CENTRO UNIVERSITÁRIO DE BRASÍLIA - UNICEUB
FACULDADE DE TECNOLOGIA E CIÊNCIAS SOCIAIS APLICADAS
CURSO: ADMINISTRAÇÃO
DISCIPLINA: MONOGRAFIA
ÁREA: TECNOLOGIA DA INFORMAÇÃO
PROFESSOR/ORIENTADOR: LEONARDO HUMBERTO SOARES

ESTUDO DE CASO DAS FONTES DE COLETA DE DADOS E DAS POLÍTICAS DE SEGURANÇA ADOTADAS PELA EMPRESA SERVIÇO DE PROTEÇÃO AO CRÉDITO DO BRASIL S/A – CHECK CHECK

Nathália Villela Ventura Guimarães Ferreira
Matrícula nº: 2060137/7

Brasília
JUN/2009

Nathália Villela Ventura Guimarães Ferreira
Matrícula nº: 2060137/7

ESTUDO DE CASO DAS FONTES DE COLETA DE DADOS E DAS POLÍTICAS DE SEGURANÇA ADOTADAS PELA EMPRESA SERVIÇO DE PROTEÇÃO AO CRÉDITO DO BRASIL S/A – CHECK CHECK

Monografia apresentada à Banca Examinadora da Faculdade de Tecnologia e Ciências Sociais Aplicadas como requisito parcial para a obtenção de grau de bacharel no curso de Administração de Empresas do Centro Universitário de Brasília.

Professor/Orientador: Leonardo Humberto Soares.

Brasília/ DF, 10 de junho de 2009.

Nathália Villela Ventura Guimarães Ferreira

ESTUDO DE CASO DAS FONTES DE COLETA DE DADOS E DAS POLÍTICAS DE SEGURANÇA ADOTADAS PELA EMPRESA SERVIÇO DE PROTEÇÃO AO CRÉDITO DO BRASIL S/A – CHECK CHECK

Monografia apresentada à Banca Examinadora da Faculdade de Tecnologia e Ciências Sociais Aplicadas como requisito parcial para a obtenção de grau de bacharel no curso de Administração de Empresas do Centro Universitário de Brasília.

Professor Orientador: Leonardo Humberto Soares

Banca examinadora:

_____
Prof.(a): Leonardo Humberto Soares
Orientador

_____
Prof(a).:
Examinador(a)

_____
Prof(a).:
Examinador(a)

Brasília/ DF, 10 de junho de 2009.

Dedico este trabalho aos meus pais, Fernando e Patricia, e à minha irmã, Aline, que estiveram presentes em todas as etapas da minha vida, e que significantemente contribuíram para a minha formação pessoal e acadêmica.

Agradeço:

A Deus, que me iluminou e me deu forças em todos os momentos;

Ao professor orientador Leonardo Humberto Soares o estímulo, a atenção e a confiança depositada em mim;

Ao Diretor de TI da Empresa SPCB – Check Check, Adriano Sérgio Rodrigues de Souza, a disponibilidade em me fornecer os dados necessários a essa pesquisa;

Ao meu namorado Luís Carlos Martins Leão e à minha querida amiga Ana Carla Braga Mendonça a paciência e a ajuda.

Os computadores são incrivelmente rápidos, precisos e burros; os homens são incrivelmente lentos, imprecisos e brilhantes; juntos, seu poder ultrapassa os limites da imaginação.

Albert Einstein

RESUMO

Desde a criação da primeira calculadora mecânica em 1642, foram necessários quase duzentos anos para que o computador fosse projetado. No entanto, o ENIAC, primeiro computador digital de grande escala, somente foi desenvolvimento no ano de 1946, e o primeiro computador pessoal, em 1981. A partir dessa data, as tecnologias evoluíram significativamente, com o advento da *internet*, cuja primeira conexão de longa distância foi realizada em 1995, que culminou na criação dos provedores de acesso privado. Nos últimos dez anos, o número de usuários cresceu de dois milhões e meio para dezoito milhões. Devido a esse expressivo número de internautas, os dados que trafegam na *internet* também aumentaram. As várias questões relativas à segurança dessas informações e a preocupação crescente com a privacidade suscitaram a elaboração do problema no qual se baseou esta pesquisa. O trabalho apresenta um estudo de caso realizado na empresa Serviço de Proteção ao Crédito do Brasil S/A – Check Check, a qual lida com a problemática da segurança diariamente, visto que o processo de negócio da organização é vinculado à prestação de consultas e, por esse motivo, informações são ativos vitais ao seu funcionamento. Verificou-se que existe na empresa uma preocupação em manter o sigilo das informações disponibilizadas, bem como os princípios básicos de segurança, quais sejam confidencialidade, disponibilidade e integridade. No entanto, existem lacunas nos planos de contingência que a organização possui, as quais podem transformar-se em graves ameaças.

Palavras-chave: Tecnologia, Informação, Segurança da Informação.

SUMÁRIO

1. INTRODUÇÃO

Em 12 de agosto de 1981, a IBM lançou no mercado o primeiro computador pessoal (PC), o IBM 5150 (IBM, 2009), que representava uma realidade completamente diferente do ENIAC (*Eletrical Numerical Integrator and Calculator*), computador desenvolvido em 1946, que pesava cerca de trinta toneladas, ocupava um espaço de 180 m² e necessitava de sessenta pessoas para operá-lo (TERRA, 2006).

Rapidamente, os PC's se popularizaram, principalmente após o advento da *internet*, que surgiu oficialmente no Brasil em 1989. Em 1995, foi autorizada a operação comercial no país, com a criação dos provedores de acesso privado à rede. A partir de então, essa passou rapidamente a ser utilizada por milhões de brasileiros. Entre 1999 e 2009, o número de usuários cresceu 732%, passando de dois milhões e quinhentos mil internautas para dezoito milhões e trezentos (TERRA, 2009).

Com o significativo número de pessoas que utilizam a *internet* atualmente, não só como meio de pesquisa, mas para compras e operações bancárias, cresceu também o número de informações que trafegam no sistema. Alguns desses dados, no entanto, são sigilosos e requerem que sejam aplicados mecanismos de segurança que evitem o acesso por parte de usuários indesejados.

A empresa Serviço de Proteção ao Crédito do Brasil S/A (SPCB) – Check Check, presente em dois mil e cem municípios, possui um banco de dados com aproximadamente trezentos e cinqüenta milhões de registros, que gera, mensalmente, cerca de cinco milhões de consultas (CHECK CHECK, 2009). Por trabalhar diretamente com dados cadastrais, que devem ser mantidos em sigilo, é uma das muitas organizações que lidam diariamente com a problemática da segurança e da privacidade das informações. Nesse contexto, surgem perguntas: Como gerir essas informações? Que mecanismos devem ser utilizados na coleta, armazenamento, manutenção e transporte desses dados? Como manter essas informações em sigilo e garantir o direito à privacidade dos clientes?

Essas perguntas levaram à formulação do problema desta pesquisa: As políticas de segurança, coleta, manuseio, armazenamento e transporte de dados da empresa SPCB – Check Check mostram-se condizentes com as expectativas do mercado?

O objetivo geral deste estudo de caso é investigar se as fontes de coleta de dados e as políticas de segurança adotadas pela empresa SPCB – Check Check garantem a confidencialidade, a disponibilidade e a integridade das informações. Os objetivos específicos que se fazem presentes são: (a) Explanar, teoricamente, sobre as principais políticas de segurança da informação existentes; (b) Comparar as práticas exercidas pelo SPCB – Check Check para manter a segurança e o sigilo das informações com essas políticas; e (c) Analisar os dados obtidos à luz das teorias de base utilizadas.

Devido à escassez de estudos realizados sobre o tema em questão, academicamente, os resultados obtidos com esta pesquisa contribuirão para estudos futuros na área. Além disso, a revisão de literatura que fundamentou esse estudo e a análise e discussão dos dados serão de fundamental importância para auxiliar pesquisadores cujo interesse esteja voltado para o tema proposto.

Gerencialmente, os resultados dessa pesquisa poderão auxiliar gestores de empresas de informações cadastrais na otimização de procedimentos ou na implantação de novos métodos para assegurar a privacidade e segurança dos dados tratados por essas organizações, contribuindo, assim, para a qualificação e aperfeiçoamento de diretivas de gestão na segurança de TI. O estudo também contribuirá para a empresa em análise, visto que possibilitará um retorno das atividades realizadas.

Para a realização desta pesquisa, adotou-se o método dedutivo. Quanto aos fins, trata-se de uma pesquisa exploratória, com características descritivas. Quanto aos meios de investigação, a pesquisa classifica-se como estudo de caso, bibliográfica e documental. O estudo é qualitativo, e como técnicas foram utilizadas a observação simples e a entrevista semi-estruturada.

O presente estudo de caso está dividido em cinco partes: Introdução, Embasamento Teórico, Método, Estudo de Caso, e Conclusão. A Introdução aborda as justificativas para escolha do tema, assim como o problema e os objetivos que fundamentaram esse estudo. O Método engloba a metodologia utilizada na elaboração da pesquisa. O Embasamento Teórico, por sua vez, apresenta as teorias utilizadas na análise dos dados. As duas últimas partes oferecem os resultados, analisados com base nas teorias adotadas, e as conclusões dessa pesquisa, respectivamente.

2. EMBASAMENTO TEÓRICO

Visto que o estudo realizado visa a averiguar se as fontes de coleta de dados e as políticas de segurança adotadas pela empresa em análise garantem a confidencialidade, a disponibilidade e a integridade das informações, fez-se necessária a construção de uma revisão de literatura que abordasse os temas segurança da informação, gestão da informação e privacidade, os quais são explicitados neste capítulo. Primeiramente, o capítulo apresenta um breve histórico da evolução da tecnologia, seguido das definições e classificações de informação.

