UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA
CIENCIA DA COMPUTAÇÃO

RAIMUNDO ALAN MATOS PESSOA

UM ESTUDO DE CASO SOBRE A GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM UMA INSTITUIÇÃO FINANCEIRA

VITÓRIA DA CONQUISTA – BAHIA

SETEMBRO – 2012

RAIMUNDO ALAN MATOS PESSOA

UM ESTUDO DE CASO SOBRE A GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM UMA INSTITUIÇÃO FINANCEIRA

Monografia final de conclusão de curso apresentada ao Departamento de Ciências Exatas – DCE-UESB para obtenção do diploma de Bacharel em Ciência da Computação.

Orientador: Francisco Carvalho

VITÓRIA DA CONQUISTA – BAHIA

SETEMBRO - 2012

AGRADECIMENTOS

Agradeço, primeiramente, a Deus por sempre permanecer ao meu lado, me guiando, e incentivando, me mantendo firme no meu objetivo.

Aos meus pais por me darem as bases para a minha formação como ser humano, estarem presentes em cada etapa de minha vida e o apoio incondicional nos momentos difíceis.

Aos meus irmãos pelo incentivo, companheirismo, e por compartilhar comigo de todos os processos e etapas que passei.

Aos colegas pelos momentos de convivência e aprendizado, compartilhando conhecimentos e momentos de alegria.

Aos professores pela preocupação, dedicação e compreensão.

Ao meu orientador pela paciência e pelos conhecimentos transmitidos que fizeram com que esse trabalho fosse realizado.

RESUMO

Este trabalho apresenta um estudo de caso sobre a gestão da segurança da informação em uma instituição financeira, onde foram analisadas as práticas de controle, relacionados à segurança da informação implementadas nesta instituição. A segurança da informação é um aspecto de extrema importância e que é tratada pela maioria das grandes organizações existentes. Sistemas eletrônicos e recursos tecnológicos utilizados atualmente - como e-mails, internet, computadores, notebooks, softwares – são necessários para que as empresas se mantenham em um alto nível de competição no mercado, notadamente uma instituição financeira. Neste trabalho, são feitas avaliações de conformidade da gestão da segurança da informação desta organização em relação à norma ABNT NBR ISO/IEC 17799 – Tecnologia da Informação – Técnicas de segurança – Código de Prática para a Gestão da Segurança da Informação e à norma ABNT NBR ISO/IEC 27002 – Código de Prática para a Gestão da Segurança da Informação. É nesse contexto que o presente trabalho é estruturado, apresentando os principais conceitos relacionados à Segurança da Informação, Gestão Segurança da Informação, fazer uma análise/avaliação de como as práticas relacionadas ao assunto estão sendo geridas dentro da instituição financeira e apresentar os resultados encontrados concluindo assim a pesquisa.

Palavras-chave: Gestão da segurança da informação, Segurança da informação, Tecnologia da informação

ABSTRACT

This work presents a case study about the management of information security in a financial institution where were analyzed the control practices, related to information security implemented at this institution. Information security is a very important subject and that is treated by majority organizations existing. Electronic systems and technological resources used today – likes email, internet, computers, notebooks, software - are needed for companies to remain at a high level of competition in the market, especially a financial institution. In this work, are reviews made of the accordance of the management of information security of this organization in relation to the rule ABNT NBR ISO/ IEC 17799 - Information technology - Security techniques - Code of Practice for Information Security Management standard and the rule ABNT NBR ISO / IEC 27002 - Code of Practice for the Management of Information Security. It is in this context that the present work is structured, presenting the main concepts related to Information Security, Information Security Management, and then, do an analysis / reviews how the practices as related to the subject being managed within the financial institution and shows the results founded concluding the search.

Keywords: Information security management, Information Technology, Management security information

SUMÁRIO

LISTA DE FIGURAS

LISTA DE GRÁFICOS

1 INTRODUÇÃO

A gestão da Segurança da Informação é um assunto que deve estar em pauta a todo instante e em toda organização que priva de conteúdo, dados. A informação sempre foi um dos bens mais importantes da organização. A diferença é que há algum tempo a informação mais crítica da empresa poderia ser guardada dentro de uma gaveta. Nos moldes das empresas modernas, a proteção da informação deve ser uma das preocupações dos executivos e proprietários. O executivo não precisa ser um especialista em segurança da informação, mas precisa sem dúvida nenhuma conhecer requisitos básicos.

É importante observar, que a segurança da informação não é um assunto que deve ser tratado e discutido exclusivamente pela área de tecnologia da informação (TI), visto que a segurança proporcionada por meios tecnológicos não satisfaz toda a demanda por segurança que este ativo apresenta, conforme a norma ABNT NBR ISO/IEC 27002 – Código de Prática para a Gestão da Segurança da Informação. Esta norma possui um repleto cardápio de controles contendo as melhores práticas para segurança da informação.

Esta norma versa acerca da grande importância da segurança da informação, contendo indicações de requisitos e melhores práticas para a gestão da segurança da informação. Nela está explícito que a gestão da segurança da informação não deve ser tratada apenas pela área de TI, mas por todas as áreas da organização, notadamente pela alta administração Deve ser uma decisão empresarial, pois se acontecer um incidente que leve a organização a um prejuízo ou a impeça de continuar a realizar seu negócio, são os proprietários ou acionistas que perderão o investimento realizado. Esta abordagem é condizente com os propósitos de governança corporativa, além de viabilizar a conscientização em segurança da informação, fazendo com que as práticas relacionadas, façam parte das atividades de seus colaboradores.

A falta de informação geralmente é o que leva as pessoas a se comportarem de maneira inadequada. Se a empresa orienta seu colaborador devidamente, os incidentes, como sair de sua estação de trabalho deixando o computador ligado e habilitado para uso através de sua identificação, passar sua senha de identificação e acesso a outro colega, utilizar internet com finalidade pessoal, deixar documentos sigilosos soltos e esquecidos na impressora, portar dados confidenciais em dispositivos móveis, entre

outros incidentes, que poderiam ser evitados mediante uma boa orientação e a criação de um código de conduta ética para preveni-los. É importante que os recursos computacionais, ferramentas básicas para agilizar negócios e mostrar confiabilidade a clientes e parceiros, sejam utilizados de forma correta e segura, para evitar a perda de produtividade dos colaboradores, o congestionamento na rede e o risco de divulgação de informações sigilosas, entre outros prejuízos que podem ser causados à imagem da organização ou ao próprio colaborador.

1.1 PROBLEMÁTICA

Devido à grande importância e valor dos ativos de informação de uma instituição financeira, ou um Banco popularmente falando, é fundamental tratá-los e protegê-los adequadamente. Proteger a informação significa mantê-los seguros contra ameaças que possam afetar as suas funções, ou seja, que possam danificá-los, acessá-los sem autorização, eliminá-los ou furtá-los. Considerando que, uma instituição financeira possui/requer um alto nível de proteção de sua informação, este trabalho teve como propósito verificar a gestão de segurança da informação em uma instituição financeira, com foco nos dois tópicos que seguem: política de segurança da informação e infra-estrutura de Tecnologia da Informação (TI), observando-se os controles propostos pela norma ABNT NBR ISO/IEC 17799 – Tecnologia da Informação – Técnicas de segurança – Código de Prática para a Gestão da Segurança da Informação e ABNT NBR ISO/IEC 27002 – Código de Prática para a Gestão da Segurança da Informação.

Adotaram-se como questões:

Como a organização gerencia a segurança da Informação?

Quais as melhores práticas de segurança da informação adotadas nesta instituição?

1.2 OBJETIVO GERAL

Analisar uma instituição financeira quanto a sua gestão de segurança da informação, através de um estudo de caso com foco nos tópicos: política de segurança da informação e infra-estrutura de Tecnologia da Informação (TI), observando-se os controles propostos pela norma ABNT NBR ISSO/IEC 17799 – Tecnologia da Informação – Técnicas de segurança – Código de Prática para a Gestão da Segurança da

Informação e ABNT NBR ISO/IEC 27002 – Código de Prática para a Gestão da Segurança da Informação.

1.3 OBJETIVOS ESPECÍFICOS

Apresentar as características principais da norma ABNT NBR ISO/IEC 17799 e ABNT NBR ISO/IEC 27002.

Elaborar um estudo de caso em uma instituição financeira (Banco), observando à gestão e as práticas da segurança da informação adotadas até então.

Verificar e também analisar controles de segurança da informação utilizados na instituição financeira relativos à política de segurança da informação e infraestrutura de Tecnologia da Informação (TI), tendo como embasamento teórico a proposta da norma ABNT NBR ISO/IEC 17799 – Tecnologia da Informação – Técnicas de segurança – Código de Prática para a Gestão da Segurança da Informação e ABNT NBR ISO/IEC 27002 – Código de Prática para a Gestão da Segurança da Informação.

1.4 JUSTIFICATIVA

Dada à grande importância e valor agregado da informação para uma instituição financeira, é necessário tratá-los e protegê-los devidamente para garantir a segurança deste ativo, fator essencial para o sucesso de uma instituição desta natureza.

Assim a justificativa do presente trabalho vêm da necessidade, da importância e criticidade de se analisar como está implementada à gestão da segurança da informação na instituição financeira estudada.

1.5 METODOLOGIA

O presente trabalho foi produzido utilizando as seguintes técnicas: pesquisa bibliográfica e estudo de caso.

