Universidade de Brasília - UnB
Faculdade de Economia Administração e Ciência da Informação e Documentação - FACE
Departamento de Ciência da Informação – CID
Programa de Pós-Graduação em Ciência da Informação – PPGCinf

Gestão de Riscos em Tecnologia da Informação como fator crítico de sucesso na Gestão da Segurança da Informação dos órgãos da Administração Pública Federal: estudo de caso da Empresa Brasileira de Correios e Telégrafos – ECT

Luiz Fernando Costa Pereira da Silva

Brasília 2010

Luiz Fernando Costa Pereira da Silva

Gestão de Riscos em Tecnologia da Informação como fator crítico de sucesso na Gestão da Segurança da Informação dos órgãos da Administração Pública Federal: estudo de caso da Empresa Brasileira de Correios e Telégrafos – ECT

Dissertação apresentada à banca examinadora como requisito parcial à obtenção do Título de Mestre em Ciência da Informação pelo Programa de Pós-Graduação em Ciência da Informação do Departamento de Ciência da Informação e Documentação da Universidade de Brasília.

Orientador: Profº. Drº. Renato Tarciso Barbosa de Sousa

Brasília 2010

FOLHA DE APROVAÇÃO

Título: "Gestão de Riscos em Tecnologia da Informação como fator crítico de sucesso na Gestão da Segurança da Informação dos órgãos da Administração Pública Federal: estudo de caso da Empresa Brasileira de Correios e Telégrafos – (ECT)"

Autor: Luiz Fernando Costa Pereira da Silva

Área de concentração: Transferência da Informação

Linha de pesquisa: Gestão da Informação e do Conhecimento

Dissertação submetida à Comissão Examinadora designada pelo Colegiado do Programa de Pós-Graduação em Ciência da Informação do Departamento de Ciência da Informação e Documentação da Universidade de Brasília como requisito parcial para obtenção do título de **Mestre** em Ciência da Informação.

Dissertação aprovada em: 24 de maio de 2010.

Aprovado por:

Prof. Dr. Renato Tarciso Barbosa de Sousa
Presidente – (UnB/PPGCINF)

Prof. Dr. Rogério Henrique de Araújo Júnior
Membro Interno – (UnB/PPGCINF)

Dr. Miguel Filho Ferreira de Oliveira
Membro Externo – (CEF)

Prof.ª Drª. Lillian Maria Araujo de Rezende Alvares
Suplente – (UnB/CID)

À minha Mãe, Tereza Costa Pereira da Silva, pela dedicação e exemplo de vida, que fazem tudo valer a pena.

Agradecimentos

Ao Profº. Drº. Renato Tarciso, meu orientador, pela paciência e orientação segura até a conclusão desta.

Aos professores e colegas do Programa de Pós-Graduação em Ciência da Informação do Departamento de Ciência da Informação e Documentação da Universidade de Brasília, pelas valorosas aulas e discussões.

A Jucilene e Martha, da Secretaria de Pós-Graduação do CID/UnB, pela disposição e presteza no trato dos assuntos "burocráticos".

Aos meus irmãos, Júnior e Vinícius, e irmã, Luciana, pelo carinho família.

À Mariana pelo amor, paciência e companheirismo.

Aos meus amigos da ECT Ricardo, Juliana, Nara, Cristiano e Nassif pelo incentivo e apoio nas minhas ausências.

A todos aqueles que, direta ou indiretamente, contribuíram para a conclusão desta.

Resumo

Este estudo visa investigar o contexto da segurança da informação e da gestão de riscos no ambiente da Empresa Brasileira de Correios e Telégrafos (ECT). Parte-se do pressuposto de que a ECT, ambiente empírico da pesquisa, assim como a maioria dos órgãos da Administração Pública Federal, não tem conhecimento suficiente sobre Gestão de Riscos para implementar uma Gestão de Segurança da Informação eficiente e eficaz. A empresa carece de uma orientação específica sobre “o que fazer” e “como fazer” acerca da implementação de uma Gestão de Riscos em Tecnologia da Informação que fomente a Gestão de Segurança de suas informações. O estado pouco desenvolvido em que se encontra os órgãos da Administração Pública Federal, tanto em nível de conhecimento quanto no tocante às implementações de sua Gestão de Riscos em Tecnologia da Informação, faz com que as orientações governamentais tenham que ser baseadas na mera aplicação das melhores práticas de Segurança da Informação adotadas nacional e internacionalmente. A pesquisa de caráter qualitativo e exploratório, envolvendo pesquisa bibliográfica, pesquisa documental e estudo de caso no ambiente da ECT, tem por objetivo verificar ações que tornam mais eficiente o processo de Gestão de Segurança da Informação, no âmbito da Administração Pública Federal (APF), a partir da Gestão de Riscos em Tecnologia da Informação, considerando a política, o comportamento e a cultura informacional.

Palavras-chave

Gestão de Risco em Tecnologia da Informação; Gestão da Segurança da Informação; Administração Pública Federal; Gestão da Informação; Empresa Brasileira de Correios e Telégrafos (ECT).

Abstract

Studies aimed at investigating the context of information security and of risk management in the environment of the Brazilian Agency for Post and Telegraphs (ECT). It has been assumed that the ECT, empirical environment of this research, and most organizations of the Federal Public Administration, is not aware enough about Risk Management to implement an Information Security Management efficiently and effectively. The company lacks of the one specific guidance about “what to do" and "how to do" for the implementation of Risk Management in Information Technology to promote the Security Management of your informations. The inceptive state where the organizations of the Federal Public Administration, both at the level of knowledge as regards the implementation of Risk Management in Information Technology, makes the government guidelines have to be based on application best practices of Information Security adopted nationally and internationally. The research qualitative and exploratory in nature, involving literature research, documentary research and case study in the ECT’s environment aims to verify actions that make more efficient the process of Information Security Management within the Federal Public Administration (APF) from the Risk Management in Information Technology, considering the policy, behavior and culture information.

Keywords

Risk Management in Information Technology, Information Security Management, Federal Public Administration, Information Management, Brazilian Post and Telegraphs (ECT).

Lista de Figuras

Figura 1 - Esquema da pesquisa 21
Figura 2 - Ciclo de vida da informação. 29
Figura 3 - Ciclo de vida da informação nas organizações 29
Figura 4 - A classificação da Informação segundo a sua finalidade 38
Figura 5 - Fatores econômicos de produção 40
Figura 6 - Classificação da Informação 45
Figura 7 - Objetos de Estudo da CI e da SI 50
Figura 8 - Ciclo de vida da informação e Segurança da Informação 52
Figura 9 - Diagrama de Ishikawa: fatores que interferem na SI 55
Figura 10 - Os pilares da Segurança da Informação 56
Figura 11 - Diagrama de Causas e Efeitos 78
Figura 12 - Matriz de Responsabilidades 86
Figura 13 – Relacionamento entre os termos associados ao risco para a SI 87
Figura 14 - Modelo de Gestão de Riscos 88
Figura 15 - Processo de gestão de riscos de segurança da informação 89
Figura 16 - Definição do contexto 90
Figura 17 - Análise/avaliação de riscos de segurança da informação 91
Figura 18 - A atividade de tratamento do risco 92
Figura 19 - Ciclo de criação da Política de Segurança da Informação da ECT 96
Figura 20 – Perigos x Riscos associados à confidencialidade, integridade e disponibilidade das informações 107
Figura 21 - Diagrama de *Ishikawa* - Desastres Naturais 108
Figura 22 - Diagrama de *Ishikawa* - Falhas no Ambiente Físico 109
Figura 23 - Diagrama de Ishikawa - Furto 109
Figura 24 - Diagrama de *Ishikawa* - *Malware* 110
Figura 25 - Diagrama de *Ishikawa* - *Hacking* 110
Figura 26 - Diagrama de *Ishikawa* - Códigos Ocultos 111
Figura 27 - Diagrama de *Ishikawa* - Falha de *Hardware* 111
Figura 28 - Diagrama de *Ishikawa* - Falha de *Software* 112
Figura 29 - Diagrama de *Ishikawa* - Erro Humano 112
Figura 30 - Matriz de Probabilidade e Impacto – Classificação da Probabilidade 114
Figura 31 - Matriz de Probabilidade e Impacto – Nível de Impacto 116
Figura 32 - Matriz Impacto X Probabilidade 117

Lista de Abreviaturas e Siglas

ABNT – Associação Brasileira de Normas Técnicas

AE – Ambiente Externo

AI – Ambiente Interno

APF – Administração Pública Federal

BS – *British Standart*

Cc – Custo consequência

CC – Common Criteria

CI – Ciência da Informação

COSO – *Committee of Sponsoring Organizations of the Treadway Commission*

CP – Custo Provável

DITEC – Diretoria de Tecnologia da Empresa Brasileira de Correios e Telégrafos

ECT – Empresa Brasileira da Correios e Telégrafos

FERMA – *Federation of European Risk Management Associations*

FR – Fatores de Riscos

GEI – Gestão Estratégica da Informação

GP – Grau de Probabilidade

GSI – Gabinete de Segurança Institucional da Presidência da República

ISO/IEC - *International Organization for Standardization* / *International Eletrotechinical Commision*

ITSEC – *Information Technology Security Evaluation Criteria*

MO – Meios Organizacionais

MTA – Meios Técnicos Ativos

MTP – Meios Técnicos Passivos

PE – Perda Esperada

PNPC – Programa Nacional de Proteção ao Conhecimento

Rc – Redução de dinheiro em caixa

ROI – *Return of Investiment* – retorno de investimentos

SI – Segurança da Informação

Sp – Substituição permanente

St – Substituição temporária

TI – Tecnologia da Informação

Sumário

Introdução 11

Parte I – Requisitos Pré-pesquisa

1. Problema da pesquisa 13
2. Justificativa 18
3. Objetivos 22
3.1. Geral 22
3.2. Específicos 22
4. Hipótese 22
5. Metodologia 22

Parte II – Revisão de Literatura e Fundamentos

6. Informação 24
6.1. Definição de informação 24
6.2. Ciclo de vida da informação 28

7. Gestão Estratégica da Informação (GEI) 31
7.1. O que é estratégia? 31
7.2. Necessidade de segurança da informação 32
7.2.1. Informação como fator estratégico 32
7.2.2. Informação como ativo de valor histórico para a organização 40
7.3. Classificação da informação 42

8. Segurança da informação 46
8.1. Definição de segurança da informação 46
8.2. Atributos da segurança da informação 47
8.2.1. Confidencialidade 47
8.2.2. Integridade 48
8.2.3. Disponibilidade 48
8.2.4. Autenticidade 49
8.2.5. Não repúdio 49
8.2.6. Legalidade 49
8.3. Segurança da informação e a Ciência da Informação 49
8.4. Pilares da segurança da informação 52
8.4.1. Pessoas 52

8.4.2. Processos 53
8.4.3. Tecnologia 54
8.4.4. A relação entre os pilares da segurança da informação 55
8.5. Arcabouço normativo e padrões de segurança da informação 56
8.5.1. *Information Technology Security Evaluation Criteria* - ITSEC 57
8.5.2. Common Criteria for Information Technology Security Evaluation 57
8.5.3. COBIT (Control Objectives for Information and Related Technology) 58
8.5.4. BS 7799 e ISO/IEC 17799 58
8.5.5. ABNT NBR ISO/IEC 27001:2006 58
8.5.6. ABNT NBR ISO/IEC 27005 59
8.5.7. ISO Guide 73 – Risk management – Vocabulary – Guidelines for Use in Standard 59
8.5.8. ISO 13335 – Guidelines for the Management of IT Security 60
8.6. Arcabouço legal de Segurança da Informação 60

9. Gestão de Riscos 64
9.1. Definição de Gestão de Riscos 64
9.2. Termos relacionados à gestão de riscos 67
9.3. Componentes do risco 70
9.3.1. Ameaça 70
9.3.2. Vulnerabilidade 71
9.3.3. Impacto 71
9.3.4. Incidente 71

10. Métodos de Análise de Riscos Organizacionais 71
10.1. Método de Mosler 72
10.2. Método de T. Fine 74
10.3. Diagrama de Causa e Efeito (Diagrama de *Ishikawa*) 77
10.4. Diagrama de Árvore 79
10.5. Técnica de *Brainstorming* 79
10.6. *Brainstorming* inverso (ou invertido) 79
10.7. *Brainswriting* 80
10.8. Brainswriting inverso (ou invertido) 80
10.9. Mapa mental 80
10.10. Diagrama de Pareto 80
10.11. Matriz de Prioridades 81
10.12. Técnica de Painel e de Delfos 81

10.13. Técnica de Análise Associativa e de Cenários 81
10.14. Método Brasiliano 82

11. Gestão de riscos de segurança da informação 87
11.1. Etapas do processo de gestão de riscos de segurança da informação 90
11.1.1. Definição do contexto 90
11.1.2. Análise/avaliação de riscos de segurança da informação 90
11.1.3. Tratamento do risco 91
11.1.4. Aceitação do risco 92
11.1.5. Monitoração e análise crítica de riscos 93
11.1.6. Comunicação do risco 93

12. Conclusão da Revisão de Literatura e Fundamentos 94

Parte III – Estudo de Caso

13. Diagnóstico do processo de gestão de segurança da informação e gestão de risco na ECT 96

14. Identificação dos espaços informacionais dos usuários e riscos aos ativos de informação da ECT 101

15. Estudo de ações para nortear o processo de Gestão de Segurança da Informação e proposta de modelo sistêmico para a Gestão de Riscos que norteie a Gestão de Segurança da Informação 103
15.1. Base normativa 103
15.2. Ambiente 103
15.3. Estratégias e Políticas 104
15.4. Metodologia de Gestão de Segurança da Informação 104
15.5. Modelo de Gestão de Riscos 104
15.6. O emprego de metodologia de análise de risco 105
15.6.1. Avaliação dos perigos analisados 117
15.6.1.1. Desastres naturais 117
15.6.1.2. Falha no ambiente físico 118
15.6.1.3. Furto 118
15.6.1.4. *Malware* 118
15.6.1.5. *Hacking* 118
15.6.1.6. Falha de *Hardware* 119

15.6.1.7. Falha de *Software*..... 119
15.6.1.8. Erro Humano 119

16. Conclusão 120

Referências Bibliográficas..... 123

Anexos
Anexo 1 – Diretrizes da Política de Segurança da Informação da ECT..... 137
Anexo 2 – Estrutura da Norma de Segurança da Informação da ECT 139
Anexo 3 – Instrução Normativa GSI nº 1, de 13 de junho de 2008..... 143
Anexo 4 – Norma Complementar nº02/IN01/DSIC/GSIPR..... 147
Anexo 5 – Método e questionário de captura de informações utilizados no estudo de caso ECT..... 154

Introdução

Em 07 de agosto de 2007, o Gabinete de Segurança da Informação da Presidência da República, por meio da portaria da Secretaria Executiva do Conselho de Defesa Nacional, instituiu um grupo de trabalho composto por representantes de diversos órgãos e entidades da Administração Pública Federal[1]. O grupo de trabalho tinha o objetivo de aperfeiçoar e propor a padronização de normas e procedimentos de Gestão de Segurança da Informação aplicáveis à Administração Pública.

As reuniões e os debates dos representantes evidenciaram a necessidade de criação de um modelo para a Gestão de Segurança da Informação e de uma metodologia de Gestão de Riscos que permitam empregar os recursos destinados à segurança da informação de maneira mais eficiente e eficaz, no âmbito da Administração Pública Federal – APF.

Constatou-se ainda que, não raramente, se tem, nos órgãos da APF, a impressão de que a melhoria nos processos de segurança da informação depende única e exclusivamente de investimentos generalizados em equipamentos de *hardware* e *software*. No entanto, as experiências têm demonstrado que o investimento em recursos de Tecnologia da Informação nem sempre traz o retorno desejado.

De acordo com o *Committee of Sponsoring Organizations of the Treadway Commission* – COSO

> a premissa inerente ao gerenciamento de riscos corporativos é que toda organização existe para gerar valor às partes interessadas. Todas as organizações enfrentam incertezas, e o desafio de seus administradores é determinar até que ponto aceitar essa incerteza, assim como definir como essa incerteza pode interferir no esforço para gerar valor às partes interessadas. Incertezas representam riscos e oportunidades, com potencial para destruir ou agregar valor. O gerenciamento de riscos corporativos possibilita aos administradores tratar com eficácia as incertezas, bem como os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor. (Coso, 2007)

É nesse contexto que se encontra a motivação para a realização desta pesquisa, uma vez que as qualidades inerentes ao gerenciamento de riscos corporativos, apesar de incipientes nas organizações públicas, podem ajudar os administradores públicos a atingirem as metas de desempenho da organização, e

[1] Advocacia Geral da União, Controladoria Geral da União, Ministério da Agricultura, Pecuária e Abastecimento, Ministério das Cidades, Ministérios das Comunicações, Ministério da Defesa, Ministério do Desenvolvimento Industrial e Comércio Exterior, Ministério da Educação, Ministério da Justiça, Ministério das Minas e Energia, Ministério da Previdência Social, Ministério da Saúde, Ministério do Trabalho e Emprego, Comando da Marinha, Comando da Aeronáutica, Banco Central do Brasil, Caixa Econômica Federal, Empresa Brasileira de Correios e Telégrafos, Infraero e Empresa Brasileira de Pesquisa Agropecuária

evitar a perda de recursos. Adicionalmente, o gerenciamento de riscos corporativos pode contribuir para assegurar a comunicação eficaz e o cumprimento de leis e regulamentos, bem como evitar danos à reputação da organização e suas conseqüências.

Em suma, o gerenciamento de riscos corporativos pode ajudar a organização a atingir seus objetivos, com economia de recursos evitando os perigos e surpresas em seu negócio.

Quando as organizações estabelecem estratégias e traçam objetivos para alcançar o equilíbrio entre as metas de crescimento e de retorno de investimentos (ROI), assim como os riscos a elas associados, conseguem explorar seus recursos com mais eficácia e eficiência e maximizar a geração de valores.

O gerenciamento de riscos corporativos tem por finalidade:

- alinhar a tolerância a risco com a estratégia adotada;
- fortalecer as decisões em resposta aos riscos;
- reduzir as surpresas e prejuízos operacionais;
- identificar e administrar riscos múltiplos e entre empreendimentos;
- aproveitar oportunidades;
- otimizar o capital.

Parte I – Requisitos Pré-pesquisa

1. Problema da pesquisa

A informação é um ativo essencial para os negócios de uma organização e, como qualquer outro ativo dessa natureza, precisa ser adequadamente protegido, independente da forma como se apresenta ou do meio pelo qual é compartilhado e/ou armazenado.

A importância da informação pode ser observada se considerarmos a transformação radical ocorrida no perfil do trabalho exercido pela mão-de-obra nas diversas atividades produtivas de um país. O trabalho intensivo foi sendo substituído pela mecanização crescente das tarefas componentes dos processos de produção e transporte, o que permitiu, ao longo dos anos, extraordinários ganhos de produtividade.

Drucker (1991), analisando o perfil da mão-de-obra existente nos países desenvolvidos, constata que apenas 20% de seu total se dedicam diretamente a tarefas operacionais. O restante, 80%, são trabalhadores intelectuais e de serviços cujo elemento de trabalho é a informação. Dessa forma, conclui que a eficácia do tratamento da informação é o elemento crítico da atividade desses trabalhadores.

Lesca e Almeida (1994) apresentam diversos argumentos para justificar a importância da informação para o desempenho das organizações contemporâneas. Um dos mais conhecidos é o da informação como um elemento redutor de incertezas, importante na tomada de decisões estratégicas pertinentes, de melhor qualidade e no momento mais adequado.

Outro argumento aborda a informação como fator de produção importante para projetar e introduzir no mercado produtos e serviços de maior valor agregado. Assim, numa sociedade onde os fatores de produção tradicionais, como energia, tecnologia da informação, mão-de-obra e recursos financeiros, passam a não ser recursos garantidores da vantagem competitiva, a informação figura como fator de produção importante para as organizações.

Sob a ótica da sinergia organizacional, constata-se que o desempenho de uma organização está condicionado à qualidade das ligações e relações entre as unidades que a constituem. A informação é um vetor estratégico importante, pois permite multiplicar a sinergia dos esforços, ao passo que, se mal utilizada, pode anular o resultado de conjunto dos esforços. Consequentemente, além de se preocuparem com o modo como suas atividades são coordenadas, as empresas deveriam estar sempre atentas para a eficácia dos fluxos de informação por meio dos quais se realizam as interdependências organizacionais.

A informação como fator determinante de comportamento é também

uma das razões para considerá-la essencial às estratégias das organizações contemporâneas. No meio social, a informação tem por sentido exercer influência sobre o comportamento dos indivíduos e dos grupos. No ambiente organizacional interno, a informação pode influenciar o comportamento dos indivíduos para que suas ações sejam condizentes com os objetivos da empresa. Externamente, a informação pode influenciar o comportamento dos atores – clientes, fornecedores, parceiros e concorrentes – de modo que seja favorável aos objetivos da empresa.

As empresas são cada vez mais globais e operam em vários lugares e culturas diferentes, o que exige múltiplas habilidades e capacidade de adaptação. Com isso, preliminarmente, ressalta-se a preocupação em garantir recursos e políticas de Segurança da Informação como fatores de salvaguarda de dados e informações. Nesse contexto, a utilização de políticas corporativas de segurança da informação auxilia as organizações a impedir que os concorrentes recolham com sucesso suas informações estratégicas, diferenciais e secretas, controlando as informações sensíveis.

O fato é que não existe segurança total. As organizações e seus sistemas de informação estão vulneráveis a diversos tipos de ameaças à segurança da informação e a exploração dessas vulnerabilidades se torna, a cada dia, mais comum e sofisticada.

Segundo Sêmola (2005), o que torna algo mais ou menos seguro é a gestão de uma série de fatores dentre os quais: política corporativa de segurança da informação; abordagem e estrutura de segurança da informação alinhada à cultura organizacional; comprometimento de todos os níveis gerenciais; conscientização dos envolvidos nos processos organizacionais; gestão de riscos.

O foco da mídia em torno de acontecimentos envolvendo fraudes eletrônicas, sabotagens, espionagens, ataques de *hackers* e vírus eletrônicos tem impactado o comportamento de executivos da maioria das organizações que, não raramente, têm sua imagem e credibilidade questionadas em razão desses incidentes. A preocupação com a gestão de uma política corporativa de segurança da informação assume um papel especialmente importante para os negócios.

O destaque dado às consequências da ausência de uma política corporativa de Segurança da Informação - que garanta a proteção dos sistemas de informação contra a negação de serviços a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados ou informações – corrobora na conscientização de que algo precisa ser feito. No entanto, a urgência em resolver a questão tem levado organizações a adotarem medidas paliativas que não atuam na raiz do problema, ou seja, não prezam pela criação e/ou atualização da política

corporativa de segurança da informação. Em alguns casos, o cenário é ainda pior, pois, além de não resolverem o problema, essas medidas mascaram pontos críticos dando margem a um falso sentimento de segurança.

Podemos observar empiricamente essa situação em parte dos órgãos da Administração Pública Federal (APF), por meio de troca de experiências com os representantes daquelas entidades que fazem parte do Grupo de Trabalho do Gabinete de Segurança da Informação da Presidência da República.

Pode-se perceber, a partir dos contatos estabelecidos, que esses órgãos não contam com conhecimento suficiente para implementar uma estrutura eficiente de gestão de segurança da informação.

Segundo Hilgenberg (2005), o governo brasileiro, por meio da proposição de leis e decretos que levaram a normatização de procedimentos de salvaguarda às informações, manifestou sua preocupação relacionada com a preservação de informações sensíveis. De acordo com o autor, informações sensíveis são aquelas que merecem tratamentos especiais quanto a sua confidencialidade, integridade e disponibilidade.

Dentre os documentos propostos, destacam-se:

- Lei nº 8.159, de 8 de janeiro de 1991 – dispõe sobre a política nacional de arquivos públicos e privados;
- Lei nº 9.983, de 14 de julho de 2000 – altera o Código Penal, inserindo penas para quem altera ou permita alterar dados em sistemas de informação;
- Lei Complementar nº 105, de 10 de janeiro de 2001 – dispõe sobre o sigilo das operações de instituições financeiras;
- Decreto 3.505, de 13 de junho de 2000 – institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, sendo que dois outros decretos foram publicados posteriormente visando ajustar detalhes, foram estes os Decretos 5.110, de 18 de junho de 2004, e 5.495, de 20 de julho de 2005; e
- Decreto 4.553, 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.

O Programa Nacional de Proteção ao Conhecimento (PNPC) é a concretização da função da Agência Brasileira de Inteligência – ABIN, descrita na Lei

nº 9.883/1999, sendo também conseqüência da aprovação da Política de Segurança da Informação, que atende tanto as empresas públicas quanto particulares, pois visa à proteção de conhecimentos sensíveis, estratégicos para a economia nacional.

Em 13 de junho de 2008, foi publicada no Diário Oficial da União a Instrução Normativa GSI/PR nº 1. Elaborada pelo Gabinete de Segurança Institucional da Presidência da República, a instrução disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal.

Essas publicações compõem parte do arcabouço legal que configura a salvaguarda da informação no governo brasileiro.

Vale ressaltar a existência de algumas referências que, ao longo dos anos, vêm moldando os conceitos e as ferramentas de Segurança da Informação, dentre as quais podemos destacar:

- BS 7799 – Publicada em1995 pela *Brithish Standart*, é uma norma padrão de Segurança da Informação. Divide-se em duas partes, sendo a primeira homologada em 2000 e a segunda em 2002. A BS 7799 é a base de gestão de Segurança da Informação usada por diversas metodologias de Governança e Gestão de TI e assim como a maioria das normas de segurança, focaliza três pontos principais para garantir a Segurança da Informação: a confidencialidade, a integridade e a disponibilidade;

- ABNT NBR ISO/IEC 27001:2006: Elaborada no Comitê Brasileiro de Computadores e Processamento de Dados, pela Comissão de Estudo de Segurança Física em Instalações de Informática, esta norma é uma tradução idêntica da ISO 27001:2005, que foi elaborada pelo *Join Technical Commitee Information Technology, subcommitee IT Security Tecchniques* e que constitui primeiro padrão da família de Segurança da Informação relacionado aos padrões ISO que espera-se sejam agrupados à série 27000; e

- ABNT NBR ISO/IEC 17799:2005: Publicada em 2005 pela Associação Brasileira de Normas Técnicas e equivalente a norma publicada em 2000 e revisada em 2005 pelo *International Organization for Standardization* e pelo *International*

> *Eletrotechinical Commision,* é uma norma de Segurança da Informação que traz um conjunto de recomendações para práticas para a gestão da Segurança da Informação.

Embora as informações sob custódia do Estado exijam um tratamento especial para sua proteção, os órgãos da Administração Pública Federal, em sua maioria, não possuem uma política de segurança da informação e nem um processo corporativo de gestão de segurança de suas informações (Gabinete de Segurança Institucional da Presidência da República – GSI, 2006).

A Empresa Brasileira de Correios e Telégrafos (ECT), ambiente empírico deste estudo, possui uma história de atuação social e de tratamento com a informação que corresponde à crescente transformação histórica do próprio País.

No Brasil, a história postal tem início no período colonial com a chegada de Pedro Álvares Cabral, em 1500, quando Pero Vaz de Caminha escreveu e enviou a primeira correspondência oficial ligada ao país. No Período Imperial, D. Pedro I reorganizou os Correios do Brasil de maneira independente e iniciou o processo de criação de administrações de correios nas províncias. O Período Republicano representou para o serviço postal brasileiro um período de modernização, decorrente da aquisição de novas máquinas e da evolução dos transportes (implantação do Correio Aéreo). Tal modernização resultou na ampliação da área de atuação interna e externa dos Correios e permitiu a expansão dos serviços postais às populações de todas as regiões do País.

A Revolução de 30 causou alterações profundas na estrutura político-administrativa do País e acabou atingindo o setor postal. Em 1931, o então presidente Getúlio Vargas baixou o decreto que fundia a Direção-Geral dos Correios com a Repartição-Geral dos Telégrafos. Originava-se assim o Departamento de Correios e Telégrafos, subordinado ao Ministério da Viação e Obras Públicas.

Em 20 de março de 1969, por meio da Lei n^{o} 509, a Empresa Brasileira de Correios e Telégrafos (ECT) foi criada como empresa pública vinculada ao Ministério das Comunicações.

Atualmente, a Empresa Brasileira de Correios e Telégrafos possui uma estrutura organizacional composta por uma Administração Central, formada pelo Conselho Fiscal, Conselho de Administração, Presidência e seis Diretorias, e 28 Diretorias Regionais, com atuação nos estados brasileiros.

Um departamento da Diretoria de Tecnologia (DITEC) é responsável pela gestão da política de segurança da informação da ECT, o que lhe confere um aporte com foco em Tecnologia da Informação e desconsidera aspectos corporativos

pertinentes às demais diretorias, tais como: comercial, econômico-financeiro e de pessoal.

O problema que motiva esta pesquisa surgiu com o aumento da complexidade organizacional somado à crescente demanda de informações das quais depende a Empresa Brasileira de Correios e Telégrafos. Tais fatores evidenciam a necessidade da ECT e dos demais órgãos, que suportam a gestão do Estado, de conhecerem e implementarem, de forma abrangente, sua política de segurança da informação e o processo corporativo de gestão de segurança da informação. Porém, o estado incipiente em que se encontram, no tocante à segurança da informação, faz com que as primeiras orientações governamentais tenham que ser simples, factíveis e alinhadas com as melhores práticas de mercado.

Nesta pesquisa, investigaremos as possíveis respostas para a seguinte questão: Como utilizar a Gestão de Risco em Tecnologia da Informação (TI) para entender os riscos que afetam os negócios dos Órgãos da Administração Pública Federal e definir uma Gestão de Segurança da Informação eficiente?

2. Justificativa

A Intel, ao lançar no mercado o microprocessador, desencadeou uma série de inovações tecnológicas – microcomputadores, serviços de rede, aplicativos empresariais, internet – que transformaram o mundo dos negócios. Hoje, é aceita como válida a ideia de que a Tecnologia da Informação (TI) é uma das peças-chave da “engrenagem comércio”. A TI atua como pilar de sustentação das operações empresariais, une entes distantes de cadeias de fornecimento e, cada vez mais, liga empresas a clientes.

Com a expansão do poder e da presença da TI, o empresariado (público e privado) cada vez mais a encara como um recurso essencial para o sucesso. Este fato fica claramente evidenciado se analisarmos o investimento de capital das empresas. Décadas atrás, os executivos menosprezavam a utilização do computador. Hoje, isso mudou. Presidentes de empresas agora falam rotineiramente sobre o valor estratégico da tecnologia da informação e as maneiras de utilizá-la para obter vantagens competitivas.

Por trás da mudança de mentalidade reside uma premissa simples: a de que com o aumento da capacidade de processamento e da presença da TI aumentou também seu valor estratégico. É uma premissa razoável, mas, atualmente, questionável. Questionável porque as funções básicas da TI – armazenamento, processamento e transporte de dados – estão disponíveis e acessíveis à maioria. Seu

poder e sua presença começam a transformá-los de recursos potencialmente estratégicos em fatores de produção padronizados. Estão virando custos de operação que precisam ser pagos por todos, mas não oferecem distinção a ninguém.

Para Carr (2003),

> [...] o que torna um recurso realmente estratégico – o que o capacita a servir de base para uma vantagem competitiva sustentada – não é sua ubiqüidade, mas sua escassez. Só ganha uma vantagem sobre os rivais aquele que tem ou faz algo que os outros não têm ou não fazem.

Analisando a utilização e a padronização de recursos infra-estruturais anteriores (energia elétrica e ferrovias) nos processos de produção, Carr (2003) destaca: ”Quando um recurso se torna essencial para a competição, mas irrelevante para a estratégia, os riscos que cria passam a importar mais do que as vantagens que oferece”.

Os riscos operacionais associados à TI são muitos – panes técnicas, interrupção de serviço, obsolescência, falhas de segurança, fornecedores ou parceiros não confiáveis, dentre outros. Hoje, um distúrbio de TI pode tornar uma empresa incapaz de produzir seus bens, prestar seus serviços e conectar-se com clientes. Pode, além disso, manchar sua reputação. Mas poucas empresas agem com rigor para identificar e amenizar suas vulnerabilidades.

As organizações continuam investindo na realização de atualizações generalizadas de *hardware* e *software* para aumentar a segurança de seus ativos de informação. Grande parte desse gasto é movida por estratégias dos fornecedores. Grandes empresas fornecedoras de *hardware* e *software* tornaram-se mestres na arte de vender novos recursos e funções de forma a forçar as empresas, principalmente aquelas da Administração Pública Federal, a comprar novos computadores, aplicativos e equipamentos de rede com frequência muito maior do que precisam.

Para Carr (2003), é incomum uma empresa ganhar uma vantagem competitiva graças ao uso distinto de uma tecnologia infra-estrutural madura. Em contrapartida, a interrupção na disponibilidade da tecnologia, por mínima que seja, pode ser devastadora. Logo, uma empresa precisa se preparar para panes técnicas, quedas no serviço e violações da segurança, transferindo sua atenção de oportunidades para a prevenção de vulnerabilidades.

O segredo do sucesso passa por um modelo de Gestão da Segurança da Informação bem definido para cada tipo de risco. Ao tratar a questão da segurança pelo viés da gestão de riscos, o gestor consegue aproximar o assunto da estratégia de

negócios. De acordo com o Instituto Gartner[2], o nível de segurança adequado é proporcional ao grau de risco, que por sua vez vai direcionar o volume de investimentos que a empresa aceita fazer. Nivelar os gastos pelo valor mais alto em segurança de TI pode não ser a decisão mais acertada. É importante mensurar o impacto das ameaças do ponto de vista dos processos. Um determinado nível de risco pode ser aceitável, enquanto outro precisa ser evitado a todo custo e, portanto, demanda um desembolso maior.

No entanto, a Empresa Brasileira de Correios e Telégrafos, assim como a maioria dos órgãos da Administração Pública Federal:

a. não conta com conhecimento sobre Gestão de Riscos em TI suficiente para implementar uma Gestão de Segurança da Informação eficiente e eficaz;
b. carece de uma orientação específica sobre “o que fazer” e “como fazer” a respeito da implementação de uma Gestão de Riscos em TI que fomente a Gestão de Segurança de suas informações. Mesmo aqueles órgãos que têm implementações na área, não contam com amparo legislativo e normativo suficientes que definam uma estratégia de Estado sobre o assunto;
c. está num estado incipiente, seja a respeito do nível de conhecimento seja no tocante às implementações de sua Gestão de Riscos em TI, que faz com que as primeiras orientações governamentais tenham que ser simples e factíveis, mantida a compatibilidade com as melhores práticas sobre Segurança da Informação adotadas nacional e internacionalmente;
d. deve possuir um sistema de operação que, além de traçar rumos, monitorar ações e adequar desvios, deve estar hierarquicamente subordinada à alta administração da organização.

É necessária uma análise cuidadosa das questões relacionadas à Gestão de Risco em TI e à Gestão de Segurança da Informação da Empresa. A melhoria desses processos poderá contribuir com o cumprimento de sua ampla missão institucional, que é "facilitar as relações pessoais e empresariais mediante a

[2] Fundado em 1979, o Instituto Gartner tem sede em Stamford, e possui 3.700 associados, sendo 1.200 analistas de pesquisa e consultores em mais de 75 localidades em todo o mundo. Dedica-se a analisar e pesquisar assuntos da áreas de tecnologia da informação a fim de aconselhar organizações em suas decisões sobre negócios e tecnologia.

oferta de serviços de correios com ética, competitividade, lucratividade e responsabilidade social". (ECT, 2007).

A figura a seguir apresenta um esquema relacionando os fatos observados nos órgão da Administração Pública Federal, o problema e a justificativa para a pesquisa.

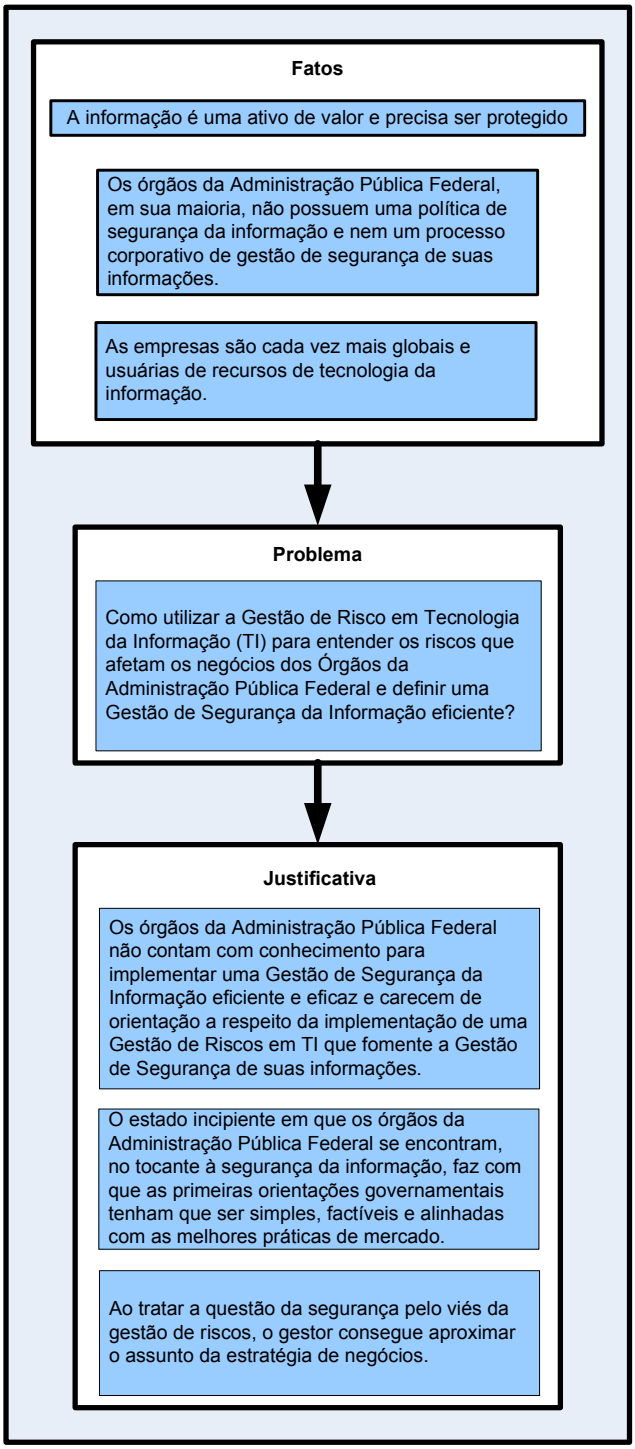


Figura 1 - Esquema da pesquisa. Fonte: elaboração própria

3. Objetivos

3.1. Geral

Estudar ações que tornam mais eficiente o processo de Gestão de Segurança da Informação, a partir da aplicação do conceito de Gestão de Riscos, considerando-se a política, o comportamento e a cultura informacional existentes.

3.2. Específicos

Os objetivos específicos da pesquisa são:

- estudar definições de Gestão de Segurança da Informação;
- diagnosticar o processo de Gestão da Segurança da Informação da Diretoria de Tecnologia da Informação da ECT;
- identificar os espaços informacionais dos empregados da Diretoria de Tecnologia da ECT;
- analisar definições e modelos de Gestão de Riscos;
- propor um modelo sistêmico para a Gestão de Riscos, alinhado com as normas e regulamentações legais, que norteie a Gestão de Segurança da Informação em uma empresa pública.

4. Hipótese

A Segurança da Informação, conceito ainda incipiente nas organizações públicas, é mais eficiente e eficaz quando adota a Gestão de Riscos.

5. Metodologia

Este trabalho caracteriza-se como uma pesquisa aplicada, pois objetiva gerar conhecimento para a aplicação dos conceitos de Gestão de Riscos à Segurança da Informação no ambiente de uma empresa pública.

A abordagem utilizada nesta pesquisa tem um caráter qualitativo. Ao empregar o método qualitativo, busca-se visualizar o contexto da Segurança da

Informação e, se possível, ter uma integração com a Gestão de Riscos, que implique em melhor compreensão da segurança da informação.

