UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA – UESB
CURSO DE CIÊNCIA DA COMPUTAÇÃO

SEGURANÇA DA INFORMAÇÃO: GESTÃO DE RISCOS E SEGURANÇA DA INFORMAÇÃO NA EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS (ECT)

BRUNO ARAUJO OLIVEIRA

VITÓRIA DA CONQUISTA – BA
2014

BRUNO ARAUJO OLIVEIRA

SEGURANÇA DA INFORMAÇÃO: GESTÃO DE RISCOS E SEGURANÇA DA INFORMAÇÃO NA EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS (ECT)

Trabalho de conclusão de curso apresentado à Universidade Estadual do Sudoeste da Bahia – UESB, como parte dos requisitos para obtenção do título Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Fabio Moura Pereira

VITÓRIA DA CONQUISTA – BA

2014

UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA – UESB
CURSO DE CIÊNCIA DA COMPUTAÇÃO

SEGURANÇA DA INFORMAÇÃO: GESTÃO DE RISCOS E SEGURANÇA DA INFORMAÇÃO NA EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS (ECT)

BRUNO ARAUJO OLIVEIRA

Este trabalho foi apresentado como requisito parcial para obtenção do título Bacharel em Ciência da Computação da Universidade Estadual do Sudoeste da Bahia, tendo sido aprovado pela banca examinadora composta pelos professores:

Prof. Dr. Fabio Moura Pereira
UESB
(Orientador e Presidente)

Prof. Dra. Alzira Ferreira da Silva
UESB

Prof. Dr. Roque Mendes Prado Trindade
UESB

AGRADECIMENTOS

Primeiramente a Deus, pelo dom da vida e por todas as bênçãos recebidas neste longo caminho.

Aos meus pais, Iris Clario de Oliveira Brito e Maria Celia Araujo Oliveira, pelo amor incondicional que me é dado até hoje, estando sempre presente em todos os momentos, e também por sempre me mostrarem os melhores caminhos com conselhos e palavras sábias.

À minha irmã, Andressa Araujo Oliveira, pelo amor de uma vida inteira e por estar conosco hoje. E também por toda a ajuda na confecção deste trabalho.

À toda minha família, avós, tios, primos pela união e acompanhamento.

À minha namorada, Taiane de Oliveira Rocha, pelos incentivos e carinhos recebidos.

Aos colegas de sala, em especial Fabiano Novaes, Roberta Oliveira e Kely Macedo, pelas risadas, pela amizade e pelo apoio dado durante o curso.

Aos professores, orientadores e funcionários da UESB, pela contribuição durante essa longa caminhada.

Aos meus amigos da ECT, Claudio, Laion, Viola e Robério pelo incentivo e apoio nas minhas ausências, além das informações concedidas para a produção deste trabalho.

RESUMO

Este trabalho apresenta o contexto da segurança da informação e da gestão de riscos no ambiente da Empresa Brasileira de Correios e Telégrafos (ECT). A metodologia de pesquisa utilizada foi do tipo exploratória, com abordagem qualitativa, buscando verificar ações que tornam mais eficiente o processo de Gestão de Segurança da Informação, no âmbito da Administração Pública, a partir da Gestão de Riscos em Tecnologia da Informação, considerando a política, o comportamento e a cultura informacional. Foram feitas consultas em pesquisas bibliográficas, pesquisa documental e estudo de caso. Ao final da investigação, pôde-se concluir que a ECT, assim como outros órgãos da Administração Pública Federal (APF), não aborda a questão da Gestão de Riscos de forma suficiente para implementá-la de forma eficiente e eficaz, precisando de uma orientação sobre “o que fazer” e “como fazer”. O estado pouco desenvolvido em que se encontram os órgãos da APF, tanto em nível de conhecimento quanto nas implementações de sua Gestão de Riscos em Tecnologia da Informação, faz com que as orientações dos governos tenham que ser baseadas na mera aplicação das melhores práticas de Segurança da Informação adotadas.

Palavras-chave: Gestão de riscos. Gestão de segurança da informação. Tecnologia da informação. Empresa Brasileira de Correios e Telégrafos (ECT).

ABSTRACT

This work shows the context of information security and risk management into the *Empresa Brasileira de Correios e Telégrafos* (ECT). We used exploratory research methodology with a qualitative approach, seeking verify actions that make the process of Information Security Management more efficient, in the scope of Public Administration, from the Risk Management in Information Technology, considering the politic, the behavior and the informational culture. At the end of the investigation, it was concluded that the ECT, as well as many agencies of the Federal Public Administration (FPA), does not address the issue of Risk Management enough to implement it efficiently and effectively shape, needing an orientation about “what to do” and “how to do”. The underdeveloped state which are the FPA agencies, both in level of knowledge as in the implementations of its Risk Management in Information Technology, makes the guidelines of governments have to be based in the mere application of best practices of Information Security taken.

Keywords: Risk management. Information security management. Information technology. *Empresa Brasileira de Correios e Telégrafos (ECT)*.

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIAÇÕES

ABNT – Associação Brasileira de Normas Técnicas

APF – Administração Pública Federal

CC - *Common Criteria*

CESEP - Central de Suporte e Produção

COBIT - *Control Objectives for Information and Related Technology Institute*

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

ECT – Empresa Brasileira da Correios e Telégrafos

GNOP - Gerência Corporativa de Normas e Padrões Tecnológicos

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

ISTEC – *Information Technology Security Evaluation Criteria*

MANTIC - Manual de Tecnologia da Informação e Comunicação

SI – Segurança da Informação

TI – Tecnologia da Informação

SUMÁRIO

1. INTRODUÇÃO

Os sistemas de informação constituem-se como ativos de grande criticidade para as organizações. Assim, prover segurança a estes ativos e garantir a manutenção efetiva desta segurança é de fundamental importância. Por isso, a segurança da informação é fundamental, ela diz respeito à proteção da informação contra ameaças que possam valer-se de vulnerabilidades do sistema. Essa proteção deve ser uma das preocupações de quem a manuseia, não precisando ser um especialista em segurança da informação, mas sem dúvida alguma conhecendo requisitos básicos.

Entretanto, a segurança da informação não se restringe apenas às questões relacionadas à tecnologia da informação (TI). A segurança proporcionada pela tecnologia não supre toda a demanda necessária, conforme a norma ABNT NBR ISO/IEC 27002, que faz parte de um grupo de controles contendo as melhores práticas para segurança da informação, juntamente com a norma ABNT NBR ISO/IEC 27001, que se refere aos requisitos de sistemas de gestão de segurança da informação que devem ser implementados por uma organização; e com a norma ABNT NBR ISO/IEC 27005, que é relativa ao processo de gestão de riscos de segurança da informação e das suas atividades; além de outras normas, como a ABNT NBR ISO/IEC 17799, que traz um conjunto de recomendações para práticas de gestão da segurança da informação.

Estas normas relatam a importância da segurança da informação, seja ela em organizações públicas ou privadas. Elas explicitam que a gestão da segurança da informação não deve ser tratada apenas pela área de TI, mas por todas as áreas da organização.

Todas as organizações enfrentam incertezas, e no âmbito da Administração Pública Federal (APF), o gerenciamento de riscos possibilita aos administradores tratar com eficácia essas incertezas, a fim de melhorar a capacidade de gerar resultados positivos. Desse contexto veio a motivação para a realização deste trabalho, uma vez que o gerenciamento de riscos na APF pode ajudar a atingir metas de desempenho e evitar perda de recursos e danos à reputação da organização.

1.1 PROBLEMA

Considerando a importância da promoção das ações relativas à segurança da informação na APF, este trabalho teve como propósito verificar a gestão de segurança da informação em uma organização específica, a Empresa Brasileira de Correios e Telégrafos (ECT).

“Empresa pública vinculada ao Ministério das Comunicações, a ECT possui uma estrutura organizacional composta por uma Administração Central, formada pelo Conselho Fiscal, Conselho de Administração, Presidência e seis Diretorias, além de 28 Diretorias Regionais com atuação nos estados brasileiros” (ECT, 2001).

A gestão da política de segurança da informação da ECT é de responsabilidade da Diretoria de Tecnologia (DITEC), departamento focado em Tecnologia da Informação e que desconsidera aspectos corporativos relativos à outras diretorias, tais como: comercial, econômico-financeiro e de pessoal.

A problemática acerca deste trabalho advém do aumento da complexidade organizacional somado à crescente demanda de informações das quais depende a ECT. Tais fatores mostram a necessidade de conhecer e implementar, de forma abrangente, a política de segurança da informação e o processo de Gestão da Segurança da Informação.

Neste trabalho serão pesquisadas possíveis respostas para a seguinte questão: “Como utilizar a Gestão de Risco em TI para entender os riscos que afetam os negócios dos órgãos da APF e definir uma gestão de segurança da informação eficiente?”.

1.2 HIPÓTESES

A segurança da informação ainda não é feita da forma devida em muitas instituições públicas, como nos Correios. Ela seria mais eficiente se fosse adotada a Gestão de Riscos.

1.3 OBJETIVO GERAL

Estudar maneiras de tornar o processo de Gestão de Segurança da Informação mais eficiente, a partir do conceito de gestão de riscos, considerando-se a política, a cultura informacional e o comportamento existentes.

1.4 OBJETIVOS ESPECÍFICOS

- Estudar conceitos de Gestão de Segurança da Informação;
- Diagnosticar o processo de Gestão da Segurança da Informação da Diretoria de Tecnologia da Informação da ECT;
- Analisar modelos e definições de Gestão de Riscos;
- Identificar espaços informacionais dos empregados da Diretoria de Tecnologia da Informação da ECT;
- Propor um modelo para Gestão de Riscos, alinhado com normas e regulamentações legais, de forma a nortear a gestão de segurança da informação em uma empresa pública.

1.5 JUSTIFICATIVA

Os riscos operacionais associados à TI são muitos – panes, interrupções de serviço, falhas de segurança, entre outros. Estes podem tornar uma empresa incapaz de produzir seus bens e prestar serviços, além disso, podem deixar sua reputação manchada.

A informação precisa ser protegida, e os órgãos da APF, em grande parte, não possuem uma política eficaz de gestão e segurança da informação. Entre estes órgãos, a Empresa Brasileira de Correios e Telégrafos:

- não possui conhecimento suficiente para implementar uma Gestão de Segurança da Informação eficiente;
- precisa de uma orientação sobre “como fazer” e “o que fazer” acerca da implementação de uma Gestão de Riscos em TI;
- figura em um estado ainda inicial a respeito do nível de conhecimento sobre as implementações de sua gestão de riscos;
- precisa possuir um sistema de operação que, além de monitorar e traçar rumos, deve estar subordinada hierarquicamente à alta administração.

É necessária uma análise criteriosa das questões sobre Gestão de Riscos em TI e segurança da informação da empresa. A melhoria desses processos pode contribuir com o cumprimento de sua missão, que é: “facilitar as relações pessoais e

empresariais mediante a oferta de serviços de correios com ética, competitividade, lucratividade e responsabilidade social" (ECT, 2001).

1.6 METODOLOGIA DE PESQUISA

O presente trabalho constitui-se numa pesquisa aplicada, uma vez que sua finalidade é gerar conhecimento para aplicação de conceitos de Gestão de Riscos e Segurança da Informação no ambiente de uma empresa pública.