2.1 Histórico e Evolução da Tecnologia

Nos primórdios, baseado na necessidade de se fazerem cálculos mais complexos, foi criado o ábaco. Acredita-se que ele tenha origem em torno do ano de 3500 a.C. No entanto, foi somente no ano de 1642 d.C que o francês Blaise Pascal desenvolveu a primeira calculadora mecânica, que efetuava apenas operações de soma e subtração, para auxiliá-lo nos cálculos de contabilidade. Trinta anos mais tarde, em 1672, o alemão Gottfried Wiilhelm von Leibnitz aperfeiçoou a calculadora de Pascal, permitindo a realização de contas de multiplicação e divisão (NASCIMENTO, 2002).

Até aquele momento, a tecnologia existia para auxiliar nos cálculos; não era aplicada aos afazeres. Foi apenas em 1801 que o francês Joseph-Marie Jacquard começou a utilizar cartões perfurados para automatizar os teares, um marco na programação. A partir de então, a tecnologia deixou de estar atrelada somente aos cálculos e passou a ser aplicada, também, na produção de bens (NASCIMENTO, 2002).

Após vinte e um anos, em 1822, o inglês Charles Babbage projetou um computador mecânico, o qual nunca foi executado. No ano de 1854, o matemático George Boole desenvolveu o sistema binário[1], que, aparentemente, não possuía utilidade, mas, anos mais tarde, tornar-se-ia a base matemática dos computadores. E em 1885, o norte-americano Herman Hollerith criou um processador

[1] Sistema numérico que utiliza apenas os dígitos 0 (zero) e 1 (um) (ASKOXFORD.COM, 2009).

eletromecânico que inseria os dados a partir de cartões perfurados, lembrando a forma com que eram usados nas máquinas de tear (NASCIMENTO, 2002).

Apenas em 1930, foi desenvolvido por Vannevar Buch, um engenheiro eletricista norte-americano, um computador que usava válvulas de rádio. Entretanto, foram necessários mais dezesseis anos para que os engenheiros norte-americanos John William Mauchly e John Presper Eckart Jr. criassem o primeiro computador eletrônico, o ENIAC (SUA PESQUISA.COM, 2009).

Em 1966, a IBM lançou o Ramac 305, com disco de memória com capacidade de 5Mb. A Intel, no ano de 1971, criou o MCS-4, primeiro microcomputador pessoal. Em 1985, a Microsoft, dez anos após sua fundação, projetou o sistema operacional Windows; e, em 1989, um pesquisador europeu desenvolveu a *Word Wide Web* (w.w.w), origem da *internet* (SUA PESQUISA.COM, 2009).

2.2 Informação

Antes de se definir o que é segurança da informação – seus princípios e sua importância para as organizações – e os meios corretos de gerir esses dados, de forma a garantir o direito à privacidade dos clientes, é vital que se compreenda, primeiramente, o que é informação.

A Academia Brasileira de Normas Técnicas (ABNT) define informação como “um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização, e conseqüentemente necessita ser adequadamente protegida” (ABNT, 2005, p. ix).

Complementar a essa idéia, Lino (2005, p. 27) defende que informação é um ativo digital de grande valor, presente em todos os processos de qualquer empresa, independentemente do ramo de atuação, e que representa vantagens competitivas.

Foina (2009, p. 2-3) sustenta que toda informação possui quatro faces complementares, que foram se agregando ao longo das últimas décadas: valor, conceito, referência e unidade. Dessa forma, o autor define formalmente informação como:

> um dado (ou valor) associado a um conceito claro, não ambíguo e de conhecimento de todos os interessados, que seja acompanhado de uma referência para efeito de comparação e possa trazer vantagens competitivas para a organização (FOINA, 2009, p. 2-3).

Ademais, para que haja unidade quanto às informações, é necessário que todas as pessoas interessadas possuam as mesmas referências e conceitos. Além disso, um dado só passa a ser informação se possuir utilidade, que é atribuída por quem dele faz uso. Caso contrário, esse dado deve ser descartado, para facilitar a tomada de decisões (FOINA, 2009, p. 3).

Laudon e Laudon (2004, p. 7) também diferenciam informações de dados alegando que as informações são “dados apresentados de forma significativa e útil para os seres humanos”. Em contrapartida, os dados são provenientes de fatos brutos que ainda não foram tratados de forma analítica, de modo a se tornarem compreensíveis às pessoas neles interessadas (LAUDON; LAUDON, 2004, p. 7).

De forma simplificada, Sêmola (2003, p. 45) afirma que informação é “um conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (...) ou transacionais (...)”. O autor destaca, também, em conformidade com Lino (2005, p. 27) e Foina (2009, p. 2-3), que as informações são ativos críticos para o desenvolvimento e continuidade da organização, por se tratarem da inteligência competitiva dos negócios.

Por ser extremamente valiosa e vital para a fluência dos processos que mantêm as operações da empresa, é necessário cuidado em todos os momentos vividos pela informação que podem colocá-la em risco, ou seja, em todas as etapas de seu ciclo de vida, que correspondem ao manuseio, armazenamento, transporte e descarte (SÊMOLA, 2003, p. 9). Entende-se que a inobservância de qualquer uma dessas fases pode ocasionar perdas irreparáveis.

A primeira etapa, o manuseio, corresponde à criação e manipulação da informação. Em seguida, tem-se o armazenamento, que pode ser feito por meio físico – arquivamento de papéis –, ou digital – banco de dados eletrônico. A fase seguinte, o transporte, é a saída da informação do local originário em que estava armazenada, o que pode ser feito via fax, telefone, correio eletrônico, ou até oralmente. Por fim, quando os dados já não possuem valor para a organização, chegam ao estágio final, que é o descarte (SÊMOLA, 2003, p. 10).

Em oposição aos autores anteriormente citados, Laureano e Morais (2005, p. 3) defendem que “nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais”. Dessa forma, Wadlow e Abreu (2000; 2001 apud LAUREANO; MORAIS, 2005, p. 3) classificam as informações em quatro categorias, de acordo

com o nível de prioridade para as organizações: pública, interna, confidencial e secreta.

A informação pública é aquela cuja integridade não é crítica e, sendo assim, pode tornar-se pública sem prejudicar o funcionamento da empresa. Informações internas, ao contrário, devem ter o livre acesso evitado; porém, a visualização por pessoal não autorizado não traz problemas graves à organização. Informações confidenciais devem limitar-se ao ambiente interno da firma, e o acesso por pessoas indevidas pode trazer prejuízos. Por fim, informações secretas são vitais ao funcionamento da organização e, por essa razão, o acesso a essas deve limitar-se a um pequeno grupo de pessoas. (WADLOW; ABREU, 2000; 2001 apud LAUREANO; MORAIS, 2005, p. 3)

Como tudo dentro da empresa gira em torno do valor atribuído às informações, estas devem ser adequadamente resguardadas (LINO, 2005, p. 27). Para tanto, conclui-se que é de fundamental importância que haja meios de assegurar que as informações e os recursos envolvidos com essas estejam protegidos, tanto de ameaças internas, quanto externas.

2.3 Gestão da Informação (G.I.)

Maximiano (2005, p. 6) define o termo administrar, ou gerir, como o processo de se tomar decisões, que envolvem planejar, organizar, executar e controlar, acerca de objetivos e do modo de se utilizar os recursos disponíveis na organização.

De acordo com Greewood (apud BRAGA, 1996, p. 2), todo processo decisório tem como ingrediente básico a informação. Dessa maneira, o fluxo de informações e as fontes de onde esses dados provêm podem determinar o limiar entre eficiência e ineficiência, e, portanto, necessitam ser geridos (BRAGA, 1996, p. 2-3).

Segundo Reis (1993 apud BRAGA, 1996, p. 3),

> para que esta gestão seja eficaz, é necessário que se estabeleçam um conjunto de políticas coerentes que possibilitem o fornecimento de informação relevante, com qualidade suficiente, precisa, transmitida para o local certo, no tempo correto, com um custo apropriado e facilidades de acesso por parte dos utilizadores autorizados.

Sendo assim, é possível concluir que o principal objetivo da gestão da informação é assegurar que informações corretas, provenientes de fontes fidedignas e seguras, sejam disponibilizadas às pessoas certas – as que necessitam dessas informações para a tomada de decisões –, no momento exato em que são necessárias.

Nesse contexto, Patrícia Marchiori (2002, p. 73) complementa que a gestão da informação exige não somente a utilização de tecnologias adequadas, como também um misto de artifícios gerenciais. Da mesma forma, Wilson (1989, apud BRAGA, 1996, p. 3) entende a G.I. como “a gestão eficaz de todos os recursos de informação relevantes para a organização, tanto de recursos gerados como os produzidos externamente e fazendo apelo, sempre que necessário, à tecnologia da informação”.

Sob esta perspectiva, Ponjuán Dante (1998, apud MARCHIORI, 2002, p. 74) defende que

> a gestão da informação deve incluir, em dimensões estratégicas e operacionais, os mecanismos de obtenção e utilização de recursos humanos, tecnológicos, financeiros, materiais e físicos para o gerenciamento da informação e, a partir disto, ela mesma ser disponibilizada como insumo útil e estratégico para indivíduos, grupos e organizações.

Zorrinhos (1995, p. 146, apud BRAGA, 1996, p. 3) afirma que “gerir a informação é (...) decidir o que fazer com base em informação (...) e sobre informação”. Para o autor, a gestão da informação consiste na capacidade gerencial de escolher, dentre todas as informações disponíveis na organização, aquelas que são relevantes para a tomada de determinada decisão.

Braga (1996, p. 3-4) defende que, para que os recursos disponíveis sejam utilizados de maneira eficiente e, assim, os objetivos sejam alcançados, as informações alocadas aos níveis estratégico, tático e operacional devem ser diferentes. Como o nível estratégico é responsável pela tomada de decisões complexas, as informações devem ser bastante variadas, mas não são muito específicas. O nível tático demanda informações um pouco mais detalhadas, disponibilizadas com freqüência alta. No nível operacional, como as decisões são

pontuais, as informações devem ser bastante específicas e devem ser obtidas, prioritariamente, do ambiente interno da organização (BRAGA, 1996, p. 3-4).