A base teórica que dá sustentação a este trabalho é construída a partir de pesquisa bibliográfica e visa estudar os conceitos, definições e modelos de Gestão de Segurança da Informação e Gestão de Riscos.

O universo de pesquisa deste estudo são os órgãos da Administração Pública Federal e, a partir da necessidade prática de selecionar uma amostra que represente corretamente o universo pesquisado, foi escolhida a Diretoria de Tecnologia da Empresa Brasileira e Correios e Telégrafos – ECT.

O diagnóstico do processo de Gestão de Segurança da Informação da Diretoria de Tecnologia da ECT inicia-se com a investigação das iniciativas de Segurança da Informação no ambiente da ECT, utilizando pesquisa documental nas normas, manuais, procedimentos e publicações internas da empresa. O diagnóstico do processo de Gestão de Segurança da Informação, tratado nesta pesquisa, é resultado da comparação entre as iniciativas de Segurança da Informação no ambiente da ECT e as boas práticas recomendadas na literatura e documentos técnicos que abordam o assunto, considerando-se os valores, a cultura e o comportamento humano na empresa.

Embora o objeto de estudo desta pesquisa seja a informação que trafega por meios eletrônicos no ambiente da ECT, o estudo envolve a entrevista com colaboradores da empresa a fim de investigar os espaços informacionais dos empregados da Diretoria de Tecnologia da ECT e entender o comportamento das pessoas envolvidas no tratamento da informação. Todavia, as informações disponíveis em outros meios – tais como unidades arquivísticas e bibliotecas – serão desconsideradas para as análises finais deste trabalho.

O procedimento técnico adotado para investigar os riscos que podem afetar a Segurança da Informação e definir um processo para Gestão da Segurança da Informação a partir da Gestão de Riscos é o estudo de caso.

A primeira etapa do estudo de caso consiste em identificar, por meio de levantamento com colaboradores da ECT, os fatores de riscos que podem afetar a Segurança da Informação e os negócios da empresa.

A etapa seguinte consiste em aplicar um método para a Gestão de Riscos, alinhada com as normas e regulamentações legais, para nortear a Gestão de Segurança da Informação. A aplicação do método é fundamentada em um estudo comparativo entre os principais modelos de Gestão de Riscos conhecidos no mercado com adaptação à realidade da ECT.

Parte II – Revisão de Literatura e Fundamentos

6. Informação

6.1. Definição de informação

No discurso científico, não existe definições verdadeiras ou falsas para conceitos teóricos, em vez disso existem construções destinadas a suportar as pesquisas da melhor forma possível. Diferentes concepções de termos fundamentais como Informação são assim mais proveitosos dependendo da teoria que se espera que eles suportem (Capurro & Hjørland, 2003).

Partindo dessa premissa, neste capítulo será apresentado um apanhado de propostas de definição para os termos dados e informação.

O conceito de informação foi definido por Le Coadic (2004, p. 4), como:

> um conhecimento inscrito (registrado) em forma escrita (impressa ou digital), oral ou audiovisual, em um suporte. A informação comporta um elemento de sentido. É um significado transmitido a um ser consciente por meio de uma mensagem inscrita em um suporte espacial-temporal: impresso, sinal elétrico, onda sonora, etc. Inscrição feita graças a um sistema de signos (a linguagem), signo este que é um elemento da linguagem que associa um significante a um significado: signo alfabético, palavra, sinal de pontuação. (Le Coadic, 2004, p. 4).

Sêmola (2003, p. 45) define informação como: “Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processo comunicativos ou transacionais“. Para o autor, a informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa.

A definição de McGee & Prusak (1994, p.23 e 24) extrapola a idéia de conjunto de dados. Para eles, informação é um conjunto de dados coletados, organizados, ordenados, aos quais são atribuídos significados e contexto. Informação deve informar, enquanto os dados absolutamente não têm essa missão. Informação representa dado em uso, e esse uso implica um usuário.

Para Davenport (1998, p. 18), antes de definir informação é necessário definir dados e conhecimento visto que esses conceitos servem como conexão entre dados brutos e o conhecimento que se pode eventualmente obter. Ele define dados como ”observações sobre o estado do mundo”, e conhecimento como “informação valiosa da mente humana“. Assim, conclui que informação é um conjunto de dados dotados de relevância. Ainda segundo Davenport a informação: requer unidade de análise; exige consenso em relação ao significado; e, exige necessariamente a mediação humana.

Boisot (1998), *apud* Roberts (2000), propõe as seguintes definições para dados, informação e conhecimento:

> Dados são definidos como uma série de observações, medidas ou fatos na forma de números, palavras, sons e/ou imagens. Os dados não têm significado próprio, mas fornecem a matéria prima a partir da qual é produzida a informação. Informação é definida como dados que foram organizados de uma forma significativa. A informação deve estar relacionada com um contexto para possuir significado. Conhecimento é definido como a aplicação e o uso produtivo da informação. (Boisot 1998)

Sianes (2005) define informação como ”uma série de dados organizados de um modo significativo, analisados e processados, que geram hipóteses, sugerem soluções, justificativas de sugestões, críticas, de argumentos, utilizada em apoio ao processo de tomada de decisão. Exige mediação humana e seu valor está associado à utilidade que ela apresenta”.

Em uma definição ampla sobre o que pode ser o conceito de informação, Carvalho (2001, p. 5) relaciona-o ao conceito de dado, significado e contexto. Ela sugere que o conjunto de dados não corresponde a informação, mas pode fazer parte de sua constituição se, para o indivíduo que o recebe, possuir algum significado, o qual é determinado pelo próprio contexto em que aquela pessoa se insere. Dessa forma, se determinados dados não possuírem significado algum para o mesmo, simplesmente são desprezados.

Stair (1998), em seu livro Princípios de Sistemas de Informação, define informação como: “um conjunto de fatos organizados de tal forma que adquirem valor adicional além do valor do fator em si“.

Robredo (2003) apresenta – no primeiro capítulo de sua obra “Da ciência da informação revisitada: aos sistemas humanos de informação” - algumas definições de informação:

- Um conjunto de dados organizado de forma compreensível registrado em papel ou em outro meio e suscetível de ser comunicado. (Harrod’s Librarian Glossary of Terms Used in Librarianship,1989 *apud* Robredo 2003, p.1);

- [...] parece aproximar-se desta definição a de dado (representação de fatos, conceitos ou instruções, de um modo convencional e adequado à comunicação, interpretação ou tratamento por meios humanos ou automáticos), tomado expressamente como sinônimo de informação (ALVES *et al*.,1993 *apud* Robredo (2003), p. 1 e 2)[3];

- 1) Noção, idéia ou mensagem contida num documento. 2) Em Processamento de Dados, o resultado do processamento de dados obtidos por meio de algum tipo de cálculo ou regra de comportamento, que constitui a saída do trabalho de computação[4];

[3] Robredo (2003, p.1) destaca, na definição de Alves (1993), a possibilidade de tratamento do dado/informação por meios automáticos.
[4] Robredo (2003, p.2) destaca a forte relação de informação e documento.

- A informação é o registro de conhecimentos para sua transmissão. Essa finalidade implica que os conhecimentos sejam inscritos num suporte, objetivando sua conservação e codificados, toda representação sendo simbólica por natureza (Dictionnaire encyclopédique de l'information et de La documentation. 2 ème édition. Paris: Nathan, 2001 *apud* Robredo (2003) p. 3);

- Informação é uma propriedade dos dados resultante de ou produzida por um processo realizado sobre os dados. O processo pode ser simplesmente a transmissão de dados (em cujo caso são aplicáveis a definição e medida utilizadas na teoria da comunicação); pode ser a seleção de dados; pode ser a organização de dados pode ser a análise de dados (HAYES, 1986 *apud* Robredo (2003), p. 3);

- A informação é um conhecimento inscrito (gravado) sob a forma escrita (impressa ou digital), oral ou audiovisual[5];

- Informação - 1) Aquilo que reduz a incerteza. (Claude Shannon *apud* Robredo (2003), p. 5); 2) aquilo que nos muda (Gregory Bateson *apud* Robredo (2003), p. 5); e

- informação era um termo (latino) escolástico especializado, menor – informatio – significando o ato de dar ou mudar a forma de uma peça particular de matéria" (Marijuán, 1994 *apud* Robredo (2003), p. 7).

Robredo (2003) ainda destaca algumas características da informação, que é suscetível de ser:

- registrada (codificada) de diversas formas;
- duplicada e reproduzida *ad infinitum*;
- transmitida por diversos meios;
- conservada e armazenada em suportes diversos;
- medida e quantificada;
- adicionada a outras informações;
- organizada, processada e reorganizada segundo diversos critérios;
- recuperada quando necessário segundo regras preestabelecidas.

Araújo (1999), em seu estudo sobre *A construção social da informação*, traz vários conceitos de informação, entre eles:

- processo de atribuição de sentido;
- elemento que provoca transformações nas estruturas (Brookes, 1980 *apud* Araújo (1999));

[5] Robredo (2003, p.4) destaca na definição de Le Codiac (1994) a relação entre o termo informação com a comunicação e a cognição.

- estrutura de qualquer texto capaz de modificar a estrutura da imagem de um receptor (Belkin & Robertson, 1976 *apud* Araújo (1999));
- prática social que envolve ações de atribuição e de comunicação de sentido que por sua vez, pode provocar transformações nas estruturas, pois gera novos estados de conhecimento;
- prática social de um sujeito cognitivo-social que desenvolve ações de atribuição e de comunicação de sentido que, por sua vez, podem provocar transformações nas estruturas (tanto individuais como sociais), pois geram novos estados de conhecimento;
- elemento que representa dupla significação, pois, por um lado, a informação mediatiza os processo de apreensão da realidade e as próprias relações sociais, e por outro, ela é um elemento que adquire características de mercadoria (*commodity*), pois torna-se indispensável à força produtiva. Assim, a informação fica submetida às leis de mercado e ganha valor de troca. Ela transforma-se em informação-mercadoria (Lyottard, 1990).

Para McGarry (1999, p. 4), a informação pode ser:

- considerada como um quase-sinônimo do termo fato;
- um reforço do que já se conhece;
- a liberdade de escolha ao selecionar uma mensagem;
- a matéria prima da qual se extrai o conhecimento;
- aquilo que é permutado com o mundo exterior e não apenas recebido passivamente;
- definida em termos de seus efeitos no receptor;
- algo que reduz a incerteza em determinada situação.

Na literatura é possível encontrar diversas definições a respeito de dado, informação e conhecimento, que pode variar de autor para autor. Apesar das diferenças de conceituação, pode-se identificar um entendimento comum: um conjunto de dados não produz necessariamente uma informação, nem um conjunto de informações representa necessariamente um conhecimento.

Nesta pesquisa o conceito adotado para informação é um conjunto de dados registrados, independente do suporte, dotados de significado e que pode ser transmitido a um usuário (receptor).

6.2. Ciclo de vida da informação

No decurso de suas atividades, uma organização produz, recebe, trata, acumula, usa e descarta informação.

O crescimento das empresas, o acesso à rede mundial de computadores e as novas tecnologias aumentam cada vez mais a quantidade de dados nas corporações. Segundo Feldman (2005), muitos desses dados serão consultados apenas nos seus primeiros dias de vida, mas outros, por legislação ou por necessidade, precisam ser armazenados por mais tempo.

Para Silva, Ferreira e Borges (2002), o ciclo de vida da informação em uma empresa pode variar em função dos fatores que lhe são inerentes, tais como: campo de atuação, porte e tipo de segmento. A importância dada a cada um desses fatores é peculiar de cada empresa e definem o modo de lida com o conjunto das atividades que envolvem a utilização da informação. Gerenciar tais atividades até chegar propriamente ao uso da informação é, segundo Sobreira (1999), uma tarefa das mais complexas e difíceis dentro das empresas.

De acordo com Lyra (2008) e Beal (2008), figuras 2 e 3, o ciclo de vida da informação dentro das organizações se inicia com a identificação das necessidades e requisitos informacionais dos grupos e indivíduos que integram a organizações e de seus públicos externos. Segundo os autores, essa identificação é uma atividade fundamental para desenvolver produtos e serviços informacionais orientados especificamente para cada grupo de pessoas ou processos internos ou externos. A recompensa para o esforço de descoberta das necessidades e dos requisitos de informação é tornar a informação mais útil e os seus destinatários mais receptivos a aplicá-la na melhoria da tomada de decisão ou na melhoria de produtos e processos.

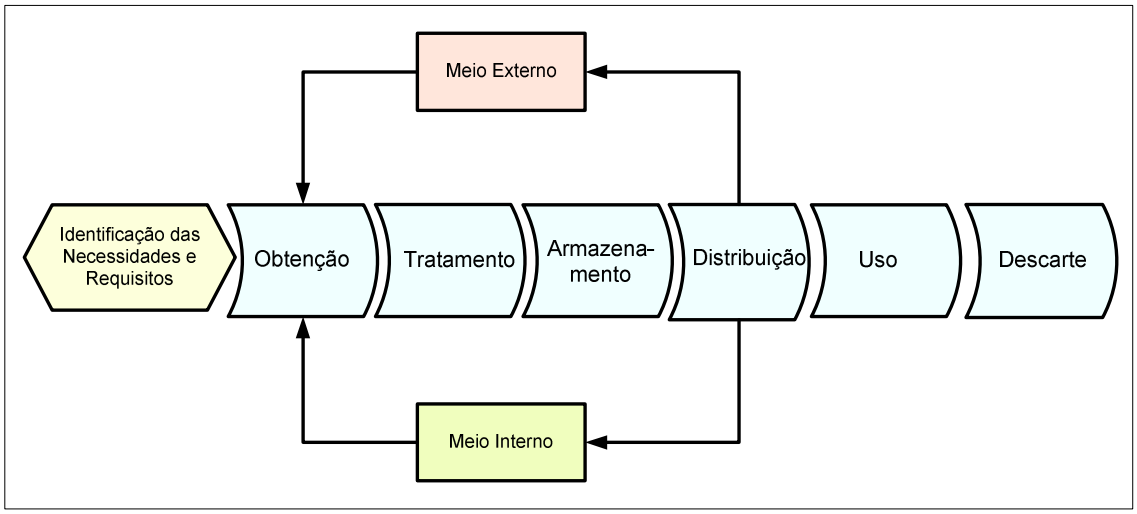


Figura 2 - Ciclo de vida da informação. Fonte: Lyra (2008, p. 9)

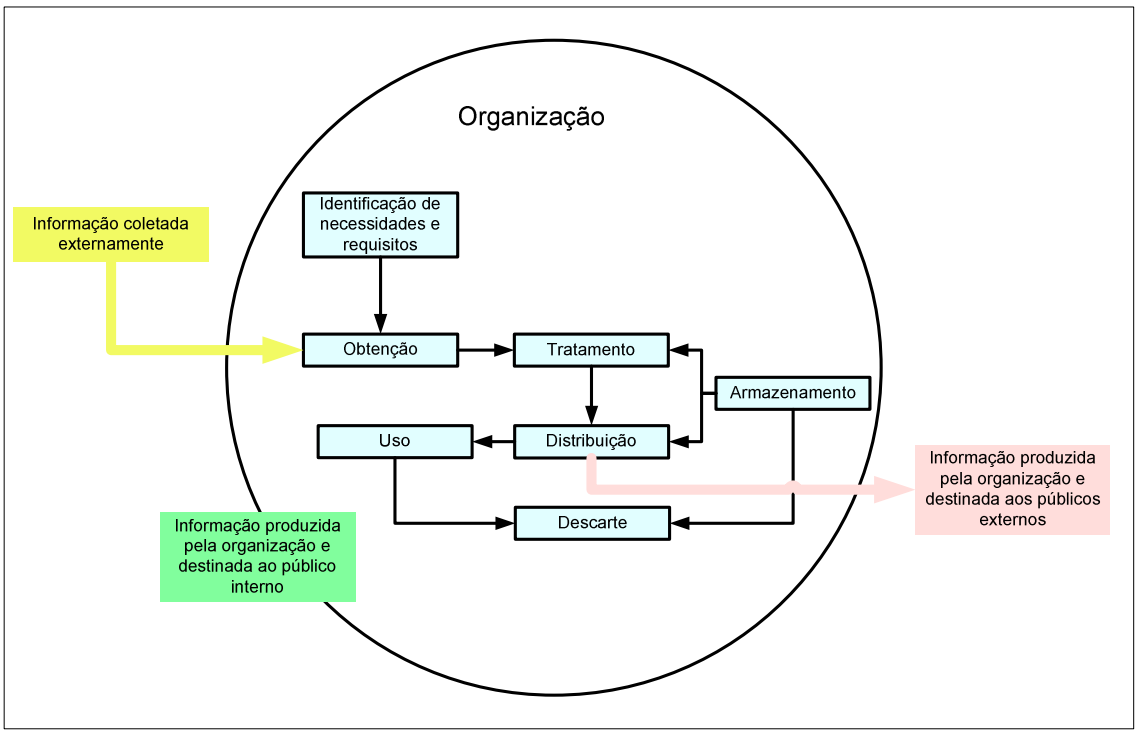


Figura 3 - Ciclo de vida da informação nas organizações. Fonte: Beal (2008, p. 4)

Definidas as necessidades de informação, na próxima etapa – a obtenção – são desenvolvidos os procedimentos de criação, recepção ou captura de informações, provenientes de fontes externas ou internas. Nessa etapa é preciso garantir a integridade da informação, isto é, que a informação é genuína, produzida por pessoa ou entidade autorizada e apresentada de forma precisa e compatível com os requisitos levantados na fase de identificação de necessidades.

Antes de ser consumida, é comum que a informação passe por processos de organização, formatação, estruturação, classificação, análise, síntese, apresentação e reprodução para tornar-se mais acessível e de fácil utilização. Nesta etapa de tratamento, é preciso garantir a integridade da informação, bem como sua confidencialidade.

A etapa de distribuição da informação consiste em levar a informação necessária até seus consumidores. A eficiência do processo de distribuição da informação está diretamente ligada a capilaridade da rede de comunicação da organização e permite que a informação certa chegue tempestivamente a quem necessite dela para a tomada de decisão.

A etapa de uso consiste em utilizar a informação para gerar valor para a organização. Para Beal (2008), a existência da informação por si só não garante melhores resultados para a organização. É necessário que as pessoas utilizem a informação para fomentar os processos ou as tomadas de decisões organizacionais. Nesta etapa os conceitos de integridade, disponibilidade e confidencialidade devem ser aplicados em sua plenitude.

O armazenamento assegura a conservação da informação permitindo o seu uso futuro dentro da organização. Os recursos investidos e a complexidade de armazenamento das informações aumentam proporcionalmente conforme a variedade de formatos e mídias utilizadas para armazená-las. Assim como na etapa de uso, os objetivos de confidencialidade, integridade e disponibilidade são fundamentais nesta etapa.

Quando uma informação torna-se obsoleta ou perde a utilidade para a organização, ela deve ser objeto de processos de descarte que obedeçam a normas legais, políticas operacionais e exigências internas (Beal, 2008). O processo de exclusão de informações corporativas permite a economia de recursos de armazenamento e aumenta a eficiência nos processos de localização da informação, melhorando o processo de Gestão da Informação.

Sêmola (2003) propõe um modelo, associando o ciclo de vida da informação aos os conceitos básicos de segurança, para demonstrar que toda a informação manipulada por uma organização passa por quatro fases distintas, a saber: o manuseio, armazenamento, transporte e descarte. Dessa forma, uma tecnologia que deseje prover segurança deve buscar o equilíbrio entre o ciclo de vida da informação criando mecanismos de proteção para todas as fases deste processo respeitando os conceitos básicos de segurança e possíveis aspectos complementares.

7. Gestão Estratégica da Informação (GEI)

7.1. O que é estratégia?

Segundo Bethlem (1981), a palavra estratégia foi inicialmente utilizada no âmbito militar, entendida como grande tática, centrada na força. A partir do século XX, a estratégia passou a significar a seleção de meios e objetivos, privilegiando fatores psicológicos em detrimento da força.

Beuren (2000, p. 41), afirma que a partir da década de 60, emergiram várias definições de estratégia. Todavia, caracterizada como a composição de planos e metas com a finalidade de atingir o objetivo da organização, configurou-se como um indicador dos negócios da empresa e dos meios para reagir frente às mudanças ambientais, auferindo, então o sentido organizacional. Em sua obra, a autora cita vários conceitos de estratégia, entre eles:

- um dos vários conjuntos de regras de decisão para orientar o comportamento de uma organização, ou melhor, é um mix de produto/mercado (Ansoff, 1990);

- é um método (intenções conscientes) de ação para diferentes situações, que pode ser geral ou específica. Quando é específica, a estratégia é vista como uma manobra que tem a intenção de amedrontar competidores. Como padrão é o próprio padrão de comportamento de uma empresa, que estar consciente dele ou não. A estratégia como posição identifica qual a situação da empresa no mercado, sua posição no ambiente. E como perspectiva, é a visão de mundo que a empresa tem (Mintzberg, 1992);

- um plano, um padrão de ações, uma posição produto mercado ou uma perspectiva específica (Simons, 1994); e

- é a criação de uma posição singular e valiosa, envolvendo um conjunto diferente de atividades. A essência do posicionamento estratégico é escolher atividades que sejam diferentes das atividades dos concorrentes (Porter, 1996).

A estratégia competitiva de uma empresa define suas atividades comerciais, a forma de operar essas atividades e, particularmente, a forma de

diferenciar seus produtos e serviços daqueles oferecidos pelos concorrentes. Em primeiro lugar, as estratégias devem considerar os clientes da empresa e os segmentos de mercado aos quais a organização almeja servir. Segundo, as estratégias devem considerar habilidades e recursos que a organização deverá reunir para fornecer produtos e recursos a esses mercados. Esses dois pontos dependem da informação.

"A questão da diferenciação é fundamental para uma compreensão da estratégia competitiva, pois uma estratégia efetiva deve definir as formas pelas quais os produtos e serviços de uma empresa serão superiores aos de seus concorrentes aos olhos dos clientes." (McGee e Prusak, 1994, p. 22)

Para Beuren (2000, p.43),

> a definição e a tradução da estratégia, de forma compreensível e factível aos membros da organização, passa pela necessidade de disponibilizar informações adequadas aos responsáveis pela elaboração da estratégia empresarial. A adaptação da empresa aos novos paradigmas de um mercado globalizante, exigindo capacidade de inovação, flexibilidade, rapidez, qualidade, produtividade, dentre outros requisitos, torna cada vez mais estratégico o papel que a informação exerce.

7.2. Necessidade de segurança da informação

7.2.1. Informação como fator estratégico

Segundo McGee e Prusak (1994), o surgimento da tecnologia da informação[6] trouxe a idéia de que computadores digitais de alta capacidade permitiriam a otimização das organizações e o fornecimento, sempre tempestivo, de informações precisas e no local apropriado. Contudo, com o decorrer dos anos, essa realização mostrou ser muito mais difícil do que se esperava.

Os autores ressaltam que, muitas vezes, as limitações da tecnologia e dos profissionais de TI são apontadas como fatores que favorecem o fracasso dessa possibilidade. As organizações – talvez de forma enganada – continuam a esperar que a próxima geração tecnológica seja capaz de materializar essa idéia ou que os profissionais melhor capacitados serão capazes de encontrar o elo perdido entre oportunidade de negócios e a promessa da tecnologia.

De fato os produtos e serviços de TI evoluem a cada dia e, além de apresentarem soluções para velhos problemas, criam novas oportunidades. Destarte, os limites tecnológicos não constituem desculpas aceitáveis para fracassos constantes

[6] "Tecnologia da Informação (TI): solução ou conjunto de soluções sistematizadas baseadas no uso de métodos, recursos de informática, de comunicação e de multimídia que visam a resolver problemas relativos à geração, tratamento, processamento, armazenamento, veiculação e reprodução de dados, e a subsidiar processo que convertem dados em informação". Beal (2005, p. 8)

na aplicação da tecnologia da informação para atender às necessidades da organização. O problema fundamental continua a ser o mesmo: definir a informação correta, em tempo hábil e no local adequado.

Acompanhamos, ao longo das últimas quatro décadas, a transição da era industrial para a era da informação. Nesse novo contexto, a concorrência entre as organizações fundamenta-se na capacidade de adquirir, tratar, interpretar e utilizar a informação de forma eficaz.

Assim, os investimentos em tecnologia por si próprios não criam valor adicional, mas sim o uso dessa tecnologia. O valor da tecnologia da informação depende da informação e do papel desempenhado por ela nas organizações.

> A criação, captação, organização, distribuição, interpretação e comercialização da informação são processos essenciais. A tecnologia utilizada para apoiar esses processos é consideravelmente menos importante do que a informação contida nos sistemas. A Informação é dinâmica, capaz de criar grande valor e é o elemento que mantém as organizações unificadas. A tecnologia da Informação pode ser um fator importante no aperfeiçoamento do uso da informação, mas facilmente poderá se transformar num "peso morto, inútil, sem a informação e os seres humanos usuários. (McGee e Prusak, 1994, p. 5).

O contraste entre os investimentos maciços em tecnologia da informação, seu evidente potencial transformador, e os lucros auferidos contribuíram para uma percepção crescente entre as organizações de que é preciso reexaminar seus pressupostos fundamentais quanto à estruturação e o uso da informação e de sua tecnologia. Os investimentos em tecnologia da informação eram apregoados por vendedores, consultores e jornalistas como ferramentas que criariam uma revolução no mundo executivo. A tecnologia da informação criaria escritórios sem papéis onde todos os empregados, executivos e escriturários, da mesma forma receberiam "poderes" para fazer contribuições mais criativas e significativas para que suas empresas alcançassem seus objetivos.

Outra idéia que encanta e atrai muitas organizações é que os investimentos em tecnologia da informação podem ser estratégicos e capazes de criar uma vantagem competitiva substancial.

Em uma análise mais ampla, Phahalad e Hamel (1990), sugerem que esses investimentos em tecnologia representam uma resposta a necessidades internas, ao invés de uma ação estratégica consciente, que proporciona vantagem competitiva em curto prazo.

Para McGee e Prusak (1994), a idéia de que problemas e situações complexas podem ser solucionados com associação de recursos financeiros a

máquinas é altamente tentadora. De fato, há situações onde isso é verdadeiro, porém, esse certamente não é o modelo a ser universalmente adotado. Essa idéia já levou empresas a gastarem milhões de dólares em sua busca por um objetivo esquivo e, em última instância, falso.

Qual será o valor da tecnologia da informação na era da informação? Certamente, uma das respostas fundamenta-se no fato de que a própria informação constitui e fornece o maior potencial de retorno às organizações. No entanto, o ritmo alucinante das mudanças na indústria da tecnologia da informação tende a manter as atenções voltadas mais para aquilo que a tecnologia é capaz de fazer do que para se obter melhores informações.

Por se tratar de um recurso estratégico a informação precisa ser administrada e merece a mesma atenção dispensada aos recursos humanos e financeiros da organização. Para isso, as organizações devem investir em processos estruturados para o gerenciamento da informação. Do ponto de vista estrutural, esses processos devem fornecer suporte e reforço mútuo, criando espaço de informação dentro do qual as pessoas possam executar suas tarefas diárias. Esses processos de administração e arquitetura da informação devem ser concebidos e desenvolvidos com uma apreciação bem completa das dimensões políticas da informação. Para que a execução da estratégia possa ocorrer sem incidentes, o processo e a arquitetura da informação deverão encorajar atitudes desejáveis quanto à informação e desencorajar atitudes pouco desejáveis.

Para Alvarenga Neto, Barbosa e Pereira (2007), existe a percepção, por parte dos dirigentes das organizações, de que a informação e o conhecimento consolidam-se como os principais fatores de diferenciação para a competitividade organizacional. Tal fato sustenta a idéia de que a Gestão Estratégica da Informação deve nortear e validar as atividades e outros temas vinculados à gestão do conhecimento, como a gestão de capital intelectual, a aprendizagem organizacional, a criação e transferência do conhecimento, a gestão da inovação, as comunidades de prática e a inteligência competitiva.

> O desafio organizacional contemporâneo traduz-se em aprender a nadar em um oceano de informações, prospectando e coletando informações relevantes para a sobrevivência organizacional e para a compreensão de um ambiente de negócios cada vez mais dinâmico e mutável. Destarte, reafirma-se que a evidência deste novo paradigma sugere também a emergência de organizações cujos principais fatores de competitividade sejam pautados no binômio informação-conhecimento. (Alvarenga Neto; Barbosa & Pereira, 2007, p. 9)

A ação organizacional tem suas origens na prospecção do ambiente organizacional – interno e externo – em busca de informações relevantes para a compreensão dos negócios, clientes e demais fatores ambientais em suas interações complexas. Tal informação pode reduzir ou aumentar a incerteza e, na hipótese da ocorrência da última, cabe à organização a tarefa de promover rodadas sucessivas de negociação e interpretação até que uma construção coletiva ou entendimento compartilhado seja alcançado.

Diversos argumentos justificam a importância da informação de qualidade relevante, precisa, consistente, clara e oportuna para as organizações.

Lesca e Almeida (1994), apontam:

a. A informação como fator de apoio à decisão

A informação possibilita a redução de incertezas na tomada de decisões e permite que essas sejam feitas de forma pertinente, tempestiva e com menor risco.

Entretanto, Beal (2004, p.21) afirma que “a qualidade das decisões irá depender tanto da qualidade da informação provida quanto da capacidade dos tomadores de decisão de interpretá-la e usá-la na escolha das melhores alternativas.“

b. A informação como fator de produção

Numa sociedade onde os fatores de produção tradicionais, como energia, tecnologia da informação, mão-de-obra e recursos financeiros, passam a não ser recursos garantidores da vantagem competitiva (Drucker, 1991), a informação figura como elemento importante para se criar e introduzir no mercado produtos de maior valor adicionado.

c. A informação como fator de sinergia

A qualidade das ligações e a inter-relação de suas unidades interferem diretamente no desempenho de uma organização. A eficácia do fluxo de informação, por meio dos quais se realizam as interdependências organizacionais, permite multiplicar a sinergia dos esforços ou anular o resultado do conjunto dos esforços.

d. A informação como fator determinante de comportamento

A informação exerce influência sobre o comportamento dos indivíduos e grupos, internos e externos às organizações. Internamente,

a informação pode influenciar o comportamento dos indivíduos para que suas ações sejam condizentes com os objetivos da empresa. Externamente, a informação pode influenciar o comportamento dos atores – clientes, fornecedores, parceiros e concorrentes – de modo que seja favorável aos objetivos da empresa.

McGee e Prusak (1994) apresentam:

a. Informação e definição de estratégia

A informação sobre o ambiente competitivo e sobre a organização atual auxilia os executivos a identificarem tanto as ameaças quanto as oportunidades para a empresa e cria o cenário para uma resposta competitiva mais eficaz. A informação funciona como um recurso essencial para a definição de estratégias alternativas.

b. Informação e execução da estratégia

A tecnologia da informação propicia novas alternativas para a elaboração de processos que criam e oferecem produtos e serviços. A informação representa uma das ferramentas mais importantes e maleáveis a serem utilizadas pelos executivos para diferenciar produtos e serviços. Em alguns casos, a informação é o próprio produto.

c. Informação e integração

O *feedback* da informação sobre desempenho é essencial para a criação de uma organização flexível onde existe um constante "aprendizado", que imediatamente implementa a realização estratégica de seus objetivos e reconhece a necessidade de modificar esses objetivos quando os mesmos se tornam ineficazes.

Choo (2003, p. 27) destaca três searas onde a criação e o uso da informação desempenham papel estratégico no crescimento e na capacidade de adaptação das empresas:

a. A organização utiliza a informação para dar sentido às mudanças do ambiente externo.

Na era da informação, o desempenho das organização é moldado pelas forças e dinâmica do mercado. A vantagem competitiva pode ser obtida a partir da capacidade de perceber a influência do ambiente externo nos processos organizacionais. Em conseqüência

disso, uma tarefa crucial na gestão organizacional é distinguir as mudanças mais significativas, interpretá-las e criar respostas adequadas para elas, garantindo que a organização de adapte e continue prosperando num ambiente dinâmico.

b. A organização cria, organiza e processa a informação de modo a gerar novos conhecimentos por meio do aprendizado

Novos conhecimentos permitem que as organizações desenvolvam novas capacidades, criem novos produtos e serviços, aperfeiçoem os produtos e serviços já existentes e melhores os processos organizacionais.

c. As organizações buscam e avaliam informações de modo a tomar decisões importantes

> Na teoria, toda decisão deve ser tomada racionalmente, com base em informações completas sobre os objetivos da empresa, alternativas plausíveis, prováveis resultados dessas alternativas e importância desses resultados na organização. Na prática, a racionalidade da decisão é atrapalhada pelo choque de interesses entre sócios da empresa, pelas barganhas e negociações entre grupos e indivíduos, pelas limitações e idiossincrasias que envolvem as decisões, pela falta de informações e assim por diante. A despeito dessas complicações, uma organização deve manter ao menos a aparência de racionalidade, para manter a confiança interna e, ao mesmo tempo, preservar a legitimidade externa. Embora a tomada de decisões seja um processo complexo, não há dúvida de que ela é uma parte essencial da vida da organização. (Choo, 2003)

A mensagem estratégica enviada por uma economia baseada na informação é clara:

- A informação torna-se cada vez mais a base para a competição;
- As necessidades do gerenciamento de informação devem acionar as alternativas tecnológicas;
- Os executivos devem identificar claramente o papel que a informação irá desempenhar na estratégia competitiva de sua empresa. (McGee e Prusak, 1994, p. 16)

A informação, segundo Sêmola (2005, p.286), torna-se um fator essencial na corrida das organizações em busca de agilidade, competitividade, modernização, lucratividade e principalmente flexibilidade e adaptabilidade para o crescimento – fatores primordiais para que as empresas prosperem na era da

informação. Isso justifica porque, a informação, como ativo, bem e patrimônio organizacional, deve estar bem guardada como um segredo de negócio.

A informação, segundo Fontes (2000, p. 34), é um bem da organização e possui valor para a organização, para seus concorrentes, para os funcionários insatisfeitos, para os ladrões eletrônicos e para os não eletrônicos. Portanto, ela deve ter um processo de segurança compatível com seu porte, que gerencie, estruture e responsabilize o seu uso. Da mesma forma que o recurso financeiro possui controles, métodos, responsáveis e auditorias, o recurso informação também precisa de um processo contínuo que controle os acessos dos usuários, descreva regras de utilização, estabeleça responsáveis e que possa ter todos estes procedimentos auditados. A liberação de um acesso à informação crítica deve ter controles equivalentes a um repasse financeiro na empresa: pedido explícito, responsáveis, registro e autorização da diretoria.

Para Moresi (2001, p. 111), a informação é um dos recursos mais importantes e sua gestão e aproveitamento estão diretamente relacionados ao sucesso de uma organização. O autor cita Chaumier (1986) para destacar duas das principais finalidades da informação: para conhecimento dos ambientes internos e externos de uma organização e para atuação nesses ambientes. Considerando o papel que a informação pode desempenhar nas atividades de uma organização, o autor propõe uma derivação da classificação do valor da informação, conforme figura abaixo:

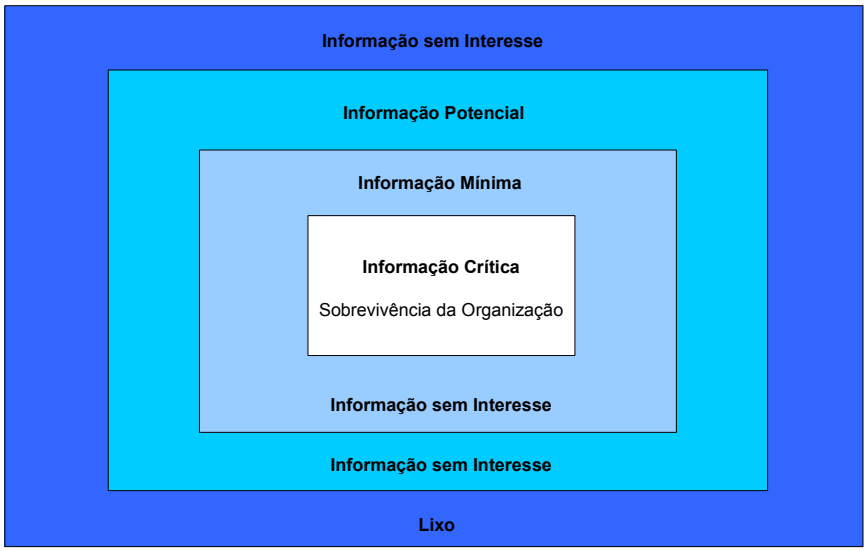


Figura 4 - A classificação da Informação segundo a sua finalidade para uma organização. Fonte: Moresi (2001, p. 112)

Barreto (1996 *apud* MORESI 2001) define valor da informação como: estruturas significantes com a competência de gerar conhecimento no indivíduo, em seu grupo ou na sociedade.

Cronin (1990 *apud* MORESI 2001) classifica o valor da informação nos seguintes tipos:

- Valor de uso: é baseado na utilização final que se fará com a informação;
- Valor de troca (ou de mercado): é aquele que o usuário está preparado para pagar e variará de acordo com as leis de oferta e de demanda;
- Valor de propriedade: reflete o custo substitutivo de um bem;
- Valor de restrição: quando o uso de informações secretas ou de interesse comercial fica restrito apenas a algumas pessoas.

Por ser um bem abstrato e intangível o valor da informação estará associado a um contexto, considerando que a partir de determinada informação uma organização poderá obter alguma vantagem competitiva ou diferencial de mercado em relação a outra organização. (Moresi, 1991, p. 113)

Portanto, considerando contextos organizacionais diferentes, uma mesma informação pode ser de extrema relevância para determinada organização em dado momento e não representar nenhum interesse para outra organização.

Para Wetherbe (1987 *apud* Moresi 2001), o valor da informação está relacionado ao efeito que ela tem sobre o processo decisório de um gestor. Se a informação adicional resultar em uma decisão melhor, então ela terá valor.

A informação é um importante ativo de valor para os negócios. Dessa forma, os processos de definição, implantação, manutenção e melhoramento contínuo da segurança da informação podem ser atividades fundamentais para assegurar a competitividade, alavancar os lucros, atender aos requisitos legais e a preservar a imagem de uma organização junto ao mercado.

É importante ressaltar que tradicionalmente as empresas dedicam atenção especial à proteção de seus ativos físicos e financeiros, mas pouca atenção aos seus ativos de informação. Para Caruso & Steffen (1999, p. 23), ainda que as informações não sejam passíveis do mesmo tratamento físico-contábil que os outros ativos, do ponto de vista do negócio elas são um ativo da empresa, pois de forma análoga envolvem os três fatores de produção tradicionais: capital, mão-de-obra e processos. Portanto, devem ser protegidas.

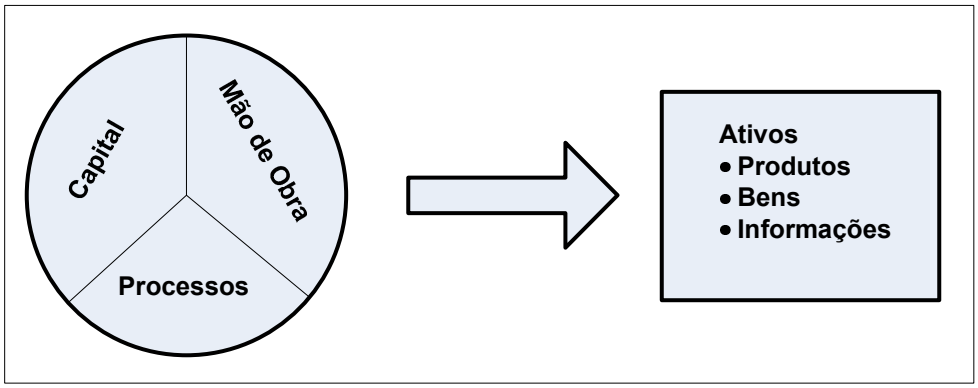


Figura 5 - Fatores econômicos de produção. Fonte: Caruso & Steffen (1999, p. 23)

7.2.2. Informação como ativo de valor histórico para a organização

Durante a Conferência de Zagreb, em 1957, o arquivista italiano A. Lombardo, *apud* Bellotto (2004), afirmou que “não há arquivos que sejam, em essência, históricos, e todo papel administrativo, desde sua criação, tem, em potencial, um valor histórico”.

