias empresas (PMEs) a situação é preocupante. De acordo com pesquisa realizada pelo *Instituto Applied Research*, a pedido da empresa de segurança Symantec, 30% das pequenas e médias empresas (PMEs) brasileiras não usam antivírus, 42% delas não implantam ferramentas de *backup* e de restauração de *desktops*, 35% não possuem *antispam*; e 40% não têm *backup* ou sistema de recuperação de servidor.

A falta de recursos e de funcionários qualificados são as principais causas para essas falhas, de acordo com as próprias PMEs (AFONSO, 2009).

Estas empresas estão expostas aos seguintes problemas, conforme destaca matéria do Jornal da Tarde (BURGHI, 2009):

- interrupção do funcionamento da rede de computadores ou do computador por conta de um vírus vindo da própria rede ou de um *pendrive* conectado;

- recebimento de *spam* (mensagem do tipo “clique aqui”);
- defeito de ordem técnica em computador;
- a direção da empresa não tem controle sobre as páginas de *internet* consultadas pelos funcionários.

Além das despesas com o conserto de equipamentos e reinstalação de sistemas, a empresa arcará com as conseqüências de ficar impossibilitada de se comunicar com os clientes e fornecedores, de ter arquivos apagados ou adulterados, e senhas roubadas. Ainda de acordo com a matéria do referido Jornal, esta situação poderá levar entre outros problemas, a extinção dos sistemas contábeis e fiscais da empresa.

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).*

O TCU fez uma série de recomendações para toda a administração federal no sentido de que melhorem o planejamento estratégico para a tecnologia da informação e para o gerenciamento da segurança da informação. Dentre elas estão promover ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso.

Quando se observa o setor da pesquisa científica e tecnológica do Brasil, e em particular a área nuclear, verificam-se poucos avanços na

implementação de segurança da informação, como prática gerencial estruturada e formalmente estabelecida.

Como administrador da rede corporativa de computadores do IPEN, e dos seus sistemas de segurança, nos últimos 25 anos, este autor vivenciou inúmeras situações relacionadas com a segurança da informação na instituição. Durante este período foi possível acompanhar as diversas etapas da evolução da tecnologia de informação na instituição, como por exemplo, o processo de *downsizing* ocorrido no início dos anos 90, quando foi realizada a migração da plataforma *mainframe* (grande porte) IBM4381 para uma plataforma baixa, baseada em estações RISC 6000.

Na área da segurança da informação o autor participou da instalação e configuração do primeiro *firewall* instalado na rede do IPEN, em 1998. Tratava-se de um “PortMaster IRX Router” da *Livingston*, substituído dois anos mais tarde por um sistema Linux/Iptables em uma arquitetura DMZ, e também do atual sistema Cisco/PIX525 instalado em 2004. Além disso, foi responsável pela criação de um sistema IDS Linux/Snort, conforme apresentado na sua dissertação de mestrado (ALEXANDRIA, 2001).

No IPEN são vários os exemplos de incidentes de segurança que afetaram diretamente as suas atividades de pesquisa e a imagem da instituição. Na TAB.1 apresentam-se alguns incidentes de segurança ocorridos na instituição, de acordo com os registros mantidos pela Gerência de Redes e Suporte Técnico (GRS).

TABELA 1 - Exemplos de incidentes de segurança ocorridos no IPEN

Data	Descrição	Conseqüência	Motivo
03/10/2005	Perda do acesso aos sistemas do Governo Federal (SERPRO)	Interrupção das atividades administrativas que dependem dos sistemas SIAFI, SICAF, SIASG, e outros	O acesso do IPEN foi bloqueado no SERPRO por ter sido identificado como disseminador do vírus Beagle.W.
12/09/2007	Descoberto na rede um computador contendo grande volume de material pornográfico / pedófilo e músicas	Violação da lei (Código Penal e Lei Nº 9.610)	
13/03/2008	Problema de *Copyright* envolvendo o IPEN	Notificação recebida da Equipe de Segurança da ANSP e da ABES	Grande quantidade de *downloads* praticados por máquinas do IPEN.
31/03/2008 10/04/2008	Interrupção de energia elétrica e o gerador não funcionou	Toda a rede do IPEN parou.	Descarga das baterias do *No-break* desligando todos os equipamentos da sala de servidores.
04/11/2008 09/02/2009	Invasão ao servidor Web	A página Web do IPEN ficou fora do ar	O atacante gravou uma página fraudulenta dentro da *Homepage* do IPEN.
14/01/2009	Problema de segurança envolvendo a rede do IPEN	Notificação recebida da Equipe de Segurança da ANSP / SpamCop. Usuários ficaram impedidos de enviar *e-mails* para determinados sites.	SPAMs gerado a partir da rede do IPEN. O domínio “ipen.br” foi incluído em Blacklists (SpamCop)

Fonte: IPEN/GRS

A gerência de TI do IPEN considera como situações críticas os vírus, o uso indevido do e-mail e a pirataria (*software*s, músicas e filmes, entre outros.)[1].

Um bom exemplo de como a gestão da segurança da informação deve ser implementada em instituições de pesquisas científicas vem do norte do país. A Fundação Centro de Análise, Pesquisa e Inovação Tecnológica (FUCAPI), do Amazonas, embora sendo uma instituição privada, é um exemplo a ser seguido. A FUCAPI é a primeira instituição desse gênero a conquistar a certificação ISO 27001.

[1] Palestra “workshop de Integração GDS/GRS” realizada em 27/06/2008.

Na FUCAPI o sistema de gestão da segurança das informações (ISO27001) foi implementado integrando-o ao sistema de gestão da qualidade ISO9001 (CAMINHA, 2006).

O Brasil contava em março de 2009, com 20 empresas certificadas em segurança da informação (ISO 27001)[2], ocupando a 19ª colocação do *ranking* mundial, que tinha Japão, Índia e Reino Unido nas três primeiras posições, com 2997, 435 e 370 certificações, respectivamente. Dentre as organizações brasileiras figuravam ainda a PRODESP - Companhia de Processamento de Dados do Estado de São Paulo, o SERPRO - Serviço Federal de Processamento de Dados e o STJ - Superior Tribunal de Justiça.

[2] http://www.iso27001certificates.com

2. REVISÃO DA LITERATURA

2.1. Sociedade da Informação

Segundo CASTELLS (2005; p. 53), cada modo de desenvolvimento possui um elemento essencial no processo produtivo. Desta forma, no modo agrário de desenvolvimento identifica-se a mão-de-obra e os recursos naturais (particularmente a terra) como elemento fonte de incremento da produção, ou seja, o aumento da produtividade / lucratividade está diretamente relacionado aos aumentos quantitativos desses recursos. No modo de desenvolvimento industrial a principal fonte de produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo do processo produtivo e de circulação. Já no novo modo informacional de desenvolvimento, a produtividade está fortemente baseada na tecnologia de geração de ***conhecimento****, de processamento da* ***informação*** *e da* ***comunicação*** *de* símbolos.

Para o supracitado autor, conhecimento e informação são elementos cruciais em todos os modos de desenvolvimento, visto que o processo produtivo sempre se baseia em algum grau de conhecimento e no processamento da informação. Contudo, o que é específico ao modo informacional de desenvolvimento é a ação de conhecimento sobre os próprios conhecimentos como principal fonte de produtividade.

STRAUBHAAR (1995 apud SQUIRRA, 2005) define sociedade da informação como "*aquela na qual produção, processamento e distribuição de informação são as atividades econômicas e sociais primárias*". Afirmando ainda que a sociedade da informação representa um passo à frente na evolução da sociedade, das suas bases originais na agricultura, na manufatura e na economia da informação, na qual a manipulação da informação é a atividade básica e principal.

CASTELLS (2005) faz ainda uma distinção entre os termos sociedade da informação e sociedade informacional. O termo sociedade da informação, segundo ele, enfatiza o papel da informação na sociedade, que como *comunicação de conhecimento* é essencial em qualquer sociedade. Porém, o termo informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação

tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico (CASTELLS, 2005; p. 65).

O termo pós-industrialismo cunhado por Daniel Bell (BELL 1973 apud FERREIRA, 2003) também pode ser encontrado como sinônimo aos termos informação e conhecimento, que serviram para caracterizar o novo tipo de sociedade que surgia diante do crescente desenvolvimento das tecnologias de computação e comunicação. Bell afirma, também, que:

> "*a sociedade pós-industrial é uma sociedade da informação, e que a economia de serviços indica o advento do pós-industrial. A informação envolve características dos tipos de vida em diferentes épocas: na sociedade pré-industrial a vida era um jogo contra a natureza, na qual se trabalhava com a força muscular; na era industrial, quando a racionalização e a técnica das máquinas predominavam, a vida era um jogo contra a natureza fabricada. Em contraste com ambas, a vida na sociedade pós-industrial é baseada em serviços, um jogo entre pessoas, onde o que vale não é a força muscular ou a energia, mas a informação*."

Para Yara Rezende (REZENDE, 2002), o último estágio da sociedade pós-industrial é a sociedade do conhecimento, na qual a criação, distribuição e manipulação da informação constituem a principal fonte de geração de riquezas. E acrescenta:

> "*o principal foco gerador de riqueza não é mais o trabalho manual, e sim o intelectual. Empresas pobres de bens, mas ricas de cérebros, passam a ser as mais valorizadas, como as consultorias, as agências de publicidade e criação, as empresas de auditoria, as empresas criadoras de softwares e de novas soluções informatizadas, bem como as empresas 'ponto com'*."

Os termos dados, informação e conhecimento têm causado muita confusão e discussões por conta das diversas definições encontradas. Peter Drucker (DRUCKER, 1988 apud DAVENPORT, 2000; p. 19) definiu informação "*como dados dotados de relevância e propósito*".

Para DAVENPORT & PRUSAK (1998 apud ALESSIO, 2004), ***informação*** é *"uma mensagem, geralmente na forma de um documento ou uma comunicação audível ou visível*". A informação tem como objetivo modelar a pessoa que a recebe no sentido de fazer alguma diferença em sua perspectiva ou percepção.

Na TAB.2 são apresentados os conceitos estabelecidos pelos referidos autores de forma sintetizada.

TABELA 2 - Conceito de dados, informação e conhecimento

Dados, Informação e Conhecimento		
Dados	**Informação**	**Conhecimento**
Simples observações sobre o estado do mundo.	Dados dotados de relevância e propósito.	Informação valiosa da mente humana. Inclui reflexão, síntese, contexto.
• Facilmente estruturado • Facilmente obtido por máquinas • Freqüentemente quantificado • Facilmente transferível	• Requer unidade de análise • Exige consenso em relação ao significado • Exige necessariamente a mediação humana	• De difícil estruturação • De difícil captura em máquinas • Freqüentemente tácito • De difícil transferência

Fonte: Davenport, 2000 - p.18

Solange Oliveira Rezende (REZENDE, 2005, p. 3) descreve “dado” como um elemento puro, quantificável sobre um determinado evento. Dados são fatos, números, texto ou qualquer mídia que possa ser processada pelo computador. Hoje em dia, as organizações estão acumulando vastas e crescentes quantidades de dados em diferentes formatos e em diferentes tipos de repositórios. Ela ressalta que o dado, por si só, não oferece embasamento para o entendimento da situação.

Enquanto que a informação é descritiva, o conhecimento é utilizado fundamentalmente para fornecer uma base de previsão com um determinado grau de certeza. O conhecimento refere-se à habilidade de criar um modelo mental que descreva o objeto e indique as ações a implementar e as decisões a tomar.

Uma decisão é o uso explícito de um conhecimento (REZENDE, 2005; p. 4). A autora supracitada conclui:

> *“o desafio dos anos de 1980 foi migrar os dados para as informações, por meio do desenvolvimento dos sistemas de Informação, que tinham por finalidade analisar dados e organizar a informação para melhorar o processo decisório empresarial. A partir da década de 1990, o desafio era criar sistemas que fossem capazes de representar e processar conhecimento, em resposta às diferentes necessidades de indivíduos, grupos e culturas”.*

Uma abstração informal que representa algo significativo para alguém, através de textos, imagens, sons ou animação; é assim que SETZER (1999) caracteriza informação.

Partindo-se, portanto, do pressuposto de que informação e conhecimento são os elementos fundamentais da sociedade da informação, é de se esperar que as organizações adotem uma postura efetiva de proteção destes tão importantes ativos, que é sem dúvida, o grande diferencial competitivo no

modo de desenvolvimento econômico atual. Esta proteção deve ser parte integrante das propagadas *governança corporativa, gestão do conhecimento ou gestão da segurança da informação*.

2.2. Segurança

A palavra segurança é freqüentemente associada a ações de restrição e cerceamento. Ou seja, segurança muita vezes é entendida como sinônimo de reprimir, impedir, proibir e punir.

Ao longo da história algumas figuras ficaram marcadas como símbolos de segurança. A figura de uma fortaleza, por exemplo, representa bem essa idéia antiga de segurança. Pode-se também recorrer à imagem de um castelo medieval como exemplo de instrumento eficaz de segurança. Isto é, uma edificação quase inviolável pelos inimigos, com muralhas altas, guardas fortemente armados, caldeirões de óleo fervente para afugentar quem se atrevesse escalar seus muros. Sem contar o fosso existente em toda sua volta cheio de crocodilos famintos.

Quando se busca através da história por práticas de segurança utilizadas em torna da proteção da informação é inevitável não se lembrar das bibliotecas da idade média.

Durante a Idade Média o principal obstáculo para a aquisição de livros era o fator econômico, pois o pergaminho utilizado nos livros tinha preço elevado.

A partir do século XIV o uso do papel, até treze vezes mais barato que o pergaminho, propagou-se pela Europa. Isto graças às novas técnicas de papelaria e à multiplicação das oficinas de papel. Porém, o custo das cópias ainda era muito elevado (CÂNDIDO & OLIVEIRA, 2005).

Esses fatores colaboravam para a restrição ao uso das bibliotecas naquela época, e, portanto, da informação e conhecimento. Apenas os homens de saber e os ricos tinham acesso aos acervos das bibliotecas.

De acordo VERGER (1999, apud CÂNDIDO & OLIVEIRA, 2005) *“a biblioteca possuía um alto valor de mercado. Ela representava uma forma de entesouramento, um capital tanto intelectual quanto financeiro que se pretendia legar aos seus herdeiros”*.

Além da questão econômica este período da historia é cercado de debates políticos, filosóficos e religiosos. Esta situação é retratada com muita

fidelidade no filme ***O nome da rosa***. A história narrada neste filme se passa em um remoto mosteiro beneditino do norte da Itália, onde era proibido aos monges acessarem aos raríssimos e importantes livros que formavam um magnífico acervo.

De acordo com a resenha do filme “O nome da rosa” (RECANTO DAS LETRAS, 2008):

> *“um monge Franciscano e Renascentista, interpretado pelo ator Sean Conery, foi designado para investigar vários crimes que estavam ocorrendo no mosteiro. Os mortos eram encontrados com a língua e os dedos roxos e, no decorrer da história, verifica-se que eles manuseavam (desfolhavam) os livros, cujas páginas estavam envenenadas. Então, quem profanasse a determinação de ‘não ler o livro’, morreria antes que informasse o conteúdo da leitura”*.

Ou seja, a punição para alguém que acessasse uma informação proibida (restrita), tendo violado, portanto, uma norma estabelecida, era a morte.

Esta relação entre segurança e restrição à informação volta à tona com muita força, na história recente, com os regimes governamentais totalitaristas. No Brasil durante o período da ditadura militar, de 1964 a 1985, os generais impuseram uma implacável censura aos meios de comunicação de massa.

Os atos institucionais, particularmente o AI-5 promulgado em 13 de dezembro de 1968, foram instrumentos ditatoriais de censura e ataques à liberdade de imprensa (acesso à informação). Durante este período era prática comum das forças de repressão do governo a invasão de redações de jornais e destruição de suas oficinas (SOARES, 1989).

Por outro lado, de acordo com MATOS (2001), a palavra ‘segurança’ tem origem no latim, língua na qual significa “sem preocupações”, e cuja etimologia sugere o sentido “ocupar-se de si mesmo” (se+cura).

Em uma definição mais comum, segurança refere-se a “um mal a evitar”. Por isso segurança é a ausência de risco, a previsibilidade, a certeza quanto ao futuro.

Para o supracitado autor, segurança é uma relação entre o segurado e o risco, onde o risco tem origem em fatos naturais ou humanos – uma dada catástrofe física ou uma ação humana que ameaça o objeto a ser protegido. O risco humano é considerado pior do que o natural, pois este é tido por inevitável ao passo que o humano é considerado arbitrário.

A palavra ‘segurança’ é empregada na língua portuguesa com múltiplos sentidos, o que a torna de difícil conceituação. Ela é empregada, por exemplo, quando se analisa a capacidade de resistência à intrusão de um determinado edifício, por hipotéticos assaltantes. Tomando-se como exemplo uma agência bancária pode-se dizer que tal prédio será mais ou menos seguro, consoante o maior ou menor grau de resistência apresentado.

O termo ‘segurança’ também é empregado ao se analisar algumas características observadas no percurso de acesso a esse mesmo edifício; por exemplo, a ausência de sinalização específica que alerte sobre a existência de uma curva acentuada ou que indique proximidade de uma escola. Estas “seguranças” são obviamente distintas (SACRAMENTO, 2007).

No primeiro caso estar-se-ia analisando a forma de impedir uma ação direta, a possibilidade de um ou mais indivíduos terem acesso intencional a esse edifício e ao que de valor (humano, material ou de informação) dele possa ser obtido. O segundo caso trata de ações indiretas, sem intervenção intencional humana. Para SACRAMENTO (2007) o primeiro caso refere-se à segurança, que corresponde na língua inglesa o vocábulo *security* e, no segundo, ao vocábulo *safety*.

Desta forma o autor citado anteriormente conclui que s*afety* pode traduzir-se por um conjunto de meios humanos, técnicos e de procedimentos que visa evitar acidentes ou incidentes não originados pela ação humana intencional. Já *security* seria o conjunto de meios humanos, técnicos e de procedimentos que visa evitar acidentes ou incidentes provocados intencionalmente pela ação humana.

2.3. Segurança da Informação

Avançando-se no tempo, já em plena era da informatização, o modelo emblemático das bibliotecas dos mosteiros, citado na Seção 2.2. Segurança, se materializa na figura dos Centros de Processamento de Dados (CPD). Os CPDs eram os prédios que abrigavam os antigos e caros computadores de grande porte (*mainframes*), os quais exigiam um ambiente operacional com muita rigidez no controle da temperatura, umidade, suprimento de energia e acesso físico. Esta estrutura atingiu seu auge na década de 70.

Na FIG.1 é mostrada a sala de operação do CPD do IPEN na sua configuração original (década de 1970). O CPD do IPEN foi construído para abrigar o recém adquirido IBM System/370-155, com 2 megabytes de memória. Na foto é possível identificar o gabinete da CPU do computador ao fundo, e as unidades periféricas enfileiradas à sua frente (fitas, discos e impressoras).

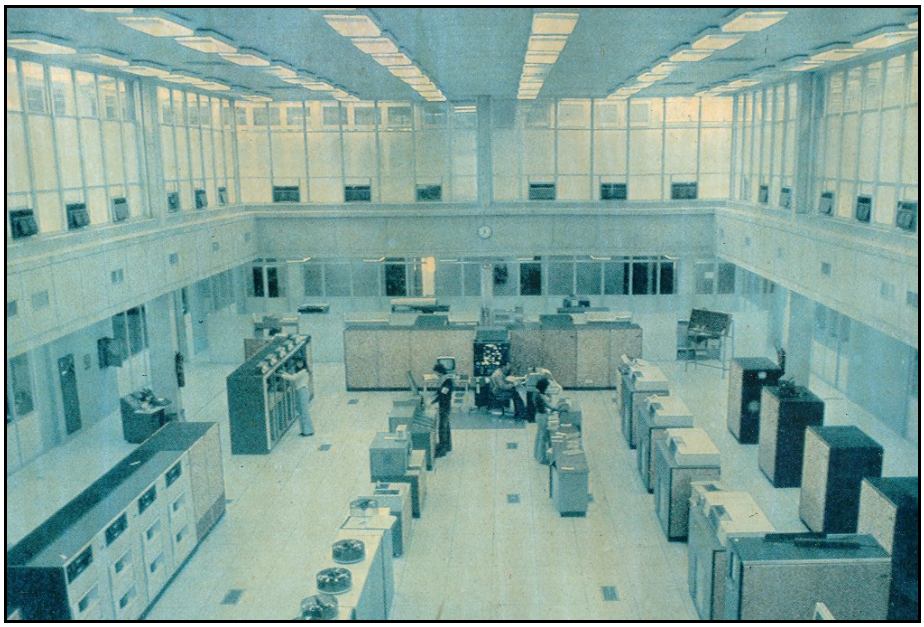


FIGURA 1 - Salão do CPD do IPEN (nos anos 70)
Fonte: Foto do acervo da GRS (digitalizada por Elis de Oliveira Lima Fº)

Este modelo centralizado de processamento de dados entrou em declínio com um movimento de racionalização de recursos chamado *downsizing*, deflagrado nos anos 80.

O termo ***downsizing*** é usado em informática para definir uma situação onde sistemas originalmente hospedados em um computador de grande porte (alta plataforma) são adaptados para mini e microcomputadores (baixa plataforma). Esse processo se deu em função do aumento da capacidade computacional dos microcomputadores e do seu menor custo (BAPTISTA, 1998; p.24).

Dois fatos importantes na evolução da tecnologia da informação foram decisivos para surgimento do processo de *downsizing* e que, conseqüentemente, decretaram o declínio do uso dos *mainframes* em muitas empresas, os quais reinavam absolutos até então: o padrão *Ethernet* e o microcomputador (IBM PC) anunciado em agosto de 1981, de acordo com matéria da revista PC WORLD (2001).

O padrão *Ethernet* foi criado por Bob Metcalfe quando ele trabalhava no *Palo Alto Research Center* (PARC) da *Xerox*, na Califórnia – USA. No dia 22 de maio de 1973, Bob Metcalfe escreveu um memorando descrevendo o sistema de rede *Ethernet* que inventou para a interconexão de estações de trabalho de computadores avançadas, possibilitando o envio de dados entre si e para impressoras a laser de alta velocidade (SPURGEON, 2000; p. 3).

O padrão oficial *Ethernet* é o IEEE 802.3, publicado pelo *Institute of Electrical and Electronics Engineers* (IEEE) em 1985. O IEEE 802.3 define várias opções de meio físico e taxa de transmissão. A especificação 10BASE5, por exemplo, significa que a taxa de transmissão é de 10 Mbps (megabits por segundo), a técnica de sinalização é banda básica, e o comprimento máximo do segmento é de 500 metros (SOARES et al., 1995; p. 213).

O microcomputador (ou computador pessoal) e o padrão *Ethernet* possibilitaram a descentralização da informação, antes confinadas no CPD, para toda a organização através de redes locais de computadores. A revolução do uso de computadores se deu, em grande parte, no uso de redes de locais (LAN), padrão *Ethernet*, que permitiu a comunicação entre computadores.

Os CPDs não acabaram totalmente, muitas empresas ainda utilização computadores de grande porte devido às necessidades das suas operações. Em outras empresas o CPD foi rebatizado de *Datacenter*, onde estão hospedados os equipamentos e servidores da rede corporativa.

Este novo modelo de comunicação, formado pelo uso do padrão *Ethernet* combinado com o aumento explosivo no uso de aplicativos de compartilhamento de informações da *Internet*, como a *World Wide Web* (WWW), fez surgir um mundo totalmente novo de tecnologia de comunicação (SPURGEON, 2000; p. 4).

A História da *Internet* começou na década de 50 no auge da “guerra fria”, quando o Departamento de Defesa dos Estados Unidos (DOD) estudava o desenvolvimento de uma rede que pudesse sobreviver a uma guerra nuclear. Na época todas as comunicações militares usavam a rede pública de telefonia considerada vulnerável.

Em dezembro de 1969, a ARPANET (*Advanced Research Projects Agency Network*) foi colocada no ar com quatro pontos de conexão, UCLA (Universidade da Califórnia, Los Angeles), UCSB (Universidade da Califórnia,

Santa Barbara), SRI (*Stanford Research Institute*) e a Universidade de Utah (TANENBAUM, 2003; p. 50-53).

No Brasil, a *Internet* chegou em 1988 por iniciativa da comunidade acadêmica de São Paulo, através da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e do Rio de Janeiro, pela Universidade Federal do Rio de Janeiro (UFRJ) e Laboratório Nacional de Computação Científica (LNCC). A *Internet* no Brasil permaneceu com uso exclusivo pela comunidade acadêmica até 1995, quando passou a ser explorada comercialmente (CYCLADES, 2002).

Maiores informações sobre o funcionamento e a tecnologia usada em redes locais / *Ethernet* e *Internet* fogem do escopo deste trabalho.

A descentralização da informação no cenário corporativo atual, em virtude da utilização maciça das redes locais e da *Internet*, além das novas tecnologias (Wi-Fi e computação móvel, entre outras), trouxe novos desafios para a proteção da informação, e dos sistemas de informação em geral, essencial para o negócio da organização.

É neste cenário de descentralização e democratização da informação, aliada a necessidade imperiosa de conectividade das organizações, que surge uma nova forma de proteção de informações com robustez e resistência nunca antes vista. Esta verdadeira fortaleza dos tempos modernos atende pelo nome de “salas-cofre”.

As salas-cofre são ambientes de alta tecnologia projetados para resistir a vários tipos de catástrofes. Suportam, por exemplo, temperaturas de até 1.200 graus Celsius, inundações, cortes bruscos de energia, gases corrosivos, explosões e até ataques nucleares (NUNES, 2003).

A segurança física ou perimetral é apenas uma das inúmeras formas de se preservar informações. Levando em consideração apenas os mecanismos de segurança física é possível encontrar uma gama de controles de segurança que podem ser aplicados. Estes controles podem variar da utilização de uma recepcionista até controles sofisticados e caros como as salas-cofre.

A escolha sobre qual tipo de controle usar vai depender da criticidade da informação para o negócio e dos seus requerimentos de segurança.

A segurança física perimetral é contemplada na seção 9 da Norma ABNT NBR ISO/IEC 27002:2005. O controle de segurança 9.1.1 – Perímetro de segurança física é estabelecido, na referida Norma, da seguinte maneira:

> *“Convém que sejam utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e instalações de processamento da informação”.*

A segurança da informação (INFOSEC - *Information Security*) visa à aplicação de medidas de segurança para proteção da informação processada, armazenada ou transmitida nos sistemas de informação e comunicações, sejam sistemas eletrônicos ou não, para prevenir a perda de confidencialidade, integridade ou disponibilidade (SACRAMENTO, 2007).

Pode-se dizer que a preocupação com a segurança da informação teve início na antiguidade, com o surgimento da escrita, sobretudo no que se refere ao aspecto da confidencialidade da informação. Com o crescimento do número de pessoas com a habilidade de ler e escrever por meio de símbolos, logo percebeu-se a necessidade de duas pessoas poderem trocar informações sem que outras pudessem lê-las.

Na antiga Grécia, os generais do exército de Esparta utilizavam formas criptográficas para enviarem informações secretas para as tropas na frente de batalha. A mensagem era escrita em uma fita de papiro estreita e cumprida, enrolada em espiral em um bastão de madeira chamado “scytale”. Após a mensagem ser escrita a fita era desenrolada tornando a mensagem incompreensível. Só poderei ler a mensagem corretamente quem possuísse um “scytale” com o formato igual àquele utilizado no momento em que a mensagem foi escrita (GARFINKEL & SPAFFORD, 1996; p. 139).

Por volta do ano de 50 A.C, Julius Caeser, líder militar e político romano, criou um modelo de *cifragem* de mensagens para prevenir que suas mensagens fossem lidas (compreendidas) pelos inimigos. O modelo consistia em deslocar as letras do alfabeto três posições à frente, ou seja, a letra A passaria a ser codificada como D, a letra B como E, e assim sucessivamente. Este modelo ficou conhecido como “Caesar cipher” (KRUTZ & VINES, 2003; p. 181).

Quando uma nova técnica de gravação, armazenamento ou transmissão de informações é desenvolvida, quase sempre é seguida por métodos que tentam se aproveitar de possíveis falhas da nova tecnologia. Em ontrapartida, mecanismos de proteção das informações processadas também são implementados.

A seguir são dados alguns exemplos ocorridos ao longo da história onde esta situação pode ser observada (RUSSELL & GANGEMI, 1991; p. 24):

1. a introdução do telégrafo de Samuel F. B. Morse, em 1844, trouxe preocupações com a confidencialidade das informações transmitidas. No ano seguinte um código de *encriptação* foi desenvolvido para manter o sigilo das mensagens transmitidas;
2. em 1881, cinco anos após a introdução do telefone foi depositada uma patente de um misturador de voz (*scrambler*);
3. na década de 1920 nos Estados Unidos, o uso de “grampos” telefônicos por parte de forças governamentais e organizações criminosas resultou em grande clamor público, o que levou a criação de legislação proibindo tal prática;
4. nos anos 40, preocupações em controlar a proliferação de informações sobre energia atômica levaram à criação da lei da energia atômica de 1946. Esta lei criava uma categoria de dados restritos que requeriam proteção especial e penalidade pela disseminação de tais informações. Controles similares foram impostos a novos avanços em outras áreas científicas.

Mais recentemente tem-se o exemplo da “Sarbanes-Oxley Act (SOX)” (USA, 2002b), lei Americana de 2002, criada para restabelecer a confiança do mercado de capitais, após os escândalos contábeis e financeiros envolvendo grandes companhias, tais como, Enron, WorldCom e Arthue Andersen (PEIXOTO, 2004).

BYRUM (2004) recomenda para as empresas que estão sujeitas às exigências da *SOX*, ou seja, companhias de capital aberto e suas subsidiárias cujas ações são negociadas nas Bolsas de valores Americanas, especial atenção aos controles que atuam na segurança da rede corporativa. Inclui-se aí a prevenção do acesso desautorizado aos sistemas e dados e a proteção da integridade e disponibilidade em caso de desastre ou outros tipos de interrupção de serviço.

PEIXOTO (2004) adverte que, no tocante à segurança de sistemas de informação, a adequação à “Sarbanes-Oxley” deve se dar em todos os recursos concernentes as informações financeiras. Isto Inclui os sistemas de gestão empresarial (*Enterprise Resource Planning* – ERP), aplicativos contábeis, sistemas de relacionamento com clientes (*Customer Relationship Management* –

CRM), sistemas de gerenciamento da cadeia de suprimentos (*Supply Chain Management*), bem como nas demais aplicações de comunicação, banco de dados e armazenamento de informações.

Proteção de comunicações tem sido particularmente crítico em tempos de guerras e de conflitos políticos. O desenvolvimento de métodos criptográficos modernos (e outros formas de proteção) está relacionado em grande parte a pesquisas conduzidas sob a pressão da segunda guerra mundial. Um bom exemplo é a máquina Enigma, dispositivo de criptografia, utilizado pelos Alemães (RUSSELL & GANGEMI, 1991; p. 167).

O rápido crescimento e disseminação do processamento eletrônico de dados e comércio eletrônico, a partir do final do século XX, com o uso da *Internet*, cominando com inúmeras ocorrências de terrorismo internacional, fomentou a necessidade de melhorar os métodos de proteção dos computadores e das informações neles armazenadas, processadas e transmitidas.

Talvez pelo fato da palavra ‘segurança’ estar historicamente relacionada com o setor militar, quase sempre vinculada à idéia de reprimir, vigiar e espionar, as iniciativas de segurança da informação dentro das organizações sejam vistas com certo temor pela comunidade de usuários.

Este é um ponto que deve ser tratado com muito cuidado e atenção pelos responsáveis pela introdução de um programa de segurança da informação. Não se deve ignorar os aspectos humanos e sociais num processo de mudança desta grandeza (como mostram as Seções 2.4. Aspectos humanos da informação e 2.5. Fator humano na segurança da informação). Pois a despeito da sofisticação tecnológica disponível, a informação é, e sempre será, um bem a serviço de pessoas – no processo de tomada de decisões ou como insumo para as suas atividades diárias.

Segurança da Informação significa proteger a informação e os sistemas de informação de acesso desautorizado, uso, revelação, modificação ou destruição a fim de garantir a sua confidencialidade, integridade e disponibilidade (USA, 2002a; WIKIPEDIA, 2007):

- Confidencialidade

  Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

- Integridade

  O conceito de integridade está associado ao estado da informação no momento de sua geração e de seu resgate. Ela estará íntegra se em tempo de resgate estiver fiel ao estado original;

- Disponibilidade

  Garantia de que os usuários autorizados tenham acesso à informação e aos sistemas correspondentes sempre que necessitarem deles.

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.

HORTON & MUGGE concluem dizendo que é preciso que as empresas compreendam e avaliem a importância de cada objetivo e apliquem mecanismos de proteção corretos para proteger os dados usando como elementos-chave pessoas, processos e tecnologia.

Para HAAR & SOLMS (2003) são as propriedades de uma organização que determinam quais são suas metas e seus níveis da segurança.

O modelo proposto por HAAR & SOLMS chamado de “Perfis de Atributo de Controle de Segurança da Informação” possui três elementos básicos:

- propriedades da organização, tais como a natureza do negócio, propósito, ambiente, cultura e investimento;
- níveis e metas da segurança da informação, tais como confidencialidade, integridade, disponibilidade, responsabilidade e autenticidade; e
- atributos de controle, como auditoria, planos de recuperação de desastres, treinamento e conscientização.

ZHANG & YANG (2002), por sua vez, acreditam que é o fluxo da informação que determina sua segurança. Para estes autores, analisando-se o

fluxo da informação ocasionado pela execução das operações fontes é possível determinar se aquele fluxo viola uma determinada política de segurança.

SOLMS & SOLMS (2004) apresentam 10 importantes aspectos, que eles chamam de “Os 10 pecados mortais da segurança da informação”, os quais costumeiramente conduzem ao fracasso a implementação de um plano de segurança da informação:

1. não perceber que segurança da informação é uma responsabilidade de governança corporativa;
2. não perceber que segurança da informação é uma questão de negócio e não uma questão técnica;
3. não perceber que a governança de segurança da informação é uma disciplina multidimensional (complexa), e que não existe uma solução pronta e/ou milagrosa que vá resolver o problema;
4. não perceber que um plano de segurança da informação deve está baseado na identificação de riscos;
5. não perceber (e utilizar) a importância das melhores práticas internacionais para a gestão da segurança da informação;
6. não perceber que a política corporativa de segurança da informação é absolutamente essencial;
7. não perceber que o cumprimento das normas e o monitoramento das mesmas são absolutamente essenciais em segurança da informação;
8. não perceber que uma estrutura organizacional adequada de governança da segurança da informação é absolutamente essencial;
9. não perceber a importância da conscientização dos usuários em segurança da informação; e
10. não disponibilizar aos gestores da segurança da informação infraestrutura, ferramentas e mecanismos de suporte adequados para o desempenho de suas responsabilidades.

A informação é um ativo valioso para a organização realizar suas operações, e como qualquer outro ativo importante (financeiro, material e humano) precisa ser protegido. Contudo, o grau de proteção mais adequado para cada um dos princípios da segurança depende da exigência do negócio (vide Seção 2.11. Processos de trabalho).

É importante salientar que qualquer medida de segurança da informação só deverá ser implementada quando efetivamente agregar valor ao negócio. Ou seja, a segurança não pode ser um fim em si mesma. Ela deve ser aplicada para o sucesso da organização.

2.3.1. Trabalhos Relacionados

Na TAB.3, a seguir, apresenta-se um comparativo entre trabalhos acadêmicos realizados no campo da segurança da informação, relacionando-os com a presente pesquisa.

TABELA 3 - Trabalhos relacionados

Autor	Título	Objetivo	Foco
MARCIANO (2006)	Segurança da Informação - uma abordagem social. Doutorado. UNB.	Apontar estratégias alternativas para a elaboração de políticas de segurança.	Abordagem social, de caráter humanista, centrada nos pontos de vista do usuário.
BERNARDES (2005)	Modelagem de governança da Segurança da Informação com apoio em sistemas de informação. Doutorado. USP - São Carlos.	Segurança da informação utilizando informações de sistemas de TI, coletadas em nível operacional.	Segurança computacional / infra-estrutura
VENTURINI (2006)	Modelo Ontológico de Segurança para Negociações de Políticas de Controle de Acesso em Multidomínios. Doutorado. POLI/USP	Política de Controle de acesso	Autenticação e autorização.
GARCIA (2005)	O modelo de Planejamento Estratégico de TI em Empresas Globais. Mestrado. UFSC.	Alinhamento de TI aos objetivos estratégicos da empresa.	Planejamento Estratégico de TI
TRABALHO PROPOSTO	Gestão da Segurança da Informação – Uma proposta para potencializar a efetividade de segurança da informação em ambiente de pesquisa científica.	Segurança da informação, de forma estruturada, como prática gerencial.	Efetividade das práticas de segurança considerando pessoas, processos e tecnologia.

Fonte: do Autor

Neste comparativo verificou-se, por exemplo, que o trabalho de MARCIANO (2006) faz uma abordagem social da segurança da informação, apontando estratégias alternativas para a elaboração das políticas de segurança.

Em contrapartida a tese de doutorado de BERNARDES (2005) tem seu foco voltado aos aspectos tecnológicos da segurança. O referido trabalho propõe

um modelo de segurança baseado em informações coletadas nos registros de *log* dos sistemas computacionais e de infraestrutura.

Já VENTURINI (2006) discute especificamente questões ligadas ao controle de acesso (autenticação e autorização), enquanto GARCIA (2005) focaliza seu trabalho no planejamento estratégico de TI.

Diferente dos trabalhos mencionados acima, o presente trabalho analisa a segurança da informação de maneira mais ampla, levando em consideração seus aspectos tecnológicos, não-tecnológicos e administrativos. Este tem como ponto primordial a elaboração da estratégia da segurança da informação na organização, elevando a gestão da segurança da informação para o nível estratégico, como prática de governança corporativa.

2.3.2. Segurança da Informação em Pesquisa Cientifica

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 analisada é possível afirmar que, na maioria dos casos, a disponibilidade e a integridade o serão.

Como citado anteriormente, a segurança da informação tem como objetivo principal preservar a confidencialidade, integridade e disponibilidade da

informação. 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 organização.

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., p. 23).

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, como será visto na subseção 2.13.1. Análise e avaliação de risco, 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 as manutenções da página;
- sistema de *backup*;
- antivírus; e
- prevenção contra *Hacking* (métodos e técnicas utilizadas pelos *hackers*).

De modo geral as aplicações *Web* estão sendo usadas para melhorar a interação com o cliente e aumentar a funcionalidade do negócio nas organizações. O uso de serviços de aplicações disponíveis pela *Internet* tem trazido visibilidade para as empresas e aumentado as suas oportunidade de negócio, mas, ao mesmo tempo, também tem trazido outros perigos para a empresa. Esta maior exposição cria novos caminhos através dos quais um usuário mal-intencionado pode atacar um sistema e a empresa (HORTON & MUGGE, 2004; p. 134).

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

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"*.

Os incidentes de segurança envolvendo aplicações *Web* constituem uma ameaça real em ambiente de pesquisa científica, prova disto são os incidentes ocorridos em 04 de novembro de 2008 e 09 de fevereiro de 2009, conforme constado na TAB.1.

Segundo dados do TCU/SEFTI, 76% dos órgãos públicos da Administração Federal prestam serviços pela *Internet* com troca bidirecional de informações entre o órgão/entidade e seus clientes (TCU, 2008; p. 22).

Ainda segundo o TCU, os sistemas *Web* desses órgãos apresentam um risco inerente relacionado à maior exposição a ações indevidas que podem afetar a integridade, a disponibilidade e a confidencialidade das informações por eles tratadas. E acrescenta: *"Esse risco é aumentado na presença de controles fracos que afetem diretamente esses sistemas, como é o caso da ausência de metodologia para desenvolvimento de sistemas ou deficiências nos controles de segurança da informação"*.