Para uma gestão eficaz, Braga (1996, p. 4) alega que a empresa deve utilizar Sistemas de Informação adequados às necessidades da organização. Esses irão apoiar o processo decisório na medida em que articulam os vários departamentos e sistemas da empresa e processam os dados provenientes de diversas fontes, propiciando informações úteis, em tempo real (BRAGA, 1996, p. 4).

2.4 Sistemas de Informação (S.I.)

Laudon e Laudon (2004, p. 7) definem sistema de informação como “um conjunto de componentes inter-relacionados que coleta (ou recupera), processa, armazena e distribui informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização”. Ademais, o autor defende que os sistemas de informação também auxiliam na análise de problemas e na visualização de assuntos complexos.

Braga (1996, p. 4) complementa a definição de Laudon e Laudon (2004, p. 7) ao afirmar que os sistemas de informação são “um conjunto de meios humanos e técnicos, dados e procedimentos, articulados entre si, com vista a fornecer informação útil para a gestão das atividades da organização onde está inserido”.

Para que os S.I. gerem as informações necessárias à tomada de decisão, três atividades se fazem presentes: a entrada, o processamento e a saída. A entrada corresponde à etapa de coleta de dados brutos, que podem ser provenientes do ambiente interno ou externo da empresa. O processamento consiste em transformar os dados brutos em informações significativas e úteis. A saída refere-se à transferência das informações às pessoas ou atividades que delas farão uso. Por fim, é necessário que haja um *feedback*, para auxiliar os gestores a avaliar ou corrigir o processo de entrada (LAUDON; LAUDON, 2004, p. 7-8).

Os S.I. podem representar vantagens competitivas para as organizações ao permitirem a oferta de produtos e serviços com valores menores, possibilitarem a fidelização de clientes, o desenvolvimento ou diferenciação de produtos, e a criação de barreiras à entrada de novos concorrentes no setor (BRAGA, 1996, p. 5-6). No entanto, Laudon e Laudon (2004, p. 25-28) afirmam que a implantação dos S.I. não é simples e, para que aconteça, os administradores enfrentam cinco desafios:

desafio estratégico das organizações, desafio da globalização, desafio da arquitetura e infra-estrutura da informação, desafio do investimento, e desafio da responsabilidade e do controle.

O desafio estratégico corresponde à necessidade de planejamento e reestruturação da empresa para obter vantagens reais com a implantação das tecnologias de informação. O desafio da globalização relaciona-se ao entendimento dos gestores em relação às exigências do cenário econômico global. Já o desafio da arquitetura e infra-estrutura da informação demanda o desenvolvimento de uma arquitetura e infra-estrutura tecnológica que apóiem os objetivos e funcionamento dos processos da organização. O desafio do investimento corresponde à dificuldade de se determinar o valor real dos S.I. para a empresa. E, por fim, o desafio da responsabilidade e do controle está relacionado com a utilização dos S.I. de maneira socialmente responsável, e com os problemas enfrentados com segurança e controle dos S.I. (LAUDON; LAUDON, 2004, p. 26-28).

É importante ressalvar que a gestão da informação, com o auxilio dos Sistemas de Informação e das Tecnologias de Informação e Comunicação, além de se preocupar com a segurança das informações que circulam na empresa, deve ater-se ao fato de que nem toda informação pode estar disponível a toda pessoa que dela queira fazer uso. Dessa forma, entende-se que é essencial que as organizações levem em consideração os princípios legais que tratam sobre a privacidade e criem políticas para assegurar que apenas os indivíduos autorizados tenham acesso a determinados dados.

2.5 Segurança da Informação

Sêmola (2003, p. 43) atesta que a segurança da informação é um campo do conhecimento que se dedica a impedir o acesso de pessoas não autorizadas e alterações indevidas às informações, garantindo que riscos que possam vir a comprometer qualquer dos três principais conceitos de segurança sejam minimizados.

De acordo com Krause e Albuquerque (1999; 2002, apud LAUREANO; MORAES, 2005, p. 4), em conformidade com Sêmola (2003, p. 43) e Fontes (2000, p. 21), os três principais conceitos que regem a segurança da informação são a confidencialidade, a disponibilidade e a integridade. Esses princípios são

interdependentes, o que significa que a violação de qualquer um deles diminui a eficiência da segurança das informações da organização (LINO, 2005, p. 30).

Edison Fontes (2000, p. 21) afirma que a confidencialidade refere-se ao uso exclusivo da informação por pessoas autorizadas. O princípio da disponibilidade rege que a informação deve estar acessível a todos que dela fazem uso, no momento em que é necessária (SÊMOLA, 2003, p. 45). A integridade, por fim, sugere que “a informação deve estar correta, ser verdadeira e não estar corrompida” (FONTES, 2000, p. 21).

Existem, ainda, outros critérios que devem ser respeitados pelos sistemas que gerenciam as informações para que elas sejam consideradas seguras. Esses critérios são a autenticidade – processo que garante que o usuário e as informações são autênticos –, o não-repúdio – a certeza de que não foi realizada nenhuma operação que modificasse a informação –, a legalidade – a informação e o uso desta estão em conformidade com as leis –, a privacidade – que garante que somente a pessoa a quem a informação se refere tenha acesso a essa – e a auditoria – que possibilita o rastreamento de todos os passos de um processo (LAUREANO; MORAES, 2005, p. 4-5).

Sêmola (2003, p. 43) afirma, também, que a segurança da informação é responsável pela criação e definição de normas que visem ao controle e à identificação das vulnerabilidades e de possíveis ameaças a qualquer estágio do ciclo de vida da informação.

A ABNT complementa a tese de Sêmola (2003, p. 43) ao alegar que a segurança da informação é responsável por proteger as informações de diversos tipos de ameaças, contribuindo para a diminuição dos danos às organizações e aumento das oportunidades de negócio, maximizando o retorno dos investimentos (ABNT, 2005, p. ix).

Ameaças são definidas como

> agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, conseqüentemente, causando impactos aos negócios de uma organização (SÊMOLA, 2003, p. 47).

Quanto à intencionalidade, Sêmola (2003, p. 47-48) as classifica como naturais – decorrentes de fenômenos da natureza – involuntárias – "(...) inconscientes, quase sempre causadas pelo desconhecimento" – e voluntárias – "ameaças propositais causadas por agentes humanos".

Vulnerabilidade, por sua vez, é uma "fragilidade presente ou associada a ativos que manipulam e/ou processam informações que (...) permite a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação (...)" (SÊMOLA, 2003, p. 48). São subdivididas em sete grupos:

> **FÍSICAS** - Instalações prediais fora do padrão, salas de CPD mal planejadas, falta de extintores, detectores de fumaça e de outros recursos para combate a incêndio em sala com armários e fichários estratégicos, risco de explosão, vazamentos ou incêndio;
> **NATURAIS** – Enchentes, terremotos, tempestades, acúmulo de poeira, umidade, tempestades eletrostáticas, etc;
> ***HARDWARE***[2] – Desgastes, obsolescência, má utilização ou erros de instalação;
> ***SOFTWARE***[3] – Erros na instalação ou na configuração causando vazamento de informações, acessos indevidos, perda de dados e indisponibilidade dos recursos;
> **MÍDIAS** – Danificação de discos rígidos e fitas pelo mau uso, armazenamento ou transporte e perda de relatórios e impressões;
> **COMUNICAÇÃO** – Acessos não autorizados ou perda de comunicação;
> **HUMANAS** – Falta de treinamento e conhecimento da necessidade de segurança das informações, compartilhamento indevido de informações críticas ou confidenciais, erros ou omissões, sabotagens, vandalismo, roubo, etc.
> (SÊMOLA, 2003, p. 48-49).

O autor complementa que as vulnerabilidades são elementos passivos, e só provocam acidentes se estiverem ligadas, necessariamente, a um agente causador ou a uma ameaça, que é condição favorável para ocorrência do incidente (SÊMOLA, 2003, p. 48).

Para minimizar riscos – probabilidade de que vulnerabilidades sejam exploradas e tornem-se ameaças às empresas, provocando violações nos princípios básicos de segurança – existem algumas práticas e mecanismos que podem ser

---

[2] "Máquinas, instalações elétricas, e outros componentes físicos de um computador" (ASKOXFORD.COM, 2009, tradução nossa).
[3] "Programas e informações operacionais utilizadas por um computador" (ASKOXFORD.COM, 2009, tradução nossa).

utilizados. São as denominadas medidas de segurança, as quais se dividem em preventivas, detectáveis e corretivas (SÊMOLA, 2003, p. 50).

Sêmola (2003, p. 50) defende que as medidas de segurança preventivas são aquelas que visam a evitar a ocorrência de incidentes. As medidas detectáveis são as que têm por objetivo identificar os indivíduos ou condições que possam ocasionar ameaças. Por último, as medidas de segurança corretivas são aplicadas para adaptar as estruturas tecnológicas e humanas já existentes às políticas e técnicas de segurança adotadas pela organização.

Lino (2005, p. 29) alega que é necessário mais que "um conjunto de ferramentas de *software* e *hardware*" para alcançar um nível aceitável de segurança. As organizações devem elaborar planos de segurança que estejam em conformidade tanto com o nível estratégico, como o tático e o operacional, de forma a garantir resultados mais eficazes com relação à segurança das informações (LINO, 2005, p. 29).

Sêmola (2003, p. 98-99) complementa que as organizações devem formalizar o Plano de Continuidade de Negócios, que terá por objetivo "contingenciar situações e incidentes de segurança que não puderem ser evitados", a fim de minimizar os impactos e possibilitar a continuidade dos processos e das informações. O autor ainda afirma que não existe um plano único, mas diversos planos integrados, cada um com foco específico em uma área.