Grande parte das organizações mantém como testemunho de outras épocas uma série de documentos – políticas, normas, relatórios, fotografias, pareceres etc – que fornecem informações fundamentais para o entendimento de sua trajetória e de seus processos contemporâneos.

Morris Rieger (1979), considerando o valor dos documentos para as organizações, define duas classes para os documentos que compõem o patrimônio documental: os documentos de valores primários e os documentos de valores secundários. “O valor primário é a própria razão do documento; já o valor secundário é um valor residual que os papéis ainda podem conservar”. Dessa forma, o arquivista considera como documentos de valor secundário:

- os que mantém valores administrativos, jurídicos, financeiros para a administração de origem ou para outras administrações, depois de ter perdido seu valor primário para as operações correntes;
- os que podem ter valor para a proteção dos direitos cívicos, jurídicos e de propriedade de certos cidadãos;
- os que refletem a evolução histórica da administração de origem, de seus métodos e operações mais importantes;
- os que possuem valor de informação, isto é, que aportem uma contribuição importante para a pesquisa e para os estudos no domínio do conhecimento.

Para Alberch Fugueras & Cruz Mundet, (1999, p.167), o patrimônio documental é resultado de uma lenta e prolongada sedimentação de documentos, gerados enquanto materialização de uma ação administrativa e, inicialmente, sem levar em conta a utilidade para uma futura exploração com finalidades culturais e científicas.

De acordo com Goulart (2002, p.8), o patrimônio documental de uma organização permite uma releitura da história econômica e social, uma maneira de reencontrar as interrogações que envolvem a compreensão das economias dominantes de consumo e de comercialização, seu nascimento e desenvolvimento.

A autora continua:

> [...] o conhecimento que daí se extrai gera a história dos produtos fabricados para alimentar o comércio interno e externo, a trajetória das manufaturas, dos empresários, das sociedades financeiras. Trata-se da história dos meios de produção em certas épocas, das condições de trabalho, dos recursos, do habitat e das relações.

Bellotto (2004, p. 114) acrescenta que a preservação do patrimônio documental, passada sua fase ativa, traz benefícios para a pesquisa histórica e para a própria organização, pois, segundo a autora:

> [...] o processo decisório só pode ser satisfatoriamente informado e adequadamente instrumentado se puder recorrer à legislação, às resoluções já tomadas, aos casos registrados em processo e em dossiês ou aos dados constantes em atos administrativos semelhantes àqueles de que se está tratando.

Segundo Menezes (1999, p.12), temas como resgate, recuperação e preservação das informações organizacionais estão em voga, não apenas como objeto de estudo de especialistas, mas, como suporte aos processos e identidade das organizações. Para o autor, todos os temas pressupõem uma essência que demanda cuidados especiais para que as informações organizacionais não se deteriorem.

Assim, é preciso enfatizar que a informação é um ativo de valor histórico para as organizações por dois motivos principais: O primeiro refere-se à natureza probatória, isto é, à história e à ação da organização. O segundo refere-se aos aspectos que elucidam fatores econômicos, políticos, sociais e de pesquisa no âmbito da organização.

7.3. Classificação da informação

De maneira geral, classificar a informação envolve atividades de inventário, definição do grau de relevância e identificação dos ativos de informação.

Para Campos (2006, p. 121) a classificação da informação é essencial na definição de quantos e quais recursos devem ser investidos para proteger cada ativo de informação, evitando que altos investimentos sejam feitos para proteger ativos de pouca importância para as organizações e vice-versa.

Sob a ótica da Segurança da Informação, o principal objetivo da classificação da informação é “assegurar que a informação receba um nível adequado de proteção” (ABNT NBR ISO/IEC 17799:2005, p. 23) permitindo determinar com maior precisão os requisitos de tratamento e proteção a ela aplicáveis.

A classificação pode ser balizada de acordo com o valor, requisitos legais, criticidade e grau de sensibilidade atribuído às informações pela organização.

Beal (2005, p. 61) enumera uma série de características que justificam a adoção de diferentes níveis de proteção para os ativos informacionais, ao invés da adoção de um nível único de proteção baseado no mais alto patamar de exigência de segurança. Dentre eles destacamos:

- O custo de proteção dos ativos informacionais – normalmente, a proteção de ativos informacionais envolve altos investimentos. A classificação da informação e dos ativos associados de acordo com seus requisitos de segurança permite uma diferenciação nos recursos utilizados para armazenar a informação e nos controles aplicados para sua proteção, resultando economias e ganhos de produtividade para a organização;

- A utilização de mecanismos de proteção para atender a determinado objetivo de segurança pode afetar negativamente o alcance de outro objetivo – é necessário definir os requisitos de segurança de cada tipo de ativo informacional e a etapa do ciclo de vida da informação para evitar que a utilização de medidas de proteção voltadas para determinado objetivo de segurança prejudique o alcance de outro objetivo;

- Independência da classificação da informação em relação a cada um dos objetivos de segurança – um mesmo ativo de informação pode, ao mesmo tempo, apresentar grandes exigências com relação a um objetivo de segurança e dispensar

exigências com relação a outro objetivo. Os requisitos de segurança precisam ser analisados separadamente para que se possam classificar corretamente os ativos informacionais;

- Periodicidade da classificação da informação – a classificação dos ativos informacionais deve ser revista periodicamente para que as informações possam ser reclassificadas e passem a receber o tratamento mais adequado de acordo com sua exigência.

O modelo de classificação da informação adotado neste trabalho é baseado nas exigências de confidencialidade, integridade e disponibilidade da informação.

O nível de confidencialidade de uma informação é definido pelo valor representativo do diferencial competitivo de mercado ou por exigências legais. Assim, algumas informações devem ter seu sigilo preservado.

O Decreto nº 4.553/2002, artigo 5º, estabelece os ditames de classificação de confidencialidade (sigilo) dos dados e informações públicas, definindo quatro categorias:

- Ultra-secretos: informações cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado;

- Secretos: informações cujo conhecimento não autorizado possa acarretar em dano grave à segurança da sociedade e do Estado;

- Confidenciais: documentos de conhecimento restrito, no interesse do Poder Executivo e das partes, e cujo conhecimento não autorizado possa afetar seus objetivos ou acarretar dano à segurança da sociedade e do Estado;

- Reservados: documentos cuja revelação não autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

Embora a legislação federal não mencione classificações relativas à integridade e disponibilidade das informações, é importante para as organizações, públicas e privadas, estabelecer estes requisitos.

Para Sêmola (2003, p. 44), os requisitos de integridade asseguram a preservação da informação na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais. Quanto aos requisitos de integridade, a informação pode ser classificada em:

- Registrada: informações classificadas como registradas são aquelas importantes para o negócio da organização que, portanto, exigem cuidados especiais quanto ao seu conteúdo, podendo em caso de modificações indesejáveis gerarem repercussões negativas, quer no âmbito interno, causando prejuízos ou resultados distorcidos, quer no âmbito externo, afetando a sua imagem;

- Controlada: informações classificadas como controladas são aquelas reservadas ao âmbito interno da organização e que não exigem os controles rigorosos de auditoria aplicáveis às classificadas como registradas, mas que requerem medidas excepcionais de controle contra modificações não autorizadas;

- Normal: informações classificadas como normais são aquelas que exigem controles quanto a modificação menos rigorosos que os aplicáveis às informações controladas.

Para definir os requisitos de disponibilidade da informação, convém analisar o custo de produção e recuperação da informação bem como as consequências para a organização e seus processos produtivos caso a informação deixe de estar disponível. Para Beal (2005, p. 65), as conclusões das análises dos impactos organizacionais decorrentes da falta ou indisponibilidade de informações e o tempo necessário para o surgimento desse efeito permitem classificar as informações e os sistemas que a processam, definido a exigência de disponibilidade e uma ordem de prioridade para a recuperação em caso de indisponibilidade. Quanto aos requisitos de disponibilidade, a informação pode ser classificada em:

- Vital: informações classificadas como vitais são aquelas essenciais para a sobrevivência da organização cuja perda ou indisponibilidade por determinado período provoca prejuízos irreparáveis para os negócios;

- Crítica: informações classificadas como críticas são aquelas cuja perda ou indisponibilidade por tempo acima do determinado implica em sérios prejuízos para a organização;

- Comum: informações classificadas como comum são aquelas que cuja perda ou indisponibilidade por tempo acima do determinado não implica em sérios prejuízos para a organização, dessa forma, não exigem os controles rigorosos de contingência e recuperação aplicáveis às vitais e críticas.

O subitem 7.2 da Norma Brasileira ABNT NBR ISO/IEC 17799:2005, que discorre sobre classificação da informação e aponta que, em geral, a classificação dada à informação é uma maneira de determinar como esta informação será tratada e protegida.

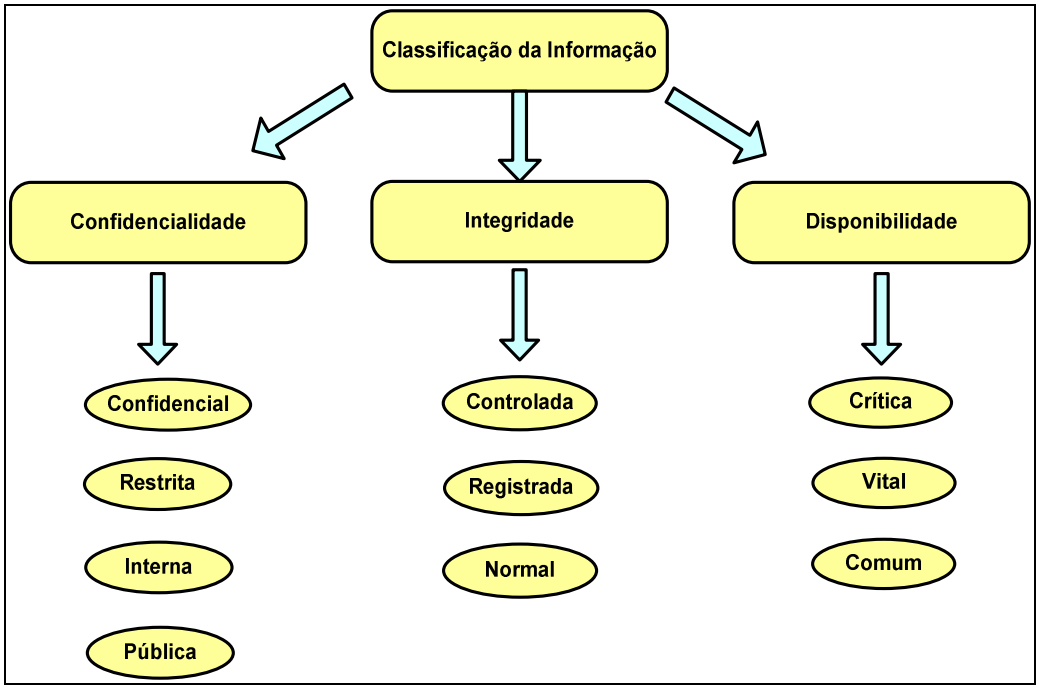


Figura 6 - Classificação da Informação. Fonte: elaboração própria

8. Segurança da informação

8.1. Definição de segurança da informação

> Segurança da informação pode ser entendida como o processo de proteger informações das ameaças para sua integridade, disponibilidade e confidencialidade. (Beal, 2005, p.1)

> Segurança é a proteção de informações, sistemas, recursos, e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança. (Dias, 2001, p.41)

Sêmola (2003, p. 43) define Segurança da Informação como ”uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas, não-repúdio ou sua indisponibilidade“. O autor considera a Segurança a Informação como a prática da gestão de riscos de incidentes que afetem a confidencialidade, integridade e disponibilidade da informação. Dessa forma, definem-se regras que incidem sobre as fases do ciclo de vida da informação (manuseio, armazenamento, transporte e descarte), viabilizando a identificação e o controle de ameaças e vulnerabilidades.

A Associação Brasileira de Normas Técnicas (2005, p.ix) define o termo Segurança da Informação (SI) como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.

Para Zapater e Suzuki (2005, p.6), o conceito de Segurança da Informação vai muito além; pressupõe a identificação das diversas vulnerabilidades e a gestão dos riscos associados aos diversos ativos da informação de uma corporação, independentemente de sua forma ou meio em que são compartilhados ou armazenados, digital ou impresso. Para eles, o objetivo da segurança é garantir a confidencialidade, a integridade e a disponibilidade desses ativos de informação de uma corporação. Alguns autores acrescentam a autenticidade e o não-repúdio a essas garantias.

Ramos (2006, p.19) faz uma distinção entre os conceitos de segurança e Segurança da Informação. Para ele, ”segurança costuma se aplicar a tudo aquilo que possui valor e, conseqüentemente, demanda proteção”. E continua: “[...] na Segurança da Informação lidamos com um tipo específico de ativo que chamamos de ativo de informação, isto é, ativos que geram processam manipulam, transmitem e armazenam informações, além das informações em si“.

Porém, Sêmola (2003, p. 44) alerta que o termo Segurança da Informação apresenta uma ambigüidade, podendo assumir dupla interpretação:

- Segurança como ”meio: é uma prática, de caráter interdisciplinar, composta de metodologias adotadas para tornar um ambiente mais seguro e aplicações que visam estabelecer: controle de segurança dos elementos constituintes de uma rede de comunicação e ou que manipulem a informação (autenticação, autorização e auditoria, por exemplo); e procedimentos para garantir a continuidade de negócios na ocorrência de incidentes.

- Segurança como “fim”: é o resultado da prática adotada e das políticas voltadas para uma padronização operacional e gerencial dos ativos e processos que manipulam a informação. É a característica que a informação adquire ao ser alvo de uma prática segura.

No contexto deste trabalho, o conceito mais adequado para segurança da informação é: a proteção da informação de vários tipos de ameaças para garantir a continuidade, integridade e disponibilidade da informação – adicionalmente, a autenticidade, responsabilidade, não repúdio, legalidade e confiabilidade, podem também estar envolvidas – minimizando o risco ao negócio e maximizando o retorno sobre os investimentos e as oportunidades de negócio. Para tanto, é necessário implementar um conjunto de controles – incluindo políticas processos, procedimentos e estruturas organizacionais – a fim de se obter a segurança da informação. (ABNT NBR ISO/IEC 17799:2005, p. ix)

8.2. Atributos da segurança da informação

8.2.1. Confidencialidade

> Garantia de que o acesso à informação é restrito aos seus usuários legítimos. (Beal, 2005, p.1)

Para Dias (2000, p.42) o conceito de confidencialidade está associado ou conceito de privacidade e implica em proteger as informações contra acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação, isto é, as informações e processos são liberados apenas a pessoas autorizadas, esse objetivo envolve medidas tais como controle de acesso e criptografia.

Para Sêmola (2003, p. 44), confidencialidade é a proteção da informação de acordo como grau de sigilo de seu conteúdo, de forma a limitar seu acesso e uso exclusivamente às pessoas para quem elas são destinadas.

Nos conceitos apresentados, nota-se que o conceito de confidencialidade está relacionado ao sigilo da informação e à legitimidade de seus usuários. O conceito de confidencialidade mais adequado no contexto deste trabalho é: propriedade que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados. (ISO/IEC 13335-1:2004)

8.2.2. Integridade

Para Beal (2005, p.1), integridade é a garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida: em especial, prevenção contra criação, alteração ou destruição não autorizada de dados e informações.

Para Dias (2000, p. 42), o conceito de integridade está relacionado a "evitar que dados – o conceito de dados nesse objetivo é amplo, englobando dados, programas, documentação, registros, fitas magnéticas etc - sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação". Infere-se que o conceito de integridade está, de alguma forma, relacionado ao conceito de confidencialidade pelo fato assegurar que os dados não serão modificados por pessoas não autorizadas. Porém, enquanto finalidade da confidencialidade é focada na leitura dos dados, a integridade preocupa-se com a gravação e alteração dos dados.

A norma ISO/IEC 13335-1:2004 conceitua integridade como a propriedade de salvaguarda da exatidão e completeza de ativos.

8.2.3. Disponibilidade

> Garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna. (Beal, 2005, p.1)

> Proteger os serviços de informática de tal forma que não sejam degradados ou tornados indisponíveis sem a devida autorização. A disponibilidade pode ser definida como a garantia de que os serviços prestados por um sistema são acessíveis, sob demanda, aos usuários ou processos autorizados. Em relação à segurança de informações, sua principal preocupação é prevenir que ataques deliberados ou maliciosos evitem ou dificultem o acesso de usuários autorizados a seus sistemas. (Dias, 2000, p.43)

Para Sêmola (2003, p. 44), disponibilidade é a garantia de que toda informação gerada ou adquirida esteja disponível aos seus usuários autorizados no momento em que os mesmos delas necessitarem para qualquer finalidade.

8.2.4. Autenticidade

> O objetivo da autenticidade da informação é englobado pelo de integridade, quando se assume que este visa a garantir não só que as informações permaneçam completas e precisas, mas também que a informação capturada do ambiente externo tenha sua fidedignidade verificada e que a criada internamente seja produzida apenas por pessoas autorizadas e atribuída unicamente ao seu autor legítimo. (Beal, 2005, p.1)

8.2.5. Não repúdio

Para Fontes (2000, p.22) não repúdio é a garantia de que o usuário não possa negar sua responsabilidade pelo uso ou envio de uma informação.

8.2.6. Legalidade

> Garantia de que a informação foi produzida em conformidade com a lei. (Beal, 2005, p.1)

> O acesso à informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos para o negócio, bem como os princípios éticos que deve ser seguidos pela organização. (Fontes, 2000, p.21)

Sêmola (2003, p. 46) define legalidade como a "característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes".

.

8.3. Segurança da informação e a Ciência da Informação

Para discorrer sobre a relação entre a Ciência da Informação (CI) e a Segurança da Informação (SI) é fundamental definir e conceituar as duas disciplinas:

Para Le Coadic (1996), Ciência da Informação

> [...] é o estudo da informação e suas propriedades gerais: natureza, gênese e efeitos, e seus objetivos são a análise dos processos de construção, sua utilização, como a concepção dos produtos, sistemas que permitem sua organização, comunicação, armazenamento e uso.

Para Borko (1968), Ciência da Informação

> [...] é a disciplina que investiga as propriedades e o comportamento da informação, as forças que regem o fluxo informacional e os meios de processamento para otimização do acesso e uso. Está relacionada com um corpo de conhecimento que abrange a origem, coleta, organização, armazenamento, recuperação, interpretação, transmissão, transformação e utilização da informação.

Como já mencionado, Segurança da Informação é definida pela ABNT NBR ISO/IEC 17799:2005 como

> [...] a proteção da informação de vários tipos de ameaças para garantir a confidencialidade, integridade e disponibilidade da informação – adicionalmente, a autenticidade, responsabilidade, não repúdio, legalidade e confiabilidade, podem também estar envolvidas – minimizando o risco ao negócio e maximizando o retorno sobre os investimentos e as oportunidades de negócio. (ISO 17799:2005, p.ix)

Ramos (2006) preconiza que se costuma aplicar segurança a tudo àquilo que possui valor e, consequentemente, demanda proteção. (Ramos, 2006, p.19)

Analogamente, a informação, como ativo de valor, precisa ser protegida. Nenhum dos aspectos abordados por Borko (1968) e Le Coadic (1996) pode ser privado da segurança sem ficar exposto ao risco. Aliás, a Segurança da Informação busca desenvolver meios para garantir que estes atinjam seus objetivos de forma mais efetiva e eficaz.

Adicionalmente, sendo o objeto de estudo da Segurança da Informação a informação com valor e o da Ciência da Informação a informação em todos os seus aspectos, pode-se inferir que o objeto de estudo da Segurança da Informação está contido no objeto de estudo da Ciência da Informação, conforme representado na figura abaixo:

Figura 7 - Objetos de Estudo da CI e da SI. Fonte: elaboração própria.

A Ciência da Informação estuda o ciclo de vida da informação, este composto pelos momentos vividos pela informação dentro de um sistema – natural, informacional, organizacional etc - em determinado espaço de tempo.

Destacamos quatro grandes momentos vividos pela informação:

a) Manuseio – momento de criação e manipulação da informação. Nesta etapa, é preciso atentar-se para a confidencialidade, integridade e disponibilidade da informação. Sob o aspecto da confidencialidade, a informação produzida ou manipulada pode ser de acesso restrito, tendo em vista o processo de classificação da informação. Da mesma forma, a preocupação com o uso legítimo da informação pode legar a requisitos de confidencialidade, restringindo o acesso e uso de dados e informações às pessoas devidamente autorizadas. No que tange a integridade, existe a preocupação para que a informação tenha sido criada de forma legítima e por alguém autorizado a produzi-la ou ser proveniente de uma fonte confiável, livre de adulterações e precisa de acordo com as necessidades levantadas em cada grupo de usuários. As questões relacionadas à disponibilidade podem prejudicar os processos decisórios e operacionais da organização.

b) Armazenamento – momento em que a informação é armazenada. Nesta etapa, é necessário assegurar a conservação dos dados e informações, permitindo o seu uso dentro da organização. Assim, os objetivos de integridade e disponibilidade dos dados e informações adquirem maior destaque.

c) Transporte – momento em que a informação é transporta, seja em meio físico ou eletrônico;

d) Descarte – momento em que a informação considerada obsoleta ou inútil para a organização é descartada física ou eletronicamente. O descarte das informações precisa ser realizado dentro dos critérios de segurança, considerando, principalmente os princípios da confidencialidade e da disponibilidade. Sob o aspecto da confidencialidade, dados de caráter sigiloso devem ser destruídos. No que tange à disponibilidade, as preocupações incluem a

legalidade da destruição de informações que podem vir a ser exigidas no futuro e a necessidade de preservação de dados históricos valiosos para a organização.

Sêmola (2003) propõe um modelo onde destaca esses momentos em que a informação é tratada por ativos físicos, tecnológicos ou humanos, suportando processos organizacionais. São fases críticas que, não raramente, expõem a informação ao risco. Tal exposição justifica os esforços das empresas para diagnosticar e trabalhar na gestão da segurança no ciclo de vida da informação. A figura a seguir representa essa interrelação:

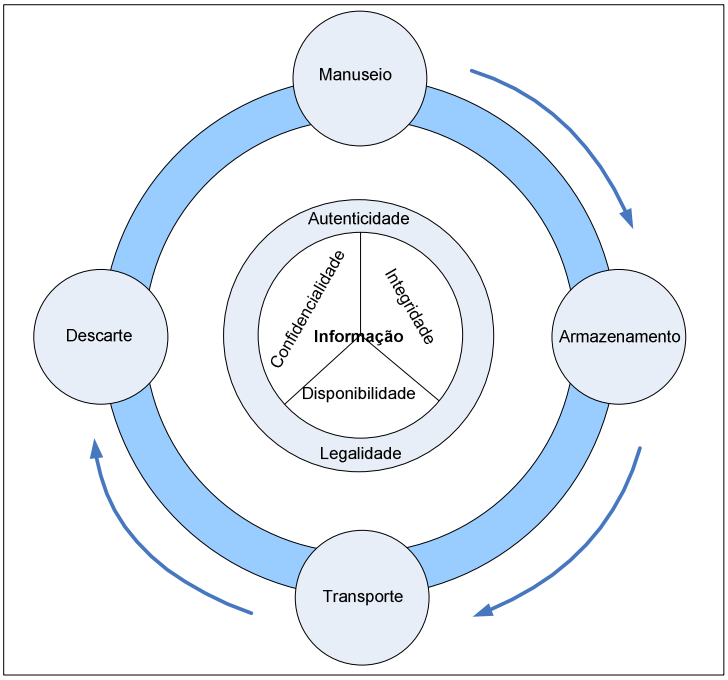


Figura 8 - Ciclo de vida da informação e Segurança da Informação. Fonte: Sêmola (2003, p.11)

8.4. Pilares da segurança da informação

8.4.1. Pessoas

"A corrente é tão forte quanto seu elo mais fraco". O ditado popular pode ser aplicado no âmbito da segurança da informação quando tratamos dos aspectos humanos a ela relacionados.

As pessoas são consideradas o elemento central de um sistema de segurança da informação e, ao mesmo tempo, o seu "elo frágil". Para Beal (2005, p. 71), "a associação pode ser entendida quando se imagina que qualquer esquema de segurança, por mais sofisticado que seja, pode ser derrubado pela atuação de uma

única pessoa que decida abusar de seus privilégios de acesso a dados ou instalações de processamento da informação".

Adicionalmente, é fato que qualquer incidente de segurança da informação envolve pessoas, quer pelo lado das vulnerabilidades exploradas, quer pelo lado das ameaças que exploram essas vulnerabilidades.

Sendo assim, é fundamental que os aspectos humanos e seus possíveis controles – incluindo definição de responsabilidades, procedimentos de seleção e política de pessoal, acordos de confidencialidade, segregação de funções, treinamento e cultura organizacional – tenham sua relevância considerada em um sistema de gestão de segurança da informação.

Outro aspecto de grande importância na relação entre pessoas e segurança da informação é a engenharia social. Engenharia social consiste em uma técnica onde agentes mal-intencionados, valendo-se da ingenuidade, confiança ou ignorância de usuários, obtêm, de forma indevida, informações confidenciais (pessoais e corporativas) que podem comprometer a segurança da organização.

8.4.2. Processos

A idéia de dividir o trabalho em atividades seqüenciais surgiu no início do século XX, quando o engenheiro francês Henry Fayol definiu gerenciamento como uma disciplina e publicou, entre seus 14 princípios gerenciais, a divisão do trabalho em tarefas.

No segundo capítulo do livro, "Gestão por processos: uma abordagem moderna", De Sordi (2005, p. 21), apresenta definições de processos propostas por vários autores, entre eles:

- Davenport (2003 *apud* De Sordi, 2005, p. 21): uma organização de atividades de trabalho, com início e fim e com entradas e saídas claramente definidas;

- Bereta (2002 *apud* De Sordi, 2005, p. 21): é o local onde os recursos e as competências da empresa são ativados a fim de criar uma competência organizacional capaz de preencher suas lacunas a fim de gerar uma vantagem competitiva sustentável;

- Hammer & Champy (1997 *apud* De Sordi, 2005, p. 21): um conjunto de atividade cuja operação conjunta produz um resultado de valor para o cliente;

- Harrington (1991 *apud* De Sordi, 2005, p. 21): um grupo de tarefas interligadas logicamente, que utilizam os recursos da organização para a geração de resultados predefinidos, visando apoiar os objetivos da empresa.

Isso posto, definiremos processos como um conjunto de atividades ou etapas da produção a serem executadas, com emprego de recursos organizacionais, a fim de gerar valores aos seus clientes.

Os processos atuam como meios integradores dos recursos organizacionais – pessoas, papéis e responsabilidades, políticas e regras, estrutura organizacional e TI – e a sua relevância é uma variável importante para a definição do impacto de um incidente de segurança da informação em determinado ambiente.

Segundo Campos (2006, p. 60), além da definição de relevância dos processos, o entendimento do fluxo da informação entre os processos, é outra variável fundamental para a compreensão de que informações precisam ser protegidas. Com a visão do fluxo das informações entre os processos, o entendimento de onde as informações são geradas torna-se mais claro e, consequentemente, a definição de controles para garantir a segurança das informações que são essenciais para os processos torna-se mais fácil.

8.4.3. Tecnologia

No atual ambiente globalizado de negócios, onde disponibilidade e acessibilidade às informações ocupam lugares de destaque, a maioria das organizações utiliza recursos tecnológicos para armazenar suas informações e dados corporativos.

Cria-se uma relação de dependência onde a diferença entre o fracasso e o triunfo organizacional está relacionada às informações fornecidas por sistemas baseados em tecnologia da informação. Dessa forma, o impacto da indisponibilidade desses sistemas pode ser comparado ao impacto da indisponibilidade da própria informação.

A despeito dos grandes investimentos feitos em tecnologia visando mitigar os problemas da disponibilidade e acessibilidade da informação, somente a

tecnologia não é suficiente para resolver estes problemas. Segundo Marciano (2007), a tecnologia da informação é capaz de apresentar parte da solução, não sendo, contudo, capaz de resolvê-los integralmente, e até mesmo contribuindo, em alguns casos, para agravá-los.

8.4.4. A relação entre os pilares da segurança da informação

De acordo com a "Pesquisa Global sobre Segurança da Informação 2006", conduzida pela Ernest & Young, entre abril e junho de 2006, com executivos de aproximadamente 1200 organizações globais e agências governamentais e sem fins lucrativos, em 48 países, nos últimos anos houve significativos investimentos em segurança da informação, incluindo, não somente a tecnologia, mas com ênfase em pessoas e processos.

Inferimos, portanto, que os três fatores – TI, processos e pessoas – interferem na Segurança da Informação e constituem os pilares que dão sustentação a Segurança da Informação, os quais, se não balanceados, podem colocar em risco todo o esforço a ela (segurança da informação) dedicado.

Neto; Martins; Côrte & Silva (2008) descrevem, por meio do diagrama de *Ishikawa*[7], os fatores que interferem na Segurança da Informação conforme apresentado na figura 9, a seguir:

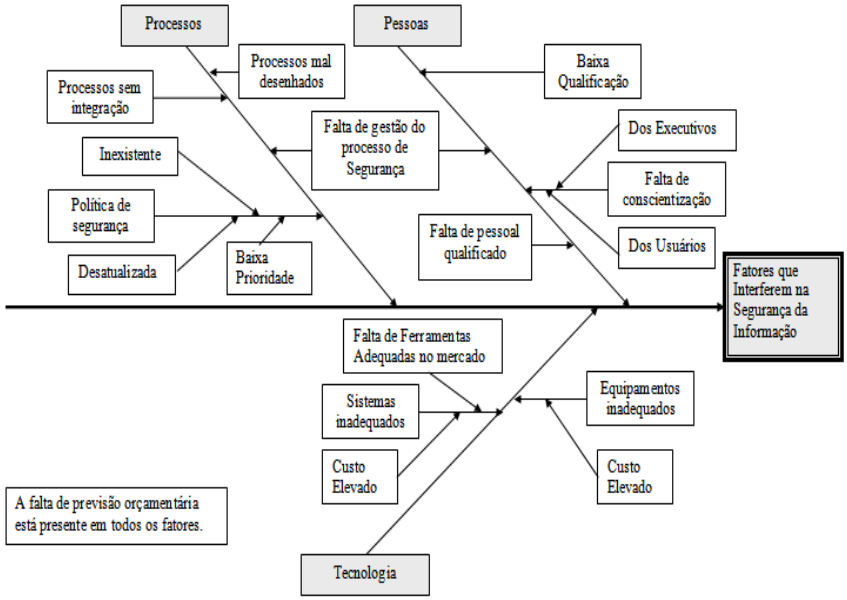


Figura 9 - Diagrama de Ishikawa: fatores que interferem na Segurança da Informação. Fonte: Neto; Martins; Côrte & Silva (2008).

[7] "Trata-se de uma forma de análise que permite esclarecer relação entre "efeitos" dos eventos e suas "causas prováveis". Permite agrupar as causas em várias categorias, o que facilita o processo de seu próprio levantamento". (Mandarini, 2005, p. 41)

Baseados no Axioma 2 de Euclides – onde é definido que "três pontos definem um plano", na geometria Euclideana – os autores representam a segurança da informação apoiada sobre um plano formado por três pilares, quais sejam, a tecnologia, os processos e as pessoas. Por fim, concluem que caso não haja equilíbrio entre estes três pilares o plano ficará inclinado, afetando diretamente a estabilidade da segurança da informação. A figura 10 apresenta graficamente esta idéia.

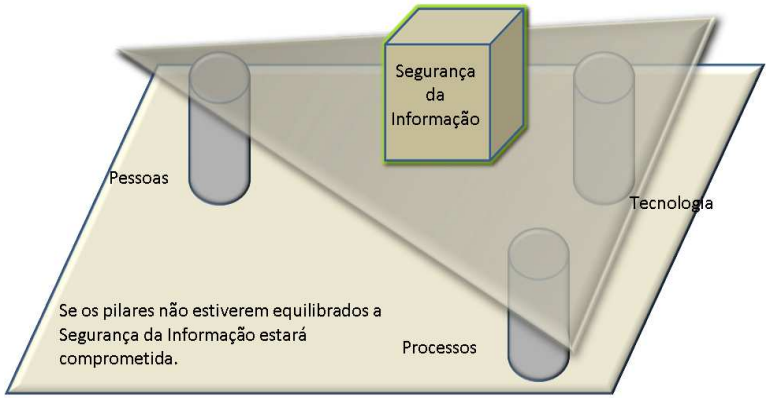


Figura 10 - Os pilares da Segurança da Informação. Fonte: Neto; Martins; Côrte & Silva (2008)

8.5. Arcabouço normativo e padrões de segurança da informação

Normas e padrões técnicos têm por objetivo definir regras, critérios e registrar as melhores práticas para promover a uniformidade e a qualidade de processos organizacionais, produtos e serviços.

As normas e padrões técnicos de Segurança da Informação prezam pela qualidade dos processos e integridade das informações. São mecanismos que orientam o comportamento das pessoas em um ambiente organizacional e, geralmente, determinam uma série de restrições e condutas obrigatórias. Adicionalmente, auxiliam as organizações a implementar as melhores práticas da Segurança e Tecnologia da Informação.

Convém que todo o sistema de Segurança da Informação esteja em conformidade com as orientações de normatização e regulamentação do mercado e em consonância com as leis, internacionais e nacionais.

A seguir, são apresentados o arcabouço normativo e alguns padrões mais conhecidos e utilizados por organizações que possuem um sistema de gestão de Segurança da Informação:

8.5.1. *Information Technology Security Evaluation Criteria* - ITSEC

Publicado pela primeira vez em 1990, é resultado do esforço conjunto dos governos da França, Alemanha, Países Baixos e Reino Unido e compreende um conjunto estruturado de padrões e critérios para avaliar a segurança de produtos e sistemas computacionais (ITSEC, 1991).

Em junho de 1991, após revisão de vários países da comunidade européia, foi publicadada a versão 1.2 do padrão ITSEC. Nos últimos tempos tem sido substituído pelo *Common Criteria*.

8.5.2. Common Criteria for Information Technology Security Evaluation

Em português: Critério Comum para Avaliação de Segurança de Tecnologia da Informação. O *Common Criteria* (CC) é um projeto patrocinado por sete organizações de seis países distintos, são eles:

- Alemanha: *Bundesamt für Sicherheit in der Informationstechnik;*
- Canadá: *Communications Security Establishment*;
- Estados Unidos: *National Institute of Standards and Technology e National Security Agency*;
- França: *Service Central de la Sécurité dês Systèmes d'Information*;
- Holanda: *Netherlands National Communicarions Security Agency*; e
- Reino Unido: *Communications-Electronics Security Group*.

Tendo como público alvo os desenvolvedores, avaliadores e usuários de sistemas e produtos de TI que requerem segurança, seu principal objetivo é ser referência para avaliação de propriedades de segurança de produtos e sistemas de TI, a partir de características do ambiente da aplicação e de um conjunto de critérios fixos que permitem especificar a segurança de uma aplicação de forma não ambígua.

O processo de avaliação estabelece os níveis de confiabilidade que as funções avaliadas atingem conforme os requisitos estabelecidos, ajudando os usuários a determinar se os sistemas e produtos de TI possuem os níveis de segurança desejados e se os riscos inerentes ao seu uso são aceitáveis.

8.5.3. COBIT (Control Objectives for Information and Related Technology)

Desenvolvido pelo *IT Governance Institute* e pela *Information Systems Audit and Control Association* – ISACF, o COBIT é um conjunto de diretrizes para a gestão e auditoria de processos, práticas e controles de TI e oferece um modelo de maturidade para o controle dos processos de TI. Suas práticas são divididas em quatro domínios: planejamento e organização, aquisição e implementação, entrega e suporte e monitoração. (COBIT, 2007)

Apresenta pontos de controles para 34 processos, dentre eles a segurança da informação. Este tem como principal objetivo auxiliar a organização a equilibrar riscos e retorno de investimento (ROI) em TI.

8.5.4. BS 7799 e ISO/IEC 17799

Publicada em 1995 pelo *British Standards Institution* – BSI, a norma BS 7799 é dividida em duas partes e trata da gestão da segurança da informação. A norma britânica BS 7799 tornou-se um padrão em 2000 quando a *International Organization for Standardzation* – ISO a adotou sob o nome de ISO/IEC 17799. No Brasil, é publicada pela Associação Brasileira de Normas Técnicas – ABNT, com a denominação NBR ISO/IEC 17799.

A primeira parte da norma BS 7799-1, oficialmente denominada "*Code of Practice for Information Security Management*", descreve os controles de segurança fundamentais ao ambiente organizacional.

A segunda parte da norma, BS 7799-2, é voltada para a definição de um Sistema de Gestão de Segurança da Informação e preconiza que os Sistemas de Gestão de Segurança da Informação devem se focar na gestão de riscos de forma a garantir a avaliação e o tratamento dos riscos, bem como a melhoria dos processos e a atualização dos sistemas frente as mudanças do ambiente de negócios.

A norma NBR ISO/IEC 17799 é uma adaptação da primeira parte da norma BS7799 e traz um conjunto de boas práticas para a gestão da Segurança da Informação. Adicionalmente, versa sobre conceitos básicos relacionados à Segurança da Informação e destaca sua importância para os negócios. (ABNT, 2005)

8.5.5. ABNT NBR ISO/IEC 27001:2006

Elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Segurança Física em Instalações

de Informática (CE-21:204.01), é uma tradução idêntica da ISO/IEC 27001:2005, que foi elaborada pelo *Join Technical Commitee Information Technology* (ISO/IEC/JTC 1), *subcommitee IT Security Tecchniques* (SC27).

Essa norma provê um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) a partir do modelo "*Plan-Do- Check-Act*" (PDCA). (ABNT, 2006)

Os requisitos previstos na norma são abrangentes e aplicáveis a todas as organizações, independente de tamanho, tipo e natureza.

8.5.6. ABNT NBR ISO/IEC 27005

Publicada em julho de 2008, a norma ABNT NBR ISO/IEC 27005 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados, pela Comissão de Estudo de Tecnologia da Informação (CE-21:027).

É uma adoção idêntica, em conteúdo técnico, estrutura e redação, à norma ISO/IEC 27005:2008, essa elaborada pelo *Technical Committee Information Technology*.

A norma ABNT NBR ISO/IEC 27005 fornece diretrizes para o processo de gestão de riscos em segurança da informação, podendo ser aplicada a todos os tipos de organização que pretendam gerir os riscos que poderiam comprometer a segurança da informação da organização. (ABNT, 2008)

8.5.7. ISO Guide 73 – Risk management – Vocabulary – Guidelines for Use in Standard

Publicada em 2002, a norma ISO Guide 73 – *Risk management – Vocabulary – Guidelines for Use in Standard* apresenta a definição de 29 termos da Gestão de Riscos, agrupados em quatro categorias: termos básicos, relacionados a pessoas ou organizações afetadas por riscos, relacionados a avaliação de riscos, relacionados a tratamento e controle de riscos.

Sua principal aplicação é equalizar o entendimento de conceitos relacionados a Segurança da Informação e Gestão de Riscos.

8.5.8. ISO 13335 – Guidelines for the Management of IT Security

Consiste em um conjunto de diretrizes de gestão de segurança aplicadas a tecnologia da informação. A norma tem por objetivos servir de base para o desenvolvimento e aprimoramento de estruturas de segurança de TI e estabelecer uma referência de gestão de segurança para as organizações.