Para a produção deste trabalho foram utilizadas as seguintes técnicas: pesquisa bibliográfica e estudo de caso. Na abordagem utilizada, busca-se visualizar e integrar os contextos de Segurança da Informação e Gestão de Riscos, com a finalidade de proporcionar uma melhor compreensão sobre segurança da informação.

O universo de pesquisa são os órgãos da Administração Pública Federal, e, a partir da necessidade de selecionar uma amostra, foi escolhida a Empresa Brasileira de Correios e Telégrafos (ECT).

A análise do processo de Gestão de Segurança da Informação na ECT inicia-se com a investigação das iniciativas de Segurança da Informação no ambiente da ECT, fazendo uso de pesquisa documental em normas, manuais, e publicações internas da empresa, destacando-se:

- Diretrizes da Política de Segurança da Informação da ECT (2001);
- Estrutura da Norma de Segurança da Informação na ECT – Módulo 5 do Manual de Tecnologia da Informação e Comunicação (MANTIC).

O objetivo do estudo de caso é fazer um diagnóstico do processo de Gestão de Segurança da Informação no ambiente da ECT, resultado da comparação entre iniciativas de Segurança da Informação e boas práticas recomendadas, considerando valores, culturas e comportamento humano na empresa.

2. SEGURANÇA DA INFORMAÇÃO E GESTÃO DE RISCOS

Neste capítulo apresentamos informações relativas aos seguintes temas: informação, gestão de riscos, gestão da informação e segurança da informação.

2.1 INFORMAÇÃO

O termo “informação” pode ser definido como um conjunto de dados utilizados para a transferência de uma mensagem, entre indivíduos ou máquinas, em um processo.

Na busca literária, é possível encontrar diversos conceitos de informação, variando para cada autor. Entretanto, apesar das divergências entre conceitos, é possível conceituar este termo de forma simples, como um conjunto de dados registrados, independente do suporte, possuidores de significado e que pode ser transmitido a um usuário (receptor).

Durante suas atividades, uma organização produz, recebe, trata, acumula, utiliza e descarta informações. Gerenciá-las até chegar ao uso é uma das tarefas mais complexas.

Segundo Beal (2008) e Lyra (2008), o ciclo de vida da informação em organizações é dividido em diversas etapas sequentes e com diferentes funções. São elas: identificação das necessidades e requisitos, obtenção, tratamento, armazenamento, distribuição, uso e descarte.

2.2 GESTÃO DE RISCOS

Com base nas palavras de Ferreira (1999), risco pode ser definido como uma situação em que há probabilidades mais ou menos previsíveis de perda ou ganho.

Quando se fala em risco, o conceito mais adequado a este trabalho é o proposto por Oliveira (2001): “risco é a probabilidade de uma ameaça explorar vulnerabilidades para causar perdas ou danos a um ativo ou grupo de ativos da organização”. Destarte, eles são determinados pela combinação de ameaças, vulnerabilidades e valores dos ativos. Estes valores são medidos baseados no impacto destes ativos aos negócios da organização, onde o impacto se apresenta como os resultados de um acontecimento não esperado.

2.2.1 Gestão de riscos

> "Gestão de riscos é um 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).

Os acontecimentos da contemporaneidade mostram que fazemos parte de um mundo cheio de incertezas, sejam elas políticas, sociais e econômicas. E no contexto das organizações, estas categorias de risco não podem ser desconsideradas. Assim, a definição de gestão de riscos é adotada de várias maneiras por diversos grupos e para finalidades distintas.

A gestão de riscos constitui-se num elemento que faz parte do planejamento estratégico da organização e deve ser praticado em todos os níveis da administração.

Partindo da premissa que todas as organizações enfrentam incertezas, o grande desafio dos administradores é determinar o limite de tolerância dessas incertezas, e também estabelecer como elas podem interferir nos processos de criação de valores às partes interessadas.

Com a gestão de riscos, os administradores podem tratar com mais eficiência as incertezas, assim como os riscos e oportunidades a elas ligados, com o intuito de melhorar a capacidade de agregar valor.

A gestão de riscos pode reduzir as surpresas e prejuízos de eventos operacionais, identificando e administrando riscos para fazer uma avaliação eficaz das necessidades, aproveitando as oportunidades de forma proativa.

2.2.2 Componentes do risco

A seguir apresentaremos os componentes do risco e suas principais características.

- *Ameaça:* "expectativa de acontecimento acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação" (BEAL, 2005, p.14). Segundo a ISO/IEC 13335-1:2004, ameaça é a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Quanto à classificação, as ameaças podem ser naturais, involuntárias ou voluntárias. Ameaças naturais são originadas em fenômenos da natureza, como enchentes, terremotos, incêndios naturais, entre outros. Ameaças involuntárias, ou acidentais, não estão condicionadas à intenção premeditada, são causadas sempre por conta do desconhecimento. Elas podem ser causadas por erros, acidentes, falta de energia, etc. Ameaças voluntárias ou intencionais são planejadas anteriormente e causadas por agentes humanos, como hackers, invasores, espiões, ladrões, etc.

- Vulnerabilidade: segundo a 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. Ela leva à ocorrência de um problema de segurança, afetando de forma negativa um ou uns dos princípios da segurança da informação (disponibilidade, integridade, confidencialidade).
- Impacto: “abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio” (SÊMOLA, 2003, p.50). Beal (2005) retrata impacto como o efeito ou consequência de um ataque ou incidente para a organização.
- Incidente: é um evento ou fato que sucede a ação de uma ameaça, e que explora uma ou mais vulnerabilidades, podendo levar à perda nos princípios da segurança da informação.

2.3 GESTÃO ESTRATÉGICA DA INFORMAÇÃO

A palavra estratégia pode ser definida de várias formas. Entretanto, pode ser considerada como composição de planos, meios e objetivos para alcance dos objetivos, configurando-se como um indicador para a organização.

Vale salientar o termo estratégia competitiva. Este define as atividades comerciais e a forma de operar essas atividades. Além disso, define como diferenciar seus produtos e serviços dos oferecidos pelos competidores. Ela deve considerar os segmentos que a organização deseja servir e definir recursos para isto.

2.3.1 Valor estratégico da informação

De acordo com McGee e Prusak (1994), do surgimento da tecnologia da informação, veio a ideia de que computadores de alta capacidade poderiam aperfeiçoar o fornecimento de informações, no qual elas seriam precisas sempre. No entanto, o passar dos anos mostrou que isso não é tão fácil quanto se imaginava. As limitações da tecnologia e dos profissionais de TI constituem fatores desse insucesso. E, por isso, as organizações esperam continuamente por melhoras em cada geração, com profissionais cada vez melhor capacitados.

É sabido que produtos e serviços de TI estão em constante evolução. Desta forma, criam novas possibilidades e apresentam soluções para antigos problemas. Assim, os investimentos em tecnologia da informação podem ser estratégicos e capazes de criar uma enorme vantagem competitiva. A segurança da informação é importante para os negócios, tanto no setor público como no privado, e sua função é viabilizar negócios e evitar ou reduzir os riscos relevantes.

A segurança da informação pode ser alcançada por meios técnicos e deve ser apoiada por uma gestão e por procedimentos apropriados. A identificação de controles a serem implantados requer um planejamento cuidadoso e atenção aos detalhes.

A informação é um recurso estratégico e necessita de uma administração, além de merecer tanta atenção quanto é dispensada a recursos financeiros e humanos. Por isso, as organizações devem fazer investimentos estruturados para gerenciar a informação.

Para Sêmola (2005), a informação é um fator essencial na corrida das organizações por agilidade, competitividade, modernização, lucratividade e, principalmente, flexibilidade e adaptabilidade ao crescimento – fatores primordiais para as empresas prosperarem na era da informação. Assim, a informação deve ser bem guardada como um segredo de negócio.

Tradicionalmente, as organizações dedicam atenção especial à proteção de seus ativos físicos e financeiros, mas pouca atenção aos seus ativos de informação. Segundo Caruso e Steffen (1999), 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 (figura 1). Portanto, devem ser protegidas.

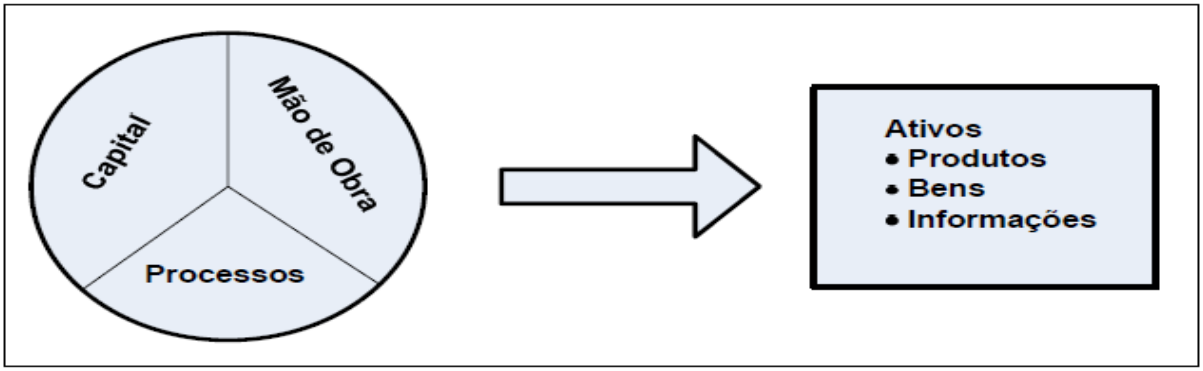

Figura 1 – Fatores econômicos de produção. Fonte: Caruso e Steffen (1999)

2.3.2 Classificação da informação

A classificação da informação é essencial para definir os recursos de proteção dos ativos da informação. Sob essa ótica, o principal objetivo é “assegurar que a informação receba um nível adequado de proteção” (ABNT NBR ISO/IEC 17799:2005), permitindo determinar com precisão os requisitos de tratamento e proteção.

Continuando com as recomendações da ABNT NBR ISO/IEC 17799:2005, convém que a informação seja classificada para indicar a necessidade, as prioridades e o nível esperado de proteção quando do tratamento da informação. Esta norma diz que a informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Convém que um sistema de classificação da informação seja usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento.

O subitem 7.2 da Norma Brasileira ABNT NBR ISO/IEC 17799:2005 dispõe sobre a classificação da informação e aponta que, em geral, a classificação da informação é uma forma de determinar como a informação deverá ser tratada e protegida.

A classificação pode ser realizada baseada em valor, requisitos legais, criticidade e grau de sensibilidade da organização pelas informações. Essas informações devem ser conduzidas, armazenadas, transferidas e até descartadas.

Tais ações são relacionadas com atributos fundamentais de segurança da informação: confidencialidade, integridade e disponibilidade (figura 2).