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

Vide seção 2.8. Tipos de Ataque para uma melhor explicação de como os ataques às aplicações *Web* acontecem.

Perguntado se “numa empresa de cientistas, a gestão de rede é diferente”, André Luis Carvalho, líder de aplicativos e banco de dados da *Du Pont* do Brasil, em entrevista à INFORMÁTICA HOJE (2009), disse: *“Nossas informações mais críticas, informações de pesquisa e desenvolvimento, ficam numa rede à parte: temos uma rede particular só para os PhDs [doutores e cientistas], o que não é comum”*.

2.4. Aspectos Humanos da Informação

Um erro bastante comum cometido em muitas organizações, e que freqüentemente conduz ao fracasso de todo um esforço para implementar um programa de segurança da informação, é não levar em consideração os aspectos sociais / humanos envolvidos nesta tarefa.

As práticas de segurança da informação são implementadas através de um conjunto de medidas (tecnológicas, não tecnológicas e administrativas) apoiado por políticas de segurança da informação, que abrangem todas as áreas da estrutura organizacional.

DAVENPORT (2000, p. 11) afirma que *“nosso fascínio pela tecnologia nos fez esquecer o objetivo principal da informação: informar”*. E acrescenta, *“Todos os computadores do mundo de nada servirão se seus usuários não tiverem interessados nas informações que esses computadores podem gerar”.*

A “ecologia da informação” de Davenport enfatiza o ambiente da informação em sua totalidade, ou seja, como um inter-relacionamento entre **pessoas, cultura, processos de negócios, política e tecnologia**. Ela se baseia na maneira como as pessoas criam, distribuem, compreendem e usam a informação, em oposição à abordagem comumente aceita para o gerenciamento de informações por meio de investimentos em novas tecnologias (o que o citado autor chama de abordagem da *‘engenharia da máquina’*). Esta prática, por conseguinte, acaba influenciando a gestão da segurança da informação em muitas organizações.

A abordagem da “ecologia da informação” também pode ser descrita como uma administração holística da informação ou administração informacional centrada no ser humano. Para Davenport *“O ponto essencial é que essa*

abordagem devolve o homem ao centro do mundo da informação, banindo a tecnologia para seu devido lugar, na periferia" (DAVENPORT, 2000; p. 21).

Poder-se-ia então falar em *"**gestão ecológica da segurança da informação**"*, em alusão à abordagem de Davenport.

FONTES & BALLONI (2006) defendem um modelo de segurança da informação que contemple os aspectos técnico-sociais do ambiente organizacional. Esta perspectiva técnico-social procura levar em consideração tanto os aspectos diretamente relacionados com os recursos tecnológicos, quanto àqueles relativos às pessoas e ao ambiente onde elas vivem ou trabalham, tais como: regulamentos, cultura e ambiente organizacional, processo continuo de treinamento e profissionalismo.

As políticas de segurança da informação são apresentadas na forma de guia de conduta ao qual os usuários dos sistemas de informação devem se adequar integralmente (MARCIANO & MARQUES, 2006). Para que essas políticas sejam efetivamente legítimas e que as pessoas as incorporem nas suas atividades do dia-a-dia é necessário o envolvimento e a participação de toda a comunidade de usuários desde o início do processo de discussão e elaboração das mesmas.

Outro ponto que merece atenção é a total transparência que deve ser adotada, de tal forma que não se deixe nenhum tipo de dúvida, quanto aos motivos e objetivos das medidas de segurança a serem adotadas.

Sem uma boa receptividade por parte da comunidade de usuários as medidas segurança serão rechaçadas, criando um ambiente de desconfiança e intranqüilidade que irá comprometer todo trabalho planejado.

MARCIANO & MARQUES (2006) propõem que, antes de apresentar-se um elemento de perturbação de uma ordem vigente (mesmo que caótica), analisem-se os indivíduos e as interações existentes.

Observa-se que as organizações, via de regra, implementam políticas totalmente desarticuladas do ambiente organizacional, sem qualquer preocupação com o nível de aceitação destas pelos usuários e sem um programa adequado de esclarecimento e conscientização. Este tipo de ambiente fará com que o usuário crie meios para burlar as normas. O descumprimento das regras e a falta de integração entre as áreas de segurança e de negócio é um dos principais fatores para o fracasso de um programa de segurança da informação.

PEMBLE (2004 apud MARCIANO & MARQUES, 2006; p. 6) sugere que a segurança da informação deve ser definida em termos das atribuições do profissional responsável por ela (proprietário e custodiante).

O autor supracitado descreve três esferas de atuação de tais profissionais em torno das quais a segurança deveria ser parametrizada e compreendida:

1) A esfera operacional, onde o impacto de um incidente pode comprometer a capacidade da organização de sustentar os processos do negócio;
2) A esfera da reputação, referente ao impacto que os incidentes têm sobre o valor da "marca" ou sobre o valor acionário; e
3) A esfera financeira, os custos em que se incorre na eventualidade de algum incidente.

A definição para ***sistema de informação*** e ***usuário,*** feita por MARCIANO & MARQUES (2006; p. 7), deixa bastante clara a importância do elemento humano dentro deste contexto, que não pode ser subjugado no processo de implementação da segurança:

> *"Um sistema de informações é composto pela somatória do sistema social no qual ele se apresenta, compreendendo os usuários e suas interações entre si e com o próprio sistema, e do complexo tecnológico sobre o qual estas interações se sustentam"; e*
>
> *"O usuário de um sistema de informação é o indivíduo para o qual se concretiza o fenômeno do conhecimento mediante as informações providas por aquele sistema".*

Percebe-se, a partir do exposto, que como a informação, todo aparato tecnológico que dá suporte a ela (sistemas de informação, infraestrutura de comunicação, e também sua segurança) está a serviço do usuário que faz uso dela para exercer suas funções dentro do propósito maior da organização - cumprir sua missão. A informação, incluindo os sistemas relacionados a ela, está a serviço do usuário, e não o contrário.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE), preocupada com o tema segurança estabeleceu uma guia com nove princípios para promover o que ela chama de "cultura de segurança".

A OCDE compreende a importância da manutenção da segurança dos sistemas de informação e das redes de computador que hoje dão suporte a uma gama de infraestruturas críticas, tais como energia, transporte e financeiro; bem

como para as companhias realizarem seus negócios, governos fornecerem serviços aos cidadãos e empresas, e para a comunicação e troca de informação entre indivíduos.

O guia OECD (2002) foi concebido para aplicação por todos os participantes da nova sociedade da informação e sugere a necessidade de um maior entendimento e conscientização das questões relativas à segurança e do desenvolvimento de uma “cultura de segurança”.

Para a OCDE a promoção da cultura de segurança requer liderança e ampla participação, e deve resultar em maior prioridade para o planejamento e administração de segurança, bem como um entendimento maior da necessidade de segurança entre todos os participantes (desenvolvedor, proprietário, provedor, administrador de serviços e usuários).

Os nove princípios da OCDE são:

1) Princípio da conscientização

   Todos os participantes devem estar cientes da necessidade de segurança para os sistemas de informação e redes, e o que cada um pode fazer para melhorá-la. A conscientização dos riscos e das salvaguardas disponíveis é a primeira linha de defesa para a segurança;

2) Princípio da responsabilidade

   Todos os participantes são responsáveis pela segurança dos sistemas de informação e redes. Os participantes devem rever regularmente suas próprias políticas, práticas e procedimentos e avaliar se elas são (e continuam sendo) apropriadas para seu ambiente;

3) Princípio responsivo (resposta, reação)

   Os participantes devem agir em tempo hábil e de maneira cooperativa para prevenir, detectar e responder aos incidentes de segurança. Eles devem compartilhar informações sobre ameaças e vulnerabilidades de forma apropriada, e implementarem procedimentos para uma rápida e efetiva cooperação, visando prevenir, detectar e responder aos incidentes de segurança;

4) Princípio ético

   Cada participante deve respeitar o interesse legítimo dos outros. Dada a penetrabilidade dos sistemas de informação e redes em nossa sociedade, os

participantes precisam reconhecer que sua ação ou omissão pode prejudicar outras pessoas;

5) Princípio da democracia

   A segurança de sistemas de informação e de redes deve ser compatível com os valores essenciais de uma sociedade democrática. A segurança deve estar de acordo com os valores reconhecidos pelas sociedades democráticas incluindo a liberdade de idéias e pensamentos, o livre fluxo de informação, a confidencialidade da informação e comunicação, a proteção das informações pessoais, franqueza e transparência;

6) Princípio da avaliação de risco

   Os participantes devem conduzir avaliações de risco. Avaliação de risco permite determinar o nível aceitável do risco e auxilia na seleção de controles apropriados para o gerenciamento do risco;

7) Princípio do projeto e implementação da segurança

   Os participantes devem incorporar a segurança como um elemento essencial dos sistemas de informação e redes. Sistemas, redes e políticas precisam ser adequadamente projetados, implementadas e coordenadas para otimizar a segurança;

8) Princípio do gerenciamento da segurança

   Os participantes devem adotar uma abordagem ampla para a gestão da segurança. A gestão da segurança deve ser baseada em avaliação de risco e deve ser dinâmica, abrangendo todos os níveis de atividades dos participantes e todos os aspectos de suas operações;

9) Princípio da reavaliação

   Os participantes devem rever e reavaliar a segurança dos sistemas de informação e redes, e promoverem as modificações necessárias nas políticas, práticas, medidas e procedimentos de segurança.

Embora os princípios da OCDE reiteradamente refiram-se à segurança de sistemas de informação e redes (aspectos tecnológicos), estes devem ser estendidos para as demais formas de apresentação da informação, tais como falada em conversas informais ou escrita em papel.

Segurança da informação é uma questão relacionada com aspectos sociais e humanos, portanto, para se ter sucesso na sua gestão deve-se conciliar tais conceitos às soluções adotadas, sejam elas tecnologias ou administrativas.

2.5. Fator Humano na Segurança da Informação

> *"Apenas duas coisas são infinitas: o universo e a estupidez humana. E não estou muito seguro a respeito do universo".* Albert Einstein.[3]

É ponto recorrente dizer que o usuário é o elo fraco da segurança da informação. Antes de tudo não se deve esquecer que os sistemas, aplicativos e produtos de *software* são criados para pessoas (TIPTON & KRAUSE, 2003, p. 239).

Quando o UNIVAC - Universal Automatic Computer, primeiro computado comercial da história foi utilizado na previsão da eleição presidencial dos Estados Unidos em 1952, os operadores da máquina recusaram-se a aceitar o resultado, que dava uma vitória esmagadora ao candidato Dwight David Eisenhower. Eles então reprogramaram o computador para produzir um resultado diferente. Contudo, o resultado das urnas confirmou o que a pesquisa de intenção de votos apontava, a vitória do Senhor Eisenhower. Isto causou algumas declarações de que "o problema com as máquinas eram as pessoas" (BOSWORTH & KABAY, 2002; p. 29.4).

Muitas organizações ignoram as questões sociais e comportamentais em seus programas de segurança da informação. É um erro imaginar que os aspectos humanos sejam menos importantes, e que o estabelecimento de políticas e a aplicação de controles técnicos sejam suficientes para garantir um ambiente seguro.

HUEBNER & BRITT (2006) analisam a segurança da informação do ponto de vista dos aspectos sócio-comportamentais utilizando a teoria da estruturação desenvolvida pelo sociólogo inglês Anthony Giddens, pesquisador da natureza das situações sociais.

---

[3] http://www.frases.mensagens.nom.br/frases-autor-a-alberteinstein.html

2.6. Teoria da Estruturação

A teoria da estruturação tem uma perspectiva balanceada em dois extremos: ação (*agency*) e estrutura. Ela tenta balancear os dois extremos por meio de forças sociais (sociedade) ou formas e aspectos individuais de nossa realidade social (GIDDENS, 1984 apud HUEBNER & BRITT, 2006).

Estruturação é a interação do agente (individualmente ou em grupo) com a estrutura. Esta interação é recursiva, com um influenciando o outro. Estruturação não é uma série de eventos distintos, mas ajuda a observar mudanças no decorrer do tempo. Estrutura são as regras, procedimentos, e normas que governam o comportamento.

Numa empresa uma estrutura óbvia é a sua própria estrutura organizacional. Isto é, a representação do relacionamento entre os empregados. Outro exemplo de estrutura é a política. Os funcionários primeiramente criam as políticas organizacionais, que estabelecem quais são os comportamentos esperados das pessoas. Outra estrutura é a cultura organizacional. Cultura, em termos da teoria da estruturação, emerge através de uma série de interações complexas entre empregados e outras estruturas.

Na teoria da estruturação, três grandes estruturas emergem em um contexto social específico. São elas: estruturas de significação, dominação e legitimação.

Na FIG.2 é mostrado o relacionamento dessas três estruturas. A estrutura da significação produz entendimento compartilhado entre as pessoas em um dado contexto - **comunicação**. A estrutura da dominação refere-se à produção e uso do **poder** (força), que tem origem no controle de recursos. E, finalmente, estrutura da legitimação refere-se aos diretos, obrigações, **normas** e regras que orientam a conduta das pessoas, e também às sanções aplicáveis quando do não cumprimento das normais, ou seja, quando ocorrem os chamados comportamentos indesejados (HUEBNER & BRITT, 2006).

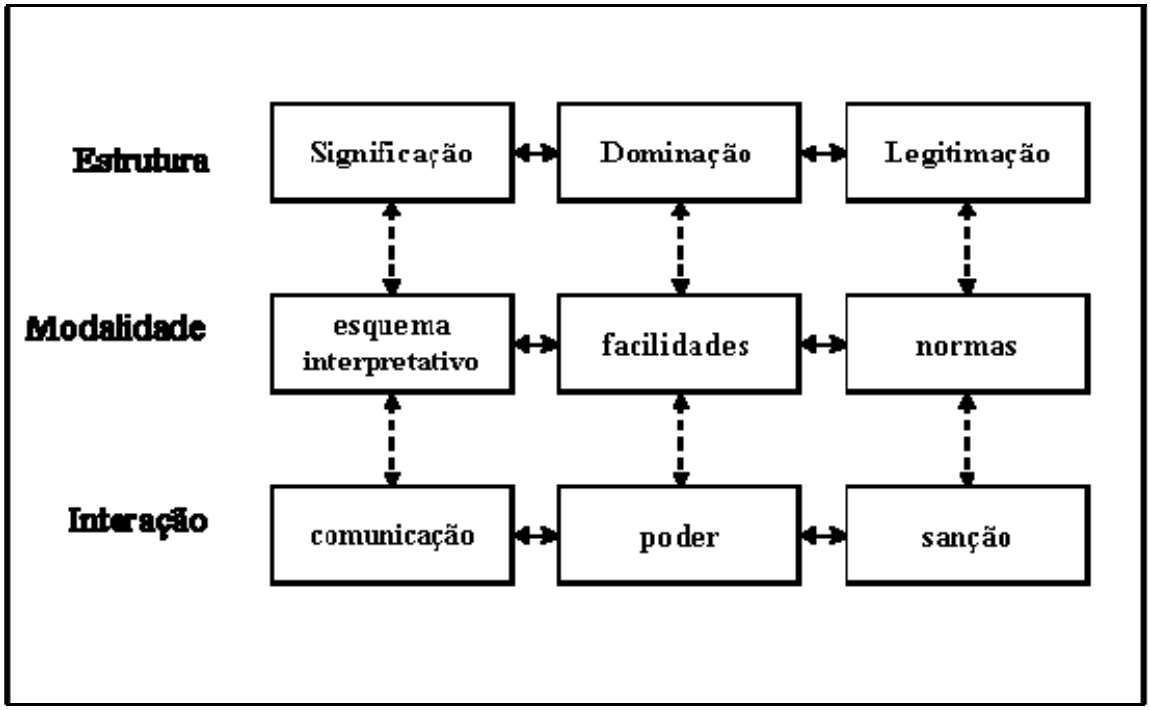


FIGURA 2 - Dimensão da dualidade da estrutura
Fonte: Giddens (2003, p. 23). A constituição da sociedade.

2.6.1. Relacionando Segurança com Estruturação

Sob a perspectiva da segurança, comportamentos indesejados incluem compartilhamento de senhas, revelação de informações restritas, e compartilhamento de segredos de negócio com estranhos.

Na concepção de GIDDENS (1984), a relação tempo e espaço com a ação humana simboliza a dinâmica da vida social. Segundo palavras do referido autor *"é na conduta cotidiana das pessoas que se moldam e se transformam as sociedades humanas"* (ASENSI, 2006).

Analisar-se-á cada uma das estruturas da teoria de Giddens sob o ponto de vista da segurança da informação (HUEBNER & BRITT, 2006):

Estruturas de significação

Estrutura de significação refere-se a entendimentos compartilhados dentro de um grupo. Também pode ser chamada de cultura organizacional. Em termos de segurança significa que todos os empregados devem ter um amplo e compartilhado entendimento sobre as práticas de segurança.

Um problema bastante comum nas organizações é que os funcionários não têm um entendimento geral das questões relativas à segurança. Isto acontece simplesmente porque eles não receberam nenhum treinamento no assunto.

Programas de treinamento e conscientização (vide Seção 2.9 – Programa de treinamento e conscientização) devem fazer parte obrigatória do plano de segurança. O que pode acontecer quando os empregados não têm um treinamento adequado em segurança? O fato em si já demonstra a existência de uma vulnerabilidade, por meio da qual os empregados podem ter comportamentos indesejados, como por exemplo, fornecer informações por telefone sem verificar a identidade do solicitante. Os empregados devem estar cientes que este tipo de comportamento compromete a segurança da empresa.

Estruturas de dominação

Estruturas de dominação são os mais diversos recursos que os funcionários se utilizam para exercer poder (força). Portanto, recomenda-se que os gerentes e o pessoal de segurança utilizem a estrutura de dominação para controlar o acesso aos recursos de informação. O controle de acesso pode ser físico ou lógico, ou ainda uma combinação de ambos.

Usando o poder que lhe foi conferido, por meio de instrumento administrativo legal e com o comprometimento da alta direção, o departamento de segurança (*Security Office*) pode exigir mudança de comportamento dos empregados.

Deve-se observar as constantes mudanças que ocorrem nas estruturas e como a segurança é afetada por elas. É através da interação que ocorre entre os agentes humanos, que novos sistemas de informação são criados. Estes novos sistemas de informação são vistos como estruturas adicionais dentro da organização. Desta maneira, conclui-se que sistemas afetam o comportamento das pessoas. Em um contexto organizacional, sistemas de informação tanto habilitam como reprimem comportamentos das pessoas.

Estruturas de legitimação

Estruturas de legitimação são direitos, normas e regras que guiam comportamentos. São códigos de conduta, os quais se espera que sejam seguidos pelos funcionários.

Cada organização estabelece determinadas expectativas de seus funcionários definindo padrões e políticas que devem ser seguidas. Estas por sua vez, podem constranger ou habilitar determinados comportamentos por parte dos funcionários.

Em termos de segurança todos devem respeitar as regras, normas e obrigações para que a organização torna-se mais segura. A melhoria da segurança requer esforço não só do pessoal técnico da área de segurança, mas também que todos na companhia sigam as medidas de comportamentos estabelecidas.

Teoria da estruturação pode ser usada para ajudar na análise de mudanças que ocorram após a implantação de uma nova política ou após a realização de um treinamento de conscientização em segurança.

Adicionalmente pode-se considerar o surgimento de novas estruturas a partir de mudanças em estruturas ou agentes existentes. A simples contratação de um novo colaborador pode alterar uma estrutura pré-existente o suficiente para que possa ser observada. Aqui vale a máxima: se X mudou e Y mudou, por que Z não poderia mudar?

Os gerentes e as lideranças poderiam considerar as seguintes questões:

1. Existe na organização algum setor que cuida dos fatores de risco relativo ao comportamento humano, tais como o setor de RH ou gestão de risco?
2. A administração tem um plano para lidar com as questões humanas e os fatores de risco associados, tal como programa de treinamento?

2.7. Entendendo Como os Atacantes Aproveitam-se da Natureza Humana

Segundo CIALDINI (2001) a manipulação de pessoas tem sido estudada há mais de 50 anos, tendo sido intensificada apartir dos programas de propaganda e persuasão utilizados na segunda guerra mundial. O referido autor resumiu a sua pesquisa apresentando “seis tendências básicas da natureza humana”, as quais estão envolvidas na tentativa de se obter uma resposta positiva (desejada) mediante uma solicitação feita.

Essas seis tendências são freqüentemente usadas pelos *“engenheiros sociais”* (consciente ou inconscientemente) em suas tentativas de manipulação de pessoas (MITNICK & SIMON, 2003; p.196).

1) Autoridade

As pessoas têm a tendência de atender uma solicitação que é feita por alguém com autoridade, ou que se pensa que ele a tenha. Uma pessoa pode ser

convencida a atender a uma solicitação se ela acreditar que o solicitante é uma pessoa com autoridade ou que está autorizada a fazer tal solicitação.

Exemplo de ataque de autoridade:

Um engenheiro social tenta impor autoridade alegando ser do departamento de TI ou dizendo ser um executivo ou uma pessoa que trabalha para um executivo da empresa.

Em seu livro “influence”, o Dr. Cialdini (CIALDINI, 2000 apud MITNICK & SIMON, 2003; p. 196) escreve um estudo sobre três hospitais dos Estados Unidos, nos quais 22 estações de enfermagem foram contatadas por um interlocutor que dizia ser um médico do hospital e receberam instruções para administrar uma droga controlada para um paciente naquela ala. As enfermeiras que recebem essas instruções não conheciam o interlocutor. Elas nem mesmo sabiam se ele era realmente um médico (e ele não era).

Elas receberam as instruções pelo telefone, o que violava a política do hospital. O “médico” disse para elas administrarem uma droga cujo uso não era autorizado naquela ala, e em dosagem duas vezes maior que a máxima diária permitida, podendo assim colocar a vida do paciente em risco.

Mesmo infringindo todos essas normas, em 95% dos casos a enfermeira obteve a dosagem necessária na sala de medicamentos e estava indo administrá-la ao paciente, antes de ser interceptada por um observador que lhe contou sobre a experiência.

2) Afabilidade

As pessoas têm a tendência de atender um pedido feito por alguém quando este se faz passar por uma pessoa agradável ou com interesses, crenças e atitudes semelhantes aos da vítima.

Exemplo de ataque de afabilidade:

Por meio de uma forma qualquer (conversa e *internet*, entre outras.), o atacante consegue descobrir um *hobby* ou um interesse da vítima e diz também ser interessado ou entusiasmado por aquele determinado assunto. Ou então alega ser do mesmo estado ou escola ou ter objetivos semelhantes.

O engenheiro social também tenta imitar os comportamentos do seu alvo para criar a aparência de semelhança.

3) Reciprocidade

As pessoas costumam atender automaticamente uma solicitação, quando recebem ou têm a promessa de receber algo de valor. O “presente” pode ser um item material, um conselho ou uma ajuda. Quando alguém faz algo por outro, este se sente inclinado a retribuir.

Essa forte tendência de retribuição existe nas situações em que a pessoa que recebeu o presente nem mesmo pediu por ele. Uma das maneiras mais eficazes de influenciar as pessoas para fazer um “favor” é dar algum presente ou auxílio que se constitui em uma obrigação implícita.

Os lideres do culto religioso *Hare Krishna* utilizaram a reciprocidade para influenciar as pessoas a fazerem doações, dando lhes uma flor ou um livro (MITNICK & SIMON, 2003; p.197).

A reciprocidade é uma característica muito forte no ser humano. Segundo Dr. Cialdini (CIALDINI et al., 1992), normalmente as pessoas são simpáticas com quem são simpáticos com elas, e cooperam com aqueles que lhes prestam cooperação. Da mesma forma as pessoas tentam prejudicar quem as prejudica.

Em situações de negociação fazem-se concessões para quem também as fazem; as pessoas dão presentes, fazem favores e prestam serviço ou ajudam a quem também prestam favores a elas.

Exemplo de ataque de reciprocidade:

Um empregado recebe uma ligação de uma pessoa que se identifica como sendo do departamento de TI. O interlocutor explica que alguns computadores da empresa foram infectados por um vírus novo que não é reconhecido pelo *Software* antivírus e que pode destruir todos os arquivos de um computador.

Ele se oferece para instruir a pessoa a tomar algumas medidas para evitar o problema. Depois disso, o interlocutor pede que a pessoa teste um utilitário de *software* que acabou de ser atualizado, o qual permite que os usuários mudem as senhas. O empregado reluta em recusar a fazer o que lhe está sendo pedido, porque o interlocutor acabou de lhe prestar ajuda que supostamente o protegerá contra um vírus.

4) Consistência

As pessoas têm a tendência de atender um pedido após fazerem um comprometimento público. Depois que prometem alguma coisa fazem de tudo para não parecerem poucos confiáveis ou incoerentes.

Exemplo de ataque de consistência:

O atacante entra em contato com uma funcionária recém contratada e a instrui sobre determinadas políticas e procedimentos de segurança que devem ser seguidos como condição para usar os sistemas de informações da empresa. Após discutir algumas práticas de segurança, o interlocutor pede à usuária para fornecer a sua senha “para verificar se ela entendeu” a política sobre escolha de senhas difíceis de adivinhar.

Depois que a usuária revela a sua senha, o interlocutor faz uma recomendação para que ela crie senhas de forma que o atacante possa adivinhá-las. A vítima atende ao pedido por causa do acordo anterior de seguir as políticas de segurança e porque supõe que o interlocutor está apenas verificando o seu entendimento.

5) Validação social

As pessoas tendem a cooperar quando isto parece estar de acordo com aquilo que as outras pessoas estão fazendo. A ação dos outros é aceita como uma validação de que o comportamento em questão está correto e apropriado.

Exemplo de ataque de validação social:

O interlocutor diz que está realizando uma pesquisa e dá o nome de outras pessoas do departamento que já teriam cooperado com ele. A vítima, acreditando que a cooperação dos outros serve de autenticidade, concorda em tomar parte na referida pesquisa. Em seguida, o interlocutor faz uma série de perguntas, entre as quais estão perguntas que levam a vítima a revelar o seu usuário e senha.

6) Escassez

As pessoas têm a tendência a cooperar quando acreditam que o objeto procurado está em falta e que outras pessoas estão competindo por ele, ou que ele só está disponível por um período curto tempo.

Exemplo de ataque de escassez:

O atacante envia um e-mail dizendo que as primeiras 50 pessoas que se registrarem no novo *website* da empresa ganharão ingressos grátis para a *première* de um filme a que todos querem assistir.

Quando um empregado desavisado se registra no *site*, ele tem de oferecer o endereço de e-mail da sua empresa e selecionar uma senha. Muitas pessoas, motivadas pela conveniência, têm a tendência de usar a mesma senha ou uma senha semelhante em todos os sistemas de computador que usam.

Aproveitando-se disso, o atacante tenta comprometer o trabalho do alvo (inclusive o computador doméstico) com o nome de usuário e a senha que foram fornecidos durante o processo de registro no *website*.

O termo “engenharia social” é utilizado para descrever os métodos de ataque onde o atacante explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. A seção 2.8. Tipos de Ataque, a seguir, fornecerá maiores informações sobre engenharia social e outros tipos de ataque.

2.8. Tipos de Ataque

Atacar e fraudar dados em um servidor de uma instituição bancária ou comercial em geral não é uma tarefa simples. Diante disto, os atacantes têm concentrado seus esforços na exploração de fragilidades dos usuários, para realizar fraudes através da *Internet*.

Os fraudadores têm utilizado amplamente *e-mails* com discursos que, na maioria dos casos, envolvem *engenharia social* e que tentam persuadir o usuário a fornecer seus dados pessoais e financeiros. Em muitos casos, o usuário é induzido a instalar algum *código malicioso* ou acessar uma página fraudulenta para que dados pessoais como senhas bancárias e números de cartões de crédito possam ser furtados.

Desta forma é muito importante que os usuários de *Internet* tenham certos cuidados com os *e-mails* que recebem e com os serviços de comércio eletrônico ou *Internet Banking* que utilizam (CERT.br - Parte IV, 2006; p. 3/17).

As descrições dos tipos de ataques normalmente utilizados, onde são empregadas técnicas de engenharia social, negação de serviço, códigos maliciosos e ataques em aplicações *web,* são apresentadas na Subseção 2.8.1 e seguintes.

2.8.1. Engenharia Social

O método de ataque conhecido como “engenharia social” tem por objetivo enganar e ludibriar pessoas, a fim de obter informações que possam comprometer a segurança da organização (NAKAMURA & GEUS, 2002; p. 55).

Engenharia social ocorre quando alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter acesso não autorizado a computadores ou informações sigilosas.

Alguns exemplos de ataque de engenharia social são (CERT.br - Parte I, 2006; p. 8/14):

a) um desconhecido liga para a casa de alguém e diz ser do suporte técnico do provedor dele. Nesta ligação, ele diz que a conexão com a *Internet* está apresentando algum problema e, então, pede a senha para corrigi-lo;
b) alguém recebe uma mensagem de *e-mail*, supostamente do fornecedor do seu antivírus, dizendo que seu computador está infectado por um vírus. A mensagem sugere que a pessoa instale uma ferramenta disponível em um *site* da *Internet*, para eliminar o vírus de seu computador; e
c) alguém recebe uma mensagem de *e-mail*, onde o remetente é o gerente ou alguém do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de *Internet Banking* está apresentando algum problema e que tal problema pode ser corrigido se for executado o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela utilizada para se ter acesso à conta bancária, aguardando que se digite a senha.

2.8.2. Negação de Serviço (DoS e DDoS)

Nos ataques de negação de serviço (DoS – *Denial of Service*) o atacante utiliza um computador para tirar de operação um serviço ou um computador conectado à *Internet*. Exemplos deste tipo de ataque são (CERT.br - Parte I, 2006; p. 9/14):

- gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo;
- gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível; e
- tirar serviços importantes de um provedor do ar, impossibilitando o acesso dos usuários a suas caixas de correio no servidor de e-mail ou ao servidor *Web*.

DDoS (*Distributed Denial of Service*) constitui um ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à *Internet*.

Normalmente estes ataques procuram ocupar toda a banda disponível para o acesso a um computador ou rede, causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede.

O objetivo de tais ataques é indisponibilizar o uso de um ou mais computadores, e não invadi-los. É importante notar que, principalmente em casos de DDoS, computadores comprometidos podem ser utilizados para desferir os ataques de negação de serviço.

Um exemplo deste tipo de ataque ocorreu no início do ano 2000, onde computadores de várias partes do mundo foram utilizados para indisponibilizar o acesso aos *sites* de algumas empresas de comércio eletrônico. Estas empresas não tiveram seus computadores comprometidos, mas ficaram impossibilitadas de vender seus produtos durante um longo período.

2.8.3. Códigos Maliciosos

Código malicioso ou *Malware* (*Malicious Software*) é um termo genérico que abrange todos os tipos de programas especificamente desenvolvidos para executar ações maliciosas em um computador (CERT.br - Parte VIII, 2006; p. 4/18).

Será apresentada uma descrição resumida dos seguintes *malwares*: *vírus, cavalos de tróia, adware e spyware, backdoors, keyloggers, worms, bots e botnets, e rootkits.*

Vírus

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando outros programas e arquivos. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

Os vírus podem tanto infectar computadores como qualquer outro dispositivo computacional (*notebooks*, telefones celulares e *PDAs*).

Um vírus pode assumir o controle total de um computador. Ele pode agir de forma inofensiva como, por exemplo, mostrando uma mensagem de “feliz aniversário” na tela do computador infectado, ou agir de forma danosa, quando poderá alterar ou destruir programas e arquivos do disco rígido.

Para que um computador seja infectado por um vírus é preciso que um programa previamente infectado seja executado. Isto pode ocorrer de diversas maneiras:

- abrir arquivos anexados aos *e-mails*;
- abrir arquivos do Word e Excel, entre outros;
- abrir arquivos armazenados em outros computadores, através do compartilhamento de recursos;
- instalar programas de procedência duvidosa ou desconhecida, obtidos pela *Internet*, de disquetes, *pen drives*, CDs e DVDs, entre outros; e
- ter alguma mídia removível infectada conectada ou inserida no computador, quando ele é ligado.

Cavalos de tróia

Conta a mitologia grega que o “Cavalo de Tróia” foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso a cidade de Tróia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Tróia. Daí surgiram os termos “Presente de Grego” e “Cavalo de Tróia”.

Em informática, um cavalo de tróia (*trojan horse*) é um programa, normalmente recebido como um “presente”, por exemplo, cartão virtual, álbum de fotos, protetor de tela e jogo, entre outros, que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia são:

- instalação de *keyloggers* ou *screenloggers*;
- furto de senhas e outras informações sensíveis, como números de cartões de crédito;
- inclusão de *backdoors*, para permitir que um atacante tenha total controle sobre o computador; e
- alteração ou destruição de arquivos.

Adware* e *spyware

Adware - *Advertising* (propaganda) *software* é um tipo de programa especificamente projetado para apresentar propagandas, seja através de um *browser* (navegador), seja através de algum outro programa instalado em um computador.

Em muitos casos, os *adwares* têm sido incorporados aos *softwares* e serviços, constituindo uma forma legítima de patrocínio ou retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos. Um exemplo do uso legítimo de *adwares* pode ser observado no programa de troca instantânea de mensagens *MSN Messenger*.

Spyware, por sua vez, é o termo utilizado para se referir a uma grande categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

Existem *adwares* que também são considerados um tipo de *spyware*, pois são projetados para monitorar os hábitos do usuário durante a navegação na *Internet*, direcionando as propagandas que serão apresentadas.

Os *spywares*, assim como os *adwares*, podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

Backdoors

Normalmente um atacante procura garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão. Na maioria dos casos, também é intenção do atacante poder retornar ao computador comprometido sem ser notado.

A esses programas que permitem o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim, dá-se o nome de *backdoor*.

A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto (através da *Internet*). Pode ser incluído por um invasor ou através de um cavalo de tróia.

Outra forma seria a instalação de pacotes de *software*, tais como o *BackOrifice* e *NetBus*, da plataforma Windows, utilizados para administração

remota. Se mal configurados ou utilizados sem o consentimento do usuário, estes *softwares* podem ser classificados como *backdoors*.

Keyloggers

Keylogger é um programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.

Dentre as informações capturadas podem estar o texto de um *e-mail*, dados digitados na declaração de Imposto de Renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito.

Em muitos casos, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um *site* específico de comércio eletrônico ou *Internet Banking*.

Normalmente, o *keylogger* contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de *e-mails*).

Worms

Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores. Este programa (*Malware*) é capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo, de computador para computador.

Worms são notadamente responsáveis por consumir muitos recursos do sistema, degradar o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar.

Bots* e *Botnets

De modo similar ao *worm*, o *bot* é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador.

Adicionalmente ao *worm*, dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente.

Normalmente, o *bot* se conecta a um servidor de IRC (*Internet Relay Chat*) e entra em um canal (sala) determinado. Então, ele aguarda por instruções do invasor, monitorando as mensagens que estão sendo enviadas para este

canal. O invasor, ao se conectar ao mesmo servidor de IRC e entrar no mesmo canal, envia mensagens compostas por seqüências especiais de caracteres, que são interpretadas pelo *bot*. Estas seqüências de caracteres correspondem a instruções que devem ser executadas pelo *bot*.

Botnets são redes formadas por computadores infectados com *bots*. Estas redes podem ser compostas por centenas ou milhares de computadores. Um invasor que tenha controle sobre uma *botnet* pode utilizá-la para aumentar a potência de seus ataques, por exemplo, para enviar centenas de milhares de *e-mails* de *phishing* ou *spam*, ou desferir ataques de negação de serviço.

Rootkits

Um invasor, ao realizar uma invasão, pode utilizar mecanismos para esconder e assegurar a sua presença no computador comprometido. O conjunto de programas que fornece estes mecanismos é conhecido como *rootkit*.

É muito importante ficar claro que o nome *rootkit* não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou Administrator) em um computador, mas sim para mantê-lo. Isto significa que o invasor, após instalar o *rootkit*, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

2.8.4. Ataques em Aplicações *Web*

As ameaças para uma empresa que está executando aplicações *Web* aparecem de duas formas (HORTON & MUGGE, 2004; p. 136):

1) a aplicação propriamente dita e como ela interage com serviços adjacentes;
2) o servidor e seu ambiente de rede que estão hospedando as aplicações.

Estes autores apresentam as seguintes diretrizes que devem nortear a segurança no ambiente de servidor de aplicações *Web*:

- Proteger o sistema operacional das máquinas. Bloquear e solidificar o sistema operacional do servidor *Web*, do servidor de aplicações e do servidor de banco de dados;
- Proteger a configuração do *software*. Bloquear e solidificar o *software* do servidor de banco de dados, do servidor de aplicações e do servidor *Web* e assegurar que a configuração oferece suporte apropriado aos parâmetros operacionais necessários;

- Proteger o ambiente em que os servidores da *Internet* residem. Implementar *firewall*, compartimentalizar serviços (inclusive servidores de banco de dados e de aplicações), executar internamente mecanismo de detecção de invasores (seja baseado na estação ou na rede), solidificar roteadores e *switches,* e registrar os alertas em tempo real;
- Implementar uma política e uma rotina de gerenciamento de *patches*. Qualquer máquina da DMZ, como servidores *Web*, precisa de um cuidado adicional com a manutenção de *patches* em todos os níveis. Isto serve para todos os sistemas fundamentais na DMZ, de roteadores a *firewalls* e servidores; e
- Fornecer um procedimento de resposta. Colocar em prática um plano de resposta a incidentes para reagir corretamente a qualquer evento de segurança que ocorra.

Além do mais, as aplicações *Web* que recebem dados de usuários através de uma interface aberta, interagem com um banco de dados ou executam autenticação de usuários, deve-se considerar a segurança com que foram construídas e/ou configuradas.

Anatomia de um ataque *Web*

Em geral, os ataques realizados na *Web* seguem uma seqüência básica de eventos, da máquina do atacante até a máquina da vítima, conforme é mostrado na FIG.3.

Um ataque *Web* típico normalmente envolve três etapas distintas (SYMANTEC, 2009):

1. O atacante invade um *website* legítimo e deposita nele um código malicioso. Códigos maliciosos (*Malware*) não são mais uma exclusividade de *Websites* maciliosos como era no passado. Eles estão cada vez mais presentes em *Websites* legítimos e, em tese confiáveis, que servem de hospedeiros para entregar o *malware* aos seus visitantes;
2. Atacando a máquina do usuário final. O *malware* depois de alojado em um *Website* chega até a máquina da vítima quando esta visita o *Website* hospedeiro. Em determinadas situações o *malware* poderá ser baixado automaticamente para o computador do usuário; e
3. Investindo na máquina do usuário final para atividades maliciosas. A maioria das atividades maliciosas começa logo após o novo *malware* se fazer presente na máquina do usuário final.

