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

1. INTRODUÇÃO 13
1.1. Objetivos 15
1.1.1. Objetivo Geral 15
1.1.2. Objetivos Específicos 15
1.2. Contribuição do Trabalho 15
1.2.1. Contribuição Original ao Conhecimento 15
1.2.2. Contribuições Específicas 16
1.3. Justificativa 16
2. REVISÃO DA LITERATURA 24
2.1. Sociedade da Informação 24
2.2. Segurança 27
2.3. Segurança da Informação 29
2.3.1. Trabalhos Relacionados 38
2.3.2. Segurança da Informação em Pesquisa Cientifica 39
2.4. Aspectos Humanos da Informação 43
2.5. Fator Humano na Segurança da Informação 48
2.6. Teoria da Estruturação 49
2.6.1. Relacionando Segurança com Estruturação 50
2.7. Entendendo Como os Atacantes Aproveitam-se da Natureza Humana 52
2.8. Tipos de Ataque 56
2.8.1. Engenharia Social 57
2.8.2. Negação de Serviço (DoS e DDoS) 57
2.8.3. Códigos Maliciosos 58
2.8.4. Ataques em Aplicações *Web* 62
2.9. Programa de Treinamento e de Conscientização 65
2.10. Gerenciamento de Mudanças 67
2.10.1. ABNT NBR ISO/IEC 27002:2005 - Gestão de Mudanças 69
2.10.2. COBIT – Gerência de Mudança 69
2.11. Processos de Trabalho 71
2.12. Governança Corporativa 72
2.13. Estabelecendo os Requisitos de Segurança da Informação 73
2.13.1. Análise, Avaliação e Tratamento de Riscos 74
2.13.2. Requisitos Legais 88
2.13.3. Política de Segurança da Informação 89
3. METODOLOGIA 91
3.1. Tipo de Pesquisa 91
3.2. O Problema 92
3.3. Hipóteses 92
3.4. Método de Diagnóstico e Avaliação 93
3.5. IPEN – O Caso Estudado 98
3.5.1. Informática no IPEN 100
3.5.2. Pesquisa Documental 103
3.5.3. Leis e Regulamentos 113
3.6. Parte Experimental 114
4. RESULTADOS E DISCUSSÃO 115
4.1. Nível Estratégico – ISG-HE 115
4.2. Nível Tático - Entrevistas 118

4.2.1. Análise Quantitativa 118
4.2.2. Análise qualitativa 121
4.3. Nível Operacional - Questionário 126
5. PROPOSTA PARA A RE-ESTRUTURAÇÃO DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO 136
5.1. Proposta de Gestão da Segurança 137
6. CONCLUSÕES 146
APÊNDICES 152
APÊNDICE A – Regulamentação (Leis, Decretos e outros) 152
APÊNDICE B - ISG Assessment Tool for Higher Education 158
APÊNDICE C – Roteiro para a Entrevista 165
APÊNDICE D - Questionário 174
APÊNDICE E - Principais processos e sistemas de informação do IPEN 177
GLOSSÁRIO 181
REFERÊNCIAS BIBLIOGRÁFICAS 183

TABELAS

Página

TABELA 1 - Exemplos de incidentes de segurança ocorridos no IPEN.....22
TABELA 2 - Conceito de dados, informação e conhecimento 26
TABELA 3 - Trabalhos relacionados 38
TABELA 4 - Ameaças humanas: origem da ameaça, motivação e ações da ameaça 79
TABELA 5 - União de vulnerabilidade e ameaça 80
TABELA 6 - Pros e contras das avaliações quantitativa e qualitativa 83
TABELA 7- Normas de segurança vigentes no IPEN.....105
TABELA 8 - Normas segurança do IPEN X Categorias de segurança da ISO 27002.....111
TABELA 9 – ISG-HE- Nível de dependência de TI 115
TABELA 10 – ISG-HE - Avaliação global da segurança 116
TABELA 11 - Comparativo entre as duas avaliações 116
TABELA 12 - Consolidação dos dados do ISG-HE.....117
TABELA 13 - Percentuais de conhecimento da normas 118
TABELA 14 - Pontuação obtida na avaliação dos entrevistados 120
TABELA 15 - Escala de referência 121
TABELA 16 - Participantes da pesquisa - questionário 126
TABELA 17 - Médias obtidas em cada questão.....132

FIGURAS

Página

FIGURA 1 - Salão do CPD do IPEN (nos anos 70) 30
FIGURA 2 - Dimensão da dualidade da estrutura.....50
FIGURA 3 - Etapas de um ataque *web*.....64
FIGURA 4 - Processo de trabalho 71
FIGURA 5 - Macro visão de processo de trabalho (negócio) 72
FIGURA 6 - Componentes do risco 76
FIGURA 7 - Modelo do processo de segurança ARBIL 85
FIGURA 8 - Diagrama do método de diagnóstico e avaliação 96
FIGURA 9 - Organograma institucional do IPEN.....99
FIGURA 10 - Organograma da Diretoria de Administração do IPEN.....101
FIGURA 11 - Normas segurança do Ipen X Seções da ISO 27002 110
FIGURA 12 - Conhecimento das políticas 118
FIGURA 13 – Amostra - distribuição por sexo 127
FIGURA 14 – Amostra - distribuição por faixa etária 127
FIGURA 15 – Amostra - distribuição por tempo de serviço 128
FIGURA 16 – Amostra - distribuição por vínculo empregatício 128
FIGURA 17 – Amostra - distribuição por grau de instrução.....128
FIGURA 18 - Médias obtidas entre homens e mulheres 130
FIGURA 19 - Médias obtidas entre as faixas etárias.....130
FIGURA 20 - Médias obtidas de acordo com o tempo de serviço 130
FIGURA 21 - Médias obtidas de acordo com o vínculo empregatício 131
FIGURA 22 - Médias obtidas de acordo com o grau de instrução.....131
FIGURA 23 – Avaliação das questões do questionário 132
FIGURA 24 - Grau de aderência da prática de backup 133
FIGURA 25 - Grau de aderência da prática de criação de senhas.....133
FIGURA 26 - Diagrama da implementação do modelo de gestão da segurança proposto138

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*