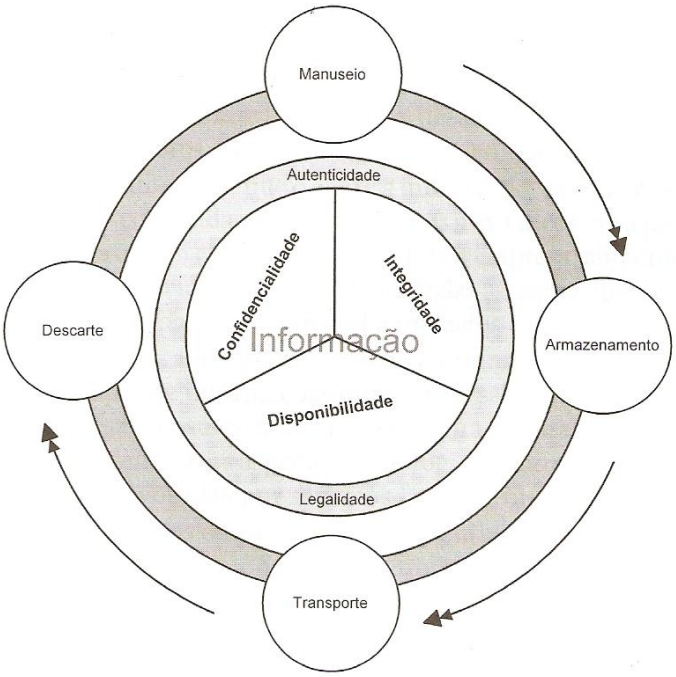

Figura 2 – Ciclo de vida da informação. Fonte: Sêmola (2003)

- Confidencialidade: é garantia de que somente pessoas, entidades, processos ou organizações envolvidas na comunicação poderão utilizar as informações transmitidas pela rede. Isto deve ser feito independentemente da segurança do sistema de comunicação utilizado. Muitas das grandes empresas têm o dever de preservar o tipo de informação que possuem. O nível de confidencialidade da informação deve ser mantido para ser um diferencial competitivo de mercado ou por exigências legais. Divulgada pela legislação federal, através do Decreto nº 4553/2002, art.5º, a classificação da confidencialidade é definida em quatro categorias: ultra-secretos, secretos, confidenciais e reservados.

- Integridade: é a garantia de que as informações trocadas não serão alteradas ou removidas no decorrer do caminho. Mesmo que as informações não sejam sigilosas, caso elas sejam destruídas ou alteradas, podem ocorrer consequências graves. Em muitos dos casos, a perda de informações confidencias significa a perda de credibilidade junto ao cliente. Quanto aos requisitos de integridade, a informação pode ser classificada em: registradas, que exigem cuidados especiais quanto ao seu conteúdo; controladas, que fazem parte do âmbito interno da organização e que

exigem menos controle que as registradas, mas requerem medidas excepcionais de controle contra alterações sem autorização; e normais: que exigem controles menos rigorosos quanto à modificação quando comparado com as controladas.

- Disponibilidade: é a propriedade de que a informação esteja acessível e possa ser utilizada quando necessário. Isto é, a oportunidade de acesso à informação. A partir dos requisitos da disponibilidade, a informação pode ser classificada em: vital, essencial para a sobrevivência da organização e cuja perda acarreta danos irreparáveis; crítica, aquela cuja perda acarreta sérios danos para a organização; e comum, aquela cuja perda não acarreta sérios prejuízos para a organização, e, por conta disto, não exigem controles rigorosos.

2.4 SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA GESTÃO DE RISCOS

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

De acordo com a Associação Brasileira de Normas Técnicas, o termo Segurança da Informação (SI) é "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".

Neste contexto, a Segurança da Informação pode ser definida como uma área dedicada à proteção de ativos da informação contra ameaças. Ela constitui-se numa prática da gestão de riscos que possam afetar a confidencialidade, integridade e disponibilidade da informação. Dessa forma, são definidas regras sobre as fases do ciclo de vida da informação, a fim de que sejam viabilizados o controle e a identificação de ameaças e vulnerabilidades.

2.4.1 Atributos da segurança da informação

- Confidencialidade: "garantia de que o acesso à informação é restrito aos seus usuários legítimos" (BEAL, 2005, p.1).

- Integridade: “garantia da criação legítima e da consistência da informação ao longo de seu ciclo de vida” (BEAL, 2005, p.1).
- Disponibilidade: “garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna” (BEAL, 2005, p.1).
- 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 legitimo” (BEAL, 2005, p.1).
- Não repúdio: significa a garantia de que o usuário não possa negar sua responsabilidade pelo uso ou envio de uma informação. Esse termo está associado com os termos confidencialidade e autenticidade.
- Legalidade: “garantia de que a informação foi produzida em conformidade com a lei” (BEAL, 2005, p.1).

2.4.2 Política de segurança da informação

Política de segurança é um conjunto de leis, regras, e práticas que regulamentam como uma organização irá gerenciar, proteger e distribuir suas informações e recursos. O principal objetivo da política de segurança é controlar, o armazenamento da informação, que em alguns casos é mais valioso do que a própria empresa.

Zwicky (2000) considerou quatro questões para a formulação da política de segurança:

- Capacidade financeira: quanto custa a segurança?
- Funcionalidade: pode-se utilizar o sistema de forma plena?
- Compatibilidade cultural: a política de segurança proposta está em conflito como a forma que as pessoas normalmente interagem com os que estão do lado de fora da empresa?
- Legalidade: A política de segurança está de acordo com os requerimentos legais exigidos?

A forma de comunicar administradores e usuários é chamada de documento da política de segurança. É importante que este documento seja explicito e de forma clara sobre todas as decisões a serem tomadas. Um documento de política de segurança fala sobre expectativas e responsabilidades entre os usuários e administradores, permite a todos saberem o que esperar de cada um. A maioria das pessoas só irá seguir as regras se compreenderem realmente a importância destas.

Mais importante do que escrever um documento de política de segurança é segui-lo. Isto é, quando a política não é seguida, a situação deve ser corrigida, e alguém precisa ser responsável por fazer estas correções.

2.4.3 Normas e padrões de segurança da informação

Objetivo das normas e padrões de segurança da informação é definir critérios e regras, além de mostrar as melhores formas de promover a qualidade e uniformidade de processos, produtos e serviços.

Estas normas e padrões prezam pela qualidade dos processos e pela integridade das informações. Eles constituem mecanismos de orientação do comportamento das pessoas no ambiente da organização, auxiliam as organizações na implementação das melhores práticas de segurança em Tecnologia da Informação e, em alguns casos, determinam restrições e obrigações.

É importante que todos os sistemas de segurança da informação estejam conforme as orientações de regulamentação e normatização e em obediência às leis.

A seguir serão citados alguns padrões e normas conhecidos e usados por organizações que seguem um sistema de gestão de segurança da informação:

- ABNT NBR ISO/IEC 17799:2005;
- ABNT NBR ISO/IEC 27001:2006;
- ABNT NBR ISO/IEC 27005:2008;
- COBIT - *Control Objectives for Information and Related Technology Institute;*
- *Common Criteria for Information Technology Security Evaluation;*
- *ISO Guide 73 – Vocabulary – Guidelines for Use in Standard;*
- ISO 13335 – *Guidelines for Management of IT Security;*
- ISTEC – *Information Technology Security Evaluation Criteria.*

2.5 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 NBR ISO/IEC 27005:2008, p.1).

Beal (2005) relaciona os termos associados ao risco à Segurança da Informação, conforme mostrado na figura 3. Para a autora, o alvo de um ataque pode ser um ativo de informação. Desta forma, a ameaça se constitui num elemento do risco que pode ser associado a uma probabilidade. Esta, por sua vez, é calculada a partir da frequência de ocorrência. Ainda segundo a autora, as medidas de proteção podem diminuir a probabilidade de concretização de uma ameaça, e, as vulnerabilidades com potencial de exploração, consequentemente reforçam para a redução do risco ao ativo da informação.

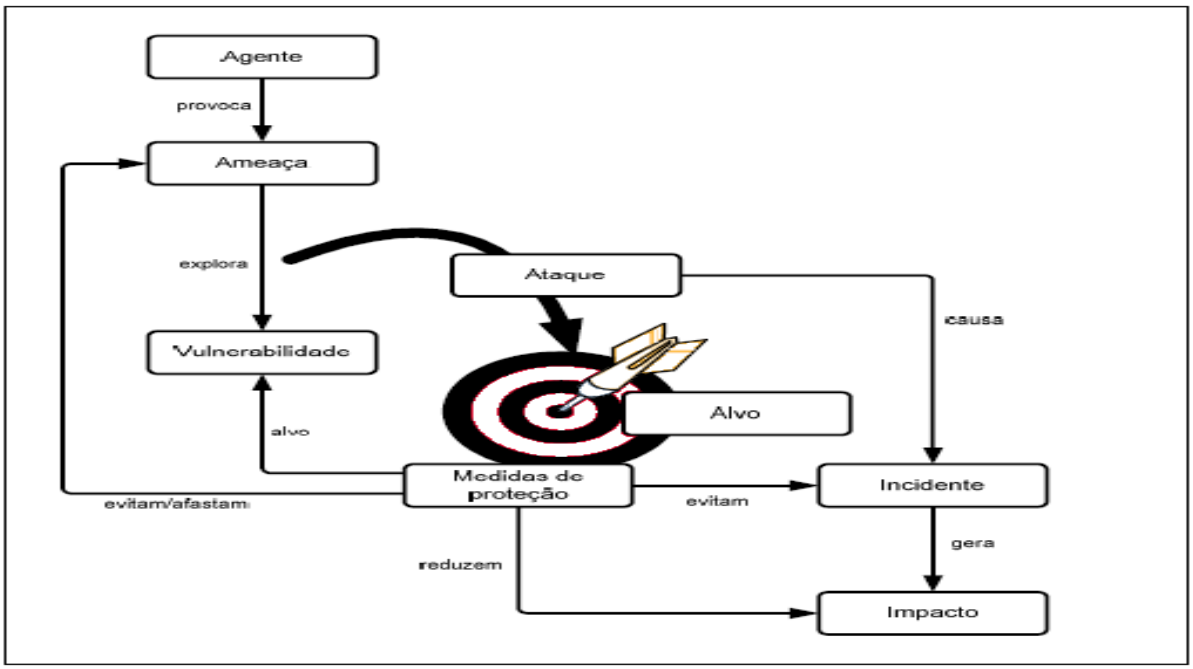

Figura 3 – Relacionamento entre os termos associados ao risco para a SI. Fonte: Beal (2005)

O modelo de processo de gestão de riscos em segurança da informação abordado nesta pesquisa é o da norma ABNT NBR ISO/IEC 27005:2008. Nele, o processo de gestão de riscos em segurança da informação é contínuo e se baseia na definição do contexto, análise/avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco e análise crítica de riscos.

A figura 3 mostra uma relação dos termos ligados ao risco à segurança da Informação. E a figura 4 mostra uma visão geral das etapas do processo de gestão de riscos conforme a ABNT NBR ISO/IEC 27005:2008.