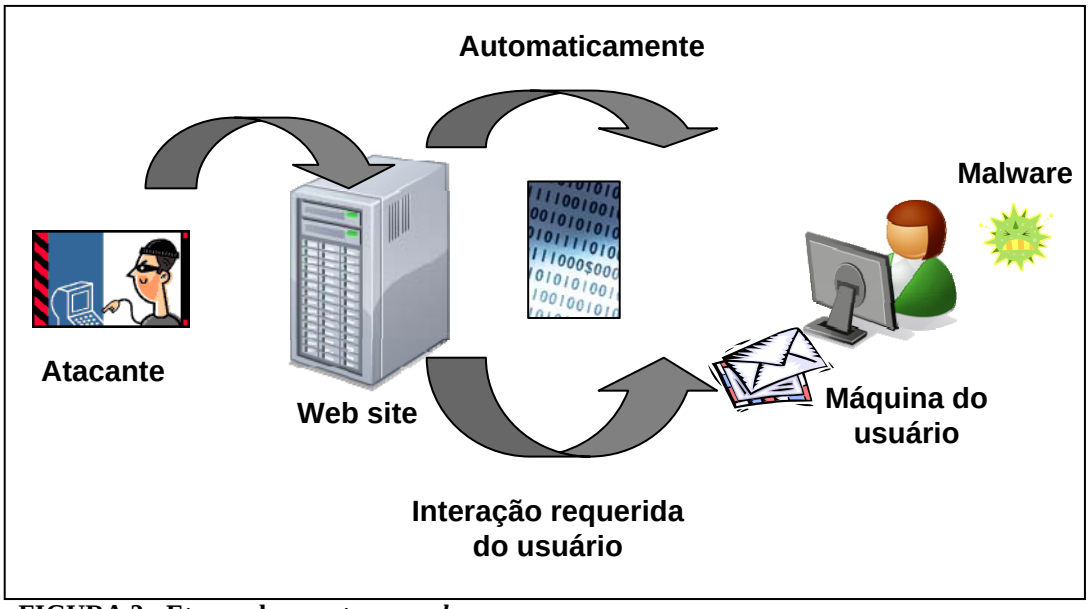


FIGURA 3 - Etapas de um ataque *web*
Fonte: SYMANTEC, 2009; p. 5

Por que *sites* de organizações comuns e conceituadas se tornaram alvo dos atacantes?

Até pouco tempo atrás, acreditava-se que as tentativas de instalação de um *malware* no computador de um usuário através da *Web* ocorriam somente a partir dos mais obscuros recantos da *Internet*. Isto é, a partir de *sites* que estimulam atividades ilícitas como os de material pornográfico ou pirataria de *software*. Os autores de *malware* sabem que neste tipo de *sites* podem encontrar um farto contingente de usuários muito mais interessados em suas necessidades imediatas do que em fazer uma avaliação mais cuidadosa daquilo que estão baixando (*download*) para seus computadores.

Nos últimos anos, porém, os desenvolvedores de *malware* começaram ampliar seus alvos. Cientes de que a grande maioria dos *Websites* da *Internet* possui vulnerabilidades de segurança, os atacantes passaram a investir contra essas máquinas e utilizá-las para hospedar e distribuir *malware* aos internautas que as visitam. O alvo dos atacantes agora inclui *sites* de notícias, viagens, venda no varejo, *games*, imóveis, governos e muitos outros.

Um das mais traiçoeiras formas de infecção de *malware* é conhecida como “*drive by download*”. A simples exibição de um *Website* no navegador pode fazer com que algum conteúdo executável seja baixado automaticamente para o computador do usuário, sem que ele tenha conhecimento ou lhes seja pedida qualquer permissão. Neste caso, nenhuma interação do usuário é requerida.

Alguns fatos têm contribuído para o agravamento nesta situação. Entre os quais está a complexidade tecnológica envolvida na construção das “páginas” atuais. Os *websites* atuais não são mais simples páginas estáticas como eram no passado. Agora eles são uma combinação de diferentes fontes de conteúdo, dinamicamente construídos usando diferentes tecnologias de *scripting* (*JavaScript*, ActiveX, *ASP* e *PHP*), *plug-in*, e banco de dados.

Maiores detalhes sobre as formas de ataques utilizadas pelos *Hackers* para ganhar acesso a um servidor *Web* fogem do escopo deste trabalho.

Diante do exposto, conclui-se que a segurança da informação deve atuar com duas preocupações distintas, no que se refere às aplicações *Web*: (1) implementar controles para prevenir que seus servidores *Web* se tornem hospedeiros de códigos maliciosos; e (2) atuar junto aos seus usuários, para que estes não sejam vítimas desses ataques, quando navegando na *Internet*, e que seus computadores de trabalho sejam infectados por códigos maliciosos e se transformem em fontes de atividades ilícitas.

2.9. Programa de Treinamento e de Conscientização

O controle 8.2.2 - Conscientização, educação e treinamento em segurança da informação da Norma ABNT NBR ISO/IEC 27002 (ABNT, 2005; p. 28) estabelece:

> *“Convém que todos os funcionários da organização e, onde pertinente, fornecedores e terceiros recebam treinamento apropriado em conscientização, e atualizações regulares nas práticas e procedimentos organizacionais, relevantes para as suas funções”.*

As organizações devem não só definir por escrito as regras das suas políticas, mas também devem se esforçar ao máximo para orientar seus funcionários para que eles conheçam e sigam as regras. Além disso, deve-se garantir que todos entendam o motivo de cada política, para que não tentem desviar-se da regra por questão de conveniência. A ignorância não pode ser usada como desculpa pelo empregado, pois é exatamente esta vulnerabilidade que os engenheiros sociais vão tentar explorar (MITNICK & SIMON, 2003; p.198).

O objetivo central de um programa de conscientização sobre segurança é influenciar as pessoas para que elas mudem seu comportamento e suas atitudes, motivando-as a fazerem sua parte para a proteção dos ativos de informações da organização.

Um bom motivador neste caso é explicar como a participação das pessoas beneficiará não apenas a empresa, mas também cada um individualmente. Como a empresa detém informações particulares sobre cada funcionário, quando os empregados fazem sua parte para proteger as informações ou os sistemas de informações, na verdade eles estão protegendo também suas próprias informações.

O esforço de treinamento precisa atingir cada pessoa que tem acesso as informações confidenciais ou aos sistemas coorporativos de computadores, deve ser contínuo e sempre revisado para atualizar os usuários sobre novas ameaças e vulnerabilidades.

O comprometimento da alta direção constitui fator decisivo para o sucesso do programa de treinamento. Os empregados precisam perceber, de forma clara e inequívoca, que a direção da casa está totalmente comprometida com o programa.

Treinamento deve ser algo criativo, variado e atraente; orientado para situações da vida real, e precisa ser freqüente. Incorporando treinamentos curtos em segurança dentro de eventos já existentes, como reuniões de funcionários ou de gerentes, e também no processo de integração dos novos contratados, costuma ser mais eficiente que um seminário de um dia inteiro uma vez por ano.

A efetividade de um treinamento é substancialmente maior quando um incidente real conhecido pelos empregados pode ser usado como exemplo de risco, ações, retribuição e conclusão, estando associado com uma ação de responsabilidade do departamento de segurança (TIPTON & KRAUSE, 2003, p. 245).

Um dos objetivos principais do treinamento dever ser a conscientização de cada empregado de que eles são a linha de frente necessária para proteger a segurança geral da organização.

A empresa poderá considerar que seu programa de conscientização está atingindo o objetivo final se todos os que realizarem o treinamento estiverem convencidos e motivados por uma noção básica: “a noção de que a segurança das informações faz parte do seu trabalho” (MITNICK & SIMON, 2003; p.199).

2.10. Gerenciamento de Mudanças

“O mundo odeia mudança, porém é a única coisa que traz progresso”
Charles F. Kettering (MACKENZIE, 2007).

Outra questão bastante importante e que merece a devida atenção do departamento de segurança é o impacto produzido no ambiente organizacional (estruturas estabelecidas) durante a implantação de qualquer tipo de medida de segurança, a qual deve ser encarada como uma mudança.

Do ponto de vista individual, mudanças em geral podem causar emoções e reações que vão do otimismo ao medo, podendo incluir ansiedade, desafio, resistência, ambigüidade, energia, entusiasmo, incapacidade, receio, pessimismo e motivação.

A mudança organizacional abrange a introdução de novos processos, procedimentos e tecnologias e se constitui do processo de reconhecer, guiar e administrar essas emoções e reações humanas, de modo a minimizar a queda de produtividade que geralmente acompanha as mudanças (Direction RH, 2007).

Gerenciamento de mudanças (*Change Management*) de TI tem o objetivo de permitir que as empresas se adaptem às transformações, controlem os processos e, assim, obtenham efetivamente os ganhos que esperam.

Normalmente o gerenciamento de mudanças é utilizado para garantir o menor impacto possível na troca de computadores, roteadores e sistemas de telefonia (INFO, 2004). Mas também vem sendo aplicada com foco em recursos humanos, já que pessoas são fundamentais no processo.

Cristhiane Quadros, da HP Consult, falando para a revista INFO Corporate disse que não dá para executar o gerenciamento da mudança sem cuidar com atenção do fator humano. Segundo a consultora o tripé **tecnologia-processo-pessoas** é importante para o sucesso do gerenciamento de mudança, principalmente as pessoas.

A preocupação com a satisfação do funcionário ajuda a atingir os resultados de negócios esperados. É por isso que a equipe de *Change Management* deve "vender" a idéia da mudança para o funcionário de forma eficiente (INFO, 2004).

Para MACKENZIE (2007), as mudanças podem ser mais aceitas ou menos aceitas pelos indivíduos na organização. Uma mudança adaptativa pode

ser menos ameaçadora por parecer familiar, ao passo que uma mudança inovadora (não familiar) traz ansiedade – inquietação.

O autor supracitado alerta aos executivos de que em organizações com forte cultura corporativa, profundamente arraigada com valores que guiam comportamentos, as mudanças podem não obter o apoio necessário durante sua implantação. Quando isto acontece, o executivo deve promover a substituição de pessoal chave dentro deste processo e se pronunciar claramente sobre os objetivos da mudança, e em determinados casos, adequar a mudança ao esquema de valores aceito pela organização.

O processo de instalação de um novo controle de segurança, seja ele tecnológico ou não-tecnológico, traz sempre algum risco que pode impactar o andamento das atividades na organização.

A implantação de uma nova medida de segurança tem dois momentos distintos: o da medida em si junto à comunidade de usuários (grau de aceitação / rejeição), e o produzido durante a instalação de um novo equipamento ou *software*, quando este for necessário para o cumprimento da medida adotada.

O IPEN, em particular, tem alguns casos de implementações (mudanças) mal sucedidos. Um exemplo disto ocorreu em março de 2000 por ocasião da instalação de um novo sistema de *firewall*, por uma empresa terceirizada. Por conta desta mudança, a rede de comunicação de dados do IPEN apresentou perdas constantes de conectividade chegando à paralisação total em determinados momentos; situação que se estendeu por várias semanas.

Em outra ocasião, a instalação de um *software* de inventário, para evitar a prática de pirataria, ou seja, utilização de programas de computador não autorizados, provocara desconfiança e reações contrárias a sua utilização.

A situação se agravou ainda mais quando algumas máquinas, onde o referido *software* tinha sido instalado, apresentaram travamento do sistema operacional (famosa tela azul do *Windows*) entre outros problemas.

O impacto negativo desta medida foi de tal ordem que se optou pelo cancelamento total do projeto, por determinação da alta direção.

Além do prejuízo financeiro e de pessoal, o falta de um gerenciamento de mudança efetivo pode resultar em grande desgaste para a imagem do departamento envolvido na sua implementação.

A administração do fator humano em um processo de mudança deve abranger todos os envolvidos no processo, incluindo tanto o usuário final que será afetado pela mudança, como o pessoal técnico responsável pela sua implantação, seja este pertencente ao quadro de funcionários da organização ou de empresa contratada.

2.10.1. ABNT NBR ISO/IEC 27002:2005 - Gestão de Mudanças

A Norma ABNT NBR ISO/IEC 27002 (ABNT, 2005; p. 41) estabelece no controle 10.1.2 *Gestão de Mudanças*, da seção 10 - *Gerenciamento de Operações e Comunicações*, as seguintes diretrizes: *"Convém que sistemas operacionais e aplicativos estejam sujeitos a rígido controle de gestão de mudanças"*. E continua; Em particular, convém que os seguintes itens sejam considerados:

- identificação e registro das mudanças significativas;
- planejamento e testes das mudanças;
- procedimento formal de aprovação das mudanças propostas;
- comunicação dos detalhes das mudanças para todas as pessoas envolvidas;
- procedimento de recuperação, incluindo procedimentos e responsabilidades pela interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

A referida Norma recomenda ainda que procedimentos e responsabilidades gerenciais formais sejam estabelecidos para garantir que haja um controle satisfatório de todas as mudanças de equipamentos, *softwares* ou procedimentos.

O controle 10.2.3 *gerenciamento de mudanças para serviços terceirizados*, adverte que mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, procedimentos e controles existentes, sejam gerenciadas levando-se em conta a criticidade dos sistemas e processos de negócio envolvidos e a reanálise / reavaliação de riscos.

2.10.2. COBIT – Gerência de Mudança

O COBIT, acrônimo inglês de *Control Objectives for Information and related Technology* é um conjunto de diretrizes (*framework*) para segurança da informação criado para ISACA - *Information Systems Audit and Control Association*, e o ITGI - *IT Governance Institute*.

Para o Cobit (ITGI, 2007; p. 93), todas as mudanças, incluindo manutenção de emergência e aplicação de *patches* de correção, relativas à infra-estrutura e aplicações em ambiente de produção devem ser formalmente gerenciadas e controladas.

Mudanças (incluindo as relativas a procedimentos, processos, sistemas e parâmetros de serviços) devem ser registradas, avaliadas e autorizadas antes da implementação; e examinadas após a implementação com relação aos resultados esperados. Isto evita que a estabilidade ou integridade do ambiente de produção sofra impactos negativos.

O gerenciamento de mudança no COBIT é tratado no processo 6 – Gerência de Mudanças, do domínio “Aquisição e Implementação”. Ele é composto por cinco atividades:

1. Mudança de padrões e procedimentos

   Estabelece procedimentos formais de gerenciamento de mudança para manipular de maneira padronizada todos os requerimentos (incluindo manutenções e *patches* de correção) para mudanças em aplicativos, procedimentos, processos, sistemas e parâmetros de serviços e nas plataformas de suporte;
2. Avaliação de impacto, priorização e autorização

   Analisa todos os requerimentos para a mudança de um modo estruturado para determinar o impacto no sistema operacional e suas funcionalidades. Seu objetivo é assegurar que as mudanças sejam categorizadas, priorizadas e autorizadas;
3. Mudanças emergenciais

   Estabelece um plano para definir, executar, testar, documentar, avaliar e autorizar mudanças de emergências, que fogem do processo de mudança estabelecido;
4. Reporte e trilha de mudança

   Estabelece um sistema de trilha e reporte (auditoria) para documentar mudanças rejeitadas e comunicar o estado de mudanças aprovadas, em andamento e concluídas. Tem como objetivo certificar que as mudanças aprovadas sejam implementadas como planejado; e

5. Documentar e encerrar a mudança

   Sempre que uma mudança é implementada, atualiza-se a documentação do sistema e do usuário, e os procedimentos conseqüentes associados a ela.

2.11. Processos de Trabalho

Processos podem ser entendidos como "a forma pela qual as coisas são feitas na empresa" (LIPNACK & STAMPS, 1997 apud GONÇALVES, 2000).

Todo trabalho importante realizado em qualquer organização faz parte de algum processo. Não existe um produto ou um serviço oferecido por uma empresa ou organização sem a existência de um processo empresarial ou de trabalho (GONÇALVES, 2000).

Na concepção mais freqüente, processo é qualquer atividade ou conjunto de atividades que toma uma entrada (*input*), adiciona valor a ela e fornece uma saída (*output*) a um cliente específico, conforme está ilustrado na FIG.4.

Na FIG.4 é mostrado um processo de trabalho genérico composto de quatro atividades para se produzir um resultado específico, que irá contribuir para o objetivo maior da organização (sua missão).

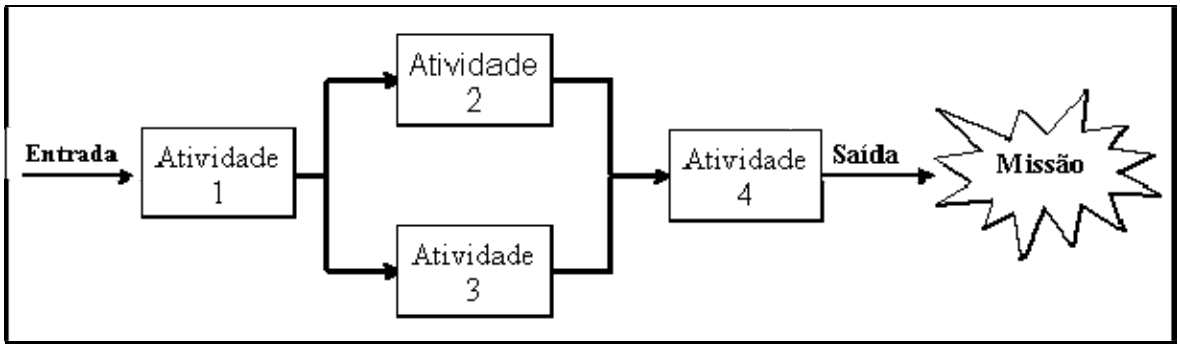


FIGURA 4 - Processo de trabalho
Fonte: Alberts C. (2006, p. 10). Common Elements of Risk.

Os processos utilizam os recursos da organização para oferecer resultados objetivos aos clientes (HARRISON, 1998).

HAMMER & CHAMPY (1994, apud GONÇALVES, 2000) definem processo de uma maneira mais formal como sendo um grupo de atividades realizadas numa seqüência lógica com o objetivo de produzir um bem ou um serviço que tem valor para um grupo específico de clientes (internos ou externos).

Essa idéia de processo como um *fluxo de trabalho* - com entradas e saídas claramente definidas e tarefas discretas que seguem uma seqüência, e

que dependem umas das outras numa sucessão clara - vem da tradição da engenharia (HARRINGTON, 1991 apud GONÇALVES, 2000). As entradas podem ser materiais - equipamentos e outros bens tangíveis, mas também podem ser ***informações e conhecimento***.

Nem sempre os processos empresariais são formados de atividades claramente delineadas em termos de conteúdo, duração e consumo de recursos definidos, nem precisam ser consistentes ou realizados numa seqüência particular. Talvez este seja o caso do processo de pesquisa e desenvolvimento científico.

Na FIG.5 mostra-se o relacionamento entre processos de negócios e tecnologia de informação (TI), onde pode ser observado o alto grau de dependência de TI nas organizações atuais.

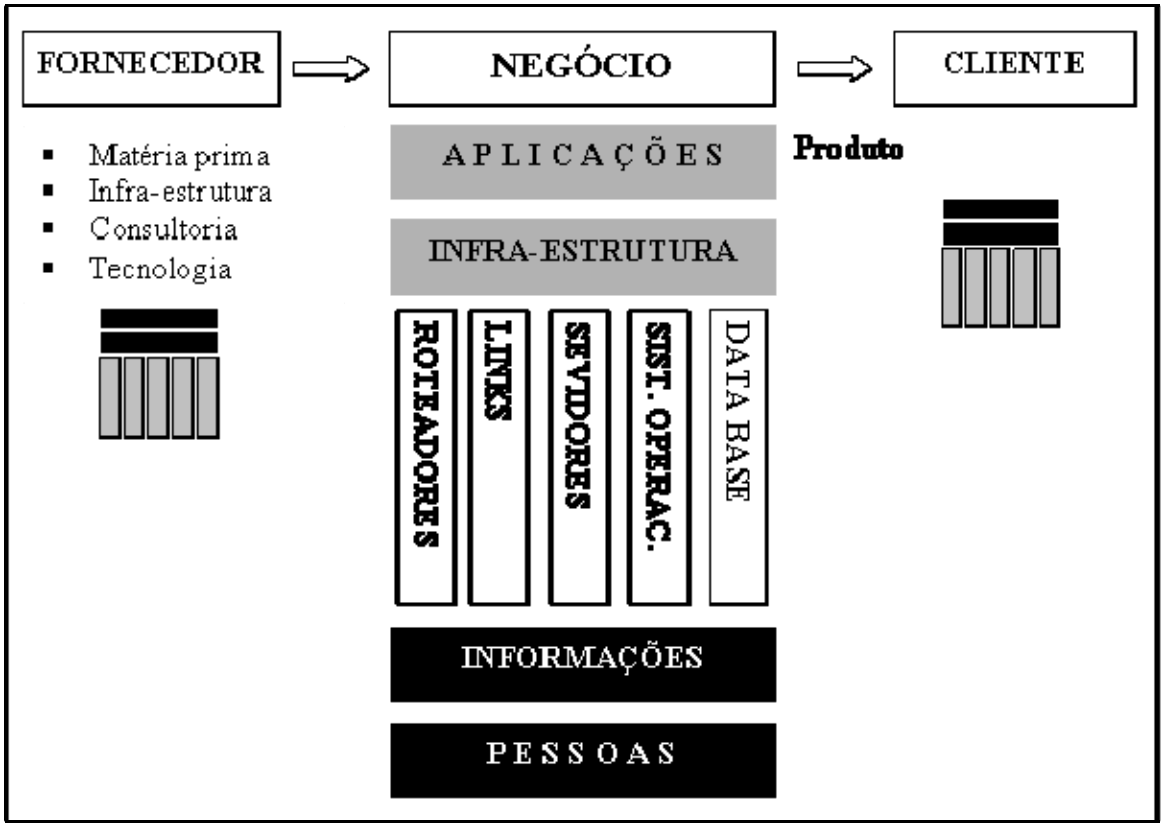


FIGURA 5 - Macro visão de processo de trabalho (negócio)
Fonte: Modulo Certified Security Officer – Módulo-1

2.12. Governança Corporativa

A Federação Internacional dos Contadores (IFAC) e a Associação de Controle e Auditoria de Sistemas de Informação (ISACA) definem governança corporativa da seguinte forma (ALLEN, 2007; p. 2):

> *"Governança corporativa é um conjunto de práticas e responsabilidades exercidas pela alta administração com o intuito de fornecer um direcionamento estratégico, para garantir que os objetivos da organização sejam alcançados; certificando-se que os riscos estão sendo gerenciados adequadamente e que os recursos da organização estão sendo usados com responsabilidade".*

O conceito de governança corporativa estende-se também, para o gerenciamento do uso de TI, sendo a segurança da informação e dos sistemas de TI parte integrante da mesma.

O propósito da *governança em segurança da informação* é garantir que a organização planeje e implemente controles de segurança apropriados para dar o suporte necessário a sua missão, a um custo compatível.

Governança em segurança da informação tem seu conjunto próprio de requerimentos, desafios, atividades, e modelos de estruturas possíveis. Por esta razão o NIST definiu governança em segurança da informação como segue (BOWEN et al. 2006; p.2):

> *"o processo de estabelecimento e manutenção de um framework (sistema), com o suporte de processos e estruturas administrativas, para garantir que as estratégias de segurança da informação estejam alinhadas aos objetivos do negócio e em conformidade com as leis e regulamentos aplicáveis; por meio de políticas e controles internos e atribuição de responsabilidades. Todo este esforço voltado para gerenciar riscos".*

2.13. Estabelecendo os Requisitos de Segurança da Informação

É primordial na implementação da segurança da informação que a organização identifique os seus requisitos de segurança. Existem três fontes principais de requisitos de segurança da informação (ABNT 27002, 2005; p. x):

1. Análise e avaliação de risco – considerando-se os objetivos e as estratégias globais de negócio da organização.

   É na análise e avaliação de risco que são identificadas as ameaças e vulnerabilidades presentes nos ativos de informação, onde é também realizada uma estimativa da probabilidade e do impacto caso um evento indesejado acorra;

2. Legislação vigente – refere-se aos estatutos, regulamentos e cláusulas contratuais que a organização, seus parceiros comerciais, contratados e prestadores de serviços têm que atender. Deve-se considerar também o ambiente sóciocultural em que a organização está inserida;

3. Política corporativa de segurança da informação – é um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação, que a organização tem que desenvolver para apoiar as suas operações.

2.13.1. Análise, Avaliação e Tratamento de Riscos

O controle 4.1 Analisando/avaliando os riscos de segurança da informação da Norma ABNT NBR ISO/IEC 27002 (ABNT, 2005; p. 6) declara:

> *"convém que a análise/avaliação de riscos inclua um enfoque sistemático de estimar a magnitude do risco (análise de riscos) e o processo de comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco)"*.

A atividade de análise e avaliação de risco constitui o primeiro passo de uma metodologia de gerenciamento de risco.

Para a FERMA (2003; p. 3) a gestão de riscos é um elemento central na gestão estratégica de qualquer organização. É o processo através do qual as organizações analisam metodicamente os riscos inerentes às respectivas atividades, com o objetivo de alcançarem uma vantagem sustentada em cada atividade individual e no conjunto de todas as atividades.

De acordo com BERNSTEIN (1998 apud KLOMAN, 2003)

> *"A essência da gestão do risco consiste em maximizar as áreas onde temos algum controle sobre a conseqüência, enquanto minimizamos as áreas onde não temos absolutamente nenhum controle sobre as conseqüências, e as ligações entre causa e efeito estão escondidas de nós"*.

PELTIER (2005; p. 7) define gerenciamento de risco como um processo que permite ao gerente de negócio balancear os custos operacionais e econômicos das medidas de proteção e obtenção de ganhos na capacidade de cumprimento da missão, pela proteção dos processos de negócio que dão suporte aos objetivos da empresa. O citado autor acrescenta que gerenciamento de risco não se restringe apenas ao domínio da tecnologia da informação e segurança. Ele é um processo de negócio que auxilia a administração a conhecer suas obrigações de confiança (fiduciárias) para proteger os ativos da organização.

O processo de identificar, analisar e avaliar o risco, para uma tomada de decisão quanto às medidas a serem adotadas é conhecido como gerenciamento de riscos. O gerenciamento de riscos determina a direção e o contexto correto para a implantação de um plano de segurança da informação e das políticas e procedimentos de segurança.

Segundo STONEBURNER et al. (2002; p. 4) o gerenciamento de riscos consiste em três processos distintos: análise do risco, mitigação do risco, e avaliação e análise.

A análise de risco é o primeiro processo em uma metodologia de gerenciamento de risco. Ele determina a extensão da ameaça potencial e o risco associado com um sistema de TI. A saída deste processo ajuda a identificar os controles apropriados para reduzir ou eliminar o risco durante o processo de mitigação (STONEBURNER et al. 2002; p. 8).

O processo de mitigação do risco envolve a priorização, avaliação e implementação dos controles necessários para o tratamento do risco, conforme as recomendações dadas pelo processo de análise de risco (STONEBURNER et al. 2002; p. 27).

O terceiro processo do gerenciamento de riscos, avaliação e análise - cria um círculo contínuo que realimenta o processo de análise de risco. Este processo é extremamente necessário em virtude do dinamismo com que os acontecimentos se sucedem em uma organização, que vão influenciar no nível de segurança estabelecido. Exemplo disto é a contínua expansão e atualização da infra-estrutura de rede e tecnologias utilizadas, bem como os sistemas e aplicativos que são adquiridos ou alterados. Ocorrem ainda admissões e demissões de empregados e contratações de terceirizados, que requerem medidas de segurança adicionais (STONEBURNER et al. 2002; p. 41).

O gerenciamento do risco é um processo contínuo de análise, avaliação, priorização e implementação de recomendações de segurança conforme o grau de criticidade do risco. Ele permite ao gerente de TI (ou gestor de segurança) balancear o custo operacional e econômico das medidas de defesa e obter ganhos protegendo os sistemas de TI, dados e informações que dão suporte à missão da organização.

Análise de risco

O principal componente de um programa de segurança é o gerenciamento de risco.

STONEBURNER et al. (2002; p. 2) sustentam que gerenciamento de risco habilita uma organização a realizar sua missão por meio de três ações primárias. Primeiro, aumentando a segurança dos sistemas de TI que armazenam, processam e transmitem informações. Segundo, permitindo que os

gerentes possam tomar melhores decisões quanto aos gastos com TI. Terceiro, auxiliando a administração na autorização (aprovação) de sistemas de TI, baseado no suporte da documentação resultante do gerenciamento de risco.

Os referidos autores definem risco como *"uma função da probabilidade de uma determinada ameaça explorar uma particular vulnerabilidade, e o impacto resultante deste evento adverso na organização"*.

De acordo com a Norma ISO/IEC Guide 73 (FERMA, 2003; p. 3), o risco pode ser definido como a combinação da probabilidade de um acontecimento e das suas conseqüências.

Riscos são incertezas. Sua probabilidade, freqüência e conseqüência são incertas. Algumas ameaças podem ocorrer muitas vezes em um período de uma hora, outras podem levar uma década entre duas ocorrências. A freqüência pode ser encontrada nos registros de salvaguardas existentes. Outras vezes podem ser deduzidas de métricas e outras fontes, mas algumas são obtidas por meio de julgamentos (GCIO, 2007; p. 15).

Na FIG.6 mostram-se os componentes do risco em segurança da informação e seus relacionamentos no processo de análise de risco.

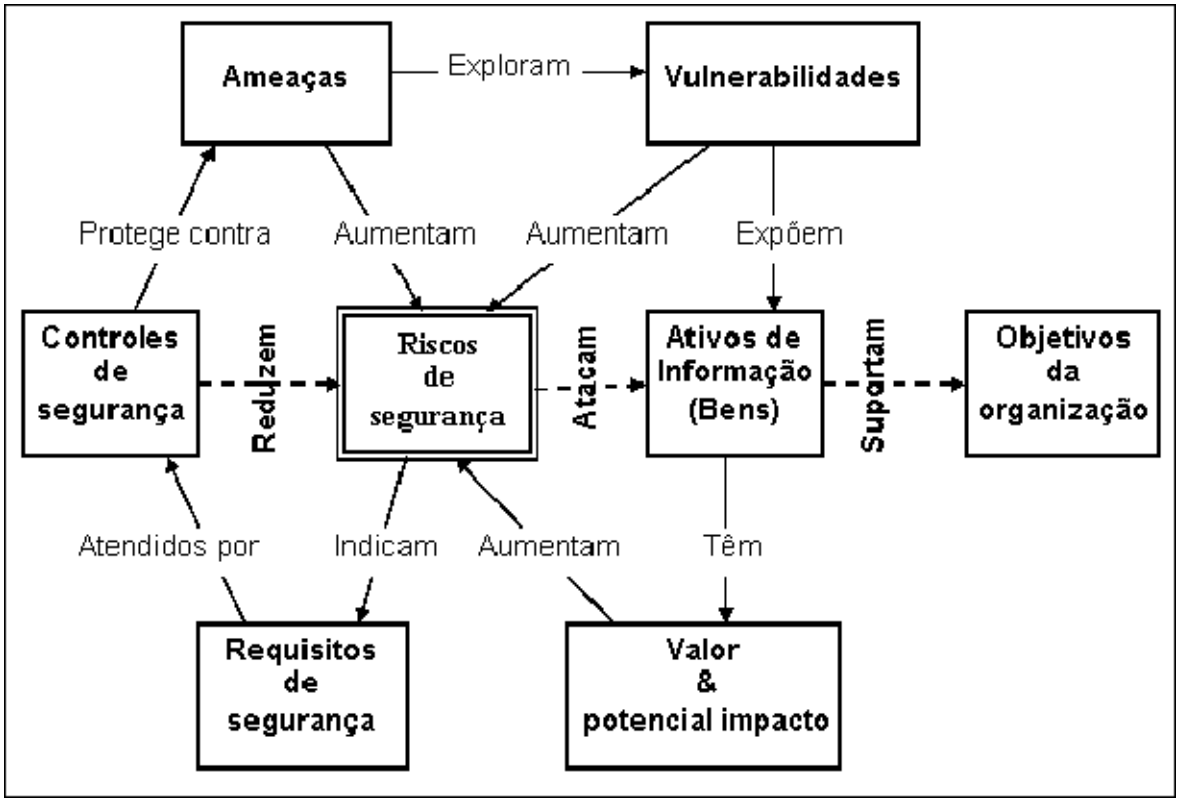


FIGURA 6 - Componentes do risco
Fonte: GCIO, 2007; p.14

Ativos de informação

Ativo, neste contexto, é tudo que manipula a informação, inclusive ela própria. Os ativos são normalmente classificados nas seguintes categorias (ABNT 27002, 2005; p. 21):

- ativos de informação: informações armazenadas, base de dados e arquivos, contratos e acordos, documentação de sistema, procedimentos de recuperação, manuais de usuários e material de treinamento, entre outros;
- ativos de *softwares*: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
- ativos físicos: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;
- serviços: serviços de computação e comunicação, utilidades gerais, por exemplo, aquecimento, iluminação, eletricidade e refrigeração;
- pessoas e suas qualificações, habilidades e experiências; e
- intangíveis, tais como a reputação e a imagem da organização.

Ameaças

Conforme estabelece a ABNT NBR ISO/IEC 27002 (2005, p. ix), as organizações, seus sistemas de informação e redes de computadores são expostas a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Segundo ainda a referida Norma, os danos causados por códigos maliciosos, *hackers* e ataque de *denial of service* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

Para STONEBURNER et al. (2002, p.13) as ameaças podem ser classificadas em três tipos :

- ameaças naturais – Inumações, enchentes, terremotos, tornados, desmoronamentos, avalanches, tempestades elétricas;
- ameaças humanas – eventos que são permitidos ou causados por seres humanos, que podem ser de dois tipos:

  ações involuntárias - como, por exemplo, erros e omissões (entrada de dados inadvertidos);

  ações deliberadas – fraudes, *upload* de *softwares* maliciosos e acesso não autorizado a informações confidenciais; e

- ameaças ambientais – interrupção de energia por longo período de tempo, poluição, vazamento de produto químico, derramamento de água.

Estatisticamente as ameaças que causam as maiores perdas para os recursos de informação são provenientes de erros ou omissões humanas (PELTIER et al., 2005; p. 188).

Em geral uma ameaça pode causar os seguintes danos (GCIO, 2007; p. 15):

- destruição de um ativo ou da sua capacidade de operar (instalações, dados, informação, equipamentos, comunicações);
- corrupção ou modificação de um ativo (dados, informação, aplicações);
- roubo, remoção ou perda de um ativo ou da sua capacidade (equipamento, dados, informação, aplicações);
- revelação de um ativo (dados ou informação confidencial);
- uso ou aceitação de um ativo ilegal (equipamento, *software* sem licença de uso (pirataria), dados e informações falsas ou repudiadas); e
- interrupção de serviços.

Na TAB.4 apresentam-se as mais comuns ameaças humanas, suas possíveis motivações, e os métodos ou ações usadas para realizar um ataque.

TABELA 4 - Ameaças humanas: origem da ameaça, motivação e ações da ameaça

Origem da Ameaça	Motivação	Ações da Ameaça
Hacker *Cracker*	Desafio Ego Protesto	• *Hacking* (ganhar acesso e explorar sistemas e redes de computadores) • Engenharia social • Invasão do sistema • Acesso não autorizado ao sistema
Crime virtual	Destruição de informação Revelação ilegal de informação Ganho financeiro Alteração desautorizada de dados	• Crime virtual (escuta eletrônica) • Ações fraudulentas (personificação, intercepção) • Adquirir informação mediante suborno • Enganar / ludibriar • Invasão de sistema
Terrorismo	Chantagem Destruição Exploração Vingança	• Bomba / Terrorismo • Guerra de informação • Ataque a sistema (DDOS) • Penetração de sistema
Espionagem industrial	Vantagem competitiva Espionagem econômica	• Exploração econômica • Roubo de informação • Invasão da privacidade pessoal • Engenharia social • Penetração de sistema • Acesso desautorizado (acessar informação sigilosa, informação relativa à propriedade industrial e/ou tecnologia)
Usuários internos (mal treinados, insatisfeitos, mal intencionados, desonestos ou empregados demitidos)	Curiosidade Ego Inteligência Ganhos financeiros Vingança Erros ou omissões sem intenção (entrada de dado errado, erro de programação)	• Assalto de um empregado • Chantagem • Acessar informações proprietárias • Mau uso do computador • Fraude e roubo • Adquirir informação mediante suborno • Entrada de dados falsificados ou corrompido • Interceptação • Código malicioso (vírus, *worms*, cavalo de tróia) • Venda de informações pessoais • Falha (*bug*) de sistema • Invasão de sistema • Sabotagem de sistema • Acesso desautorizado ao sistema

Fonte: STONEBURNER et al., 2002; p.14

Vulnerabilidades

Vulnerabilidades são fragilidades (ou falhas) presentes em ativos ou na capacidade da organização prover seu negócio. Uma vulnerabilidade é uma condição ou um conjunto de condições que possibilite que uma ameaça atinja (e ataque) o ativo. Para uma vulnerabilidade ser explorada, ela deve ser conhecida ou descoberta pelo agente da ameaça.

As ameaças vão, na verdade, se concretizar explorando alguma vulnerabilidade ou brechas de segurança presente nos sistemas. A segurança da informação deve, portanto, cuidar para que as potenciais vulnerabilidades sejam eliminadas.

Desta forma, uma vulnerabilidade que não possa ser explorada, ou um ativo sem qualquer vulnerabilidade conhecida, não pode ser considerado um risco de segurança. Normalmente, as vulnerabilidades surgem em função de procedimentos falhos, baixa qualificação de pessoas, e de tecnologia defeituosa ou incorretamente configurada (GCIO, 2007; p. 16).

Na TAB.5 são listados alguns exemplos da junção vulnerabilidade / ameaça e as possíveis conseqüências dessa união. Na referida TABELA é apresentado o perigo que esta combinação representa para a segurança da informação.

TABELA 5 - União de vulnerabilidade e ameaça

Vulnerabilidade	**Agente da ameaça**	**Ação da ameaça**
As identificações de empregados (*user ID*) demitidos não são removidas do sistema	Empregados demitidos (usuários desligados)	Entrar na rede de computadores na empresa e acessar dados proprietários da companhia.
"Firewall" da companhia permite *telnet* para dentro da rede interna, e o ID *guest* está habilitado no servidor XYZ	Usuário desautorizado (tais como *hackers*, funcionários demitidos, criminosos virtuais, terroristas)	Usar o *telnet* para o servidor XYZ e ter acesso aos arquivos do sistema como usuário *guest*
O fornecedor identificou falhas de segurança no projeto do seu sistema; entretanto, as novas correções não foram aplicadas neste sistema instalado na empresa	Usuário desautorizado (tais como *hackers*, funcionários insatisfeitos, criminosos digitais, terroristas)	Obter acesso não autorizado a arquivos sensíveis do sistema baseado em vulnerabilidades conhecidas
Data Center usa *sprinklers* (vaporizador de água) para combater incêndios; porém a proteção *tarpaulins* (Impermeável) não foi colocada sobre os equipamentos	Fogo, pessoas negligentes	O vaporizador de água (*sprinklers*) é acionada no *data center*

Fonte: STONEBURNER et al., 2002; p.15

Talvez a mais perversa dentre todas as vulnerabilidades, e também a mais difícil de se controlar, seja a susceptibilidade dos empregados aos ataques de "engenharia social" – vide subseção 2.7.1.

Controles de segurança

A Norma ABNT NBR ISO/IEC 27002 (ABNT, 2005) define controle como *"uma forma de gerenciar o risco, incluído políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal"*.

A ABNT NBR ISO/IEC 27002:2005 possui ao todo 133 controles de segurança. Todos esses controles devem ser considerados durante um processo de análise de risco, porém só serão usados aqueles que forem aplicáveis e necessários ao ambiente em questão. Em determinadas situações controles adicionais poderão ser necessários (GCIO, 2007; p. 41).

O caráter de intangibilidade da informação a torna um ativo de características bastante peculiar, uma vez que a mesma pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas.

Seja qual for a forma em que a informação se apresente ou o meio em que ela é compartilhada ou armazenada, recomenda-se que seja sempre protegida adequadamente.

Avaliação quantitativa versus avaliação qualitativa

Uma análise qualitativa do risco é uma análise de natureza subjetiva, baseada nas melhores práticas do mercado e na experiência do profissional que a realiza. Geralmente, as conclusões de uma análise qualitativa são mostradas em uma lista de vulnerabilidades com uma escala relativa dos riscos (baixo, médio, ou alto).

Por outro lado, a análise qualitativa tende a ser mais aberta e flexível, fornecendo ao avaliador uma grande liberdade na determinação do escopo da avaliação. Dado que cada ambiente de TI potencialmente representa uma única combinação de ameaças, vulnerabilidades, e salvaguardas; esta flexibilidade é muito útil na obtenção de resultados rápidos e significativos (TIPTON & KRAUSE, 2003; p. 333).