A primeira etapa da elaboração desse Plano é a análise de impactos, mundialmente conhecida pela sigla BIA (*Business Impact Analysis*), que consiste em determinar o grau de importância das atividades e processos para a continuidade do negócio, e mapear todos os ativos necessários a essas atividades, para então definir possíveis impactos caso haja paralisação total ou parcial. Com a análise BIA concluída, podem-se determinar as prioridades de contingência (SÊMOLA, 2003, p. 100).

A etapa seguinte consiste em definir estratégias de contingência. Estas podem ser: ***hot-site*** – estratégia para objetos com pouco ou nenhum tempo de tolerância a falhas; ***warm-site*** – para objetos com maior tolerância à paralisação; ***cold-site*** – para objetos com grande tolerância de indisponibilidade; **realocação de operação** – alocar a atividade atingida para outro equipamento ou ambiente físico, dentro da própria empresa; ***bureau* de segurança** – alocar a atividade atingida para um ambiente terceirizado; e **auto-suficiência** – para impactos não-significativos, ou

para empresas com alto padrão de estrutura que não necessitam de outras estratégias (SÊMOLA, 2003, p. 102-103, grifo nosso).

Para finalizar, são elaborados planos de contingência “para cada ameaça considerada em cada um dos processos pertencentes ao escopo, definindo em detalhes os procedimentos a serem executados em estado de contingência”. Os planos de contingência são subdivididos em três módulos, quais sejam plano de administração de crise, plano de continuidade operacional e plano de recuperação de desastres, e todos devem ser severamente testados para garantir a eficiência (SÊMOLA, 2003, p. 103-105).

Sêmola (2003, p. 104) defende que o plano de administração de crise define todos os passos a serem adotados pelas “equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente”, e os procedimentos para que as operações retornem à normalidade. O plano de continuidade operacional refere-se ao “contingenciamento dos ativos que suportam cada processo de negócio”. Por fim, o autor alega que o plano de recuperação de desastres visa a definir as táticas para recuperação e restauração dos ativos afetados.

Fontes (2000, p. 57-60) complementa que, para que se entenda e planeje melhor o Plano de continuidade do negócio, cinco aspectos devem ser considerados. O primeiro refere-se aos recursos a serem contemplados. Nesse aspecto, o autor afirma que a solução de contingência deve abranger todos os ativos da organização, tecnológicos e não tecnológicos. Em seguida, devem-se estabelecer prioridades, uma vez que, para garantir a continuidade do negócio, é necessário que haja recursos financeiros. Sendo assim, entende-se que é vital determinar em que serão gastos os recursos financeiros.

Definir o escopo – que recursos, áreas e situações de desastre serão contemplados no Plano –, com base nos recursos financeiros disponíveis, é outro aspecto relevante. Além disso, é necessário avaliar as opções de que a empresa dispõe para recuperação de recursos, considerando-se o custo-benefício. Por fim, é necessário que a solução implantada seja continuamente testada e que existam procedimentos de manutenção (FONTES, 2000, p. 58-59)

Como “o processo de segurança da informação na organização envolve aspectos técnicos, humanos e organizacionais” (FONTES, 2000, p. 107) é importante que exista, também, uma política de segurança para normatizar o

comportamento dos ativos humanos. A política de segurança da organização deve especificar a todos os usuários a filosofia da empresa acerca das investidas em segurança (FONTES, 2000, p. 107).

Sêmola (2003, p. 105) afirma que a política de segurança tem o objetivo de apoiar as ações dos administrados relativas à segurança. Por ser muito abrangente, é subdividida em diretrizes, normas, e procedimentos e instruções, para os níveis estratégico, tático e operacional, respectivamente.

As diretrizes comunicam aos colaboradores a importância dada às informações, os valores da organização, e as ações que orientarão as atividades daqueles. As normas norteiam a utilização das informações e detalham todas as situações e processos envolvidos na segurança. Por último, os procedimentos e instruções, presentes em maior número, dado seu caráter operacional, devem "descrever meticulosamente cada ação e atividade associada a cada situação distinta de uso das informações" (SÊMOLA, 2003, p. 105-107).

Fontes (2000, p. 107-108) defende que, para que a política seja respeitada, esta deve possuir algumas características. Entre elas, a política deve ser verdadeira – ser coerente com o pensamento e ações da empresa –; deve ser assinada pela direção, demonstrando o apoio dessa; deve definir todas as regras e controles de acesso, diferenciando-se, assim, de um manual; não deve ser um documento técnico, com definições técnicas; e deve ser simples, para ser compreendida por todos.

2.6 NBR ISO/IEC 17799:1

A NBR ISO/IEC 17799:1 é a Norma criada pela ABNT que "estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização" (ABNT, 2005, p. 1).

A norma ABNT – ISO/IEC 17799:1 é dividida em doze seções: onze seções de controle de segurança da informação, subdivididas em categorias, totalizando trinta e nove, e uma seção introdutória (ABNT, 2005, p. 4). Abaixo, estão listadas as seções de controle de segurança, com os respectivos objetivos.

a) **Política de Segurança da Informação:** “Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes” (ABNT, 2005, p. 8).

b) **Organizando a Segurança da Informação:** “Gerenciar a segurança da informação dentro da organização e manter a segurança dos recursos (...) que são acessados, processados, comunicados ou gerenciados por partes externas” (ABNT, 2005, p. 10-15).

c) **Gestão de Ativos:** “Alcançar e manter a proteção adequada dos ativos da organização e assegurar que a informação receba um nível adequado de proteção” (ABNT, 2005, p. 21-23).

d) **Segurança em Recursos Humanos:** “Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis”; que adotem política de segurança de informação da empresa no desenvolvimento das tarefas habituais; e que “deixem a organização ou mudem de trabalho de forma ordenada (ABNT, 2005, p. 25-29).

e) **Segurança Física e do Ambiente:** “Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização”, além de “perdas, (...) furto ou comprometimento de ativos e interrupção das atividades (...)” (ABNT, 2005, p. 32-35).

f) **Gestão das Operações e Comunicações:** “Garantir a operação segura e correta dos recursos de processamento da informação” (ABNT, 2005, p. 40).

g) **Controle de Acesso:** “Controlar acesso à informação” (ABNT, 2005, p. 65).

h) **Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação: “**Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações; e proteger a confidencialidade, a autenticidade ou a integridade das informações (...)” (ABNT, 2005, p. 85-87).

i) **Gestão de Incidentes de Segurança da Informação:** “Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil” (ABNT, 2005, p. 98).

j) **Gestão da Continuidade do Negócio:** “Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou

desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso" (ABNT, 2005, p. 103).

k) **Conformidade:** "Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação" (ABNT, 2005, p. 108).

É possível deduzir que, em um futuro próximo, esta Norma deve tornar-se um selo de qualidade para a área de Tecnologia. Dessa maneira, as organizações poderão exigir de seus parceiros e fornecedores que se adéqüem aos padrões estabelecidos na NBR ISO/IEC 17799.

2.7 Privacidade de Dados

Após a Segunda Guerra Mundial, o termo privacidade passou a estar presente em muitas declarações internacionais de direitos, citado pela primeira vez na Declaração Americana de Direitos e Deveres do Homem, em 1948. A Assembléia Geral das Nações Unidas aprovou, ainda em 1948, a Declaração Universal dos Direitos do Homem, na qual constava o direito à privacidade. O termo também foi mencionado em 1950 na Convenção Européia dos Direitos do Homem; em 1969 na Convenção Americana dos Direitos do Homem; e em 2000 na Carta dos Direitos Fundamentais da União Européia (DONEDA, 2006, p. 9).

No Brasil, o direito à privacidade foi assegurado na Constituição da República Federativa promulgada em cinco de outubro de 1988, em seu artigo quinto, inciso X, o qual determina que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 2007, p. 6).

Uadi Lâmego Bulos (apud DEZEN JUNIOR, 2006, p. 37) atesta que a intimidade é "o modo de ser do indivíduo que consiste na exclusão do conhecimento alheio de tudo quanto se refere ao mesmo indivíduo". Fundamentado na proteção da intimidade, o inciso XII do artigo 5º afirma que:

> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, **de dados** e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei

> estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 2007, p. 6, grifo nosso).

Em decorrência do explicitado no inciso supracitado, e para o contexto organizacional, a privacidade de dados, ou informações, é, para Alan Westin (1987, apud ISHITANI, 2003, p. 5), definida como “a reivindicação de indivíduos, grupos ou instituições de poderem determinar quando, como e quanto de suas informações podem ser divulgadas a outros”. Wang, Lee e Wang (1998, apud ISHITANI, 2003, p. 5) completam ao afirmar que “invasão de privacidade é geralmente interpretada como coleta, publicação ou outro uso não-autorizado de informações pessoais (...)”.

A ABNT, na norma que regulamenta as práticas de segurança da informação, NBR ISO/IEC 17799, determina que a privacidade e a proteção dos dados pessoais devem ser garantidas conforme exigidos nas legislações, e que as empresas implantem políticas de privacidade. Ademais, afirma que existem países que já estão adotando políticas de controle na coleta, processamento e transmissão daqueles dados (NBR ISO/IEC 17799, 2005, p. 110).

O Decreto 3535/2000, o qual fundamenta a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, regulamenta, no Brasil, a privacidade de dados. No entanto, essa norma específica se aplica apenas à Administração Pública, não atingindo outras esferas, como a Administração Privada (ALMEIDA FILHO, p. 2-3).

Visto que preocupações com a privacidade existem em qualquer lugar onde informações pessoais são coletadas e armazenadas, faz-se necessária a criação e adoção de políticas de privacidade também nas organizações da esfera privada.

O maior desafio das empresas de dados cadastrais nesse âmbito, portanto, é recolher e compartilhar informações, mantendo a segurança e a privacidade dos dados disponibilizados por seus clientes.