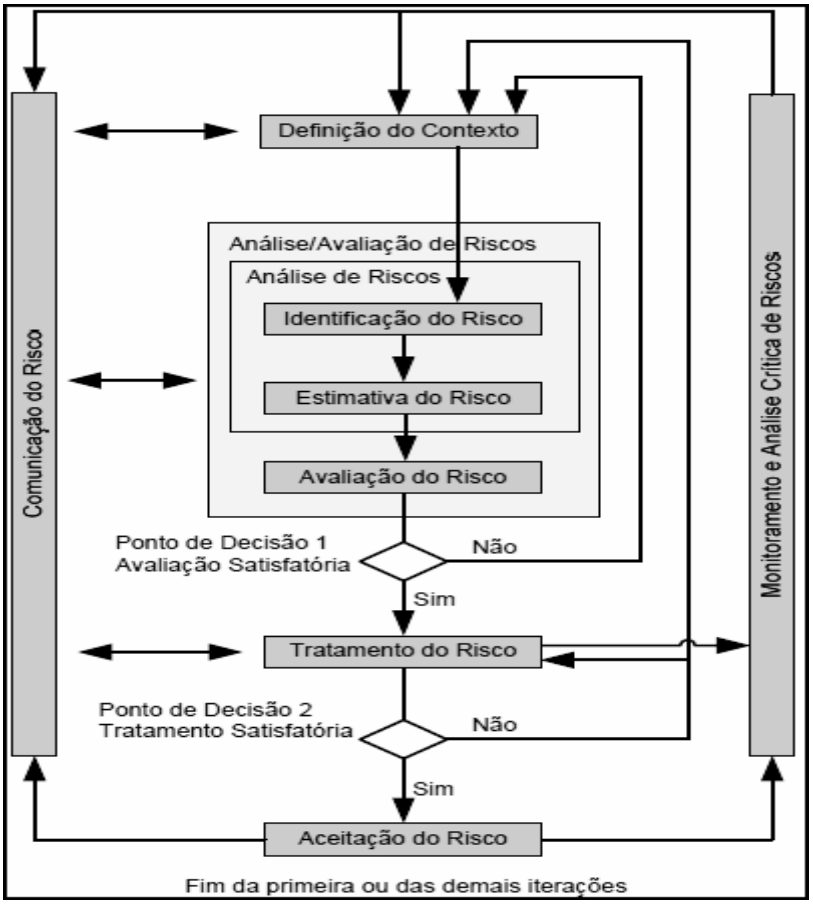

Figura 4 – Processo de gestão de riscos de segurança da informação.
Fonte: ABNT NBR ISO/IEC 27005 (2008)

2.5.1 Fases do processo de gestão de segurança da informação

- Definição do contexto: segundo a norma ABNT NBR ISO/IEC 27005:2008, é nesta etapa do processo que o contexto da gestão de riscos em segurança da informação é formado, originado das informações sobre a organização, para definir: critérios básicos necessários, escopo da gestão de riscos e estrutura apropriada para operar esta gestão.
- Análise/avaliação de riscos de segurança da informação: nesta etapa, os critérios de avaliação e análise envolvem identificar, quantificar e priorizar os riscos. Deste subprocesso, fazem parte as seguintes atividades:

- ✓ Identificação e classificação de riscos: determina eventos que podem causar perdas e identifica as situações que podem gerar essas perdas;
- ✓ Estimação de riscos: descreve as consequências do risco e a possibilidade de ocorrência dessas consequências;
- ✓ Avaliação de riscos: é realizada comparando os níveis dos riscos e os critérios de avaliação e aceitação dos riscos.

- Tratamento do risco: durante esta etapa, os riscos são tratados para serem mitigados, retidos, evitados ou transferidos. O resultado é um plano de tratamento que, respeitando os requisitos legais, compreenda a relação de controles, acompanhada de custos, benefícios e prioridades.
- Aceitação do risco: "a decisão de aceitar os riscos deve ser formalmente registrada juntamente com a responsabilidade pela decisão" (ABNT NBR ISO/IEC 27001:2005, 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).
- Monitoração e análise crítica de riscos: segundo a ABNT NBR ISO/IEC 27005:2008, os riscos devem ser ser monitorados e analisádos de forma crítica, com a finalidade de identificar possíveis mudanças no contexto da organização. O monitoramento dos riscos gera uma linha contínua de gestão de riscos com as metas da organização e critérios para que os riscos sejam aceitos.
- Comunicação do risco: para a norma ABNT NBR ISO/IEC 27005:2008, o objetivo da 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. Essa comunicação, sendo eficaz, tende a produzir impactos significativos nos processos de decisão da gestão de riscos em segurança da informação.

3. METODOLOGIA

No estudo de caso, foram analisadas variáveis utilizadas no processo de gestão de riscos. Essa análise foi feita com base em seis macrofatores: processos operacionais, processos de controle, segurança, recursos humanos, processos de apoio e ambiente externo.

O objetivo dessa análise é permitir a identificação da origem/causa de cada perigo que pode por em risco a confidencialidade, a integridade e a disponibilidade das informações dentro do ambiente de uma empresa pública. Para tanto, foram utilizadas as seguintes variáveis: falha de software, falha de hardware, erro humano, falha no ambiente físico, *hacking*, *malware*, desastres naturais e furto de informação.

3.1 TIPO DE PESQUISA QUANTO AOS OBJETIVOS

Este trabalho caracteriza-se como uma pesquisa exploratória, pois possui, como objetivo, a geração de conhecimento para a devida aplicação dos conceitos de Gestão de Riscos à Segurança da Informação no ambiente de uma empresa pública.

3.2 TIPO DE PESQUISA QUANTO À ABORDAGEM

Sobre a abordagem utilizada nesta pesquisa, esta possui caráter qualitativo. Ao empregar tal método, busca-se visualizar o contexto da Segurança da Informação e, se possível, ter uma integração com a Gestão de Riscos, que possa implicar em um melhor entendimento acerca da segurança da informação.

3.3 TIPO DE PESQUISA QUANTO AOS PROCEDIMENTOS TÉCNICOS

Estudo de caso é o procedimento técnico que foi adotado para investigar os riscos que podem afetar a Segurança da Informação, além de definir um processo para a Gestão da Segurança da Informação a partir da Gestão de Riscos.

3.4 INSTRUMENTOS DE PESQUISA

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. Foi utilizada pesquisa documental em manuais, normas, procedimentos e publicações internas da empresa. Tal diagnóstico é resultado de uma comparação entre as iniciativas de Segurança da Informação no ambiente da ECT e as boas práticas recomendadas na literatura e em normas e documentos técnicos que abordam este tema, considerando a cultura, os valores e o comportamento humano na empresa.

3.5 UNIVERSO E AMOSTRA

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

3.6 COLETA DE DADOS

A base teórica que dá sustentação a este trabalho é construída a partir de pesquisa bibliográfica e visa estudar conceitos, definições e modelos de Gestão de Segurança da Informação e Gestão de Riscos. Alguns dados utilizados foram cedidos por grupos de usuários da informação da ECT, dessa forma, alimentaram a base de dados do estudo em questão.

4 ESTUDO DE CASO: 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 começa com a análise de protocolos relativos à segurança da informação e gestão de riscos em segurança da informação na Empresa Brasileira de Correios e Telégrafos. Esse diagnóstico foi realizado a partir do levantamento das iniciativas corporativas e da análise de documentos e manuais corporativos.

Verificou-se que a ECT possui uma política de segurança de suas informações, homologada em novembro de 2001. Para a ECT, a política de segurança da informação é um conjunto de normas e diretrizes que devem ser seguidas; “visa conscientizar e orientar os empregados, clientes, parceiros e fornecedores para o uso seguro do ambiente informatizado da ECT” (ECT, 2007).

O cumprimento da Política de Segurança da Informação é de responsabilidade de todos os colaboradores, empregados ou prestadores de serviços, que devem obedecer a uma série de diretrizes. Essas diretrizes estão descritas no anexo 1.

A ECT possui um Manual de Tecnologia da Informação e Comunicação (MANTIC), e, o módulo 5 deste manual, compõe um conjunto de 21 capítulos que possuem as normas de segurança da informação da ECT. O principal objetivo das normas de segurança da informação é assegurar que a política de segurança da informação seja implementada, mantida ou modificada de forma harmônica e convergente, em 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 no Anexo 2.

As normas e a política de Segurança da Informação da ECT são os pilares para o estabelecimento de todos os padrões corporativos de segurança. Sua abrangência compreende todos os ambientes de informática da ECT.

Na estrutura organizacional, a Administração Central possui uma gerência corporativa para tratar de padrões e normas. Incluindo a segurança da informação. Essa gerencia 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

ligados à segurança da informação fazem parte das responsabilidades de uma equipe técnica subordinada à Central de Suporte e Produção (CESEP).

Em fevereiro de 2008, uma Portaria PRESI-027/2008 foi emitida, ela instituiu um grupo de trabalho para propor organização e estruturação da gestão de riscos e uma reorganização das atividades de segurança empresarial na ECT. Para chegar ao entendimento sobre o que é segurança empresarial, estabeleceu-se objetos e valores como elementos protegidos por medidas de segurança no ambiente da ECT. Os seguintes valores foram identificados: vida, negócio, conhecimento e recursos. Essa identificação permitiu relacionar os seguintes objetos: pessoas, objetos postais, informação, receitas e patrimônio.

A proposta definida pelo grupo de trabalho é executar a segurança empresarial na ECT de acordo com os diferentes bens protegidos, de forma coordenada por todas as áreas e em sintonia com os outros segmentos de atuação da empresa, com o intuito de chegar às metas da instituição, de acordo com a organização relacionada à segurança: patrimonial, postal, das pessoas, das informações e das receitas.

4.1 IDENTIFICAÇÃO DOS ESPAÇOS DE INFORMAÇÕES DOS USUÁRIOS E RISCOS AOS ATIVOS DE INFORMAÇÃO DA ECT

A partir do momento que os computadores passaram a transmitir dados, eles passaram também a ter alguns problemas de segurança, isso porque quando certas informações são acessadas por muitas pessoas, é preciso ter cuidados para evitar que ocorram acessos indevidos, maus usos ou imprudências. Essas ameaças podem colocar em risco a confidencialidade, a integridade e a disponibilidade das informações na ECT.

Considerando a ECT em seus espaços informacionais virtuais – por exemplo: banco de dados, web sites, comunidades práticas de conhecimento e bibliotecas virtuais – identificamos alguns riscos que afetam as informações corporativas. Dentre estes se destacam:

- Concentração de informações: ao multiplicar o número de dados que podem ser armazenados em espaços restritos, o uso de computadores evidenciou um problema já existente.

- Acesso indiscriminado às informações: usualmente, usuários têm acesso a mais recursos e informações do que precisam para o exercício de suas funções.
- Obscuridade das informações: a partir do uso de computadores, a obscuridade das informações foi potencializada, isso porque as informações em meios eletrônicos não podem ser vistas diretamente, ou seja, precisam de recursos de software e hardware. Dessa forma, as informações são mais difíceis de serem controladas, sendo assim mais fáceis de serem fraudadas ou roubadas.
- Concentração de funções: pode tornar a organização vulnerável à vontade de poucos indivíduos, permitindo que este obtenha conhecimentos para ações ilícitas e obter vantagens por conta do uso das informações manuseadas.
- Falta de controle: pode atrasar no descobrimento de irregularidades, impossibilitando a tomada de ações que possam remediar as situações não desejadas e seus impactos.
- Relacionamento e combinação de informações: a junção de informações pode mostrar dados sigilosos e quebrar a confidencialidade. Os recursos de informática podem facilitar os processos de relacionamento e cruzamento de informações, possibilitando a aquisição de informações sensíveis.
- Introdução de códigos ocultos: são erros ou linhas de código que podem ser inseridas nas rotinas de processamento da informação e comprometer a integridade e confidencialidade das informações geradas.

4.2 ESTUDO DE AÇÕES QUE POSSAM SISTEMATIZAR A GESTÃO DE RISCOS PARA NORTEAR O PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

O ambiente de estudo das ações necessárias para nortear o processo de gestão de segurança da informação será a ECT, a partir da aplicação do conceito de gestão de riscos, cujo ponto de partida é um exame minucioso realizado pelo Grupo de Gestão de Riscos nomeado por meio de portaria com o intuito de atuar no âmbito interno da organização.