A análise quantitativa do risco tem muitos pontos em comum com a metodologia de análise qualitativa - com a tarefa adicional de determinar o custo associado com a ocorrência de uma vulnerabilidade ou grupo de vulnerabilidades. Estes custos são calculados pela determinação do valor do ativo, da freqüência

da ameaça, fator de exposição à ameaça, efetividade das medidas de proteção, custo da salvaguarda, e outras fatores de incertezas.

Em um processo de análise de risco deve-se levar em consideração as vantagens e desvantagens da avaliação qualitativa versus a quantitativa.

Para PELTIER (2005, p. 77) a principal vantagem da análise qualitativa é que ela prioriza os riscos e identifica as áreas que requerem ações imediatas e aprimoramento da segurança frente às vulnerabilidades. A desvantagem é que ela não fornece uma medida específica (quantificável) da magnitude do impacto. Portanto, fazer uma análise de custo-benefício de qualquer controle de segurança recomendado é muito difícil.

A principal vantagem da análise quantitativa é que ela fornece um dimensionamento melhor da magnitude do impacto, o qual pode ser usado na análise do custo-benefício dos controles recomendados. A desvantagem é que, dependendo do conjunto numérico usado para expressar o cálculo do risco, o resultado obtido pode não ser muito claro, requerendo que o mesmo seja interpretado de maneira qualitativa.

Fatores adicionais freqüentemente devem ser considerados para determinar a magnitude do impacto. Entre outros pode-se incluir (PELTIER, 2005, p. 78):

- uma estimativa da freqüência com que a fonte da ameaça pode explorar a vulnerabilidade sobre um período de tempo específicado (por exemplo, um ano);
- um custo aproximado para cada execução bem sucedida da fonte de ameaça; e
- um peso (fator), baseado na subjetividade da análise, do impacto relativo de uma ameaça explorar uma vulnerabilidade específica.

Na TAB.6 apresenta-se um resumo das vantagens e desvantagens das duas abordagens.

TABELA 6 - Pros e contras das avaliações quantitativa e qualitativa

Avaliação quantitativa do risco	**Avaliação qualitativa do risco**
Vantagens	**Vantagens**
Os resultados são obtidos substancialmente por meio de processos e métricas objetivas	Empregam-se cálculos simples
Grande esforço é requerido para a definição do valor do ativo e da mitigação do risco	Não é necessário determinar o valor monetário do ativo
Uma avaliação custo-benefício é essencial	Não é necessário quantificar a freqüência da ameaça
Os resultados podem ser expressos numa linguagem especificamente gerencial	É mais fácil obter o envolvimento do pessoal não-técnico / segurança
	Flexibilidade no processo e na apresentação de relatórios
Desvantagens	**Desvantagens**
Complexidade de cálculos	É muito subjetiva
Historicamente, só funciona bem com uma ferramenta automatizada e com uma base de conhecido associada	Quase nenhum empenho é requerido para estabelecer um valor monetário para o ativo alvo
Grande quantidade de trabalho preliminar	Não existe base para uma análise custo-benefício da mitigação do risco
Não é apresentado em um nível pessoal	
Participantes não podem ser treinados facilmente durante o processo	
É difícil realizar alterações de direção	
Dificuldade para atendimento de questões fora do escopo	

Fonte: PELTIER (2005, p. 80). Information Security Risk Analysis

Ferramentas disponíveis

Uma das primeiras iniciativas para o desenvolvimento de um padrão em segurança de sistemas foi patrocinada pelo Departamento de Defesa (DOD) dos Estados Unidos.

Em outubro de 1967 o DOD criou um grupo de trabalho para discutir medidas de segurança em computador para proteger informações em sistemas remotos - sistemas computacionais de recursos compartilhados. O relatório final deste grupo de trabalho intitulado *"Security Controls for Computer Systems"* foi publicado em 1970 (USA, 1985).

O esforço empreendido pelo o DOD evoluiu e resultou num documento mais completo chamado "Trusted Computer System Evaluation Criteria" (TCSEC), popularmente conhecido como "Livro Laranja" (*Orange Book*). Os critérios para avaliação da segurança de sistemas de computação definidos neste documento classificam os sistemas em quatro grupos de proteção: D, C, B e A, correspondendo respectivamente à proteção mínima, proteção arbitrária, proteção obrigatória e proteção comprovada.

Os critérios de classificação da segurança dos sistemas de computação definidos pelo DOD têm três objetivos principais (SOARES et al. 1995; p. 472):

- fornecer aos fabricantes um padrão definindo os aspectos de segurança que deveriam ser incorporados aos seus produtos. O DOD pretendia com isto incentivar o desenvolvimento de sistemas, em grande escala, satisfazendo requisitos de segurança para aplicações sensíveis (com ênfase na prevenção contra revelação não autorizada de informações);
- prover os seus órgãos membros com uma métrica para ser usada na avaliação do grau de confiança que pode ser atribuído a um sistema de computação, que será utilizado no processamento de informações classificadas ou outras informações sensíveis; e
- fornecer uma base para a definição dos requisitos de segurança nas especificações de aquisição de equipamento.

Apesar de ter sido escrito para ser utilizado pelos órgãos do governo dos EUA, o Livro Laranja tornou-se um padrão comercial de uso geral. De um lado os fabricantes começaram a utilizar esses critérios para classificar seus produtos, e do outro, os compradores dispunham de um esquema que permitia uma melhor avaliação da segurança fornecida pelos produtos.

O ARBIL (*Asset and Risk Based INFOSEC lifecycle*), ciclo de vida da segurança das informações baseado em bens e riscos, é um modelo de representação do ciclo de vida da segurança da informação para implementação de um plano de segurança e de uma estratégia de gerenciamento de riscos para os recursos de TI. Este modelo gira em torno da proteção dos bens (ativos) e do gerenciamento de riscos, ameaças e vulnerabilidades (HORTON & MUGGE, 2004; p. 4).

O modelo ARBIL é composto por dois círculos inter-relacionados formando uma barreira de proteção em torno dos bens da empresa, conforme mostrado na FIG.7.

O círculo externo do diagrama ARBIL preocupa-se com a qualidade e a consistência do plano de segurança da informação e do programa de gerenciamento de risco. O círculo externo desempenha as seguintes tarefas:

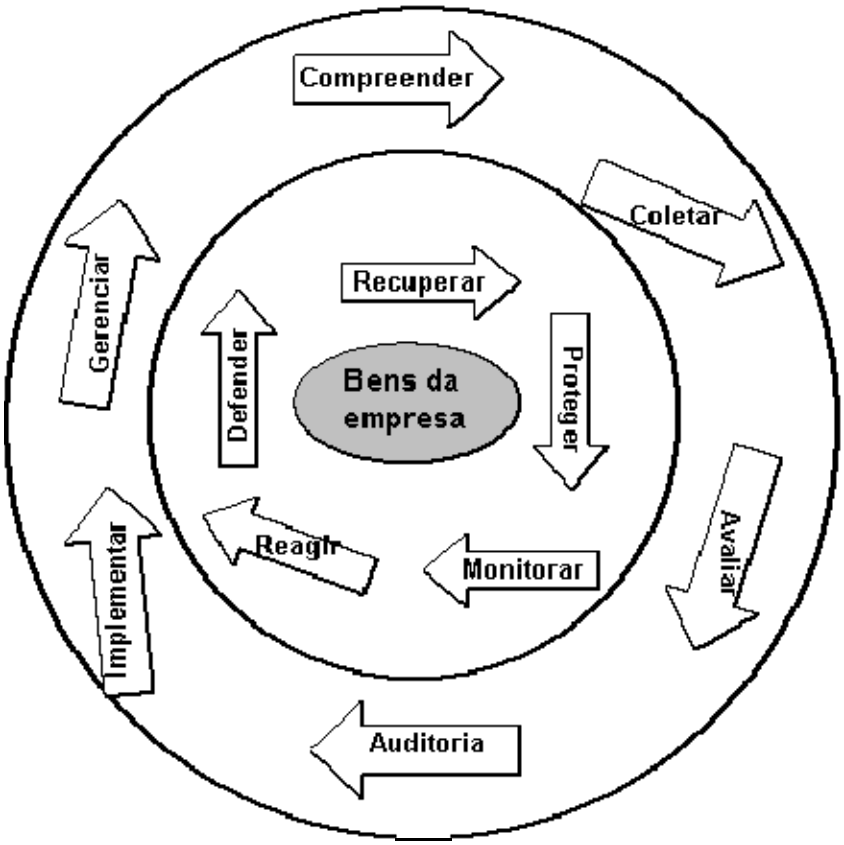


FIGURA 7 - Modelo do processo de segurança ARBIL
Fonte: Horton e Mugge, 2004; p. 5

Compreender – Procura compreender o papel da empresa, de seus produtos e serviços, de seus funcionários, dos locais e departamentos que compõem a empresa, e dos seus bens que a faz funcionar e atingir suas metas e objetivos;

Coletar – Compila as informações sobre recursos organizacionais, incluindo tipos de dados e pessoas, infra-estrutura de rede e computacional, mecanismos de proteção adotados, processos e procedimentos aplicados e ausentes. Esta tarefa é realizada por meio de entrevistas, questionários e pesquisas em documentos em geral;

Analisar – Toda informação deve ser analisada, desde as informações comerciais até a arquitetura computacional e de rede, para determinar quem, o que, quando, onde, por que e como elas estão inseridas no papel da empresa. Essas informações devem ser analisadas considerando-se os mecanismos de proteção e controles de segurança que estão sendo aplicados ou propostos, tanto os de aspectos técnicos como administrativos;

Fazer auditoria – Depois que se está familiarizado com os ambientes e os recursos que fazem parte deles, deve-se realizar uma auditoria abrangente nos mesmos para avaliar a postura da segurança atual;

Implantar – As ações corretivas identificadas devem ser priorizadas e designadas para implementação; e

Gerenciar – Após serem aplicados, os mecanismos de proteção devem ser efetivamente gerenciados usando os princípios do círculo interno do modelo ARBIL.

O círculo interno do diagrama de ARBIL é formado por controles e mecanismos de proteção orientados por ações.

Mecanismos de proteção – Implementar as medidas de proteção, as quais englobam processos, procedimentos, medidas administrativas, *hardware* e *software* para os bens organizacionais;

Monitorar – Auditar e registrar os alertas e dados do sistema;

Reagir – Tomar as providências apropriadas quando da ocorrência de algum incidente de segurança. Preparar recursos para iniciar a defesa e a recuperação em tempo hábil;

Defender – Pode ser necessário adotar medidas reativas de proteção ou de minimização dos danos aos bens; e

Recuperar – Implementar medidas de recuperação e reavaliar as necessidades de segurança.

No círculo interno, se for necessário, a fase de recuperação deve retornar à fase de proteção, embora seu maior esforço seja dedicado a fase de monitoração.

Existem no mercado inúmeras ferramentas e metodologias de análise de risco, tanto comerciais quanto de uso gratuito. Diversas instituições e órgãos regulamentadores da área de TI em todo o mundo desenvolvem métodos de avaliação da segurança da informação para seus afiliados.

Dentre outros órgãos, o NIST (*National Institute of Standards and Technology*) dos Estados Unidos se destaca como uma das mais importantes instituições do mundo, particularmente no que se refere à segurança da informação.

O NIST desenvolveu uma metodologia de análise de risco composta de nove passos, descrita na publicação “NIST SP 800-30” (STONEBURNER et al. 2002), cobrindo todas as etapas do processo de análise e avaliação de risco em sistemas de TI:

- caracterização do sistema;

- identificação das ameaças;
- identificação das vulnerabilidades;
- análise de controles;
- determinação da probabilidade;
- análise de impacto;
- determinação do risco;
- recomendações de controles; e
- documentação dos resultados.

Além do NIST, o *Institute of Risk Management* (IRM, 2002) e o *National Infrastructure Protection Center* (NIPC, 2002) também criaram seus próprios métodos de análise de risco. A Microsoft disponibiliza em seu site o guia de gerenciamento de riscos de segurança - *The Security Risk Management Guide* (MICROSOFT, 2006).

Todas estas ferramentas, com maior ou menor profundidade e respeitando as particularidades das instituições de origem, abordam todos os elementos essenciais para uma análise de risco completa.

O SEI (*Software Engineering Institute*) da Universidade de Carnegie Mellon desenvolveu uma metodologia para avaliação de risco da segurança da informação chamada OCTAVE - *Operationally Critical Threat, Asset, and Vulnerability Evaluation*.

O OCTAVE é uma ferramenta de análise de risco desenvolvida para que a própria organização conduza sua avaliação de risco – denominada “auto-conduzida”. Uma equipe multidisciplinar chamada de “Time de Análise” (TA) formada por representantes das áreas de negócio e do departamento de TI coordena o processo de avaliação.

Desta forma, o OCTAVE vai fornecer uma visão global dos riscos da informação tanto nos aspectos tecnológicos quanto organizacionais.

As atividades do OCTAVE estão organizadas em torno de três fases, que são executadas para examinar os problemas tecnológicos e organizacionais, com o objetivo de montar um panorama geral das necessidades de segurança da informação da organização. Estas atividades são desenvolvidas em uma série progressiva de “workshops”, através da interação de seus participantes (ALBERTS, C. & DOROFEE, 2007; p. 44).

As três fases do método OCTAVE são (ALBERTS et al., 2003; p. 5):

- Fase 1 – Visão (perspectiva) organizacional - Traçar o perfil das ameaças dos ativos. Esta é uma avaliação organizacional dos ativos relacionados à informação e dos mecanismos utilizados atualmente para protegê-los.

  O Time de Análise seleciona aqueles ativos que são considerados mais importantes para a organização (ativos críticos) e descreve os requerimentos de segurança para cada um deles. Finalmente, identifica as ameaças criando um perfil das ameaças para cada ativo;
- Fase 2 – Visão tecnológica – Identificar as vulnerabilidades na infra-estrutura. Esta é uma avaliação da infra-estrutura da informação.

  O TA examina as rotas de acesso à rede, identificando os componentes de TI relacionados a cada ativo crítico - identificados na fase-1. O Time de Análise então determina o grau de resistência a ataques de cada componente; e
- Fases 3 – Desenvolver uma estratégia e planos de segurança. Durante esta parte da avaliação, o Time de Análise identifica os riscos para os ativos críticos da organização e decide o que fazer com eles. Cria, então, uma estratégia de segurança para a organização e os planos de mitigação para tratar estes riscos, com base na análise de todas as informações reunidas nas fases anteriores.

2.13.2. Requisitos Legais

Como já foi dito, os requisitos legais se referem à legislação vigente, ou seja, as leis, estatutos, regulamentos e contratos que a organização, seus parceiros comerciais, contratados e prestadores de serviço têm que atender.

O APÊNDICE A Regulamentação (Leis, Decretos e outros) apresenta uma relação de instrumentos regulatórios, que dizem respeito à administração pública federal do Brasil, no tocante à proteção da informação, as quais o IPEN, como uma instituição de pesquisa vinculada a uma autarquia federal (CNEN), deve obedecer.

2.13.3. Política de Segurança da Informação

O documento da política de segurança da informação deve ser aprovado pela Direção, publicado e comunicado a todos os funcionários e partes externas relevantes. Este documento é a declaração explicita do comprometimento da Direção e estabelece o enfoque da organização para gerenciar a segurança da informação (ABNT, 2005; p. 8).

A definição da política de segurança é um dos primeiros passos para o reconhecimento da importância da segurança da informação na organização e seu tratamento.

De acordo com o TCU (2008), 64% dos órgãos públicos não têm política de segurança da informação. Isso é um indício de que a gestão de segurança da informação é inexistente ou incipiente na maior parte dos órgãos e entidades da administração pública.

A Instrução Normativa GSI nº 1 (BRASIL, 2008b) define Política de Segurança da Informação e Comunicações como sendo um documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

Segundo a FEBRABAN (1998, p. 17), o objetivo da Política de Segurança da Informação é, acima de tudo, explicar o posicionamento da organização com relação ao assunto, além de servir de base para o desenvolvimento das diretrizes de segurança.

Antes de se começar a escrever uma política, deve-se conduzir uma avaliação de risco, identificar os bens que se deseja proteger, e determinar o que se deseja fazer para protegê-los (STANG & MOON, 1994; p. 754).

Uma boa política deve:

- apoiar os objetivos da organização;
- descrever seu programa geral de segurança;
- listar os resultados de sua determinação de risco, com as ameaças que estão combatendo e as proteções propostas;
- definir responsabilidades para a implementação e manutenção de cada proteção; e

- definir comportamentos adequados e inadequados para usuários de modo que o documento seja utilizado no tribunal se ocorrer alguma violação.

Os empregados devem entender que são pessoalmente responsáveis pelo cumprimento das determinações sobre segurança.

De acordo com STANG & MOON (1994; p. 757) um termo de conhecimento e consentimento deve ser assinado por todos os empregados, para garantir que estes têm conhecimento das políticas adotadas, e que foram instruídos sobre as suas responsabilidades.

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 busca 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*".

Delineamento da pesquisa.

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

a) aqueles que se valem das fontes de "papel", onde estão a pesquisa bibliográfica e a pesquisa documental; e
b) aqueles cujos dados são fornecidos por pessoas, o que englobam a pesquisa experimental, a pesquisa *ex-post facto*, o levantamento e o estudo de caso.

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

Por outro lado, o mesmo autor adverte que: *"Esta classificação não pode ser tomada como absolutamente rígida, visto que algumas pesquisas, em função de suas características, não se enquadram facilmente num ou noutro modelo".*

Para YIN (2005, p. 24) a pesquisa exploratória é empregada quando as questões de pesquisa são principalmente do tipo "o que", como no seguinte exemplo: "O que pode ser feito para tornar as escolas mais eficazes?". 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

Um problema é uma questão que mostra uma situação necessitada de discussão, investigação, decisão ou solução (KERLINGER, 1980 apud SOUSA, 2001).

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 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 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 de pesquisas científicas; e
4. gestão inadequada da segurança da informação.

3.4. Método de Diagnóstico e Avaliação

O método de diagnóstico e avaliação proposto neste trabalho é formado por três instrumentos de levantamento de dados, que vão abranger os três níveis hierárquicos organizacionais da organização (estratégico, tático e operacional).

- Nível estratégico

  Instrumento utilizado: "Information Security Governance Assessment Tool for Higher Education (ISG-HE)"[4] - vide APÊNDICE B.

No nível estratégico, o instrumento utilizado é o "Information Security Governance Assessment Tool for Higher Education". 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 método proposto neste trabalho a aplicação do ISG-HE é realizada junto à Alta Direção (Diretor-Presidente) e também junto ao nível gerencial responsável pela segurança da informação na organização. Em organizações com gestão de segurança pouco estruturada, normalmente, a responsabilidade pela segurança da informação fica a cargo do departamento de TI.

Este instrumento pode ainda funcionar como uma forma de conscientização da Alta Direção sobre a necessidade da estruturação formal da segurança da informação, bem como para demonstrar a importância estratégica da informação, o que compreende a TI como um todo (sistemas de informação e comunicação, infraestrutura de rede, e capacitação de pessoas - usuários e administradores, dentre outros).

Em determinados casos, é possível verificar que o Diretor-Presidente da organização não tem conhecimento suficiente do tema para responder

[4] http://www.educause.edu/ir/library/excel/SEC0421.xls

integralmente todas as seções do ISG-HE. Isto poderá ser constatado pela manifestação expressa do respondente ou por grandes disparidades constatadas quando da comparação dos resultados obtidos nas duas avaliações (Diretor-Presidente X Gerência de TI).

Neste caso, os dados obtidos no ISG-HE deverão ser complementados com uma entrevista (conversa). Esta situação deverá ser utilizada pelo avaliador como uma oportunidade singular para prestar esclarecimentos à Alta Direção sobre as questões relativas à segurança da informação de modo geral e dentro do contexto da organização em particular. Isto inclui os benefícios para os processos e atividades de negócio, as leis e regulamentos que a organização deve observar, e situações de risco em geral.

O avaliador deve ter em mente que a conquista da Alta Direção é fator decisivo para o sucesso da implantação da segurança da informação.

Na impossibilidade da realização dessa “conversa” com a Alta Direção, o avaliador deverá consolidar os dados obtidos nas duas avaliações, de modo a formar com bloco único representativo de informações obtidas.

Este trabalho propõe o seguinte método para a realização da consolidação dos dados do ISG-HE:

1) utilizar a seção 1 da avaliação feita pelo Diretor-Presidente; e
2) utilizar as seções de 2 a 5 da avaliação feita pela gerência de TI.

- Nível tático:

  Instrumento utilizado: Entrevista - vide APÊNDICE C.

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

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

- Nível operacional:

  Instrumento utilizado: Questionário - vide APÊNDICE D.

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

O referido questionário é uma adaptação feita do “Instrumento de captura da percepção da segurança da informação” encontrado no trabalho de MARCIANO (2006).

Os aspectos psicológicos envolvidos na aplicação desse tipo de instrumento fogem do escopo da presente pesquisa. Este assunto é abordado em detalhes no supracitado trabalho.

O questionário é 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.

Este questionário pode ainda incluir, dependendo do caso, situações e costumes praticados pelos usuários, dentro do contexto cultural da organização. O objetivo do questionário é mensurar o grau de aderência dos usuários frente às normas de segurança avaliadas, ou seja, como eles se comportam diante das situações de segurança apresentadas.

Como resultado, a aplicação do método de diagnostico e avaliação deve gerar um relatório com os dados obtidos nos três instrumentos de avaliação. Este relatório deve conter também a relação dos sistemas de informação e comunicação mais importantes utilizados nos processos críticos de trabalho da organização, e o principal requerimento de segurança dos mesmos.

Além disso, o relatório deve listar os mais comuns tipos de evento de segurança ocorridos nos últimos doze meses, identificando as possíveis causas.

Por fim, o relatório deverá fornecer uma proposta para a estruturação da segurança da informação na organização, com base nos dados levantados.

Na FIG.8 é mostrado o diagrama da aplicação deste método de diagnóstico e avaliação, onde pode ser visto seus componentes de entrada, o processamento dos instrumentos de coleta de dados e o resultado produzido (saída).

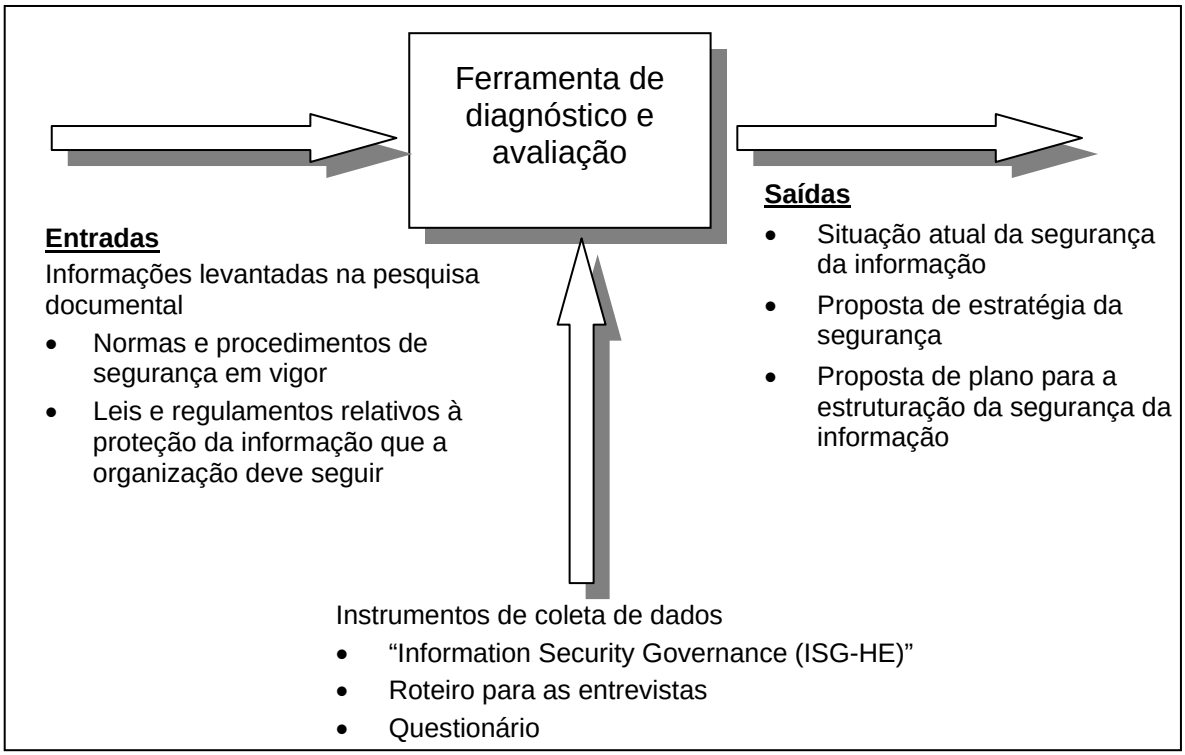


FIGURA 8 - Diagrama do método de diagnóstico e avaliação
Fonte: do autor

Resultados esperados

Ao final do processo de diagnóstico e avaliação da segurança da informação da organização, o avaliador deverá elaborar um relatório contendo todas as informações levantadas na pesquisa documental, com as devidas referências.

O relatório deverá conter ainda os seguintes planos:

1. estratégia para a proteção das informações da organização; e
2. estruturação da segurança da informação;

Maiores detalhes sobre o funcionamento do método de diagnóstico e avaliação são encontrados a seguir na Seção 3.5. IPEN, o caso estudado.

Stan Gatewood, CSO (*Chief Security Officer*) da Universidade da Geórgia (EUA), sugere os seguintes passos para se criar – ou reestruturar – uma estratégia de segurança da informação em uma organização (SCALET, 2006):

1. identifique um executivo líder. Um executivo patrocinador precisa defender a nova estratégia do programa de segurança;
2. selecione uma pessoa principal. O CSO ou outro líder de segurança deve gerenciar diariamente as atividades;
3. defina ou priorize os objetivos. Tente amarrar os objetivos de negócio aos de segurança;

4. estabeleça um mecanismo de revisão. Um processo revisto pela diretoria, por executivos de tecnologia da informação, segurança física, recursos humanos, jurídico, auditoria e pela área de segurança da informação avaliará e aprimorará as iniciativas;
5. estime o estado corrente da segurança. Considere política, processos, sugestões, padrões, tecnologias existentes (*hardware* e *software*), treinamento e educação;
6. estabeleça ou restabeleça, a organização da segurança. O grupo deve ter o foco na segurança das informações, não só as limitações das tecnologias que possui;
7. revise a posição existente e desenvolva novas de acordo com as necessidades. Isso pode incluir uma política aceitável e configuração de segurança mínima para qualquer equipamento da rede;
8. monte times de implementação. Coloque juntos grupos com funções complementares, com funções técnicas e de negócio para orquestrar os planos para as novas políticas, iniciativas, ferramentas e processos;
9. tenha um executivo da diretoria de segurança revisando os planos. Este grupo deve considerar o orçamento, tempo de execução e prioridades;
10. revise as possibilidades técnicas. Isto pode ser feito por um técnico de segurança que represente o departamento do CIO e do CTO, mais o pessoal de operações, serviços de produção e suporte;
11. determine, programe, execute e discuta o que pode ser feito e entregue (implementado). Dê claras responsabilidades individuais e de grupo;
12. coloque toda a equipe de trabalho no plano estratégico. Qualquer membro do departamento de segurança deve estar apto a introduzir e explicar os objetivos do plano de segurança e detalhar como os projetos estão contribuindo para a meta da empresa; e
13. mensure resultados com métricas. As métricas de segurança de TI devem estar baseadas em objetivos que terminem em decisões certas e melhorias de negócio.

3.5. IPEN – O Caso Estudado

O Instituto de Pesquisa Energéticas e Nucleares – IPEN é uma autarquia estadual vinculada à Secretaria de Desenvolvimento do Estado de São Paulo e associada à Universidade de São Paulo – USP na sua finalidade de ensino. Desde novembro de 1982, o IPEN é gerido técnica e administrativamente pela Comissão Nacional de Energia Nuclear – CNEN, órgão vinculado ao Ministério da Ciência e Tecnologia – MCT, do Governo Federal.

Localizado no campus da Universidade de São Paulo, na capital paulista, o instituto ocupa uma área de 500.000 m^2, sendo que seus laboratórios e instalações totalizam 100.000 m^2 de áreas edificadas (IPEN, 2007).

O IPEN é uma instituição de Pesquisas e Desenvolvimento (P&D), Ensino e Produção, que atua nas áreas de Ciência, Tecnologia e Aplicações Nucleares, Biotecnologia, Lasers, Energias Renováveis, Meio Ambiente e Materiais.

De acordo com o Plano Diretor do IPEN (IPEN, 2007), seu quadro de pessoal totalizava, em dezembro de 2006, 1.735 colaboradores, assim constituído: 1.045 (60,23%) Funcionários Públicos Federais, 5 (0,29%) Comissionados, 635 (36,60%) Bolsistas e Estagiários e 50 (2,88%) trabalho voluntário.

Na FIG.9 é mostrado o organograma institucional do IPEN. Como pode ser visto, a estrutura organizacional do IPEN é constituída por um Conselho Superior, formado por membros representantes da USP, FIESP, Secretaria de Desenvolvimento e CNEN; um Conselho Técnico Administrativo – CTA, composto pelo Superintendente da instituição e seus Diretores (5) – Diretoria de Radiofarmácia (DIRF), Diretoria de P&D e Ensino (DPDE), Diretoria de Administração (DAD), Diretoria de Infraestrutura (DI) e Diretoria de Segurança e Radioproteção (DSR), às quais estão subordinadas as Unidades de Pesquisa e Desenvolvimento (Centros de Pesquisa).

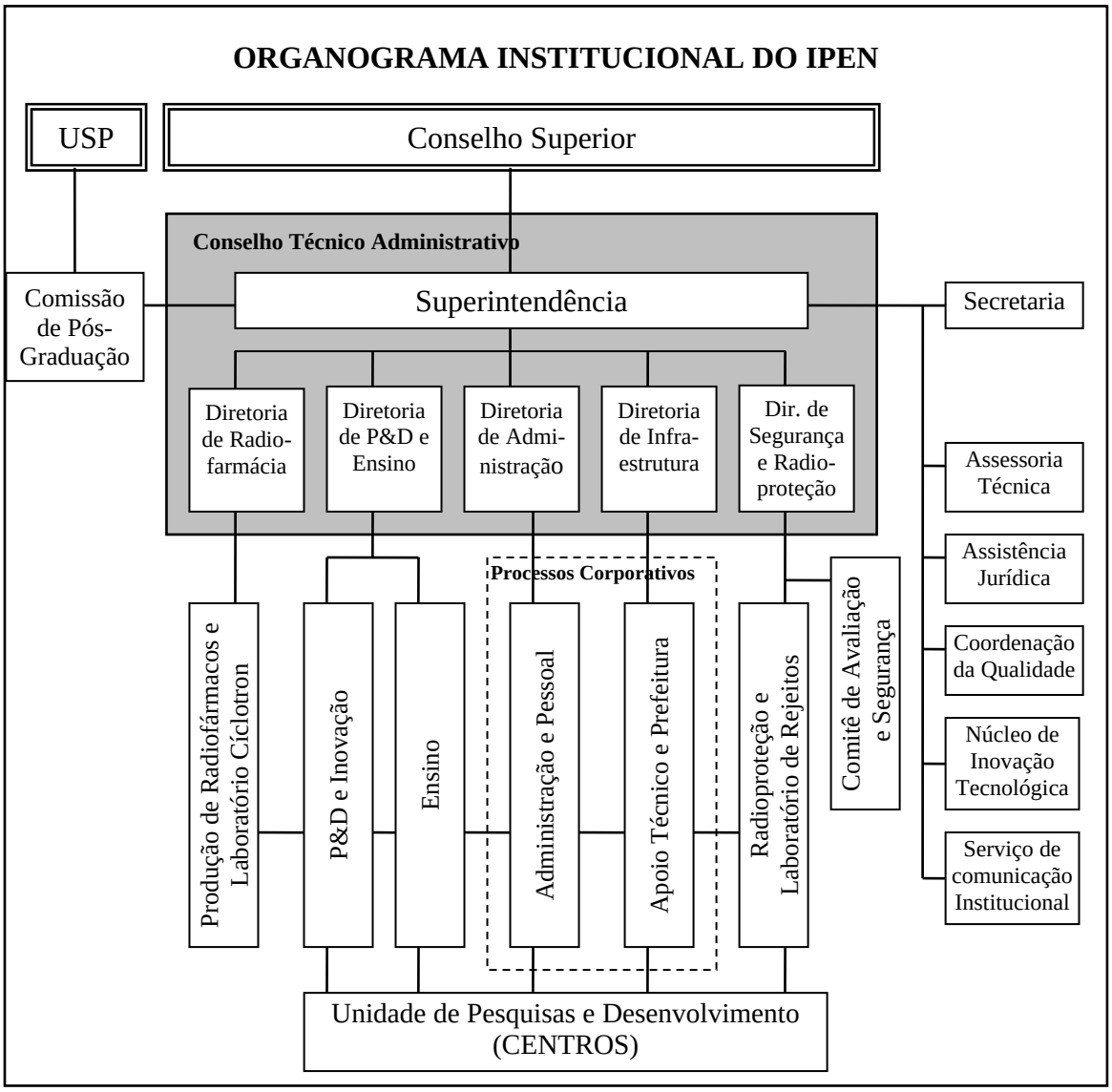


FIGURA 9 - Organograma institucional do IPEN
Fonte: Plano Diretor do IPEN, 2007; p. 13

Os projetos e atividades de P&D da instituição são executados pelos dez Centros de Pesquisas, a saber: Centro de Biotecnologia (CB), Centro de Ciência e Tecnologia de Materiais (CCTM), Centro de Células a Combustível e Hidrogênio (CCCH), Centro de Combustíveis Nucleares (CCN), Centro de Engenharia Nuclear (CEN), Centro de Lasers e Aplicações (CLA), Centro de Metrologia das Radiações (CMR), Centro de Química e Meio Ambiente (CQMA), Centro de Reator de Pesquisa (CRPq) e o Centro de Tecnologias das Radiações (CTR).

O IPEN tem mais duas importantes áreas de atuação: a produção de radiofármacos sob a responsabilidade da Diretoria de Radiofarmácia (DIRF), formada pelo Centro de Radiofarmácia (CR) e o Centro de Aceleradores cíclotron

(CAC); e a função ensino em nível de Mestrado e Doutorado nos campos da Tecnologia Nuclear e áreas correlatas, vinculada à Pós-Graduação da Universidade de São Paulo (USP).

Márcia Orrico Pupak (PUPAK, 2003) faz um relato histórico sobre o IPEN, desde sua criação em 31 de agosto de 1956, incluindo toda sua trajetória vitoriosa que o tornou a principal instituição de pesquisa nuclear do País. A pesquisadora relata com fidelidade e entusiasmo o desenvolvimento da tecnologia nuclear do Brasil, narrando passagens históricas, como a da construção da infraestrutura para a instalação do primeiro reator nuclear de pesquisa do Hemisfério Sul, o IEA-R1.

Este reator foi doado pelo Governo Americano, dentro do Programa Átomos para a Paz.

3.5.1. Informática no IPEN

A atividade de informática do IPEN está descrita no Plano Diretor – Programas e Atividades de 2009, como atividade nº 1320 do programa Administração e Infraestrutura da Diretoria de Administração.

O referido documento descreve os objetivos da informática da seguinte maneira (IPEN, 2009; p. 192):

> *"Planejamento, implantação e gerenciamento de redes de comunicação de dados com garantia da segurança das informações armazenadas e disponibilizadas em servidores de rede institucionais. Atendimento aos usuários na solução de problemas de comunicação, hardware e software. Desenvolvimento, manutenção e evolução os sistemas informatizados com administração dos bancos de dados institucionais"*.

O IPEN conta com uma rede local de computadores onde todas as unidades de pesquisa e administrativas estão interligadas. Segundo a GRS a rede de computadores do IPEN possuía, em junho de 2008, as seguintes características[5]:

- nº de prédios interligados 36;
- forma de interligação ± 10km - fibra óptica;
- nº de pontos de rede ativos ± 1.200;
- forma de interligação (interna) ± 45km-par trançado;
- nº de servidores de rede 15;

[5] Palestra "workshop de Integração GDS/GRS" realizada em 27/06/2008

- nº de usuários cadastrados ± 1.500;
- disponibilidade da rede 7 x 24;
- índice de operação rede/ano 98%.

Na FIG.10 apresenta-se o organograma da Diretoria de Administração do IPEN, onde se pode ver em destaque a Gerência de Redes e Suporte Técnico (GRS) responsável pela segurança da informação na instituição.

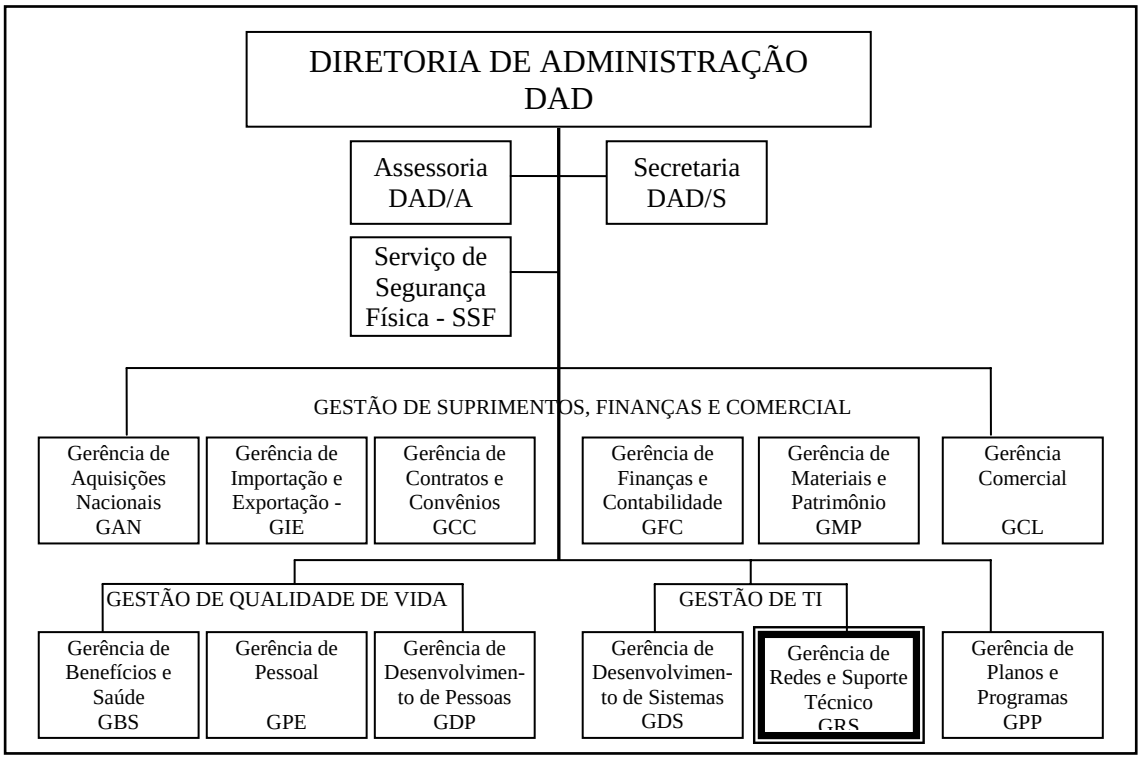


FIGURA 10 - Organograma da Diretoria de Administração do IPEN
Fonte: *Intranet* do IPEN

A tecnologia de informação do IPEN desempenha papel decisivo para a realização das atividades da instituição, seja nos processos de pesquisa e ensino, como nas rotinas administrativas, igualmente importantes para o cumprimento da missão institucional.