A norma ISO 13335 trata conceitos e modelos para a segurança de TI; administração e planejamento de segurança de TI; técnicas para a gestão da segurança de TI; escolha e definição de medidas de proteção; e, da orientação gerencial em segurança de redes de computadores. (ISO/IEC 13335-1:2004, 2004)

8.6. Arcabouço legal de Segurança da Informação

A legislação brasileira, com relação à Segurança da Informação, é incipiente se comparada a legislações de países europeus ou dos Estados Unidos. Porém existem alguns dispositivos legais sobre assuntos relativos à tecnologia da informação, direitos autorais, sigilo de informações e Segurança da Informação, inclusive no âmbito da Administração Pública, dentre eles:

- **Constituição Federal**, Artigo 5º, inciso X: Sigilo das informações relacionadas à intimidade ou vida privada de alguém;

- **Constituição Federal**, Artigo 5º, inciso XXXIII e Artigo 37º, § 3º, inciso II: Disponibilidade das informações constantes nos órgãos públicos, exceto das sigilosas.

- **Constituição Federal**, Artigo 216, § 2º: Obrigação da Administração Pública de promover a gestão documental.

- **Constituição Federa**l, Artigo 37º, caput: Vinculação da Administração Pública aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

- **Lei n. 7.170**, de 14 de dezembro de 1983: define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo de julgamento. Artigo 13º: Sigilo de dados sigilosos relacionados à segurança nacional.

- **Lei n. 7.232**, de 29 de outubro de 1984: dispõe sobre a Política Nacional de Informática. Artigo 2º, inciso VIII: Sigilo dos dados relacionados à intimidade, vida privada e honra, especialmente dos dados armazenados através de recursos informáticos.

- **Consolidação das Leis do Trabalho – CLT**, Artigo 482º, alínea g: Proteção das informações sigilosas acessadas no exercício de emprego público.

- **Decreto nº 1.171**, de 22 de junho de 1994: aprova o Código de Ética do Servidor Público Civil do Poder Executivo Federal. Alíneas "h" e "I" do inciso XV da Seção II: Proteção da integridade e disponibilidade das informações públicas.

- **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. Artigo 5º, incisos I e V: Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.

- **Código Penal**, Artigo 153º: Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.

- **Código Penal**, Artigo 154º: Proteção do sigilo das informações conhecidas em razão de função, ministério, ofício ou profissão.

- **Código Penal**, Artigo 297º: Proteção da integridade e autenticidade dos documentos públicos.

- **Código Penal**, Artigo 305º: Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.

- **Código Penal**, Artigos. 313º A e 313º-B: Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.

- **Código Penal**, Artigo 314º: Proteção da disponibilidade das informações constantes nos órgãos e entidades públicos.

- **Código Penal**, Artigo 325º: Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

- **Código Processo Penal**, Artigo 20º: Sigilo do inquérito policial.

- **Código Processo Penal**, Artigo 745º: Sigilo do processo de reabilitação do condenado.

- **Código Tributário Nacional**, Artigo 198º: Proteção do sigilo fiscal.

- **Código Processo Civil**, Artigo 347º, inciso II c/c Artigo 363º, inciso IV: Direito da parte de guardar sigilo profissional.

- **Código Processo Civil**, Artigo 406º, inciso II c/c Artigo 414º, § 2º: Direito da testemunha de guardar sigilo profissional.

- **Lei nº 6.538**, de 22 de junho de 1978, Artigo 41º: Sigilo de correspondência.

- **Lei nº 7.492**, de 16 de junho de 1986: define os crimes contra o sistema financeiro nacional, Artigo 18º: Proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.

- **Lei nº 8.112**, de 11 de dezembro de 1990: dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Artigo 116º, inciso

VIII e Artigo 132º: Sigilo das informações produzidas ou conhecidas no exercício de cargo ou função pública.

- **Lei no 8.159**, de 8 de janeiro de 1991: trata da política nacional de arquivos públicos e privados. Foi retificada no Diário Oficial da União de 28/01/1991;

- **Lei nº 9.296**, de 24 de julho de 1996: regulamenta o inciso XII, parte final, do artigo 5º da Constituição Federal. Artigo 10º: Sigilo dos dados e das comunicações privadas. O disposto nessa lei aplica-se a interceptação do fluxo de comunicações em sistemas de informática e telemática;

- **Lei nº 9.507**, de 12 de novembro de 1997: regula o direito de acesso a informações e disciplina o rito processual do *habeas data*.

- **Lei nº 8.159**, de 08 de janeiro de 1991: dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.

- **Lei Complementar 105**, de 10 de janeiro de 2001: dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

- **Lei nº 11.111**, de 05 de maio de 2005: regula o direito à informação e ao acesso aos registros públicos.

- **Decreto no 2.134**, de 8 de janeiro de 1991: regulamenta o Artigo 23º da Lei nº 8.159, que dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles;

- **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.

- **Decreto nº 4.553**, 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.

- **Decreto nº 5.301**, de 09 de dezembro de 2004: institui a Comissão de Averiguação e Análise de Informações Sigilosas, dispõe sobre suas atribuições e regula seu funcionamento.

- **Decreto nº 5.584**, de 18 de novembro de 2005: dispõe sobre o recolhimento ao Arquivo Nacional dos documentos arquivísticos públicos produzidos e recebidos pelos extintos Conselho de Segurança Nacional - CSN, Comissão Geral de Investigações - CGI e Serviço Nacional de Informações - SNI, que estejam sob a custódia da Agência Brasileira de Inteligência - ABIN.

- **Decreto no 79.099**, de 06 de janeiro de 1977: aprova o regulamento para a salvaguarda de assuntos sigilosos;

- **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.

- **Resolução nº 7**, de 29 de julho de 2002: estabelece regras e diretrizes para os sítios na Internet da Administração Pública Federal.

9. Gestão de Riscos

9.1. Definição de Gestão de Riscos

Segundo Salles (2006, p. 19), o termo “risco” tem origem no italiano antigo *risicare*, que quer dizer ousar (Bernstein, 1997), e no sentido de incerteza, é derivada do latim *risicu* e *riscu*. Nesse contexto, o termo risco deve ser interpretado

como um conjunto de incertezas encontradas quando ousamos fazer algo, e não apenas como problema.

No contexto deste trabalho, a definição mais adequada de risco é a proposta por Oliveira (2001, p. 55): “risco é a probabilidade de uma ameaça explorar vulnerabilidades para causar perdas ou danos a um ativo ou grupo de ativos da organização”. Desta forma, riscos são determinados pela combinação das ameaças, vulnerabilidades e valores dos ativos, valores estes mensurados com base no impacto destes ativos aos negócios da organização, onde impacto se traduz como os resultados de um incidente inesperado.

Nos dias de hoje, os meios de comunicação tem registrado diariamente várias questões que trazem preocupação para a humanidade: devastação do meio ambiente, instabilidade financeira, violência, drogas, desastres naturais decorrentes de mudanças climáticas.

Os acontecimentos sócio-econômicos corroboram para caracterizar que vivemos em um mundo repleto de incertezas sociais, políticas e econômicas e com novas categorias de riscos que não podem ser desconsideradas no contexto das organizações.

O conceito de gestão de risco tem sido adotado de formas dispersas por diferentes grupos e para questões bastante distintas.

Cicco (1990, p.25) apresenta várias definições de gestão de riscos sob o prisma de várias áreas:

- Para organizações ligadas à área de seguro, gestão de riscos é a ciência que se ocupa dos chamados riscos seguráveis e da redução dos custos de seguro;
- Para profissionais da área financeira, a gestão de riscos consiste no uso de técnicas de proteção de ativos financeiros e no manejo adequado de taxas de juros;
- Para muitos políticos e analistas sociais, representa o controle de situações que podem afetar o meio ambiente e são decorrentes do avanço tecnológico crescente e desordenado;
- Para administradores hospitalares, pode significar o mesmo que garantia da qualidade dos serviços prestados aos pacientes.

Na verdade, a existência de todas estas abordagens é resultado das crescentes incertezas[8] que cercam o mundo que vivemos e suas limitações advêm do fato de focalizarem somente uma parte de todo o espectro de riscos a que as organizações estão expostas.

A gestão de riscos é um elemento central que faz parte do planejamento estratégico da organização e deve ser praticado por todos os níveis da administração.

O *Committee of Sponsoring Organizations of the Treadway Commission – COSO* (2004, p.4) define gestão de riscos como um processo aplicado no estabelecimento de estratégias formuladas para identificar na organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com a tolerância da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

A *Federation of European Risk Management Associations - FERMA* (2003, p.3) define gestão de riscos como o processo por meio do qual as organizações analisam metodicamente os riscos inerentes às suas respectivas atividades, com o objetivo de atingirem uma vantagem sustentada em cada atividade individual e no conjunto de todas as atividades.

O COSO (2004, p. 3) admite duas premissas inerentes a gestão de riscos corporativos. A primeira é que as organizações existem para gerar valor às partes interessadas. A segunda é que todas as organizações enfrentam incertezas. Diante disso, o grande desafio de seus administradores é determinar até que ponto tolerar essas incertezas, assim como estabelecer como essas incertezas podem interferir nos processos de geração de valores às partes interessadas.

A gestão de riscos corporativos permite que os administradores tratem como maior eficácia as incertezas bem como os riscos e oportunidades a elas associados, a fim de melhorar a capacidade de gerar valor.

Ainda de acordo com aquele comitê, o planejamento estratégico e a definição de objetivos para alcançar o equilíbrio entre as metas de crescimento, o retorno de investimentos e os riscos a eles associados permitem que as organizações maximizem a geração de valor e melhorem a exploração de seus recursos na buscas de seus objetivos.

O *framework* proposto pelo *Committee of Sponsoring Organizations of the Treadway Commission* – COSO (2004, p. 3) enumera algumas finalidades da gestão de riscos, dentre elas:

[8] Incertezas representam riscos e oportunidades, com potencial para destruir ou agregar valor aos negócios. (COSO, 2004, p. 3)

- Alinhar a tolerância ao risco com o planejamento estratégico corporativo;
- Subsidiar as decisões em respostas aos riscos corporativos;
- Reduzir as surpresas e prejuízos operacionais decorrentes de eventos potenciais;
- Identificar e administrar riscos múltiplos e entre empreendimentos possibilitando respostas eficazes a impactos inter-relacionados;
- Identificar e aproveitar as oportunidades de forma proativa;
- Conduzir uma avaliação eficaz das necessidades de capital e aprimorar a alocação desse capital.

Neste estudo vamos nos ater à aplicação da gestão de riscos na segurança da informação. Nesta abordagem, definiremos gestão de riscos como: “conjunto de processos que permite às organizações identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos“. (Beal, 2005, p. 11)

Devemos ter como premissa básica que não existe sistema seguro em todos os aspectos. Existem diferenças de complexidade, emprego de recursos e custos financeiros para manter os ativos de informação a salvo de ameaças à sua confidencialidade, integridade e disponibilidade. Partindo dessa premissa, o enfoque de gestão baseado nos riscos específicos para o negócio assume um papel de suma importância, pois conhecendo as ameaças e as vulnerabilidades a que estão sujeitas as informações, bem como os impactos decorrentes do comprometimento de sua segurança, a tomada de decisão sobre como empregar recursos para proteger os dados corporativos torna-se melhor fundamentada e mais confiável.

9.2. Termos relacionados à gestão de riscos

A seguir serão apresentadas as definições adotadas nesta pesquisa para vários termos relacionados à gestão de riscos. Diante da existência de vários diferentes cenários organizacionais de aplicação da gestão de riscos, é importante promover ajustes na terminologia adotada para adequação ao escopo em que está sendo estudada a gestão de riscos.

Aceitação do risco: decisão de aceitar um risco. (ABNT ISO/IEC Guia 73:2005)

Agente: fonte produtora de um evento que pode ter efeitos adversos sobre um ativo e informação. (Beal, 2005, p.14)

Alvo: ativo de informação que pode ser objeto de um ataque/incidente. (Beal, 2005, p.14)

Análise do risco: uso sistemático de informação para identificar fontes e estimar o risco. A análise de risco oferece ma base para a avaliação, o tratamento e a aceitação do risco. (Beal, 2005, p. 12)

Ataque: evento decorrente da exploração de uma vulnerabilidade por uma ameaça. (Beal, 2005, p.14)

Atenuação: limitação de quaisquer conseqüências negativas de um evento em particular. (Beal, 2005, p. 13)

Avaliação do risco: processo de comparação do risco estimado com o critério de risco determinado para determinar sua relevância. (Beal, 2005, p. 12)

Controle do risco: ações para implementação das decisões de gestão do risco. O controle do risco pode envolver monitoração, reavaliação e conformidade com decisões. (Beal, 2005, p. 13).

Comunicação do risco: traça o compartilhamento da informação sobre o risco feita entre o tomador de decisão e outros *stakeholders*. (Beal, 2005, p. 12)

Conseqüência: resultado de um evento. [ABNT ISO/IEC Guia 73:2005]

Critérios de risco: termos de referência pelos quais a relevância do risco é avaliada. [ABNT ISO/IEC Guia 73:2005]

Estimativa do risco: processo usado para atribuir valores à probabilidade e as conseqüências de um risco. A estimativa do risco pode considerar

custo, benefícios, preocupações de *stakeholders* e outras variáveis apropriadas para a avaliação do risco. (Beal, 2005, p. 12)

Estudo do risco: processo global de análise e avaliação do risco. (Beal, 2005, p. 13)

Evasão do risco: decisão de não envolver, ou ação de fuga de uma situação de risco. (Beal, 2005 p. 13)

Evento: evento é a ocorrência de um conjunto particular de circunstâncias, que caracterizam uma ocorrência ou série delas. (ABNT ISO/IEC Guia 73:2005)

Para o COSO (2004, p. 16), evento é um incidente ou ocorrência gerada a partir de fontes inter ou extra-organizacionais que pode causar impactos negativos e/ou positivos na realização dos objetivos organizacionais.

Fonte: item ou atividade associada a uma consequência potencial

Gestão do risco: atividades coordenadas para diferenciar e controlar uma organização no que se refere a riscos. (ABNT ISO/IEC Guia 73:2005)

Identificação do risco: processo de localizar, listar e caracterizar elementos do risco. Os elementos podem incluir fonte, evento, consequência e probabilidade.

Otimização do risco: processo relacionado a um risco para minimizar as consequências negativas e maximizar as consequências positivas e suas respectivas probabilidades. (Beal, 2005, p. 13)

Parte interessada: pessoa ou grupo que possui interesse no desempenho ou sucesso de uma organização. (Beal, 2005, p. 12)

Percepção do risco: maneira pela qual um *stakeholder* vê um risco, com base em um conjunto de valores ou preocupações. (Beal, 2005, p. 12)

Probabilidade: número real na escala de 0 a 1 associado a um evento aleatório, que pode estar relacionado a uma frequência de ocorrência relativa de longo prazo ou a um grau de confiança de que um evento irar ocorrer. (Beal, 2005, p. 12)

Redução do risco: ações tomadas para reduzir a probabilidade, as consequências negativas ou ambas, associadas a um risco (Beal, 2005, p. 13)

Risco: combinação da probabilidade de um evento e de suas consequências. (ABNT ISO/IEC Guia 73:2005)

Risco residual: risco remanescente após o tratamento de riscos. (ABNT ISO/IEC Guia 73:2005)

Stakeholder: qualquer indivíduo, grupo ou organização que pode influir, sofrer influência ou perceber-se como sendo afetado por um risco. (Beal, 2005, p. 12)

Tratamento do risco: processo de seleção e implementação de medidas para modificar um risco. (ABNT ISO/IEC Guia 73:2005)

9.3. Componentes do risco

9.3.1. Ameaça

De acordo com a norma ISO/IEC 13335-1:2004, ameaça é a "causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização".

Beal (2005, p.14) define ameaça como expectativa de acontecimento acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação.

No contexto deste estudo, ameaças são agentes ou condições que causam incidentes que comprometam as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e consequentemente, causando impactos aos negócios de uma organização.

Considerando a intencionalidade, as ameaças podem ser divididas nos seguintes grupos:

Naturais – ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, maremotos, aquecimento, poluição etc.

Involuntárias – ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia etc.

Voluntárias – ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões etc.

9.3.2. Vulnerabilidade

De acordo com a norma ABNT NBR ISO/IEC 17799:2005, vulnerabilidade é a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Para esta pesquisa, o conceito mais adequado para vulnerabilidade é: fragilidade presente ou associada a ativos que manipulam e/ou processam informações que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

Segundo Sêmola (2003, p.48), as vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou condição favorável, que são as ameaças.

9.3.3. Impacto

Sêmola (2003, p. 50) define impacto como a “abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio”.

Beal (2005, p. 14) faz uma correspondência da definição do termo impacto com a definição do termo conseqüência proposta pela ABNT na norma ISO/IEC Guia 73:2005. Dessa forma, na definição da autora, impacto é o efeito ou conseqüência de um ataque ou incidente para a organização.

9.3.4. Incidente

Fato ou evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação. (Sêmola, 2003, p.50)

10. Métodos de Análise de Riscos Organizacionais

Realizar a análise de riscos em uma organização implica em aplicar metodologias, técnicas e artifícios a fim de descrever, analisar e interpretar dados estatísticos e o histórico de incidentes.

O resultado dessa análise é a construção de parâmetros e a utilização de dispositivos que permitam prospectar, inferir, organizar e formalizar julgamentos probabilísticos acerca da segurança institucional.

A análise de risco permite ainda quantificar a relação entre o investimento nos recursos de segurança que podem ser empregados para minimizar os riscos institucionais e os benefícios obtidos contra eventos com potencial para causar danos.

A seguir, serão apresentados os principais métodos empregados na análise de riscos organizacionais:

10.1. Método de Mosler

O método de Mosler é um artifício útil e bastante utilizado em organizações que carecem de banco de dados suficiente sobre a problemática que se pretende abordar.

Deve ser empregado para cada risco individualmente, projetando seu impacto sobre determinada atividade. Depende puramente de opiniões dos analistas para a valoração das funções utilizadas como parâmetros de interferência na atividade institucional, o que lhe dá um caráter subjetivo.

O método de Mosler é composto por quatro fases distintas e interdependentes, a saber:

- 1ª Fase – Definição do risco ou ameaça: nesta fase o objetivo é levantar e identificar o risco ou ameaça a se analisado, integrando com determinada atividade da empresa;

- 2ª Fase – Análise do risco ou ameaça: nesta fase a análise do risco ou ameaça é realizada com base em seis critérios, voltados para avaliar a influência do evento em determinada atividade da empresa. Cada um dos critérios pode ser pontuado, em uma escala de 1 a 5 – sendo 5 o maior grau, conforme sua gravidade. Os critérios considerados são:

  – Critério da Função – F: refere-se ao nível de gravidade das conseqüências negativas ou dos danos sobre a atividade da organização, podendo variar entre muito grave, grave, mediano, leve e muito leve;

- Critério da Substituição – S: avalia o impacto da concretização do risco ou ameaça sobre os bens, podendo variar entre muito difícil, difícil, sem muita dificuldade, fácil e muito fácil;
- Critério da Profundidade – P: projeta o grau de perturbação e os efeitos psicológicos que o evento poderá causar à imagem da empresa, podendo variar entre perturbações muito graves, graves, limitadas, leves e muito leves;
- Critério da Extensão – E: mede o alcance e a extensão dos danos que o evento pode causar à empresa, podendo variar entre extensão internacional, nacional, regional, local e individual;
- Critério da Agressão – A: avalia a possibilidade de o evento acontecer, considerando características conjunturais e físicas da organização. A escala pode variar entre muito alta, alta, normal, baixa e muito baixa;
- Critério de Vulnerabilidade – mede a intensidade das perdas financeiras possíveis caso o evento venha a se concretizar. A escala pode variar entre muito alta, alta, normal, baixa e muito baixa.

- 3ª Fase – Evolução do Risco (ER): nesta fase, o objetivo é quantificar o grau do risco analisado. Primeiramente, calcula-se a "magnitude do risco" (C) e, em seguida, quantifica-se a "probabilidade de ocorrência"(PB), projetando-se a potencialidade do evento. A fórmula para cálculo da evolução do risco é:

$$ER = C \times Pb$$

A magnitude do risco (C) é calculada pela fórmula C = I + D, onde I representa a importância do sucesso e D, os danos causados.

A importância do sucesso é o resultado do produto entre os critérios de Função e de Substituição (I = F x S), e o dano

causado é o resultado do produto entre os critérios de Profundidade e Extensão (D = P x E).

A probabilidade de ocorrência do risco é calculada pela multiplicação dos critérios de Agressão e de Vulnerabilidade, assim:

$$Pb = A \times V$$

- 4ª fase – Comparação e classificação: nessa fase o resultado obtido para a evolução do Risco nas etapas anteriores é comparado com a tabela abaixo, para verificar a classe de risco:

Valor "ER" Quantificado	Classe de Risco
02 – 250	Muito baixo ou baixíssimo
251 – 500	Pequeno ou baixo
501 – 750	Normal
751 – 1.000	Grande
1.001 – 1250	Elevado

A priorização de procedimento para prevenção ou mitigação dos riscos organizacionais pode ocorrer de acordo com a classe de risco.

10.2. Método de T. Fine

Promove a integração entre o grau de riscos e as limitações orçamentárias das organizações, estabelecendo prioridades de atuação, o esforço e os investimentos a serem empregados, a partir da criticidade de cada risco ou ameaça.

Assim como o método de Mosler, o método T. Fine utiliza grades de probabilidade e é baseado no cálculo do perigo de cada situação, estabelecendo seu Grau de Criticidade (GC).

O Grau de Criticidade determina a urgência das medidas necessárias, e estabelece parâmetros para justificar os investimentos. É calculado com base em três fatores:

- Conseqüência – C: corresponde aos impactos financeiros e pessoais mais passíveis de ocorrerem caso o evento venha a se concretizar;

- Exposição ao risco – E: é a freqüência de ocorrência de determinado evento em uma organização ou em organizações similares;

- Probabilidade – P: é a chance real de o evento vir a acontecer, num determinado Período de tempo.

Para que possam ser mensurados e projetados, os três fatores possuem uma escala de valores numéricos, baseada na experiência de T. Fine.

O Grau de Criticidade é o resultado do produto entre os três fatores – Conseqüência, Exposição do Risco e Probabilidade – que constitui uma escala de valores compreendida entre 0,05 e 10 mil. Tais valores resultam de uma classificação intermediária dos fatores de risco, que decresce de forma linear, assegurando uma correção no incremento do GC. Estatísticas e referencias históricas são utilizadas no processo de fixação desses valores.

A tabela a seguir apresenta os valores fixados:

Fator	Classificação	Valor
Conseqüência C	a) Dano superior a US$ 1 milhão – quebra da atividade – fim da empresa – Insuportável.	100
	b) Dano entre US$ 500 mil e US$ 1 milhão – Gravíssima.	50
	c) Dano entre US$ 100 e US$ 500 mil – Grave	25
	d) Dano entre US$ 1 mil e US$ 100 mil – Baixa	15
	e) Dano abaixo de US$ 1 mil – Muito Baixa	5
	f) Pequenos danos – Baixíssima	1
Exposição E	a) Várias vezes ao dia – Frequentemente	10
	b) Uma vez ao dia – Sistematicamente	5
	c) Uma vez por semana / mês – Ocasionalmente	3
	d) Uma vez por mês / ano – Irregularmente	2
	e) Ocorre, mas não se sabe com que freqüência – Raramente	1

	f) Não se sabe se já ocorreu	0,5
Probabilidade P	Espera-se que ocorra – Provavelmente	10
	Completamente Possível – 50% de chance de ocorrer – Possivelmente	6
	Coincidência, se ocorrer – Coincidentemente	3
	Coincidência remota – sabe-se que já ocorreu – Remotamente	
	Extremamente remota – porém possível ocorrer – Muito Remotamente	0,5
	Praticamente impossível ocorrer – Dificilmente	0,1

A escala de valores para a priorização dos riscos é:

Grau de Criticidade	Prioridades – Ações a tomar
GC maior ou igual a 200	Correção imediata – o risco deve ser diminuído.
GC menor que 200 e maior ou igual a 85	Correção urgente – risco requer atenção.
GC menor que 85	O risco deve ser eliminado mais cedo ou mais trade.

O cálculo da justificativa de investimento é dado pela razão entre o Grau de Criticidade e o produto entre o Fator de Custo e o Grau de Correção.

$$JI = \frac{GC}{\text{Fator de Custo x Grau de Correção}}$$

As tabelas a seguir apresentam as escalas de valores para o Fator de Custo e para o Grau de Correção:

Tabela de Fator de Custo

Classificação	Valor
Maior que US$ 50 mil	10
Entre US$ 25 mil e US$ 50 mil	6
Entre US$ 10 mil e US$ 25 mil	4

Entre US$ 1.000 e US$ 10 mil	3
Entre US$ 100 e US$ 1.000	2
Entre US$ 25 e US$ 100	1

Tabela de Grau de Correção

Classificação	Valor
Risco eliminado – 100%	1
Risco reduzido – 75%	2
Risco reduzido – entre 50 e 75%	3
Risco reduzido – entre 25 e 50%	4
Risco reduzido – menor que 25%	6

Para determinar se o investimento proposto é justificável, deve-se aplicar os valores das classificações correspondentes e obter um valor numérico, denominado índice de justificação do rendimento do investimento proposto.

Para que o investimento seja considerado justificável, o índice de justificação deverá ser superior a 10. Quanto maior o índice de justificação, maior será o interesse para com o programa de prevenção.

R. Pickers, estudioso de riscos, propôs uma variação na escala de valoração do índice de justificação do método de T. Fine, conforme apresentado na tabela a seguir. Essa escala foi estabelecida como padrão, em 1976, pela Associação Americana de Gerenciamento de Riscos.

Fator índice de Justificação – IJ	Comentários
IJ menor que 10	Investimento duvidoso
IJ entre 10 e 20	Investimento normalmente justificado
IJ maior que 20	Investimento plenamente justificado; grande redução de risco.

10.3. Diagrama de Causa e Efeito (Diagrama de Ishikawa)

Desenvolvido pelo professor *Kaoru Ishikawa* – presidente do *Musashi Institute of Technology* – em 1943, trata-se de um método de análise que permite estabelecer relação entre efeitos dos eventos e todas as possibilidades de suas

causas prováveis. Permite agrupar as causas em diversas categorias, o que pode facilitar o processo e seu próprio levantamento.

O efeito ou problema é colocado na direita de um gráfico e as causas para esse problema são colocadas à esquerda. Para efeito ou problema existem inúmeras categorias de causas, sendo que as principais podem ser agrupadas nas seguintes categorias: material, mão de obra, método, máquinas, meio ambiente e medição.

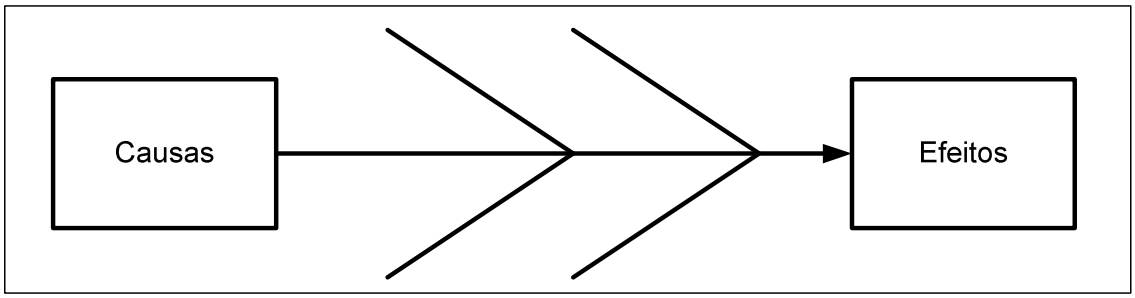


Figura 11 - Diagrama de Causas e Efeitos. Fonte: elaboração própria.

Para construir o Diagrama de Causa e Efeito é necessário executar as seguintes etapas:

- 1ª Etapa: definir claramente o problema selecionado identificando em que consiste, onde ocorre, quando ocorre e qual a sua extensão;

- 2ª Etapa: detectar as possíveis causas para o problema definido. Nessa etapa, pode-se empregar os métodos de *brainstorming*, *brainswriting* etc;

- 3ª Etapa: construir o diagrama de causa e efeito para a problemática, estabelecendo as categorias de causas aplicáveis, aplicando o resultado do método utilizado para a geração das categorias de causas prováveis e questionado a razão de sua ocorrência.

- 4ª Etapa: consiste em interpretar os resultados alcançados buscando estabelecer relação entre cada efeito e as causas que podem levar a sua ocorrência.

A partir de um diagrama de causa e efeito bem definido, as causas mais prováveis são identificadas e selecionadas para uma análise mais detalhada. Convém investigar em profundidade a causar e o que contribui para sua ocorr6encia, a fim de eliminá-la.

10.4. Diagrama de Árvore

Trata-se de um desdobramento gráfico dos caminhos que conduzem às causas fundamentais de um determinado evento a partir do qual pergunta-se o por quê de seu acontecimento, para cada causa aventada.

A partir de sua aplicação, pode-se identificar as causas mais relevantes, bem como as soluções para estas e definir a priorização conforme critérios estabelecidos.

A técnica é aplicada em três tempos: primeiramente, é necessário identificar todas as causas relevantes possíveis. Em seguida, vislumbra-se soluções para as diversas causas. Por fim, deve-se priorizar as soluções vislumbradas.

10.5. Técnica de *Brainstorming*

Consiste em uma reunião cujos participantes tenham conhecimento sobre determinado evento, para geração espontânea e ilimitada de ideias, o que justifica o método também ser conhecido como “tempestade de idéias”.

Obedece a uma rotina que não admite criticas ou avaliações durante o processo, pois este está voltado para a quantidade e não para a qualidade das idéias geradas.

A técnica de *brainstorming* emprega como tema para a discussão o objetivo que se deseja alcançar.

10.6. *Brainstorming* inverso (ou invertido)

O método de *Brainstorming* inverso é indicado para problemas em que há dificuldade para definir ou propor a solução a partir do emprego de outros métodos.

Deve ser utilizado quando a aplicação de outros métodos não for eficiente.

Fundamenta-se no fato de que, por vezes, é mais fácil definir aquilo que não se quer. Dessa forma, a inversão ocorre na discussão do objetivo que não se

deseja alcançar. O processo funciona da mesma forma como o do método de *Brainstorming*.

10.7. *Brainswriting*

Geralmente, o método de *Brainswriting* é empregado para solucionar problemas complexos e que exigem a participação de uma equipe multidisciplinar ou cuja formação inclua componentes com diferentes níveis intelectuais, hierárquicos, técnicos etc.

Previne a inibição e o desconforto de se manifestar por parte dos componentes dos níveis mais baixos, evitando que o processo de geração de idéias seja prejudicado.

O tema empregado para a discussão é o objetivo que se deseja alcançar.

10.8. *Brainswriting* inverso (ou invertido)

O método de *Brainswriting* inverso é empregado nos mesmos casos e de forma análoga ao método *Brainswriting*, porém, apresenta a inversão do objeto da discussão, empregando-se aquele que não se deseja alcançar.

10.9. Mapa mental

O processo de mapa mental consiste em resumir o tema ou problema a uma única palavra, proposta para a discussão por um pequeno grupo de debate. Dessa forma, pretende-se levantar de forma aleatória, outras idéias que se correlacionem com a idéia central.

Geralmente é utilizado quando de dispõe de pouco tempo para elaborar idéias de forma organizada, para uma possível apresentação em curto prazo.

10.10. Diagrama de Pareto

O Diagrama de Pareto representa graficamente, a partir de dois eixos cartesianos e de um histórico dos incidentes mais comuns, os problemas que ocorrem em um determinado sistema.

Um dos eixos cartesianos representa os eventos o outro a incidências desses eventos.

O Diagrama de Pareto permite vislumbrar o comportamento dos eventos no sistema considerado e previne atribuição de prioridades inadequadas ao revelar os eventos mais críticos.

10.11. Matriz de Prioridades

O método de Matriz de Prioridades consiste numa tabela bidimensional que permite avaliar opções em relação a critérios previamente definidos. Deste cruzamento, resulta uma avaliação a ser considerada.

São exemplos de matrizes empregadas na segurança empresarial para avaliar a prioridade de problemas: a Matriz GUT (Gravidade, Urgência e Tendência) e a Matriz PARE (Prazo, Aceitação, Recursos e Efetividade).

10.12. Técnica de Painel e de Delfos

A técnica de Painel tem como objetivo principal obter uma opinião coletiva que represente um ponto de vista dominante, a partir de uma reunião de especialistas experientes para debater um assunto específico.

A técnica de Delfos obtém e combina em sequências, as opiniões de especialistas experientes, tendo em vista alcançar consenso em relação a determinado assunto. Nesse caso, após tabulação de um questionário, discutem-se as questões em que não houve consenso, seguidamente e em consecutivas consultas, até que se evidencie uma opinião convergente. Essa técnica não prevê a realização de debates entre os participantes.

10.13. Técnica de Análise Associativa e de Cenários

A técnica de Análise Associativa consiste em aplicar as relações entre os principais aspetos de determinados assunto, valendo-se de matrizes de associação.

A técnica de Cenários, implica em descrever as alternativas futuras e plausíveis para a evolução de determinado assunto. Efetiva-se mediante análises prospectivas que tratam o assunto sob diversos prismas de interpretação e envolvem variáveis de diversas naturezas.

10.14. Método Brasiliano

O método Brasiliano é uma forma de acompanhar a evolução dos perigos organizacionais. A aplicação do método resulta em uma matriz de vulnerabilidade, resultante do cruzamento da probabilidade de ocorrência do perigo versus o impacto financeiro para a organização.

Ao contrário dos métodos de Mosler e T. Fine, que classificam o perigo, o método Brasiliano estima a probabilidade de ocorrência do perigo considerando as influências do ambiente interno e externo da organização.

A elaboração do Grau de Probabilidade implica em estudar o Critério dos Fatores de Riscos e o Critério da Exposição. “O Grau de Probabilidade está alicerçado em uma fórmula simples, que calcula de forma direta, através da multiplicação dos dois critérios, o nível de possibilidade do perigo ou evento vir a acontecer, frente a situação de segurança e sua exposição”. (Brasiliano, 2008)

O Grau de Probabilidade pode ser classificado de forma objetiva ou de forma subjetiva. Baseado nessa classificação e no cruzamento com o impacto (operacional e/ou financeiro) decorrente da concretização do perigo é possível montar a matriz de vulnerabilidade e priorizar o tratamento que será dado aos riscos da organização.

O método Brasiliano possui quatro fases. São elas:

- 1ª Fase – Identificação dos Fatores de Riscos: nessa fase, são identificadas a origem/causa de cada perigo. Para dissecar os fatores que podem influenciar na concretização do perigo é utilizado o Diagrama de Causa e Efeito, também conhecido como Diagrama de *Ishikawa*. Os fatores de riscos podem ser classificados em seis categorias (sub critérios) principais. São elas:
  - Meios organizacionais (MO): identifica se a organização possui normas de rotina, política de tratamento e gerenciamento de riscos;
  - Recursos humanos da segurança (RH): identifica o nível de qualificação, quantidade, posicionamento tático da equipe de segurança;
  - Meios técnicos passivos (MTP): identifica a existência de recursos físicos, não existentes na organização, que corroboram para a ocorrência do perigo;

– Meios técnicos ativos (MTA): identifica a existência de sistemas eletrônicos que corroboram, ou não, para a concretização de perigos;
– Ambiente interno (AI): é o levantamento do nível de relacionamento dos colaboradores da organização;
– Ambiente externo (AE): identifica fatores externos que influenciam na concretização de perigos.

- 2ª Fase – Determinação do Grau de Probabilidade (GP): o cálculo do Grau de Probabilidade é feito multiplicando-se critério de Fatores de Riscos (FR) com o critério de Exposição (E).

Para calcular o critério de Fator de Risco, basta somar a pontuação de cada um dos seis sub critérios e dividir por 6. Segue tabela que correlaciona a escala e a pontuação dos sub fatores:

Escala	Pontuação
Influencia muito	05
Influencia	04
Influencia medianamente	03
Influencia levemente	02
Influencia muito levemente	01

$$FR = \frac{AI + AE + RH + MO + MTA + MTP}{6}$$

O critério de Exposição (E) é a freqüência que o perigo costuma se manifestar na organização ou em organizações similares. A tabela a seguir apresenta a escala de gradação para esse critério:

Escala	Pontuação
várias vezes ao dia	05
frequentemente	04
ocasionalmente	03
irregularmente	02
remotamente possível	01

Grau de Probabilidade = Fator de Risco x Exposição

O produto dessa multiplicação é o Grau de Probabilidade que por sua vez é classificado em cinco níveis:

Escala	Nível da Probabilidade	Nível da Probabilidade
1 – 5	Muito Baixo	Improvável
5,1 – 10	Pequeno	Remota
10,1 – 15	Normal	Ocasional
15,1 – 20	Alta	Provável
20,1 – 25	Elevado	Frequente

A transformação dessa classificação subjetiva em objetiva, dá-se multiplicando o Grau de Probabilidade pelo fator 4. A explicação para utilização do fator 4 está na equivalência entre o numero máximo obtido pela multiplicação entre os fatores de riscos e de exposição - 25 e a probabilidade máxima – 100%.

- 3a fase – Determinação do Impacto Financeiro: nessa etapa o objetivo é projetar os custos que os perigos causam nos negócios da organização, levantando suas conseqüências. A multiplicação entre a probabilidade de ocorrência de cada risco com o seu impacto financeiro indica o investimento necessário para mitigar, eliminar ou transferir o perigo. O produto dessa multiplicação é denominado Perda Esperada (PE) e é considerado o investimento máximo a ser realizado pela organização.

O método Brasiliano sugere um estudo baseado nos custos prováveis caso determinado perigo venha a se concretizar. Nesse estudo, a organização deve considerar os seguintes dados:

– Custo conseqüente (Cc): é avaliado o prejuízo resultante de um risco à organização;
– Indenização do Seguro (I): avalia quanto o seguro irá reembolsar à empresa no caso de ocorrência do sinistro;
– Prêmio pago até o momento do sinistro (P): avalia quanto já foi pago à seguradora;

– Redução de dinheiro em caixa (Rc): refere-se à redução efetiva do numerário em caixa;
– Substituição permanente (Sp): enquadram-se os custos definitivos que a empresa não obterá mais;
– Substituição temporária (St): enquadram-se os custos que a empresa perde temporariamente.

Assim, o custo provável das perdas reais e potenciais (CP) é calculado pela fórmula:

CP = Sp + St + Cc + Rc – (I – P)

Para Brasiliano (2008), a classificação de impacto no negócio é própria de cada empresa, porém sugere a seguinte escala: leve, moderado, severo e catastrófico. Tal parâmetro é fundamental para que o gestor possa definir quais perigos e em que urgência devem ser tratados.

- 4ª Fase – Elaboração da Perda Esperada (PE) e Matriz de Vulnerabilidade: nessa etapa o objetivo é calcular um parâmetro (PE) para a comparação entre investimento em prevenção e conseqüências empresariais. Este parâmetro pode ser representado por meio de uma matriz – a Matriz de Vulnerabilidade.

Dessa forma, a Matriz de Vulnerabilidades representa o cruzamento entre a probabilidade de ocorrência de um perigo e o impacto financeiro que sua concretização resultará para a organização.