3. MÉTODO

Este capítulo aborda o método desta pesquisa, definido por Lakatos e Marconi (2003, p. 83) como o “conjunto de atividades sistemáticas e racionais que (...) permite alcançar o objetivo (...), traçando o caminho a ser seguido (...)”. Apresenta, de forma detalhada, o tipo de pesquisa e as técnicas utilizados no desenvolvimento deste estudo.

O método científico adotado foi o dedutivo, o qual parte de premissas tidas como verdadeiras, permitindo inferências conclusivas sobre o assunto, decorrentes única e exclusivamente da sua lógica (GIL, 2007). Neste estudo, utilizaram-se as teorias apresentada no embasamento teórico para verificar a incidência dos fenômenos abordados na unidade de negócio específica.

Adotando a taxionomia de Vergara (2000, p. 46-47), quanto aos fins, essa pesquisa é de caráter exploratório, visto que, apesar da ampla literatura acerca dos temas abordados, não existem produções bibliográficas sobre o objeto de estudo deste trabalho. De acordo com Lakatos e Marconi (2003, p. 188), pode-se classificar a pesquisa como um estudo exploratório-descritivo combinado, já que se trata de um estudo de caso que “têm por objetivo descrever completamente determinado fenômeno”, no caso as práticas de segurança adotadas pela empresa analisada.

Quanto aos meios de investigação (VERGARA, 2000, p. 46), a pesquisa classifica-se como bibliográfica, documental e, principalmente, estudo de caso.

A pesquisa bibliográfica, “desenvolvida a partir de material já elaborado” (GIL, 2007, p. 65), foi realizada em livros, monografias, teses e artigos científicos, com enfoque em segurança e gestão de TI e privacidade de dados. Pretendeu-se construir um embasamento teórico que vislumbrasse os efeitos que a TI exerce na difusão de dados e apontasse as principais formas de se garantir a segurança desses.

A análise documental, que difere da pesquisa bibliográfica apenas pela natureza das fontes, dado que estas ainda não foram tratadas analiticamente (GIL, 2007, p. 66), foi realizada em documentos institucionais da empresa pesquisada, e *sites* da *internet*, a fim de complementar o embasamento teórico e a coleta de dados.

Especificamente, trata-se de um estudo de caso, definido como um levantamento aprofundado de poucos objetos, analisados sob todos os aspectos possíveis. Este permite um entendimento mais amplo do objeto em estudo, no

entanto é restrito, por se limitar ao caso analisado, o que torna impossível a construção de generalizações (GIL, 2007, p. 72-73)

O método de abordagem da pesquisa é qualitativo, visto que não se preocupa em produzir medidas estatísticas para analisar o comportamento dos pesquisados, mas sim em compreender detalhadamente os significados e características situacionais que eles apresentam (LAKATOS; MARCONI, 2003, p. 187-189).

Como técnica de pesquisa, realizou-se a entrevista semi-estruturada com o responsável pela área de Tecnologia da organização em estudo. Por entrevista semi-estruturada, entende-se que há um roteiro a ser seguido, mas a entrevista pode seguir diferentes rumos, dependendo das respostas do entrevistado (GIL, 2007, p. 120). Objetivou-se com esta averiguar a proveniência dos dados que compõem o banco de dados da organização, e quais políticas de segurança são adotadas nos demais momentos do ciclo de vidas dessas informações.

Os dados da entrevista foram coletados no próprio ambiente de trabalho daquele profissional, com a devida formalização prévia à presidência da empresa. Dessa forma, o entrevistador pôde observar o local, a disposição e atuação dos funcionários, assim como as ferramentas tecnológicas utilizadas na organização. A observação utilizada caracteriza-se como simples, por ter o pesquisador observado espontaneamente os fatos e ter permanecido alheio à situação estudada (GIL, 2007, p. 111).

Visto que esta pesquisa é qualitativa, os dados coletados na entrevista e em documentos institucionais foram analisados por meio de inferências. Após, contrastaram-se essas inferências com as teorias utilizadas no embasamento teórico, para averiguar se as práticas implantadas pela organização condiziam com aquelas.

Essa metodologia foi empregada com o intuito de responder o problema dessa pesquisa – As políticas de segurança, coleta, manuseio, armazenamento e transporte de dados da empresa SPCB – Check Check mostram-se condizentes com as expectativas do mercado? –, e alcançar o objetivo proposto, que se trata de investigar se as fontes de coleta de dados e as políticas de segurança adotadas pela empresa SPCB – Check Check garantem a confidencialidade, a disponibilidade e a integridade das informações.

4. ESTUDO DE CASO

4.1 Informações sobre a Empresa

A empresa Serviço de Proteção ao Crédito do Brasil S/A – Check Check – atua no mercado há quarenta e nove anos. A organização possui uma matriz, que se situa na cidade de Goiânia, duas filiais, e cento e dezenove franquias espalhadas pelo país. Está presente em mais de dois mil e cem municípios, atende, em média, sessenta mil clientes, e possui número superior a cem postos de atendimento, disseminados estrategicamente pelos vinte e seis estados da Federação e o Distrito Federal (CHECK CHECK, 2009).

Por mês, são efetuadas aproximadamente cinco milhões de consultas no banco de dados da empresa, que armazena trezentos e cinqüenta milhões de registros e é atualizado todos os dias. Além disso, a organização oferece grande diversidade de meios para realização de consultas, visto que alega investir em integrar telecomunicações e informática (CHECK CHECK, 2009).

Com base no documento de apresentação institucional da empresa, foi possível averiguar a missão e a visão dessa, conforme transcrição abaixo:

> Visão
> Propiciar ao cliente atendimento diferenciado voltado para a qualidade, ampliando nosso banco de dados com informações de crédito e cadastrais, por meio de parcerias que agreguem valores a Empresa, destacando-se na evolução tecnológica do mercado, bem como o fortalecimento da relação Cliente x Franqueado x Empresa.
> Missão
> Assessorar os clientes na realização de transações seguras, sendo referência no segmento de informações de créditos e cadastro, pela busca de excelência no atendimento e satisfação do cliente.

Para efeitos desta pesquisa, foi realizado um estudo de caso na filial do Distrito Federal, situada no Núcleo Bandeirante. A empresa, considerada como organização de médio porte, lota cerca de setenta funcionários e possui oito departamentos, dentro dos quais está o de Tecnologia, que possui um Centro de Processamento de Dados (CPD).

4.2 Apresentação e Análise dos dados

A Coordenação de TI é composta por um Diretor, um Gerente e treze funcionários, dos quais sete fazem parte da equipe de desenvolvimento e seis são operadores do CPD. A equipe de desenvolvimento é formada por cinco desenvolvedores de sistemas, dos quais um realiza suporte técnico a desenvolvedores externos, um profissional responsável especificamente pelo suporte técnico a franquias, e um estagiário.

Não existe na empresa a formalização das práticas de segurança da informação adotadas. No entanto, o Diretor do departamento de TI, profissional devidamente qualificado para o exercício do cargo, elaborou um documento de políticas de segurança, que, apesar de nunca ter sido formalizado, é adotado informalmente na organização. Os motivos que inviabilizam, até o momento, a implantação do documento são decorrentes de limitações orçamentárias e de tempo.

Visto que a franquia do SPCB – Check Check analisada não possui um documento formal de políticas de segurança, pôde-se concluir que não são adotadas políticas de segurança padrão na matriz, filiais e franquias, o que representa uma falha na segurança.

O processo de negócio da organização consiste em prestar consultas aos clientes. São sete modalidades de consultas e serviços, quais sejam: **aceitação de cheques** – consulta se existem cheques sem fundo, irregulares, contra ordenados, etc.; **análise de crédito** – se não existem restrições; **informações cadastrais** – nome/razão social, CPF/CNPJ, idade/data de fundação, nome da mãe; **consulta de veículos** – dados referentes ao veículo, e não ao proprietário; **localização e pesquisa de dados cadastrais** – pesquisa de endereço e telefone; **recuperação de crédito** – inclusão do devedor em uma lista de restrição de crédito; e **monitoramento** – única consulta acessível também a pessoas físicas, que recebem via SMS e *e-mail* toda movimentação referente ao CPF**.**

Dessa maneira, são vitais para o funcionamento da empresa as informações referentes a cadastro – nome/ razão social, CPF/CNPJ e sua situação, data de nascimento/fundação da empresa, data de óbito, nome da mãe, endereço, telefone – , e as referentes ao crédito – restrições, pendências, financiamentos, ocorrência de cheques irregulares, entre outras. Em escala hierárquica secundária, também são importantes as informações relativas aos veículos.

Para dar suporte ao banco de dados, o SPCB – Check Check possui um CPD com cinqüenta servidores, todos máquinas *Dell.* Essas máquinas ficam dispostas em raques, agrupadas de seis em seis, visto que os concentradores de teclado e monitor da empresa trabalham com no máximo seis máquinas. Todos os raques estão ligados a um só teclado e monitor e estão sempre bloqueados, exigindo um usuário e uma senha para se ter acesso às informações neles contidas.

Como o processo de negócio da empresa é vinculado à prestação de serviços e consultas relativos à obtenção de informações, a organização demonstra, assim como alega Sêmola (2003, p. 9), conhecer a importância que as informações exercem para a fluência dos processos. Por esse motivo, todas as etapas do ciclo de vida das informações são cuidadosamente observadas e resguardadas, na tentativa de protegê-las de ameaças e diminuir possíveis riscos, em concordância com Lino (2005, p. 27).

Todas as informações da organização são coletadas junto a parceiros – bancos, companhias telefônicas, entre outros – e a *sites* de acesso público, dos quais qualquer pessoa pode obtê-las. As informações fornecidas pelos parceiros são gravadas em mídias digitais e criptografadas. Antes de serem adicionadas ao banco de dados, todas as informações passam por um processo de higienização, para que sigam um mesmo padrão, e sejam descartados os dados que não possuam valor.