Como pode ser visto no APÊNDICE E, todos os sistemas de informação e documentação da instituição fazem uso de TI, seja em rede departamental, *Intranet* (rede local) ou através da *Internet*. Exemplo disso são os sistemas administrativos internos, onde se inclui os sistemas de controle orçamentário, compras e licitação, gestão de estoque e administração de patrimônio; sistemas do Governo Federal (SIASG, SIAFI, SIAPE e SICAF, entre outros), sistema de informação científica (base de dados *online* e periódicos eletrônicos); e sistemas de produção e fornecimento de serviços. Isto demonstra o

alto grau de dependência que o IPEN tem da tecnologia de informação para realizar suas atividades.

De acordo com o Relatório de Gestão do IPEN (IPEN, 2008; p. 57) a disponibilização das informações se dá por meio de sistemas integrados, que permitem acesso simultâneo para diversos usuários, através de uma rede de comunicação de dados, para a execução das tarefas e para a tomada de decisão.

Segundo o relatório supracitado, a segurança das informações armazenadas e disponibilizadas nos servidores de rede institucionais obedece duas perspectivas: Segurança física e Segurança lógica. Quanto à segurança física, destaca-se no *datacenter* (sala de servidores):

a) ambiente monitorado por câmeras (7 x 24);
b) acesso restrito aos administradores de rede;
c) condições de umidade e temperatura controladas;
d) rede elétrica estabilizada;
e) *no-breaks* e gerador instalados; e
f) contratos de manutenção para equipamentos e serviços críticos.

Quanto à segurança lógica destaca-se a existência de:

a) *firewalls* e Sistema de Detecção de Intrusos configurados;
b) sistema corporativo de antivírus;
c) atualizações constantes de versões e correções na plataforma computacional;
d) controle físico de acesso, ou seja, nenhum equipamento consegue conectar-se à rede corporativa e nenhum ponto de rede consegue habilitar-se sem prévia autorização;
e) procedimentos diários e semanais de *backup* dos sistemas institucionais;
f) sistema de contingência (físico e lógico) para o Sistema de Produção de Radiofármacos;
g) sistema de espelhamento para sistemas essenciais (Banco de Dados e *Intranet*);
h) ambiente de testes de novos sistemas separado do ambiente de produção; e
i) impedimento de acesso remoto.

Em 2007, o IPEN investiu na aquisição de um equipamento de grande porte para *backups,* na ampliação da sua capacidade de armazenamento de dados (*storage*)*,* na implantação de um novo *backbone* óptico nos Centros de Pesquisa e na ampliação da rede, interligando todos os prédios do campus à

velocidade de 1GB e substituindo todos os *hubs* da rede por *switches* (IPEN, 2008; p. 58).

Todas as medidas de segurança listadas acima encontram consonância com a Norma ABNT NBR ISO/IEC 27002:2005. Podendo-se destacar entre outros os controles 9.1.1 - Perímetro de segurança física, 9.1.2 – Controle de entrada física, 9.2.2 – Utilidades, 9.2.3 – Segurança do cabeamento, 11.4.5 – Segregação de redes e 11.4.6 – Controle de conexão de rede. Em alguns casos, no entanto, os controles de segurança supracitados não foram implementados integralmente, restringindo-se a um ou outro item (alínea) das diretrizes para implementação.

3.5.2. Pesquisa Documental

Para a elaboração da entrevista e do questionário (usados na Seção 3.6 – Parte experimental) foi realizada uma pesquisa documental nos canais de comunicação oficiais do Instituto (comunicados e *e-mails*, entre outros) com o objetivo de levantar as normas de segurança estabelecidas e devidamente comunicadas.

Na TAB.7 apresentam-se as normas de segurança da informação regulamentadas no IPEN, as quais encontram-se disponíveis na *Intranet* institucional para acesso de todos os funcionários. Neste trabalho, as normas levantadas durante a pesquisa documental foram agrupadas em seis domínios de segurança, a saber: senhas, vírus, recursos computacionais, *e-mails*, *backups*, e propriedade intelectual.

Foi também realizada uma análise de conformidade com a Norma ABNT NBR ISO/IEC 27002:2005, relacionando cada medida de segurança identificada na pesquisa documental com controles estabelecidos pela referida Norma.

Os documentos analisados na pesquisa documental, e referenciados na TAB.7, foram os seguintes (em ordem cronológica):

1. Execução de cópias de segurança das redes de comunicação do IPEN. Publicado por meio da PO-IPN-0502.01, de 04 de março de 1999 (Gestão do sistema da qualidade do IPEN);
2. Recomendações sobre *software*. Divulgado por meio do Comunicado IPEN nº 250, de 26 de novembro de 1999;

3. Regulamento para uso dos recursos computacionais do IPEN. Divulgado na Circular CNEN/IPEN nº 003, de 11 de maio de 2000;
4. Sistema de gerenciamento da documentação controlada. Publicado na PO-IPN-0503.03, de 22 de agosto de 2001 (Gestão do sistema da qualidade);
5. Política interna de proteção à propriedade industrial e à propriedade intelectual da CNEN/IPEN. Divulgado por meio da Circular CNEN/IPEN nº 011, de 24 de dezembro de 2002;
6. Norma para Utilização de Correio Eletrônico na Administração Pública. Recomendação nº 1 da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (Comunicado IPEN nº 012, de 22 de janeiro de 2003);
7. Política de Senhas. Publicado na *Intranet* do IPEN, em janeiro de 2006;
8. Problemas de *Copyright* na Rede do IPEN. Divulgado por meio do Comunicado IPEN nº 031, de 19 de março de 2008; e
9. Alertas de segurança diversos, informados aos usuários via *e-mails*.

A pesquisa documental levantou também os principais processos e sistemas de informação do IPEN, conforme pode ser visto no APÊNDICE E.

TABELA 7- Normas de segurança vigentes no IPEN

Normas de segurança do IPEN		Regulamentos / Documentos			ISO 27002 (práticas)
		Circular 03/2000[6]	Comunic. 12/2003[7]	Outros	
1- Senhas	Criação e uso de senhas: 1. Misture letras maiúsculas com minúsculas; 2. Use Caracteres não alfabéticos tais como: ; ! @ # $ % & * ( ) + = - 0 1 2 3 4 5 6 7 8 9 como parte integrante da senha. 3. Não fixar senhas no monitor, na torre do micro, ou na sua mesa de trabalho (Memorize-a!); 4. É vedada a utilização de senhas de terceiros. 5. Ao ausentar-se da sala onde está seu o microcomputador, aconselha-se a dar sua saída *logout* da rede, para evitar espionagem ou mesmo sabotagem.	Cap. 3.1		Política senhas[8]	11.2.3 11.3 11.3.1 11.3.2 11.5.3
2- Vírus	Amenizar a ação dos vírus: 1. Não abra arquivos anexados em mensagens, a menos que você o esteja esperando receber daquele remetente em particular. 2. Ignorar mensagens de empresas como VIVO e TIM. Idem para fotos de celebridades (ex. Angelina Jolie e Nicole Kidman) 3. Ignore mensagens de órgãos oficiais. Eles não se relacionam com os cidadãos através de mensagens eletrônicas.			*E-mails* 19/04/02 10/09/07 18/02/08	10.4.1

[6] Circular CNEN/IPEN nº 003, de 11 de maio de 2000. Regulamento para uso dos recursos computacionais do IPEN. Disponível na Intranet do IPEN
[7] Comunicado IPEN nº 012, de 22 de janeiro de 2003. Ref. Recomendação nº 1 da Secretaria de Logística e Tecnologia da Informação. Disponível na Intranet do IPEN
[8] Política de Senhas. Disponível na Intranet do IPEN.

TABELA 7- Normas de segurança vigentes no IPEN (cont.)

	Normas de segurança do IPEN	Regulamentos / Documentos			Norma ISO 27002 (práticas)
		Circular 03/2000	Comunic. 12/2003	Outros	
3- Recursos computacionais	Uso da Rede-IPEN / Recursos Computacionais: 1. Toda conta (ex. e-mail, *Windows*) é de responsabilidade e de uso exclusivo de seu titular, não podendo esse permitir ou colaborar com o acesso aos Recursos Computacionais do IPEN por parte de pessoas não autorizadas. 2. Os recursos computacionais do IPEN destinam-se ao uso em atividades de ensino, pesquisa, extensão e serviços; e não devem ser extensivamente utilizados para fins privativos. 3. É vetada a utilização dos recursos computacionais do IPEN às pessoas externas à Instituição, sem vínculo com as atividades do Instituto.	Cap. 2.1.1 Cap. 4.4 Cap. 4.4	Art. 4		11.3 11.5.2 15.1.5 6.2 6.2.1
	Infra-estrutura física: 4. Alterações da infra-estrutura física da rede somente serão permitidas após a análise e aprovação da Gerência de Informática. 5. As identificações dos computadores não devem ser alteradas sem autorização do responsável local ou superior imediato (ex. endereço IP).	Cap. 2.2 Cap. 2.3			10.6 10.6.1 6.1.4
	Segurança 6. Se uma falha na segurança dos sistemas computacionais é detectada, esta deverá ser informada ao administrador do sistema.	Cap. 4.2			8.1.1

TABELA 7- Normas de segurança vigentes no IPEN (cont.)

Normas de segurança do IPEN		Regulamentos / Documentos			ISO 27002 (práticas)
		Circular 03/2000	Comunic. 12/2003	Outros	
4- E-mails	Uso do correio eletrônico corporativo: 1. É proibida a distribuição voluntária ou desapercebida de mensagens não desejadas, como circulares, correntes de cartas ou outros esquemas que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os sistemas computacionais. 2. É vedada tentativa de acesso não autorizado às caixas postais de terceiros.	Cap. 4.1	Art. 11 Art. 07		10.8.1 10.8.4
5- Backups	Copia de Segurança 1. É de responsabilidade de todo usuário realizar e manter cópia de segurança de seus arquivos a fim de evitar que qualquer falha de equipamento coloque a perder o trabalho de vários dias e prejudique os objetivos da instituição.			PO-IPN 0502.01[9] (At. 5.1.2)	10.5 10.5.1

[9] PO-IPN-0502.01. Execução de cópias de segurança das redes de comunicação do IPEN. Disponível na Intranet do IPEN.

TABELA 7- Normas de segurança vigentes no IPEN (cont.)

Normas de segurança do IPEN		Regulamentos / Documentos			ISO 27002 (práticas)
		Circular 03/2000	Comunic. 12/2003	Outros	
6- Propriedade Intelectual	Proteção à Propriedade Industrial 1. É vedada a qualquer pessoa envolvida, direta ou indiretamente, nos processos regulados pela legislação em vigor, a divulgação de informações pertinentes a esse assunto, bem como o trato com terceiros, pessoas físicas ou jurídicas, sem a expressa autorização da direção da Instituição.			Circular 11/2002[10] (Art. 02)	6.1.5 8.1.3
	Gerenciamento de documentação controlada 2. O armazenamento de documentos controlados deve ser feito de modo a minimizar danos, perdas ou deterioração, e de forma que sejam acessíveis por todas as pessoas autorizadas que deles necessitem.			PO-IPN 0503.03[11] (Art. 5.6.4)	11.3 11.3.3
	Direitos Autorais (Copyright) 3. É proibida a instalação, sob qualquer justificativa ou pretexto, de cópias não licenciadas de *software* em equipamento de propriedade da CNEN. 4. É proibido o uso (*download*) de material protegido por *copyright*, tais com *softwares*, músicas, filmes e jogos, entre outros.		Art. 12	Comunic. 250/1999[12] (alínea 1) Comunic. 31/2008[13]	15.1 15.1.1 15.1.2

Fonte: do autor

[10] Circular CNEN/IPEN nº 011, de 24 de dezembro de 2002. Política interna de proteção à propriedade industrial e à propriedade intelectual da CNEN/IPEN. Disponível na Intranet do IPEN.
[11] PO-IPN-0503.03. Sistema de gerenciamento da documentação controlada. Disponível na Intranet do IPEN.
[12] Comunicado IPEN nº 250, de 26 de novembro de 1999. Ref. Recomendações sobre software. Disponível na Intranet do IPEN.
[13] Comunicado IPEN nº 031, de 19 de março de 2008. Problemas de Copyright na Rede do IPEN. Disponível na Intranet do IPEN.

Norma ABNT NBR ISO/IEC 27002:2005

A norma ISO/IEC 27002:2005, bem como sua versão ABNT foi inicialmente publicada como ISO 17799, em 2000. A ISO/IEC 17799:2000 foi homologada com base na Norma Britânica BS7799:1995.

A Norma Britânica BS7799, denominada “Code of Practice for Information Security Management”, por sua vez, baseou-se em outros padrões anteriormente existentes, como “Guidelines to the Management of Information Technology Security (GMITS)”. Sua elaboração teve início em 1987, quando o departamento de comércio e indústria do Reino Unido criou um centro de segurança de informações, o CCSC (*Commercial Computer Security Centre*). O CCSC tinha dentre suas atribuições a tarefa de criar uma norma de segurança das informações para companhias britânicas que comercializavam produtos para segurança de TI através da criação de critérios para avaliação da segurança (CASANAS & MACHADO, 2001; MARCIANO, 2006).

A Norma ABNT NBR ISO/IEC 27002:2005 possui um total 133 controles de segurança, e está estruturada em 15 capítulos, contendo 39 categorias principais de segurança distribuídas em 11 seções de controles de segurança. A referida Norma contém, ainda, uma seção introdutória sobre análise, avaliação e tratamento de riscos.

Na FIG.11 é mostrado o mapeamento das políticas e procedimentos de segurança do IPEN, levantadas durante a pesquisa documental, relacionando-as com as seções de controles de segurança da norma ABNT NBR ISO/IEC 27002:2005.

Na FIG.11 é possível observar, por exemplo, que a seção “Operações”, ou melhor, Gerenciamento das Operações e Comunicações da Norma ABNT NBR ISO/IEC 27002:2005, possui dez categorias de segurança. Dessas dez categorias, quatro foram encontradas dentre as políticas e procedimentos de segurança do IPEN.

A barra à esquerda (mais clara no gráfico / azul) corresponde à quantidade de categorias de segurança que uma determinada seção possui, e a barra à direita (escura / vermelho vinho) representa as categorias, cujos controles de segurança faziam parte das políticas ou procedimentos de segurança do IPEN.

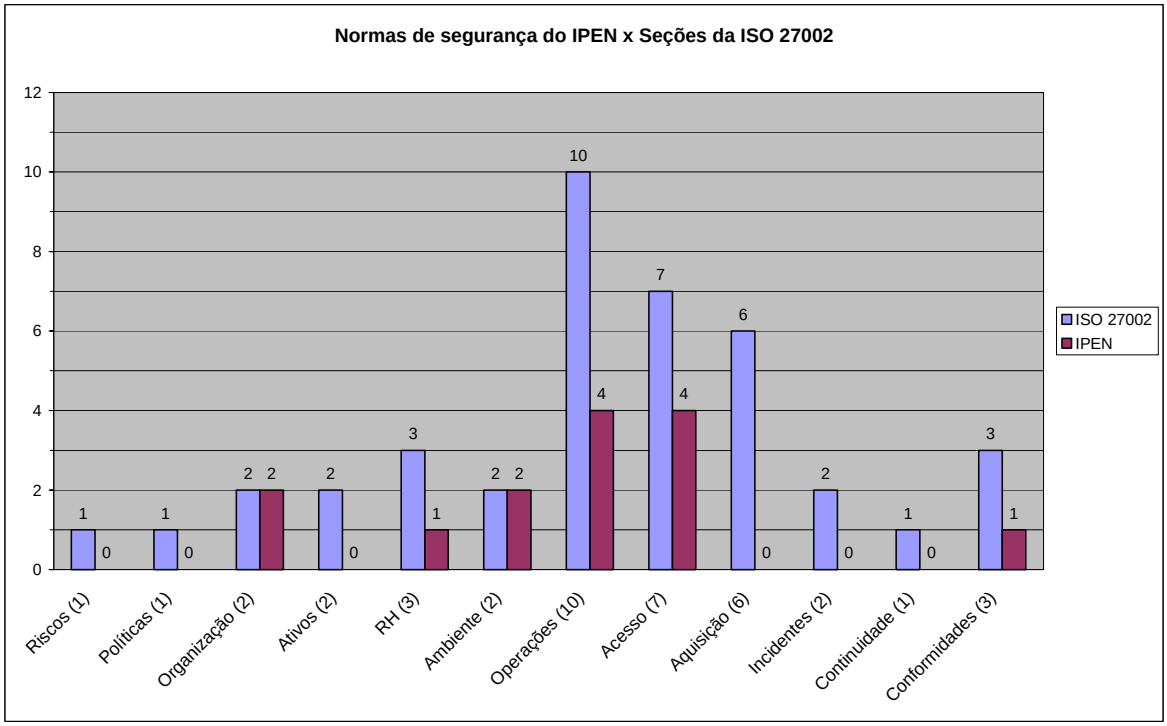


FIGURA 11 - Normas segurança do Ipen X Seções da ISO 27002
Fonte: do autor

Na TAB.8 é apresentada uma análise mais detalhada dos procedimentos de segurança do IPEN e sua consonância com a Norma ABNT NBR ISO/IEC 27002:2005, mostrando o número de categorias de cada seção, e também os respectivos controles, que cada categoria possui (coluna 3). A quarta coluna da TAB.8 refere-se às categorias e controles identificados nas políticas regulamentadas no IPEN, o que correspondendo à FIG.11.

Na TAB.8 pode ser visto que a seção “Organizando a Segurança da Informação” – capítulo 6 da referida Norma, por exemplo, possui duas categorias, que juntas somam onze controles de segurança. Embora a FIG.11 tenha mostrado que as duas categorias de segurança da seção “Organizando a Segurança da Informação” figuravam entre os procedimentos de segurança do IPEN, verificou-se, no entanto, que apenas três controles de segurança, dos onze pertencentes a esta categoria, achavam-se implementados na instituição.

Esta análise revelou ainda a inexistência de controles de segurança em seis das doze seções da Norma (considerando-se também a seção especial Análise, avaliação e o tratamento de riscos).

TABELA 8 - Normas segurança do IPEN X Categorias de segurança da ISO 27002

Norma ISO 27002:2005			IPEN
Capítulo	**Seção de controles**	**Categorias / Controles**	
4	Análise/avaliação e tratamento de riscos (seção introdutória)		
5	Políticas de Segurança da informação	1 / 2	
6	Organização da Segurança da informação	2 / 11	2 / 3
7	Gestão de ativos	2 / 5	
8	Segurança em Recursos humanos	3 / 9	1 / 2
9	Segurança Física e do Ambiente (sala de servidores)	2 / 13	2 / 4
10	Gestão das Operações e Comunicações	10 /23	4 / 5
11	Controle de Acesso	7 / 25	4 / 8
12	Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	6 / 16	
13	Gestão de Incidentes de Segurança da informação	2 / 5	
14	Gestão da Continuidade do Negócio	1 / 5	
15	Conformidades	3 / 10	1 / 3
Totais de categorias / Controles		**39 / 133**	**14 / 25**

Fonte: do autor

Com base nesses dados, é possível fazer as seguintes inferências:

Políticas de Segurança da Informação:

Segundo a Norma ABNT NBR ISO/IEC 27002:2005, o objetivo da política de segurança da informação é fornecer uma orientação aos usuários e mostrar o comprometimento e apoio da direção para a segurança da informação de acordo com os requisitos de negócio e com as leis e regulamentos relevantes.

Embora tenha sido identificado, durante a pesquisa documental, um conjunto de procedimentos de segurança da informação no IPEN, não se pode, contudo, classificá-lo como política de segurança.

A Norma ABNT NBR ISO/IEC 27002 (2005, p.8) considera que o documento da política de segurança da informação contenha, por exemplo:

- uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento de informação;
- uma estrutura para estabelecer os objetivos de controles e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco;

- definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação; e
- que a mesma seja analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Organização da Segurança da Informação

Com respeito à seção “Organização da Segurança da Informação”, as suas duas categorias de segurança contemplam um total de onze controles. Foram identificados como procedimentos de segurança do IPEN três deles, sendo um controle pertencente à categoria “Infraestrutura de segurança da informação” e dois da categoria ”Partes externas”.

Segurança em Recursos Humanos

A seção “Segurança em Recursos Humanos” é composta por três categorias de segurança, que juntas somam nove controles. Nos procedimentos de segurança adotados pelo IPEN verificou-se a presença dos controles 8.1.1 – Papéis e responsabilidades e 8.1.3 – Termos e condições de contratação.

Gestão das Operações e Comunicações

De um total de 32 controles distribuídos de dez categorias, cinco foram encontrados como práticas oficialmente regulamentadas no IPEN.

Controle de Acesso

A Norma ABNT NBR ISO/IEC 27002:2005 define vinte e cinco controles de acesso em sete categorias de segurança diferentes. Desses, seis foram identificados no IPEN.

Conformidades

O IPEN adota três dos dez controles de segurança da seção 15 da Norma ABNT NBR ISO/IEC 27002:2005.

Não foram encontrados procedimentos de segurança no IPEN relativos a cinco seções, são elas: (1) Política de segurança da informação; (2) Gestão de ativos; (3) Segurança física e do ambiente (implementado apenas na sala de servidores, vide Seção 5.1. Informática no IPEN); (4) Aquisição, desenvolvimento e manutenção de sistemas de informação; (5) Gestão de incidentes de segurança da informação; e (6) Gestão da continuidade do negócio.

Entretanto, é possível atestar a existência de alguns controles pertencentes a estas seções. São exemplos disso os controles de “Inventário dos ativos” e “Uso aceitável dos ativos” (Gestão de ativos); “Proteção dos dados para teste de sistema” e “Controle de acesso ao código-fonte de programas” (Aquisição, desenvolvimento e manutenção de sistemas de informação); e “Registro de ocorrências” (Gestão de incidentes de segurança da informação).

Por outro lado, em muitos casos, controles estabelecidos nas políticas ou presentes no ambiente IPEN não foram implementados na sua íntegra, estando restrito a apenas alguns itens das diretrizes de implementação estabelecidas na referida Norma.

3.5.3. Leis e Regulamentos

Vide APÊNDICE A para uma relação de leis e decretos do Governo Federal Brasileiro acerca da segurança da informação nos órgãos públicos.

3.6. Parte Experimental

Este trabalho foi elaborado com base numa pesquisa exploratória, que buscou verificar as percepções dos usuários de sistemas de informação (gestores e funcionários) do Instituto de Pesquisas Energéticas e Nucleares – IPEN, com referência à segurança da informação.

Foram utilizados três instrumentos de coleta de dados (vide Seção 3.4. Método de Diagnóstico e Avaliação). A coleta de dados aconteceu no período de julho a dezembro de 2008, e contou com a participação total de 169 pessoas, assim distribuídas:

1º. ISG-HE – superintendente da instituição e gerência 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, disponível em <http://audacity.sourceforge.net/?lang=pt>. A versão utilizada foi a 1.2.6 em plataforma “Windows”.

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

O resultado da análise dos dados coletados será apresentado no CAPÍTULO 4. Resultados e Discussão, a seguir.

4. RESULTADOS E DISCUSSÃO

A seguir serão apresentados os resultados e discussão da análise da pesquisa realizada:

4.1. Nível Estratégico – ISG-HE

O instrumento de avaliação “ISG Assessment Tool for Higher Education” é destinado aos altos executivos da organização ou representantes destes. No IPEN a ferramenta foi submetida à superintendência, instância máxima da administração da instituição, e a gerência de TI (responsável pela segurança da informação no IPEN).

A ferramenta ISG-HE é composta 100 questões divididas em cinco seções (dependência organizacional da tecnologia da informação, gestão de risco, pessoas, processos e tecnologia).

A pontuação obtida na seção 1 (dependência de TI) define grau de dependência de tecnologia da informação da organização. As pontuações relativas às seções subseqüentes, ou seja, gestão de risco, pessoas, processos e tecnologia, são consolidadas em um quadro resumo para se determinar o resultado global da avaliação. Este resultado pode variar de organização para organização de acordo com as características verificadas na seção-1 da ferramenta.

A ISG-HE utiliza as TAB.9 e TAB.10 como referência para os valores computados na seção 1 e nas demais seções (2 a 5), respectivamente, para calcular o resultado global da avaliação.

TABELA 9 – ISG-HE- Nível de dependência de TI

Menor	Maior	Dependência
0	8	Muito Baixa
9	16	Baixa
17	32	Média
33	48	Alta
49	64	Muito Alta

Fonte: ISG-HE

TABELA 10 – ISG-HE - Avaliação global da segurança

Dependência da TI	Pontuação da Segurança da Informação		Avaliação Global
Muito Alta	0	199	Pobre
	200	274	Necessidade de Melhorias
	275	336	Boa
Alta	0	174	Pobre
	175	249	Necessidade de Melhorias
	250	336	Boa
Média	0	149	Pobre
	150	224	Necessidade de Melhorias
	225	336	Boa
Baixa	0	124	Pobre
	125	199	Necessidade de Melhorias
	200	336	Boa
Muito Baixa	0	99	Pobre
	100	174	Necessidade de Melhorias
	175	336	Boa

Fonte: ISG-HE

Durante a análise dos dados obtidos nas duas avaliações (superintendência e gerência de TI), reproduzidos na TAB.11, foi constatada a existência de disparidades importantes entre os valores apresentados. O item “gestão de risco”, por exemplo, na avaliação da gerência de TI, apresentou pontuação zero (0), o que significa dizer que não existe nenhuma implementação relativa a esta prática de segurança da informação na instituição.

TABELA 11 - Comparativo entre as duas avaliações

Seções	**Superintendente**	**Gerência de TI**
Dependência de TI	**34**	**24**
Gestão de risco	24	0
Pessoas	48	5
Processos	79	36
Tecnologia	-	25
Total de pontos	**151**	**66**

Obs.: A seção 5, tecnologia, da avaliação do Superintendente não foi preenchida pelo referido respondente, que alegou não possuir conhecimento suficiente sobre o assunto.

Na TAB.12 mostra-se a consolidação dos dados do “ISG Assessment Tool for Higher Education” na avaliação realizada pelo superintendente e pela

gerência de TI do IPEN, conforme recomenda a Seção 3.4. Método de Diagnóstico e Avaliação, ou seja:

a. utilizar a seção 1 da avaliação feita pelo Diretor-Presidente; e
b. utilizar as seções de 2 a 5 da avaliação feita pelo responsável pela segurança (gerência de TI).

TABELA 12 - 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 (TAB.12), verificou-se que o grau de dependência da instituição com relação à tecnologia da informação obteve **34** pontos, ficando situado na faixa entre 33 e 48 da TAB.9. Esta pontuação corresponde a uma dependência de TI elevada (**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 o IPEN numa situação "**pobre**" no que se refere à gestão da segurança da informação, de acordo com o quadro de referência da TAB.10.

Quando se analisa, individualmente, a pontuação obtida em cada uma das seções da ferramenta ISG-HE, verifica-se que a seção 5 (tecnologia) apresentou 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. Nível Tático - Entrevistas

4.2.1. Análise Quantitativa

Para a realização da entrevista as normas de segurança em vigor no IPEN (levantadas por meio da pesquisa documental – subseção 3.5.2) foram agrupadas em seis domínios de segurança, a saber: senhas, vírus, recursos computacionais, *e-mails*, *backup* e propriedade intelectual.

Na TAB.13 sumariza-se, em termos percentuais, as resposta obtidas dos dez entrevistados relativas à Pergunta 1 (nos seis domínios de segurança avaliados): *"Senhor (a) Gerente, os funcionários deste Centro de Pesquisa têm conhecimento da política do IPEN para o referido domínio de segurança?"*.

TABELA 13 - Percentuais de conhecimento da normas

	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.12 é mostrado o número total de "SIM" e "NÃO" relativos à TAB.13 e o percentual que cada um representa. Ela mostra que no geral as políticas de segurança do IPEN são conhecidas por 63,33% dos funcionários.

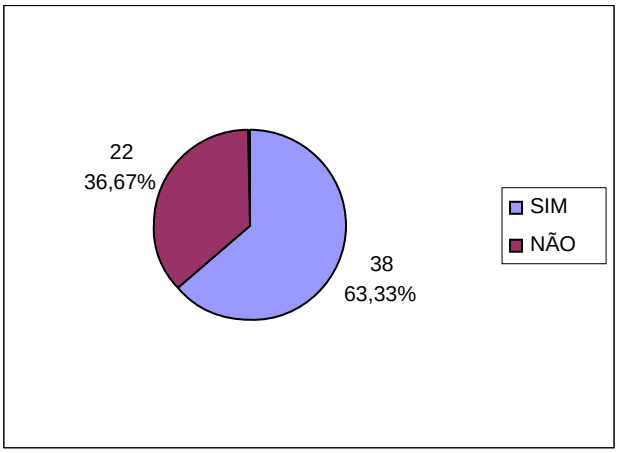


FIGURA 12 - Conhecimento das políticas

Por outro lado, analisando-se os seis domínios de segurança separadamente, os dados apresentados na TAB.13 mostraram 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 TAB.13 mostrou ainda que as normas e procedimentos de segurança para a utilização dos recursos computacionais da instituição obtiveram o melhor índice de conhecimento perante os usuários de sistemas de informação, alcançando o percentual de 90%.

Este percentual relativo ao conhecimento das normas e procedimentos para a utilização dos recursos computacionais tem a influência do instrumento regulatório ”Regulamento para uso dos recursos computacionais do IPEN” - Circular CNEN/IPEN nº 003/2000.

Para a segurança da informação, igualmente importante são as ações desencadeadas a partir dos instrumentos regulatórios. Neste particular merece destaque a atuação da GRS (Gerência de Redes e Suporte Técnico) no estabelecimento de regras para o cumprimento do regulamento supracitado. Entre as ações implementadas pela GRS estão os controles de segurança para a conexão de equipamento na rede de computadores, o que só é permitido mediante verificação se o mesmo possuir *software* licenciado, e compatível com o ambiente corporativo.

Além disso, o equipamento deve está patrimoniado, ou ter autorização expressa do responsável da unidade, declarando sua procedência (projeto de pesquisa ou propriedade pessoal).

Outro controle implementado pela GRS é administrar a liberação de endereços IP’s sob demanda, associando cada endereço IP liberado ao endereço MAC (físico) do equipamento que vai utilizá-lo.

A pontuação relativa às perguntas 2, 3, 4 e 7 (adicional) está sumarizada na TAB.14.

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 7 (adicional): *"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. 14 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 14 - 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.14 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.15). 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 escala de referência - TAB.15);

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 15 - 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

4.2.2. Análise qualitativa

A idéia de segurança da informação predominante na instituição pode muito bem ser retratada a partir dos três depoimentos que se seguem:

a) *"... eu não conheço a política de segurança do IPEN... Eu estou aqui há 20 anos... e eu não me lembro de saber qual é a política de segurança do IPEN".* (Entrevistado E).

b) *"... Em casos gerenciais, eu acho que seria muito importante... (importância de uma política de senhas)... para usar e-mail eu acho que não..."* (Entrevistado H).

c) *"... Integridade e disponibilidade são extremamente importantes... e a segurança também... tem informações ali que são confidenciais..."* (Entrevistado F).

O primeiro depoimento indica que os funcionários, de forma geral, não têm conhecimento da política de segurança da informação da instituição. No segundo discurso nota-se uma minimização da importância das informações usadas nas atividades rotineiras, ou seja, aquelas que estão no microcomputador do usuário. Tem-se a sensação que informações importantes são aquelas que estão contidas nos grandes sistemas de informação gerenciais da instituição.

Já no terceiro depoimento percebe-se uma noção errônea de segurança da informação. O Entrevistado F passa a idéia de que segurança da informação significa confidencialidade.

Esta visão de segurança relacionada com a confidencialidade da informação reaparece em outros depoimentos. Isto os fazem acreditar que a segurança da informação seja necessária apenas quando a confidencialidade é o principal requerimento de proteção da informação.

Neste aspecto, a entrevista revelou que o principal requerimento de segurança das informações institucionais é a **integridade**, seguida de perto pela

disponibilidade. Na opinião dos gerentes ouvidos, a confidencialidade não é um requerimento de segurança importante para as informações da instituição.

Dois gerentes consideraram que os três requerimentos de segurança (integridade, disponibilidade e confidencialidade) são igualmente importantes; e um dos entrevistados disse: *"Não vejo nada que viole a segurança da informação não"*.

Apesar de a integridade ter sido eleito principal requerimento de segurança da informação, foi a disponibilidade que produziu os maiores discursos em seu favor:

> *"... eu preciso que meu sistema opere 24hs... de sábado, domingo... meia noite... eu não quero saber se ele está no IPEN... se ele está no Canadá... se ele está na Coréia... o importante é que... a hora que eu abro o meu micro a informação esteja disponível..."* (Entrevistado C).
>
> *"... é um horror quando você chega aqui e não tem rede... então ninguém consegue trabalhar porque não tem rede..."* (Entrevistado H).

Quando perguntado sobre os ativos de informação mais importantes para as atividades da casa, os sistemas mais citados foram o **correio eletrônico** (com oito indicações); as **bases de dados da biblioteca** (com quatro indicações); e o **sistema de produção da DIRF** - Diretoria de Radiofarmácia (três indicações).

Os pronunciamentos em defesa da importância desses sistemas de informação incluíram os seguintes discursos:

a) *"... hoje sem o e-mail a gente não vive!... alias é a coisa mais importante no IPEN no momento...* por exemplo... *eu me comunico com o Superintendente... com os gerentes... com os funcionários..."* (Entrevistado E).

b) *"... uma das informações mais importantes hoje são os e-mails... isso é inegável. É importante porque é por ele que você recebe todos os inputs da casa..."* (Entrevistado H).

c) *"... pra mim isso é a maior modernidade que existe no mundo... não existe coisa melhor..."* (Entrevistado G) – sobre as bases de dados da biblioteca.

d) *"... não só o sistema de produção (da DIRF)... como também a interface com o SAC (Depto. Comercial)... emissão de documentos... isso não dá pra você imaginar..."* (Entrevistado C).

Foram ainda citados os seguintes ativos de informação: informações do Centro de Pesquisa, pessoas, sistema de requisição e compras, *Internet*, rede de computadores, *Windows Office,* SIGEPI e sistema da qualidade (SGI e TNCMC).

Ainda com relação aos sistemas de informação, houve também quem se queixasse deles, como por exemplo, da página da *Internet* do IPEN e do correio eletrônico:

a) *"... a página do IPEN hoje é uma tragédia... eu diria que é uma tragédia porque nós somos responsáveis pela informação que tá disponibilizada... mas infelizmente... por uma questão cultural... acho que a gente não dá importância para esse canal de comunicação. A instituição faz muito mais do que você consegue visualizar (através da página web)... ela não espelha a realidade... os dados são desatualizados... as informações não são adequadas..." (Entrevistado C).*

b) *"... a página do IPEN não serve para nada... não tem informações adequadas. A casa está perdendo uma grande (oportunidade)..."* (Entrevistado E).

c) *"... eu acho que melhorou bastante (e-mail)... agora se conseguisse segurar mais um pouco o SPAM..."* (Entrevistado G).

d) *"... a quantidade de mensagem (tamanho permitido) que eu posso mandar... esse é um grave problema para gente... que muitas vezes tem que mandar uma apresentação... então você tem que::: pegar seu documento e fatiar em três ou quatro... isso é um problema". "... enquanto nos e-mails aí fora... GMAIL... ou BOL você manda documentos extremamente robustos e não retornam..."* (Entrevistado C*).*

A entrevista procurou saber que outras medidas de segurança o IPEN deveriam adotar, além daquelas discutidas nos seis domínios de segurança avaliados. As principais sugestões dadas pelos gerentes foram:

- Controlar o acesso ao espaço físico dos laboratórios.

  "... chega um visitante, sabe-se lá de onde, você já mostra tudo. Você não dá acesso ao seu computador, mas você dá acesso às informações do seu trabalho" (Entrevistado A).

- Segurança no desenvolvimento de sistemas

  "... essas empresas que desenvolvem softwares... são empresas pequenas... amanhã desaparece a empresa... como vai ficar a manutenção desses sistemas?... os programas fontes não nos pertencem!..." (Entrevistado C).

- Restringir o acesso à *Internet*

  "... o pessoal grava muita coisa da Internet... eu vejo no meio de expediente eles gravando coisas... isto o IPEN deveria restringir mais... é abusivo..." (Entrevistado G).

  "... controlar o que as pessoas estão acessando... o Orkut, por exemplo..." (Entrevistado H).

  "... não se pode permitir que as pessoas utilizem uma coisa institucional para baixar esse tipo de documento (músicas e filmes)" (Entrevistado C).

- Treinamento

> *"... as falhas que ocorrem estão mais ligadas às pessoas que transitam por aqui... estagiários.. alunos... que não têm vínculo... aí eu acho que é mais frágil. Uma sugestão seria que quando da matrícula... ou quando do credenciamento... recebessem uma apostila informando."* (Entrevistado J).

Quanto ao treinamento e conscientização dos usuários para melhorar a efetividade das políticas de segurança, os entrevistados apontaram as seguintes ações (por ordem decrescente de citação):

1º. palestras;

2º. envio de *e-mails* informativos;

3º. elaboração de manual de boas práticas, colocando as conseqüências, os perigos e riscos, que o usuário corre quando não adota procedimentos adequados;

4º. criação de *folder* mostrando qual é o comportamento que o usuário deve seguir no uso dos recursos computacionais e sistemas de informação;

5º. notas de esclarecimentos (afixadas nos quadros de avisos); e

6º. treinamento

Os incidentes de segurança, ocorridos nos últimos doze meses, relatados pelos entrevistados foram:

- roubo de computador contendo informações sigilosas de projeto de pesquisa;
- rompimento de fibra ótica deixando o Centro de Pesquisa isolado da rede corporativa de dados;
- princípio de incêndio ocasionado por computador ligado durante a noite;
- perda de dados por mau dimensionamento da base de dados quando do desenvolvimento do sistema;
- mensagem de e-mail ofensiva / difamatória contra funcionário;
- utilização de *softwares* não licenciados (computador de bolsista);

Sobre o tratamento dado pelo IPEN por ocasião dos incidentes de segurança, os entrevistados foram unânimes em afirmar que não foi desenvolvido nenhum procedimento formal que possa evitar que os mesmos tornem a acontecer.

Os dados apresentados, coletados nas entrevistas realizadas com dez gerentes de Centros de Pesquisa do IPEN, mostraram que as pessoas não têm a percepção de que as informações contidas no seu microcomputador são importantes para a instituição – para o desenvolvimento das suas atividades.

Informações como *e-mails* trocados com parceiros, documentos diversos do *Word*, planilhas eletrônicas, relatórios, material de pesquisa e tantas outras parecem ter uma importância menor quando o assunto é segurança da informação.

Este fato leva o usuário a negligenciar os procedimentos de segurança estabelecidos para a preservação deste tão importante repositório de informações institucionais, que é o computador pessoal de cada colaborador. O que vai se traduzir em uma situação de risco para essas informações.

Os gerentes ouvidos mostraram-se mais preocupados com a preservação das informações ditas gerenciais, ou seja, informações relacionadas ao nível estratégico da instituição. Estas são informações providas pelos sistemas gerenciais, como, por exemplo, sistema de gestão da qualidade, SIGEPI (Sistema de Informação Gerencial e de Planejamento do IPEN) e outros que utilizam o banco de dados institucional.

É importante salientar que, em geral, dados coletados em levantamentos desse tipo, principalmente, por meio de entrevistas traduzem a percepção pessoal do entrevistado sobre o fato pesquisado.

Para melhor compreender os resultados obtidos, é necessário considerar em que circunstâncias os dados foram coletados, tais como, o período em que o levantamento foi realizado, abordagem e formulação das questões, as características dos participantes, entre outras.

Esses dados, em boa parte, representam a opinião das pessoas, portanto, possuem uma forte dose de julgamento individual.

Em razão da própria simplicidade do Método de Diagnóstico e Avaliação apresentado neste trabalho de pesquisa (Seção 3.4), é possível que a veracidade de algum dado mostrado aqui possa ser questionada.

O referido Método de Diagnóstico e Avaliação não tem a intenção de fazer uma investigação profunda da situação da segurança da informação. Esta tarefa deverá ser realizada com a implementação de uma ferramenta de análise, avaliação e tratamento de risco.