A figura a seguir apresenta uma das formas de representação da Matriz de Vulnerabilidade:

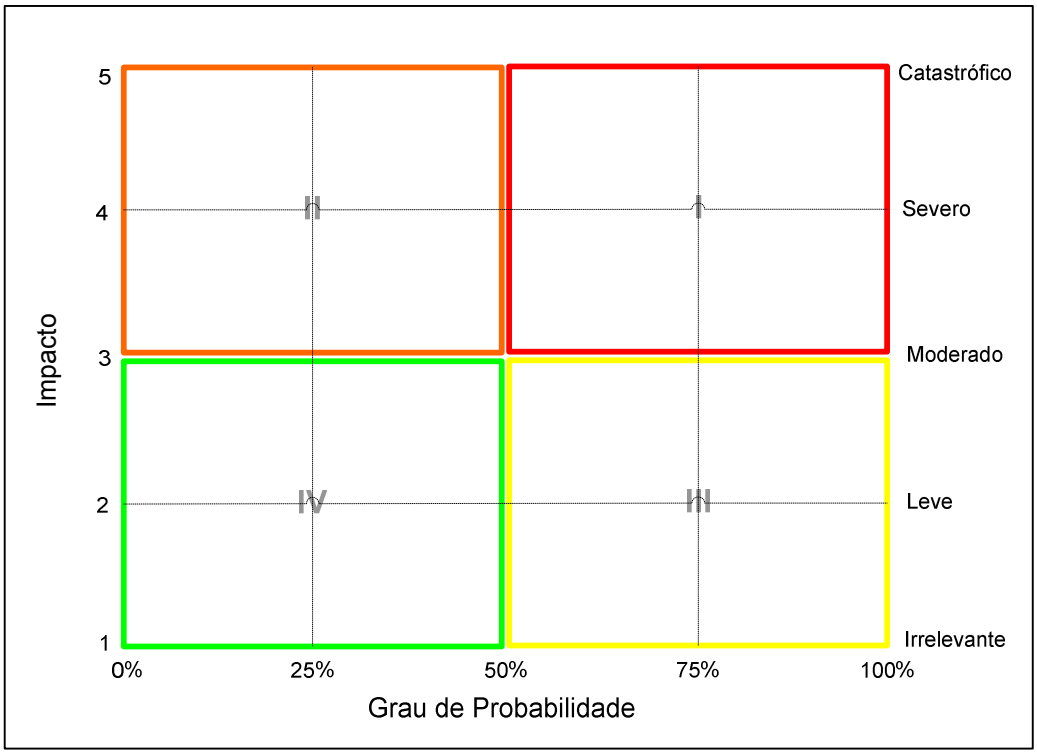


Figura 12 - Matriz de Responsabilidades. Fonte: Brasiliano (2005, p.34)

A Matriz de Responsabilidade pode fundamentar as estratégias organizacionais de proteção, pois representa uma justificativa para os investimentos conforme a influência dos perigos nos resultados da organização.

Observa-se na figura acima que a matriz é dividida em quatro quadrantes, donde podemos considerar:

a. Os riscos existentes no quadrante I são aqueles que possuem alta probabilidade e ocorrência e, caso se concretizem, poderão resultar em impactos severos ou catastróficos à organização. Assim, exigem a pronta implantação de estratégias de proteção e prevenção;

b. Os riscos existentes no quadrante II podem resultar em impactos severos ou catastróficos à organização, porém, possuem menor probabilidade de ocorrência. Sugere-se que sejam monitorados de forma sistemática e periódica;

c. No quadrante III, estão os riscos com alta probabilidade de ocorrência, mas que causam poucos danos à

organização. Para essas ameaças deve ser previsto um plano de contingência com respostas rápidas e planejadas;

d. Os riscos do quadrante IV possuem baixa probabilidade e, caso se concretizem, resultam em pequenos impactos para a organização. Podem, portanto, serem somente gerenciados e monitorados caso venham a se concretizar.

11. Gestão de riscos de segurança da informação

> Risco de segurança da informação é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos de informação, desta maneira prejudicando a organização. (ABNT, 2008, p.1)

Beal (2005, p.16) relaciona os termos associados ao risco à Segurança da Informação, conforme mostrado na figura 13:

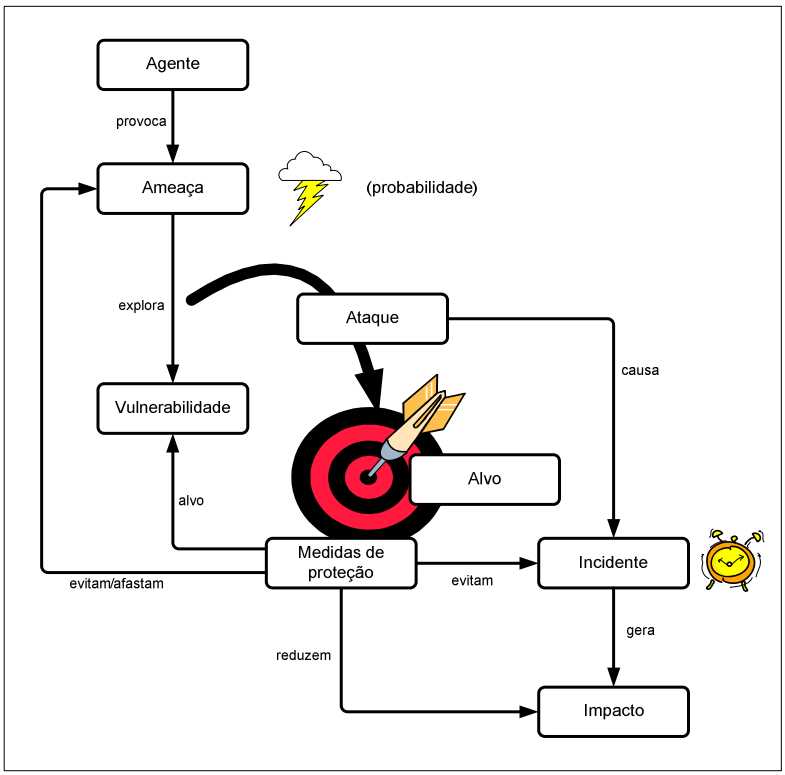


Figura 13 – Relacionamento entre os termos associados ao risco para a SI. Fonte: Beal (2005, p.16 - adaptado)

Para Beal (2005, p.15), o alvo de um ataque pode ser um ativo de informação. Nesse contexto, a ameaça é um elemento do risco ao qual pode-se

associar uma probabilidade que por sua vez é calculada a partir da frequência de ocorrência. As medidas de proteção podem reduzir a probabilidade de concretização de uma ameaça e as vulnerabilidades com potencial de exploração, consequentemente corroboram para a redução do risco ao ativo de informação.

De acordo com Braithwaite (2002), realizar o gerenciamento de riscos em segurança da informação consiste em aplicar os conceitos de gerenciamento de riscos sobre o tema segurança da informação.

Para fundamentar sua teoria, Braithwaite (2002) apresenta o modelo de gerenciamento de riscos proposto por Campbell e Sands (1979). Esse modelo é apresentado na figura abaixo:

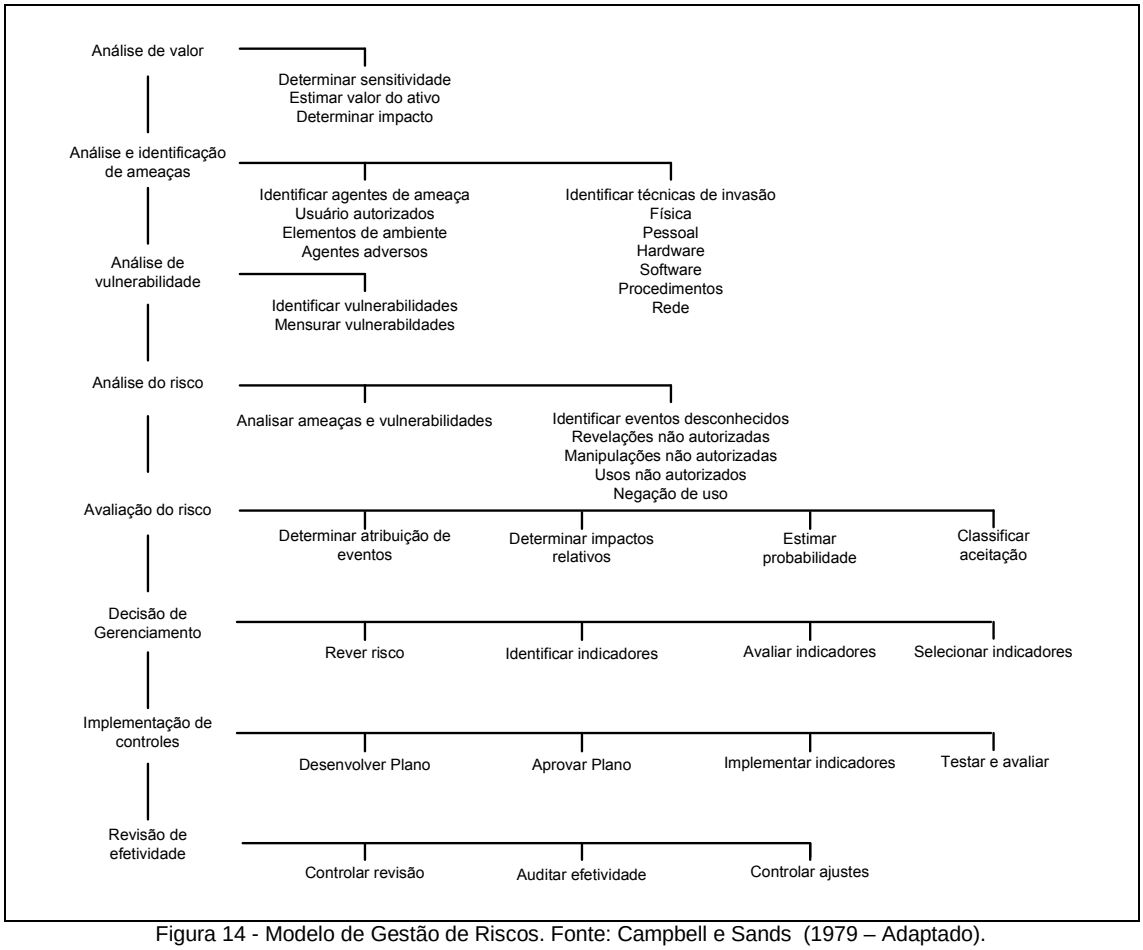


Figura 14 - Modelo de Gestão de Riscos. Fonte: Campbell e Sands (1979 – Adaptado).

Alberts & Dorofee (2002) propõem um modelo para o processo de gerenciamento de riscos em segurança da informação composto por cinco etapas: identificação e análise, planejamento, implementação, monitoração e controle.

O modelo de processo de gestão de riscos em segurança da informação que será abordado nesta pesquisa é proposto pela Norma ABNT NBR ISO/IEC 27005: 2008.

Neste modelo, o processo de gestão de riscos em segurança da informação é um processo contínuo e consiste na definição do contexto, análise/avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco e monitoramento e análise crítica de riscos.

A figura 15 mostra uma visão geral das etapas do processo de gestão de riscos em segurança da informação.

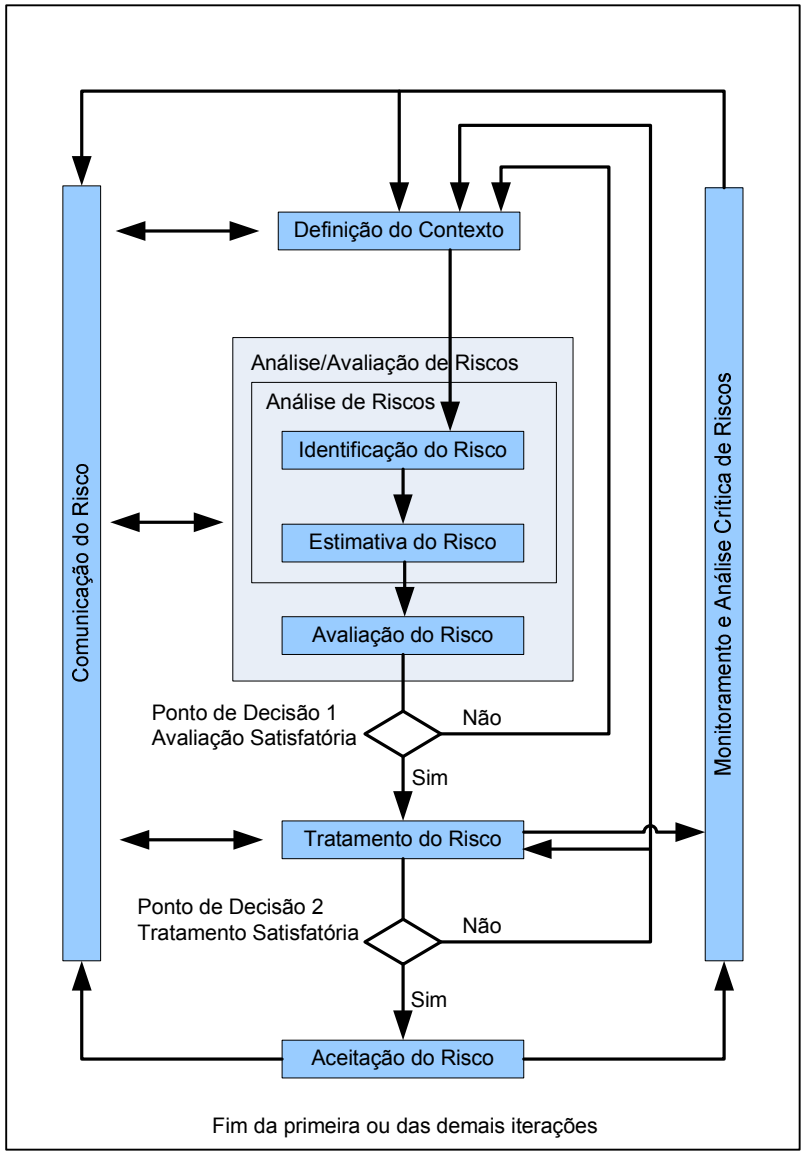


Figura 15 - Processo de gestão de riscos de segurança da informação. Fonte: ABNT ISO/IEC 27005 (2008, p.5).

11.1. Etapas do processo de gestão de riscos de segurança da informação

11.1.1. Definição do contexto

De acordo com a norma ABNT NBR ISO/IEC 27005:2008, nesta etapa do processo, o contexto da gestão de riscos em segurança da informação é estabelecido a partir das informações sobre a organização de forma a definir: os critérios básicos necessários para a gestão de riscos, o escopo da gestão de riscos e a estrutura apropriada para operar a gestão de riscos de segurança da informação.

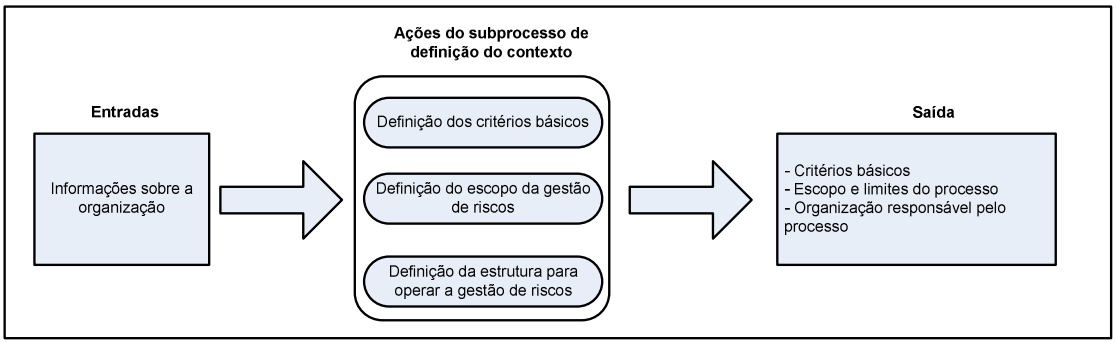


Figura 16 - Definição do contexto. Fonte: elaboração própria.

Os critérios básicos para a gestão de riscos em segurança da informação definem os parâmetros necessários para avaliar os riscos, bem como seus impactos e os critérios de aceitação no contexto organizacional.

A definição do escopo do processo de gestão de riscos de segurança da informação é fundamental para assegurar que os ativos organizacionais mais relevantes sejam considerados durante o subprocesso de análise/avaliação dos riscos. (ABNT NBR ISO/IEC 27005:2008, p.8)

Por fim, convém que a organização (estrutura funcional) para o processo de gestão de riscos de segurança da informação e as alçadas para a tomada de decisões sejam especificadas de forma a definir os papéis e responsabilidades das partes envolvidas.

11.1.2. Análise/avaliação de riscos de segurança da informação

Definidos os critérios básicos, o escopo e a organização do processo de gestão de riscos de segurança da informação, a etapa de análise/avaliação de riscos envolve identificar, quantificar e priorizar os riscos tendo como parâmetro os critérios de avaliação de riscos e os objetivos organizacionais.

De acordo com a ABNT NBR ISO/IEC 27005 (2008, p.10),

> “A análise/avaliação de riscos determina o valor dos ativos de informação, identifica as ameaças e vulnerabilidades aplicáveis existentes, identifica os controles existentes e seus efeitos no risco identificado, determina as conseqüências possíveis, prioriza os riscos derivados e ordena-os de acordo com os critérios de avaliação de riscos estabelecidos na definição do contexto”.

Fazem parte do subprocesso de análise/avaliação de risco as seguintes atividades:

- Identificar e classificar os riscos: o objetivo da identificação dos riscos é determinar os eventos que podem causar perdas para a organização e identificar as causas e as situações em que as perdas podem ocorrer.

- Estimar os riscos: tem como objetivo principal descrever a magnitude das consequências potenciais do risco e a probabilidade dessas consequências ocorrerem.

- Avaliar os riscos: a avaliação é feita a partir da comparação entre os níveis dos riscos e os critérios de avaliação e aceitação dos riscos decididos durante a definição do contexto.

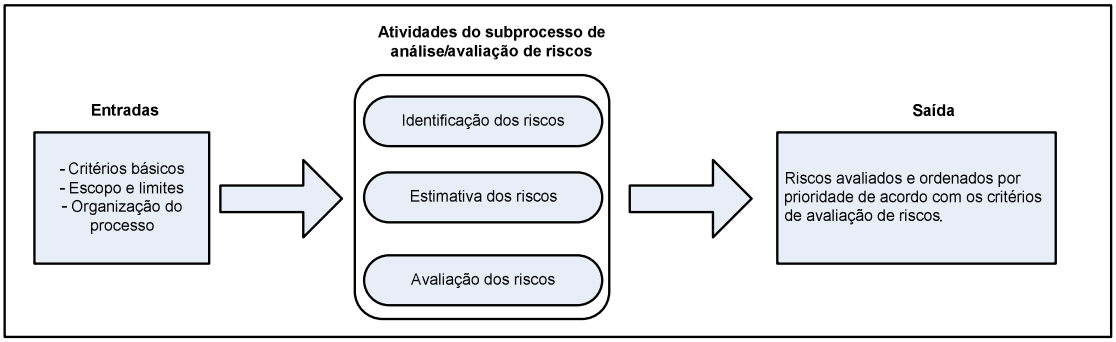


Figura 17 - Análise/avaliação de riscos de segurança da informação. Fonte: elaboração própria.

11.1.3. Tratamento do risco

O subprocesso de análise/avaliação dos riscos produz uma lista de riscos ordenados por prioridade e associados aos cenários de incidentes que os provocam. Essa lista fomenta o subprocesso de tratamento do risco e permite definir o plano de tratamento e os controles para mitigar, reter, evitar ou transferir os riscos.

A figura 18 mostra a atividade de tratamento do risco no processo de gestão de riscos da informação.

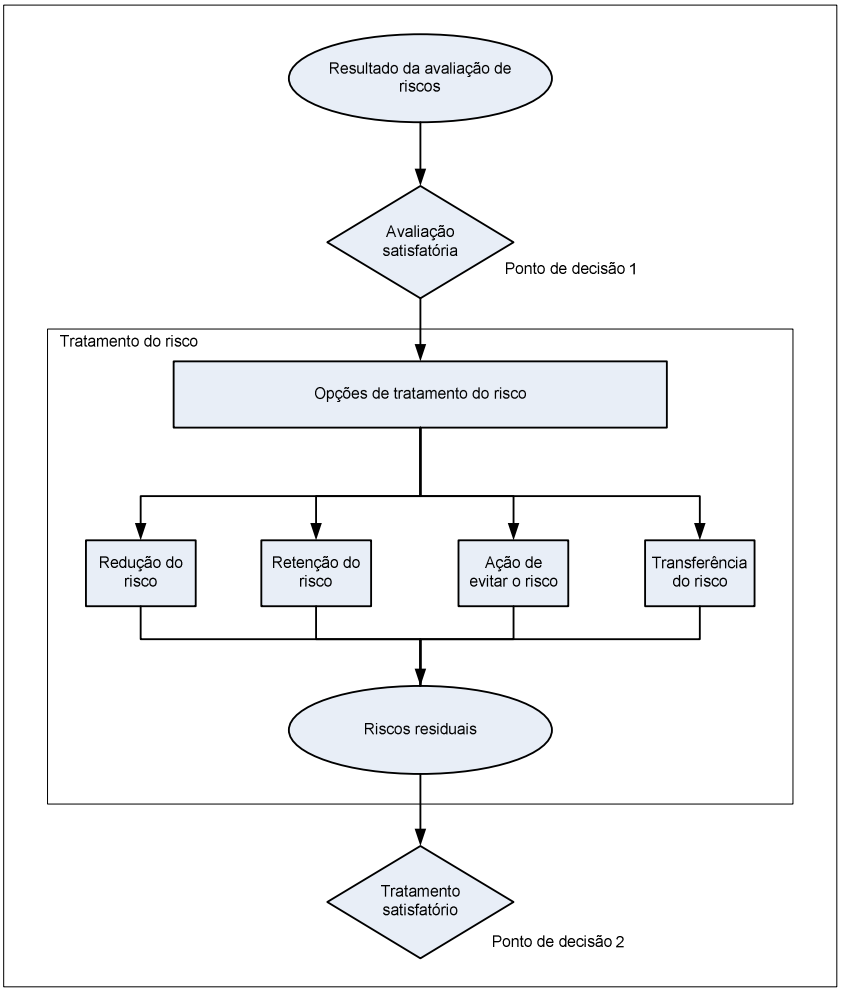


Figura 18 - A atividade de tratamento do risco. Fonte: ABNT NBR ISO/IEC 27005 (2008, p.18).

O resultado dessa etapa é um plano de tratamento dos riscos que compreende a relação de controles possíveis, acompanhada de seus custos, benefícios e prioridades de implementação, sujeitos à decisão de aceitação por parte dos gestores da organização.

Convém que a decisão do tratamento que será dado a determinado risco considere, além dos critérios para aceitação dos riscos, os requisitos legais e regulatórios vigentes.

Durante a seleção dos controles é fundamental mensurar os custos da aquisição, implementação, administração, operação dos controles em relação ao valor dos ativos protegidos (ABNT NBR ISO/IEC 27005:2008, p.19).

11.1.4. Aceitação do risco

Em alguns casos, ao avaliar o plano de tratamento do risco, é preciso que se aceite o risco no âmbito organizacional, seja porque a probabilidade de se

concretizar é pequena, seja porque os impactos nos processos são irrelevantes ou porque os custos de sua redução são demasiadamente elevados.

No entanto, a decisão de aceitar os riscos deve ser formalmente registrada juntamente com a responsabilidade pela decisão (ABNT NBR ISO/IEC27001, p.6).

O produto desse subprocesso é a relação dos riscos aceitos acompanhada das justificativas para aqueles que não satisfaçam os critérios normais para aceitação do risco (ABNT NBR ISO/IEC 27005:2008, p. 21).

11.1.5. Monitoração e análise crítica de riscos

Os riscos são eventos dinâmicos, visto que as ameaças, as vulnerabilidades, a probabilidade e as consequências no ambiente organizacional podem mudar repentinamente, e vir a ampliar os riscos anteriormente avaliados como pequenos.

Assim, de acordo com a ABNT NBR ISO/IEC 27005:2008, convém que os riscos e seus fatores sejam monitorados e analisados criticamente, a fim de se identificar tempestivamente as eventuais mudanças no contexto organizacional e se manter uma visão geral.

O resultado da atividade de monitoramento de riscos é um alinhamento contínuo da gestão de riscos com os objetivos da organização e com os critérios para a aceitação do risco.

11.1.6. Comunicação do risco

A percepção do risco pode variar devido a diferenças de conceitos, necessidades e interesses das partes envolvidas no processo de gestão de risco em segurança da informação.

Dessa forma, o objetivo do subprocesso de comunicação do risco é assegurar um consenso e um bom entendimento sobre como os riscos devem ser gerenciados, o porquê de determinadas decisões e os motivos de certas ações. (ABNT NBR ISO/IEC 27005:2008, p.21)

A comunicação eficaz e a interrelação das partes envolvidas no tratamento dos riscos pode ter um impacto significativo nos processos de decisão da gestão de riscos em segurança da informação.

12. Conclusão da Revisão de Literatura e Fundamentos

A informação é um ativo essencial para os negócios de uma organização – seja por seu valor estratégico, seja por seu valor histórico – na corrida em busca de agilidade, competitividade, modernização, lucratividade e principalmente flexibilidade e adaptabilidade para o crescimento.

Do ponto de vista estratégico, a mensagem enviada por uma economia global e baseada na informação denota que a informação é a base para a competição. Tal fato exige que os gestores sejam eficazes e eficientes para identificar o papel que a informação irá desempenhar na estratégia competitiva de suas organizações.

Considerando o valor histórico da informação, destacam-se a natureza probatória da informação e seus aspectos que elucidam fatores econômicos, políticos, sociais e de pesquisa no âmbito da organização.

Tais fatores justificam porque a informação, como ativo, bem e patrimônio organizacional, deve ser protegida e guardada como um segredo de negócio.

É neste contexto que a Segurança da Informação, como área do conhecimento dedicada à proteção de ativos da informação, adquire papel de destaque nas organizações. O estudo da Segurança da Informação permite implementar controles de proteção da informação contra vários tipos de ameaças garantindo a confidencialidade, integridade e disponibilidade da informação, minimizando o risco ao negócio, direcionando o emprego de recursos e maximizando o retorno sobre os investimentos e as oportunidades de negócio.

No entanto, não raramente, tem-se nas organizações a impressão de que a melhoria nos processos de segurança da informação depende única e exclusivamente de investimentos generalizados em equipamentos de *hardware* e *software*. As experiências têm demonstrado que o investimento em recursos de Tecnologia da Informação nem sempre traz o retorno desejado. Adicionalmente, é necessário dedicar atenção especial aos processos e aos recursos humanos da organização. Esses três fatores (TI, processos e pessoas) constituem os pilares que dão sustentação à Segurança da Informação, os quais, se não balanceados, podem colocar em risco todo o esforço dedicado a proteção dos ativos de informação.

Atualmente, existe um arcabouço legal e normativo que orienta o comportamento das pessoas e baliza os controles organizacionais que prezam pela qualidade dos processos e a integridade da informação. As boas práticas de segurança da informação apontam que os sistemas de segurança da informação estejam em consonância com as leis e em conformidade com as orientações de normatização e regulamentação do mercado. Todavia, os valores, a cultura e o

comportamento humano no ambiente organizacional não podem ser ignorados na concepção e na implementação de controles de segurança da informação.

Partindo das premissas que não existe sistema totalmente seguro e que há diferenças de complexidade, emprego de recursos e custos financeiros para manter os ativos de informação a salvo de ameaças à sua confidencialidade, integridade e disponibilidade, o enfoque de gestão baseada nos riscos específicos ao negócio torna-se fundamental para o processo de Gestão de Segurança da Informação das organizações.

A gestão de riscos em segurança da informação fornece subsídios que fundamentam a tomada de decisões sobre como empregar recursos para proteção dos ativos de informação de uma organização. Por meio da gestão de riscos, é possível conhecer as ameaças e as vulnerabilidades a que estão sujeitas as informações, bem como os impactos resultantes do comprometimento de sua segurança. Assim, a tomada de decisão sobre como empregar recursos para proteger os dados corporativos torna-se melhor fundamentada e mais confiável.

Parte III – Estudo de Caso

13. Diagnóstico do processo de gestão de segurança da informação e gestão de risco na ECT

O diagnóstico do processo de gestão de segurança da informação inicia-se com a análise do panorama atual das questões relativas à segurança da informação e gestão de riscos em segurança da informação da Empresa Brasileira de Correios e Telégrafos. Esse diagnóstico foi realizado em julho de 2009 a partir de levantamento das iniciativas corporativas e da análise de documentos e manuais corporativos.

Verificou-se que, ao contrário da maioria dos órgãos da Administração Pública Federal, a ECT possui uma política corporativa de segurança de suas informações, homologada em novembro de 2001. A ECT define política de segurança da informação como o conjunto de diretrizes e normas que devem ser seguidas no âmbito corporativo e ”visa conscientizar e orientar os empregados, clientes, parceiros e fornecedores para o uso seguro do ambiente informatizado da ECT” (ECT, 2007).

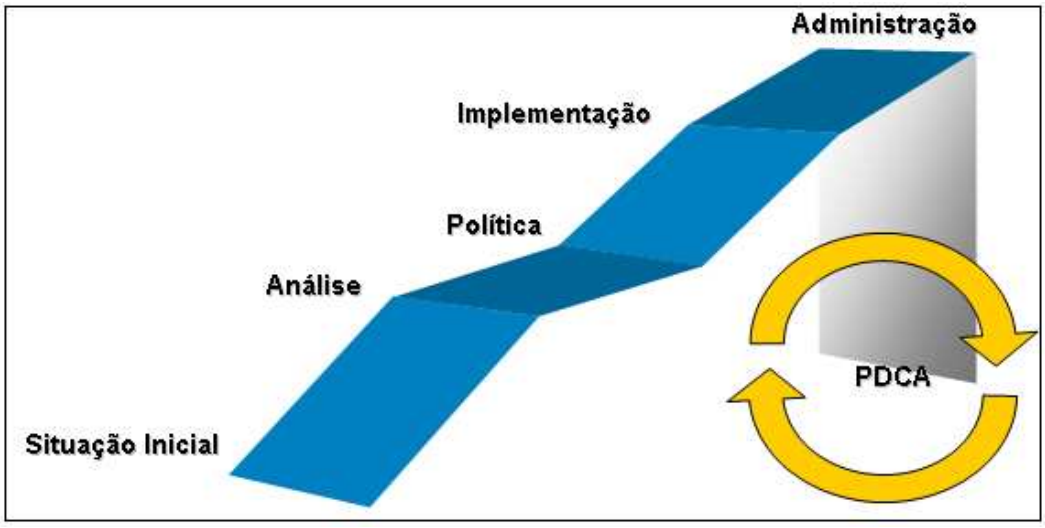


Figura 19 - Ciclo de criação da Política de Segurança da Informação da ECT. Fonte: elaboração própria.

O cumprimento da Política de Segurança da Informação é de responsabilidade de todos colaboradores, empregados ou prestadores de serviços, que devem obedecer à uma série de diretrizes. As diretrizes da Política de Segurança da Informação da ECT estão descritas no Anexo 1.

Adicionalmente, está publicado no Manual de Informática da ECT – MANINF, módulo 07, um conjunto de 21 capítulos que compõem as normas de segurança da informação da ECT. As normas de segurança da informação têm como objetivo principal assegurar que a política de segurança da informação seja implementada, mantida ou modificada de forma harmônica e convergente, de acordo

com os objetivos estabelecidos, garantindo a Segurança da Informação na ECT, a continuidade do negócio e a mitigação de riscos". As normas de segurança da informação da ECT estão estruturadas conforme Anexo 2.

A política e as normas de Segurança da Informação da ECT são as bases para o estabelecimento de todos os padrões corporativos de segurança. Sua abrangência compreende todos os ambientes de informática da ECT.

Como estrutura organizacional, há na Administração Central uma gerência corporativa para tratar de normas e padrões, incluindo a segurança da informação. Essa gerência corporativa (Gerência Corporativa de Normas e Padrões Tecnológicos - GNOP) é subordinada ao Departamento de Planejamento de Tecnologia da Informação e Comunicação – DETIC. Os assuntos operacionais relacionados à segurança da informação são de responsabilidade de uma equipe técnica subordinada a Central de Suporte e Produção – CESEP.

Baseado nas recomendações da Instrução Normativa GSI Nº 1 (Anexo 3), publicada em 13 de junho de 2008 pelo Gabinete de Segurança da Informação da Presidência da República, foram identificadas as principais falhas no processo de gestão de segurança da ECT. São elas:

a. Ausência de uma estrutura organizacional única e vinculada diretamente à alta administração da empresa, responsável por coordenar as ações de segurança da informação, aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra da segurança das informações e propor programa orçamentário específico para as ações de segurança da informação;

b. Ausência de profissional nomeado para Gestor de Segurança da Informação e responsável por: promover a cultura de segurança da informação, acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança, propor recursos necessários às ações de segurança da informação, coordenar o comitê de segurança da informação e a equipe de tratamento e resposta a incidentes em redes computacionais, realizar e acompanhar estudos de novas tecnologias, manter contato com os demais órgãos da APF e propor normas relativas à segurança da informação;

c. Ausência de comitê de segurança da informação, constituído por representantes das diversas diretorias da empresa, para tratar temas e propor soluções específicas sobre segurança da informação;

d. Falta de integração com os demais órgãos da Administração Pública Federal, incluindo o Gabinete de Segurança da Informação da Presidência da República, para tratar de assuntos referentes à Segurança da Informação;

Adicionalmente, destacamos como falha no processo de gestão de segurança da ECT a ausência do processo corporativo que defina a classificação da informação e a tabela de temporalidade[9] dos documentos corporativos.

Quanto às atividades de gestão de riscos na ECT, não existe órgão na estrutura organizacional nem modelo de gestão de riscos sistematizado em aplicação. Há o uso setorizado de alguns conceitos de análise de riscos, entretanto não há um uso corporativo do conhecimento sobre o tema.

Em fevereiro de 2008, foi emitida a Portaria PRESI-027/2008 que instituiu um Grupo de Trabalho para propor a organização e estruturação da gestão de riscos e a reorganização das atividades de segurança empresarial na ECT.

De acordo com o grupo de trabalho, a reorganização das atividades de segurança empresarial na ECT envolve inicialmente o entendimento do conceito de Segurança Empresarial, o seu contorno e limites na relação com as demais atividades desenvolvidas na Empresa.

Para o correto entendimento do conceito de segurança empresarial, procurou-se estabelecer os objetos e respectivos valores protegidos por intermédio das medidas de segurança no ambiente da ECT.

Os seguintes valores foram identificados como elementos da atuação da segurança empresarial: Vida, Negócio, Conhecimento e Recursos. A partir desta identificação foram relacionados os seguintes objetos, razão da atuação da segurança empresarial: Pessoas, Objetos Postais, Informação, Receitas e Patrimônio.

Dessa forma, a proposta do grupo de trabalho é desempenhar a segurança empresarial na ECT considerando os diferentes bens protegidos, de modo coordenado por todas as áreas e em harmonia com os demais segmentos de atuação

[9] A tabela de temporalidade define quais documentos serão preservados para fins administrativos ou de pesquisa e em que momento poderão ser eliminados ou destinados aos arquivos intermediário e permanente, segundo o valor e o potencial de uso que apresentam para a administração que os gerou e para a sociedade.

da Empresa, visando atingir os objetivos da instituição, conforme a organização a seguir relacionada:

1. Segurança patrimonial: compreende as ações e os recursos voltados à proteção ao patrimônio, incluindo-se os bens móveis, os estoques, os bens imóveis e o numerário disponível na Empresa em decorrência de atividades que lhes são peculiares.

2. Segurança das pessoas: envolve ações e recursos direcionados à proteção das pessoas que atuam na organização considerando-se dois grupamentos:
    a. A segurança dos empregados e colaboradores envolvendo os riscos, as doenças e os acidentes que decorram das operações da ECT. Traduz-se no conjunto de medidas e ações que visam prevenir, detectar e corrigir os atos inseguros e as condições ambientais inadequadas ao trabalho, de modo a prevenir a ocorrência dos acidentes do trabalho;

    b. A segurança dos gestores e técnicos envolvendo os riscos caracterizados pela natureza e o nível de exposição das decisões vinculadas às atividades típicas da função exercida. Traduz-se no conjunto de benefícios garantidos ao gestor e aos técnicos para o legal e regular exercício do mandato recebido da Empresa.

3. Segurança das informações: abrange ações e recursos voltados à proteção das informações, entendidas como relatórios, documentos, dados, conhecimento intrínseco e outras formas de registros oficiais relativos, dentre outros, aos processos, produtos, estudos e projetos, decorrentes das atividades da ECT. Divide-se em três grupamentos:
    a. Informações físicas – envolvem todos os papéis oficiais da Empresa, incluindo seus documentos fiscais, processos de todas as naturezas, expedientes e demais instrumentos de comunicação, que registram os atos praticados na ECT;

b. Informações lógicas – envolvem os registros digitais da Empresa, incluindo arquivos operacionais e administrativos relativos a todos os sistemas em operação na Empresa.

c. Comportamental – inclui as Informações intrínsecas, o conhecimento tácito, não explícito, específico de cada profissional técnico ou gestor na Empresa.

4. Segurança postal – compreende as ações e recursos direcionados à proteção dos objetos postais integrados ao processo operacional de recebimento, expedição, transporte e entrega. Inclui as medidas, os procedimentos, os instrumentos e os equipamentos adotados pelos Correios com a finalidade de prevenir e de detectar as infrações e as irregularidades no serviço postal e de telegramas. Está subdividida em quatro grupamentos:
    a. Processos de Recebimento;
    b. Processos de Expedição;
    c. Processos de Transporte;
    d. Processos de Entrega.

5. Segurança das Receitas – compreende as ações e recursos destinados aos controles das receitas a vista e a faturar, incluindo os registros físico-financeiros.

Definida a organização da segurança empresarial, e considerando a sinergia do assunto com a gestão de riscos, a proposta do grupo de trabalho é criar um comitê de gestão de riscos e segurança empresarial, vinculado ao Comitê Executivo da Empresa Brasileira de Correios e Telégrafos.

O comitê executivo de gestão de riscos e segurança da informação teria como missão construir a sinergia entre as diversas áreas da Empresa envolvidas com os temas, desenvolver e propor as políticas globais, coordenar a elaboração dos planos de ação, de contingência e de continuidade de negócios e acompanhar a evolução dos indicadores e metas relativas aos temas.

14. Identificação dos espaços informacionais dos usuários e riscos aos ativos de informação da ECT

Desde o início da década de 80, com o advento dos equipamentos de processamento de dados, as organizações humanas tornam-se cada vez mais dependentes de informações armazenadas em computadores.

A velocidade e a capacidade de processamento de informações dos computadores são utilizadas para agilizar o processo de tomada de decisões e auxiliar o processo de definição/alteração de estratégias.

Por outro lado, a mesma facilidade proporcionada pelos computadores contribui sobremaneira para o aumento das ameaças aos espaços informacionais[10] da ECT e, dessa forma, podem colocar em risco a confidencialidade, a integridade e a disponibilidade das informações.

Analisando os espaços informacionais virtuais da ECT – tais como: web sites, bancos de dados, bibliotecas virtuais e comunidades práticas de conhecimento – identificamos alguns riscos que afetam as informações corporativas. Dentre eles destacamos:

- Concentração de informações: ao multiplicar a quantidade de informações que podem ser armazenadas em espaços restritos, a utilização de computadores potencializou um problema que já existia antes da era do advento da informática;

- Acesso indiscriminado às informações: não raramente, usuários têm acesso a mais recursos e informações do que necessitam para executar suas funções.

- Obscuridade das informações: com os computadores o problema da obscuridade das informações tornou-se crucial, uma vez que a informações disponíveis em meios eletrônicos não pode ser vistas diretamente, isto é, precisam de recursos de *hardware* e *software*. Assim, são mais difíceis de serem controladas e, conseqüentemente, mais fáceis de serem roubadas ou fraudadas.

[10] Um “espaço informacional” significa qualquer sistema que inclua a interação com usuários, com o objetivo de resgatar ou trocar informações. (Agner & Silva, 2003)

- Concentração de funções: a concentração de funções pode tornar a organização vulnerável ao humor de poucos indivíduos e permitir que um mesmo indivíduo adquira conhecimentos para executar ações ilícitas e obter vantagens por meio das informações que manuseia.

- Falta de controle: a ausência de controles pode retardar a descoberta de irregularidades impossibilitando a tomada de ações que poderiam remediar as situações indesejadas e seus impactos.

- Relacionamento e combinação de informações: o cruzamento e combinação de informações podem revelar informações sigilosas e permitir a quebra de confidencialidade. Os recursos de informática facilitam os processos de relacionamento e combinação de informações permitindo a obtenção de informações sensíveis.