Para que as análises fossem feitas, o grupo mencionado acima identificou empresas públicas e privadas cuja gestão possui nível de complexidade compatível

com a ECT. Nesse trabalho somente serão consideradas as que se referem à Segurança da Informação.

Visitas técnicas foram realizadas nas seguintes empresas: HSBC, Caixa Econômica Federal, SERPRO, Banco do Brasil, UNIBANCO e BR Distribuidora. Além disso, foram realizadas pesquisas sobre os principais correios internacionais (Alemanha, França e Canadá) e empresas privadas do setor, tais como Fedex e UPS e mantendo contatos com institutos de pesquisa e desenvolvimento do tema como a COPEAD/UFRJ. Como resultado das visitas e observações foram propostas várias ações para o processo de Gestão de Riscos em Segurança da Informação.

4.2.1 Base normativa

Para que a gestão de riscos e segurança da informação seja estruturada e organizada é determinante a base normativa. Dessa forma, é conveniente que a organização esteja conforme os padrões e normas que são referência para o mercado. São eles: Acordo Basiléia II, ITIL, COBIL, AS/NZS 4360/2004, norma ABNT ISO/IEC 17799, ABNT ISO/IEC 15999-1/2007, norma ABNT ISO/IEC 27001, norma ABNT ISO/IEC 27002 e norma ABNT ISO/IEC 27005.

4.2.2 Ambiente

Para a implementação da gestão de riscos e segurança da informação, os ambientes das empresas analisadas apontaram como elementos fundamentais:

- comprometimento da alta administração com a gestão de riscos;
- identificação dos processos críticos referentes ao negócio;
- existência da cultura de controle;
- existência de um sistema de informação estruturado e profissionais capacitados em Gestão de Riscos;
- gerenciamento da organização por processo;
- difusão do tema em todos os níveis da organização, e ainda, a existência de imposição regulatória.

4.2.3 Políticas e estratégias

Sobre as políticas e estratégias das empresas analisadas, destacam seus seguintes elementos:

- disciplinamento ético dos empregados e colaboradores;
- conformidade das informações;
- transparência da gestão;
- separação de atividades;
- o total armazenamento dos registros;
- retorno ajustado ao risco sobre capital;
- limite de perdas e de exposição ao risco;
- unicidade de fonte de dados e definição de responsabilidades.

4.2.4 Metodologia de Gestão de Segurança da Informação

O uso de métodos de análise de riscos proporciona às organizações operarem seus recursos de forma eficaz e identificarem níveis aceitáveis de risco aos negócios. Essa identificação dos níveis aceitáveis pode variar entre as empresas.

Para a análise dos riscos envolvidos nos processos de gestão de segurança da informação foi utilizado um método que permite estimar a probabilidade de ocorrência do perigo. Um método simples do ponto de vista da aplicação e com possibilidade de conciliação com a cultura de gestão de segurança usada na ECT. O resultado dessa aplicação pode fundamentar a escolha dos recursos a serem utilizados para a segurança necessária dos ativos de informação. Sua execução é dividida em duas fases.

A primeira fase é baseada na identificação da origem ou causa de cada perigo. Foram marcados oito perigos principais que podem por em risco a confidencialidade, a integridade e a disponibilidade das informações dentro do ambiente de uma empresa pública. São eles:

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

- Falha de hardware: queda de desempenho ou indisponibilidade de equipamentos do ambiente computacional que processam informações corporativas;
- Erro humano: queda de desempenho ou indisponibilidade de equipamentos, serviços, aplicativos ou programas por conta de ação não proposital de empregados e/ou colaboradores;
- Falha no ambiente físico: indisponibilidade de recursos do ambiente computacional ou da estrutura do ambiente físico. Exemplo: incêndio, pane elétrica, entre outros;
- *Hacking*: queda no desempenho ou indisponibilidade de equipamentos, serviços, aplicativos ou programas em razão de ato proposital de pessoas mal intencionadas que procuram autopromoção, benefícios econômicos, concorrência desleal ou roubar informação;
- *Malware*: programas desenvolvidos para pratica de atos maliciosos em computadores. Dentre os mais conhecidos são vírus, *worms*, cavalos de Tróia e *spyware;*
- Desastres naturais: quando ocorre queda no desempenho ou indisponibilidade de equipamentos, aplicativos ou programas, por conta de fatores da natureza, como, por exemplo, enchentes, raios e inundações;
- Furto de informação: subtração com intenção não legítima de apropriar-se de informação para si ou para outra pessoa.

A segunda fase é caracterizada pela análise de seis macrofatores: processos operacionais, processos de controle, segurança, recursos humanos, processos de apoio e ambiente externo.

- Processos operacionais: principais processos operacionais e produtos inter-relacionados à atividade da ECT;
- Processos de controle: principais processos de controle da regional ligados à atividade da ECT;
- Segurança: todos os equipamentos, meios, processos e instrumentos de segurança ligados à atividade da ECT;
- Recursos humanos: tudo que se refere aos colaboradores ligados à atividade da ECT;

- Processos de apoio: principais processos de apoio da regional relacionados à atividade da ECT;
- Ambiente externo: características, variáveis e circunstâncias externas, sem controle do gestor e relacionadas à atividade da ECT.

Abaixo, estão apresentadas análises individuais com os principais fatores que contribuem para a ocorrência de cada perigo.

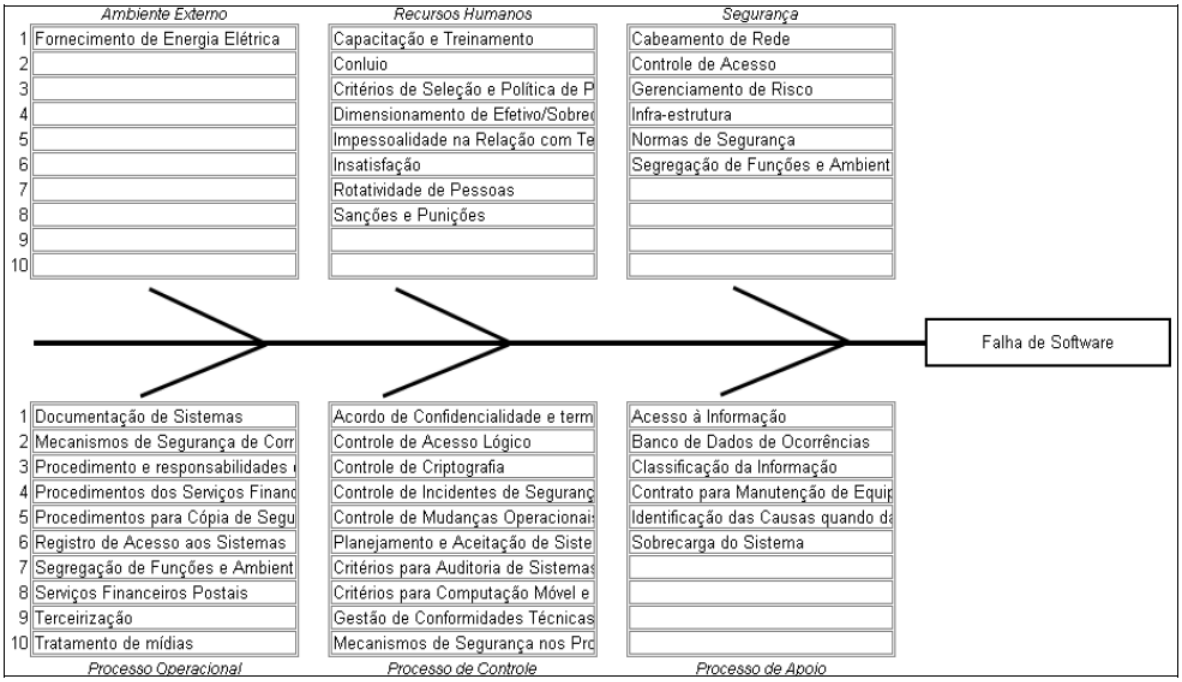

Figura 5 – Diagrama: falha de software.

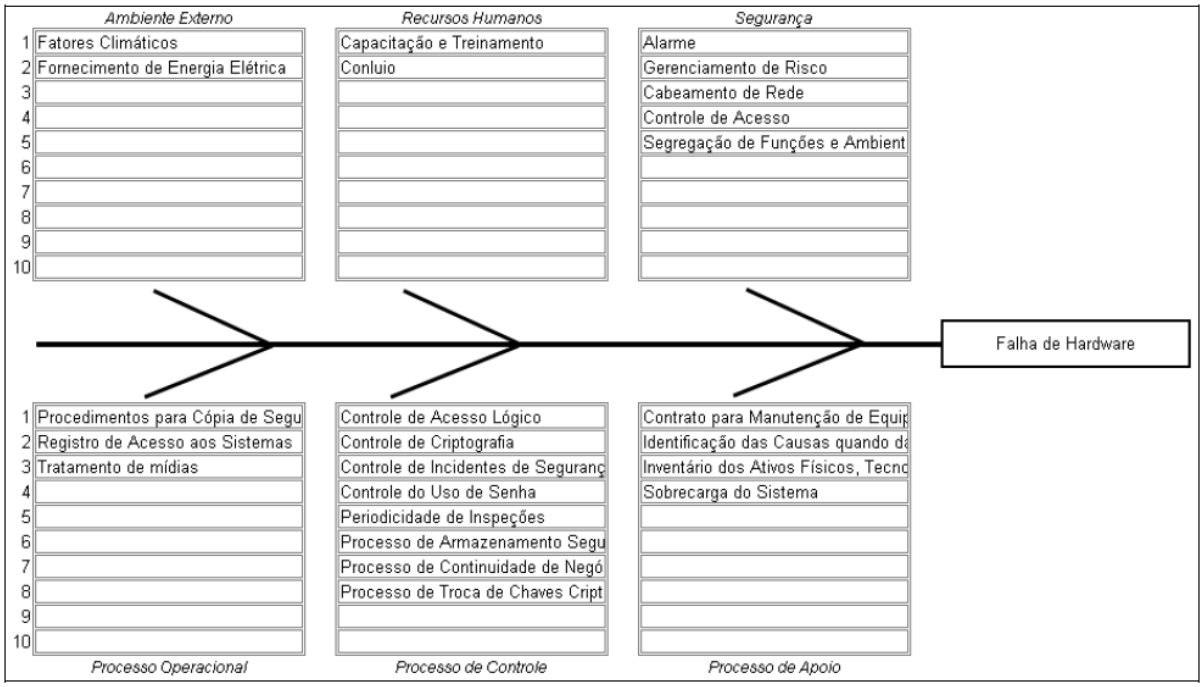

Figura 6 – Diagrama: falha de hardware.