4.3. Nível Operacional - Questionário

O questionário foi aplicado durante o ciclo de palestras “Utilização do e-mail do IPEN”, realizado por este autor, no período de 22 de setembro a 06 de outubro de 2008.

Na TAB.16 é mostrado que participaram 157 usuários da pesquisa, de doze diferentes unidades organizacionais do IPEN (Centros de Pesquisa e Diretorias), o que corresponde a 10,2% dos 1532 usuários cadastrados na rede do IPEN naquela ocasião.

TABELA 16 - Participantes da pesquisa - questionário

Centro de Pesquisa	Participantes
CB	17
LRR	07
CQMA	15
CCTM	6
CR	10
CCN	18
CRPq	21
CMR	19
SRP	07
CEN	11
PCI e DAD	15
CAC	11
Total	**157**

Os gráficos mostrados nas FIGURAS 13 a 17 representam o perfil dos usuários da amostra pesquisada relativo à aplicação do questionário, caracterizada por sexo, faixa etária, tempo de serviço no IPEN, vínculo empregatício e grau de instrução.

Na FIG.13 é mostrado que do total de 157 usuários que responderam o questionário, 109, ou seja, 69,43% deles eram homens e 48 (30,57%) eram mulheres.

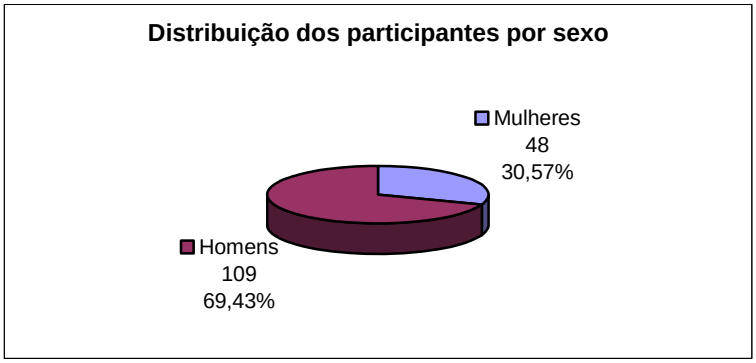


FIGURA 13 – Amostra - distribuição por sexo

Quanto à faixa etária (FIG.14), os participantes deste terceiro instrumento de coleta de dados estavam assim distribuídos: 87,26% tinham 40 ou mais anos; 9,55% tinham idade inferior a 30 anos, e 3,18% estavam entre 30 e 39 anos.

Observa-se que a somatória dos percentuais apresentados na referida figura é de 99,99%. Isto acontece em função do arredondamento realizado pelo *software* utilizado na geração dos gráficos (*Microsoft Excel*). Este arredondamento de 0,01% pode ocorrer para menos ou para mais, como é o caso da FIG.15, que totaliza 100,01%.

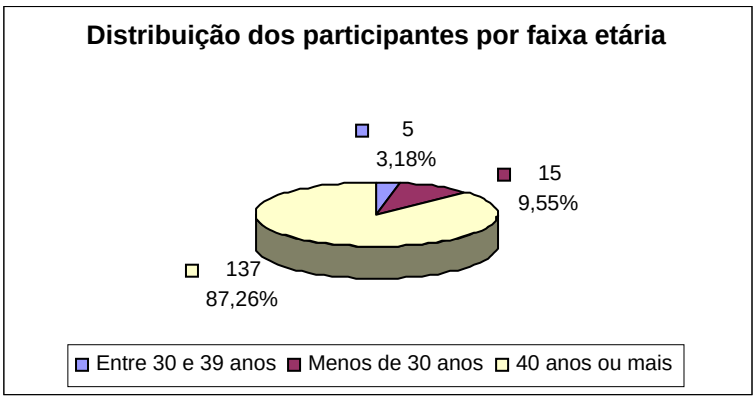


FIGURA 14 – Amostra - distribuição por faixa etária

A FIG.15 corresponde ao tempo de trabalho na instituição: 69,43% dos pesquisados trabalhavam no IPEN há mais de 20 anos, 15,29% estavam na instituição por um período entre 10 e 20 anos, e os outros 15,29% haviam sido contratados há menos de 10 anos.

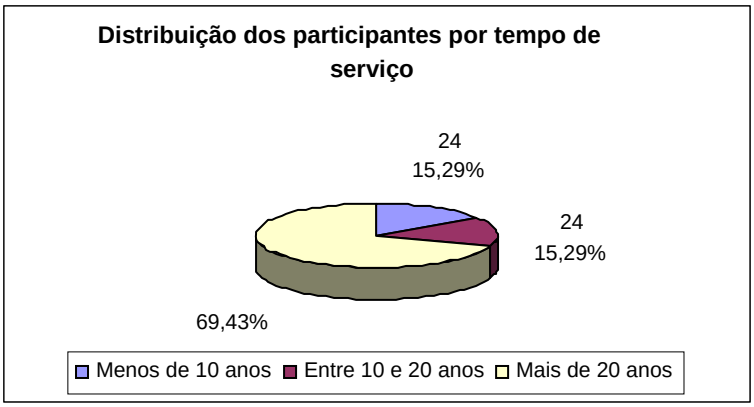


FIGURA 15 – Amostra - distribuição por tempo de serviço

Com relação ao vínculo empregatício, FIG.16, 89,17% pertenciam ao Regime Jurídico Único do Governo Federal, e 10,83% correspondiam aos demais tipos de vínculo indicados, isto é, comissionado, bolsista / estagiário, trabalho voluntário e prestador de serviço.

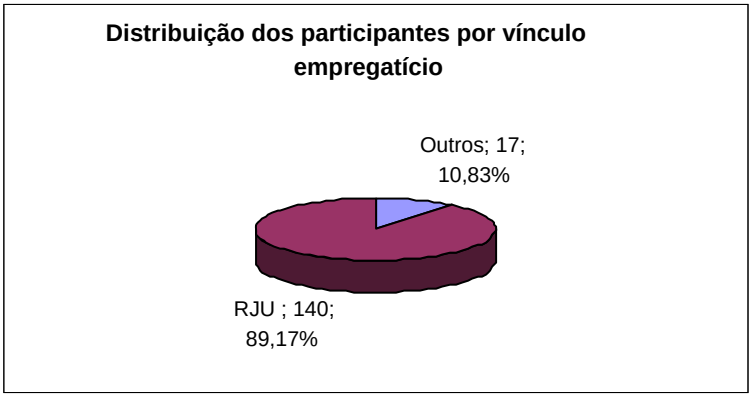


FIGURA 16 – Amostra - distribuição por vínculo empregatício

De acordo com a FIG.17, a amostra pesquisada foi constituída por 51,59% de mestre ou doutores, 19,75% de usuários com nível superior completo, 5,73% de especialistas e 22,93% outros graus de instrução indicados no questionário (superior incompleto, ensino médio e fundamental).

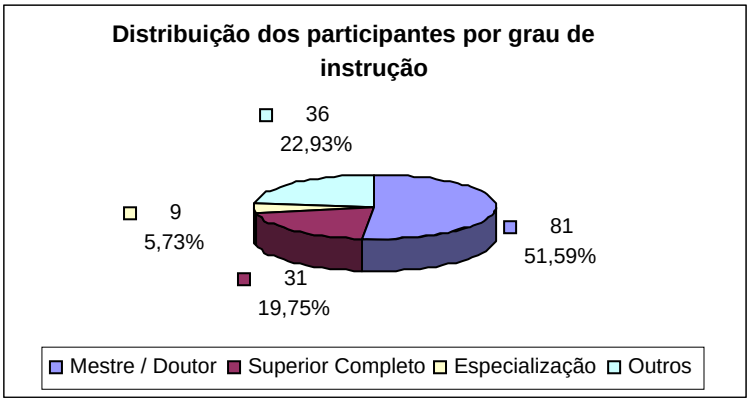


FIGURA 17 – Amostra - distribuição por grau de instrução

Conforme pode ser visto no APÊNDICE D, o questionário utilizado continha quatro alternativas de resposta (sempre, freqüentemente, raramente, nunca) para cada questão formulada. O respondente deveria escolher a opção que melhor expressasse o seu comportamento diante de cada questão apresentada.

Para realizar a estratificação dos dados foi atribuído um peso numérico, de 1 a 4, para cada resposta fornecida, onde “4” representava a opção mais adequada, ou seja, o comportamento considerado aceitável, e “1” representava o comportamento indesejado, prejudicial à segurança da informação, e também uma violação da norma estabelecida.

Desta forma, na questão número 1, por exemplo, “*Utilizo senhas fáceis de lembrar (compostas por nomes ou suas iniciais, datas de aniversários, seqüências de letras ou números)*”, as alternativas possíveis tinham os seguintes pesos: sempre = 1, freqüentemente = 2, raramente = 3, e nunca = 4. Neste caso, a opção “nunca” era a resposta mais adequada do ponto de vista da proteção da informação. Este padrão se mantém até a questão 14.

A partir da questão 15 o padrão se inverte, ou seja, “sempre” passa a valer “4”, “freqüentemente” corresponde a “3”, “raramente” é igual a “2”, e “nunca” tem peso “1”.

A análise quantitativa das respostas obtidas na aplicação do questionário apresentou o resultado mostrado nas FIGURAS 18 a 22, de acordo com o perfil da amostra.

Na FIG.18 apresenta-se a média obtida de homens e mulheres, a qual representa o grau de conformidade (aderência) às medidas de segurança regulamentadas na instituição. Em uma escala de 1 a 4, as mulheres obtiveram média de 3,45 e os homens 3,33.

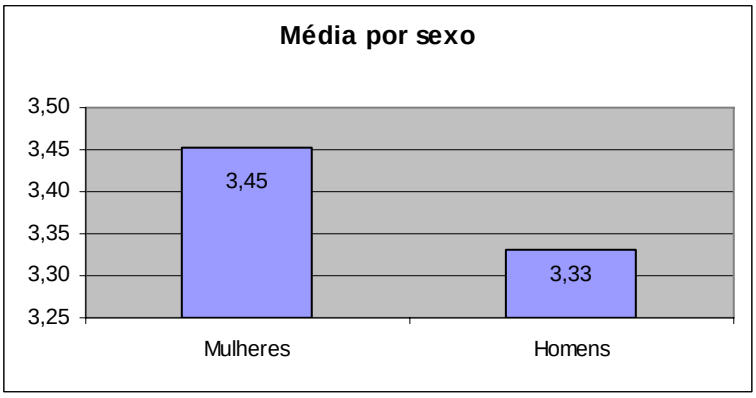


FIGURA 18 - Médias obtidas entre homens e mulheres

Considerando-se a faixa etária dos usuários, a média ficou distribuída da seguinte forma (FIG.19): usuários com idade entre 30 e 39 anos tiveram média de 3,56; na faixa até 29 anos a média foi de 3,39; e para os respondentes com 40 ou mais anos a média obtida foi de 3,36.

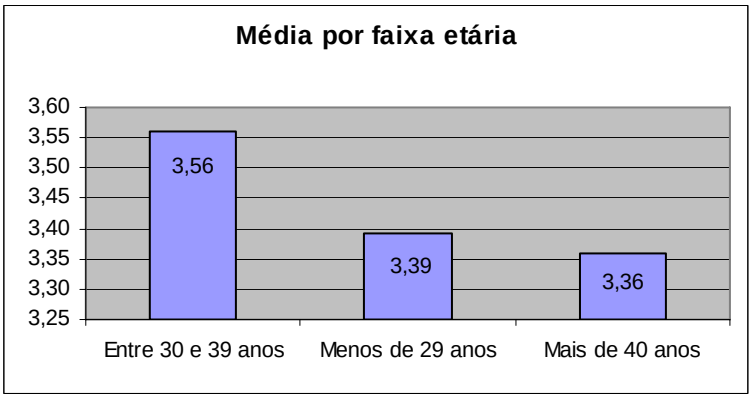


FIGURA 19 - Médias obtidas entre as faixas etárias

Analisando-se pelo tempo de trabalho (ou de estudo – no caso de alunos) no IPEN (FIG.20), os usuários com menos de 10 anos obtiveram a melhor média (3,44); com tempo de trabalho entre 10 e 20 anos a média foi de 3,37; e aqueles com mais de 20 anos no IPEN tiveram média de 3,35.

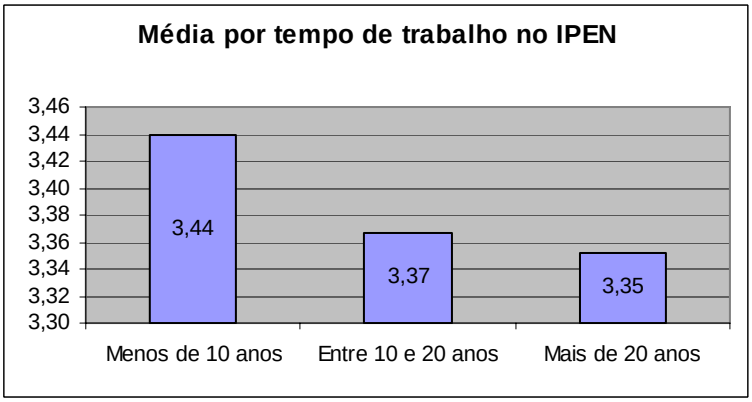


FIGURA 20 - Médias obtidas de acordo com o tempo de serviço

A FIG.21 corresponde aos funcionários contratados sob o Regime Jurídico Único, os quais tiveram média de 3,36, enquanto os usuários pertencentes aos outros vínculos empregatícios ficaram com média de 3,42.

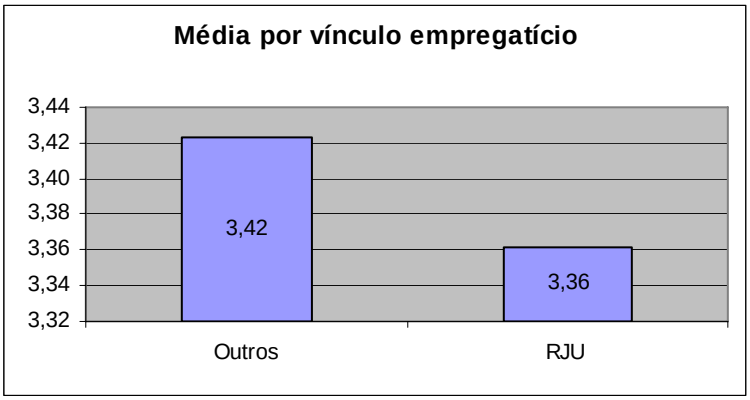


FIGURA 21 - Médias obtidas de acordo com o vínculo empregatício

Com relação ao grau de instrução, na FIG.22 mostra-se que os mestres e doutores atingiram média de 3,41, os usuários de nível superior completo tiveram média de 3,38, os especialistas atingiram uma média de 3,37 e os demais tiveram 3,27.

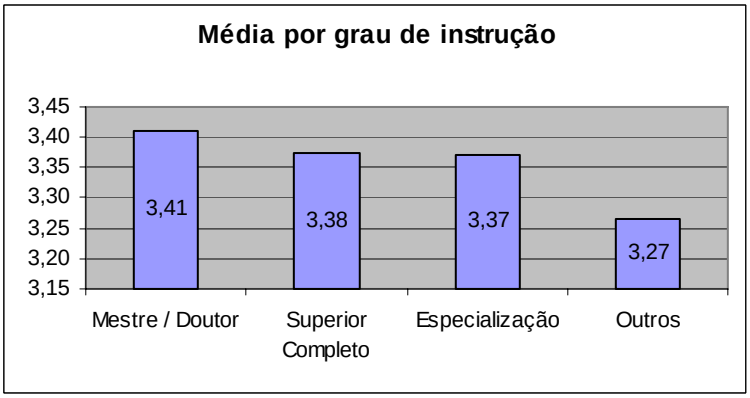


FIGURA 22 - Médias obtidas de acordo com o grau de instrução

Diante dos dados obtidos na pesquisa verificou-se que a pior situação, relativa à observância das normas de segurança em vigor no IPEN recaiu sobre homens acima dos 40 anos, que trabalhavam na instituição há mais de 20 anos, contratados sob a égide do Regime Jurídico Único e que não completaram o ensino superior. Por outro lado, o perfil do usuário que melhor obedecia às normas de segurança correspondia à mulher, com idade entre 30 e 39 anos, não pertencente ao RJU, no IPEN há menos de 10 anos, e portadora do título de mestre ou doutor.

Na análise geral das questões avaliadas, 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, com médias de **2,59** e **2,62,** respectivamente, conforme mostrado na FIG.23 e na TAB.17.

Por outro lado, as questões com maior grau de aderência foram as de números 7 e 12, com médias **3,9** e **3,83**. A questão 7: *"Altero a infra-estrutura física da rede do IPEN (ponto de rede, entre outras) sem prévia aprovação da Gerência de Informática ou responsável imediato"*, e a questão 12 *"Forneço informações pessoais quando solicitadas por e-mails de órgãos públicos ou de empresas conceituadas no mercado (bancos, correios, receita federal, justiças eleitoral, entre outros)",* foram, no geral, respondidas negativamente.

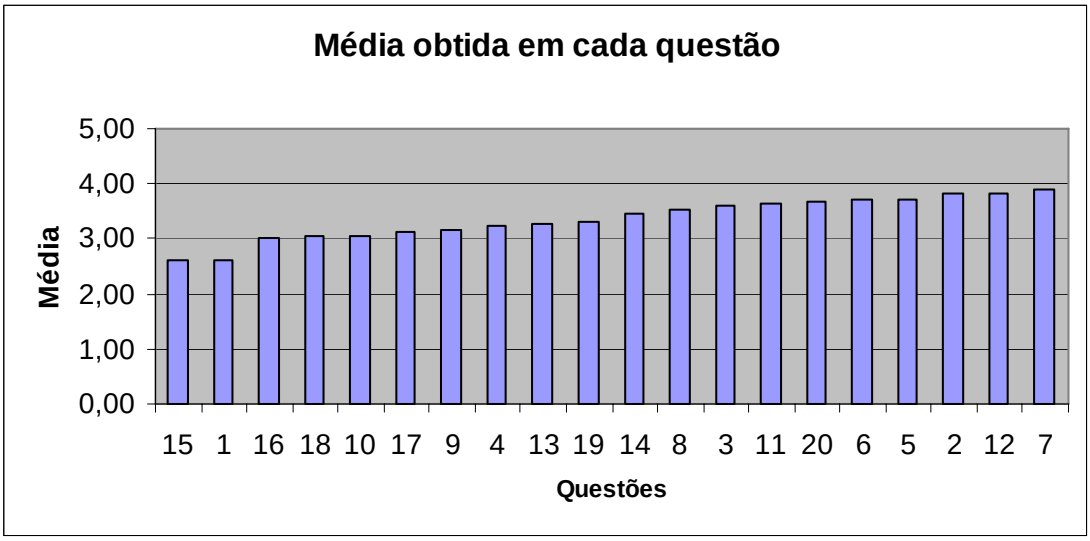


FIGURA 23 – Avaliação das questões do questionário

TABELA 17 - 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.24 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".

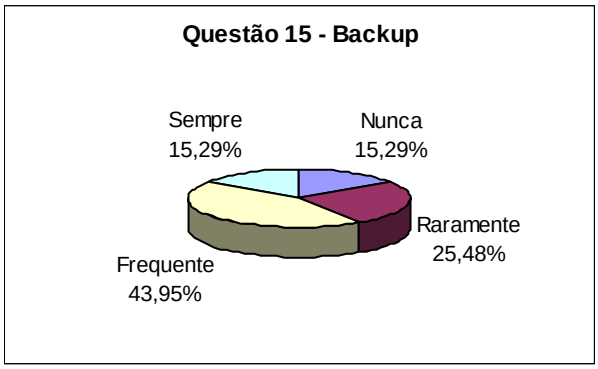


FIGURA 24 - Grau de aderência da prática de backup

A questão 1 *"Utilizou senhas fáceis de lembrar (composta por nomes ou suas iniciais, datas de aniversários, seqüência de letras e números)",* apresenta, conforme é mostrado na FIG.25, 54,77% para "nunca" e "raramente" contra 45,22% para "sempre" e "freqüentemente".

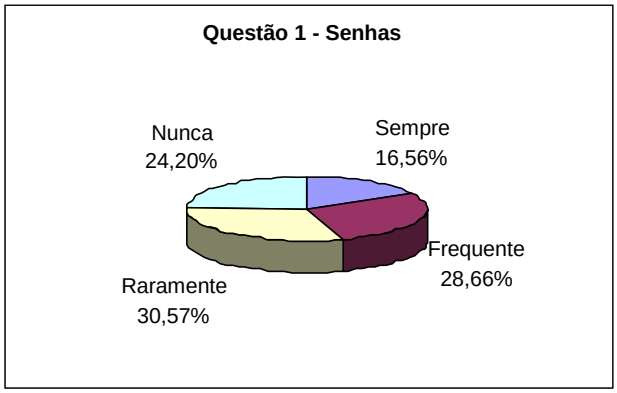


FIGURA 25 - Grau de aderência da prática de criação de senhas

Este resultado confirma uma informação levantada nas entrevistas (TAB.13), 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.12. 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 internalizadas pelos usuários sistemas de informação. Ou sejam, eles ainda não as 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.14, o nível de conscientização dos funcionários obteve média de 2,52 (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. Na TAB.14 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.12, 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 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 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.14).

Entretanto, a avaliação feita com a ferramenta ISG-HE apresentou um resultado geral de 66 pontos, o que mostrou que a instituição vive uma situação considerada “pobre” em relação a sua gestão da segurança da informação (vide TAB.12).

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, na maior parte das vezes, por iniciativa dos próprios administradores de tais sistemas, ou quando muito por discussão 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 visto na Hipótese C, a aplicação da ferramenta ISG-HE contabilizou um total de 66 pontos na avaliação geral da segurança da informação do IPEN. Aliado a isto, a TAB.14 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 uma proposta para a re-estruturação da gestão da segurança da informação na instituição (vide CAPÍTULO 5. PROPOSTA PARA A RE-ESTRUTURAÇÃO DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO).

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", demonstrado na FIG.23.

Os incidentes de segurança visto na TAB.1, e os depoimentos dos gerentes, reforçam esta constatação.

Conclui-se também que os usuários, em geral, têm conhecimento das normas existentes, mas ainda não as internalizaram, ou seja, não incorporaram-nas em seu cotidiano.

Para melhorar o nível de aderência das medidas de segurança junto à comunidade do IPEN propõe-se a implantação de um programa de conscientização e treinamento em segurança da informação amplo e contínuo, que abranja funcionários, alunos, parceiros e prestadores de serviço.

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.

Concluiu-se que, a gestão da segurança da informação atualmente em curso no IPEN é insuficiente para assegurar o nível de proteção que a instituição exige, dada a dependência de TI de suas atividades.

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 desta tarefa, os quais, durante a pesquisa realizada, se revelaram ausentes ou inexpressivos na gestão da segurança atualmente praticada.

A palavra “modelo” neste contexto significa: *dar forma ou contorno a;* ou seja, *adaptar, acomodar, conformar, harmonizar*[14]. O modelo proposto, portanto, não deve ser entendido como um método científico / matemático, como, por exemplo, em “modelo de Roche”.

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.

A subseção 5.1 – Proposta de Gestão da Segurança, a seguir, apresenta o modelo de gestão proposto em detalhes.

5.1. Proposta de Gestão da Segurança

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.26 apresenta-se o diagrama das etapas de implementação do modelo de gestão proposto.

---

[14] [14] Novo dicionário AURÉLIO. Ed. Nova Franteira.

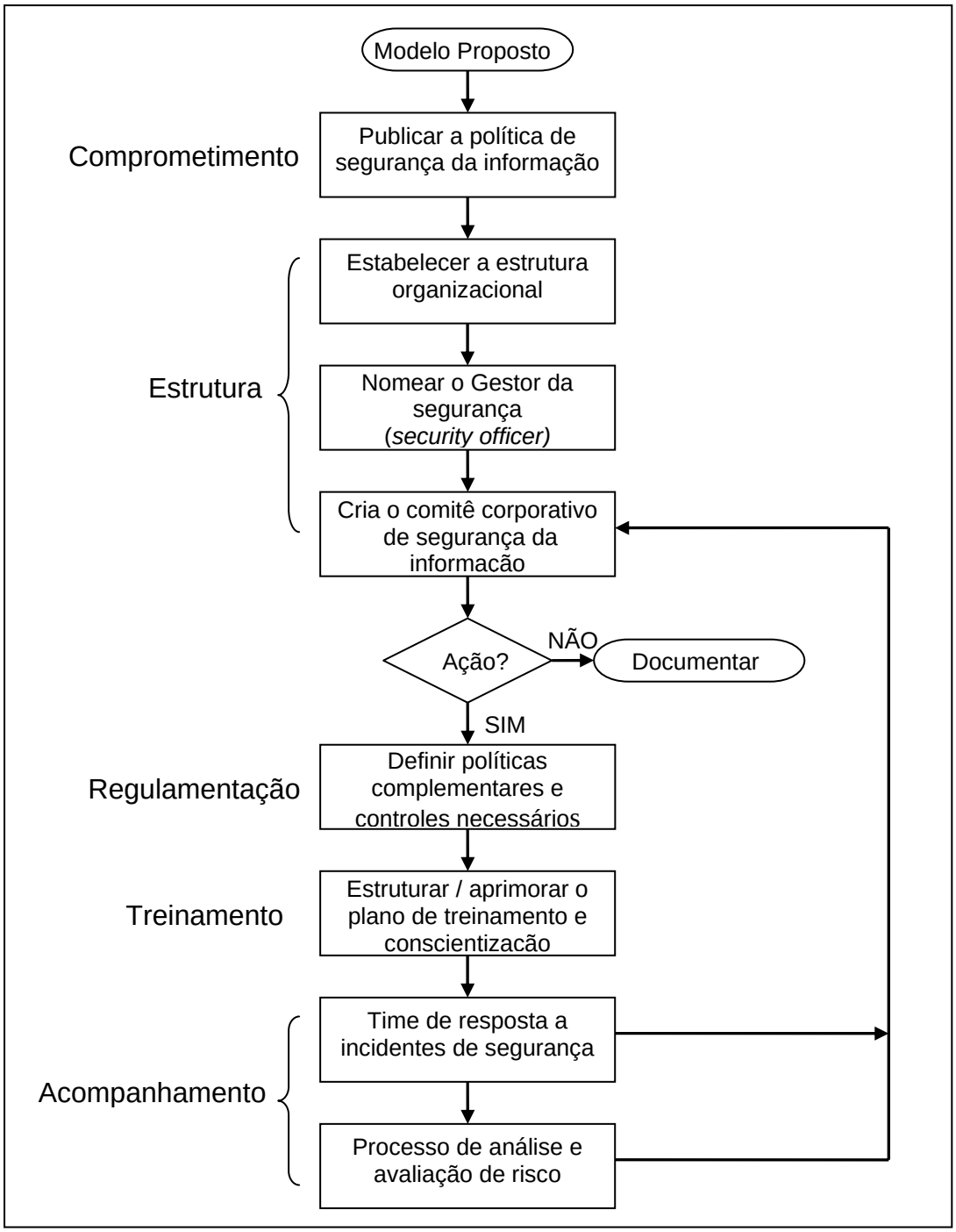


FIGURA 26 - Diagrama da implementação do modelo de gestão da segurança proposto

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

1) 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 corporativa 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 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. Isto requer respaldo da alta direção.

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, 2008b) 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) para o trato de assuntos relativos à segurança da informação e comunicações; e

VII- propor normas relativas à segurança da informação e comunicações.

ROBINSON (2003) descreve oito responsabilidades típicas de um CSO *(Chief Security Officer*):

I- agir como o representante da companhia no que se refere à indagações dos clientes, parceiros, e público em geral quanto à estratégia de segurança da organização;

II- representar a empresa junto às autoridades policiais durante investigação de ataques à rede e roubos de informações realizados por empregados;

III- reduzir o fosso existente entre áreas de negócio e o departamento de TI para balancear as necessidades de segurança com o plano de negócio estratégico da organização, identificar os fatores de risco, e determinar soluções em ambas às partes;

IV- desenvolver políticas e procedimentos de segurança que forneçam adequada proteção às aplicações de negócio sem interferir nas necessidades do *core business* (negócio principal) da organização;

V- planejar e testar respostas para violações de segurança, incluindo a possibilidade de discussão do evento com clientes, parceiros ou com o público em geral;

VI- supervisionar a seleção, testes, desenvolvimento, e manutenção de produtos de segurança (*hardware* e *software*) bem como contratação de serviço externo (*outsourced*);

VII- Supervisionar o quadro de funcionários responsável pela segurança corporativa, abrangendo desde técnicos responsáveis pela administração de dispositivos de *firewall* a guardas de segurança; e

VIII- As características mais importantes de um CSO são: ter bom inter-relacionamento, ter habilidade para escrever comunicados, ter sólidos conhecimentos de segurança em instalações físicas e em meios eletrônicos, bem como dos requerimentos de negócio da organização. Além disso, este indivíduo deve possuir capacidade de liderança para reunir na mesa de discussão executivos do departamento de TI e das áreas de negócio, para encontrar o equilíbrio entre negócio e requerimentos de segurança, e persuadir todas as partes envolvidas para juntos perseguirem o curso das ações planejadas.

Na atual estrutura do IPEN, a gestão da segurança da informação está a cargo da GRS (departamento de TI), 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.

Como visto, segurança da informação é uma atividade complementar da GRS, que tem como função principal administrar a rede corporativa de computadores.

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).

No caso do IPEN, a estrutura organizacional da segurança da informação poderá ser integrada ao sistema de gestão da qualidade ISO 9001,

CQAS (Coordenação da Qualidade Meio Ambiente e Segurança), já existente no organograma da instituição (vide FIG.9), subordinada à Superintendência.

Esta união de gestão da segurança da informação com gestão da qualidade foi adotado com sucesso na FUCAPI (CAMINHA, 2006).

Outra possibilidade é a criação de uma estrutura organizacional independente, como é o caso da ANVISA, onde a Assessoria de Segurança Institucional responde diretamente ao Diretor-Presidente da organização (ANVISA, 2006; ANVISA, 2007).

A gestão da qualidade do IPEN possui características importantes que poderão acelerar a efetividade da segurança da informação na instituição. Trata-se de uma prática já consolidada no ambiente de pesquisa (Centros de Pesquisas e laboratórios), com rotinas bem definidas para atualizações periódicas de documentação de processos de trabalho e procedimentos, sistematização de não-conformidades e auditorias, além de permear por todas as áreas finalísticas da organização.

A infraestrutura da segurança da informação na organização é tratada no item 6.1 da ABNT NBR ISO/IEC 27002:2005.

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 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.

A política de segurança da informação é tratada no item 5 da ABNT NBR ISO/IEC 27002:2005.

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*).

No IPEN, este plano de conscientização deverá ser viabilizado com a participação conjunta de outros setores da administração da instituição; como é o caso da GDP (Gerência de Desenvolvimento de Pessoas), com sua experiência na elaboração e coordenação de treinamentos e o SCI (Serviço de Comunicação Institucional) na divulgação e organização de eventos.

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.

Um exemplo disso é a prática de *backups*. A análise do questionário revelou que 64 dos 157 respondentes assinalaram “nunca” ou “raramente”, quando perguntado se realizavam cópias de segurança dos seus dados, isto corresponde a 40,77% dos usuários.

No caso do *backup,* é necessário verificar que ferramentas podem atender as necessidades dos usuários e instruí-lo para usá-las adequadamente.

A conscientização, educação e treinamento em segurança da informação na organização é tratada no item 8.2.2 da ABNT NBR ISO/IEC 27002:2005.

5) Acompanhamento

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

Neste elemento, se incluem as observações realizadas pela equipe de segurança nas suas atividades cotidianas (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)" na denominação americana*,* 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".*

O usuário deve ser um aliado dentro de um programa de segurança da informação, pois é ele quem irá perceber no primeiro momento a evidência ou o indício de um evento que poderá se configurar em uma ameaça à segurança. Quando motivado e se sentindo parte do processo, ciente dos benefícios para a organização e para ele mesmo, não hesitará em acionar os canais existentes para a devida verificação do fato e das previdências necessárias (ALEXANDRIA, 2006).

Outro instrumento pertencente à componente "Acompanhamento" é o processo de análise, avaliação e tratamento de riscos (vide Subseção 2.13.1. Análise e Avaliação 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 for se consolidando 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.

Utilizando-se como exemplo o uso de "senhas" - questão número 1 do questionário (APÊNDICE D), que obteve a segunda pior pontuação (vide FIG.23), pode-se-ia implementar as seguintes ações, conforme estabelece a subseção

11.3.1 Uso de senhas, da Norma ABNT NBR ISO/IEC 27002:2005, alíneas “e” e “f” das diretrizes para implementação:

e) modificar senhas regularmente ou com base no número de acessos (convém que senhas de acesso a contas privilegiadas sejam modificadas mais freqüentemente que senhas normais) e evitar a reutilização ou reutilização do ciclo de senhas antigas;

f) modificar senhas temporárias no primeiro acesso ao sistema;

Além disso, é necessário que a instituição implemente medidas de segurança que a coloque em conformidade com a legislação estabelecida para os órgãos e as entidades da Administração Pública Federal.

Na Subseção 2.13.2. Requisitos Legais foi feito uma macroanálise das leis e decretos do Governo Federal Brasileiro acerca da segurança da informação nos órgãos públicos.

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 pesquisado, o Instituto de Pesquisas Energéticas e Nucleares – IPEN, poderá servir de ponto de partida para a implantação da segurança da informação em outras organizações. Estas, por sua vez, deverão promover as adaptações necessárias para atender suas particularidades internas.

A proposta apresentada foi concebida procurando-se utilizar as estruturas e competências existentes de eficácia comprovada, e já consagradas na instituição. Um bom exemplo de ação institucional bem sucedida no IPEN é a campanha de combate ao tabagismo, na qual utilizou-se palestra de conscientização, cartazes e folhetos.

Este modelo proposto também pode ser entendido como um divisor de águas ou um delimitador. Um marco para uma nova postura frente ao desafio de gerir, de forma mais estruturada e efetiva, a segurança da informação corporativa.

6. CONCLUSÕES

A aplicação dos três instrumentos de coleta de dados, que compõem método de diagnóstico e avaliação apresentado neste trabalho de doutorado, evidenciou a existência de lacunas na administração da segurança da informação na instituição avaliada (IPEN).

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 acontecer novamente, já que não foram implementadas ações efetivas para evitar que os mesmos se repitam.

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 realização de cópias de segurança (*backup*) e os procedimentos para a proteção de senhas de acesso são práticas de segurança que precisam ser incorporadas na rotina de trabalho dos usuários.

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 adequado.

A ausência da política de segurança é um indício de que a gestão da segurança da informação é inexistente ou incipiente na organização.

Não se pode, entretanto, alegar falta de regulamentação na administração pública federal do Brasil. O referido setor conta com uma série de instrumentos regulatórios relacionados com a segurança da informação endereçada a seus órgãos e entidades.

São exemplos da regulamentação vigente no Brasil o Decreto nº. 3.505 de 2000, que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal; e a Instrução Normativa GSI nº 1 de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal direta e indireta.

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.

É neste cenário que o método de diagnstico e avaliação, apresentado neste trabalho, tem sua área de aplicabilidade definida.

A aplicação do método de diagnóstico e análise, no ambiente de pesquisa científica estudado, revelou que a idéia de segurança da informação está fortemente associada com a garantia da confidencialidade.

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

A confidencialidade, por sua vez, tem pouca importância para as informações da instituição, na avaliação dos gerentes ouvidos.

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 pode ser conseguido por meio de uma de gestão bem estruturado.

Verificou-se também que impera no ambiente da pesquisa científica 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 é o de que a salvaguarda das informações seja uma 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 a 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).

Além disso, é necessário atentar para os pequenos incidentes, que por vezes passam despercebidos, mas como os grandes acidentes de segurança, causam impactos negativos ao negócio.

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.

Só desta forma pode-se garantir o funcionamento correto e preciso do serviço. Priorizando-se, neste caso específico, a preservação da integridade de seus dados e a disponibilidade do sistema, seus principais requerimentos de segurança.

O método de diagnóstico e avaliação, apresentado na Seção 3.4, tem a seu favor o fato de possibilitar a realização de um levantamento preliminar do estágio atual da segurança da informação de uma organização, de uma maneira muito simples se comparada com a utilização de uma ferramenta de análise de risco convencional.

Ele não exige a formalidade nem o custo financeiro e operacional que se teria na aplicação de uma metodologia de análise e avaliação de risco. O método de diagnóstico e avaliação pode ser conduzido por uma única pessoa, na forma de um levantamento de dados.

A aplicação de uma ferramenta de análise de risco, por se tratar de um processo mais sofisticado e minucioso, vai exigir uma estruturação em segurança da informação que estas organizações ainda não possuem ou, no mínimo, uma boa dose de conscientização da alta direção.

Este, na verdade, é o grande dilema vivido pelas organizações: 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?

O método de diagnóstico e avaliação apresentado neste trabalho tem a vantagem de ser aplicada na forma de um levantamento de dados, pois ele utiliza métodos de levantamento de dados comuns, como por exemplo, questionário e entrevistas.

O principal objetivo deste método é fomentar uma discussão interna sobre a questão da segurança da informação corporativa, envolvendo os três níveis hierárquicos administrativos.

Esta discussão deverá lançar a semente para a criação de uma conscientização coletiva da importância da segurança da informação na organização. O que levará à implementação de uma gestão melhor estruturada.

De qualquer maneira, seja na aplicação de uma ferramenta convencional de análise e avaliação de risco, seja na aplicação deste instrumento de diagnóstico e avaliação, deverá sempre existir a figura de um tutor (patrocinador) de nível gerencial, que se interesse pelo projeto e que sirva de porta-voz em sua defesa dentro da organização.

Além disso, deve-se obter autorização expressa da Administração para a aplicação de qualquer instrumento ou *software* no ambiente corporativo.

Em suma, as organizações em geral 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.

Trabalhos futuros

Este trabalho poderá ganhar novas contribuições e desdobramentos. A seguir são apresentados três possíveis desenvolvimentos futuros.

1) Automatização do processo de análise dos dados coletados

O processo de análise dos dados coletados pelo método de diagnóstico e avaliação poderá ser aprimorado. O processo poderá ter algumas etapas automatizadas.

Esta primeira utilização da ferramenta mostrou que a análise dos dados é uma etapa bastante trabalhosa. É preciso muita atenção na transcrição dos dados, pois qualquer erro poderá alterar o resultado final, e por conseqüência, as conclusões obtidas.

É possível adicionar outras funções nas planilhas eletrônicas utilizadas. Bem como a incorporação de outros *softwares* para um tratamento estatístico mais aprofundado, e para uma análise qualitativa mais precisa.

Como exemplos de *softwares* que poderão ser agregados na ferramenta estão o **Statistica** e o **Sphinx Léxica**.

2) Aplicação da ferramenta em diferentes ambientes

Realizar um estudo comparativo dos resultados obtidos aqui, uma instituição pública de pesquisa científica, com resultados obtidos em organização de outros segmentos.

3) Método de diagnóstico e avaliação versus Ferramenta de análise e avaliação de riscos.

Algumas questões a serem estudadas:

a. O que uma ferramenta poderá agregar a outra?
b. É possível identificar uma área de interseção entre as duas ferramentas?
c. Vantagens e desvantagens (custo, horas de trabalho e complexidade, entre outros.)
d. Poderá haver situações, tais como, tipo de organização, em que apenas o Método de diagnóstico e avaliação seja suficiente para orientar a implementação dos controles de segurança necessários?

APÊNDICES

APÊNDICE A – Regulamentação (Leis, Decretos e outros)

1) **Medida Provisória nº 2.200-2**, de 24 de agosto de 2001.

Institui a ICP-Brasil (BRASIL, 2001).