A manipulação dos dados, etapa referente ao primeiro estágio do ciclo de vida (SÊMOLA, 2003, p.10), é feita sempre por meio de *softwares*. O acesso a esses é autorizado somente dentro da empresa, com permissão apenas para leitura dos dados. Qualquer necessidade de escrita – alteração ou inserção de dados –, é feita em tabelas à parte, e os funcionários não estão autorizados a remover ou alterar qualquer dado. A desobediência dessa norma pode levar à demissão por justa causa, além de ser considerada crime a intervenção indevida nos dados de um indivíduo.

Os dados são armazenados de forma segura e guardados dentro do CPD da própria empresa. Para se ter acesso a essas informações, é necessário possuir um nível de autorização de aplicação[4] ou de desenvolvedor. No entanto, nem todos os desenvolvedores têm acesso às bases de dados da produção. Esse profissional trabalha em um ambiente que é uma cópia da produção, mas com dados fictícios ou

[4] “Programa de computador projetado para executar um objetivo específico” (ASKOXFORD.COM, 2009, tradução nossa).

desatualizados. Os dados da produção somente são acessados por aplicações da produção, ou por pessoas com níveis específicos de autorização, que podem, ou não, ser desenvolvedores.

Além disso, as máquinas dos desenvolvedores são protegidas por um usuário e uma senha, e são programadas para se bloquearem após determinado tempo sem uso. As senhas devem ser complexas, exigindo uma variação de letras e números. Ademais, a equipe não possui permissão para transportar o código fonte e/ou os modelos de banco de dados para ambientes externos à empresa.

O transporte dos dados, terceira fase do ciclo (SÊMOLA, 2003, p. 10), é feito pela *internet,* e os dados são criptografados. A cada conexão estabelecida, muda-se a chave de criptografia, para dificultar o acesso às informações por pessoas não autorizadas.

Com relação à última etapa do ciclo de vida das informações (SÊMOLA, 2003, p. 10), um dado só é descartado quando for oriundo do cliente, e o conteúdo for duvidoso ou estiver fora do protocolo, o que se considera “lixo”. Quando um mesmo cliente envia mais de cinco vezes um pacote com “lixo”, ele é bloqueado nas regras de conexão da empresa.

Sêmola (2003, p. 43) defende que a segurança da informação tem como objetivo não somente a proteção contra acessos não autorizados às informações, como também a garantia de que os dados não sejam indevidamente alterados, de forma a não comprometer os princípios básicos de segurança: confidencialidade, disponibilidade e integridade.

Laureano e Morais (2005, p. 4-5) complementam que, além dos princípios mencionados anteriormente, a autenticidade, o não-repúdio, a legalidade, a privacidade e a auditoria também são critérios que devem ser observados para que uma informação seja considerada segura.

Para assegurar que as informações são utilizadas apenas por pessoas autorizadas, princípio da confidencialidade (FONTES, 2000, p. 21), e que os usuários são autênticos, princípio da autenticidade (LAUREANO; MORAIS, 2005, p. 4-5), todo cliente da organização possui um usuário e uma senha exclusivos. Por se tratarem de informações que requerem sigilo, a fim de se garantir a privacidade dos indivíduos a quem os dados se referem, o cliente responsabiliza-se por utilizá-las apenas para fins legais. Antes de qualquer consulta, o sistema exibe um quadro de aviso com a seguinte especificação:

> Estas informações são confidenciais e deverão ser utilizadas única, e exclusivamente, para orientação das transações comerciais do usuário, responsabilizando-se civil e criminalmente por danos que ocasionar a terceiros, quando utilizadas em desacordo com a legislação em vigor. (CHECK CHECK, 2009)

As informações da organização estão disponíveis apenas para os clientes que pagam por aquela informação, ou pelo serviço de disponibilização quando ela for pública. Os sistemas de consulta do SPCB – Check Check podem ser acessados vinte e quatro horas por dia, assegurando aos clientes a disponibilidade da informação em qualquer momento em que dela necessitarem.

Ademais, a empresa garante a integridade das informações disponibilizadas, princípio que afirma que os dados não podem ser adulterados em nenhuma etapa do ciclo de vida, como defende Fontes (2000, p. 21). Além de buscá-las em diferentes fontes seguras, o que também garante a autenticidade das informações, todas são criptografadas, se decidido por meio de acordos comerciais no momento da transação. Para certificar que as informações são 100% (cem porcento) íntegras, elas ainda passam por uma checagem de CRC[5].

Essa checagem é um mecanismo que assegura, também, o princípio do não-repúdio, que se trata da certeza de que nenhuma operação que modificasse a informação foi realizada (LAUREANO; MORAIS, 2005, p. 4-5).

A empresa demonstra preocupar-se, ainda, com o princípio da auditoria. Todo o tráfego de dados e todas as consultas realizadas por todos os clientes são armazenados, caso seja necessário o rastreamento de algum processo. Dessa maneira, a organização pode prevenir-se contra o uso indevido das informações por parte dos clientes.

No entanto, o SPCB – Check Check não é capaz de assegurar que as informações estejam disponíveis apenas às pessoas a quem elas referem-se, princípio da privacidade (LAUREANO; MORAIS, 2005, p. 4-5). Todavia, não fere o princípio da legalidade, uma vez que o banco de dados da empresa está em conformidade com o código de defesa do consumidor, legislação que os regulamenta, conforme transcrição a seguir. E como mencionado anteriormente, o

---

[5] Do inglês, *Cyclic Redundancy Check.* O CRC é um código de detecção de erros, em que são realizados cálculos matemáticos com os dados antes que estes sejam transmitidos ao receptor. O receptor, que recebe os dados e o resultado desse cálculo, realiza as mesmas operações. Se obtiver um resultado diferente, ocorreram modificações nos dados (BENFICA; COSTA, 2004, p. 1).

cliente responsabiliza-se civil e criminalmente pelo uso impróprio das informações, não a organização.

> SEÇÃO VI
> Dos Bancos de Dados e Cadastros de Consumidores
>
> Art. 43. O consumidor (...) terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
> (...)
> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
> (BRASIL, 2009).

Além de visar à proteção das informações, a segurança da informação, como alegam Sêmola (2003, p. 43) e a ABNT (2005, p. ix), é responsável por criar normas que identifiquem e controlem vulnerabilidades e ameaças, a fim de minimizar possíveis riscos, e, assim, diminuir o impacto desses às organizações.

Em consonância com Sêmola (2003, p. 47-48), que classifica as ameaças, quanto à intencionalidade, em naturais, involuntárias e voluntárias, e alega que as vulnerabilidades podem ser físicas, naturais, de *hardware, software*, mídias, comunicação ou humanas, abaixo são apresentados os principais riscos evidenciados na empresa, e classificado o tipo de vulnerabilidade e ameaça que podem vir a causá-los, em ordem decrescente de probabilidade de ocorrência:

a) **Ataque de *hackers*** – Probabilidade altíssima. Risco decorrente de possível vulnerabilidade de *software* e ameaça voluntária, que pode gerar a paralisação dos serviços críticos e dos serviços secundários – administrativos, marketing, *e-mail*, entre outros.
b) **Ataque de vírus** - Probabilidade altíssima. Risco decorrente de possível vulnerabilidade de *software* e ameaça voluntária, que pode gerar a paralisação dos serviços críticos e dos serviços secundários.

c) **Falhas em *softwares* de apoio** - Probabilidade alta. Risco decorrente de vulnerabilidade de *software* e ameaça involuntária, que pode gerar a paralisação dos serviços administrativos.

d) **Falhas em *softwares* críticos** - Probabilidade média. Risco decorrente de vulnerabilidade de *software* e ameaça involuntária, que pode gerar a paralisação dos serviços críticos.

e) **Bombas (explosivos)** - Probabilidade baixa. Risco decorrente de vulnerabilidade humana e ameaça voluntária, que pode gerar a paralisação dos serviços críticos e secundários, e ocasionar danos à estrutura da empresa.

f) **Falhas em *hardwares* de apoio** - Probabilidade baixa. Risco decorrente de vulnerabilidade de *hardware* e ameaça involuntária, que pode gerar a paralisação dos serviços secundários.

g) **Falhas em canais de comunicação** - Probabilidade baixa. Risco decorrente de possível vulnerabilidade de comunicação ou de *software*, e ameaça voluntária ou involuntária, que pode gerar a paralisação dos serviços críticos e secundários.

h) **Ausência de funcionários do ambiente de produção** - Probabilidade baixa. Risco decorrente de vulnerabilidade humana e ameaça voluntária ou involuntária, que pode gerar a diminuição e possível paralisação dos serviços de suporte interno e externo.

i) **Tempestades** - Probabilidade baixa. Risco decorrente de vulnerabilidade e ameaça natural, que pode gerar a paralisação dos serviços críticos e secundários, e ocasionar danos à estrutura da empresa.

j) **Incêndios** - Probabilidade baixa. Risco decorrente de possível vulnerabilidade humana ou natural, e ameaça voluntária ou involuntária, que pode gerar a paralisação dos serviços críticos e secundários, e ocasionar danos à estrutura da empresa.

k) **Falhas em *hardwares* críticos** - Probabilidade baixíssima. Risco decorrente de vulnerabilidade de *hardware* e ameaça involuntária, que pode gerar a paralisação dos serviços críticos e de determinados serviços secundários, como *e-mail*, acesso de colaboradores e parceiros à *internet*.

l) **Sabotagem interna (funcionários)** - Probabilidade baixíssima. Risco decorrente de vulnerabilidade humana e ameaça voluntária, que pode gerar a paralisação dos serviços críticos e secundários, além do vazamento de informações sigilosas.

m) **Sabotagem externa (agentes externos)** - Probabilidade baixíssima. Risco decorrente de possível vulnerabilidade humana e de *software,* e ameaça voluntária, que pode gerar o vazamento de informações sigilosas.

n) **Breves interrupções no fornecimento de energia elétrica e *Blackout*** - Probabilidade baixíssima. Risco decorrente de possível vulnerabilidade humana ou natural, e ameaça voluntária ou natural, que pode gerar a paralisação dos serviços críticos e secundários, e ocasionar danos à estrutura da empresa.

o) **Enchentes, Vulcões, Desastres nucleares, Tornados, Furacões e Terremotos** – Probabilidade inexistente. Risco decorrente de vulnerabilidade e ameaça natural. Esses eventos foram considerados de risco zero por não haver histórico de acontecimento no Distrito Federal.