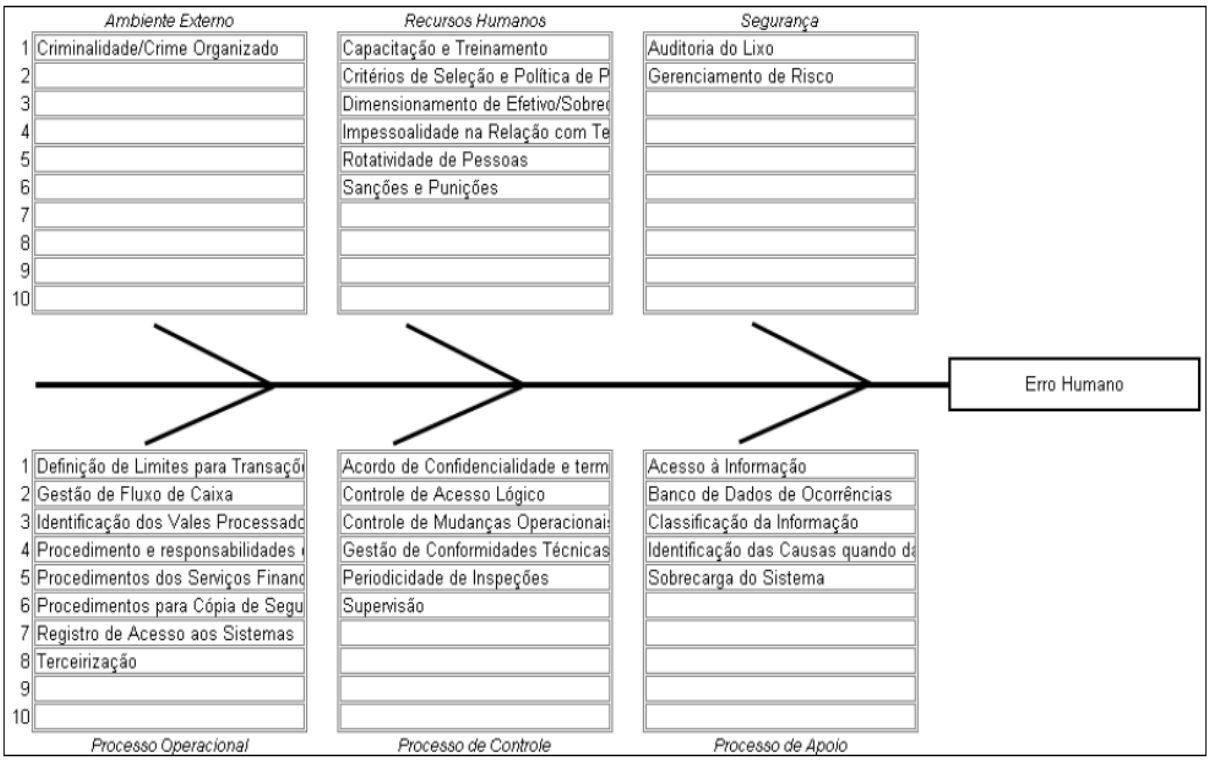

Figura 7 – Diagrama: erro humano.

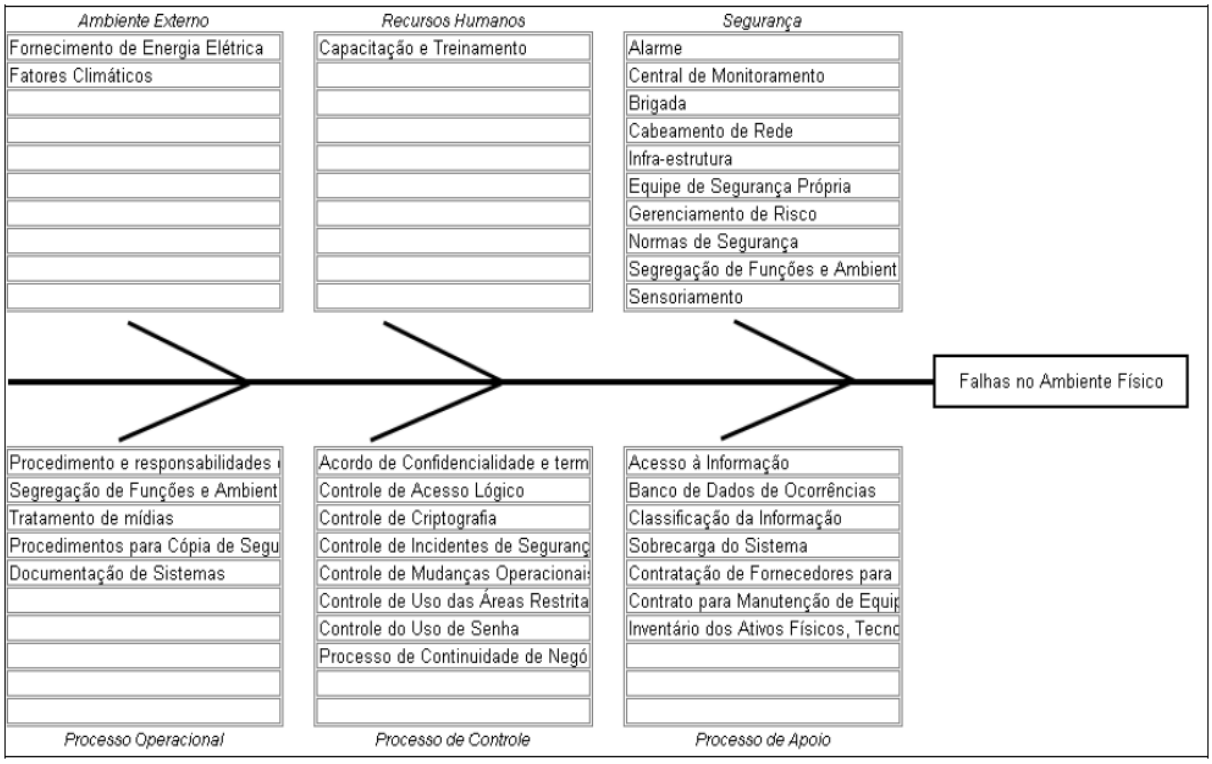

Figura 8 – Diagrama: falhas no ambiente físico.

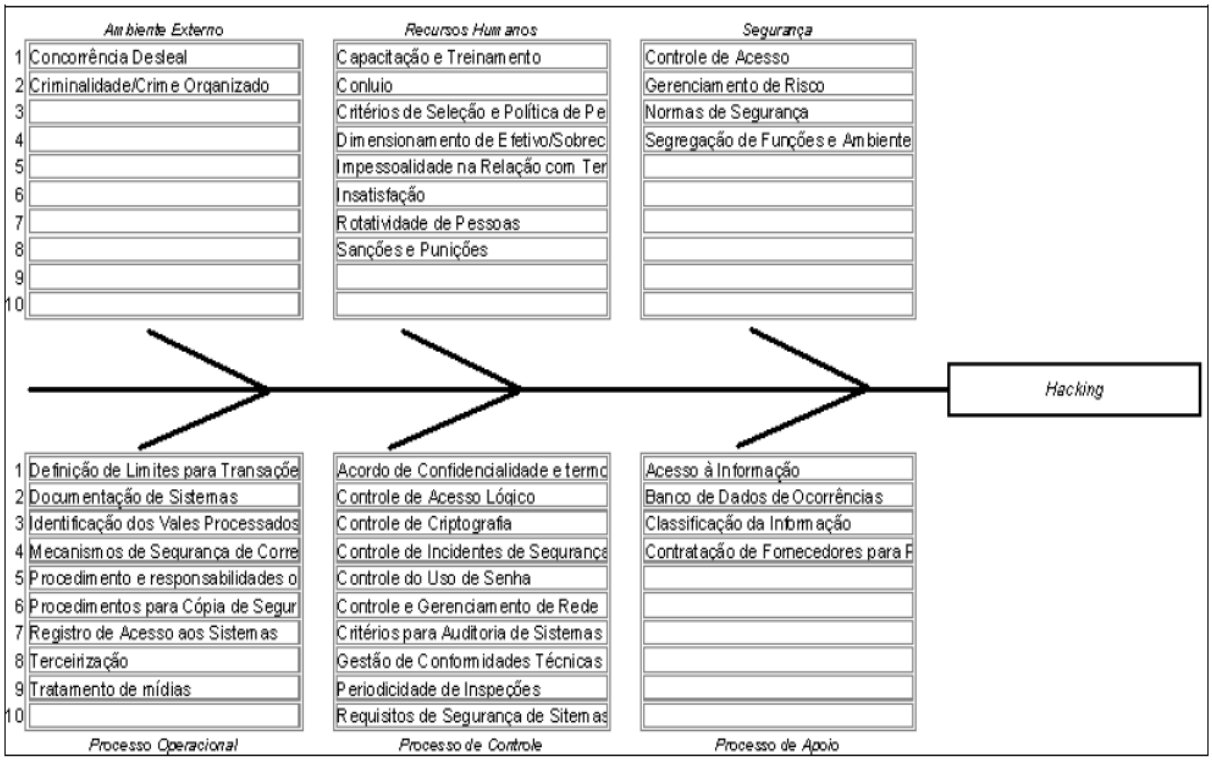

Figura 9 – Diagrama: hacking.

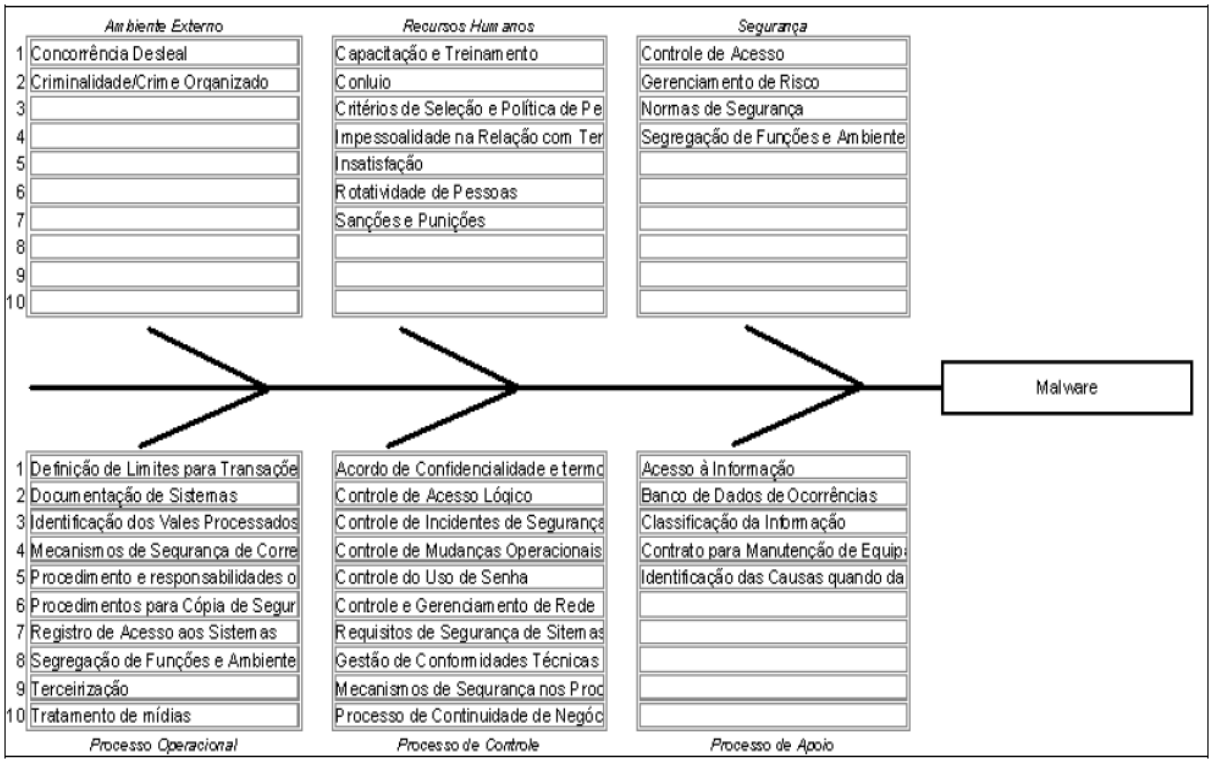

Figura 10 – Diagrama: malware.