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

2) **Decreto nº. 2.910**, de 29 de dezembro de 1998.

Estabelece normas para a salvaguarda de documentos, materiais, áreas, comunicações e sistemas de informação de natureza sigilosa, e dá outras providências (BRASIL, 1998c).

3) **Decreto nº. 3.505**, de 13 de junho de 2000.

Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Cria o Comitê Gestor da Segurança da Informação - CGSI (BRASIL, 2000a).

Art. 1º Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos:
I - assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
II - proteção de assuntos que mereçam tratamento especial;
III - capacitação dos segmentos das tecnologias sensíveis;
IV - uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;
V - criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
VI - capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e
VII - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

4) **Decreto nº. 4553**, de 27 de dezembro de 2002.

Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências (BRASIL, 2002b).

5) **Decreto nº. 5.563**, de 11 de outubro de 2005 - Lei de Inovação

Regulamenta a Lei nº. 10.973 (BRASIL, 2005b).

Art. 13. É vedado ao dirigente, ao criador ou a qualquer servidor, militar, empregado ou prestador de serviços de ICT (Instituições de Ciência e Tecnologia) divulgar, noticiar ou publicar qualquer aspecto de criações de cujo desenvolvimento tenha participado diretamente ou tomado conhecimento por força de suas atividades, sem antes obter expressa autorização da ICT.

6) **Decreto nº. 5.555**, de 04 de outubro de 2005

Promulga o Acordo entre o Governo da República Federativa do Brasil e o Governo da República da Coréia para Cooperação nos Usos Pacíficos da Energia Nuclear, celebrado em Seul, em 18 de janeiro de 2001 (BRASIL, 2005a).

ARTIGO VII - Informação
As partes tomarão todas as medidas apropriadas de acordo com suas respectivas leis e regulamentos para preservar as restrições e reservas com respeito à informação e para proteger direitos de propriedade intelectual, inclusive segredos comerciais e industriais que tenham sido transferidos entre pessoas autorizadas sob a jurisdição de qualquer das Partes. Para fins do presente Acordo, entende-se que propriedade intelectual tem a acepção determinada pelo Artigo 2 da Convenção que Institui a Organização Mundial para a Propriedade Intelectual, celebrada em Estocolmo, em 14 de julho de 1967.

7) **Lei nº 8.159**, de 08 de janeiro de 1991

Dispõe sobre a política nacional de arquivos públicos e privados (BRASIL, 1991).

8) Lei nº 9.279, de 14 de maio 1996 (BRASIL, 1996).

Art. 1º Esta Lei regula direitos e obrigações relativos à propriedade industrial
Art. 2º A proteção dos direitos relativos à propriedade industrial, considerado o seu interesse social e o desenvolvimento tecnológico e econômico do País, efetua-se mediante:

- *Concessão de patentes de invenção e de modelo de utilidade;*
- *Concessão de registro de desenho industrial;*
- *Concessão de registro de marca;*
- *Repressão às falsas indicações geográficas; e*
- *Repressão à concorrência desleal.*

9) **Lei n° 9.609**, de 19 de fevereiro de 1998

Dispõe sobre a Proteção da Propriedade Intelectual do Programa de Computador (BRASIL, 1998a).

10) Lei n° 9.610, de 19 de fevereiro de 1998

Altera, atualiza e consolida a legislação sobre direitos autorais (BRASIL, 1998b).

11) Lei n° 9.983, de 14 de julho de 2000

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências (BRASIL, 2000b).

Dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública.

"Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:" (AC)
"Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa." (AC)

"Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:" (AC)
"Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa." (AC)

12) **Lei nº 8.027**, de 12 de abril de 1990

Dispõe sobre normas de Conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas e dá outras providências (BRASIL, 1990).

Art. 5º São faltas administrativas, puníveis com a pena de demissão, a bem do serviço público:
I – valer-se, ou permitir dolosamente que terceiros tirem proveito de informação, prestígio ou influência, obtidos em função do cargo, para lograr, direta ou indiretamente, proveito pessoal ou de outrem, em detrimento da dignidade da função pública;
Parágrafo único. A penalidade de demissão também será aplicada nos seguintes casos:
V - revelação de segredo de que teve conhecimento em função do cargo ou emprego.

13) **RESOLUÇÃO Nº 7**, DE 29 DE JULHO DE 2002.

Estabelece regras e diretrizes para os sítios na *internet* da Administração Pública Federal (BRASIL, 2002a).

CAPÍTULO VI - DA SEGURANÇA DOS SÍTIOS
Art. 14. A segurança dos sítios dos órgãos e entidades da Aministração Pública Federal observará o disposto neste Capítulo e, sem prejuízo do Decreto nº 3.505, 13 de junho de 2000.
Art. 15. Os serviços Web devem ser providos por equipamentos dedicados com acessos físico e lógico controlados.
Art. 16. As infra-estruturas computacionais e de rede dedicadas à prestação dos serviços Web devem estar isoladas da rede interna do proprietário do sítio.
Art. 17. As páginas Web deverão ser providas e atualizadas de modo a não comprometer a segurança das redes internas do proprietário do sítio.
Art. 18. O servidor Web deverá ser configurado de modo seguro tanto no que se refere à segurança física, quanto aos sistemas operacionais e aplicativos instalados.
Art. 19. A segurança do sítio deve ser permanentemente atualizada de modo a resistir aos ataques que exploram vulnerabilidades para as quais já existam correções.

Art. 20. Deverão ser implementados mecanismos de registro de eventos e acessos ao sítio e ao seu ambiente de funcionamento.
Art. 21. Os relatórios produzidos pelos mecanismos citados no art. 20 deverão ser armazenados de modo seguro por período compatível com o caráter da informação.
Art. 22. Quando da ocorrência de ataques bem sucedidos, dever-se-á preservar a maior quantidade possível de evidências digitais relevantes.
Art. 23. Os registros de eventos e acessos deverão ser monitorados regular e freqüentemente, objetivando a identificação de falhas relevantes.
Art. 24. Para o ambiente do sítio deverão ser utilizados mecanismos de sincronização automática de tempo por meio das fontes oficiais de tempo.
Art. 25. O ambiente da rede do sítio do órgão ou entidade deve contar com planos de contingência implementados e atualizados, visando ao pronto restabelecimento do ambiente e dos serviços, assim como o não comprometimento da imagem da Administração Pública Federal;
Art. 26. Os planos de contingência deverão ser periodicamente testados para que seja verificada a sua eficácia ou necessidade de adequação.
Art. 27. Devem ser estabelecidas diretrizes em cada órgão ou entidade que orientem a realização de cópias de segurança periódica das informações críticas dos ambientes dos sítios governamentais.
Art. 28. Deve existir pelo menos um responsável técnico para atuar como contato no que se refere à segurança do ambiente do sítio.
Parágrafo único. O responsável técnico somente poderá ser servidor público em efetivo exercício no órgão ou entidade.
Art. 29. Deverão ser estabelecidas rotinas de programas:
I - de treinamento e atualização específicos aos responsáveis técnicos pela segurança do ambiente do sítio;
II - de conscientização de todos os envolvidos.
Art. 30. Sempre que necessário, os servidores Web deverão ser configurados para usar tecnologias de autenticação e criptografia, visando a garantir a integridade, o sigilo e a autenticidade das informações.
Art. 31. O responsável técnico deverá certificar-se de que entende todas as funcionalidades de qualquer programa externo a ser utilizado e suas possíveis vulnerabilidades.
Art. 32. Devem ser adotados conceitos e procedimentos de auditoria interna que permitam análise do ambiente computacional.
Art. 33. Toda a documentação técnica referente aos componentes e configurações do ambiente do sítio deverá ser conservada para eventuais verificações.
Art. 34. Todos os documentos normativos elaborados e implementados pelo órgão ou entidade, que versem sobre o ambiente do sítio, deverão ser mantidos atualizados e em condições de sofrer auditorias.
Art. 35. É vedada a utilização de provedores externos para prestar serviços considerados sigilosos, bem como aqueles que possam expor a privacidade dos usuários.
Art. 36. Caso os serviços Web estejam sendo prestados por provedores externos, compete ao órgão ou entidade contratante estabelecer cláusulas no contrato de prestação de serviço que estipulem a observância às normas sobre segurança de sítios aplicáveis à Administração Pública Federal.

§ 1º Os provedores externos de que trata o caput deverão submeter, por força do contrato, seu ambiente à periódica auditoria do órgão ou entidade contratante.
§ 2º Na auditoria de que trata o § 1º, incluem-se todas as partes do ambiente do contratado que possam afetar a segurança do sítio.
Art. 37. O serviço de certificação dos sítios dos órgãos ou entidades somente poderá ser feito por Autoridades Certificadoras integrantes da ICP-Brasil, observado o disposto no Decreto nº 3.996, de 31 de outubro de 2001.
Art. 38. Os órgãos e entidades deverão adotar medidas necessárias para preservar a segurança dos sítios sob sua responsabilidade, inclusive se hospedados por provedores externos, devendo estipular de forma clara as responsabilidades da unidade que gerencia o sítio.

CAPÍTULO VII - DAS DISPOSIÇÕES FINAIS
Art. 39. Os órgãos e entidades da Administração Pública Federal deverão, até o final de 2002, adaptar todos seus sítios na internet ao disposto nesta Resolução.

14) **Instrução Normativa GSI nº 1**, de 13 de junho de 2008.

Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências (BRASIL, 2008b).

Art. 5º Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:
I - coordenar as ações de segurança da informação e comunicações;
II - aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;
III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;
IV - nomear Gestor de Segurança da Informação e Comunicações;
V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;
VI - instituir Comitê de Segurança da Informação e Comunicações;
VII - aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações;
VIII - remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o GSI.

15) **Instrução Normativa nº 4** do Secretário de Logística e Tecnologia da Informação, de 19 de maio de 2008.

Dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional (BRASIL, 2008a).

Art. 5º Não poderão ser objeto de contratação:
III – gestão de processos de Tecnologia da Informação, incluindo gestão de segurança da informação.
Art. 13. O plano de sustentação, a cargo da Área de Tecnologia da Informação, com o apoio do Requisitante do Serviço, abrange:
I - segurança da informação;

Art. 14. A Estratégia de Contratação, elaborada a partir da Análise de Viabilidade de Contratação, compreende as seguintes tarefas:
II - indicação, pela Área de Tecnologia da Informação com o apoio do Requisitante do Serviço, dos termos contratuais, observado o disposto nos parágrafos 1º e 2º deste artigo, sem prejuízo do estabelecido na Lei no 8.666, de 1993, relativo a:
f) definição de direitos autorais e de propriedade intelectual;
g) termo de compromisso, contendo declaração de manutenção de sigilo e ciência das normas de segurança da informação vigente no órgão ou entidade, a ser assinado pelo representante legal do fornecedor e seus empregados diretamente envolvidos na contratação;

APÊNDICE B - ISG Assessment Tool for Higher Education

	Section I: Organizational Reliance on IT This section is designed to help you determine your institution's reliance on information technology for business continuity. Your overall security evaluation rating will depend in part on your institution's reliance on information technology. It should be completed by the president, chancellor, chief executive officer, or a designee.	
	Scoring: Very Low = 0; Low = 1; Medium = 2; High = 3; Very High = 4	**Score**
1	**Characteristics of Organization**	
1,1	**Annual budget of the organization** Less than $10 million = very low $10 million to $100 million = low $100 to $500 million = medium $500 million to $1 billion or more = high $1 billion or more = very high	
1,2	**Number of employees** Less than 500 employees = very low 500 to 1,000 employees = low 1,000 to 5,000 employees = medium 5,000 to 20,000 employees = high more than 20,000 employees = very high	
1,3	**Number of students** Less than 1,000 students = very low 1,000 to 5,000 students = low 5,000 to 10,000 students = medium 10,000 to 20,000 students = high more than 20,000 students = very high	
	Higher Education Characteristics	
1,4	Dependence on information technology systems and the Internet to conduct academic, research, and outreach programs and offer support services	
1,5	Value of organization's intellectual property stored or transmitted in electronic form	
1,6	Impact of major system downtime on operations	
1,7	Impact to your operations from an Internet outage	
1,8	Dependency on multinational and multisite operations	
1,9	Plans for multinational and multisite operations (outsourced business functions, multiple campus locations, new research collaborations, student enrollment overseas)	
1,10	Impact to national or critical infrastructure in case of outage or compromise to your systems	
1,11	The sensitivity of stakeholders (including but not limited to students, faculty, staff, alumni, governing boards, legislators, donors, and funding agencies) to privacy	
1,12	Stakeholders' sensitivity to security	
1,13	Level of regulation regarding security (FERPA, HIPAA, GLBA, other applicable international, federal, state, or local regulations)	
1,14	Potential impact on reputation of a security incident (student enrollment, faculty recruitment, ability to attract donors, negative press)	

1,15	Extent of operations dependent on third parties (business partners, contractors, suppliers)	
1,16	Does your organization have academic or research programs in a sensitive area that may make you a target of violent physical or cyber attack from any groups?	
	TOTAL RELIANCE ON IT SCORE	0

Section II: Risk Management

This section assesses the risk management process as it relates to creating an information security strategy and program. Please note the change in scoring. This method of scoring applies throughout the remainder of this document. It should be completed by the president, chancellor, chief executive officer, or a designee.

	Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to Completion = 3; Fully Implemented = 4	**Score**
2	**Information Security Risk Assessment**	
2,1	Does your organization have a documented information security program?	
2,2	Has your organization conducted a risk assessment to identify the key objectives that need to be supported by your information security program?	
2,3	Has your organization identified critical assets and the functions that rely on them?	
2,4	Have the information security threats and vulnerabilities associated with each of the critical assets and functions been identified?	
2,5	Has a cost been assigned to the loss of each critical asset or function?	
2,6	Do you have a written information security strategy?	
2,7	Does your written information security strategy include plans that seek to cost-effectively reduce the risks to an acceptable level, with minimal disruptions to operations?	
2,8	Is the strategy reviewed and updated at least annually or more frequently when significant changes require it?	
2,9	Do you have a process in place to monitor federal, state, or international legislation or regulations and determine their applicability to your organization?	
	TOTAL RISK MANAGEMENT SCORE	0

	Section III: People	
	This section assesses the organizational aspects of your information security program. It should be completed by the president, chancellor, chief executive officer, or a designee.	
	Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to Completion = 3; Fully Implemented = 4	**Score**
3	**Information Security Function/Organization**	
3,1	Is there a person or organization that has information security as their primary duty, with responsibility for maintaining the security program and ensuring compliance?	
3,2	Do the leaders and staff of your information security organization have the necessary experience and qualifications?	
3,3	Does your information security function have the authority it needs to manage and ensure compliance with the information security program?	
3,4	Does your information security function have the resources it needs to manage and ensure compliance with the information security program?	
3,5	Is responsibility clearly assigned for all areas of the information security architecture, compliance, processes and audits?	
3,6	Has specific responsibility been assigned for the execution of business continuity and disaster recovery plans (either within or outside the information security function)?	
3,7	Do you have an ongoing training program in place to build skills and competencies for information security for members of the information security function?	
3,8	Is someone in the information security function responsible for liaising with units to identify any new security requirements based on changes to operations?	
3,9	Does the information security function actively engage with other units (human resources, student affairs, legal counsel) to develop and enforce compliance with information security policies and practices?	
3,10	Does the information security function report regularly to institutional leaders and the governing board on the compliance of the institution to and the effectiveness of the information security program and policies?	
3,11	Are the senior officers of the institution ultimately responsible and accountable for the information security program, including approval of information security policies?	
3,12	Do the unit heads and senior managers have specific programs in place to comply with information security policies and standards with the goal of ensuring the security of the information and systems that support the operations and assets under their control?	
3,13	Have you implemented an information security education and awareness program such that all administrators, faculty, staff, contractors, external providers, students, guests, and others know the information security policies that apply to them and understand their responsibilities?	
	TOTAL PEOPLE SCORE	0

	Section IV: Processes This section assesses the processes that should be part of an information security program. It should be completed by the president, chancellor, chief executive officer, or a designee.	
	Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to Completion = 3; Fully Implemented = 4	**Score**
4	**Security Technology Strategy**	
4,1	Does your institution have an official information security architecture, based on your risk management analysis and information security strategy?	
4,2	Is the security architecture updated periodically to take into account new needs and strategies as well as changing security threats?	
4,3	As the architecture evolves, is there a process to review existing systems and applications for compliance and for addressing cases of noncompliance?	
4,4	Have you instituted processes and procedures for involving the security personnel in evaluating and addressing any security impacts before the purchase or introduction of new systems?	
4,5	If a deployed system is found to be in noncompliance with your official architecture, is there a process and defined timeframe to bring it into compliance or to remove it from service, applications or business processes?	
4,6	Do you have a process to appropriately evaluate and classify the information and information assets that support the operations and assets under your control, to indicate the appropriate levels of information security?	
4,7	Are there specific, documented, security-related configuration settings for all systems and applications?	
4,8	Do you have a patch management strategy, policy, and procedures in place and responsibilities assigned for monitoring and promptly responding to patch releases, security bulletins, and vulnerabilities reports?	
	Policy Development and Enforcement	
4,9	Are written information security policies consistent, easy to understand, and readily available to administrators, faculty, employees, students, contractors, and partners?	
4,10	Is there a method for communicating security policies to administrators, faculty, employees, students, contractors, and partners?	
4,11	Are consequences for noncompliance with corporate policies clearly communicated and enforced?	
4,12	Are there documented procedures for granting exceptions to policy?	
4,13	When policies are updated or new policies are developed, is an analysis conducted to determine the financial and resource implications of implementing the new policy?	
4,14	Do your security policies effectively address the risks identified in your risk analysis/risk assessments?	
4,15	Are relevant security policies included in all of your third-party contracts?	

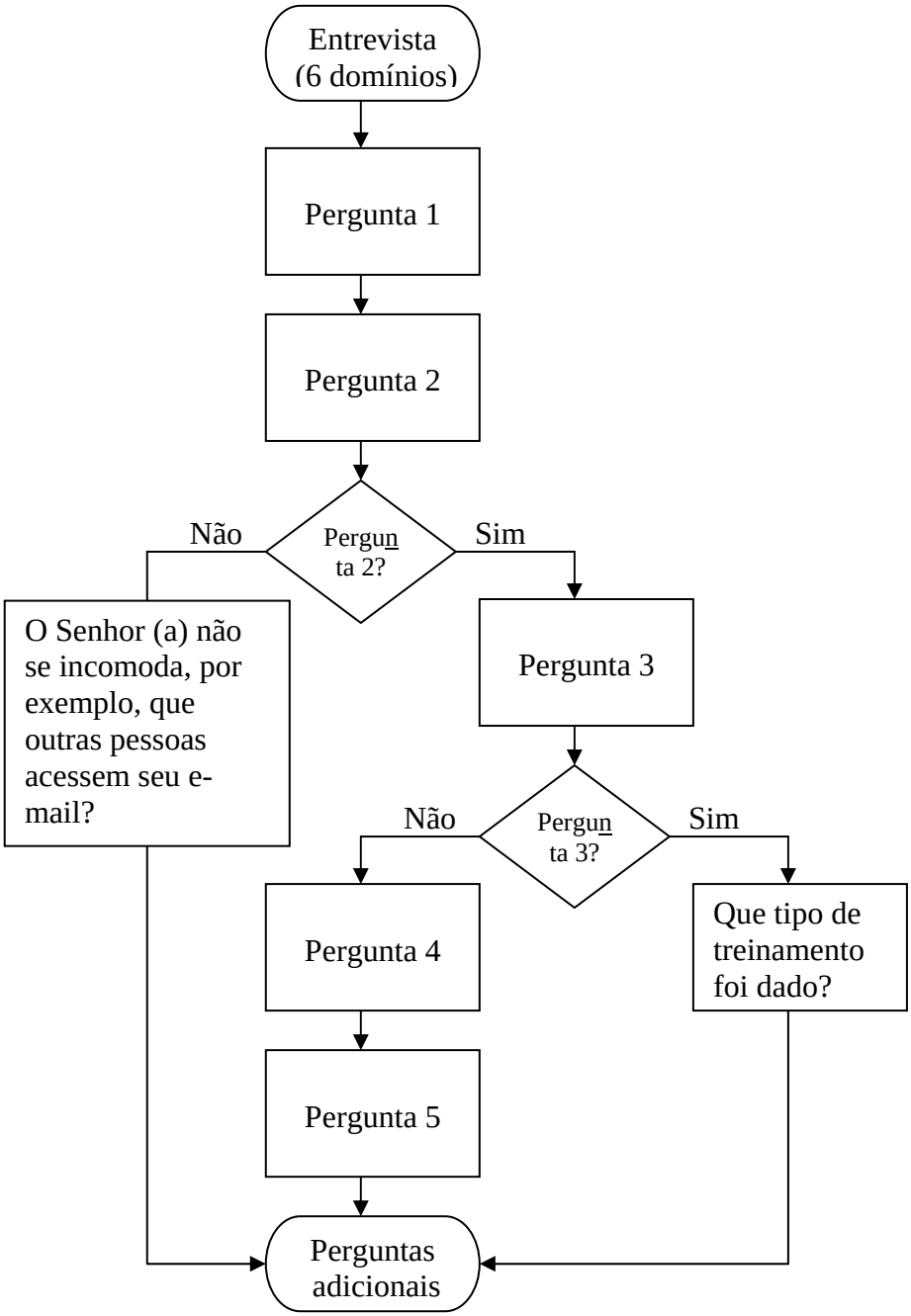
4,16	Are information security issues considered in all important decisions within the organization?	
	Information Security Policies and Procedures	
	Based on your information security risk management strategy, do you have official written information security policies or procedures that address each of the following areas?	
4,17	Individual employee responsibilities for information security practices	
4,18	Acceptable use of computers, e-mail, Internet, and *intranet*	
4,19	Protection of organizational assets, including intellectual property	
4,20	Managing privacy issues, including breaches of personal information	
4,21	Identity management, including excursions or breaches of sensitive identity information	
4,22	Access control, authentication, and authorization practices and requirements	
4,23	Data classification, retention, and destruction	
4,24	Information sharing, including storing and transmitting institutional data on outside resources (ISPs, external networks, contractors' systems)	
4,25	Vulnerability management (patch management, antivirus software)	
4,26	Disaster recovery contingency planning (business continuity planning)	
4,27	Incident reporting and response	
4,28	Security compliance monitoring and enforcement	
4,29	Change management processes	
4,30	Physical security and personnel clearances or background checks	
4,31	Reporting security events to affected parties, including individuals, public, partners, law enforcement, and other security organizations as appropriate	
4,32	Prompt investigation and correction of the causes of security failures	
4,33	Data backups and secure off-site storage	
4,34	Secure disposal of data, old media, or printed materials that contains sensitive information	
	Physical Security	
	For your critical data centers, programming rooms, network operations centers, and other sensitive facilities or locations:	
4,35	Are multiple physical security measures in place to restrict forced or unauthorized entry?	
4,36	Is there a process for issuing keys, codes, and/or cards that require proper authorization and background checks for access to these sensitive facilities?	
4,37	Is your critical hardware and wiring protected from power loss, tampering, failure, and environmental threats?	
	Security Program Administration	
4,38	Do you maintain a current inventory of both the physical network elements (routers/switches, subnets, DNS, DHCP servers) and also the logical network assets (domain names, network addresses, access control lists)?	

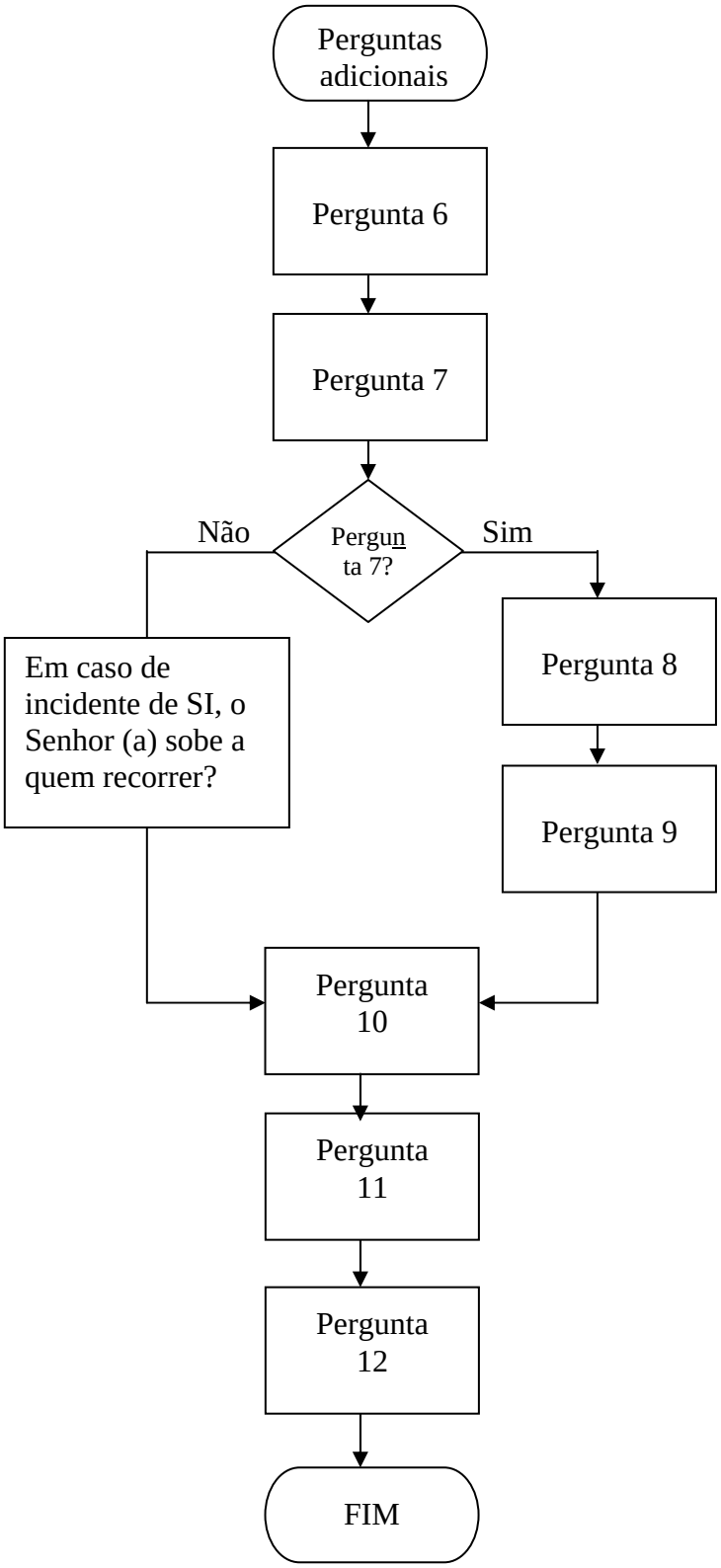
4,39	Do you have a configuration-management process in place to ensure that changes to your critical systems are for valid business reasons and have received proper authorization?	
4,40	Does your organization periodically test and evaluate or audit your information security program, practices, controls, and techniques to ensure they are effectively implemented?	
4,41	Do you conduct a periodic independent evaluation or audit of your information security program and practices for each business unit?	
4,42	Does each periodic independent evaluation or audit test the effectiveness of information security policies, procedure, and practices of a representative subset of each business unit's information systems?	
4,43	Does each periodic independent evaluation or audit assess the compliance of each business unit with the requirements of a standard information security framework and related information security policies, standards, procedures, and guidelines?	
4,44	Are security-performance metrics instituted, evaluated, and reported?	
	TOTAL PROCESSES SCORE	0

	Section V: Technology This section assesses the major technology topics related to information security. It should be completed by the president, chancellor, chief executive officer, or a designee with input from the chief security officer or chief information officer.	
	Scoring: Not Implemented = 0; Planning Stages = 1; Partially Implemented = 2; Close to Completion = 3; Fully Implemented = 4	**Score**
5	**Security Technology**	
5,1	Are Internet-accessible servers protected by more than one security layer (firewalls, network IDS, host IDS, application IDS)?	
5,2	Are there controls between the layers of end-tier systems?	
5,3	Are your networks, systems, and applications periodically scanned to check for vulnerabilities as well as integrity of configurations?	
5,4	Do you constantly monitor in real time your networks, systems and applications for unauthorized access and anomalous behavior such as viruses, malicious code insertion, or break-in attempts?	
5,5	Are security-related activities such as hardware configuration changes, software configuration changes, access attempts, and authorization and privilege assignments automatically logged?	
5,6	Is sensitive data encrypted and associated encryption keys properly protected?	
5,7	Are there effective and reliable mechanisms in place to manage digital identities (accounts, keys, tokens) throughout their life cycle, from registration through termination?	
5,8	Do all of your systems and applications support and enforce automatic password change management or automatic expiration of passwords, as well as password complexity and reuse rules?	
5,9	Do you have an authentication system in place that applies higher levels of authentication to protect resources with higher levels of sensitivity?	

5,10	Do you have an authorization system that enforces time limits and defaults to minimum privileges?	
5,11	Do your systems and applications enforce session/user management practices including automatic timeouts, lockout on login failure, and revocation?	
5,12	Do you employ specific measures to prevent and detect rogue access for all of your wireless LANs?	
5,13	Do you employ specific measures to secure the servers that manage your network domain names and addresses (DNS and DHCP servers)?	
5,14	Do you employ specific measures to secure your remote access services (VPN and dial-up) as well as to secure remote access client systems?	
5,15	Is every desktop workstation and server protected with antivirus software?	
5,16	Is there an audit trail to verify that virus definitions files are updated frequently and systematically?	
5,17	Is every desktop workstation and server updated regularly with the latest operating system patches?	
5,18	Taking into account severity and urgency, are there mechanisms in place to report and respond to a variety of anomalies and security events?	
	TOTAL TECHNOLOGY SCORE	0

APÊNDICE C – Roteiro para a Entrevista




Perguntas adicionais
Pergunta 6
Pergunta 7
Pergunta 7?
Não
Sim
Em caso de incidente de SI, o Senhor (a) sobe a quem recorrer?
Pergunta 8
Pergunta 9
Pergunta 10
Pergunta 11
Pergunta 12
FIM

1- Senhas	Boas práticas para criação e uso de senhas: • Misturar letras maiúsculas com minúsculas; • Usar caracteres não alfabéticos tais como: ; ! @ # $ % & * ( ) + = - 0 1 2 3 4 5 6 7 8 9 como parte integrante da senha. • Não fixar senhas no monitor, na torre do microcomputador, ou na sua mesa de trabalho (Memorize-a!); • Não utilizar de senhas de terceiros.				
Perguntas: 1. O Senhor (a) tem conhecimento da política de senhas do IPEN?		☐ Sim ☐ Não			
2. Em sua opinião, é importante que o IPEN tenha uma política de senhas (para o bom desempenho das atividades, e cumprimento da missão da instituição)? Por favor, quantifique sua resposta!		1	2	3	4
3. Os funcionários deste Centro de Pesquisa têm um nível adequado de conscientização e treinamento em procedimentos de uso seguro de senhas? Por favor, quantifique sua resposta!		1	2	3	4
4. O Senhor (a) acha importante que o IPEN promova uma ação mais efetiva, junto aos usuários, sobre a guarda e os cuidados com as senhas? Por favor, quantifique sua resposta!		1	2	3	4
5. Que tipo de ação o IPEN deveria implementar para melhorar a efetividade da sua política de senhas?					

2- Vírus	Boas práticas para amenizar a ação dos vírus: • Não abrir arquivos anexados em mensagens, a menos que se esteja esperando recebê-lo daquele remetente em particular. • Ignorar mensagens de empresas, como por exemplo, VIVO e TIM. Bem como as que contêm fotos de celebridades (ex. Angelina Jolie e Nicole Kidman). • Ignorar mensagens de órgãos oficiais. Pois, eles não se relacionam com os cidadãos através de mensagens eletrônicas.				
Perguntas: 1. O Senhor (a) tem conhecimento da política de proteção contra vírus de computador do IPEN?		☐ Sim ☐ Não			
2. Em sua opinião, é importante que o IPEN tenha uma política de proteção contra vírus de computador (para o bom desempenho das atividades, e cumprimento da missão da instituição)? Por favor, quantifique sua resposta!		1	2	3	4
3. Os funcionários deste Centro de Pesquisa têm um nível adequado de conscientização e treinamento em procedimentos para se evitar vírus de computador? Por favor, quantifique sua resposta!		1	2	3	4
4. O Senhor (a) acha importante que o IPEN promova uma ação mais efetiva, junto aos usuários, sobre os riscos dos vírus de computador? Por favor, quantifique sua resposta!		1	2	3	4
5. Que tipo de ação o IPEN deveria implementar para melhorar a efetividade da sua política de proteção contra de vírus de computador?					

3- Recursos Computacionais	Boas práticas para o uso dos Recursos Computacionais: • Toda conta (ex. e-mail, *Windows*) é de responsabilidade e de uso exclusivo de seu titular, não podendo esse permitir ou colaborar com o acesso aos Recursos Computacionais da organização por parte de pessoas não autorizadas. • Os recursos computacionais da organização destinam-se ao uso em atividades de negócio (ensino, pesquisa, extensão e serviços); e não devem ser extensivamente utilizados para fins privativos. • É vetada a utilização dos recursos computacionais às pessoas externas à Instituição, sem vínculo com suas atividades. • Ao ausentar-se da sala onde está o microcomputador, aconselha-se a dar saída (*log-out*) da rede, para evitar espionagem ou mesmo sabotagem. Infraestrutura física: • Alterações da infra-estrutura física da rede somente serão permitidas após a análise e aprovação da Gerência de Informática. • As identificações dos computadores não devem ser alteradas sem autorização do responsável local ou superior imediato (ex. endereço IP). Segurança • Se uma falha na segurança dos sistemas computacionais é detectada, esta deverá ser informada ao administrador do sistema.				
Perguntas: 1. O Senhor (a) tem conhecimento da política de uso dos recursos computacionais do IPEN?	☐ Sim ☐ Não			
2. Em sua opinião, é importante que o IPEN tenha uma política de uso dos recursos computacionais (para o bom desempenho das atividades, e cumprimento da missão da instituição)? Por favor, quantifique sua resposta!	1	2	3	4
3. Os funcionários deste Centro de Pesquisa têm um nível adequado de conscientização e treinamento em procedimentos de uso seguro de recursos computacionais? Por favor, quantifique sua resposta!	1	2	3	4
4. O Senhor (a) acha importante que o IPEN promova uma ação mais efetiva, junto aos usuários, sobre o uso dos seus recursos computacionais? Por favor, quantifique sua resposta!	1	2	3	4
5. Que tipo de ação o IPEN deveria implementar para melhorar a efetividade da sua política de uso dos recursos computacionais?				

4- E-mails	Uso do correio eletrônico corporativo: • É proibida a distribuição voluntária ou desapercebida de mensagens não desejadas, como circulares, correntes de cartas ou outros esquemas que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os sistemas computacionais. • É vedada tentativa de acesso não autorizado às caixas postais de terceiros.				
Perguntas: 1. O Senhor (a) tem conhecimento da política de uso do correio eletrônico do IPEN?		☐ Sim ☐ Não			
2. Em sua opinião, é importante que o IPEN tenha uma política de uso do correio eletrônico (para o bom desempenho das atividades, e cumprimento da missão da instituição)? Por favor, quantifique sua resposta!		1	2	3	4
3. Os funcionários deste Centro de Pesquisa têm um nível adequado de conscientização e treinamento em procedimentos de uso seguro do correio eletrônico? Por favor, quantifique sua resposta!		1	2	3	4
4. O Senhor (a) acha importante que o IPEN promova uma ação mais efetiva junto aos usuários sobre o uso do correio eletrônico? Por favor, quantifique sua resposta!		1	2	3	4
5. Que tipo de ação o IPEN deveria implementar para melhorar a efetividade da sua política de uso do correio eletrônico?					

5- Backups	Copia de Segurança • É de responsabilidade de todo usuário realizar e manter cópia de segurança de seus arquivos a fim de evitar que qualquer falha de equipamento coloque a perder o trabalho de vários dias e prejudique os objetivos da organização.				
Perguntas: 1. O Senhor (a) tem conhecimento da política de *backups* (cópia de segurança) IPEN?		☐ Sim ☐ Não			
2. Em sua opinião, é importante que o IPEN tenha uma política de *backups* (para o bom desempenho das atividades, e cumprimento da missão da instituição)? Por favor, quantifique sua resposta!		1	2	3	4
3. Os funcionários deste Centro de Pesquisa têm um nível adequado de conscientização e treinamento em procedimentos para realização de *backups*? Por favor, quantifique sua resposta!		1	2	3	4
4. O Senhor (a) acha importante que o IPEN promova uma ação mais efetiva junto aos usuários sobre a sua política de *backups*? Por favor, quantifique sua resposta!		1	2	3	4
5. Que tipo de ação o IPEN deveria implementar para melhorar a efetividade da sua política de *backups*?					

6- Prop. Intelectual	Proteção à Propriedade Industrial / Intelectual: • É vedada a qualquer pessoa envolvida, direta ou indiretamente, nos processos regulados pela legislação em vigor, a divulgação de informações pertinentes a esse assunto, bem como o trato com terceiros, pessoas físicas ou jurídicas, sem a expressa autorização da direção da Instituição. Direitos Autorais (*Copyright*) • Proibir a instalação, sob qualquer justificativa ou pretexto, de cópias não licenciadas de *software* em equipamento de propriedade da Instituição. • Proibido o uso (download) de material protegido por *copyright*, tais com *softwares*, músicas, filmes, jogos, entre outros. Gerenciamento de documentação controlada • O armazenamento de documentos controlados deve ser feito de modo a minimizar danos, perdas ou deterioração, e de forma que sejam acessíveis por todas as pessoas autorizadas que deles necessitem.				
Perguntas: 1. O Senhor (a) tem conhecimento da política de não divulgação de informações (Proteção à Propriedade Industrial / Intelectual), direito autoral e de armazenamento de documentos controlados do IPEN?		☐ Sim ☐ Não			
2. Em sua opinião, é importante que o IPEN tenha uma política de proteção à propriedade intelectual, direito autoral e de documentos controlados (para o bom desempenho das atividades, e cumprimento da missão da instituição)? Por favor, quantifique sua resposta!		1	2	3	4
3. Os funcionários deste Centro de Pesquisa têm um nível adequado de conscientização e treinamento em procedimentos de proteção à propriedade intelectual, direito autoral e de documentos controlados? Por favor, quantifique sua resposta!		1	2	3	4
4. O Senhor (a) acha importante que o IPEN promova uma ação mais efetiva junto aos usuários sobre procedimentos sobre este item? Por favor, quantifique sua resposta!		1	2	3	4
5. Que tipo de ação o IPEN deveria implementar para melhorar a efetividade da sua política de proteção à propriedade intelectual, direito autoral e de documentos controlados?					

Questões adicionais

1. Que outras medidas de segurança o IPEN deveria adotar para o bom funcionamento de suas atividades, para o cumprimento da legislação em vigor ou obrigações contratuais, e para preservar a imagem da instituição perante a sociedade?				
2. Este Centro de Pesquisa sofreu algum tipo de incidente de segurança da informação nos últimos 12 meses? Se sim, que tipo de incidente ocorreu?				
3. Como o incidente foi tratado?				
4. Foi desenvolvido algum tipo de procedimento ou implementada alguma medida para prevenir que tal evento volte a acontecer?				
5. Quais são os ativos de informação (recursos) mais importantes para as atividades deste Centro de Pesquisa? *Considere:* • *Informações* • *Sistemas* • *Softwares* • *hardware* • *pessoas*				
6. Quais são os requerimentos de segurança mais importantes para cada ativo de informação identificado? Considerar: • confidencialidade • integridade • disponibilidade • outros				
7. 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!	1	2	3	4

APÊNDICE D - Questionário

Prezado (a) colega do IPEN,

O questionário que segue é parte integrante de uma pesquisa de campo para uma tese de doutorado sobre o tema Segurança da Informação no IPEN.