- Introdução de códigos ocultos: são erros ou linhas de códigos que podem ser inseridas nas rotinas de processamento da informação e comprometer a confidencialidade, integridade e confidencialidade das informações geradas.

Caruso & Steffen (1999) afirmam, no Capítulo 2 de seu livro, Segurança em Informação e de Informações, que os riscos decorrem de fatores que, em maior ou menor grau, aparecem nas organizações humanas e sua principal diferença é a escala e o grau de acesso existente.

15. Estudo de ações para nortear o processo de Gestão de Segurança da Informação e proposta de modelo sistêmico para a Gestão de Riscos que norteie a Gestão de Segurança da Informação.

A ECT será utilizada como ambiente empírico para estudar as ações necessárias para nortear o processo de Gestão de Segurança da Informação, a partir da aplicação do conceito de Gestão de Riscos, que tem como ponto de partida uma prospecção realizada pelo Grupo de Gestão de Riscos instituído por meio de portaria para atuar no âmbito interno da organização.

Para a realização das prospecções, o Grupo identificou empresas públicas e privadas com nível de complexidade de gestão compatível com a ECT e realizou *benchmarking* para absorção de suas experiências, no tocante a Gestão de Riscos e Segurança Empresarial. Para este trabalho, consideramos somente as iniciativas referentes à Segurança da Informação.

Foram realizadas visitas técnicas nas seguintes empresas: Banco do Brasil, Caixa Econômica Federal, SERPRO, HSBC, UNIBANCO e BR Distribuidora. Foram realizadas pesquisas junto aos principais correios internacionais Canadá, França e Alemanha, e empresas privadas que atuam no setor, como : Fedex e UPS e ainda mantido contatos com institutos de pesquisa e desenvolvimento do tema como a COPEAD/UFRJ. Como resultado das observações das visitas e do *benchmarking* propomos as seguintes ações convenientes ao processo de Gestão de Riscos em Segurança da Informação:

15.1. Base normativa

A base normativa é determinante na organização e estruturação da área de gestão de riscos e segurança da informação. Assim, convém que a organização esteja em consonância com as normas e padrões que servem de referência para o mercado. São elas: Acordo Basiléia II; Lei *Sarbanes-Oxley*; AS/NZS 4360/2004; norma ABNT ISO/IEC 15999-1/2007; norma ABNT ISO/IEC 27001; norma ABNT ISO/IEC 27002; norma ABNT ISO/IEC 27005; norma ABNT ISO/IEC 17799; COBIT e ITIL.

15.2. Ambiente

O ambiente comum às empresas pesquisadas apontou como elementos fundamentais à implementação da gestão de riscos e segurança da informação:

a) comprometimento da alta administração com o tema gestão de riscos;
b) identificação dos processos críticos referentes ao negócio;
c) existência da cultura de controle;

d) existência de sistema de informação estruturado e profissionais capacitados em Gestão de Risco;
e) gerenciamento da organização por processo;
f) difusão do tema em todos os níveis da organização e, ainda, a existência de imposição regulatória.

15.3. Estratégias e Políticas

Dentre os elementos que integram as estratégias e políticas das empresas pesquisadas destacam-se:

a) o disciplinamento ético dos empregados e colaboradores;
b) a conformidade das informações;
c) a transparência da gestão;
d) a segregação de atividades;
e) a acurácia dos registros;
f) o retorno ajustado ao risco sobre capital;
g) o limite de exposição ao risco e de perdas;
h) A unicidade de fonte de dados e a definição de responsabilidades.

15.4. Metodologia de Gestão de Segurança da Informação

A ECT é uma empresa que compõe a Administração Pública Federal, assim, convém que a metodologia de gestão de segurança da informação esteja aderente à metodologia proposta pelo Gabinete de Segurança da Informação da Presidência da República – GSIPR, por meio da Norma Complementar nº02/IN01/DSIC/GSIPR.

Essa metodologia de gestão de segurança da informação baseia-se no processo de melhoria contínua, denominado Ciclo PDCA (*Plan-Do-Check-Act*), referenciado pela norma ABNT ISO/IEC 27001:2006.

O anexo 4 apresenta os detalhes da Norma Complementar nº02/IN01/DSIC/GSIPR – Metodologia de Gestão de Segurança da Informação e Comunicações, publicada no DOU nº 199, de 14 de outubro de 2008 – seção 1.

15.5. Modelo de Gestão de Riscos

Como forma de organização das atividades de segurança empresarial e de gestão de riscos pode-se observar como prática comum:

a) a existência de estrutura exclusiva de Gestão de Risco e segurança da informação;

b) a vinculação da Gestão de Risco à alta administração;
c) a definição de responsabilidades;
d) método de reconhecimento pela boa prática da Gestão de Risco.

15.6. O emprego de metodologia de análise de risco

O emprego de metodologias de análise de riscos permite que as organizações operem seus recursos com eficácia e identifique níveis aceitáveis de riscos aos negócios. Observou-se que a definição de risco aceitável e a abordagem de gerenciamento de riscos podem variar de empresa para empresa.

Há várias metodologias e modelos de gestão de riscos sendo utilizados nas organizações contemporâneas. Cada modelo busca equilibrar, à sua maneira, a precisão, os recursos, o tempo, a complexidade e a subjetividade.

Para analisar os riscos envolvidos nos processos de Gestão de Segurança da Informação utilizamos o Método Brasiliano porque permite estimar a probabilidade de ocorrência do perigo. O método é simples do ponto de vista de aplicação e suscetível a conciliação com a cultura de gestão de segurança em uso na ECT. Além disso, o resultado prático de sua aplicação é uma matriz de vulnerabilidade, resultante do cruzamento da probabilidade de ocorrência e o impacto do perigo, que pode fundamentar a escolha dos recursos a serem empregados para a segurança adequada dos ativos de informação.

Conforme mencionado anteriormente, a aplicação do Método Brasiliano é composta de quatro fases. A primeira fase consiste em identificar a origem/causa de cada perigo. Foram identificados oito principais perigos que podem colocar em riscos a confidencialidade, integridade e confidencialidade das informações no ambiente corporativo de uma empresa pública. São eles:

- Falha de *hardware:* queda de desempenho ou indisponibilidade de equipamentos do ambiente computacional que processam informações corporativas.

- Falha de *software*: queda de desempenho ou indisponibilidade de aplicativos/programas do ambiente computacional que processam informações corporativas.

- Falha no ambiente físico: indisponibilidade dos recursos do ambiente computacional e/ou infraestrutra predial do ambiente

físico. Exemplo: pane elétrica, incêndio, falha no sistema de ar-condicionado.

- Erro humano: queda no desempenho ou indisponibilidade de equipamentos, serviços, aplicativos ou programas em razão de ato não proposital de empregados e colaboradores.

- *Hacking:* queda no desempenho ou indisponibilidade de equipamentos, serviços, aplicativos ou programas em razão de ato proposital de pessoas mal-intencionadas em busca de auto promoção, benefícios financeiros, concorrência desleal ou roubo de informação.

- *Malware*: termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador. Na literatura de segurança o termo *malware* também é conhecido por "software malicioso". Alguns exemplos de *malware* são: vírus, *worms*, *bots*, *backdoors*, cavalos de tróia, *keyloggers*, *spyware*, *rootkits*.

- Desastres naturais: queda no desempenho ou indisponibilidade de equipamentos, aplicativos ou programas em razão fatores naturais tais como enchente, raio e inundação.

- Furto de informação: subtração com ilegítima intenção de apropriação de informação para si ou para outra pessoa.

A figura a seguir correlaciona os perigos identificados aos riscos associados aos ativos de informação, com base no entendimento dos usuários da informação da ECT.

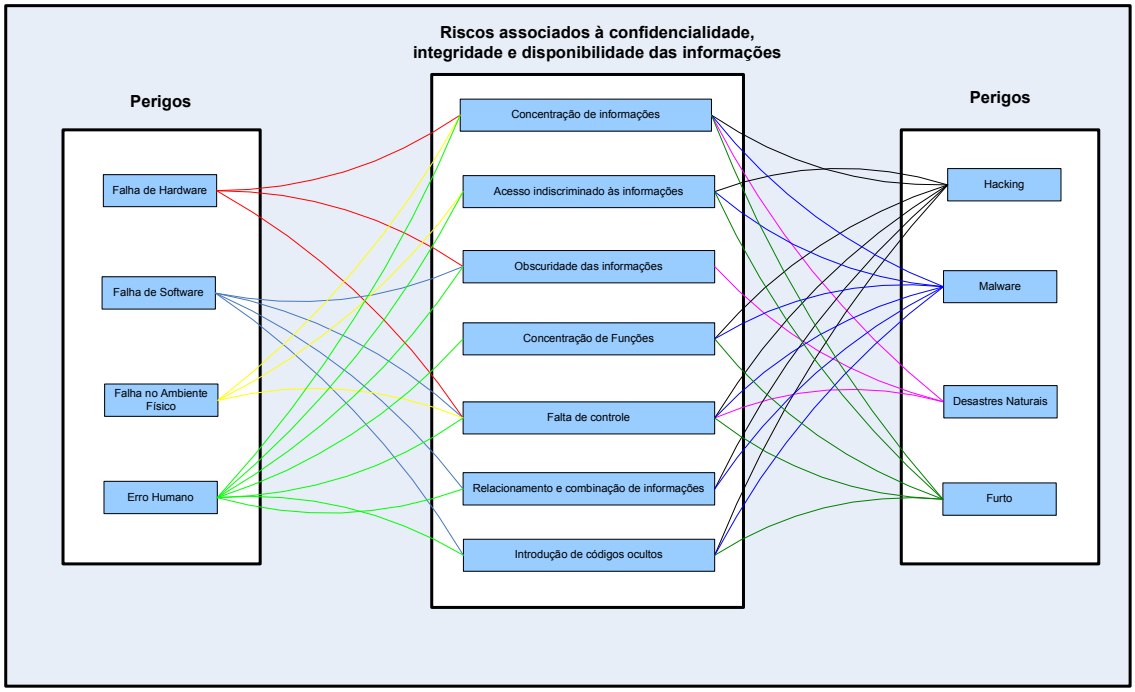


Figura 20 – Perigos x Riscos associados à confidencialidade, integridade e disponibilidade das informações.
Fonte: elaboração própria.

Para detalhar os fatores que podem influenciar na concretização do perigo é utilizado o Diagrama de Causa e Efeito, também conhecido como Diagrama de *Ishikawa*.

O Diagrama de *Ishikawa* foi elaborado a partir de estudos de seis macrofatores, também conhecidos como 6M (Meio Ambiente, Método, Mão de Obra, Monitoramento, Material e Máquina).

No Método de Avaliação de Risco os macrofatores foram ajustados para: Ambiente Externo, Processos de Apoio, Recursos Humanos, Segurança, Processos de Controle e Processos Operacionais conforme a seguir:

- Ambiente Externo (AE) – variáveis, características e circunstâncias externas, incontroláveis pelo gestor, vinculadas à atividade da Empresa sob risco.
- Processos de Apoio (PA) – principais processos de apoio da regional existentes ligados à atividade da Empresa sob risco.
- Recursos Humanos (RH) – tudo que envolve os colaboradores ligados direta ou indiretamente à atividade da Empresa sob risco.
- Processos de Controle (PC) – principais processos de controle da regional ligados à atividade da Empresa sob risco.

- Segurança (SE) – todos os meios, equipamentos, instrumentos e processos de segurança relacionados à atividade da Empresa sob risco.
- Processos Operacionais (PO) – principais processos operacionais e produtos inter-relacionados à atividade da Empresa sob risco.

A seguir, são apresentadas as análises individuais (Diagramas de *Ishikawa*) contendo os principais fatores que contribuem para ocorrência de cada um dos perigos. Nesta análise, contamos com a colaboração de empregados e colaboradores das centrais de serviços de sistemas e serviços de produção que compõem a Diretoria de Tecnologia da ECT. O método de coleta de dados é descrito no Anexo 5.

- Desastres Naturais

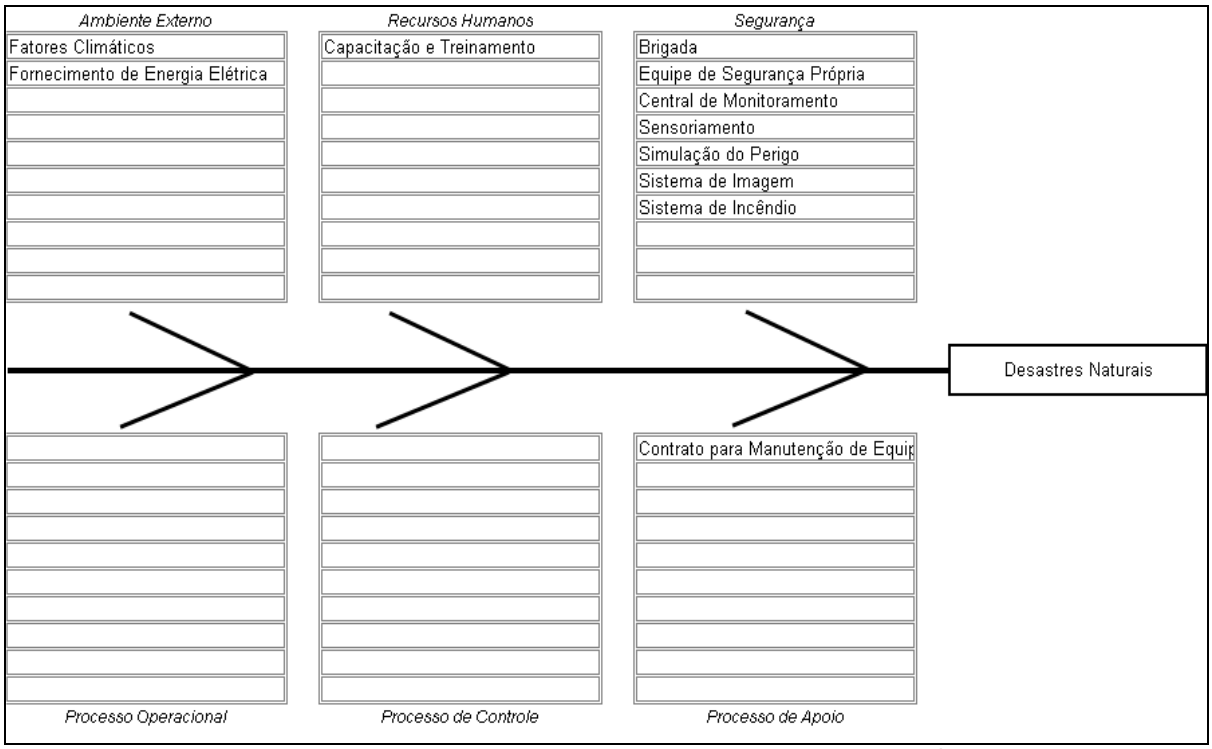


Figura 21 - Diagrama de *Ishikawa* - Desastres Naturais. Fonte: elaboração própria.

- Falhas no Ambiente Físico

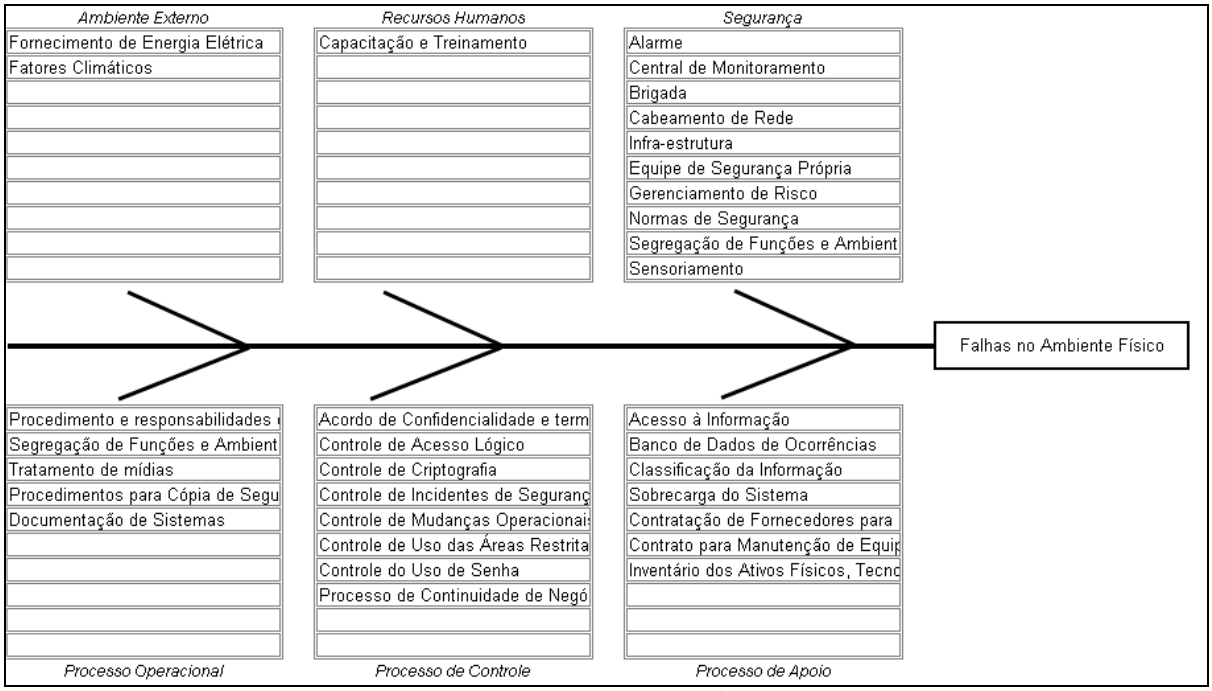


Figura 22 - Diagrama de *Ishikawa* - Falhas no Ambiente Físico. Fonte: elaboração própria.

- Furto

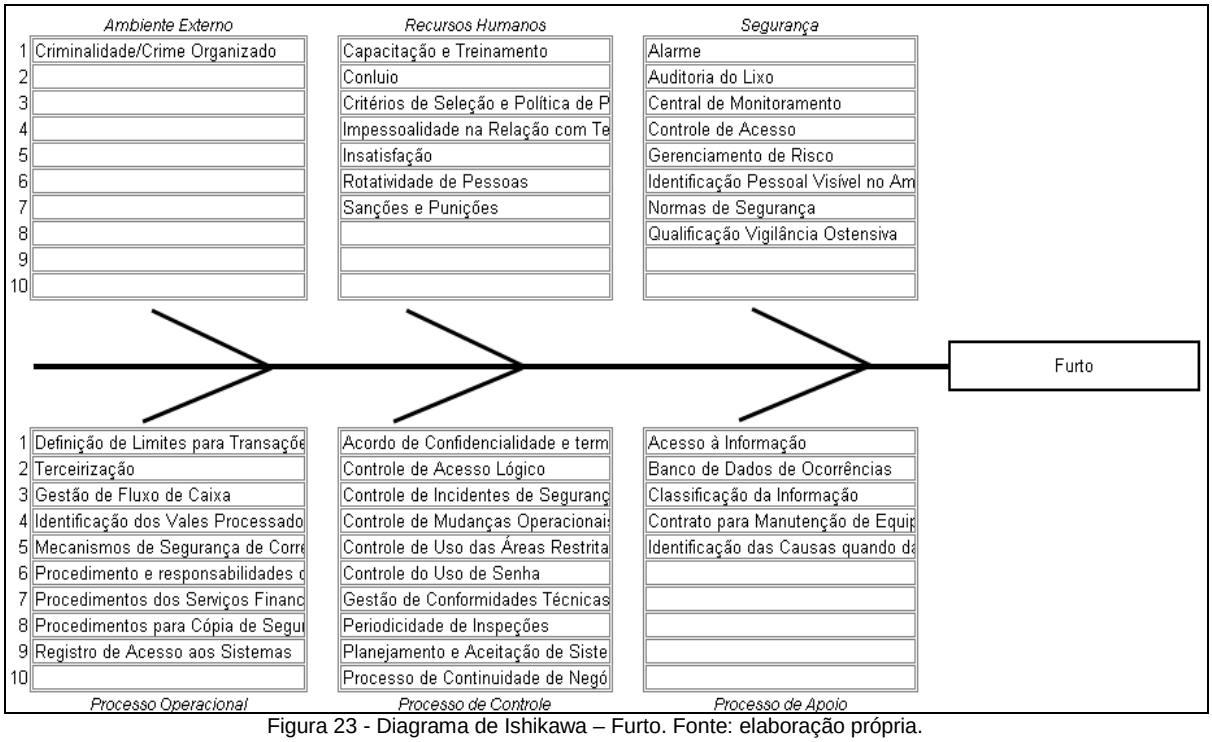


Figura 23 - Diagrama de Ishikawa – Furto. Fonte: elaboração própria.

- *Malware*

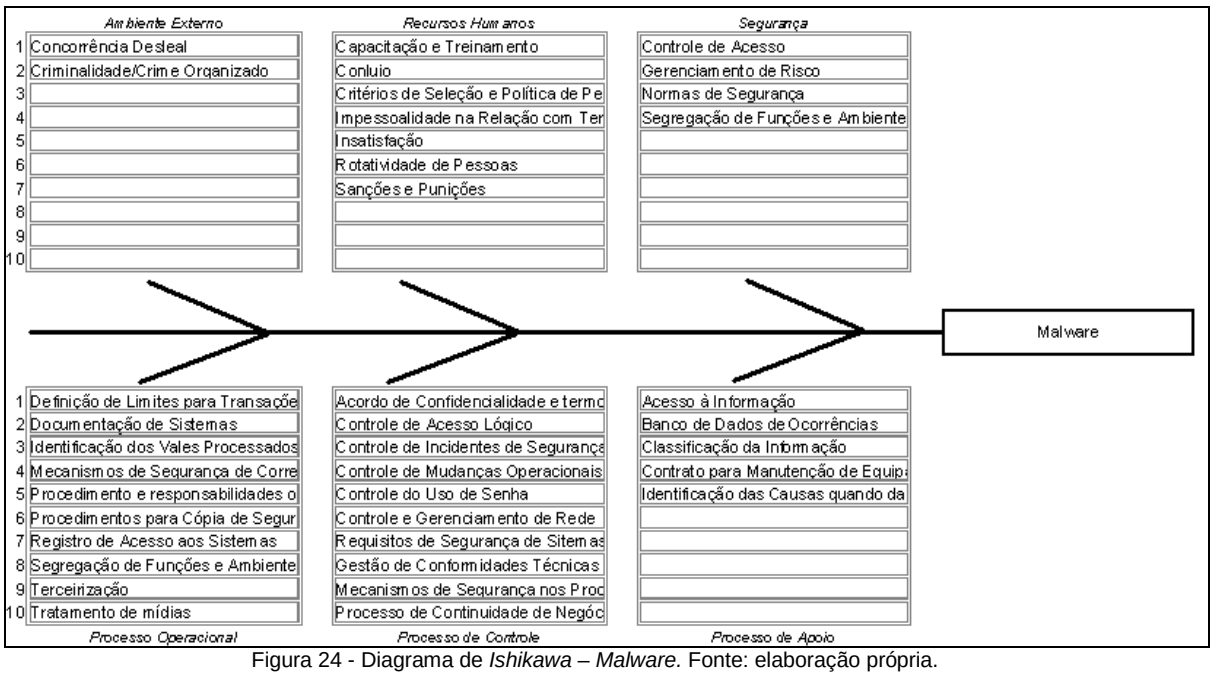


Figura 24 - Diagrama de *Ishikawa – Malware.* Fonte: elaboração própria.

- *Hacking*

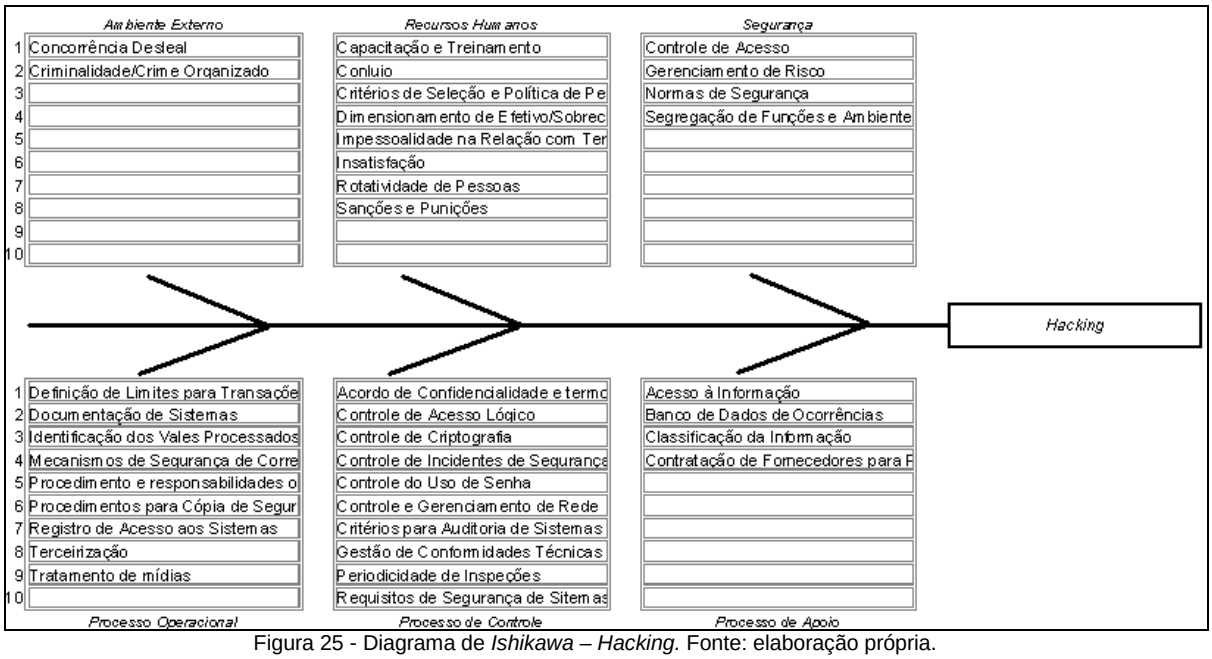


Figura 25 - Diagrama de *Ishikawa – Hacking.* Fonte: elaboração própria.

- Códigos Ocultos

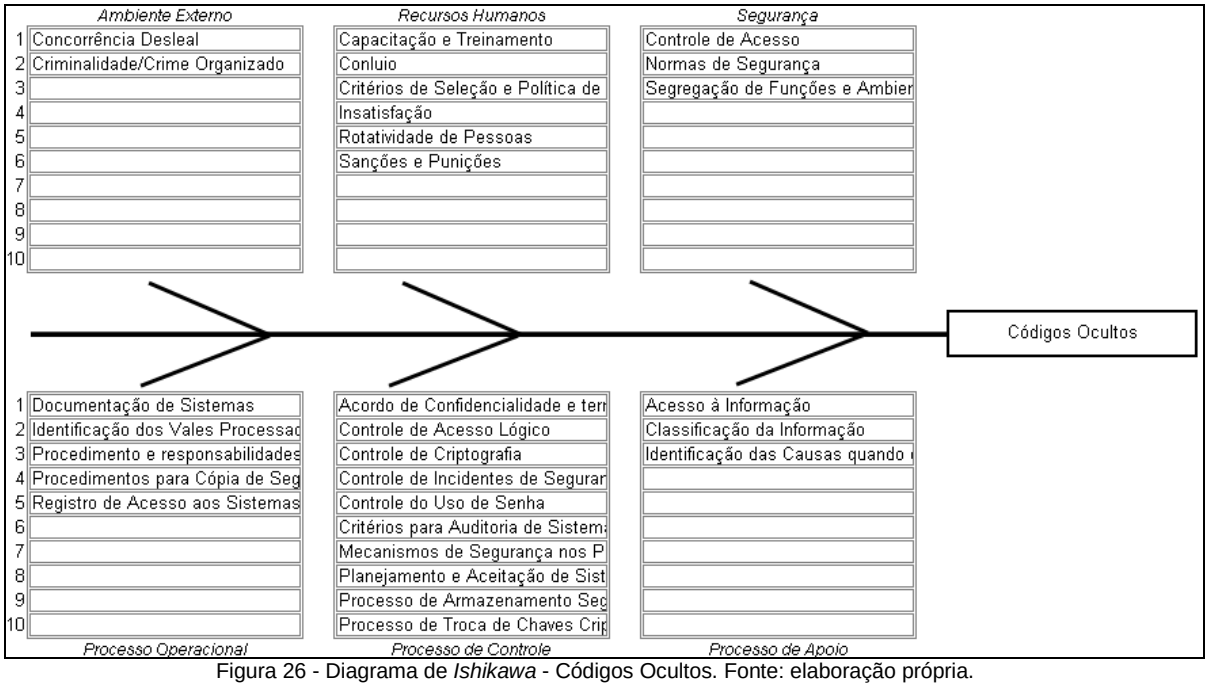


Figura 26 - Diagrama de *Ishikawa* - Códigos Ocultos. Fonte: elaboração própria.

- Falha de *Hardware*

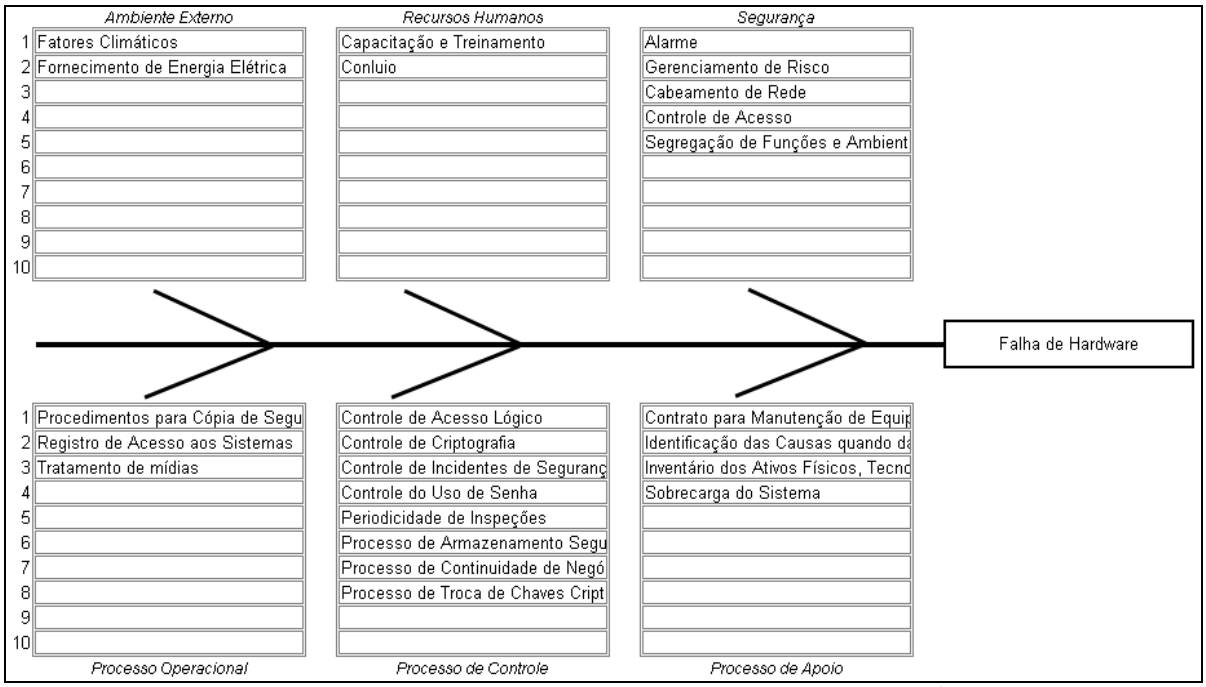


Figura 27 - Diagrama de *Ishikawa* - Falha de *Hardware.* Fonte: elaboração própria.

- Falha de *Software*

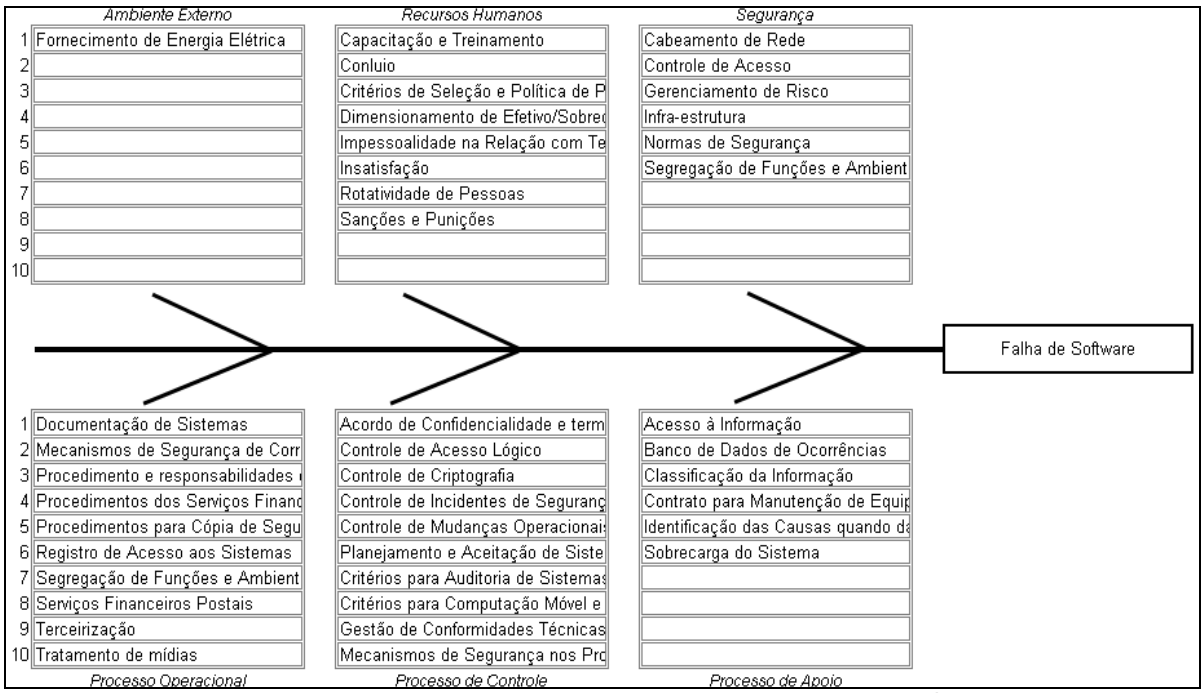


Figura 28 - Diagrama de *Ishikawa* - Falha de *Software.* Fonte: elaboração própria.

- Erro Humano

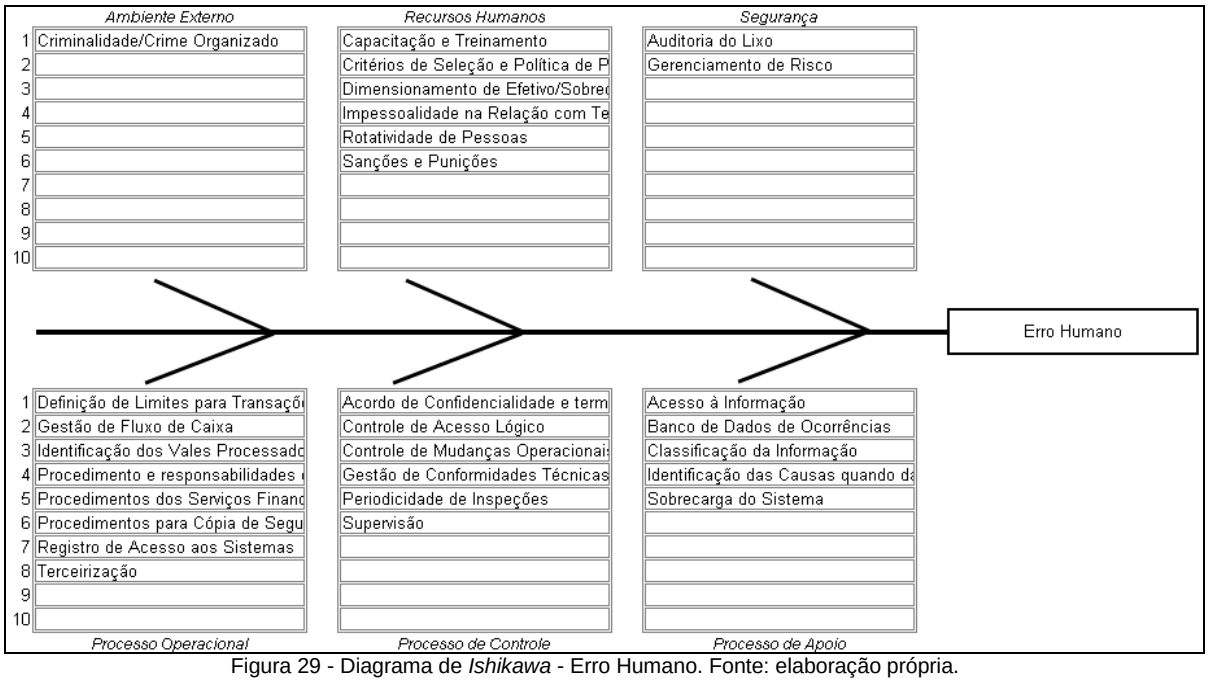


Figura 29 - Diagrama de *Ishikawa* - Erro Humano. Fonte: elaboração própria.

Após identificar os fatores que podem influenciar cada perigo, foi definido o grau de influência de cada macrofator. Conforme Tabela 1, o grau de

influência de cada macrofator estudado no Diagrama de *Ishikawa* recebe a seguinte ponderação:

Peso	Grau de Influência do Macrofator
1	Irrelevante ou quase nada
2	Pouco relevante
3	Medianamente relevante
4	Muito relevante
5	Extremamente relevante

Tabela 1 – Grau de Influência do Macrofator

A gradação final será o resultado da média aritmética simples de todos os valores estabelecidos aos macrofatores.

$$MFR = \frac{AE + PA + RH + PC + SE + PO}{6}$$

A segunda fase do Método Brasiliano consiste em determinar o grau de probabilidade de ocorrência de cada perigo. Para o cálculo do Grau de Probabilidade de ocorrência de cada perigo, utilizamos o Grau de Influência dos Macrofatores (MFR) e a Exposição ao Perigo (E) – freqüência com que o perigo costuma se manifestar num determinado intervalo de tempo dos perigos durante o último ano.

O padrão para estabelecer os pesos da Exposição ao Perigo obedece ao padrão:

Peso	Frequência de Ocorrência
1	Menos que trimestralmente
2	Ocorre trimestralmente
3	Ocorre mensalmente
4	Ocorre semanalmente
5	Ocorre diariamente

Tabela 2 – Exposição ao Perigo

O cálculo da Probabilidade de ocorrência do Perigo é o resultado do produto entre o Fator de Risco (MFR) e a Exposição ao Perigo (E). O escalonamento do nível de probabilidade é representado pela tabela de classificação a seguir:

Escala (FR x E)	Nível de probabilidade	Probabilidade
1,00 a 5,00	Baixa – Improvável	4,0% a 20,0%
5,01 a 10,00	Média – Ocasional	20,4% a 40,0%
10,01 a 15,00	Alta - Provável	40,4% a 60,0%
15,01 a 20,00	Muito Alta – Freqüente	60,4% a 80,0%
20,01 a 25,00	Elevada	80,4% a 100%

Tabela 3 – Probabilidade de ocorrência do perigo

A matriz a seguir nos mostra os graus de influência dos macrofatores definidos, a frequência de ocorrência e o grau de probabilidade de ocorrência do perigo.

	MATRIZ DE PROBABILIDADE E IMPACTO	Macrofator de Perigo							E	GP	Classificação - Grau Probabilidade
		AE	RH	SE	PO	PC	PA	MFR		MFR x E	
1	Desastres Naturais	1	1	1	1	1	1	1	1	1	BAIXA
2	Falhas no Ambiente Físico	3	4	2	5	3	3	3	1	3	BAIXA
3	Erro Humano	3	5	4	5	5	4	4	3	13	ALTA
4	Furto	4	3	4	5	3	5	4	1	4	BAIXA
5	Malware	5	5	5	5	5	5	5	3	15	ALTA
6	Hacking	5	5	5	5	5	5	5	1	5	BAIXA
7	Falha de Software	5	5	3	5	4	4	4	3	13	ALTA
8	Falha de Hardware	3	4	2	5	3	3	3	1	3	BAIXA
9											
10											
11											
12											
13											
14											
15											

Figura 30 - Matriz de Probabilidade e Impacto – Classificação da Probabilidade

A terceira fase do Método Brasiliano consiste em determinar o impacto[11] decorrente da ocorrência do perigo. O impacto é analisado em cinco aspectos, e para cada aspecto é atribuído um peso diferenciado em razão da relevância para a Empresa. Os aspectos analisados e seus respectivos pesos são:

a) Imagem – peso 2;
b) Financeiro – peso 5;
c) Legal – peso 2;
d) Operacional – peso 5;
e) Social – peso 3.