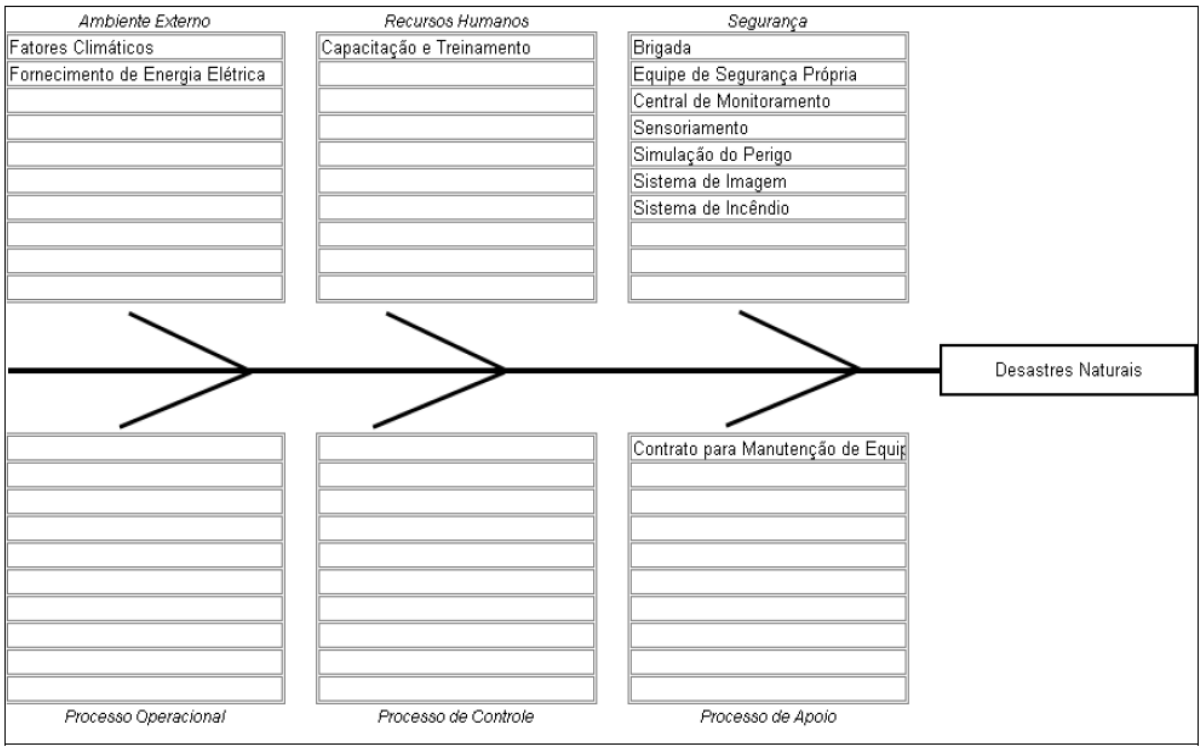

Figura 11 – Diagrama: desastres naturais.

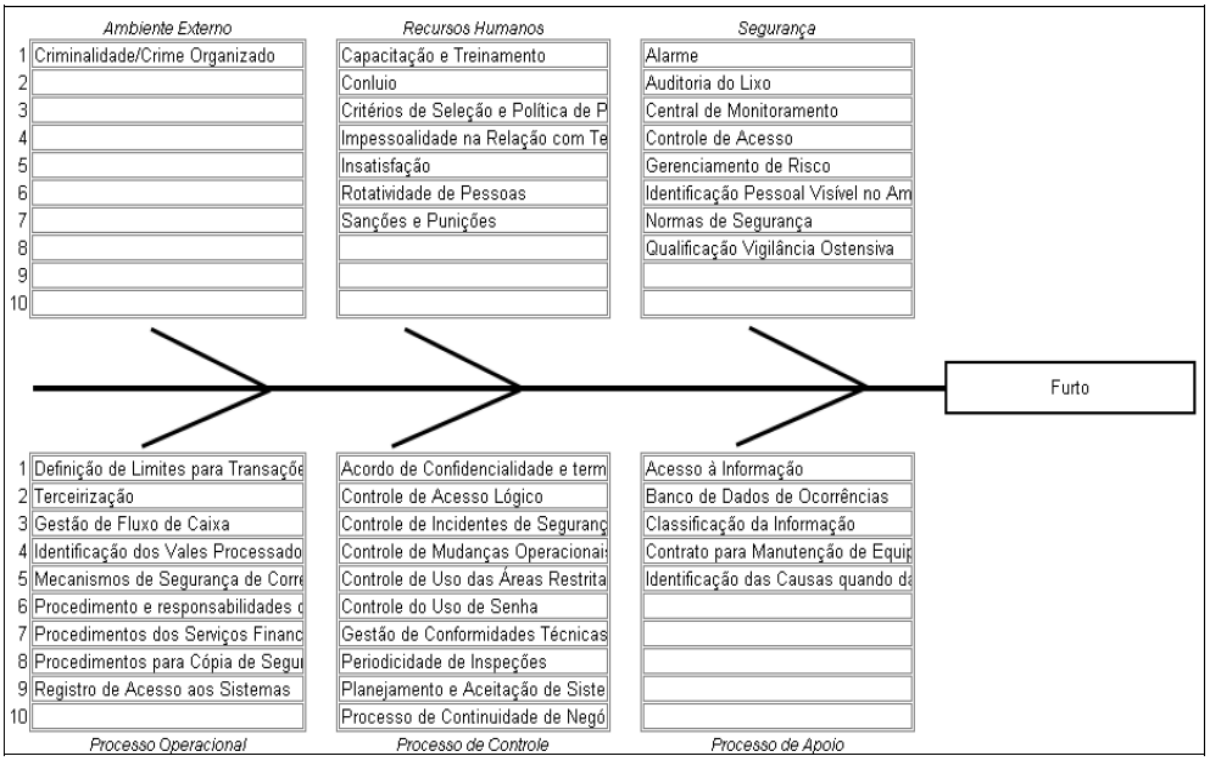

Figura 12 – Diagrama: furto.

É pertinente salientar que os incidentes dispostos nesses diagramas vieram de informações disponibilizadas por grupos de usuários da informação da ECT, que alimentaram a base de dados para o estudo.

4.2.5 Avaliação dos perigos analisados

Esta parte explica o impacto da ocorrência de cada perigo. Ela é feita com base no grau de influência dos macrofatores da fase anterior e na frequência que o perigo costuma expor-se em um determinado intervalo de tempo. Esse impacto é avaliado em cinco aspectos, e em cada um é apresentada sua relevância para a ECT. Os aspectos avaliados são:

- Imagem: credibilidade ou percepção de confiança do público na ECT;
- Legislação: as normas legais as quais a ECT está sujeita devem ser respeitadas;
- Social: relativo aos efeitos do perigo na relação entre as pessoas que estão inseridas no ciclo de vida da informação;
- Operacional: relativo à interrupções totais ou parciais dos processos operacionais da ECT;
- Financeiro: relativo a valores de perdas decorrentes da ocorrência dos perigos.

✓ Falha de software: mostra grau de possibilidade alto e impacto mediano. Para minimizar esse risco é aconselhável: manter os documentos de sistemas atualizados e à disposição dos envolvidos; promover aos envolvidos treinamentos de capacitação e formação; garantir que mudanças em códigos de sistema sejam realizadas e testadas em um ambiente de testes antes de serem colocadas em produção; fazer revisões periódicas de processos de controle de acesso somente quem for autorizado; dar aos usuários regras que contenham direitos e deveres atribuídas ao acesso.

✓ Falhas de hardware: apresenta grau de possibilidade baixo e impacto mediano. Os principais equipamentos de hardware responsáveis pelo processo de informações estão instalados em um ambiente isolado, que possui formas de

controle e manutenção para a garantia da integridade física. Na ECT, para que aumente a disponibilidade das informações trafegadas por meio eletrônico, estuda-se a probabilidade de replicação dos principais equipamentos relativos ao processamento de informações em outro Centro Corporativo de dados, cuja infraestrutura é similar à da sala do Edifício da Administração Central.

✓ Erro humano: este perigo mostra grau de possibilidade alto e impacto mediano. Para diminuir as probabilidades desse perigo, as principais ações a serem tomadas serão relacionadas à capacitação, treinamento e conscientização dos envolvidos. Convém evitar também que o acumulo de funções e atividades em um risco sofram sobrecargas.

✓ Falha no ambiente físico: este perigo representa grau de possibilidade baixo e impacto mediano. Na ECT, os equipamentos de computação de processamento e armazenamento de informações são instalados fisicamente em um ambiente isolado, que tem a disposição vários mecanismos que garantem segurança e disponibilidade, por exemplo: alarme, mecanismos de combate a incêndios e a problemas na rede elétrica, sistema de monitoramento de imagem e controle de acesso físico. Recomendações: revisar, periodicamente, a relação de todas as pessoas que têm direito de acesso ao ambiente físico; fazer manutenções preventivas nos recursos de infraestrutura (sistemas de prevenção de incêndios, sistemas de monitoramento de imagens, cabeamentos, fornecimento de energia); revisar os processos de controle ainda restantes.

✓ Malware: este perigo representa grau de possibilidade alto e impacto severo. Dentro da ECT, este é o perigo com maior potencial de risco às informações. A ECT faz uso de alguns meios de segurança para prevenir esse tipo de ataque. Os mais destacáveis são: uso de sistemas de prevenção de intrusão (IPS), *firewalls*, *anti-malwares* e métodos de conscientização de usuários internos. Desta forma, o risco associado ao *malware* é aceitável e inerente a qualquer sistema disponível.

✓ Hacking: este perigo representa grau de possibilidade baixo e impacto severo. Assim como com o *malware*, a ECT faz uso de meios de segurança para prevenir

essa forma de ataque. É importante ressaltar que este perigo tem menos probabilidade de ocorrência do que o *malware* por conta de sua baixa incidência de tentativas bem sucedidas no ambiente computacional da ECT.

✓ Desastres naturais: este perigo apresenta grau de possibilidade baixo, mas nos casos de ocorrência, pode gerar impactos moderados no ambiente. Na ECT, boa parte dos equipamentos e sistemas de processamento de informações está instalada numa sala cofre localizada no prédio da Administração Central. Essas instalações são projetadas para serem preparadas contra inundações, fogo e mudanças climáticas. Entretanto, não existe a necessidade de maiores investimentos que minimizem as vulnerabilidades que contribuem para a ocorrência desse perigo. É recomendável revisar periodicamente as instituições físicas e os processos de incidentes relacionados a esse perigo.

✓ Furto de informação: este perigo representa grau de probabilidade baixo e impacto moderado. Na ECT, alguns controles computacionais contribuem para o baixo grau de risco envolvido, são eles: sistema de monitoramento; controle de acesso.