Responda às questões, assinalando a opção que melhor corresponde ao seu comportamento no ambiente de trabalho, diante das situações apresentadas. Não é necessário se identificar.

Muito obrigado por sua colaboração.

Nº	Questões
1	Utilizo senhas fáceis de lembrar (compostas por nomes ou suas iniciais, datas de aniversários, seqüências de letras ou números). ☐ Sempre ☐ Freqüentemente ☐ Raramente ☐ Nunca
2	Escrevo minhas senhas em um pedaço de papel e o deixo afixado no monitor, na torre do micro, ou na minha mesa de trabalho. ☐ Sempre ☐ Freqüentemente ☐ Raramente ☐ Nunca
3	Compartilho minha senha com terceiros (colegas de serviço). ☐ Sempre ☐ Freqüentemente ☐ Raramente ☐ Nunca
4	Executo / abro arquivos recebidos em *e-mails* (anexos), alheios às minhas atividades. ☐ Sempre ☐ Freqüentemente ☐ Raramente ☐ Nunca
5	Clico em links de *e-mails* recebidos de origem desconhecida, quando seu conteúdo me parece interessante (ou o assunto é de meu interesse). ☐ Sempre ☐ Freqüentemente ☐ Raramente ☐ Nunca
6	Permito o acesso aos recursos computacionais do IPEN (meu computador de trabalho, etc) por pessoas não autorizadas (amigos, fornecedores, visitantes). ☐ Sempre ☐ Freqüentemente ☐ Raramente ☐ Nunca
7	Altero a infra-estrutura física da rede do IPEN (ponto de rede, etc) sem prévia aprovação da Gerência de Informática ou responsável imediato. ☐ Sempre ☐ Freqüentemente ☐ Raramente ☐ Nunca
8	Altero as configurações de computadores (*hardware* ou *software*), onde tenho tais direitos, sem autorização do responsável local ou superior imediato. ☐ Sempre ☐ Freqüentemente ☐ Raramente ☐ Nunca
9	Repasso para os colegas mensagens de *E-mails* não relacionadas com as atividades do IPEN, tais como circulares, correntes e piadas. ☐ Sempre ☐ Freqüentemente ☐ Raramente ☐ Nunca
10	Utilizo os recursos computacionais do IPEN (computador, impressora, *Internet*, etc) para fins particulares. ☐ Sempre ☐ Freqüentemente ☐ Raramente ☐ Nunca

11	Compartilho com outras pessoas informações restritas, pertinentes a projetos de pesquisas de que participo no IPEN, ou que tenho conhecimento no exercício de minhas funções. ☐ Sempre ☐ Frequentemente ☐ Raramente ☐ Nunca
12	Forneço informações pessoais quando solicitadas por *e-mails* de órgãos públicos ou de empresas conceituadas no mercado (Bancos, Correios, Receita Federal, justiça eleitoral, etc). ☐ Sempre ☐ Frequentemente ☐ Raramente ☐ Nunca
13	Nos computadores em que possuo tais direitos, instalo programas baixados da *internet* ou que são conseguidos de colegas. ☐ Sempre ☐ Frequentemente ☐ Raramente ☐ Nunca
14	Faço *download* de músicas e vídeos da *Internet* para o meu computador. ☐ Sempre ☐ Frequentemente ☐ Raramente ☐ Nunca
15	Realizo cópia de segurança *(backup)* dos dados / informações que se encontram sob a minha guarda (no meu computador). ☐ Sempre ☐ Frequentemente ☐ Raramente ☐ Nunca
16	Ao me ausentar do local de trabalho, encerro a sessão aberta no computador (faço *logout*), bloqueio a sessão com uso de senha, ou o desligo. ☐ Sempre ☐ Frequentemente ☐ Raramente ☐ Nunca
17	Guardo documentos de caráter sigiloso em local seguro. ☐ Sempre ☐ Frequentemente ☐ Raramente ☐ Nunca
18	Quando percebo uma falha na segurança nos sistemas computacionais, informo-a imediatamente ao administrador do sistema ou ao responsável pela informática do meu setor. ☐ Sempre ☐ Frequentemente ☐ Raramente ☐ Nunca
19	Leio com atenção as notícias e os avisos relacionados com segurança da informação que são emitidas pela Gerência de Informática. ☐ Sempre ☐ Frequentemente ☐ Raramente ☐ Nunca
20	Quando preciso conectar um novo computador na Rede do IPEN, o faço pelas vias normais estabelecidas pela Gerência de Informática (ou seja, solicito a sua autorização). ☐ Sempre ☐ Frequentemente ☐ Raramente ☐ Nunca

Por gentileza, forneça agora algumas informações sobre a sua pessoa para uma melhor análise (entendimento) dos dados gerais coletados na presente pesquisa.

Estes dados não serão utilizados para a identificação do respondente.

21	Sou do sexo: ☐ Masculino ☐ Feminino
22	Minha idade é: ☐ Menos de 20 anos ☐ Entre 20 e 29 anos ☐ Entre 30 e 39 anos ☐ 40 anos ou mais

23	Trabalho no IPEN: ☐ Há menos de 10 anos ☐ Entre 10 e 20 anos ☐ Há mais de 20 anos
24	Meu vínculo com o IPEN é: ☐ Funcionário Público (RJU) ☐ Comissionado ☐ Bolsista / Estagiário ☐ Trabalho Voluntário ☐ Prestador de Serviço
25	Meu grau de instrução é: ☐ Fundamental Incompleto ☐ Fundamental completo ☐ Médio Incompleto ☐ Médio completo ☐ Superior Incompleto ☐ Superior completo ☐ Especialização ☐ Mestrado ou Doutorado
O espaço abaixo está disponível para sugestões e comentários. Fique à vontade para fazer qualquer observação adicional sobre o tema segurança da informação no IPEN. (Opcional)	

APÊNDICE E - Principais processos e sistemas de informação do IPEN

Macro-processo	Processo	Sistema	Finalidade do Sistema	Mecanismo de difusão da informação
Responsabilidade da Direção	Planejamento Estratégico	Plano Diretor	Consolidar as atividades que deverão ser desenvolvidas pela organização pelo período de um ano.	***Intranet*** e documentação física completa e compacta.
		Sistema de Inform. Gerencial e de Planej. do IPEN (SIGEPI)	Acompanhar e apoiar a execução da produção dos serviços e produtos do IPEN, de acordo com o previsto no Plano Diretor.	***Intranet***.
		Sistema para o Diagnóstico do Clima Organizacional	Ferramenta de gestão participativa que se baseia na percepção que os colaboradores têm acerca das práticas executadas pela instituição.	Efetua o diagnóstico de clima a partir da entrada de dados dos questionários respondidos, via ***Intranet***
	Sistema de Gestão Integrada Qualidade, Meio Ambiente e Segurança	SGI	Disponibilizar, os seguintes principais tipos de documentos: Manual de Gestão Integrada do *ipen;* Informe Anual, Relatório de Gestão, Circular CNEN//*IPEN,* Progress Report; Plano do Negócio, de Ação e de Projeto Especial; Relatório de Análise de Segurança; de Análise de Segurança da Instalação Nuclear; de Análise de Segurança da Instalação Radioativa; Manual da Qualidade Setorial; Procedimento Gerencial; Procedimento Gerencial Setorial ; Especificações Técnicas – Instalações, Especificações Técnicas – Produtos; Programa de Garantia da Qualidade – Instalação; Manual da Qualidade de Laboratório, Plano da Qualidade, Planos de Segurança e Meio Ambiente; de Emergência (corporativo), de Proteção Física (corporativo), de Radioproteção (corporativo), de Segurança para Substâncias Controladas e Salvaguarda (Plano de Controle de Material Nuclear) (corporativo), e demais planos	***Intranet*** ou meio físico.
		TNCMC	Tratamento de não - conformidade e melhoria contínua detectado no SGI	***Intranet***

Gestão de recursos	Processos de apoio técnico e administrativo	Sistemas de Controle Administrativo	Para controle orçamentário (integrado ao SIGEPI), compras e licitações, gestão de estoque, recebimento de materiais e serviços, requisições remotas, requisições remotas de almoxarifado, gestão de transportes, gestão administrativa de contratos, controle dos estoques e da produção de radiofármacos.	***Intranet***
		SIASG (CATMAT/ CATSER/SICAF/SICON/SIDEC/SIREPE) / COMPRASNET	**Sistemas da União** para área de Suprimentos que disponibilizam, através da ***Internet***, informações sobre materiais, serviços, fornecedores, contratos, registro de preços, etc, permitindo e facilitando o gerenciamento das aquisições da instituição.	Restritos aos servidores da DAD/A, GAN e GCC
		Sistemas para acompanhamento de Importações	Cadastramento, consultas e controle de processos de importação; Acompanhamento da legislação brasileira sobre comércio exterior	Restrito as servidores da GIE
		Siscomex	**Sistema da União** para importações e exportações.	Restrito as servidores da GIE
		Sistemas para Acompanhamento Financeiro	Sistemas internos para Cobrança Bancária, Execução Financeira e Controle de Diárias e Passagens.	Restrito aos servidores GFC
		SIAFI	**Sistema da União** para o recebimento da dotação orçamentária, realização de empenho, pagamento de fornecedores e recebimento de faturas.	Restritos aos servidores da DAD/A, GFC e GCC
		Sistemas para a Administração Patrimonial	Sistemas internos para cadastramentos, consultas, controle dos bens patrimoniais e permissão para transferência provisória.	***Intranet***
		Sistema de Comercialização de Produtos e Serviços	Sistema, disponibilizado através da ***Homepage*** do Ipen que permite ao cliente cadastrado efetuar pedido de compra, solicitação de serviço e acompanhamento, através da *Internet*.	Acesso aberto aos clientes
		Sistemas de Pessoal/ RH-online	Sistemas internos para a área de Recursos Humanos que disponibilizam, através da *Intranet*, informações (férias, ponto, dossiê, etc) sobre o servidor e para o servidor respectivamente.	Pessoal - restrito aos servidores da GPE RH-online - ***Intranet***
		SIAPE/ SIAPENET	**Sistemas da União** com informações (dados cadastrais, dados variáveis, abonos, pagamento, etc) sobre o servidor e para o servidor respectivamente.	SIAPE - restrito aos servidores da GPE www.siapenet.gov.br

		Sistema Gestor de Desempenho (SGD)	Verificar o desempenho individual dos servidores e da Instituição, baseado no planejamento, acompanhamento e execução das etapas/sub-etapas e/ou atividades definidas conforme o Plano de Trabalho da CNEN.	***Intranet***
		Intranet	Conjunto de dados, sistemas e informações online para uso interno da instituição.	Acesso a partir de qualquer computador conectado à r**ede interna**
		Homepage	Conjunto de dados e informações institucionais disponibilizados para o público em geral	Acesso a partir de qualquer computador conectado à ***Internet***
Realização do produto	Processos de produção e fornecimento de serviços	Sistemas de Gestão da Produção da DIRF	Sistemas para acompanhar a programação, o processamento, o controle da produção e a distribuição de radiofármacos.	Restrito aos servidores da área, com acesso a este serviço da **rede local** da DIRF.
		SIGEPI	Acompanhar e apoiar a execução da produção de serviços e produtos do *ipen*, de acordo com o previsto no Plano Diretor.	***Intranet***
		Sist. de Salvaguarda	Controle de materiais nucleares.	Microcomputador da área.
		Sistema de Informações científicas	Sistema para prover apoio bibliográfico, atualização e disseminação da informação.	***Intranet*** e consulta local ao acervo físico
	Processos de Ensino	Sistema Fênix	Sistema da USP para o acompanhamento dos alunos da Pós-graduação do IPEN.	Restrito aos computadores da área, com acesso a este serviço, na rede USP
		FenixWeb	Sistema da USP com informações da Pós - graduação para alunos, orientadores e responsáveis por disciplinas.	***Internet***
		Sistema de bolsistas e estagiários	Cadastramento, ponto, relatório, estatísticas e declarações.	***Intranet*** - restrito aos orientadores e alunos
		Sistema de coleta de dados	Acompanhamento da Formação de Recursos Humanos	Acesso aberto (**Web**) aos interessados
			Acompanhamento de Seminário PIBIC/PROBIC	
		SIGEPI	Acompanhar e apoiar a execução da função ensino do IPEN, de acordo com o previsto no Plano Diretor.	***Intranet***
		Sistema de Informações científicas	Sistema para prover apoio bibliográfico, atualização e disseminação da informação.	***Intranet*** e consulta local ao acervo físico

	Processos de P&D&E	SIGEPI	Acompanhar e apoiar a execução da função P&D&E do IPEN, de acordo com o previsto no Plano Diretor.	***Intranet***
		Produção Técnico-Científica	Interface para registrar e encaminhar a PTC do IPEN à Biblioteca para validação e inserção no SIGEPI	***Intranet***
		Sistema de Informações científicas	Sistema para prover apoio bibliográfico, atualização e disseminação da informação.	***Intranet*** e consulta local ao acervo físico

Fonte: Relatório de Gestão 2007 do IPEN

GLOSSÁRIO

Backdoor - Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

BackOrifice – Programa desenvolvido pelo grupo *cracker* "*Cult of the Dead Cow*" (Culto à Vaca Morta) que se instala em computadores ligados à *Internet* e permite que estes sejam controlados remotamente.

Backups – O termo é usado para se referir às cópias de arquivos, feitas periodicamente, do disco rígido de um computador para fitas magnéticas ou outro tipo de mídia removível.

Blacklists - *Blacklists* ou *blocklists* são listas de endereços IP, nomes de domínios ou endereços de *e-mails* que podem ser utilizadas para ajudar a identificar spam.

Códigos maliciosos - Termo genérico que abrange todos os tipos de programas especificamente desenvolvidos para executar ações maliciosas em um computador.

Criptografia - Método usado para embaralhar ou codificar dados, de modo a impedir que usuários não autorizados leiam ou adulterem os dados.

Criticidade - Grau de importância da informação para a continuidade dos negócios.

Custodia / custodiante – Guardar, cuidados, tutela.

Disco rígido (HD) - É o dispositivo de armazenamento de dados mais usado nos computadores.

DMZ *DeMilitarized Zone* ou "zona desmilitarizada", em português. Também conhecida como Rede de Perímetro, a DMZ é uma pequena rede situada entre uma rede confiável e uma não confiável, geralmente entre a rede local e a Internet.

Downsizing - O termo *downsizing* é usado em informática para definir uma situação onde sistemas originalmente hospedados em um computador de grande porte são adaptados para minis e microcomputadores. O principal motivo desta migração é a redução de custo.

Falha (*bug*) de sistema - Um erro de programação em um programa de *software* que pode ter efeitos colaterais indesejáveis. Alguns exemplos incluem vários problemas de segurança de navegador da *Web* e problemas de *software* relativos ao ano 2000 (*bug* do milênio).

Firewall - Um sistema de segurança de rede, cujo principal objetivo é filtrar o acesso a uma rede.

Hacking Técnicas e métodos utilizados para ganhar acesso não autorizado e explorar sistemas e redes de computadores. O *hacking*, assim como o *phreaking*, consiste em entender o funcionamento dos sistemas de informação como um todo e então tirar vantagem dele.

Hardware - É a parte física do computador, ou seja, seu conjunto de componentes eletrônicos, circuitos integrados e placas.

Homepage - É a página inicial de um site da *internet*.

Integridade - Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Invasão – Acesso não autorizado a um sistema, *software*, arquivo, dispositivo ou serviço.

Log (*logging*) - Termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Um arquivo de *log* pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.

NetBus - O NetBus é um sistema de administração remoto similar ao *Back Orifice.*

No-break - É um sistema de alimentação elétrico que entra em ação, alimentando os dispositivos a ele ligados, quando há interrupção no fornecimento de energia.

Outsourced - Designa a ação que existe por parte de uma organização em obter mão-de-obra de fora da empresa, ou seja, mão-de-obra terceirizada

Servidor *Web* - Um computador que executa um programa que provê serviço *Web*, ou seja, equipamento onde reside o *website* da organização.

Software – Programa de computador

SPAM - É uma mensagem eletrônica não solicitada enviada em massa.

REFERÊNCIAS BIBLIOGRÁFICAS

1. AFONSO R. 30% das pequenas e médias empresas do País não usam antivírus. ***COMPUTERWORLD.*** São Paulo, 08 jun. 2009. Seção Segurança. Disponível em: <http://computerworld.uol.com.br/seguranca/2009/06/08/30-das-pequenas-e-medias-empresas-do-pais-nao-usam-antivirus/>. Acesso em: 12 jun. 2009.

2. AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA. Estrutura Organizacional. Portaria nº 354, de 11 de agosto de 2006. DOU de 14 de agosto de 2006. Disponível em: <http://www.anvisa.gov.br/institucional/anvisa/estrutura/index.htm>. Acesso em: 14 Mai. 2009.

3. AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA. Política de Segurança Institucional. Portaria nº 20, de 9 de janeiro de 2007. DOU de 11 de janeiro de 2007. Disponível em: <ftp://ftp.saude.sp.gov.br/ftpsessp/bibliote/informe_eletronico/2007/iels.janeiro.07/iels12/U_PT-MS-ANVS-20_090107.pdf>. Acesso em: 14 Mai. 2009.

4. ALBERTS, C. Common Elements of Risk, 2006. Disponível em: <http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tn014.pdf>. Acesso em: 26 set. 2007.

5. ALBERTS, C.; DOROFEE, A. Managing information security risks: The OCTAVE Approach. New York, N.Y.: Pearson Education, Inc., 2007.

6. ALBERTS, C.; DOROFEE, A.; STEVENS J.; WOODY C. Introduction to the OCTAVE Approach, 2003 – CERT/SEI. Disponível em: <http://www.cert.org/octave/approach_intro.pdf>. Acesso em: 27 set. 2007.

7. ALESSIO, P. A. Informação e conhecimento: um modelo de gestão para potencializar a inovação e a cooperação universidade-empresa. 2004. Tese (Doutorado) - Universidade Federal de Santa Catarina, Florianópolis.

8. ALEXANDRIA, J. C. S. Implantação de um sistema de detecção de intrusos de baixo custo na Rede-IPEN baseado em Snort sobre Linux. 2001. Dissertação (Mestrado). Instituto de Pesquisas Tecnológicas do Estado de São Paulo. São Paulo.

9. 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.

10. ALLEN, J. H. Governing for Enterprise Security (GES) Implementation Guide - Article 1: Characteristics of Effective Security Governance, 2007; Carnegie Mellon University, Software Engineering Institute, CERT. Disponível em: <http://www.cert.org/archive/pdf/GES_IG_1_0702.pdf>. Acesso em: 27 set. 2007.

11. ASENSI, F. D. O espaço da ação coletiva na teoria da estruturação de Anthony Giddens. Revista Habitus: revista eletrônica dos alunos de graduação em Ciências Sociais – IFCS/UFRJ, Rio de Janeiro, v. 3, n. 1, p.44-51, 30 mar. 2006. Anual. Disponível em: <http://www.habitus.ifcs.ufrj.br/3gidde.htm>. Acesso em: 27 set. 2006.

12. 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.

13. 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.

14. BAPTISTA D. J. V. DOWNSIZING: da Teoria à Prática – O Processo de Descentralização da Prodabel. 1998. Dissertação (Mestrado). Escola de Governo – Fundação João Pinheiro. Belo Horizonte.

15. BELL, D. O advento da sociedade pós-industrial. São Paulo, S.P.: Cultrix, 1973.

16. BERNARDES, M. C. Modelagem de governança da Segurança da Informação com apoio em sistemas de informação. 2005. Tese (Doutorado) – Universidade de São Paulo - São Carlos.

17. BERNSTEIN, P. L. Against the Gods: The Remarkable Story of Risk. John Wiley and Sons, 1998. Disponível em: <http://books.google.com.br>. Acesso em: 16 nov. 2007.

18. BOSWORTH, S.; KABAY, M. E. Computer security handbook. 4.ed. USA: Wiley, 2002.

19. BOWEN, P.; HASH, J. & WILSON, M. Information Security Handbook: A Guide for Managers, 2006 (NIST Special Publication 800-100). Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>. Acesso em: 27 set. 2007.

20. BRASIL. Lei nº 8.027, de 12 de abril de 1990. Brasília, 1990. Disponível em: <http://www.planalto.gov.br/CCIVIL/leis/L8027.htm>. Acesso em: 19 jun. 2009.

21. BRASIL. Lei nº 8.159, de 8 de janeiro de 1991. Brasília, 1991. Disponível em: <http://www.planalto.gov.br/CCIVIL/leis/L8159.htm>. Acesso em: 12 fev. 2008.

22. BRASIL. Lei nº 9.279, de 14 de maio 1996. Brasília, 1996. Disponível em <http://www.planalto.gov.br/CCIVIL/Leis/L9279.htm>. Acessado em 12/02/2008.

23. BRASIL. Lei n° 9.609, de 19 de fevereiro de 1998. Brasília, 1998a. Disponível em: <http://www.planalto.gov.br/ccivil/Leis/L9609.htm>. Acesso em: 12 fev. 2008.

24. BRASIL. Lei n° 9.610, de 19 de fevereiro de 1998. Brasília, 1998b. Disponível em: <http://www.planalto.gov.br/CCIVIL/Leis/L9610.htm>. Acesso em: 12 fev. 2008.

25. BRASIL. Decreto nº. 2.910, de 29 de dezembro de 1998. Brasília, 1998c. Disponível em: <http://www.planalto.gov.br/CCIVIL/decreto/D2910.htm>. Acesso em: 12 fev. 2008.

26. BRASIL. Decreto nº. 3.505, de 13 de junho de 2000. Brasília, 2000a. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 12 fev. 2008.

27. BRASIL. Lei n° 9.983, de 14 de julho de 2000. Brasília, 2000b. Disponível em: <http://www.planalto.gov.br/CCIVIL/leis/L9983.htm>. Acesso em: 12 fev. 2008.

28. BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Brasília, 2001. Disponível em: <http://www.planalto.gov.br/ccivil/mpv/Antigas_2001/2200-2.htm>. Acesso em: 12 fev. 2008.

29. BRASIL. Resolução nº 7, de 29 de julho de 2002. Brasília, 2002a. Disponível em:<http://www.planalto.gov.br/ccivil_03/Resolu%C3%A7%C3%A3o/2002/RES07-02web.htm>. acesso em: 28 abr. 2009.

30. BRASIL. Decreto nº. 4.553, de 27 de dezembro de 2002. Brasília, 2002b. Disponível em: <http://www.planalto.gov.br/gsi/cgsi/DEC38365.xml>. Acesso em: 12 fev. 2008.

31. BRASIL. Decreto nº. 5.555, de 04 de outubro de 2005. Brasília, 2005a. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/Decreto/D5555.htm>. Acesso em: 12 fev. 2008.

32. BRASIL. Decreto nº. 5.563, de 11 de outubro de 2005. Brasília, 2005b. Disponível em: <http://www.planalto.gov.br/ccivil/_ato2004-2006/2005/Decreto/D5563.htm>. Acesso em: 12 fev. 2008.

33. BRASIL. Instrução Normativa nº 4 do Secretário de Logística e Tecnologia da Informação, de 19 de maio de 2008. Brasília, 2008a. Disponível em: <http://www.governoeletronico.gov.br/anexos/instrucao-normativa-in-nb0-4>. Acesso em: 18 jun. 2009.

34. BRASIL. Instrução Normativa GSI nº 1, de 13 de junho de 2008. Brasília, 2008b. Disponível em: <http://dsic.planalto.gov.br/documentos/instrucao_normativa_01_cgsi.pdf>. Acesso em: 18 jun. 2009.

35. BURGHI M. Pequena empresa não investe em proteção. ***Jornal da Tarde***. São Paulo, 13 jun. 2009. Seção Economia. Ataque Virtual. Disponível em: <http://txt.jt.com.br/editorias/2009/06/13/eco-1.94.2.20090613.4.1.xml>. Acesso em 22 jun. 2009.

36. 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.

37. CADERNO DIGITAL. Especialista adverte sobre o mau uso da Internet no trabalho. 2008. Disponível em: <http://www.cadernodigital.inf.br/interna_noticia.php?idN=2615>. Acesso em: 13 jun. 2008.

38. CAMINHA, J.; LEAL, R. & MARQUES, R. Implantação da Gestão da Segurança da Informação em um Instituto de Pesquisa Tecnológica. In: Congresso ABIPTI 2006, 2006, Campinas. Experiências de modelo de gestão voltado à competitividade, 2006.

39. CÂNDIDO, F. C.; OLIVEIRA, N. Biblioteca: Um caminho para a informação e o conhecimento. ETD - Educação Temática Digital, Campinas, v.7, n.1, p.1-10, dez. 2005 – ISSN: 1676-2592. Disponível em: <http://www.fae.unicamp.br/etd/include/getdoc.php?id=853&article=296&mode=pdf>. Acesso em: 09 jun. 2009.

40. CASANAS, A. D. G.; MACHADO, C. S. O impacto da implementação da norma NBR ISO/IEC 17799 – Código de práticas para a gestão da segurança da informação – nas empresas. 2001. Disponível em: <http://www.abepro.org.br/biblioteca/ENEGEP2001_TR20_0956.pdf>. Acesso em: 13 jun. 2008.

41. 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.

42. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, Cartilha de Segurança para *Internet*- Parte I: Conceitos de Segurança, Versão 3.1, 2006. Disponível em: <http://cartilha.cert.br>. Acesso em: 18 out. 2007.

43. CIALDINI, R. B. Influence: science and Practice. 4.ed. Allyn and Bacon, 2000.

44. CIALDINI, R. B. The Science of Persuasion. Scientific American, 284:2, 2001, 76-81, fev. 2001.

45. CIALDINI, R. B.; GREEN, B. L. & RUSCH, A. J. When Tactical Pronouncements of Change Become Real Change: The Case of Reciprocal Persuasion. Journal of Personality and Social Psychology: Vol. 62(1), 1992, 30-40.

46. CYCLADES. Guia *Internet* de conectividade / Cyclades Brasil. 9º edição. São Paulo. Editora SENAC, 2002.

47. DAVENPORT, T. H. Ecologia da Informação: Porque só a tecnologia não basta para o sucesso na era da informação**.** 2.ed. São Paulo, S. P.: Futura, 2000.

48. DAVENPORT, T. H; PRUSAK, L. Conhecimento Empresarial. Rio de Janeiro: Ed. Campus, 1998.

49. DIRECTION RH. Mudanças organizacionais, 2007. Disponível em: <http://www.directionrh.com.br/mudancas4.htm>. Acesso em: 18 out. 2007.

50. DRUCKER, F. P. The coming of the new organization. Harvard Business Review 66, janeiro / fevereiro de 1988, p. 45-53.

51. 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.

52. FEBRABAN. Padrões de Segurança da Informação: Sistema bancário brasileiro. São Paulo. S.P. :1º. Edição. 1998.

53. FERMA. Norma de Gestão de Riscos. 2003. Disponível em: <http://www.ferma.eu/Portals/2/documents/RMS/RMS-Portugal.pdf>. Acesso em: 17 nov. 2007.

54. FERREIRA, D. A. A. Tecnologia: fator determinante no advento da sociedade da informação?, Perspect. cienc. inf., Belo Horizonte, v. 8, n. 1, p. 4-11, jan./jun. 2003.

55. FONTES, E. L. G.; BALLONI, A. J. Security in Information Systems: Socio-technical Aspects. Artigo apresentado no International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering <http://www.cisse2005.org/cisse2006.aspx>. Disponível em: <http://www.cenpra.gov.br/publicacoes/pdf/2007/cisse_cism.cisa_cenpra.pdf >. Acesso em: 01 nov. 2007.

56. GARCIA W. J. O modelo de Planejamento Estratégico de TI em Empresas Globais. 2005. Dissertação (Mestrado). Universidade Federal de Santa Catarina. Florianópolis.

57. GARFINKEL, S.; SPAFFORD, G. Computer Security: Practical unix & *internet* security. 2.ed. Sebastopol, C.A.: O'Reilly, 1996.

58. GCIO - Government Chief Information Office. Information Security Guidelines for NSW Government Agencies. NSW Department of Commerce. 2007. ISBN: 0734743904. Disponível em: <http://www.gcio.nsw.gov.au/products-and-services/policies-guidelines/InformationSecurityGuidelineV1.1.pdf>. Acesso em: 20 jun. 2009.

59. GIDDENS, A. A constituição da sociedade. 2.ed. São Paulo, S.P.: Martins Fontes, 2003.

60. GIDDENS, A. The Constitution of Society: Outline of the Theory of Structuration. Cambridge, UK: Polity Press, 1984.

61. GIL, A. C. Como elaborar projetos de pesquisa. 4º ed. São Paulo, S.P.: Atlas, 2008.

62. 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.

63. GONÇALVES, J. E. L. As empresas são grandes coleções de processos, RAE - Revista de Administração de Empresas, v. 40. n. 1 . Jan./Mar. 2000.

64. HAAR, H. V. D; SOLMS, R. V. A model for deriving information security control attribute profiles. Computers & Security Vol. 22, No 3, pp 233-244. 2003.

65. HAMMER, M.; CHAMPY, J. Reengineering the corporation. New York, N.Y.: HarperBusiness, 1994.

66. HARRINGTON, H.J. Business Process Improvement. New York, N.Y.: McGraw Hill, 1991.

67. HARRISON, A. Investigating business processes: does process simplification always work? Business Process Management Journal, v.4(2), 137, 1998. Retrieved September 19, 2007, from ABI/INFORM Global database. (Document ID: 84987167).

68. HORTON M.; MUGGE C. Segurança em Redes – Referência rápida. Rio de Janeiro, R.J.: Elsevier Editora, 2004.

69. HUEBNER, A. R.; BRITT, M. M. Analyzing Enterprise Security Using Social Networks and Structuration Theory; Journal of Applied Management and Entrepreneurship, Jul 2006; 11, 3; ABI/INFORM Global pg. 68.

70. INFO CORPORATE. Os perigos de mudar, Nº8 - Março/2004. Disponível em: <http://www.companyweb.com.br/lista_artigos.cfm?id_artigo=28>. Acesso em: 18 out. 2007.

71. INFORMÁTICA HOJE. Quem não vigia direto, corre mais riscos. São Paulo, Junho de 2009, seção mesa-redonda, pags. 34-37.

72. INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES. Plano Diretor 2007-2010. São Paulo, 2007.

73. INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES. Relatório de Gestão 2007. São Paulo, 2008.

74. INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES. PLANO DIRETOR- Programas & Atividades. 2009. Disponível em <http://intranet.ipen.br/diretos/SAR/plan_est/Plano%20Diretor/Plano%20Diretor%202009%20Previsto.pdf>. Acesso em 20 abr. 2009.

75. INSTITUTO OF RISK MANAGEMENT. A Risk Management Standard, Published by AIRMIC, ALARM, IRM: 2002. Disponível em: <http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf>. Acesso em: 26 set. 2007.

76. 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.

77. ITGI - IT GOVERNANCE INSTITUTE. Cobit 4.1 - Framework Control Objectives Management Guidelines Maturity Models – 2007. Disponível em: <http://www.isaca.org>. Acesso em: 18 out. 2007.

78. KERLINGER, F. N. Metodologia da pesquisa em Ciências Sociais. São Paulo: EPU / EDUSP, 1980.

79. KLOMAN, H. F. Enterprise Risk Management: Past, Present and Future. Risk Management Reports May, 2003 - Volume 30, No. 5. Disponível em: <http://www.riskreports.com/protected/archive/rmr0503.html>. Acesso em: 16 nov. 2007.

80. KRUTZ, R. L.; VINES, R. D. CISSP Prep guide. Gold edition. Indianapolis, IN.: Wiley, 2003.

81. LIPNACK, J.; STAMPS, J. Virtual teams. New York: Wiley, 1997.

82. MACKENZIE, M. L. Leadership in the Information Age: A Culture of Continual Change. Bulletin of the American Society for Information Science and Technology; Apr/May 2007; 33, 4; ABI/INFORM Global pg. 10.

83. MARCIANO, J. L. P. Segurança da Informação - uma abordagem social. 2006. Tese (Doutorado) – Universidade de Brasília, Brasília.

84. MARCIANO, J. L.; MARQUES, M. L. O enfoque social da segurança da informação, Ci. Inf., Brasília, v. 35, n. 3, p. 89-98, set./dez. 2006.

85. MATOS, L. S. Dicionário de Filosofia Moral e Política. Instituto de Filosofia da Linguagem. 2001. Disponível em: <http://www.ifl.pt/main/Portals/0/dic/seguranca.pdf>. Acesso em: 27 set. 2007.

86. MICROSOFT. The Security Risk Management Guide, 2006. Disponível em: <http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspx>. Acesso em: 26 set. 2007.

87. MITNICK, K. D.; SIMON, W. L. A arte de enganar: Ataques de Hackers - Controlando o fator humano na segurança da informação. Pearson education, 2003.

88. Modulo Certified Security Officer. Curso Security Officer - Módulo 1: Conceitos Gerais. 2002.

89. 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.

90. NAKAMURA, E. T.; GEUS, P. L. Segurança de redes em ambientes cooperativos. São Pauo, S.P.: Berkiley, 2002.

91. 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.

92. National Infrastructure Protection Center. Risk Management: An Essential Guide to Protecting Critical Assets, 2002. Disponível em: <http://www.iwar.org.uk/comsec/resources/risk/risk-mgmt.pdf>. Acesso em: 26 set. 2007.

93. NUNES V. Segurança da Informação - As câmaras invioláveis do DF. ***Jornal Correio Brasiliense***, Brasília, 15 jun. 2003. Disponível em: <http://www2.correioweb.com.br/cw/EDICAO_20030615/pri_eco_150603_202.htm>. Acesso em: 12 jun. 2009.

94. Organisation for Economic Co-operation and Development. Guidelines for the security of information systems and networks: towards a culture of security. Paris, 2002. Disponível em: <http://www.oecd.org/dataoecd/16/22/15582260.pdf>. Acesso em: 09 ago. 2007.

95. PC WORLD. PC aos 20 anos. São Paulo, S.P, n. 110, p. 43-49, ago. 2001.

96. 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.

97. PELTIER, T. R. Information Security Risk Analysis. 2^{0} Edição. Boca Raton, FL.: Auerbach, 2005.

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

99. PEMBLE, M. What do we mean by “information security”. Computer fraud & security, v. 2004, n. 5, p. 17–19, May 2004.

100. 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.

101. PUPAK, M. O. Identificação dos valores organizacionais do Instituto de Pesquisas Energéticas e Nucleares – IPEN: Uma contribuição para a gestão organizacional baseada em valores. 2003. Tese (Doutorado) - Instituto de Pesquisas Energéticas e Nucleares, São Paulo.

102. RECANTO DAS LETRAS. Resenhas. Filme “O nome da Rosa”. 2006. Disponível em: <http://recantodasletras.uol.com.br/resenhasdefilmes/249488>. Acesso em: 13 out. 2007.

103. REZENDE, S. O. Mineração de Dados, V Encontro Nacional de Inteligência Artificial, UNISINOS, São Leopoldo – RS, 2005. Disponível em: <http://www.addlabs.uff.br/enia_site/dw/mineracaodedados.pdf>. Acesso em: 13 out. 2007.

104. REZENDE, Y. Informação para negócios: os novos agentes do conhecimento e a gestão do capital intelectual, Ci. Inf., Brasília, v. 31, n. 2, p. 120-128, maio/ago. 2002.

105. ROBINSON, C. The Role of a Chief Security Officer. ***CSO online***, USA, Fev. 2003. Disponível em: <http://www.csoonline.com/article/217494/The_Role_of_a_Chief_Security_Officer_?page=1>. Acesso em: 30 abr. 2009.

106. RUSSELL D.; GANGEMI G. T. Computer security basics. USA: O’Reilly, 1991.

107. SACRAMENTO, A. J. C. A. Uma Reflexão Sobre a Segurança nas Comunicações. Revista Militar Nº2464. Maio de 2007, Portugal. Disponível em: <http://www.revistamilitar.pt/modules/articles/article.php?id=60>. Acesso em: 18 out. 2007.

108. SCALET S. D. A 13-point plan for starting a strategic security group. ***CSO online***, USA, Mar. 2006. Disponível em <http://www.csoonline.com/article/220811/A_point_plan_for_starting_a_strategic_security_group>. Acesso em: 01 ago. 2009.

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

110. SETZER, V. Dado, Informação, Conhecimento e Competência. São Paulo: Revista de Ciência da Informação, nº zero, dez. 1999.

111. SOARES L. F. G.; LEMOS G. & COLCHE S. Redes de computadores: Das LANs MANs e WANs às Redes ATM. 2ª Edição. Rio de Janeiro, R.J.: Editora Campus, 1995.

112. SOARES, G. A. D. Censura durante o regime autoritário. Revista Brasileira de Ciências Sociais, São Paulo, v. 4, n. 10, p. 21-43, jun. 1989.

113. SOLMS, B. V.; SOLMS, R. V. The 10 deadly sins of information security management. Computers & Security, v. 23, n. 5, p. 371–376. 2004.

114. 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.

115. SOUSA, I. S. F. A Pesquisa e o Problema de Pesquisa: quem os determina?. Embrapa. 2001. Disponível em: <http://www22.sede.embrapa.br/unidades/uc/sge/texto1.pdf>. Acesso em: 25 mar. 2009.

116. SPURGEON C. E. Ethernet – o guia definitivo. Rio de Janeiro, R.J.: Editora Campus, 2000.

117. SQUIRRA, S. C. M. Sociedade do conhecimento, 2005. Disponível em: <http://www.comtec.pro.br/prod/artigos/squirra_soc.pdf>. Acesso em: 13 out. 2007.

118. STANG, J. D.; MOON, S. Segredos de Segurança de Rede. Tradução Claudio Lobo. Rio de Janeiro, R.J.: Editora Berkeley, 1994.

119. STONEBURNER, G.; GOGUEN, A. & FERINGA, A. Risk Management Guide for Information Technology Systems, 2002 (NIST Special Publication 800-30). Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. Acesso em: 27 set. 2007.

120. STRAUBHAAR, J.; LAROSE, R. Communications media in the information society. Belmont, Wadsworth Publ.Co., 1995.

121. SYMANTEC. Web Based Attacks. 2009. Disponível em: <http://www.symantec.com/connect/sites/default/files/web%20based%20attacks.pdf>. Acesso em: 25 jun. 2009.

122. TANENBAUM A. S. Computer Networks. 4º edição. New Jersey, USA. Prentice Hall PTR. 2003.

123. THOMÉ C. 1h Brasil inaugura unidade para enriquecer urânio. ***O Estado de São Paulo***. São Paulo, 06 mai. 2006. Disponível em: <http://www.mre.gov.br/portugues/noticiario/nacional/selecao_detalhe3.asp?ID_RESENHA=223652>. Acesso em: 27 set. 2007.

124. TIPTON, H. F.; KRAUSE, M. Information Security Management – Handbook. New York, N.Y.: Auerbach Publications, 2003.

125. 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.

126. 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.

127. 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.

128. USA - DEPARTMENT OF DEFENSE. Department of Defense Trusted Computer System Evaluation Criteria. Publicação DOD 5200.28-STD, 1985. Disponível em: <http://csrc.nist.gov/publications/history/dod85.pdf>. Acesso em: 04 nov. 2007.

129. VENTURINI, Y. R. Modelo Ontológico de Segurança para Negociações de Políticas de Controle de Acesso em Multidomínios. 2006. Tese (Doutorado) - Universidade de São Paulo. São Paulo.

130. VERGER, J. Os livros na idade média. Bauru, S.P.: Ed. Edusc. 1999.

131. WIKIPEDIA. Information security, Wikipedia, The Free Encyclopedia, 24 de setembro de 2007, 12:38 UTC. Disponível em: <http://en.wikipedia.org/w/index.php?title=Information_security&oldid=160000515>. Acesso em: 26 set. 2007.

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

133. ZHANG, C. N.; YANG C. Information flow analysis on role-based access control model. Journal: Information Management & Computer Security, Volume:10 Issue:5 Page:225 – 236. 2002.