A pesquisa bibliográfica relatou os conceitos relacionados à segurança da informação sobre os quais foi avaliada a instituição financeira.

O estudo de caso foi realizado em uma instituição financeira com o objetivo de analisar os aspectos relacionados à gestão e práticas de segurança da informação, verificando os controles e ações adotadas.

Em relação ao estudo de caso, a coleta de dados foi através das seguintes fontes:

- Questionário de Segurança da Informação;
- Entrevistas individuais.

2 SEGURANÇA DA INFORMAÇÃO E ASPECTOS RELACIONALDOS

Este capítulo apresenta princípios e conceitos a cerca da segurança da informação, bem como nos mostram elementos e aspectos relacionados a este assunto que influenciam nas questões de segurança e proteção da informação.

2.1 O DIREITO E A SEGURANÇA DA INFORMAÇÃO

Direito da informática é um campo do Direito que se propõe a estudar aspectos jurídicos do uso de computadores, com fundamentos no crescente desenvolvimento da Internet e na importância da tecnologia da informação e da informática nas relações jurídicas, sendo por isso, uma nova área do estudo do Direito.

Há ainda os que designam esta área do Direito como "Direito Informático", "Direito Eletrônico", "Direito Digital", "Direito da Tecnologia da Informação", "Direito da Internet", ou ainda "Direito Cibernético", termos que parecem ter menor aceitação na comunidade acadêmica.

Segundo Patrícia Peck Pinheiro (2010, p. 41),

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicadas até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.

Desta forma podemos entender o conceito acima a cerca do Direito Digital como sendo uma evolução necessária, com o objetivo de regular e criar parâmetros jurídicos para a interação existente entre o ser humano e os meios tecnológicos, abrangendo a esfera cível, comercial, autoral dentre outras.

2.2 A INFORMAÇÃO

A informação tornou-se patrimônio tanto de uma empresa quanto da pessoa que a possui. Segundo Pinheiro (2010, p 82),

> A informação recebe o título de ativo intangível, ou seja, o uso indevido ou divulgação não autorizada pode gerar danos e envolver ilícitos que vão desde quebra de sigilo profissional, a vazamento de informação confidencial de uma instituição ou exposição da vida íntima ou privacidade de uma pessoa.

Informação: Ato ou efeito de informar ou informar-se; comunicação, indagação ou devassa. Conjunto de conhecimentos sobre alguém ou alguma coisa; conhecimentos obtidos por alguém. Fato ou acontecimento que é levado ao conhecimento de alguém ou de um público através de palavras, sons ou imagens. Elemento de conhecimento suscetível de ser transmitido e conservado graças a um suporte e um código.

2.3 A SEGURANÇA DA INFORMAÇÃO

A segurança da Informação é o meio que a empresa possui para proteger, envolve um conjunto de ações que necessitam ser planejadas e programadas de forma a abranger as questões técnicas, comportamentais e jurídicas. O trabalho da segurança da informação requer um preparo adequado de modo a minimizar riscos no uso das medidas de proteção da empresa. Muitas empresas que se materializam através das pessoas que a gerenciam, somente percebem a necessidade de um processo de segurança em situações de crise, também não deve surgir do nada, é necessário que este processo esteja alinhado aos objetivos da organização. A partir dos objetivos do negócio é que se planejam os objetivos da segurança da informação, com o intuito de possibilitar a realização do negócio no que depende do uso dos recursos da informação, conforme indicado em Fontes (2010).

Para a própria norma ABNT NBR ISO/IEC 17799, Segurança da Informação 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.

Com o aumento da facilidade de carregar informações, é necessário cada vez mais aplicar maior segurança ao processo. É notável que hoje os colaboradores das empresas possuam cada vez mais conhecimento e facilidade de acesso a tecnologia.

Vulnerabilidades existem e não são poucas, até mesmo muito desconhecidas e despercebidas dentro de qualquer organização, seja ela de TI ou não. As condutas inadequadas mais comuns no âmbito de uma empresa envolvem na maioria das vezes, falta de informação. As empresas não orientam adequadamente seus colaboradores, então incidentes que poderiam ser evitados como deixar o computador ligado sem

bloquear o acesso, nesse caso, outro colaborador mal intencionado pode utilizar rapidamente a estação de trabalho e realizar alguma operação não autorizada, conforme indicado em Santos (2007).

É essencial para aumentar o nível de segurança da informação, a criação de um Código de Ética da TI, que esteja preparada para tratar eventuais incidentes. É nesse momento que a Segurança da Informação envolve a prevenção e preservação de evidências. Dessa forma tende a garantir que determinada pessoa ou máquina esteja envolvida em determinado evento. Devido à má formulação ou a inexistência de um código de ética, vários casos não possuem evidências necessárias para encontrar o culpado pelo incidente, segundo Santos (2007).

Empresas do mundo todo estão sujeitas a terem seus dados extraviados, seja por descuido de seus colaboradores, como por ações furtivas realizadas por eles mesmos ou por alguém externo. O extravio de informações gera um custo enorme as empresas, e muitos eventos podem ser poupados apenas supervisionando seus clientes internos.

Para Peixoto (2006), as organizações tendem a pensar que uma vez que se contrata um funcionário, o mesmo se torna confiável e será sempre leal as causas da empresa. Muitas delas não se preocupam em verificar as referências antes de contratá-los, o que pode ser um erro muito caro. Por isso, algumas empresas têm adotado o papel de orientar sobre a Segurança da Informação ao contratar um funcionário. Criando políticas para uso de e-mail corporativo e internet, fazendo com que este assine um contrato demonstrando estar ciente das políticas adotadas por tal empresa.

2.4 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Levando-se em consideração que negócio é sinônimo de capital, pode-se concluir que não somente deixar de inovar/atualizar a chegada de informações na empresa, como também não conduzir, armazenar, transferir e até mesmo descartar alguns tipos de informações leva a constatar uma empresa *"sem vida"*, que pouco valoriza três conceitos fundamentais em termos de segurança da informação, conforme indica Peixoto (2006). A segurança da informação tem o objetivo de preservar as características da informação relativas à sua confidencialidade, a integridade e a disponibilidade.

- **Disponibilidade** – propriedade que a informação apresenta, de estar disponível e utilizável numa eventual requisição de uma entidade autorizada ABNT (2006).

- **Integridade** – propriedade que a informação apresenta, de estar completa e fiel ao estado original ABNT (2006).
- **Confidencialidade** – propriedade que a informação apresenta, de estar disponível apenas para àqueles que estão autorizados a obtê-la ABNT (2006).

A manutenção das propriedades e dos aspectos da informação depende do estabelecimento de uma ação gerencial, que é chamada de Gestão da Segurança da Informação. Pode-se observar a relação entre o ciclo de vida da informação, e suas propriedades, na figura 2.1

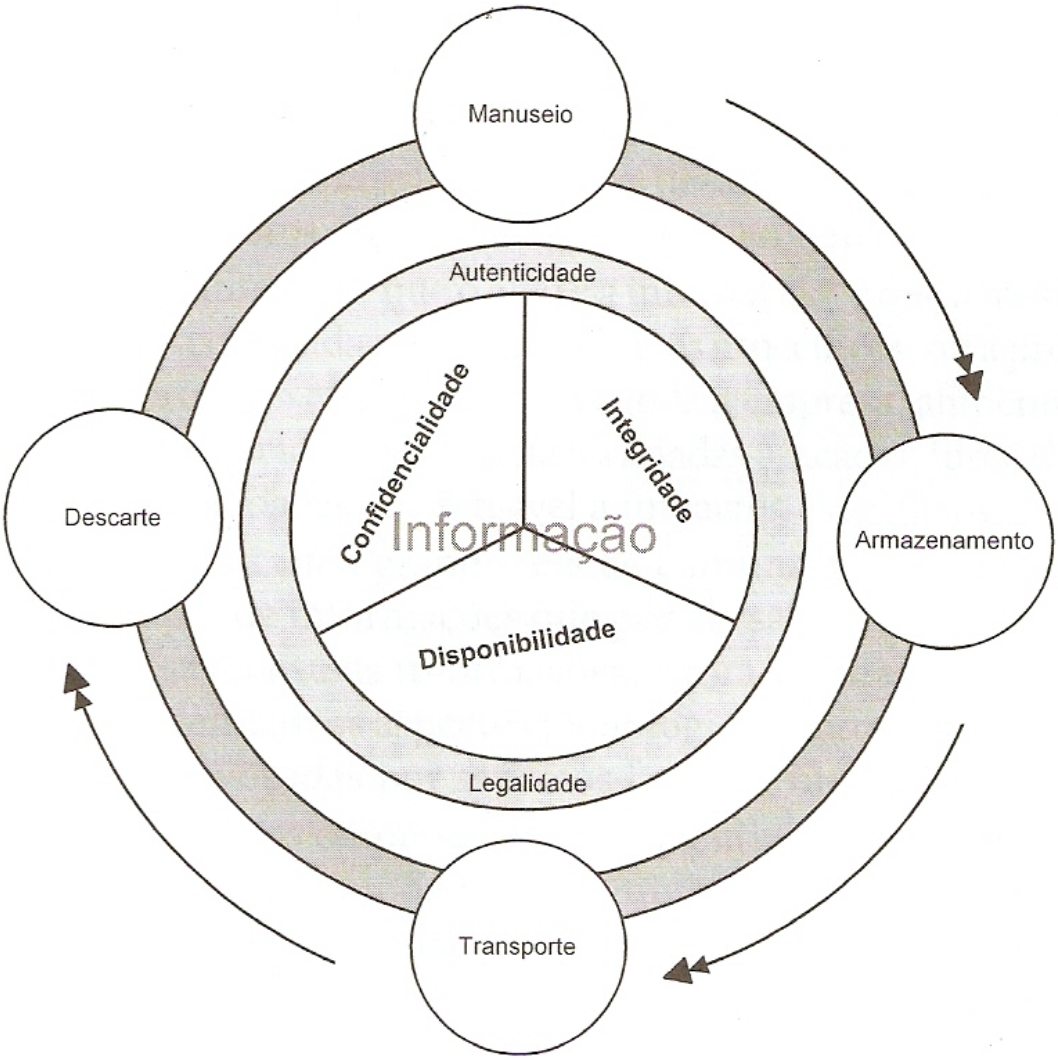

Figura 2.1 – Ciclo de vida da informação de acordo com Sêmola (2003).