5 CONCLUSÃO

A informação, seja por seu valor estratégico ou histórico, é essencial para o bom percurso dos negócios de qualquer organização. Esse percurso se baseia na busca pela modernização, competitividade, flexibilidade e, principalmente, lucratividade e adaptação ao crescimento.

Considerando o valor estratégico da informação, os seus gestores devem ser eficazes e eficientes para identificar o papel que a informação desempenhará estrategicamente na competição entre organizações.

Neste contexto, a Segurança da Informação exerce função de destaque nas organizações. Seu estudo propicia a implementação de controles de proteção da informação contra diversas formas de ameaças, para garantia da confiabilidade, integridade e disponibilidade da informação, minimizando riscos, direcionando o uso de recursos e melhorando o retorno dos investimentos e oportunidades de negócio.

Entretanto, em algumas organizações é possível perceber que a preocupação com a segurança da informação só está relacionada a investimentos em aparelhos de *hardware* e *software*. Contudo, é possível perceber que nem sempre o que é investido em recursos de tecnologia da informação traz o resultado aspirado. Assim, é precisa uma atenção especial aos processos e aos recursos humanos. O conjunto formado por TI, pessoas e processos constitui-se nos pilares que sustentam a segurança da informação, e, se este conjunto não for balanceado, pode por em risco todo o esforço feito para a proteção dos ativos da informação.

A partir do pressuposto de que não há nenhum sistema completamente seguro e que existem divergências de complexidade e do uso de recursos financeiros para manter os ativos de informação a salvo de ameaças à confidencialidade, integridade e disponibilidade, o foco da gestão com base em riscos específicos é fundamental para a Gestão de Segurança da Informação nas organizações.

Por intermédio da gestão de riscos, é possível conhecer ameaças e vulnerabilidades a que as informações estão sujeitas, bem como os impactos que resultam do comprometimento de sua segurança. Dessa forma, a tomada de decisões sobre o emprego de recursos para proteção de dados corporativos fica mais bem fundamentada e mais confiável.

A informação deve ser protegida de forma adequada, seja ela falada ou registrada em papel ou meio eletrônico. Essa proteção pode ser conseguida através da inserção de políticas, processos, procedimentos, estruturas organizacionais, funções de *hardware* e *software*. Esses meios devem passar por fases de definição, implantação e monitoramento, com o propósito de melhorar procedimentos e permitir que os objetivos sejam atingidos, tanto na parte dos negócios quanto na de segurança da informação.

Com relação à Administração Pública Federal, é conveniente que suas entidades tenham uma metodologia definida sobre gestão de segurança da informação com base em processos de melhorias contínuas. Assim, a inserção de ações de segurança na Administração Pública é justificada no valor da informação para que a prestação de serviços ocorra de forma eficiente e também no interesse da comunidade como beneficiária dos serviços prestados.

No tocante à inserção de conceitos de gestão de riscos à segurança da informação dentro da APF, este trabalho leva a concluir que no tratamento da segurança da informação pela gestão de riscos, os gestores podem relacionar estratégia de negócios e melhor uso de recursos. Isso porque, conhecendo as ameaças, as vulnerabilidades as quais as informações estão passíveis e os impactos de uma falha de segurança, a tomada de decisões objetivadas a proteger dados fica mais confiável e melhor fundamentada.

Diante disso, um dos grandes desafios da APF é determinar até que ponto essas incertezas são toleráveis, tal como o estabelecimento da forma que essas incertezas podem interferir na geração de valores aos interessados.

O uso de métodos de análise de riscos pode ser útil no desempenho dessas tarefas. O método usado neste trabalho é adequado para fundamentar o processo de análise de riscos em segurança da informação na ECT. Isso porque este método é seguro e de simples aplicação.

O uso deste método pode identificar diversos fatores que podem mostrar a ocorrência de perigos que oferecem riscos à confiabilidade, integridade e disponibilidade das informações no ambiente da ECT. Foram estudadas, origens ou causas de impactos e a probabilidade dos seguintes perigos: erro humano, falha de *software*, falha de *hardware*, *malware*, *hacking*, códigos ocultos, desastres naturais, falhas no ambiente físico e furto.

É importante destacar que os perigos analisados podem variar de acordo com a natureza do negócio e a percepção dos gestores e dos usuários da informação na organização. Desta forma, a análise de riscos, por ser contínua, deve considerar diferentes perigos de acordo com o momento vivido e o ambiente da organização.

Foi possível observar, também, que o grau de tolerância a riscos é variável e depende de cada organização. O impacto e a probabilidade de ocorrência do risco podem justificar as ações da gestão para acabar com este perigo.

Diante dessas constatações, é possível concluir que a Gestão de Riscos é uma área desafiadora que assume um papel de fundamental importância para as organizações que a produzem, utilizam e trocam informações num ambiente cada vez mais acirrado pela concorrência e globalização. Entretanto, apesar do uso de recursos de TI no processamento de informações ser um assunto evidente, é preciso considerar os quesitos relacionados aos processos e, principalmente, às pessoas.

5.1 TRABALHOS FUTUROS

A proposta de continuação para este trabalho seria realizar um mesmo estudo proposto neste trabalho em organizações de diferentes segmentos no mercado e confrontar os resultados obtidos com os resultados deste trabalho.

6 REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO 17799, International Organizations Standardization. **Código de pratica para a gestão da segurança da informação**, 2005.

ABNT NBR ISO 27001, International Organizations Standardization. **Sistema de gestão de segurança da informação**, 2006.

ABNT NBR ISO 27005, International Organizations Standardization. **Gestão de riscos de segurança da informação**, 2008.

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. **Gestão da informação: princípios e melhores praticas 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.** São Paulo: Atlas, 2008.

BERNSTEIN,T; BHIMANI, A; SHUTZ, E. **Segurança na Internet.** Rio de Janeiro, 1997.

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.

COBIT 4.1, ***Control Objectives for Information and Related Technology Institute***, 2007.

ECT, Empresa Brasileira de Correios e Telégrafos. **Política de segurança da informação da ECT**, 2001.

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 de 2014.

FERREIRA, A. B. H.; **Novo Aurélio – O dicionário da Língua Portuguesa;** Nova Fronteira, 1999, 3ª Ed.; ISBN 85-209-1010-6; p. 1772.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu, **Política de segurança da informação: Guia prático para embalagem e implementação.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2006.

FONTES, Edison. **Praticando a segurança da informação**. Rio de Janeiro: Brasport, 2010.

ISO/IEC 13335-1:2004, **Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts on models for information and communications technology security management**, 2004.

LYRA, Mauricio Rocha. **Segurança e auditoria em segurança da informação.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

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, 1994.

MENESES, Ulpiano T. Bezerra de. **A crise da memória, história e documento: reflexões para um tempo de transformações.** In: SILVA, Zelia Lopes da. Arquivos, patrimônio e memória: trajetória e perspectivas. São Paulo: Editora UNESP / FAPESP, p. 11-29, 1999.

MOREIRA, Nilton Stringasci. **Segurança mínima: Uma visão corporativa da segurança de informações.** Rio de Janeiro: Axcel Books, 2001.

OLIVEIRA, Wilson José de. **Segurança da Informalção – Técnicas e soluções.** Florianópolis: Editora Visual Books, maio de 2001.

PEIXOTO, Mário César Pintaudi. **Engenharia social e segurança da informação na gestão corporativa**, Rio de Janeiro, Brasport 2006.

ROBREDO, Jaime. **Da ciência da informação revisitada aos sistemas humanos de informação.** Brasília, 2003.

SANTOS, L.A.L. **Engenharia social e Segurança**.pdf. Universidade Tiradentes Aracaju-SE, 2004.

SÊMOLA, Marcos. **Gestão de segurança da informação: visão executiva da segurança da informação.** Rio de Janeiro, 2003.

SÊMOLA, Marcos. **Gestão de segurança da informação: Gestão estratégica da informação e inteligência competitiva.** São Paulo, 2005.

SIANES, Marta. **Compartilhar ou proteger conhecimentos? Grande desafio no comportamento informacional das organizações.** São Paulo, 2005.

TANENBAUM, A. S.: **Redes de Computadores**, Editora Campus, 1994.

ZWICKY, E.; COOPER, S.; CHAPMAN, D.B. ***Building Internet Firewalls***. Sebastpol: O' Reilly, 2000. ISBN 1-56592-871-7; p.859.

ANEXO I – 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 II – ESTRUTURA DA NORMA DE SEGURANÇA DA INFORMAÇÃO NA ECT – MÓDULO 5 DO MANUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (MANTIC)

O Manual de Tecnologia da Informação e Comunicação (MANTIC) tem a função de estabelecer normas, padrões, políticas e procedimentos, gerais e específicos, para a gestão da TIC, relacionado a projetos, gerência e operação nas áreas de redes de computadores, produção, atendimento e suporte, desenvolvimento e manutenção de sistemas de informação e comunicação, funcionamento técnico/operacional e definição dos processos e orientações gerais. O módulo 5 deste manual é dividido em 21 capítulos.

- Capítulo 1 - Administração de Contas de Ambientes Computacionais: define critérios para a criação, alteração, desabilitação e exclusão de contas de usuários, bem como estabelece a política de senhas, de horário para utilização dos recursos de informática, de criação de contas especiais e de utilização do serviço de correio eletrônico.
- Capítulo 2 - Segurança para o 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, documentação, tratamento e segurança da informação.
- Capítulo 3 - 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 - Administração de Estação de Trabalho: estabelece requisitos para manter a integridade e a disponibilidade das estações de trabalho e assegurar a devida proteção das informações nelas armazenadas.
- Capítulo 5 - Operação de Estação de Trabalho: estabelece padrões de segurança para utilização das estações de trabalho.
- Capítulo 6 - Banco de Dados: descreve as condições para a correta configuração, proteção e uso de banco de dados e sua inter-relação com os sistemas.

- Capítulo 7 - 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 - 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 - 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 - Acesso à Internet, Intranet e Extranet: define critérios para administração e utilização dos serviços de Internet, Intranet e Extranet.
- Capítulo 11 - Disponibilizar 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 à prevenção do acesso não autorizado às informações da ECT.
- Capítulo 12 - 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 redes públicas, ou qualquer outro meio de comunicação.
- Capítulo 13 - Segurança de 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 - Segurança da Informação para Usuários de Recursos de TIC: 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 - Detecção de Intrusão 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 – Adoção de Medidas Anti-*spam*: estabelece critérios de gestão de mensagens eletrônicas denominadas *spam*.
- Capítulo 17 - Utilização de Equipamentos de Rede Sem Fio: define critérios para a utilização e administração de equipamentos de rede sem fio.
- Capítulo 18 - 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.
- Capítulo 19 - Utilização de Dispositivos de Armazenamento Removíveis: define o uso de dispositivos de armazenamento removíveis (*pen-drives*, HDs externos e cartões de memória) no ambiente computacional da ECT.
- Capítulo 20 - Gestão de Riscos em Segurança da Informação e Comunicação: define critérios para identificar e implementar medidas de proteção visando minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação da ECT.
- Capítulo 21 - Segurança para Dispositivos Móveis: define maneiras de utilizar dispositivos móveis (smartphones e tablets), corporativo ou particular, para acessar recursos computacionais da ECT, implementando medidas de proteção que visam mitigar os riscos a que estão sujeitos os ativos de informação da ECT.