Onde:

[11] consequência maléfica que o perigo, se concretizado, poderá causar.

- **Imagem** – é a credibilidade ou percepção pública de confiança na ECT. Os pesos foram determinados, conforme o caráter de abrangência de abalo da imagem:

Peso	Escala	Abrangência – Abalo da Imagem
1	Individual	Somente a uma pessoa
2	Bairro	O bairro ou comunidade
3	Cidade	Uma cidade
4	Regional	A regional ECT ou estadual
5	Nacional	Nacional

Tabela 4 - Impacto à imagem

- **Legislação** – é a transgressão dos dispositivos legais a que está sujeita a ECT. Elas podem ser em decorrência de sanções por reguladores e indenizações por danos a terceiros, por má interpretação ou falhas nos pagamentos de tributos e por contratos omissos, mal redigidos ou sem devido amparo legal.

Peso	Escala	Abrangência – Bem Jurídico Atingido
1	Irrelevante	Não atinge nenhum bem jurídico na legislação vigente
3	Médio	Individual ou de uma pessoa
5	Superior	Da coletividade ou de grupos de pessoas

Tabela 5 - Impacto legal

- **Social** – configura os efeitos do perigo na relação entre as pessoas envolvidas no ciclo de vida da informação. Os pesos foram determinados, conforme o caráter de abrangência social:

Peso	Escala	Abrangência – Reflexo nas pessoas (força de trabalho)
1	Irrelevante	Não atinge ninguém
2	Pouco Importante	Atinge pessoas indiretamente
3	Médio	Atinge uma pessoa diretamente
4	Alto	Atinge mais de uma pessoa diretamente
5	Superior	Atinge toda unidade ou efetivo da unidade

Tabela 6 - Impacto social

- **Operacional** – configura a interrupção total ou parcial dos processos operacionais da ECT. Os pesos foram determinados, conforme o caráter de abrangência operacional:

Peso	Escala	Abrangência
1	Irrelevante	Não gera nenhuma alteração no processo produtivo
2	Pouco Importante	Gera pequenas alterações no processo produtivo
3	Médio	Gera grandes alterações no processo produtivo
4	Muito Importante	Gera parcial paralisação no processo produtivo
5	Superior	Gera a paralisação total do processo de uma unidade

Tabela 7 - Impacto operacional

O impacto é o resultado da média ponderada dos cinco aspectos analisados, considerando o peso e a ponderação atribuídos:

$$\text{Impacto} = \frac{(IMA \times 2) + (FIN \times 5) + (LEG \times 2) + (OPE \times 5) + (SOC \times 3)}{17 \text{ (soma dos pesos)}}$$

O impacto é classificado conforme tabela abaixo:

Grau de Impacto	Nível de Impacto
Até 1,51	Irrelevante
De 1,52 a 2,51	Leve
De 2,52 a 3,51	Moderado
De 3,52 a 4,51	Severo
Acima de 4,52	Catastrófico

Tabela 8 - Classificação do impacto

A matriz a seguir nos mostra o impacto dos perigos relatados nos aspectos: imagem, financeiro, legislação, operacional e social. O aspecto financeiro recebeu a ponderação mínima, visto que não foi possível levantar precisamente os valores das perdas ocasionadas pela ocorrência dos perigos.

	MATRIZ DE PROBABILIDADE E IMPACTO	Impacto							
		Imagem	Financeiro	Legislação	Operacional	Social	Nota	Impacto	Nível de Impacto
		2	Cálculo	2	5	3	17		
1	Desastres Naturais	5	1	3	4	4	53,0	3,12	MODERADO
2	Falhas no Ambiente Físico	5	1	3	4	4	53,0	3,12	MODERADO
3	Erro Humano	4	1	3	3	4	46,0	2,71	MODERADO
4	Furto	5	1	3	3	3	45,0	2,65	MODERADO
5	Malware	5	1	3	5	5	61,0	3,59	SEVERO
6	Hacking	5	1	3	5	5	61,0	3,59	SEVERO
7	Falha de Software	3	1	5	4	4	53,0	3,12	MODERADO
8	Falha de Hardware	5	1	3	4	4	53,0	3,12	MODERADO
9									
10									
11									
12									
13									
14									
15									

Figura 31 - Matriz de Probabilidade e Impacto – Nível de Impacto

A quarta e última fase do Método Brasiliano envolve a criação da matriz de vulnerabilidade a partir da relação entre o impacto e o grau de probabilidade dos perigos analisados. O gráfico abaixo apresenta a consolidação do grau de probabilidade e impacto dos perigos analisados e permite avaliar comparativamente os diversos riscos a que o ambiente está exposto a partir da interpretação em quatro quadrantes:

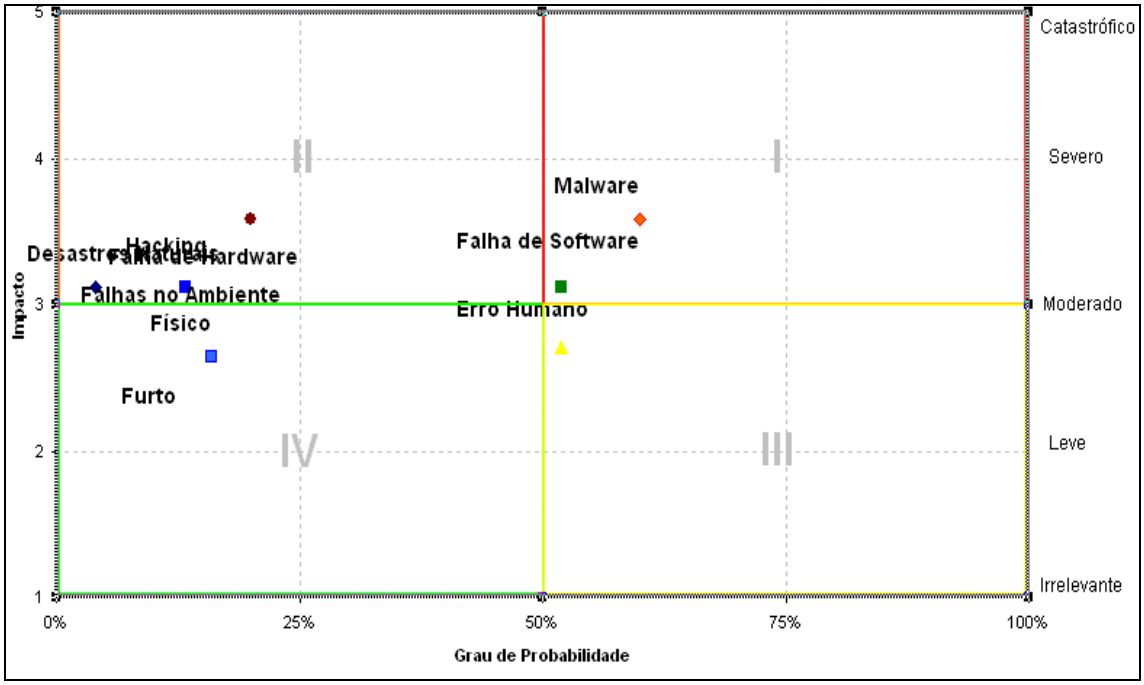


Figura 32 - Matriz Impacto X Probabilidade

15.6.1. Avaliação dos perigos analisados

15.6.1.1. Desastres naturais

Este perigo possui grau de probabilidade baixo e em caso de ocorrência pode resultar impactos de proporções moderadas para o ambiente analisado.

Grande parte dos equipamentos e sistemas que processam informações corporativas da ECT está instalada numa sala cofre localizada no edifício da Administração Central. Essas instalações estão preparadas contra inundações, fogo e alterações climáticas. Portanto, não há necessidade de mais investimentos para minimizar as vulnerabilidades que corroboram para a ocorrência desse perigo. Recomenda-se realizar revisões periódicas nas instalações físicas da sala cofre e nos processos de incidentes relacionados a esse perigo.

15.6.1.2. Falha no ambiente físico

Este perigo apresenta grau de probabilidade baixo e impacto moderado. Os principais equipamentos do parque computacional da ECT que processam e armazenam informações estão instalados fisicamente em ambiente isolado (sala cofre) que dispõe de vários mecanismos que garantem sua segurança e disponibilidade, tais como: controle de acesso físico, sistema de monitoramento de imagem, alarme, sensores e mecanismos de combate a incêndio e redundância de rede elétrica. Recomenda-se: revisar periodicamente a relação de pessoas com direito de acesso ao ambiente físico, incluindo os prestadores de serviços; revisar os demais processos de controle; realizar manutenção preventiva nos recursos de infraestrutura (fornecimento de energia, cabeamento, sistemas de monitoramento de imagem, sistemas de prevenção de incêndio).

15.6.1.3. Furto

Este perigo apresenta grau probabilidade baixo e impacto moderado. Alguns controles implementados no parque computacional da ECT – tais como: segregação de áreas, segregação de funções, sanções previstas no Manual de Pessoal, controle de acesso, sistema de monitoramento – corroboram para o baixo grau de risco envolvido

15.6.1.4. *Malware*

Este perigo apresenta grau de probabilidade alta e impacto severo. Dentre os perigos analisados, é o que representa maior risco para as informações corporativas da ECT. A ECT utiliza alguns meios de segurança para a prevenção contra este tipo de ataque, dentre os quais destacam-se: a utilização de sistemas de prevenção de intrusão (IPS), *firewalls*, soluções *anti-malwares*, além dos processos de conscientização dos usuários internos. Portanto, o risco associado a este perigo é aceitável e inerente a qualquer sistema disponível em ambiente computacional.

15.6.1.5. *Hacking*

Este perigo apresenta grau de probabilidade baixo e impacto severo. Da mesma forma como que o *malware*, a ECT utiliza meios de segurança necessários para a prevenção deste tipo de ataque. Constata-se que este perigo apresenta o grau de probabilidade menor que o *malware* devido à baixa incidência de tentativas de ataque bem sucedidas no ambiente computacional da ECT.

15.6.1.6. Falha de *Hardware*

Este perigo apresenta grau de probabilidade baixo e impacto moderado. Os principais equipamentos de *hardware* que processam informações corporativas estão instalados fisicamente em ambiente isolado (sala cofre) que dispõe de mecanismos de controle e contratos de manutenção que garantem sua integridade física. Para aumentar a disponibilidade das informações que trafegam por meio eletrônico na ECT, convém estudar a possibilidade de replicação dos principais equipamentos envolvidos no processamento de informações em outro Centro Corporativo de Dados, com infraestrutura similar à da sala do Edifício da Administração Central.

15.6.1.7. Falha de *Software*

Este perigo apresenta grau de probabilidade alto e impacto moderado. Para mitigar o risco inerente a esse perigo, convém: manter as documentações de sistemas atualizadas e disponíveis aos envolvidos; prover treinamentos de capacitação e reciclagem às pessoas envolvidas; garantir que as alterações no código do sistema sejam executadas e testadas no ambiente de testes antes de serem postas em produção; revisar periodicamente os processos de controle de acesso que garantam acesso somente a pessoas devidamente autorizadas e que essas executem suas funções com efetiva performance; prover aos usuários regras escritas contento seus direitos de acesso e responsabilidades a eles atribuídas.

15.6.1.8. Erro Humano

Este perigo apresenta grau de probabilidade alto e impacto moderado. Para mitigar o risco desse perigo as principais ações a serem tomadas estão relacionadas à capacitação, treinamento e conscientização dos envolvidos na solução. Adicionalmente, convém evitar o acúmulo de funções e atividades em um único colaborador - que implicam em sobrecarga de trabalho.

16. Conclusão

A informação é um ativo que, independente da forma em que se apresenta – impressa, falada, registrada no papel ou armazenada eletronicamente – deve ser protegida adequadamente.

A proteção da informação pode ser obtida a partir da implementação de políticas, processos, procedimentos, estruturas organizacionais, funções de *software* e *hardware*. Esses controles precisam ser definidos, implantados e monitorados regularmente a fim de melhorar os processos e garantir que os objetivos do negócio e de segurança da informação na organização sejam atendidos.

Constatou-se que existem pelo menos três fatores fundamentais a serem considerados para definir os requisitos de segurança da informação de forma eficaz e eficiente. O primeiro fator é composto pelo arcabouço legal e pelo arcabouço normativo. Este último tem por objetivo definir regras, critérios e registrar as melhores práticas para promover a uniformidade e a qualidade de processos organizacionais, produtos e serviços. Embora considerada incipiente, se comparada a legislações de países europeus ou dos Estados Unidos, a legislação brasileira dispõe de vários documentos que discorrem sobre segurança da informação, principalmente no âmbito da Administração Pública Federal.

O segundo fator é particular de cada organização e envolve os princípios, objetivos e os requisitos de negócio necessários ao processamento da informação e de suas atividades, além do fator humano, da cultura e do ambiente sociocultural.

O terceiro fator é obtido a partir da análise e gestão dos riscos a que estão suscetíveis a organização e seus ativos. Embora esta pesquisa tenha se limitado a estudar os riscos relacionados à segurança da informação, convém que sejam consideradas outras vertentes da Gestão de Riscos Corporativos para elaboração dos controles e requisitos de segurança da informação e de planejamento estratégico organizacional.

No âmbito da Administração Pública Federal e à luz da Instrução Normativa nº 01 do Gabinete de Segurança da Informação da Presidência da República, constatou-se que para tornar o processo de gestão de segurança da informação mais eficiente é fundamental instituir um comitê na estrutura organizacional de cada órgão com competência para propor, aplicar e coordenar as ações de Segurança da Informação.

Adicionalmente, convém que as entidades da Administração Pública Federal definam uma metodologia de gestão de segurança da informação baseada no processo de melhoria contínua. Nesta pesquisa, sugere-se que as entidades da

Administração Pública Federal estejam aderentes à metodologia proposta pelo Gabinete de Segurança da Informação da Presidência da República, por meio da Norma Complementar nº02/IN01/DSIC/GSIPR.

A implantação das ações de segurança na Administração Pública justifica-se pelo valor da informação para a eficiente prestação dos serviços públicos e no interesse do cidadão como beneficiário dos serviços prestados.

Quanto à aplicação dos conceitos de gestão de riscos à segurança da informação no âmbito da APF, esta pesquisa permite concluir que ao tratar a questão da segurança da informação pelo viés da gestão de riscos, o gestor consegue aproximar o assunto da estratégia de negócios e empregar melhor os recursos, pois conhecendo as ameaças, as vulnerabilidades a que estão sujeitas as informações e os impactos decorrentes do comprometimento de sua segurança, a tomada de decisão para proteger os dados corporativos torna-se melhor fundamentada e mais confiável.

Isso posto, confirma-se a hipótese desta pesquisa, onde, inicialmente, admitiu-se a proposição de que a Segurança da Informação é mais eficiente e eficaz quando adota a Gestão de Riscos.

Parte-se do pressuposto que as entidades que compõem a APF, assim como as entidades privadas, existem para gerar valor e enfrentam incertezas. Diante disso, um dos grandes desafios dos administradores públicos é determinar até que ponto tolerar essas incertezas, assim como estabelecer de que forma essas incertezas podem interferir nos processos de geração de valores às partes interessadas e no emprego dos recursos corporativos.

O emprego de metodologias de análise de riscos pode ser útil no desempenho dessas tarefas. Constatou-se que o Método Brasiliano é adequado para fundamentar um modelo sistêmico aplicável ao processo de análise de riscos em segurança da informação nas entidades da APF. Isso porque o Método Brasiliano é simples do ponto de vista de aplicação, suscetível a conciliação com a cultura de gestão de segurança em uso nas organizações públicas e coerente com as práticas de qualidade e gestão adotadas em órgãos públicos brasileiros.

A partir da aplicação do método, verificamos que diversos fatores podem corroborar para a ocorrência dos perigos que colocam em risco a confidencialidade, integridade e disponibilidade das informações no ambiente corporativo de uma empresa pública. Nesta pesquisa foram estudadas a origem/causa, o impacto e a probabilidade dos seguintes perigos: desastres naturais, falhas no ambiente físico, furto, *malware*, *hacking*, códigos ocultos, falha de *hardware*, falha de *software* e erro humano.

Vale destacar que os perigos considerados em uma análise de riscos variam de acordo com a natureza do negócio e a percepção dos gestores e usuários da informação de uma organização. Por ser um processo contínuo, a análise riscos pode considerar diferentes perigos de acordo com momento vivido e o ambiente em que está inserida a organização.

Observamos que o grau de tolerância ao risco varia de organização para organização. O impacto e a probabilidade de ocorrência do perigo podem justificar as ações dos gestores para mitigar o risco.

Por se tratar de uma pesquisa estritamente acadêmica, uma proposta de trabalho futuro é a efetiva implantação dos comitês de segurança da informação e dos comitês de gestão de riscos corporativos nas estruturas organizacionais dos órgãos da APF. Além disso, é importante que esses órgãos realizem um planejamento estratégico organizacional para que os planos de trabalho desses comitês estejam alinhados.

Outra proposta de trabalho é o estudo e definição de um modelo de classificação da informação aplicável aos órgãos da Administração Pública Federal. Na verdade, a classificação da informação deve ser uma atividade que precede as questões relacionadas à segurança da informação, pois define os ativos de informação que demandam mais recursos para sua proteção.

Sugere-se ainda que seja elaborado um estudo a fim de propor a definição e implementação de um sistema de medição que permita avaliar o desempenho e a maturidade da gestão da segurança da informação nas organizações públicas.

Por fim, a Gestão de Segurança da Informação e a Gestão Riscos são áreas desafiadoras que assumem papéis de extrema importância para as organizações contemporâneas que produzem, consomem e trocam informações em um ambiente cada vez mais competitivo, globalizado e informatizado. Porém, embora a utilização de recursos de TI no processamento de informações seja um assunto em evidência, há que se considerar as questões relacionadas aos processos e principalmente às pessoas que os operam.

Referências Bibliográficas

AGNER, L.; SILVA, F. L. C. M. **Uma introdução à arquitetura da informação: conceitos e usabilidade**. In: 2º Congresso Internacional de Pesquisa em Design. Artigo. Rio de Janeiro, 2003.

ALBERCH FUGUERAS, Ramón; CRUZ MUNDET, José Ramón. ***Arquivese*! *Los documentos Del poder: El poder de los documentos***. Madrid: Alianza Editotial, 1999, p.167.

ALBERTS, C.; DOROFEE, A.; ***Managing Information Security Risks***. United States: Addison- Wesley, 2002; p.10-25; 81-113.

ALVARENGA NETO, Rivadária Correa Drummond de; BARBOSA, Ricardo Rodrigues; PEREIRA, Heitor José. **Gestão do conhecimento ou gestão de organizações da era do conhecimento? Um ensaio Teórico-prático a partir de intervenções na realidade brasileira.** Perspectivas em Ciência da Informação, Belo Horizonte, v.12, n.1, p. 5-24, jan./abr. 2007.

ALVES, Ivone *et al*. **Dicionário de terminologia arquivística**. Lisboa: Instituto da Biblioteca Nacional e do Livro, 1993, p 30 e 57 (*apud* SILVA, Armando Malheiro da; RIBEIRO, Fernanda; RAMOS, Júlio; REAL, Manuel) *Apud* ROBREDO, Jaime. **Da ciência da informação revisitada: aos sistemas humanos de informação**. Jaime Robredo. Brasília: Thesaurus; SSRR Informações, 2003.

ANSOFF, H. Igor. **A nova estratégia empresarial**. São Paulo: Atlas, 1990.

ARAÚJO, Eliany Alvarenga de. A construção social da informação: práticas informacionais no contexto de Organizações não governamentais/ONGs brasileiras. **Ciência da Informação**, Brasília, v.29, n.2, p. 155-167, mai./ago. 1999.

AS/NZS 4360:2004 ***Australian Standard for Risk Management***, 2004.

Associação Brasileira de Normas Técnicas – **ABNT ISO/IEC Guia 73:2005 – Gestão de riscos - Vocabulário - Recomendações para uso em normas**. Rio de Janeiro: ABNT, 2005.

Associação Brasileira de Normas Técnicas – **ABNT NBR ISO/I 17799:2005 –**

Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão de segurança da informação. Rio de Janeiro: ABNT, 2005.

Associação Brasileira de Normas Técnicas – **ABNT NBR ISO/I 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de segurança da informação – Requisitos**. Rio de Janeiro: ABNT, 2006 40p.

Associação Brasileira de Normas Técnicas – **ABNT NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Gestão de riscos de segurança da informação. Associação Brasileira de Normas Técnicas**. Rio de Janeiro ABNT, 2008 55p.

BARRETO, A. de A. A eficiência técnica e econômica e a viabilidade de produtos e serviços de informação. **Ciência da Informação**, Brasília, v. 25. nº 3, p. 405-414, set./dez. 1996.

BEAL, Adriana. **Gestão estratégica da informação: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações**. São Paulo: Atlas, 2004.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações** – 1ª edição – 2ª reimpressão – São Paulo: Atlas, 2008.

BELKIN, N. J.; ROBERTSON, S. E. *Science and the phenomenon of information.* ***Journal of the American Society form Information Science***, v. 27, no 4, 1976.

BELLOTTO, Heloísa Liberalli. **Arquivos permanentes: tratamento documental** – 2ª edição revisada e ampliada. Rio de Janeiro: Editora FGV, 2004. p. 112-124.

BERETA, Sergio. *Unleashing the integration potencial of ERP system.* **Bussiness Process Management Journal**, Bradford, v. 8, n.3, p. 259, 2002.

BERSTEIN, P. L. **Desafio aos deuses: a fascinante história do risco**. São Paulo: Elsevier/Campus, 1997.

BETHLEM, Agrícola. Os conceitos de política e estratégia. **Revista de Administração de Empresas**. Rio de Janeiro, v, 21, nº 1, p. 7-15, jan./mar. 1981.

BEUREN, Ilse Maria. **Gerenciamento da informação: um recurso estratégico no processo de gestão empresarial**. São Paulo: Atlas, 2000. p.41-58.

BOISOT, Max**.** ***Knowledge Assets: Securing Competitive Advantage in the Information Economy***. Oxford; New York: Oxford Universit Press, 1998.

BORKO, H. ***Information science: what is this?*** American Documentation, v. 19, 3-5, 1968.

BRASIL, Constituição (1988), **Constituição da República Federativa do Brasil. Brasília, 2004**. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao.htm>. Acesso em: maio 2008.

BRASIL, Lei nº 8.159, de 08 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial da República Federativa do Brasil**. Brasília, 09 jan. 1991. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8159.htm>. Acesso em: maio 2008.

BRASIL, Lei nº 9.883, de 07 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. **Diário Oficial da República Federativa do Brasil**. Brasília, 08 dez. 1999. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L9883.htm>. Acesso em: maio 2008.

BRASIL, Lei nº 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. **Diário Oficial da República Federativa do Brasil**. Brasília, 17 jul. 2000. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L9983.htm>. Acesso em: maio 2008.

BRASIL, 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. **Diário Oficial da República Federativa do Brasil**. Brasília, 14 jun. 2000. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: maio 2008.

BRASIL, Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. **Diário Oficial da República Federativa do Brasil** Brasília, 11 jan. 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm >. Acesso em: maio 2008.

BRASIL, Decreto nº 4.553, 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. **Diário Oficial da República Federativa do Brasil**. Brasília, 30 dez. 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2002/D4553Compilado.htm>. Acesso em: maio 2008.

BRASIL, Decreto nº 5.110, de 18 de junho de 2004. Acresce inciso ao art. 7º do 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. **Diário Oficial da República Federativa do Brasil**. Brasília, 21 jun 2004. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Decreto/D5110.htm>. Acesso em: maio 2008.

BRASIL, Decreto nº 5.495, de 20 de junho de 2005. Acresce incisos ao art. 7o do 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. **Diário Oficial da República Federativa do Brasil**. Brasília, 21 jun. 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5495.htm>. Acesso em: maio 2008.

BRAITHWAITE, T.; ***Securing E-Business Systems***; John Wiley and Sons, 2002; ISBN 0-471-07298-2; p. 109-145.

BRASILIANO, Antônio Celso Ribeiro. Matriciamento de Riscos. **Revista Eletrônica Brasiliano & Associados**, São Paulo, nº 20, p. 34-38, 2005. Disponível em <http://www.brasiliano.com.br>. Acesso em: junho 2009.

BRASILIANO, **Antônio Celso Ribeiro. Análise de Risco (Método Brasiliano)**. 2008. Artigo Técnico. Disponível em: <www.brasiliano.com.br>. Acesso em: maio 2009.

BROOKES, B.C. *The foundations of informations of information science*. ***Journal of Information Science***, v.2, p. 209-221, 1980.

BRYMAN, Alan. ***Quantity and Quality in social Research***. Canadá: Routledge, 1996.

BS 7799-2:2002, ***Information Security Management – Part 2: Specification for Information Security Management System***. BSI, 2001.

CAMPBELL, R.P.; SANDS, G.A. **A modular approach to computer security risk management**. Artigo. In: AFIPS National Computer Conference. 1979. p. 293-303.

CAMPOS, André L. N. **Sistemas de segurança da informação: controlando os riscos**. Florianópolis: Visual Books, 2006. 180p.

CÂNDIDO, Carlos Aparecido; VALENTIM, Marta Lígia Pomim; CONTANI, Miguel Luiz. Gestão Estratégica da Informação: semiótica aplicada ao processo de tomada de decisão. **Ciência da Informação**, Brasília, vol. 6, n. 3, 2005.

CAPURRO, R.; HJØRLAND, B. ***The concept of information***. In. Annual Review of Information Science and Technology, v. 37, p. 343-411, 2003.
Disponível em: <http://www.capurro.de/infoconcept.html>. Acessado em: dez/2008.

CARR, Nicholas G. **TI já não importa**. Harvard Business Review. Harvard: maio/2003.

CARUSO, C. A. A. & STEFFEN, F.D**. Segurança em informática e de informações**. 2ª edição. Revisada e ampliada. São Paulo: Editora SENAC. São Paulo, 1999. Capítulo 2. p. 35-47.

CARVALHO, Gilda Maria Rocha de. **Informação e conhecimento: uma abordagem organizacional.** Rio de Janeiro: Qualitymark, 2001, 152p.

CHAUMIER, J. **Systemes marche et tecnologies D' information**. Paris: Editora Entreprise Moderne d' Édition, 1986. *Apud* MORESI, Eduardo Amadeu Dutra. **Gestão da Informação e do conhecimento.** In: TARAPANOFF, Kira. **Inteligência organizacional e competitiva**. Brasília: Editora Universidade de Brasília, p. 111-141, 2001

CHECKLAND, Peter. ***Systems thinking, systems pratice***. Chichester: John Wiley & Sons, 1999.

CHOO, Chun Wei. **A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões**. Tradução: Eliana Rocha. São Paulo: Editora SENAC São Paulo, 2003.

CICCO, Francesco M. G. A. F de. **O gerenciamento dos riscos empresariais nos anos 90**. Revista do IRB (Instituto de resseguros do Brasil), Rio de Janeiro, ano 51, n. 254, p. 25 e 26, out./dez. 1990.

CRONIN, Blaise. **Esquemas conceituais e estratégicos para a gerência da informação**. Revista da Escola de Biblioteconomia da UFMG, v. 19, n. 2, p. 195-220, set. 1990.

COBIT 4.1., ***Control Objectives for Information and Related Technology Institute****,* 2007.

COSO, Committee of Sponsoring Organizations of the Treadway Commission. ***Enterprise Risk Management – Integrated Framework: Executive Summary and Framework and Enterprise Risk Management – Integrated Framework: Application Techniques***, vol. 2. New Jersey: COSO, set. 2004.

DAVENPORT, Thomas H. ***Process inovation***. Boston: Harvard Business School Press, 1993.

DAVENPORT, Thomas H. **Ecologia da informação: por que só a tecnologia não basta para o sucesso na era da informação**. Tradução: Bernadette Siqueira Abrão. São Paulo: Futura, 1998.

DE SORDI, José Osvaldo. **Gestão por processos: uma abordagem da moderna administração**. São Paulo: Saraiva, 2005. Capítulo 2. p. 17-27.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books do Brasil, 2000. p.39-83.

Dictionnaire encyclopédique de l'information et de La documentation. 2 ème édition. Paris: Nathan, 2001, p.297. URL: HTTP://www.natahn.u.com. ISBN:2-09-191252-2. *Apud* ROBREDO, Jaime. **Da ciência da informação revisitada: aos sistemas humanos de informação**. Jaime Robredo. Brasília: Thesaurus; SSRR Informações, 2003.

DRUCKER, Peter. **Fator Humano e Desempenho**. São Paulo: Pioneira,1991.

ECT, Empresa Brasileira de Correios e Telégrafos. **Política de Segurança da Informação da ECT**, 2001.

ECT, Empresa Brasileira de Correios e Telégrafos. **Conheça os Correios**. Disponível em: <http://www.correios.com.br/institucional/conheca_correios/conheca.cfm>. Acessado em: junho 2007.

Ernest & Young. **O sucesso em um mundo globalizado: Seu caminho está seguro? - Pesquisa Global sobre Segurança da Informação 2006**. Disponível em www.ey.com.br. Acessado em: outubro 2008.

FELDMAN, Jacob. **Qual informação é útil?**. 2005. Revista TI Master - Artigo. Disponível em:
http://www.timaster.com.br/revista/artigos/main_artigo.asp?codigo=1004
Acessado em: abril 2009.

FERMA, Federation of European Risk Managemente Associations. **Norma Européia de Gestão de Riscos**. AIRMIC, ALARM, IRM: 2002, translation copyright FERMA: 2003.

FERREIRA, Sueli Mara Soares Pinto. Novos Paradigmas e novos usuários de informação. **Ciência da Informação**, vol. 25, nº. 2, 1995.

FONTES, Edison Luiz Gonçalves. **Vivendo a segurança da informação: orientações práticas para as organizações**. 1ª Edição. São Paulo: Sicurezza: Brasiliano e Associados, p. 21-39, 2000.

GIL, Antônio Carlos: **Como Elaborar Projetos de Pesquisa**. São Paulo: Atlas, 1991.

GODOY, Arilda S. **Introdução à pesquisa qualitativa e suas possibilidades**. Revista de Administração de Empresas, v. 35, n2, p. 57-63, Mar./abr. 1995.

GOULART, Silvana. **Patrimônio documental e história Institucional**. São Paulo: Associação de Arquivistas de São Paulo. 2002.

Gabinete de Segurança Institucional da Presidência da República – GSI. **Metodologia para Gestão de Segurança da Informação pra a Administração Pública Federal – Relatório Final**. Maio/2006. Disponível em: http://www.presidencia.gov.br/estrutura_presidencia/gsi/publicacoes/ Acessado em: abr/2007.

GUAN, B-C. et al. ***Evaluation of information security related risks of an organization: the application of the multi-criteria decision-making method***. In: Marciano, João Luiz Pereira. **Segurança da Informação – uma abordagem social**. Brasília: CID/FACE – UnB, 2006.

HAMMER, Michael; CHAMPY, James. ***Reengineering the corporation***. London: Nicholas Breadley Publishing, 1997.

Harrod's Librarian Glossary of Terms Used in Librarianship, Documentation and the Book Crafts and Reference Book. 6th edition. Aldershot: Gower, 1989, p.281 *Apud* ROBREDO, Jaime. **Da ciência da informação revisitada: aos sistemas humanos de informação**. Jaime Robredo. – Brasília: Thesaurus; SSRR Informações, 2003.

HARRINGTON, James. ***Business process improvement***. New York: McGraw-Hill, 1991.

HAYES, Robert M. ***Information Science Education***. In: *ALA World Encyclopedia of Library and Information Sciences*. 2nd edition. Chicago: American Library Association, p. 358-360, 1986.

HILGENBERG, Alexandre Bento. **Necessidade de uma política de proteção à informação.** Universidade do Legislativo Brasileiro e Universidade Federal do Mato Grosso do Sul. Dissertação (Pós Graduação). Brasília, 2005.

ISO/IEC 13335-1:2004, ***Information technology – Security techniques – Management of information and mommunications technology security – Part 1: Concepts ond models for information and commuications technology security management***, 2004.

ISO 17799, International Organization for Standardization. ***Code of practice for information security management***, 2007.

ISO 27001, ***International Organization for Standardization. Information Security Management Systems – Requirements*****,** 2005.

ISO Guide 73, ***Risk management - Vocabulary - Guidelines for use in standards***, 2002.

ITSEC (June 1991). ***Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harnonised Criteria. Documente COM (90) 314, Version 1.2*****.** Commission of the European Communities. Retrieved on 2006-06-02.

ITIL. Office of Government. ***Information Technology Infrastructure Library Commerce****,* 2007.

LE COADIC, Yves-Francois. **A Ciência da Informação**. Brasília: Briquet de Lemos Livros, 1996, p.4. ISBN: 85-85637-08-0 (tradução do original francês La science de l'information. Paris: PUF, 1994 – Collection Que sais-je?).

LE COADIC, Y-F. **A Ciência da Informação**. 2ª. ed. Tradução de Maria Yêda F. S. de Figueiras Gomes. Brasília: Briquet de Lemos Livros, 124 p, 2004.

LESCA, Humbert; ALMEIDA, Fernando C. De. **Administração estratégica da informação**. Revista de Administração - RAUSP. São Paulo, v.29, n.03, p.66-75, jul./set., 1994.

LOMBARDO, A. ***Une table ronde utile à l'histoire***. Paris: Conseil International des Archives, 1958. *apud* BELLOTTO, Heloísa Liberalli. **Arquivos permanentes: tratamento documental** – 2ª edição revisada e ampliada – Rio de janeiro: Editora FGV, p. 112-124, 2004.

LYOTARD, J. F. **O que é pós-moderno**. 3ª edição. Rio de Janeiro: J. Olympio, 1990.

LYRA, Mauricio Rocha. **Segurança e Auditoria em Segurança da Informação**. Rio de Janeiro: Ed. Ciência Moderna Ltda, 2008.

MANDARINI, Marcos. **Segurança corporativa estratégica: fundamentos**. Barueri, SP: Manole, p. 293-315, 2005..

MARIJUAN, Pedro C. **Introduction**. In: ***Proceedings of the First Conference on the Foudations of Information Science: From Computers and Quantum Physics to Cell, Nervous Systems, and Societies***. July 11-15, 1994. Madrid. URL: HTTP://fis.iguw.tuwien.ac.at/index1.html. *Apud* ROBREDO, Jaime. **Da ciência da informação revisitada: aos sistemas humanos de informação**. Jaime Robredo. – Brasília: Thesaurus; SSRR Informações, 2003.

MENESES, Ulpiano T. Bezerra de. **A crise da memória, história e documento: reflexões para um tempo de transformações**. In: SILVA, Zélia Lopes da. Arquivos, patrimônio e memória: trajetória e perspectivas. São Paulo: Editora UNESP / FAPESP, p.11-29, 1999.

MCGARRY, Kevin. **O contexto dinâmico da informação: uma análise introdutória**. Tradução de Helena Vilar de Lemos. Brasília, DF: Briquet de Lemos/Livros, 1999.

MCGEE, James; PRUSAK, Laurence. **Gerenciamento estratégico da informação: aumente a competitividade e a eficiência de sua empresa utilizando a informação como ferramenta estratégica**. Tradução de Astrid Beatriz de Figueiredo. Rio de Janeiro: Campus, 1994.

MINTZBERG, Henry, QUINN, James Brian. ***The stragy process: concepts and contexts.*** Engle Wood Cliffs, New Jersey: Prentice Hall International, p. 12-19, 1992.

MORESI, Eduardo Amadeu Dutra. **Gestão da Informação e do conhecimento.** In: TARAPANOFF, Kira. **Inteligência organizacional e competitiva**. Brasília: Editora Universidade de Brasília, p. 111-141, 2001

NATIONAL INFORMATION ASSURANCE PARTNERSHIP. ***Common Criteria For Information Technology Security Evaluation – v.2.2.: Part 1 – Introduction and general model***. Washington, 2006.
Disponível em: <http://www.commoncriteriaportal.org/thecc.html>. Acesso em: abril.2009.

NETO, C.; MARTINS, J. B.; CÔRTE, K. & SILVA, L. F. C. P da. **Os Pilares da Segurança da Informação**. Set/2008. Programa de Pós-Graduação em Ciência da Informação – PPGCInf. Disciplina: Fundamentos da Ciência da Informação.
Disponível em: < http://aprender.unb.br>. Acesso em: dezembro 2008.

OLIVEIRA, Wilson José de. **Segurança da Informação – Técnicas e soluções**. Florianópolis: Editora Visual Books, maio 2001.

PRAHALAD, C.K & G. HAMEL. ***The Core Competence of the Organizations***, Harvard Bussines Review, p. 118-125, 1990.

PORTER, Michael. ***What is strategy?*** Harvard Business Review, nov./dez. 1996.

RAMOS, Anderson. ***Security Officer*** **– 1. Guia Official para Formação de Gestores em Segurança da Informação**. Porto Alegre: Módulo Security Solutions, 2006.

RIEGER, Morris. ***Procedes moderns de disposition ET dévaluation dês dossiers***. Rusiba, v. 1, n.3, p. 209-219. Jul./sept. 1979 . *apud* BELLOTTO, Heloísa Liberalli. Arquivos permanentes: tratamento documental – 2ª edição revisada e ampliada – Rio de janeiro: Editora FGV, p. 112-124, 2004.

ROBERTS, Joanne. ***The Drive to Codify: Implications for the Knowledge – Based Economy***. In: Proceedings of the 8th International Joseph A. Schumpeter Society Conference, 28th June-1st July 2000, University of Manchester: UK

ROBREDO, Jaime. **Da ciência da informação revisitada: aos sistemas humanos de informação**. Brasília: Thesaurus; SSRR Informações, 2003.

SALLES JUNIOR, Carlos Alberti Corrêa et al. **Gerenciamento de riscos em projetos**. Rio de Janeiro: Editora FGV, 160p, 2006.

SÊMOLA, Marcos. **Gestão de segurança da informação: visão executiva da segurança da informação: aplicada ao *Security Officer***. Rio de Janeiro: Campus, p. 43-73, 2003.

SÊMOLA, Marcos. Ge**s**tão **da Segurança da Informação**. In STAREC, Cláudio; GOMES, Elisabeth; BEZERRA, Jorge. **Gestão estratégica da informação e inteligência competitiva**. São Paulo: Saraiva, p. 285-305, 2005.

SIANES, Marta. **Compartilhar ou proteger conhecimentos? Grande desafio no comportamento informacional das organizações**. In STAREC, Cláudio; GOMES, Elisabeth; BEZERRA, Jorge. **Gestão estratégica da informação e inteligência competitiva**. São Paulo: Saraiva, p. 259, 2005.

SILVA, Adailton. **Segurança da Informação – Análise e Avaliação de Riscos**. Centro de Pesquisa, Desenvolvimento e Educação Continuada da Unicamp, dezembro/2003.

SILVA, Adailton. OCTAVE – **Como Gerenciar Riscos em Segurança da Informação**. Revista Economia & Tecnologia, vol. 7, nº 4, julho/agosto 2004.

SILVA, Janete Fernandes; FERREIRA, Marta Araújo Tavares; BORGES, Mônica Erichsen Nassif. **Análise metodológica dos estudos de necessidades de informação sobre setores industriais brasileiros: proposições**. Revista Ciência da Informação. Vol.31 nº 2. Brasília Maio/Agosto 2002.

SIMONS, Robert. ***Levels of control: how managers use innovative control systems to drive strategic renewal***. Boston, Massachusetts: Havard Business School Press, 1994, p.154.