2.5 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Conforme indicado em Fontes (2010), a segurança da informação versa a respeito da proteção da informação e manutenção de suas propriedades (confidencialidade, integridade e disponibilidade), minimizando os riscos de que as vulnerabilidades dos ativos relacionados sejam explorados por ameaças e possam trazer conseqüências para o negócio de uma organização.

A proteção da informação não é apenas um assunto de tecnologia, soluções técnicas, programas antivírus, são fundamentais, mas não o suficiente para que o sistema esteja protegido, é indispensável conta com uma equipe especializa em segurança para tratar de outros aspectos tais como, humanos, organizacionais e estratégicos. A proteção da informação também não acontece por milagre, exige dedicação de recursos financeiros, de tempo e de pessoas. O custo dispensado com segurança da informação deve fazer parte do negócio da organização, é mais um requisito que agrega valor ao preço final do produto, conforme Fontes (2010).

A GSI tem como principal objetivo fazer com que as decisões e ações a cerca da segurança da informação estejam alinhadas aos objetivos e estratégias do negócio da organização.

Para Santos (2007), qualquer ação de segurança exige alinhamento com o negócio da empresa, como também as iniciativas de negócio devem considerar as questões de segurança. Não se deve pensar em um novo produto de negócio para depois considerar a proteção da informação. Segurança da Informação é um processo que não acaba nunca. Mas ela não existe por si só. É ela é que vai tornar possível a realização do negócio de forma protegida no que diz respeito aos recursos de informação.

3 PRÁTICAS PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Este capítulo apresenta as principais diretrizes e princípios para iniciar, manter e melhorar a gestão de segurança da informação em uma organização.

3.1 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Organizações que pretendem gerenciar a segurança da informação em seus negócios precisam fazê-lo de forma sistêmica. A segurança da informação precisa fazer parte das atividades de todos na organização. Para isso, é necessário um documento que promova tal necessidade. Uma Política de Segurança da Informação é uma das mais importantes medidas a serem tomadas, já que será a base de princípios que seguidos pela gestão.

Para Fontes (2010), uma política de segurança tem como objetivo definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente de tecnologia da organização e que são os princípios fundamentais de como a organização exige que a informação seja utilizada, além de que se aplica a todos os usuários que utilizam as informações da organização.

Conforme a própria norma ABNT NBR ISO/IEC 17799, convêm que o documento de política de segurança da informação declare o comprometimento da direção e estabeleça o enfoque da organização para gerenciar a segurança da informação. Convêm que o documento da política contenha declarações relativas a:

a) definição da segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação.
b) declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhadas ao negócio.
c) estrutura para estabelecer os objetivos de controle e os controles, incluindo uma estrutura de gerenciamento de risco.
d) definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo registro dos incidentes de segurança da informação.

Este documento deve ser acessível e compreensível para o leitor em foco.

3.2 ANÁLISE, AVALIAÇÃO E TRATAMENTO DE RISCO

Risco é a probabilidade de que as vulnerabilidades sejam exploradas pelas ameaças existentes, danificando ou ocasionando perdas aos ativos e acarretando prejuízos aos negócios da empresa, conforme a CERT BR.

Para a norma ABNT (2005), espera-se que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a organização. Convém que os resultados determinem ações para o gerenciamento dos riscos de segurança da informação e para a implantação dos devidos controles. O processo de avaliar riscos precisa ser um processo contínuo de forma a cobrir todo o ambiente organizacional.

Convém também, que a análise/avaliação de riscos de segurança da informação tenha seu escopo definido e inclua os relacionamentos com as análises de outras áreas, se necessário. Exemplos de análise/avaliação de riscos são discutidas no ISO/IEC TR 13335-3 (*Guidelines for the management of TI security: Techniques for the management of TI secutiry*).

Segundo ABNT (2005), antes de considerar o tratamento de um risco, a organização deve definir os critérios para determinar se os riscos podem ser ou não aceitos. O risco é aceito se ele é baixo ou se seu custo do tratamento não é economicamente viável para a organização.

Para cada um dos riscos identificados, uma decisão sobre o tratamento do risco precisa ser tomada. Algumas opções incluem:

- aplicar controles apropriados para reduzir os riscos;
- conhecer e objetivamente aceitar o risco, se for o caso;
- evitar riscos, não possibilitando ações que poderiam causar outros riscos;
- transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

Para aqueles riscos aceitos, onde necessitam de tratamento e aplicações de controles apropriados, estes controles devem assegurar que os riscos sejam reduzidos a um nível aceitável, levando-se em conta:

- os requisitos e restrições das legislações vigentes;
- objetivos do negócio;
- os requisitos e restrições operacionais;

- custo de implementação e operação;
- necessidade de balancear o investimento na implementação e operação, contra a probabilidade de danos que resultem em falhas de segurança da informação.

Deve-se lembrar que nenhum conjunto de controles pode garantir a segurança completa, e que uma ação de gestão deve existir para monitorar, avaliar e melhorar a eficiência e eficácia dos controles de segurança da informação, sendo que estas ações devem sempre está alinhada ao negócio da organização.

3.3 INFRAESTRUTURA DA SEGURANÇA DA INFORMAÇÃO

Segundo a norma ABNT (2005), uma estrutura de gerenciamento deve ser estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização. É fundamental que a alta direção aprove a política de segurança da informação, delegue as funções de segurança, coordene e analise criticamente a implementação da segurança da informação por toda a organização. Se necessário, uma consultoria especializada em segurança pode ser contratada e disponibilizada dentro da organização.

Para que a infra-estrutura da segurança da informação consiga efetivamente gerenciar as questões relativas à segurança dentro da organização é necessário:

- Comprometimento da direção com a segurança da informação – por meio da definição de atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação;
- Coordenação da segurança da informação – através de representantes de diversas partes da organização, com funções e papéis relevantes;
- Atribuição de responsabilidades para a segurança da informação – estejam definidas claramente;
- Processo de autorização para os recursos de processamento da informação – através de um processo de gestão de autorização para recursos de processamento da informação;
- Acordos de confidencialidade – requisitos de confidencialidade ou acordos de não divulgação devem ser identificados e analisados.

É evidente que toda organização deve tratar o assunto de forma profissional. Normas e políticas que valem para todos envolvidos. Se outros assuntos não são tratados profissionalmente, essa cultura dificulta o processo de proteção. A organização

conta com prestadores de serviço, terceirizados, consultores, funcionários. Todos são colaboradores e devem ser lembrados no processo de segurança da informação. Não adianta uma ótima estrutura técnica se seus colaboradores não internalizam o conceito de segurança.

3.4 GESTÃO DE ATIVOS

A informatização é hoje peça fundamental no dia-a-dia profissional. Por que ela é necessária para a constante utilização dos ativos de uma empresa.

Ativo de informação é qualquer elemento de valor para a empresa que manipula, processa, armazena, transporta ou descarta a informação, incluindo a informação em si, conforme ABNT NBR ISO/IEC 13335-1.

Segundo a norma ABNT (2005), a gestão de ativos tem como principal meta, a proteção adequada dos ativos da organização e que estes sejam inventariados e tenham um proprietário responsável. É necessário que os ativos possuam identificação e a eles seja atribuída a responsabilidades pelos controles.

Os ativos de informação, excluindo-se as pessoas, são de exclusiva propriedade das instituições, que arcam com seus custos de aquisição, aluguel e manutenção. Além disso, os empregadores são responsáveis por seus empregados no exercício do trabalho e, por isso, o uso dos recursos tecnológicos deve ser feito de maneira correta, a partir dos interesses definidos pela instituição e voltados, prioritariamente aos interesses profissionais.

Para alcançar e manter esta proteção a gestão deve tratar dos seguintes aspectos:

- Inventário dos ativos – todos os ativos devem ser explicitamente identificados e um inventário dos ativos importantes precisa ser estruturado e mantido. Além disso, os inventários devem conter todas as informações necessárias tais como, tipo do ativo, formato e localização, para que em caso de um desastre, as mesmas não sejam perdidas juntamente com o próprio ativo;
- Proprietário dos ativos – informações e ativos devem ter um proprietário designado pela organização;
- Uso aceitável dos ativos – todos os envolvidos na organização devem seguir as regras para o uso permitido de informações e ativos associados ao processamento, regras para o uso da internet e do correio eletrônico.