Para garantir a minimização desses riscos, a organização adota determinadas medidas de segurança preventivas – que objetivam evitar a ocorrência de incidentes – e detectáveis – que sinalizam indivíduos ou condições que possam ocasionar ameaças (SÊMOLA, 2003, p. 50).

Como medida preventiva, primeiramente, toda a fiação do CPD foi feita por baixo do chão tablado, que possui vinte centímetros de altura, evitando, assim, a exposição dos cabos de energia. Além disso, todos os cabos são identificados e estão ligados a uma máquina que sinaliza exatamente o cabo defeituoso, caso ocorra algum problema, o que pode ser considerada uma medida detectável.

Para detectar e prevenir, respectivamente, possíveis ameaças, o CPD também possui seis detectores de fumaça, e extintores de incêndio em pontos estratégicos. No entanto, não existe na organização nenhum treinamento para os funcionários, e, principalmente, para os operadores do CPD, quanto à utilização dos extintores, caso ocorra algum incêndio, o que representa uma vulnerabilidade.

O acesso limitado à *internet* também pode ser classificado como medida preventiva. O controle de acesso é feito pelo *firewall,* e a estrutura da organização foi

desenvolvida em função dele. Dessa maneira, sempre que necessário, basta alterar o *firewall* para que todas as regras da empresa sejam alteradas. Ademais, a empresa possui anti-vírus atualizados, com checagem diária, o que também previne ameaças.

Além disso, todos os *softwares* da empresa são constantemente testados. Os *softwares* de uso do cliente passam por três processos de teste. O primeiro é realizado pela equipe de desenvolvimento; o segundo, pela equipe de homologação; e, por fim, os próprios usuários testam a aplicação. Dessa maneira, além de prevenir possíveis erros, os usuários já estarão familiarizados com o *software* quanto ele for implantado.

No caso de *softwares* do tipo servidor – *software* de solicitação e resposta de consultas –, os testes restringem-se à área de tecnologia da empresa. O servidor em desenvolvimento é submetido a consultas de testes reais com os respectivos resultados. Caso as respostas desse servidor não difiram das do antigo, é iniciada a segunda etapa de teste. Nessa fase, o servidor é submetido a várias consultas simultâneas, em que são adicionadas solicitações com “lixo”. Se o comportamento do *software* for estável, o servidor é implantado.

Além da identificação dos cabos do CPD e dos detectores de fumaça, outra medida detectável utilizada é o controle de acesso aos principais setores da empresa. A entrada ao CPD é controlada por meio de biometria, com leitor digital. Já os demais setores vitais para a organização, como o suporte e o financeiro, são controlados por meio de leitor magnético.

Todos os departamentos da empresa, inclusive o CPD, são monitorados vinte e quatro horas por câmeras de segurança, podendo-se considerar a prática como outra medida detectável. Essas filmagens são gravadas em mídias digitais e guardadas em local sigiloso. A empresa também possui alarme anti-roubo ligado diretamente à polícia, além de seguranças vinte e quatro horas por dia.

Para “contingenciar situações e incidentes de segurança que não puderam ser evitados” (SÊMOLA, 2003, p. 98-99) pelas medidas adotadas, a organização necessita elaborar um Plano de Continuidade de Negócios, como afirmam Sêmola (2003, p. 98) e Lino (2005, p. 29), em conformidade com a NBR ISO/IEC 17799. Esse plano é composto por planos de contingência, que devem ser elaborados para cada ameaça detectada (SÊMOLA, 2003, p. 103). Sêmola (2003, p. 103-105) ainda defende que os planos de contingência são subdivididos em planos de continuidade

operacional, planos de recuperação de desastres e planos de administração de crises.

. Para garantir a continuidade operacional da empresa, existem três *no-breaks* alimentados por cem baterias, cada um com capacidade para manter doze servidores ativos por seis horas. No caso de interrupções no fornecimento de energia elétrica, por exemplo, os *no-breaks* entram em atividade e mantêm as máquinas do CPD ativas. Todas as operações da empresa são checadas, e as de menor prioridade são desativadas temporariamente. Caso o fornecimento de energia estenda-se a um prazo maior que a capacidade dos *no-breaks*, o gerador silenciado é ativado prontamente.

A organização também possui um contrato com a empresa de computadores *Dell* que assegura que qualquer defeito em máquinas que estejam na garantia deve ser solucionado em até cinco horas. Primeiramente, estabelece-se contato com a *Dell* e um operador tenta resolver o problema pelo telefone. Caso não seja solucionado, um técnico é mandado de São Paulo para verificar o problema pessoalmente. Se for constatado que o problema é físico, a máquina é substituída imediatamente.

Para recuperar e restaurar possíveis ativos afetados, o que corresponde ao plano de recuperação de desastres (SÊMOLA, 2003, p. 104), existem dois processos de *backup*[6] na organização. O primeiro, denominado *backup* total[7], ocorre diariamente. O segundo, *backup* diferencial[8], ocorre a cada quinze minutos. Todos os *backups* são armazenados em fitas eletromagnéticas, e o local em que essas são guardadas é sigiloso.

Ademais, os servidores são espelhados, o que significa dizer que todo servidor possui outro servidor que contenha exatamente as mesmas informações daquele. Dessa maneira, podem-se recuperar facilmente os dados de um servidor, caso ocorra um problema e ele pare de funcionar.

Uma falha evidenciada no Plano de Continuidade de Negócios da empresa é que não existem equipes envolvidas com a ativação da contingência após a ocorrência do incidente de segurança (SÊMOLA, 2003, p. 104); ou seja, não existe

---

[6] Processo que armazena os dados em outro local que não o original, para posterior recuperação, se necessária.

[7] Modalidade de backup que captura todos os dados de todas as unidades. Por meio desse tipo de backup, pode-se restaurar completamente um servidor. (MICROSOFT, 2004).

um plano de administração de crise. Dessa forma, caso uma crise aconteça e interrompa completamente o funcionamento do CPD da organização, os sistemas financeiros, administrativos e operacionais seriam paralisados, além de suspensos imediatamente quase todos os serviços prestados aos clientes. Para a estruturação de novos servidores em outro local, seriam necessárias no mínimo duas semanas, o que acarretaria em um prejuízo financeiro homérico decorrente das consultas e da possível perda de clientes.

Para finalizar este estudo, é relevante destacar que, em contraposição à afirmação de Fontes (2000, p.107), que defende que as políticas de segurança devem ser especificadas a todos os ativos humanos da organização, em concordância com a ABNT (2005, p. 25-29), não parece existir na empresa uma cultura de segurança adequada. Foi possível observar falhas básicas de segurança entre os colaboradores, como a exposição de senhas, o que os tornam vulnerabilidades graves à empresa.

[8] Backup que captura apenas os dados modificados desde a realização do último backup total (MICROSOFT, 2004).

5. CONCLUSÃO

A discussão a respeito da segurança da informação enquanto medida estratégica para as empresas demonstra-se extremamente relevante, por se tratar de um ativo de grande valor, principalmente para organizações cuja rentabilidade dependa, sobretudo, das informações, como é o caso do SPCB – Check Check, empresa analisada neste trabalho de pesquisa.

Devido aos constantes avanços tecnológicos, entende-se que não somente a disponibilização de informações é facilitada, como também o acesso a essas por parte de pessoas não autorizadas. Nesse cenário, surgem discussões acerca do tema privacidade de dados.

Nesta concepção, conclui-se que estabelecer medidas de segurança capazes de proteger os ativos da organização e garantir a privacidade é de vital importância para a captação de clientes, e conseqüente sobrevivência das empresas.

Ponderando sobre essas questões, pode-se retornar ao problema de pesquisa proposto neste trabalho: As políticas de segurança, coleta, manuseio, armazenamento e transporte de dados da empresa SPCB – Check Check mostram-se condizentes com as expectativas do mercado?

A formulação desse problema parte do entendimento de que uma empresa que lida diariamente com dados cadastrais, que são considerados sigilosos, necessita de possuir meios que assegurem que esses dados não sejam compartilhados com pessoas que a eles não possam ter acesso.

Verificou-se que a organização entende a relevância que as informações possuem para o seu processo de negócios. Também se percebeu que existe uma preocupação acerca da disponibilização das informações apenas para pessoas legalmente autorizadas. Dessa maneira, com exceção da consulta de monitoramento do CPF, todas as demais consultas são realizadas somente por pessoas jurídicas que necessitem dos dados para transações comerciais e estejam permitidas a obtê-los.

Por esses motivos, existem na empresa práticas que visam à segurança da informação. Primeiramente, os dados são coletados junto a parceiros confiáveis, já que se tratam de empresas que possuem informações referentes a cadastro e a crédito atualizadas, como bancos e companhias telefônicas. Ademais, como

mencionado no desenvolvimento deste trabalho, os dados são criptografados, não apenas no momento da coleta, como também em todo o tráfego.

Os dados são armazenados no CPD da empresa, e pôde-se concluir que esse possui estrutura física adequada para mantê-los em segurança. Os equipamentos do CPD são de última geração, existem detectores de fumaça, extintores de incêndio, monitoramento de vídeo, vidros blindados e controle de acesso biométrico.

O manuseio das informações é realizado por meio de *software*s, e apenas os desenvolvedores possuem acesso a esses. Para manter a segurança, os funcionários autorizados têm um nome de usuário e uma senha.

Como os dados são coletados de fontes seguras e são adotadas na empresa políticas para garantir os princípios básicos de segurança em todos os momentos do ciclo de vida das informações, conclui-se que a resposta ao problema é afirmativa.