SOBREIRA, Isabela Figueiredo. **A disseminação da informação na avaliação institucional e seus reflexos na cultura organizacional da UFMG**. 1999. Dissertação (Mestrado) - UFMG, Belo Horizonte, 1999.

STAIR, Ralph M. **Princípios de Sistemas de Informação – Uma Abordagem Gerencial**. Rio de Janeiro: Editora LTC, 1998.

STRAUSS, Anselm; CORBIN, Juliet. ***Basics of qualitative research – Techniques and procedures for developing grounded*** **theory**. 2ª Ed. Califórnia: SAGE *publications*, 1998.

TARAPANOFF, Kira. **Referencial Teórico: introdução**. In: TARAPANOFF, Kira. **Inteligência organizacional e competitiva**. Brasília: Editora Universidade de Brasília, p. 33-46, 2001.

THIOLLENT, Michel. **Metodologia da Pesquisa- ação**. São Paulo: Cortez,1996.

TOMANIK, Eduardo Augusto. **O olhar no espelho "conversas" sobre a pesquisa em Ciências Sociais**. 2ª edição revista. Maringá: Eduem, 2004.

WETHERBE, James C. **Análise de sistema para sistemas de informação por computador**. 3ª Ed. Rio de Janeiro: Campus, 1987

ZAPATER, Márcio; SUZUKI, Rodrigo. **Segurança da Informação – Um diferencial na competitividade das corporações**. Rio de Janeiro: Promon Businnes & Technology Review, 2005.

Anexos

Anexo 1 – Diretrizes da Política de Segurança da Informação da ECT

a. proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;
b. assegurar que os recursos de informação colocados à disposição dos empregados e prestadores de serviços sejam utilizados apenas para finalidades aprovadas pela ECT;
c. garantir que os sistemas e informações sob a responsabilidade dos empregados e prestadores de serviços estejam adequadamente protegidos;
d. garantir a continuidade do processamento das informações criticas de negócio;
e. selecionar os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
f. comunicar imediatamente ao seu chefe imediato ou ao gestor responsável pela sua área de trabalho, qualquer descumprimento da política e normas de segurança da informação que tenha conhecimento;
g. toda informação gerada ou adquirida pela ECT com a utilização de seu recursos é de sua propriedade e somente deve ser utilizada atendendo a seus interesses;
h. as informações devem receber classificação conforme o seu risco e importância para o negócio, devendo seu tratamento obedecer a esta classificação;
i. todos os recursos que armazenam, processam ou transportam informação, merecem o mesmo tratamento que é dão à própria informação e só devem ser utilizados para os fins estabelecidos e de acordo com os padrões vigentes;
j. o acesso de terceiros às normas da ECT é disponibilizado e controlado conforme contratos, termos e acordos estabelecidos entre as partes, garantindo-se o sigilo e observando-se as necessidades de negócio;
k. a comunidade ecetista deve atuar como agente ativo, comprometido com a segurança da informação;
l. a implementação de segurança da informação não pode ser prejudicial ao desenvolvimento e continuidade dos negócios da ECT;
m. a preservação do negócio depende da continuidade operacional dos processos críticos da ECT;
n. o estabelecimento de estrutura funcional adequada para a administração de ações que envolvam todas as áreas da Instituição, deve propiciar o desenvolvimento e segurança da informação da ECT;
o. a avaliação da eficácia e a eficiência dos controles internos, disciplinados pela política de segurança da informação, subsidiam as ações de segurança da informação na ECT;

p. avaliar o cumprimento da política e das normas de segurança da informação no âmbito da ECT é tarefa que deverá ser desempenhada pelo Departamento de Auditoria. No entanto cabe aos empregados, clientes, parceiros e fornecedores o cumprimento da política e das normas de segurança da informação e a todas as chefias o papel de supervisão do cumprimento da política;
q. atualizar a política e as normas de segurança da informação da ECT é tarefa que deverá ser desempenhada pelo Departamento de Planejamento de Tecnologia da Informação e Comunicação.

(ECT 2001, p. 2)

Anexo 2 – Estrutura da Norma de Segurança da Informação da ECT

- Capítulo 1 – Norma de Segurança da Informação para Administração de Contas – define critérios para a criação, alteração, desabilitação e exclusão de contras de usuários, bem como estabelece a política de senhas, do horário para utilização dos recursos de informática, da criação de contas especiais e de utilização do serviço de correio eletrônico.

- Capítulo 2 - Norma de Segurança da Informação para Desenvolvimento de Sistemas – estabelece regras para o desenvolvimento e aquisição de sistemas, com nível de segurança e padronização adequados, visando à otimização das rotinas de trabalho, a documentação, o tratamento e a segurança da informação.

- Capítulo 3 - Norma de Segurança da Informação para Acesso ao Ambiente Computacional – estabelece requisitos para acesso físico e características dos ambientes da rede corporativa da ECT, dos centros corporativos de dados da Administração Central e diretorias regionais, preservando a Empresa quanto à ocorrência de acessos não autorizados.

- Capítulo 4 - Norma de Segurança da Informação para Administração de Estação de Trabalho – estabelece requisitos para manter a integridade e a disponibilidade das estações de traalho e assegurar a devida proteção das informações nelas armazenadas.

- Capítulo 5 - Norma de Segurança da Informação para Operação de Estação de Trabalho – estabelece padrões de segurança para utilização das estações de trabalho.

- Capítulo 6 - Norma de Segurança da Informação para Banco de Dados – descreve as condições para a correta configuração, proteção e uso de

banco de dados e sua interrelação com os sistemas.

- Capítulo 7 - Norma de Segurança da Informação para Cópia de Segurança – define critérios para a execução e utilização das copias de segurança das informações e das configurações dos equipamentos de rede.

- Capítulo 8 - Norma de Segurança da Informação de Critérios para Classificação das Informações – define critérios para a classificação das informações e seus recursos de acordo com a sua importância para a ECT, visando a preservação e a proteção adequada.

- Capítulo 9 - Norma de Segurança da Informação para Auditoria, Geração e Análise de Registros – estabelece critérios para a geração, auditoria e as análises dos eventos ocorridos, visando a rastreabilidade e avaliação das ocorrências.

- Capítulo 10 - Norma de Segurança da Informação para Acesso à Internet, Intranet e Extranet – define critérios para administração e utilização dos serviços de Internet, Intranet e Extranet.

- Capítulo 11 - Norma de Segurança da Informação para Acesso Remoto – define critérios para a disponibilização do serviço de acesso remoto à rede corporativa da ECT, bem como as regras a serem obedecidas pelos usuários, visando a prevenção do acesso não autorizado às informações da ECT.

- Capítulo 12 - Norma de Segurança da Informação para Transmissão de Informações – define requisitos tecnológicos e aspectos a serem obedecidos pelos usuários para a transmissão de dados entre as unidades da ECT e dessas com os clientes externos e parceiros,

garantindo que não haja perda, modificação ou acesso indevido às informações transmitidas através da rede corporativa da ECT e deres públicas, ou qualquer outro meio de comunicação.

- Capítulo 13 - Norma Geral de Segurança da Informação para Técnicos – agrega segurança às atividades desempenhadas pelos técnicos, orientando-os para auxílio nas ações de segurança e definindo critérios para manipulação e disponibilização dos recursos de tecnologia da informação da ECT.

- Capítulo 14 - Norma Geral de Segurança da Informação para Usuários – agrega segurança às atividades desempenhadas pela comunidade ecetista, definindo critérios e responsabilidades para utilização e disponibilização das informações e dos recursos de informação da ECT.

- Capítulo 15 - Norma de Segurança da Informação para os Casos de Detecção de Intrusos nos Sistemas de Informação da ECT – visa à regulamentação das Ações mínimas a serem executadas, em caso de detecção de intrusos, nos sistemas de informação da ECT. Abrange todos os sistemas de informação da ECT, seja nas dependências da ECT ou de parceiros.

- Capítulo 16 - Norma de Segurança da Informação AntiSpam – estabelece critérios de gestão de mensagens eletrônicas denominadas SPAM.

- Capítulo 17 - Norma de Segurança da Informação para Utilização de Equipamentos de Rede sem Fio (Wireless) – define critérios para a utilização e administração de equipamentos de rede sem fio.

- Capítulo 18 - Norma de Segurança da Informação para Controle de

Acesso aos Sistemas de Informação – define quesitos de segurança que deverão ser usados pelos desenvolvedores, gestores, usuários e administradores de sistemas, objetivando prevenir a perda, modificação ou uso impróprio de dados.

- Anexo 1. Termo de Responsabilidade
- Anexo 2. Formulário de Solicitação de Acesso a Sistemas
- Anexo 3. Modelo de CI

- Capítulo 19 - Norma de Segurança da Informação para Especificação e Organização da CDI-ECT – define os requisitos de especificação e organização da Certificação Digital Interna da ECT.
    - Anexo 1: Termo de Responsabilidade para Certificação Digital Interna

- Capítulo 20 - Norma de Segurança da Informação para Administração dos Serviços da CDI-ECT - define os critérios para administração dos serviços de Certificação Interna da ECT.

- Capítulo 21: Norma de Segurança da Informação para Criação e Fluxo de e-CIs, e-NIs e e-MAILs com Assinatura Digital – estabelece o fluxo para circulação de documentos eletrônicos (comunicações internas, notas internas e e-mails) assinados digitalmente no âmbito da ECT.

Anexo 3 – Instrução Normativa GSI nº 1, de 13 de junho de 2008.

Extraída do Diário Oficial da União nº 115, seção 1, junho/2008, ISSN 1677-7042, p. 6-7

CONSELHO DE DEFESA NACIONAL
SECRETARIA EXECUTIVA

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.

O MINISTRO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, na condição de **SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL**, no uso de suas atribuições;

CONSIDERANDO:

o disposto no artigo 6º e parágrafo único do art. 16 da Lei nº 10.683, de 28 de maio de 2003;

o disposto no inciso IV do caput e inciso III do §1º do art. 1º e art. 8º do Anexo I do Decreto nº 5.772, de 08 de maio de 2006;
o disposto nos incisos I, VI, VII e XIII do artigo 4º do Decreto nº 3.505, de 13 de junho de 2000;

as informações tratadas no âmbito da Administração Pública Federal, direta e indireta, como ativos valiosos para a eficiente prestação dos serviços públicos;

o interesse do cidadão como beneficiário dos serviços prestados pelos órgãos e entidades da Administração Pública Federal, direta e indireta;

o dever do Estado de proteção das informações pessoais dos cidadãos;

a necessidade de incrementar a segurança das redes e bancos de dados governamentais; e

a necessidade de orientar a condução de políticas de segurança da informação e comunicações já existentes ou a serem implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

RESOLVE:

Art. 1º Aprovar orientações para Gestão de Segurança da Informação e Comunicações que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

Art. 2º Para fins desta Instrução Normativa, entende-se por:

I - Política de Segurança da Informação e Comunicações: 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;

II - Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

III - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

IV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

V - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

VI - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

VII - Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

VIII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

IX - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

Art. 3º Ao Gabinete de Segurança Institucional da Presidência da República - GSI, por intermédio do Departamento de Segurança da Informação e Comunicações - DSIC, compete:

I - planejar e coordenar as atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta;

II - estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta;

III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da Administração Pública Federal, direta e indireta, denominado CTIR.GOV;

IV - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e comunicações;

V - orientar a condução da Política de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

VI - receber e consolidar os resultados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta;

VII - propor programa orçamentário específico para as ações de segurança da informação e comunicações.

Art. 4º Ao Comitê Gestor de Segurança da Informação compete:

I - assessorar o GSI no aperfeiçoamento da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta;

II - instituir grupos de trabalho para tratar de temas específicos relacionados à segurança da informação e comunicações.

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.
Parágrafo único. Para fins do disposto no caput, deverá ser observado o disposto no inciso II do art. 3º desta Instrução Normativa.

Art. 6º Ao Comitê de Segurança da Informação e Comunicações, de que trata o inciso VI do art. 5º, em seu âmbito de atuação, compete:

I - assessorar na implementação das ações de segurança da informação e comunicações;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

III - propor alterações na Política de Segurança da Informação e Comunicações; e

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

Art. 7º 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 a possíveis impactos na segurança da informação e comunicações;

VI - manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações;

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

Art. 8º O cidadão, como principal cliente da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta, poderá apresentar sugestões de melhorias ou denúncias de quebra de segurança que deverão ser averiguadas pelas autoridades.

Art. 9º Esta Instrução Normativa entra em vigor sessenta dias após sua publicação.

JORGE ARMANDO FELIX

Anexo 4 – Norma Complementar nº02/IN01/DSIC/GSIPR - Metodologia de Gestão de Segurança da Informação e Comunicações – publicada no DOU nº 199, de 14 de outubro de 2008 – seção 1.

PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de segurança da Informação e Comunicações

METODOLOGIA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ORIGEM
Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA
Instrução Normativa GSI nº 1, de 13 de junho de 2008.
ABNT NBR ISO/IEC 27001:2006.

CAMPO DE APLICAÇÃO
Esta Norma se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO
1. Objetivo
2. Metodologia
3. Ciclo da Metodologia
4. Responsabilidades
5. Considerações Finais
6. Vigência

INFORMAÇÕES ADICIONAIS
Não há

APROVAÇÃO
RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1 OBJETIVO

Definir a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

2 METODOLOGIA

2.1 A metodologia de gestão de segurança da informação e comunicações baseia-se no processo de melhoria contínua, denominado ciclo “PDCA” (Plan-Do-Check-Act), estabelecido pela norma ABNT NBR ISO/IEC 27001:2006.

2.2 A escolha desta metodologia levou em consideração três critérios:

a) Simplicidade do modelo;

b) Compatibilidade com a cultura de gestão de segurança da informação em uso nas organizações públicas e privadas brasileiras; e

c) Coerência com as práticas de qualidade e gestão adotadas em órgãos públicos brasileiros.

3 CICLO DA METODOLOGIA

3.1 (**“Plan – P”**) Planejar - É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações planejará as ações de segurança da informação e comunicações que serão implementadas, considerando os requisitos ou pressupostos estabelecidos pelo planejamento organizacional, bem como as diretrizes expedidas pela autoridade decisória de seu órgão ou entidade. Para planejar é necessário:

3.1.1 Definir o escopo e os limites onde serão desenvolvidas as ações de segurança da informação e comunicações;

3.1.2 Definir os objetivos a serem alcançados com a implementação das ações de segurança da informação e comunicações, considerando as expectativas ou diretrizes formuladas pela autoridade decisória de seu órgão ou entidade;

3.1.3 Definir a abordagem de gestão de riscos de seu órgão ou entidade, sendo necessário:

a) definir uma metodologia de gestão de riscos que seja adequada ao escopo, limites e objetivos estabelecidos;

b) identificar os níveis de riscos aceitáveis e os critérios para sua aceitação, considerando decisões superiores e o planejamento estratégico do órgão ou entidade;

3.1.4 Identificar os riscos, sendo necessário:

a) Identificar os ativos e seus responsáveis dentro do escopo onde serão desenvolvidas as ações de segurança da informação e comunicações;

b) Identificar as vulnerabilidades destes ativos;

c) Identificar os impactos que perdas de disponibilidade, integridade, confidencialidade e autenticidade podem causar nestes ativos;

3.1.5 Analisar os riscos, sendo necessário:

a) identificar os impactos para a missão do órgão ou entidade que podem resultar de falhas de segurança, levando em consideração as conseqüências de uma perda de disponibilidade, integridade, confidencialidade ou autenticidade destes ativos;

b) identificar a probabilidade real de ocorrência de falhas de segurança, considerando as vulnerabilidades prevalecentes, os impactos associados a estes ativos e as ações de segurança da informação e comunicações atualmente implementadas no órgão ou entidade;

c) estimar os níveis de riscos;

d) determinar se os riscos são aceitáveis ou se requerem tratamento utilizando os critérios para aceitação de riscos estabelecidos em 3.1.3;

3.1.6 Identificar as opções para o tratamento de riscos, considerando a possibilidade de:

a) aplicar ações de segurança da informação e comunicações além das que já estão sendo executadas;

b) aceitar os riscos de forma consciente e objetiva, desde que satisfaçam o planejamento organizacional, bem como a diretrizes expedidas pela

autoridade decisória de seu órgão ou entidade, bem como aos critérios de aceitação de riscos estabelecidos em 3.1.3;

c) evitar riscos;

d) transferir os riscos a outras partes, por exemplo, seguradoras ou terceirizados;

3.1.7 Selecionar as ações de segurança da informação e comunicações consideradas necessárias para o tratamento de riscos. (Alguns exemplos de ações de segurança da informação e comunicações são: Política de Segurança da Informação e Comunicações, infra-estrutura de segurança da informação e comunicações, tratamento da informação, segurança em recursos humanos, segurança física, segurança lógica, controle de acesso, segurança de sistemas, tratamento de incidentes, gestão de continuidade, conformidade, auditoria interna, além de outras que serão exploradas em outras normas complementares);

3.1.8 Obter aprovação da autoridade decisória de seu órgão ou entidade quanto aos riscos residuais propostos;

3.1.9 Obter autorização da autoridade decisória de seu órgão ou entidade para implementar as ações de segurança da informação e comunicações selecionadas, mediante uma Declaração de Aplicabilidade, incluindo o seguinte:

a) Os objetivos e os recursos necessários para cada ação de segurança da informação e comunicações selecionada e as razões para sua seleção;

b) Os objetivos de cada ação de segurança da informação e comunicações que já foram implementadas em seu órgão ou entidade;

c) Um resumo das decisões relativas à gestão de riscos; e

d) Justificativas de possíveis exclusões de ações de segurança da informação e comunicações sugeridas pelo Gestor de Segurança da Informação e Comunicações e não autorizadas pela autoridade decisória de seu órgão ou entidade.

3.2 (**“Do – D”**) Fazer - É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações implementará as ações de segurança da informação e comunicações definidas na fase anterior. Para fazer é necessário:

3.2.1 Formular um plano de metas para cada objetivo das ações de segurança da informação e comunicações aprovadas na fase do planejamento em ordem de prioridade, incluindo a atribuição de responsabilidades, os prazos para execução, e os custos estimados;

3.2.2 Obter autorização da autoridade decisória de seu órgão ou entidade para implementar o plano de metas com a garantia de alocação dos recursos planejados;

3.2.3 Implementar o plano de metas para atender as ações de segurança da informação e comunicações aprovadas;

3.2.4 Definir como medir a eficácia das ações de segurança da informação e comunicações, estabelecendo indicadores mensuráveis para as metas aprovadas;

3.2.5 Implementar programas de conscientização e treinamento, sendo necessário:

a) assegurar que todo pessoal que tem responsabilidades atribuídas no plano de metas receba o treinamento adequado para desempenhar suas tarefas;

b) manter registros sobre habilidades, experiências e qualificações do efetivo do órgão ou entidade relativos à segurança da informação e comunicações;

c) assegurar que todo efetivo do órgão ou entidade esteja consciente da relevância e importância da segurança da informação e comunicações em suas atividades e como cada pessoa pode contribuir para o alcance dos objetivos das ações de segurança da informação e comunicações;

3.2.6 Gerenciar a execução das ações de segurança da informação e comunicações;

3.2.7 Gerenciar os recursos empenhados para o desenvolvimento das ações de segurança da informação e comunicações; e

3.2.8 Implementar procedimentos capazes de permitir a pronta detecção de incidentes de segurança da informação e comunicações, bem como a resposta a incidentes de segurança da informação e comunicações.

3.3 (**"Check – C"**) Checar - É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações avaliará as ações de segurança da informação e comunicações implementadas na fase anterior. Para checar é necessário:

3.3.1 Executar procedimentos de avaliação e análise crítica, a fim de:

a) detectar erros nos resultados de processamento;

b) identificar incidentes de segurança da informação e comunicações;

c) determinar se as ações de segurança da informação e comunicações delegadas a pessoas ou implementadas por meio de tecnologia da informação e comunicações estão sendo executadas conforme planejado;

d) determinar a eficácia das ações de segurança da informação e comunicações adotadas, mediante o uso de indicadores;

3.3.2 Realizar análises críticas regulares, a intervalos planejados de pelo menos uma vez por ano;

3.3.3 Verificar se os requisitos ou pressupostos estabelecidos pelo planejamento organizacional, bem como as diretrizes expedidas pela autoridade decisória de seu órgão ou entidade foram atendidos;

3.3.4 Atualizar a avaliação/análise de riscos a intervalos planejados de pelo menos uma vez por ano;

3.3.5 Conduzir auditoria interna, também denominada auditoria de primeira parte, das ações de segurança da informação e comunicações a intervalos planejados de pelo menos uma vez ao ano;

3.3.6 Atualizar os planos de segurança da informação e comunicações, considerando os resultados da avaliação e análise de crítica; e

3.3.7 Registrar e levar ao conhecimento da autoridade superior os possíveis impactos na eficácia da missão de seu órgão ou entidade.

3.4 (**"Act – A"**) Agir - É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações aperfeiçoará as ações de segurança da informação e comunicações, baseando-se no monitoramento realizado na fase anterior. Para aperfeiçoar e promover a melhoria contínua é necessário:

3.4.1 Propor à autoridade decisória de seu órgão ou entidade a necessidade de implementar as melhorias identificadas;

3.4.2 Executar as ações corretivas ou preventivas de acordo com a identificação de não conformidade real ou potencial;

3.4.3 Comunicar as melhorias à autoridade decisória de seu órgão ou entidade; e

3.4.4 Assegurar-se de que as melhorias atinjam os objetivos pretendidos.

4 CONSIDERAÇÕES FINAIS

A metodologia apresentada nesta norma deve ser complementar aos primeiros processos de Gestão de Segurança da Informação e Comunicações, previstos na IN 01 GSI, de 13 de junho de 2008, a serem implementados pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

5 VIGÊNCIA DA NORMA

Esta Norma entra em vigor na data de sua publicação.

Anexo 5 – Método e questionário de captura de informações utilizados no estudo de caso ECT.

As perguntas a seguir foram proferidas aos grupos de usuários da informação da ECT e as respostas alimentaram a planilha eletrônica que compõe a base de dados para o estudo em questão.

1º Passo

Identificar e definir os principais perigos que podem colocar em riscos a confidencialidade, integridade e confidencialidade das informações no ambiente corporativo de uma empresa pública.

Pergunta: Em sua opinião, que incidentes podem colocar as informações corporativas da ECT?

2º Passo

Cadastrar os principais perigos identificados que podem colocar em riscos a confidencialidade, integridade e confidencialidade das informações no ambiente corporativo de uma empresa pública que foram definidos no 1º Passo.

Os principais perigos identificados pelos representantes da central de serviços de sistemas foram: erro humano, *malware*, *hacking* e falha de *software.*

Ao passo que os principais perigos elencados pelos representantes da central de serviços de produção foram: desastres naturais, falhas no ambiente físico, furto de informação e falha de *hardware*.

Figura 33- Cadastro de Perigos

3º passo:

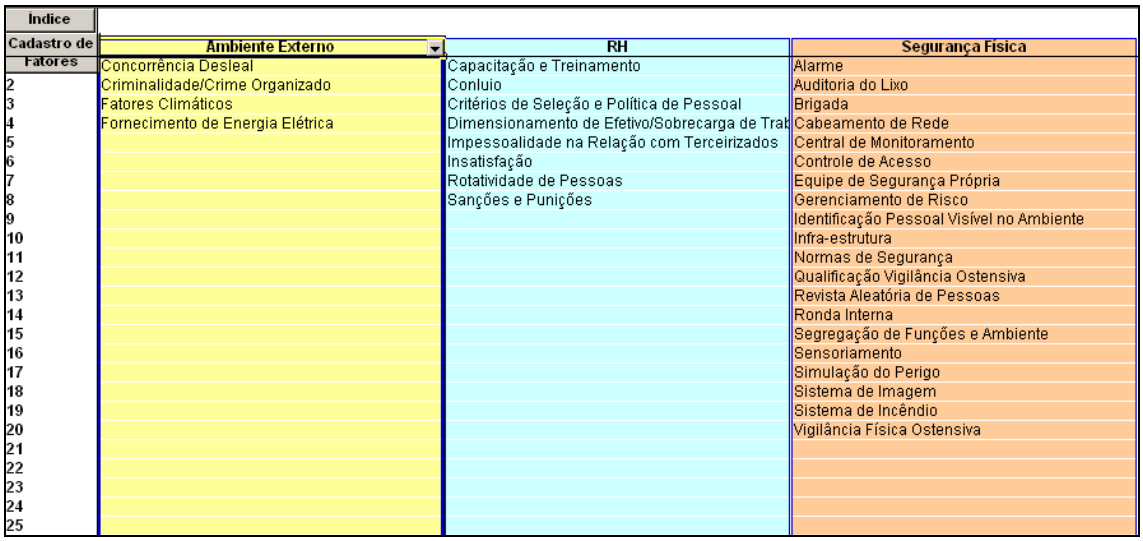
Detalhar os fatores que podem influenciar na concretização de cada perigo por meio do Diagrama de Causa e Efeito, também conhecido como Diagrama de *Ishikawa*.

Pergunta: Que fatores podem influenciar na concretização dos perigos identificados?

A relação de fatores corresponde ao registro das ideias expostas pelos usuários, de forma espontânea e ilimitada, acerca dos fatores que poderiam potencializar a ocorrência de um incidente.

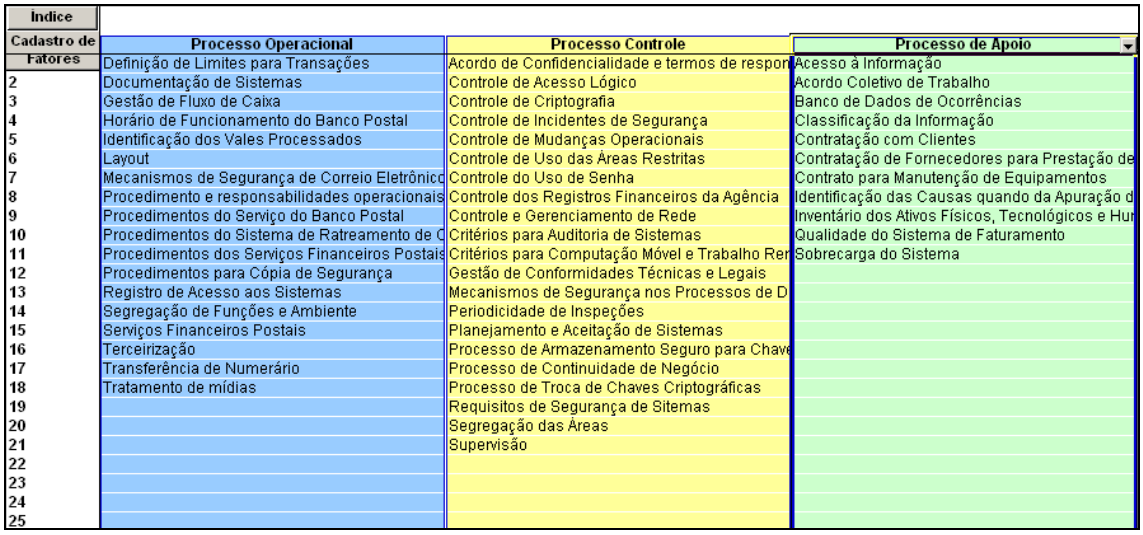
Os fatores identificados foram agrupados em seis macrofatores. São eles: Ambiente Externo, Processos de Apoio, Recursos Humanos, Segurança, Processos de Controle e Processos Operacionais.

Figura 34 - Cadastramento de Fatores



Índice			
Cadastro de Fatores	Ambiente Externo	RH	Segurança Física
1	Concorrência Desleal	Capacitação e Treinamento	Alarme
2	Criminalidade/Crime Organizado	Conluio	Auditoria do Lixo
3	Fatores Climáticos	Critérios de Seleção e Política de Pessoal	Brigada
4	Fornecimento de Energia Elétrica	Dimensionamento de Efetivo/Sobrecarga de Trab	Cabeamento de Rede
5		Impessoalidade na Relação com Terceirizados	Central de Monitoramento
6		Insatisfação	Controle de Acesso
7		Rotatividade de Pessoas	Equipe de Segurança Própria
8		Sanções e Punições	Gerenciamento de Risco
9			Identificação Pessoal Visível no Ambiente
10			Infra-estrutura
11			Normas de Segurança
12			Qualificação Vigilância Ostensiva
13			Revista Aleatória de Pessoas
14			Ronda Interna
15			Segregação de Funções e Ambiente
16			Sensoriamento
17			Simulação do Perigo
18			Sistema de Imagem
19			Sistema de Incêndio
20			Vigilância Física Ostensiva
21			
22			
23			
24			
25			

Figura 35 - Fatores cadastrados (Ambiente Externo, Recursos Humanos e Segurança Física)



Índice			
Cadastro de Fatores	Processo Operacional	Processo Controle	Processo de Apoio
1	Definição de Limites para Transações	Acordo de Confidencialidade e termos de respon	Acesso à Informação
2	Documentação de Sistemas	Controle de Acesso Lógico	Acordo Coletivo de Trabalho
3	Gestão de Fluxo de Caixa	Controle de Criptografia	Banco de Dados de Ocorrências
4	Horário de Funcionamento do Banco Postal	Controle de Incidentes de Segurança	Classificação da Informação
5	Identificação dos Vales Processados	Controle de Mudanças Operacionais	Contratação com Clientes
6	Layout	Controle de Uso das Áreas Restritas	Contratação de Fornecedores para Prestação de
7	Mecanismos de Segurança de Correio Eletrônico	Controle do Uso de Senha	Contrato para Manutenção de Equipamentos
8	Procedimento e responsabilidades operacionais	Controle dos Registros Financeiros da Agência	Identificação das Causas quando da Apuração d
9	Procedimentos do Serviço do Banco Postal	Controle e Gerenciamento de Rede	Inventário dos Ativos Físicos, Tecnológicos e Hu
10	Procedimentos do Sistema de Ratreamento de C	Critérios para Auditoria de Sistemas	Qualidade do Sistema de Faturamento
11	Procedimentos dos Serviços Financeiros Postais	Critérios para Computação Móvel e Trabalho Rem	Sobrecarga do Sistema
12	Procedimentos para Cópia de Segurança	Gestão de Conformidades Técnicas e Legais	
13	Registro de Acesso aos Sistemas	Mecanismos de Segurança nos Processos de D	
14	Segregação de Funções e Ambiente	Periodicidade de Inspeções	
15	Serviços Financeiros Postais	Planejamento e Aceitação de Sistemas	
16	Terceirização	Processo de Armazenamento Seguro para Chave	
17	Transferência de Numerário	Processo de Continuidade de Negócio	
18	Tratamento de mídias	Processo de Troca de Chaves Criptográficas	
19		Requisitos de Segurança de Sitemas	
20		Segregação das Áreas	
21		Supervisão	
22			
23			
24			
25			

Figura 36 - Fatores cadastrados (Processo Operacional, Processo de Controle e Processo de Apoio)

A construção do Diagrama de *Ishikawa* consiste em identificar, dentre os fatores cadastrados, os principais fatores que compõem o macrofator de cada perigo analisado. As perguntas a seguir correspondem à análise do perigo “Falha de Software”. A pesquisa consistiu em repeti-las para os demais perigos analisados.

Pergunta: Considerando a tabela “Ambiente Externo”, que fatores contribuem para a ocorrência de “Falha de Software” no ambiente da ECT?

Pergunta: Considerando a tabela “Recursos Humanos”, que fatores contribuem para a ocorrência de Falha de Software no ambiente da ECT?

Pergunta: Considerando a tabela “Segurança”, que fatores contribuem para a ocorrência de Falha de Software no ambiente da ECT?

Pergunta: Considerando a tabela “Processo Operacional”, que fatores contribuem para a ocorrência de Falha de Software no ambiente da ECT?

Pergunta: Considerando a tabela “Processo de Controle”, que fatores contribuem para a ocorrência de Falha de Software no ambiente da ECT?

Pergunta: Considerando a tabela “Processo de Apoio”, que fatores contribuem para a ocorrência de Falha de Software no ambiente da ECT?

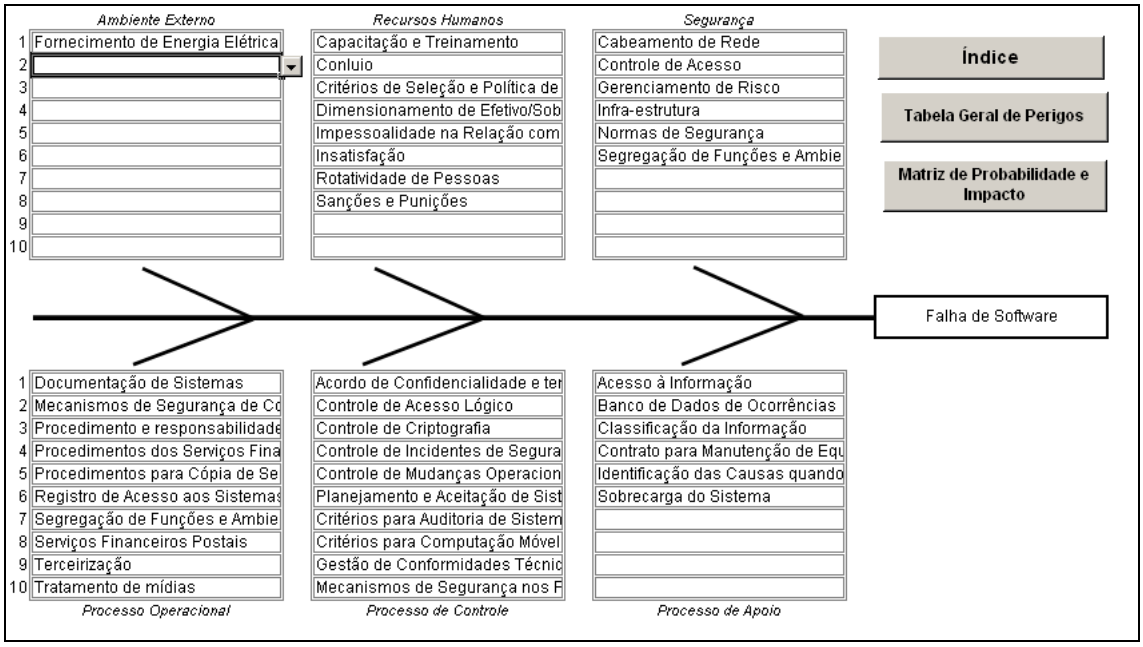


Figura 37 - Diagrama de *Ishikawa* - Falha de Software

4º Passo:

Definir, a partir da percepção do usuário, o grau de influência de cada macrofator para a ocorrência do perigo.

Pergunta: Considerando a tabela a seguir, informe na Matriz de Probabilidade e Impacto, o grau de influência dos macrofatores – Ambiente Externo (AE), Recursos Humanos (RH), Segurança (SE), Processo Operacional (PO), Processo de Controle (PC) e Processo de Apoio (PA) – para a ocorrência de cada um dos perigos.

Peso	Grau de Influência do Macrofator
1	Irrelevante ou quase nada
2	Pouco relevante
3	Medianamente relevante
4	Muito relevante
5	Extremamente relevante

MATRIZ DE PROBABILIDADE E IMPACTO		Macrofator de Perigo							E	GP	Classificação - Grau Probabilidade
		AE	RH	SE	PO	PC	PA	MFR		MFR x E	
1	Desastres Naturais										
2	Falhas no Ambiente Físico										
3	Erro Humano										
4	Furto da Informação										
5	Malware										
6	Hacking										
7	Falha de Software										
8	Falha de Hardware										
9											
10											
11											
12											
13											
14											
15											

Figura 38 - Matriz de Probabilidade e Impacto

5º passo:

Definir a Exposição ao Perigo (E), ou seja, a frequência com que o perigo costuma se manifestar num determinado intervalo de tempo.

Pergunta: Considerando a tabela a seguir, informe na coluna (E) da Matriz de Probabilidade e Impacto a freqüência com que cada um dos perigos se manifestou no ambiente da ECT no último ano.

Peso	Frequência de Ocorrência
1	Menos que trimestralmente
2	Ocorre trimestralmente
3	Ocorre mensalmente
4	Ocorre semanalmente
5	Ocorre diariamente

MATRIZ DE PROBABILIDADE E IMPACTO		Macrofator de Perigo							E	GP	Classificação - Grau Probabilidade
		AE	RH	SE	PO	PC	PA	MFR		MFR x E	
1	Desastres Naturais	1	1	1	1	1	1	1			
2	Falhas no Ambiente Físico	3	4	2	5	3	3	3			
3	Erro Humano	3	5	4	5	5	4	4			
4	Furto da Informação	4	3	4	5	3	5	4			
5	Malware	5	5	5	5	5	5	5			
6	Hacking	5	5	5	5	5	5	5			
7	Falha de Software	5	5	3	5	4	4	4			
8	Falha de Hardware	3	4	2	5	3	3	3			
9											
10											
11											
12											
13											
14											
15											

Figura 39 - Matriz de Probabilidade e Impacto

6º passo:

Determinar o impacto decorrente da ocorrência de cada perigo, considerando os seguintes aspectos: imagem, financeiro, legal, operacional e social.

As perguntas a seguir correspondem à análise do perigo “Falha de Software”. A pesquisa consistiu em repeti-las para os demais perigos analisados.

Pergunta: Imagem – na sua percepção e com base na tabela a seguir, qual é a abrangência de abalo à imagem e credibilidade da ECT quando ocorre uma “Falha de Software”? Informe na coluna correspondente da Matriz de Impacto e Probabilidade.

Peso	Escala	Abrangência – Abalo da Imagem
1	Individual	Somente a uma pessoa
2	Bairro	O bairro ou comunidade
3	Cidade	Uma cidade
4	Regional	A regional ECT ou estadual
5	Nacional	Nacional

Pergunta: Legislação – na sua percepção e com base na tabela a seguir, quando ocorre “Falha de Software” no ambiente da ECT há transgressão de dispositivos legais a que estão sujeitos a ECT? Informe na coluna correspondente da Matriz de Impacto e Probabilidade.

Peso	Escala	Abrangência – Bem Jurídico Atingido
1	Irrelevante	Não atinge nenhum bem jurídico na legislação vigente
3	Médio	Individual ou de uma pessoa
5	Superior	Da coletividade ou de grupos de pessoas

Pergunta: Social – na sua percepção e com base na tabela a seguir, como “Falha de Software” afeta a força de trabalho no ambiente da ECT? Informe na coluna correspondente da Matriz de Impacto e Probabilidade.

Peso	Escala	Abrangência – Reflexo nas pessoas (força de trabalho)
1	Irrelevante	Não atinge ninguém
2	Pouco Importante	Atinge pessoas indiretamente
3	Médio	Atinge uma pessoa diretamente
4	Alto	Atinge mais de uma pessoa diretamente
5	Superior	Atinge toda unidade ou efetivo da unidade

Pergunta: Operacional – na sua percepção e com base na tabela a seguir, como “Falha de Software” afeta os processos produtivos no ambiente da ECT? Informe na coluna correspondente da Matriz de Impacto e Probabilidade.

Peso	Escala	Abrangência – Alterações nos Processos Produtivos
1	Irrelevante	Não gera nenhuma alteração no processo produtivo
2	Pouco Importante	Gera pequenas alterações no processo produtivo
3	Médio	Gera grandes alterações no processo produtivo
4	Muito Importante	Gera parcial paralisação no processo produtivo
5	Superior	Gera a paralisação total do processo de uma unidade

	MATRIZ DE PROBABILIDADE E IMPACTO	Impacto							
		Imagem	Financeiro	Legislação	Operacional	Social	Nota	Impacto	Nível de Impacto
		2	Cálculo	2	5	3	17		
1	Desastres Naturais		1						
2	Falhas no Ambiente Físico		1						
3	Erro Humano		1						
4	Furto da Informação		1						
5	Malware		1						
6	Hacking		1						
7	Falha de Software		1						
8	Falha de Hardware		1						
9			1						
10			1						
11									
12									
13									
14									
15									

Figura 40 - Matriz de Probabilidade e Impacto