3.4.1 CLASSIFICAÇÃO DA INFORMAÇÃO

Para Fontes (2010), a principal razão para classificar as informações é que estas não possuem os mesmos níveis de confidencialidade, ou ainda, as pessoas podem ter interpretações diferentes sobre o grau de confidencialidade. Ainda para Fontes (2010), classificar a informação é uma tarefa de esforço pequeno, mas implantar em todas as informações da organização é uma grande tarefa em termos de tempo e de associação com as demais áreas, contudo, é um assunto que merece uma abordagem profissional, quanto mais seriedade, maiores as chances de proteção da informação.

3.5 SEGURANÇA EM RECURSOS HUMANOS

O recurso humano é o principal ativo que as organizações possuem, pois segundo “Abraham Maslow” (Motivation and Personality), o ser humano vive em uma busca frenética para satisfazer suas necessidades pessoais, que são escalonadas em ordem de prioridades, a cada novo desafio vencido sempre haverá outro que ira surgir, é uma realidade aplicada às grandes organizações.

A era industrial foi um importante passo rumo ao progresso, e uma das figuras históricas da época foi Fayol (Funções Administrativas - Planejar, Organizar, Liderar e Controlar – Teoria Geral da Administração). Naquele período, as indústrias visavam notadamente os processos, sua eficiência e a produtividade acima de tudo, deixando o ser humano em segundo plano, realidade esta que ao passar dos anos foi se modificando.

O processo de recrutamento e seleção de um funcionário em uma organização, precisa ser gerido de forma cautelosa. O Departamento de Recursos Humanos tem um papel estratégico e fundamental (atrair, reter e desenvolver o capital humano no âmbito interno das organizações) esse é um paradigma que ainda não foi quebrado em muitas organizações.

3.5.1 Antes da contratação

Conforme a norma ABNT (2005), a segurança em recursos humanos deve garantir que os funcionários e todos os envolvidos, entendam suas responsabilidades e estejam de acordo com seus papéis, e reduzir o risco de roubo, fraude ou mau uso dos

recursos. As responsabilidades devem ser atribuídas antes da contratação, nas descrições de cargos e nos termos e condições de contratação, além de assinar termos de responsabilidades pela segurança da informação.

3.5.2 Durante a contratação

Segundo a mesma norma citada anteriormente, este é o momento em que os funcionários e envolvidos estejam conscientes das ameaças relativas á segurança da informação, obrigações e responsabilidades, e preparados para reduzir o risco de erro humano.

A pessoa é o elemento por onde a segurança da informação acontece na organização, conforme afirma Fontes (2010), por isso, é necessário um nível adequado de conscientização, educação e treinamento relativos aos processos que envolvem a segurança da informação e na utilização correto dos recursos de processamento da informação, voltado a todos os funcionários e envolvidos no processo, com o objetivo de minimizar possíveis riscos.

3.5.3 Encerramento ou mudança da contratação

A segurança de recursos humanos deve assegurar que funcionários deixem a organização de forma ordenada, controlada e que sejam devolvidos todos os equipamentos, bem como cancelar todos os direitos de acesso a informação, conforme requer a norma ABNT (2006), que também devem ser levado em consideração, as mudança de responsabilidades.

É fundamental que, nos casos em que o encerramento da atividade seja da iniciativa do gestor, os funcionários, podem propositalmente corromper a informação ou realizar qualquer procedimento não autorizado, ou até mesmo coletar informações para uso futuro. Funcionários insatisfeitos representam uma das principais ameaças a segurança da informação.

3.6 SEGURANÇA FÍSICA E DO AMBIENTE

3.6.1 Áreas seguras

Qualquer que seja as instalações de processamento da informação críticas ou sensíveis, com o objetivo de prevenir o acesso físico não autorizado, danos e modificações das instalações e informações confidenciais da organização, é necessário que estas instalações sejam fisicamente protegidas, conforme ABNT ISO/IEC 17799.

Perímetros de segurança tais como barreiras, paredes, divisórias, portões de entrada com cartões, podem ser utilizados, mas para isso é fundamental levar em consideração que cada medida de controle que venha a ser utilizada deve esta sempre alinhada aos ativos existentes no interior do perímetro, e dos resultados da análise de risco. Quanto maior o valor dos ativos existentes, maior será a capacidade de resistência da solução implantada.

Principais requisitos a serem analisados:

- Área de recepção;
- Alarmes;
- Sistemas adequados de detecção de intrusos;
- Processamento gerenciado pela organização em localização diferente da gerenciada por terceiros.

3.6.2 Segurança de equipamentos

Conforme a norma ABNT ISO/IEC 17799, a proteção dos equipamentos é fundamental para reduzir o risco de acesso não autorizado às informações e para proteger também a parte de infra-estrutura de equipamentos.

Equipamentos devem ser alocados em lugares protegidos e estratégicos dentro da organização, para reduzir os riscos de ameaças, e do meio ambiente. Ao realizar a instalação dos equipamentos algumas diretrizes devem ser levadas em consideração pela equipe de gestão da segurança:

- Instalação de equipamentos que manipula informações sigilosos em locais restritos;
- Itens que exigem proteção especial isolados;
- Regras estabelecidas de como comer, beber e fumar nas proximidades das instalações;

- Análise de condições ambientais.

É de suma importância que os equipamentos da organização sejam protegidos contra falta de energia elétrica e outras interrupções. Todas as instalações e equipamentos devem ser inspecionados e testados regularmente para que se reduza os riscos de interrupções casuais, além de providenciar um suprimento de energia elétrica compatível com as especificações do fabricante dos equipamentos.

3.7 GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

Toda organização que presa por qualidade deve garantir a operação segura e correta dos recursos de processamento da informação, além disso, definir as responsabilidades pela gestão e operação de todos os recursos de processamento das informações. A segregação de função também deve está inserida neste processo, visto que o recomendável é que uma pessoa faça uma ou algumas partes de um processo, mas não todas, conforme Fontes (2010).

Para gerenciar serviços terceirizados, deve-se implementar e manter o nível apropriado de segurança da informação e em conformidade com acordos de entrega de serviços terceirizados.

Segundo ABNT (2005), é de extrema importância realizar um planejamento e preparação com o intuito de garantir a disponibilidade de recursos do sistemas para minimizar o risco de falhas, bem como prever a capacidade futura dos sistemas, de forma a reduzir os riscos de sobrecarga. Também deve-se prevenir e detectar a introdução de códigos maliciosos e os usuários devem estar conscientes sobre isso.

Procedimentos para a geração de cópias de segurança e sua recuperação também devem ser estabelecidos.

Outro aspecto que também deve ser levado em consideração é a garantia do gerenciamento seguro de redes. Controles adicionais podem até mesmo ser necessários para proteger informações confidenciais que trafegam em redes públicas. As trocas de informações entre organizações devem ser baseadas em uma política formal específica, devendo ser efetuadas a partir de acordos entre as partes e sempre em conformidade com toda a legislação pertinente, diz ABNT NBR ISO/IEC 18028.

Mecanismos de monitoração e registro apropriados sejam aplicados, para controlar atividades não autorizadas de processamento da informação. Os eventos de segurança da informação devem ser registrados, lembrando que as organizações devem

estar aderentes aos requisitos legais aplicáveis para suas atividades de registro e monitoramento.

3.8 CONTROLE DE ACESSOS

Para a ABNT (2005), o acesso à informação, aos recursos de processamento das informações e aos processos de negócios deve ser controlado com base nos requisitos de negócio e na segurança da informação. Portanto, deve ser assegurado o acesso de usuário autorizado e prevenido o acesso não autorizado a sistemas de informação. Para isso, deve haver procedimentos que englobem desde o cadastro inicial de um novo usuário até o cancelamento final do seu registro, garantindo assim que já não possuem mais acesso a sistemas de informação e serviços.

Os usuários sempre devem estar conscientes de suas responsabilidades, particularmente no que se refere ao uso de senhas e de segurança dos equipamentos de usuários. Nesse sentido, sugere-se ainda a adoção da “política de mesa e tela limpa”, para reduzir o risco de acessos não autorizados ou danos a documentos, papéis, mídias e recursos de processamento da informação que estejam ao alcance de qualquer um.

Boa parte das organizações possui controle total para limitar o acesso ao conteúdo de seus funcionários. Através dos conhecidos e mais utilizados firewall para proteção. Um firewall é uma espécie de filtro projetado para bloquear ou admitir determinados tipos de trafico na rede. Por exemplo, pode bloquear sites entendidos como impróprios, ou que não se adéquam aos objetivos da empresa.

Define quais informações o usuário tem acesso, quais dados ele pode visualizar, alterar ou excluir. Autorização e controle de acesso é uma forma de dividir responsabilidades. A informação dentro de uma empresa deve ser classificada e disponibilizada de acordo com a necessidade de cada usuário. A autenticação é o mecanismo de controlar quem pode e quem não pode visualizar determinada informação.

Pelo fato do controle de acesso ser dependente da identificação do usuário, a autorização de uso é frequentemente integrada com os mecanismos de autenticação, conforme Masahiro (2009).

3.9 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

Segundo a norma, “Sistemas de informação incluem sistemas operacionais, infraestrutura, aplicações de negócios, produtos de prateleira, serviços e aplicações desenvolvidas pelo usuário”. Por essa razão, os requisitos de segurança de sistemas de informação devem ser identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, já que o projeto e a implementação de sistemas de informação criados com o intuito de apoiar o processo de negócios, são tidos como pontos cruciais para a segurança.