No entanto, percebeu-se a existência de lacunas nas medidas adotadas, e a principal delas refere-se à disseminação das práticas de segurança entre os próprios colaboradores da organização – culminando na formação de uma cultura organizacional que entende a importância da segurança para o funcionamento da empresa – visto que, apesar de existir um possível projeto de políticas de segurança, este não foi formalmente implantado.

Ao responder o problema, foi possível alcançar o objetivo geral deste estudo de caso que foi o de investigar se as fontes de coleta de dados e as políticas de segurança adotadas pela empresa SPCB – Check Check garantem a confidencialidade, a disponibilidade e a integridade das informações.

Verificou-se que as políticas de segurança da empresa conseguem manter o sigilo e a confidencialidade das informações. A integridade também é assegurada pelas fontes em que são coletados os dados e pelas checagens que a organização realiza.

No entanto, apesar de as informações estarem disponíveis no sistema vinte e quatro horas por dia, caso ocorra algum incidente que cesse o funcionamento do CPD, a falta de um plano de administração de crise inviabiliza a disponibilidade das informações por no mínimo duas semanas, tempo necessário à aquisição de novas máquinas e estruturação de um CPD alternativo.

Além disso, entende-se que não adianta existirem regras formais de segurança, o que não contempla a organização em análise, se os ativos humanos

não possuírem conhecimento sobre elas, visto que eles são os principais responsáveis pela manutenção dessas regras. Como mencionado no desenvolvimento deste estudo, não existe na organização uma cultura de segurança cem porcento adequada.

Concluiu-se que a organização preocupa-se com a escolha das fontes que propiciam os dados, a fim de assegurar que as informações sejam íntegras e confiáveis. E que, apesar das lacunas existentes, as políticas de segurança adotadas garantem, em grande parte, a confidencialidade, a disponibilidade e a integridade das informações.

Ao alcançar este Objetivo Geral, validam-se também os objetivos específicos apresentados pela pesquisa:

a. Explanar, teoricamente, sobre as principais políticas de segurança da informação existentes;
b. Comparar as práticas exercidas pelo SPCB – Check Check para manter a segurança e o sigilo das informações com essas políticas; e
c. Analisar os dados obtidos à luz das teorias de base utilizadas.

O objetivo específico (a.) foi alcançado na apresentação do tópico (2.5), denominado “Segurança da Informação”. Os objetivos específicos (b.) e (c.), por sua vez, foram evidenciados no item (4.2), “Apresentação e análise dos dados”.

5.1 Contribuições

Enquanto contribuições, o presente trabalho de pesquisa pode auxiliar gestores na elaboração e implantação de políticas de segurança que visem a minimizar riscos aos principais ativos organizacionais. Metodologicamente, o trabalho pode ser consultado como fonte de conteúdo para pesquisas futuras na área. Ademais, contribui para a organização analisada, visto que apresenta uma análise de risco simplificada, além de apontar fragilidades da empresa.

5.2 Limitações

Partindo da premissa de que toda pesquisa científica possui limitações, o presente estudo não é uma exceção. Devido ao fator tempo e ao limite de páginas

permitido para o desenvolvimento da pesquisa, determinados aspectos teóricos podem não ter sido suficientemente abordados.

Além disso, o fator tempo inviabilizou o alcance do escopo pretendido, uma vez que partes do discurso da organização quanto às práticas de segurança empregadas não foram evidenciadas, devido à impossibilidade de uma análise aprofundada acerca desses elementos.

5.3 Sugestões e Recomendações

Visto que um trabalho de pesquisa nunca se esgota em si, abaixo são levantadas questões complementares que viabilizariam pesquisas futuras em continuidade aos resultados alcançados com este estudo.

a. Como uma análise de risco detalhada pode influenciar na elaboração de medidas de segurança, e, assim, viabilizar planos de contingência capazes de proteger todos os ativos de uma organização?

b. Em que medida a adoção de um plano de políticas de segurança formal auxilia na formação de uma cultura organizacional de segurança?

6. REFERÊNCIAS

ABNT. *NBR ISSO/ IEC 17799: Tecnologia da informação: código de prática para a gestão da segurança da informação***.** Rio de Janeiro: ABNT, 2005.

ALMEIDA FILHO, José C. A. *A segurança da informação no processo eletrônico e a necessidade de regulamentação da privacidade de dados.* In: WORLD CONGRESS OF PROCEDURE LAW, XIII. Comunicação científica.

ASKOXFORD.COM. *The Compact Oxford English Dictionary.* Brasília, 2009. Disponível em: <http://www.askoxford.com/dictionaries/?view=uk>. Acesso em: 08 jun 2009.

BENFICA, Alex Teixeira; COSTA, Fábio Nunes da. *Algoritmos de CRC's (Cyclic Redundancy Codes).* 2004. 12f. Artigo (Graduação) – Departamento de Ciência da Computação, Universidade de Minas Gerais, Minas Gerais, 2004.

BRAGA, Ascenção. *A gestão da informação*. Portugal, 1996.

BRASIL. Constituição da República Federativa do Brasil, promulgada em 5 de outubro de 1988. *Coleção Saraiva de legislação.* São Paulo, 40.ed., 2007, p. 6.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990.* Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 2009. Disponível em: <http://www.planalto.gov.br/ccivil/leis/l8078.htm >. Acesso em: 03 jun 2009.

CHECKCHECK. *A Empresa Check Check.* Brasília, 2009. Disponível em: <http://www.checkcheck.com.br/>. Acesso em: 14 maio 2009.

DEZEN JUNIOR, Gabriel. *Curso completo de Direito Constitucional.* 10. ed., v. 1. Brasília: Vestcon, 2006.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.

FOINA, Paulo Rogério. *Tecnologia de Informação: Planejamento e Gestão.* 2. ed. São Paulo: Atlas, 2009.

FONTES, Edison Luiz Gonçalves. *Vivendo a segurança da informação: orientações práticas para pessoas e organizações.* 1. ed. São Paulo: Sicurezza: Brasiliano & Associados, 2000.

GIL, Antonio Carlos. *Métodos e técnicas de pesquisa social.* 5. ed. São Paulo: Atlas, 2007.

IBM. *The birth of the IBM PC.* Brasília, 2009. Disponível em: <http://www-03.ibm.com/ibm/history/exhibits/pc25/pc25_birth.html>. Acesso em: 12 mar 2009.

ISHITANI, Lucila. *Uma arquitetura para controle de privacidade na Web.* 2003. 84 f. Tese (Doutorado) – Ciências da Computação, Universidade Federal de Minas Gerais, 2003.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Fundamentos de metodologia científica*. 5. ed. São Paulo: Atlas, 2003.

LAUDON, Kenneth C.; LAUDON, Jane P. *Sistemas de Informação Gerenciais: administrando a empresa digital.* São Paulo: Pearson Prentice Hall, 2004.

LAUREANO, Marcos A. P.; MORAES, Paulo E. S. Segurança como estratégia de gestão da Informação. *Economia e Tecnologia*, v. 8, n. 3, p. 39 – 44, 2005.

LINO, Marcelo Nogueira. *Aplicação de uma política de segurança da informação nas organizações.* 2005. 87 f. Monografia (Superior) – Faculdade de Tecnologia em Ciências Sociais: Administração, Centro Universitário de Brasília, 2005.

MAXIMIANO, Antonio C. A. *Teoria Geral da Administração: da revolução urbana à revolução digital.* 5. ed. São Paulo: Atlas, 2005.

MICROSOFT. *Configuração dos serviços de backup e recuperação.* Brasília, 2004. Disponível em: <http://www.microsoft.com/brasil/>>. Acesso em: 04 jun 2009.

NASCIMENTO, Patrícia Helaine L. *História da Tecnologia da Computação.* Brasília, 2009. Disponível em: < http://www.lia.ufc.br/~paty/icc/notas/2/index.html >. Acesso em: 08 jun 2009.

SÊMOLA, Marcos. *Gestão da Segurança da Informação: uma visão executiva.* 2.ed. Rio de Janeiro: Campus, 2003.

TERRA. *Anos 90: o desenvolvimento da internet no Brasil.* Brasília, 2009. Disponível em:<http://tecnologia.terra.com.br/internet10anos/interna/0,,OI541825-EI5026,00.html>. Acesso em: 12 mar 2009.

_____. *Primeiro computador do mundo completa 60 anos.* Brasília, 2006. Disponível em: <http://tecnologia.terra.com.br/interna/0,,OI892512-EI4799,00.html>. Acesso em: 12 mar 2009.

VERGARA. Sylvia Constant. *Projetos e Relatórios de Pesquisa em Administração.* 3. ed. São Paulo: Atlas, 2000.

APÊNDICES

Apêndice A

Roteiro da entrevista realizada com o responsável pela área de Tecnologia da empresa SPCB – Check Check, elaborado pela aluna Nathália Villela Ventura Guimarães Ferreira.

Nome:
Cargo:
Tempo de atuação na empresa:

1. O quão importante o Sr(a). qualifica as informações que a empresa possui sobre pessoas?
2. Como é feito o controle de acesso dos funcionários a essas informações? E de demais pessoas não autorizadas?
3. Quando um cliente deseja receber informações, qual(is) caminho(s) é(são) percorrido(s) pela informação até o destino?
4. Que políticas de segurança são adotadas no tráfego das informações?
5. Qual a periodicidade de atualização das informações?
6. O critério de garantir a qualidade da informação é baseado em higienização computadorizada ou ela é entregue da forma que foi cadastrada?
7. A empresa tem política de backup dos dados?
8. Como as informações são armazenadas?
9. Existe algum plano de contingência caso ocorra uma situação de emergência?
10. Se sim, este plano de contingência leva em consideração a segurança da informação?
11. Que tecnologias a empresa utiliza na coleta, distribuição e armazenamento dos dados cadastrais?
12. Que fontes são utilizadas pela organização para coletar os dados?
13. Que políticas são adotadas para garantir a privacidade desses dados?
14. Como é feito o gerenciamento dessas informações?