Requisitos de sistemas para a segurança da informação e os processos para implementá-las devem ser integrados aos processos iniciais dos projetos de sitemas de informação, já que assim reduz o custo significativamente em relação aqueles incluídos após a implementação, conforme indicado em ABNT (2005).

3.10 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Segundo a CERT.BR (2006), um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores. São exemplos de incidentes de segurança:

- tentativas de ganhar acesso não autorizado a sistemas ou dados;
- ataques de negação de serviço;
- uso ou acesso não autorizado a um sistema;
- modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;
- desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

Ainda para a CERT.BR (2006), as principais ameaças à segurança da informação para as organizações são mostradas no Gráfico 3.1 abaixo:

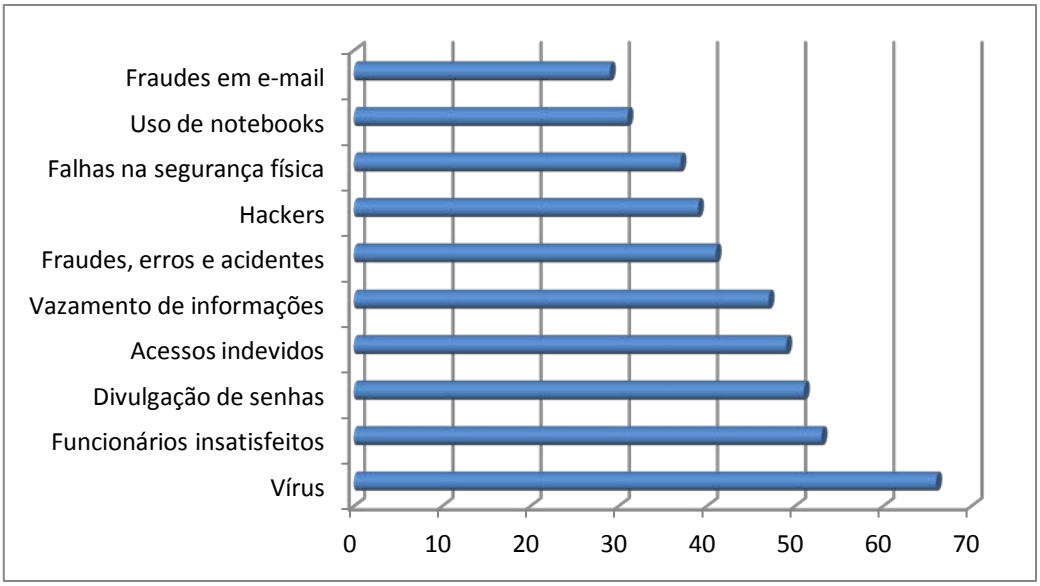

Gráfico 3.3 - Principais ameaças à segurança da informação. Valores em percentagem. Observação: o total de citações é superior a 100% devido à questão aceitar múltiplas respostas.

A norma ABNT NBR ISO/IEC 17799, sugere que se deve assegurar que qualquer evento de segurança da informação, seja o quanto antes comunicado, de tal forma que a tomada de ação corretiva ocorra em tempo hábil. Para isso, devem ser estabelecidos procedimentos formais de registro e escalonamento, bem como todos os funcionários, fornecedores e terceiros devem estar conscientes sobre os procedimentos para notificação dos diferentes tipos de eventos.

3.11 GESTÃO DE CONTINUIDADE DO NEGÓCIO

Segundo a norma ABNT NBR ISO/IEC 17799, a gestão de continuidade do negócio tem como objetivo, impedir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar que a sua retomada ocorra em tempo hábil.

Para isso, planos de continuidade do negócio, incluindo controles para identificar e reduzir riscos, devem ser desenvolvidos e implementados, visando assegurar que as operações essenciais sejam rapidamente recuperadas.

No Brasil atualmente, as atividades relacionadas à continuidade dos negócios estão basicamente restritas às organizações em que os processos de negócios dependente de forma relevante da TI, diante deste panorama, é necessário que as

organizações, convivam com crises e as administrem de maneira que possam contorná-las de forma rápida e eficiente.

3.12 CONFORMIDADE

A norma ABNT ISSO/IEC 17799, relata que a Conformidade deva garantir e evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

Para isso, é conveniente contratar, caso necessário, consultoria especializada, bem como analisar criticamente a segurança dos sistemas de informação a intervalos regulares, verificando, sobretudo, sua conformidade e aderência a requisitos legais e regulamentares.

Em resumo, nota-se claramente ao longo de toda a norma, que a característica predominante é a prevenção, evitando-se a todo o custo, a adoção de medidas de caráter reativo. Mesmo as que forem reativas, como por exemplo, a execução de um plano de continuidade de negócios, são previamente planejadas para que, no momento oportuno e se necessárias, sejam devidamente implementadas.

Segundo Peixoto (2006), um teste de conformidade tem como principal objetivo, permitir a percepção relativa ao grau de conformidade que a organização possui em relação aos controles sugeridos pelo código de conduta de gestão de segurança da informação definidos pela norma ABNT NBR ISO/IEC 17799.

4 INSTITUIÇÕES FINANCEIRAS NO BRASIL E SEGURANÇA DA INFORMAÇÃO

Neste capítulo são apresentadas algumas definições e aspectos relacionados às instituições financeiras no Brasil, além de fazer uma análise do contexto atual destas instituições no que se refere à segurança da informação.

4.1 INSTITUIÇÕES FINANCEIRAS

Segundo Fortuna (2008), as instituições financeiras no Brasil estão divididas em dois tipos, monetárias e não monetárias, sendo a primeira mais conhecida até mesmo pela natureza e múltiplas funções, onde os Bancos Comerciais tem papel de destaque constituindo a base do sistema monetário, devido muito aos serviços prestados.

Ainda de acordo com Fortuna (2008), instituições financeiras monetárias são aquelas que possuem depósito à vista e, portanto, multiplicam a moeda, dentre elas destacam-se:

- Bancos Comerciais;
- Caixas Econômicas;
- Bancos Cooperativos;
- Cooperativas de Crédito.

4.2 SEGURANÇA DA INFORMAÇÃO NA ESFERA DAS INSTITUIÇÕES FINANCEIRAS

Para Fortuna (2008), a Tecnologia da Informação (TI) se apresenta como um vetor de diferenciação, competitividade e eficiência em qualquer negócio. Na esfera financeira não é diferente, em diversas atividades, mas principalmente nos processos de negócios e na criação de diversos serviços que necessitam de canais de comunicação entre a financeira e os clientes, tais como *Home Banking* ou do *Mobile Bank.*

No entanto, as tecnologias utilizadas para suporte de processos de instituições financeiras são um importante fator de risco que precisa ser monitorado e controlado.

Segundo a empresa KPMG (cutting throug complexity), um dos maiores bancos britânicos foi multado em um milhão de Libras quando um portátil que continha informações de clientes, fora roubado da casa de um funcionário. O disco do computador não estava protegido, e com isso, entidades reguladoras concluíram que o banco falhou no seu dever de proteger informação dos seus clientes.

Fraudes bancárias, funcionários insatisfeitos, acessos indevidos, má utilização de correio eletrônico corporativo, hackers, divulgação de senhas, falhas de infraestrutura, são as principais ameaças a qualquer organização, e no setor financeiro, com toda complexidade envolvida é de extrema importância que a alta diretoria juntamente com a área de TI tome providências com o objetivo de:

- Proteger seus ativos de informação;
- Garantir uma capacidade de resposta eficaz, quando da ocorrência de incidentes e minimizar i impacto financeiro, operacional e a imagem da instituição;
- Respeitar a legislação vigente;
- Manter a confiança dos clientes, funcionários, entidades reguladoras e acionistas.

5 ESTUDOS DE CASO COMO ESTRATÉGIA DE PESQUISA NA ÁREA DE SEGURANÇA DA INFORMAÇÃO

Conforme indicado em Fernandes (2010), a característica exploratória dos estudos de casos é importante para analisar gestão de segurança da informação em organizações. Neste capítulo, são apresentadas algumas teorias a respeito da técnica de pesquisa, e também o próprio estudo de caso realizado como proposta deste trabalho.

5.1 ESTUDO DE CASO

A pesquisa baseada em estudo de caso diz respeito à investigação de uma situação dentro de um ambiente específico. Variáveis e fatores são observados nesse contexto, além de suas relações, na busca por evidências que mostrem ou descrevam uma determinada situação, conforme indicado em Gomes (2006).

Segundo Fernandes (2010), estudos de caso podem além de poderem servir de pressupostos a generalizações, como também descrevem uma determinada configuração de ambiente. Em estudos de casos utilizados para verificar o estado atual da segurança da informação em uma instituição financeira, por exemplo, é possível conceber uma pesquisa de caráter incipiente, com o intuito de diagnosticar a situação deste ambiente.

5.2 ESTUDO DE CASO REALIZADO NA INSTITUIÇÃO FINANCEIRA IFB

Este estudo de caso teve como objetivo primordial observar, analisar e descrever à cerca da gestão da segurança da informação em uma instituição financeira, e baseou-se em tópicos principais relativos á segurança da informação: políticas de segurança da informação, infra-estrutura de tecnologia da informação (TI) e práticas de gestão da segurança da informação. Estes tópicos foram escolhidos por que grande parte dos controles de segurança da informação estão especificados em ABNT (2005) e ABNT (2006). A instituição financeira IFB foi assim denominada para que não fossem expostas informações confidenciais, vulnerabilidades, dentre outros.

O estudo de caso objeto desta pesquisa, fora de natureza exploratória, com o intuito de avaliar a situação atual da segurança da informação na instituição IFB. Os métodos e técnicas de pesquisa foram os seguintes:

- **Observação direta –** Através de análise do dia-a-dia de trabalho na agência;

- **Entrevistas –** Através de questionários que se encontram no anexo deste trabalho, foram realizadas entrevistas com os responsáveis pelas ações relacionadas a TI e à segurança da informação, com o objetivo principal de coletar dados acerca da segurança da informação na instituição IFB, além da coleta de depoimentos de funcionários e colaboradores das agências.

  As entrevistas como foco no elemento política de segurança da informação e com foco em infra-estrutura de segurança da informação foram realizadas com um gerente executivo do ambiente de TI e também com um gerente executivo de agência. O questionário verificador de conformidade com a norma ABNT (2005) foi aplicado aos colaboradores mais aptos e familiarizados com cada questão proposta. A tabela abaixo indica os participantes que foram entrevistados com cada de tipo de questionário.

Participante	Cargo/Função	Foco do Questionário
1	Gerente executivo de TI	Política de Segurança
2	Gerente executivo de agência	Política de Segurança
3	Gerente executivo de TI	Infraestrutura de TI
4	Gerente executivo de agência	Infraestrutura de TI
5	Gestores, analistas, contratados, etc.	Verificador de Conformidade

Figura 5.1: Participantes entrevistados e focos dos questionários utilizados.

5.3 A INSTITUIÇÃO FINANCEIRA IFB

A IFB é uma instituição financeira de economia mista que atua como banco de desenvolvimento e diferencia-se da maioria instituições financeiras pela missão que tem a cumprir: atuar como instituição financeira, promovendo o desenvolvimento sustentável em sua área de atuação, integrando-se na dinâmica da economia nacional.

Tem como principal aspiração fazer uma política de desenvolvimento sustentável seletiva e ágil, capaz de influenciar de maneira decisiva para a superação dos problemas e para a construção de um modo de vida que esteja alinhado aos recursos, oportunidades e potencialidades da região em que atua.

5.3.1 Gestão e Estrutura Organizacional

Existe na IFB uma presidência e uma diretoria composta por seis integrantes, cada uma responsável por uma área da instituição.

- Diretoria de gestão do desenvolvimento
- Diretoria de negócios
- Diretoria financeira e de mercado de capitais
- Diretoria de administração de recursos de terceiros
- Diretoria de controle e risco
- Diretoria administrativa e de tecnologia da informação.

Além destas diretorias, existe ainda a área jurídica vinculada diretamente à presidência.

Os processos relativos a TI da IFB são geridos pela diretoria administrativa e de tecnologia da informação e executados pelo Ambiente de Tecnologia da Informação e suas células específicas a cada assunto.

5.4 A SEGURANÇA DA INFORMAÇÃO NA IFB

A segurança da informação na IFB apresenta um nível elevado de maturidade, pois existe uma preocupação clara e evidente por parte de todos os envolvidos nas atividades da instituição. Existe uma política de segurança bem elaborada e alinhada ao código de conduta ética dos funcionários e colaboradores. A sua elaboração teve a participação de todas as áreas que constituem a instituição e com direto apoio da presidência e diretoria, além de possuir uma diretoria específica para tratar dos assuntos relacionados a TI. Um analista de TI ressalta em depoimento que:

> “Muitos dos requisitos de conformidade, exigências de órgãos reguladores (BACEN, por exemplo), são assegurados pela política de segurança da instituição”.

A IFB possui inclusive um planejamento estratégico de tecnologia que estabelece o direcionamento, ações e os recursos da área de TI para um período estipulado entre três e quatro anos, alinhado ao planejamento estratégico institucional geral.

Este planejamento é aprovado pela diretoria da IFB, além de ser elaborado de forma estruturada, realizado em três fases: diagnóstico, definição do cenário futuro e definição do programa. Uma das principais motivações para realização deste planejamento é a definição do orçamento de TI. Depois de definido tal orçamento é

avaliado e gerenciado, sistematicamente, em conformidade com natureza dos gastos, prazos e valores. Um dos gerentes de ambientes de TI expressa que:

> "A diretoria dá total apoio à segurança da informação, com claro direcionamento e demonstração de comprometimento. Há cinco anos, a presidência juntamente com seu corpo diretor criou uma diretoria para tratar destes assuntos, inclusive com mesmo nível hierárquico das outras".

A IFB investe muitos recursos financeiros na conscientização de seus funcionários e colaboradores acerca da segurança da informação e na utilização correta de seus sistemas. Os treinamentos existentes visam à divulgação da Política de Segurança, treinamentos específicos, palestras externas. Existe um curso de segurança da informação, na comunidade de aprendizagem virtual que a IFB mantêm, aberto para todos os colaboradores, inclusive estagiários, mas os cursos mais abrangentes relacionados ao assunto têm preferencialmente o corpo gerencial da agência como público alvo, conforme relata um gerente de suporte:

> "Os cursos externos, fornecidos para os funcionários tem tratamento diferenciado para gerentes, analistas e contratados terceirizados, dificilmente um analista fará este tipo de curso. E os gerentes quando do retorno tentam passar o conhecimento adquirido a todos em reuniões aos finais de expediente".

Já para um analista de negócio:

> "O banco estimula pouco. Acredito que por se tratar de uma questão de extrema relevância, deveria ser exigido de cada colaborador a realização do curso de segurança da informação via comunidade virtual".

Pelo fato de a IFB possuir milhares de funcionários e colaboradores não é tarefa trivial gerenciar e monitorar o passo a passo de cada envolvido. A IFB realiza isso através de uma gestão de *log* que controla e registra quaisquer tentativas de acesso direto e indireto de usuários (autorizados ou não) ocorridos nos recursos de infra-

estrutura (servidores, redes, entre outros). A utilização deste recurso é para que ocorrências sejam registradas a fim de detectar eventos ou ações que indiquem falhas de segurança em processos. As informações que farão parte do *log* são organizadas levando-se em consideração a importância que as mesmas têm para a IFB e são armazenadas de forma centralizada de forma que seja possível garantir sua integridade.

A instituição IFB possui uma gestão de incidentes de segurança, que tem como responsabilidade, tratar e solucionar qualquer evento adverso que comprometa ativos tecnológicos, pessoas, patrimônio ou processos de negócio, que talvez possam causar prejuízo à IFB. Todos os colaboradores têm a responsabilidade de notificar vulnerabilidades e eventos que possam causar impacto aos ativos da instituição ao ambiente de segurança e este tratar, monitorar e acompanhar adequadamente aspectos que envolvam incidentes de segurança. Um analista de negócio ao ser entrevistado ressalta que:

> "Todos nós, colaboradores somos instruídos a ler a norma da instituição referente a todos os assuntos, inclusive acerca de segurança da informação, possíveis ameaças, novos incidentes relatados, além de recebermos diariamente lembretes através de correio eletrônico com qualquer atualização normativa."

A IFB dividiu os incidentes em duas modalidades: segurança da informação e segurança bancária. Também criou uma lista dos principais eventos, os mais importantes, os mais freqüentes e ainda, estabeleceu um nível de criticidade e um tempo máximo de atendimento para cada tipo de incidente.

Na IFB, é de responsabilidade de cada colaborador proteger a informação e os recursos de processamento da informação, contra modificação e divulgação não autorizadas, furto e roubo. Informações secretas ou confidenciais devem ser guardadas em mobílias com tranca ou cofres, quando da não utilização. Este mesmo tipo de informação está armazenada em servidores de rede, disponíveis apenas para pessoas autorizadas, mediante acesso às pastas onde estão localizadas. Informações institucionais são classificadas no momento da elaboração e estas são realizadas pelo gestor responsável pela informação.

Foi possível observar que por conta da enorme quantidade de serviços e um número de funcionários insuficiente, muitas vezes funcionários, geralmente com

funções comissionadas, fornecem suas senhas de identificação para que colaboradores terceirizados realizem operações com o objetivo de agilizar suas atividades, mesmo sabendo que é vedado ao colaborador compartilhar a conta pessoal e a respectiva senha de acesso, conforme resposta do gerente executivo de agência abaixo.

> "Trabalhamos todo dia buscando a eficiência e eficácia em nossas atividades nas agências. Em virtude da grande demanda de serviços e muitas vezes baixa quantidade de funcionários concursados, existe uma prática eu diria comum de funcionários passar suas senhas de identificação na rede para terceiros para a realização de atividades e consecução das metas".

Observou-se também que todo acesso a pastas contendo imagens, vídeo, áudio entre outros, é considerado indevido, pois não estão em conformidade com os interesses institucionais.

Todos os assuntos relativos a incidentes de segurança, tratamento da informação, responsabilidades de cada funcionário, ameaças, riscos, vulnerabilidades, enfim, aspectos relacionados à segurança da informação, são abordados em um curso interno promovido pela própria IFB, e que todo colaborador deve realizar, fazendo parte do processo de conscientização em segurança.

Em relação à segurança física e do ambiente, a IFB possui uma gestão dos recursos de segurança bancária e patrimonial, dentre os principais recursos de segurança destacam-se:

- **Vigilância Ostensiva** – atividade exercida no interior das instalações com o objetivo de resguardar a integridade física individual de colaboradores e clientes, proteger o patrimônio da empresa e imagem da IFB.
- **Sistema de alarme** – implantados sistemas de alarme antiassalto, antiincêndio e antiintrusão.
- **Porta Giratória Detectora de Metais** – recomenda às instituições financeiras, pelo Ministério da Justiça.
- **Sistema de Circuito Fechado de Televisão** – proporciona observação eletrônica, dos ambientes internos da unidade, gravando e, quando necessário, transmitindo as imagens a uma central de monitoramento.
- **Fragmentadora de papéis** – evita ações de engenharia social.

- **Sistema de Caixas-fortes e Cofres** – propicia, de forma adequada, a guarda e a proteção de valores e de vens sob a responsabilidade das unidades.

O fornecimento de energia elétrica e climatização também são entendidos como elementos de infra-estrutura de TI. Estes itens são planejados e atendem de forma adequada às necessidades dos serviços de TI. O servidor principal de cada unidade, bem como os equipamentos de rede, estão localizados em sala climatizada de acordo com as especificações do fabricante de todos os equipamentos ali localizados. Cada unidade também dispõe de um gerador de energia que é acionado no momento da falta de energia elétrica da rede pública. Além do gerador alguns microcomputadores críticos das agências possuem um *no-break*, proporcionando assim redundância no fornecimento de energia possibilitando a continuidade dos serviços oferecidos. A IFB através do ambiente de tecnologia possui um plano contemplando sistemáticas de contingência e recuperação de desastres de forma a manter a continuidade dos serviços essenciais à realização dos negócios, conforme afirmado pelo gerente executivo em resposta a este assunto.

> "Existe um plano que contém soluções de alimentação elétrica, climatização, segurança física, acomodação de equipamentos e mídias eletrônicas."

Observa-se que em relação à aquisição, desenvolvimento e manutenção de sistemas de informação, a instituição possui uma célula de gestão de suporte ao desenvolvimento que trata do desenvolvimento e melhoria do processo de software na instituição, que administra dados e objetos, apoiando as equipes de desenvolvimento, prospecta e acompanha o mercado de fornecedores de software, prover suporte às equipes de desenvolvimento, mantêm equipe desenvolvedora dentro das empresas para auxiliar na implementação e monitoração dos sistemas desenvolvidos.

Já em realização ao processo de backup das agências foi identificado um grande problema, pois a realização deste processo se dá apenas nos finais de expediente e não de forma automática, conforme mencionado pelo gerente executivo de TI.

> "O sistema de backup é realizado ao final de cada expediente, em servidor próprio nas agências e replicados a uma central de tecnologia da IFB. Os dados ficam armazenados em fitas guardadas

> numa sala de equipamentos dentro de uma estrutura a prova de desabamentos e incêndios, acessados apenas por pessoas autorizadas".

Os contratos de serviços de mão de obra são sempre vinculados a pessoa jurídica provedora. As agências em caráter de excepcionalidade para atender uma demanda por um serviço urgente e não rotineiro, podem contratar esses serviços. A gerência de recursos humanos e de logística é responsável pelo acompanhamento e fiscalização dos serviços prestados.

5.5 AVALIAÇÃO DO ATENDIMENTO DOS OBJETIVOS DE CONTROLES DE SEGURANÇA DA INFORMAÇÃO NA IFB

Foi formulado um questionário verificador de conformidade com a norma ABNT NBR ISO/IEC 17799 e ABNT NBR ISO/IEC 27002, presente no Anexo deste trabalho com base em Praticando a Segurança da Informação em Edison Fontes (2010).

Com base nos resultados obtidos através da aplicação do questionário, contata-se que a Política de Segurança da Informação e demais controles e regulamentos é baseada na ABNT NBR ISO/IEC 27002. Avaliaram-se os objetivos de controle de segurança da informação presentes na IFB em relação ao seu atendimento. As respostas apresentadas abaixo como ***sim*** significa que todos os controles de dado objetivo são atendidos, ***parcialmente*** significa que alguns controles são atendidos e ***não*** significa que nenhum controle é atendido.

Objetivo do Controle	**Atendimento ao objetivo de controle**
Política de Segurança da Informação	Parcialmente
Fatores Críticos de Sucesso	Sim
Infraestrutura de segurança da informação	Sim
Gestão de Ativos	Sim
Segurança em Recursos Humanos	Não
Segurança Física e do Ambiente	Sim
Gerenciamento das Operações de Comunicação	Sim
Controle de Acesso	Sim
Aquisição, Desenvolvimento e Manutenção de Sistemas	Parcialmente
Gestão de Incidentes de Segurança	Sim

Gestão da Continuidade do Negócio	Sim
Conformidade	Sim

Figura 5.5: Avaliação do atendimento dos objetivos de controle de segurança da informação na IFB

5.6 ANÁLISE DOS RESULTADOS

Além da atual situação da gestão de segurança da informação na instituição IFB, o estudo de caso proposto neste trabalho através do questionário verificador de conformidade com a norma ABNT verificou outros pontos sobre os quais pode-se atuar para melhorar a segurança da informação, tais como:

- Observou-se que apesar de a IFB possuir uma política de segurança da informação elaborada e alinhada ao código de conduta ética dos funcionários, não existe um documento que formalize o conhecimento de todos os envolvidos acerca desta política, nem mesmo um controle que garanta que a política é obrigatoriamente de conhecimento geral, diante disto o atendimento a este objetivo se deu de forma parcial;
- Ficou constatado também, que diante da grande demanda de serviço na instituição, existe uma prática comum de que gestores passam suas senhas de acesso aos sistemas de informação da instituição para funcionários terceirizados e estagiários, com o objetivo de agilizar as tarefas e conseguir metas, com isso o objetivo de controle de recursos humanos não foi atendido de maneira adequada segunda a norma proposta;
- O objetivo do controle aquisição, desenvolvimento e manutenção de sistemas, foi atendido parcialmente, segundo a norma, pois no ambiente computacional existe apenas um ambiente para tratar do desenvolvimento, teste e produção, quando deveria ser em ambientes distintos, além disso, não existe uma preocupação da instituição relativo ao grau de certeza da continuidade do fornecedor de sistemas no mercado de tecnologia.

5.7 CONSIDERAÇÕES FINAIS

Neste capítulo foi relatado o cenário de gestão da segurança da informação na instituição financeira IFB, os dados foram levantadas por meio de estudo de caso proposto para este trabalho.

Estudos de caso, semelhante ao realizado neste trabalho relativo à gestão da segurança da informação na instituição IFB, podem inclusive ser utilizados para preparar e orientar organizações, para que estejam em conformidade com os requisitos, políticas de segurança da informação aos quais estão sujeitas. Assim sendo, pode-se utilizar estudos como este como forma de preparação para auditorias, com o intuito de identificar eventuais falhas e adequações necessárias.

6 CONCLUSÃO

Por meio deste trabalho, e do estudo de caso utilizado, foi possível realizar uma avaliação da instituição financeira IFB quanto à sua gestão de segurança da informação e práticas de segurança da informação, observando seus controles e à observação as normas e legislações a que está sujeita.

Percebeu-se que a gestão da segurança da informação nesta instituição é uma questão já bem desenvolvida, inclusive por contar com uma política de segurança bem definida e de acesso a todos os colaboradores, embora ainda não exista um bom mecanismo para divulgação e conscientização desta política. Por se tratar de uma instituição financeira e por isso, a informação ser algo considerado como elemento crítico, o conhecimento da política de segurança da instituição deve ser de conhecimento de todos, contudo se faz necessário uma melhor prática para solução deste problema, mesmo diante de toda a complexidade de uma instituição financeira.

Pôde-se se observar também que a alta administração da IFB, através de seu planejamento estratégico e políticas orçamentárias consideram as questões relacionadas à infraestrutura de tecnologia, o orçamento direcionado aos recursos de TI e a segurança da informação. Existe na instituição uma diretoria para tratar dos assuntos relacionados a TI, e esta diretoria ocupa o mesmo nível hierárquico que, por exemplo, uma diretoria de negócio.

Houve também a percepção da necessidade de algumas melhorias em alguns processos tais como a realização de backup e o tratamento dos contratos de prestadores de serviços terceirizados, bem como uma melhor conscientização dos funcionários no que se refere à utilização de senhas de acesso a rede.

Outra observação importante é a preocupação evidente da administração da IFB com questões relativas à segurança de pessoal e do ambiente, existem implantados controles com o objetivo de prover a segurança dos seus clientes, colaboradores e ativos de TI, por meio de uma gestão de segurança bancária e patrimonial. A IFB também dispõe de um plano bem definido de análise de riscos, contingência e recuperação de desastres.

6.1 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.

7 REFERENCIAL BIBLIOGRÁFICO

ABNT. **Associação Brasileira de Normas Técnicas**. ABNT NBR ISO/IEC 17799. ABNT, Rio de Janeiro, (2005).

ABNT. **Associação Brasileira de Normas Técnicas**. ABNT NBR ISO/IEC 27002. ABNT, Rio de Janeiro, (2007).

CERT.BR, **Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil, Incidentes Reportados ao Cert,** Disponível em < http://www.cert.br/stats/incidentes/2012-apr-jun/tipos-ataque.html>, acesso em 12 de ago de 2012.

CERT.BR, **Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil, Estatísticas dos Incidentes Reportados ao CERT.** Disponível em < http://www.cert.br/stats/incidentes/>, acesso em 12 de out de 2012.

CERT.BR, **Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil, Cartilha de Segurança para Internet.** Disponível em < http://cartilha.cert.br/>, acess em 12 de ago de 2012

FERNANDES, J. H. C. **Metodologia de Pesquisa de Estudo de Caso no Programa de Formação de Especialistas para Desenvolvimento da Estratégia e Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações**. Brasília, Universidade de Brasília 2010.

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

FORTUNA, Eduardo. **Mercado Financeiro – Produtos e serviços**. Rio de Janeiro: Quality mark 2008.

GOMES, J. S. **O Método de Estudo de Caso Aplicado à Gestão de Negócios**. Atlas, 2006.

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

PINHEIRO, Patrícia Peck. **Advogados Especialistas em Direito Digital.** Disponível em http://www.pppadvogados.com.br, acesso em 09 de ago de 2012.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo, Saraiva, 2010.

SANTOS, Alfredo Luiz dos. **Gerenciamento de identidades: Segurança da Informação**. Rio de Janeiro, Brasport, 2007.

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

APÊNDICE A

Instrumento de Pesquisa – Respostas dos Questionários

Os dados e informações coletados através deste questionário serão utilizados unicamente para a pesquisa acadêmica do curso de bacharelado em Ciência da Computação da Universidade Estadual do Sudoeste da Bahia (UESB). As informações serão apresentadas sem a identificação dos entrevistados e da instituição, com o objetivo de analisar a gestão de segurança da informação.

Respostas aos questionários relativos à política de segurança da informação, gestão da segurança da informação e infraestrutura de tecnologia da informação.

Política de Segurança da Informação e Gestão de Segurança da Informação

Entrevistado: Gerente Executivo de TI

1. **A instituição financeira possui uma política de segurança da informação? Ela considera as visões de todos os envolvidos?**
   Sim, existe um documento de política de segurança que é disponibilizada a todos os colaboradores, mas não existe um controle de que todos leram.
2. **Qual o intervalo de tempo que a política de segurança da informação é revisada? Este intervalo de tempo é definido ou ocorre quando mudanças significativas na instituição?**
   A política de segurança é revisada de dois em dois anos, ou quando houver necessidade, por conta de alguma alteração na instituição.
3. **Existe uma conscientização da importância da política de segurança da informação por parte dos colaboradores? Como isto é mensurado?**
   Acredito que sim, conseguimos mensurar isto com a realização de cursos em nosso canal de aprendizado em segurança da informação e através também da diminuição do índice de incidentes.
4. **A política de segurança da informação define os papéis e responsabilidades pela segurança da informação?**
   Sim.

5. **Quando da formulação do planejamento estratégico da organização, a segurança da informação é considerada?**

   Sim, o planejamento estratégico institucional é realizado em consonância com o planejamento estratégico de TI.

6. **A diretoria da instituição considera a gestão da segurança da informação como questão crítica para a organização?**

   Sim, já que existe uma diretoria (diretoria administrativa e de tecnologia da informação) que trata deste assunto.

7. **As decisões relacionadas com a segurança da informação são tomadas exclusivamente pela área de TI ou em conjunto com a equipe responsável pelas decisões estratégicas da organização?**

   Por todas as áreas da instituição representadas por suas diretorias.

8. **O acesso ás informações preserva os critérios de confidencialidade, integridade e disponibilidade?**

   A nossa infra-estrutura de tecnologia trabalha com esse objetivo, mas é claro que existem falhas eventuais, até mesmo por se tratar de uma instituição financeira de grande porte.

9. **Como é feita a identificação dos riscos? Eles são previstos através de um plano de contingência?**

   Os riscos são identificados, mensurados e tratados. Existe um plano de contingência que define a criticidade do risco e o seu tempo de atendimento.

10. **Existem controles e requisitos de segurança da informação quando dos contratos com terceiros?**

    Existe uma grande quantidade de contratos com terceiros na instituição, o objetivo é diminuir ao máximo. Ainda ocorre que funcionários terceirizados possuem acesso a informações não necessárias para o desenvolvimento de suas atividades. As agências, através de seus gerentes executivos e de recursos humanos, gerencia estes colaboradores.

Infraestrutura de Tecnologia da Informação (TI) e Gestão de Segurança da Informação

1. **Como é vista a infraestrutura de TI na organização? Há compreensão, dentro da instituição, da influência da infraestrutura de TI no cumprimento da missão?**

   É sabido por todos que a infra-estrutura de TI é considerada fundamental, já que se trata de uma instituição financeira e boa parte dos serviços oferecidos são suportados por sistemas.

2. **A diretoria vê a infraestrutura de TI como elemento estratégico da instituição? Como a diretoria trata dos investimentos em infraestrutura de TI pela organização?**

   Sim. O orçamento de ações empresariais é discutido juntamente o orçamento de TI através de uma política orçamentária. Todos os gastos em TI são submetidos a uma célula de governança em TI.

3. **A cultura organizacional relaciona a infraestrutura de TI aos riscos da instituição?**

   Sim. A cultura da IFB entende como fator preponderante para os resultados financeiros a infraestrutura de TI.

4. **Como as falhas em elementos da infra-estrutura de TI afetam a prestação de serviços e confiabilidade da organização? Qual a relação entre eficiência da instituição e sua infraestrutura de TI?**

   Sabemos que a maior parte dos nossos serviços são suportados por sistemas, com isso, a indisponibilização de qualquer serviço gera um desgaste com os clientes, e impacta negativamente na imagem da IFB.

5. **O fornecimento de energia elétrica e climatização são vistos como elementos de infraestrutura de TI?**

   Sim. É considerado fator crítico para o sucesso.

6. **Quais controles de acesso físico aos ambientes de TI e ambientes de acesso restrito?**

   Geralmente os controles são realizados através da identificação do funcionário, além da divulgação e conscientização que estes controles precisam da colaboração de todos. Infelizmente isto por si só, não garante a eficácia do controle.

7. **Os equipamentos de uso individual são vistos como ativos da infra-estrutura de TI da organização e elementos necessários à eficiente prestação de serviço pela instituição?**
   Sim.

8. **Como é realizado o processo de armazenamento e recuperação de dados utilizados pela instituição?**
   O sistema de backup é realizado ao final de cada expediente, em servidor próprio nas agências e replicados a uma central de tecnologia da IFB. Os dados ficam armazenados em fitas guardadas numa sala de equipamentos dentro de uma estrutura a prova de desabamentos e incêndios, acessadas apenas por pessoal autorizado.
9. **O monitoramento do correto funcionamento dos equipamentos da infra-estrutura de TI é feito? Os resultados do monitoramento são usados para melhoria da infra-estrutura de TI?**
   Sim. Algumas vezes a própria central detecta os erros antes mesmo dos funcionários das agências. Os funcionários das agências ainda reclamam da demora no atendimento por partes dos colaboradores da central de TI.

Entrevistado: Gerente Executivo de agência

1. **A instituição financeira possui uma política de segurança da informação? Ela considera as visões de todos os envolvidos?**
   Sim, a política de segurança da informação existe e é disponibilizada a todos, mas poderia se adotar melhores práticas de conscientização e divulgação deste regulamento.
2. **Qual o intervalo de tempo que a política de segurança da informação é revisada? Este intervalo de tempo é definido ou ocorre quando mudanças significativas na instituição?**
   A política de segurança é revisada de dois em dois anos, ou caso aconteça alguma eventualidade nas leis nacionais, que se façam necessário uma alteração imediata.
3. **Existe uma conscientização da importância da política de segurança da informação por parte dos colaboradores? Como isto é mensurado?**

Sim. Mesmo por conta do próprio contexto atual, onde tudo gira em torno de tecnologia. É possível mensurar essa conscientização através da quantidade de colaboradores que realizaram cursos em nossa comunidade virtual de aprendizagem bem como pelo número de incidentes reportados à central de TI.

4. **A política de segurança da informação define os papéis e responsabilidades pela segurança da informação?**

   Sim.

5. **Quando da formulação do planejamento estratégico da organização, a segurança da informação é considerada?**

   Sim, o planejamento estratégico institucional é realizado concomitantemente com o planejamento estratégico de TI.

6. **A diretoria da instituição considera a gestão da segurança da informação como questão crítica para a organização?**

   Sim, existe até mesmo uma diretoria própria com esta finalidade (diretoria administrativa e de tecnologia da informação).

7. **As decisões relacionadas com a segurança da informação são tomadas exclusivamente pela área de TI ou em conjunto com a equipe responsável pelas decisões estratégicas da organização?**

   Por todas as áreas da instituição representadas por suas diretorias.

8. **O acesso ás informações preserva os critérios de confidencialidade, integridade e disponibilidade?**

   Trabalhamos todo dia buscando a eficiência e eficácia em nossas atividades nas agências. Em virtude da grande demanda de serviços e muitas vezes baixa quantidade de funcionários concursados, existe uma prática eu diria comum de funcionários passar suas senhas de identificação na rede para terceiros para a realização de atividades e consecução das metas.

9. **Como é feita a identificação dos riscos? Eles são previstos através de um plano de contingência?**

   Tenho conhecimento do plano de contingência e acredito que a identificação dos riscos é feita pelos funcionários das agências quando da comunicação com os ambientes responsáveis.

10. **Existem controles e requisitos de segurança da informação quando dos contratos com terceiros?**

Existe uma grande quantidade de contratos com terceiros na instituição, a IFB está trabalhando para enxugar o quadro de terceirizados. Os controles são realizados pelas agências e pelo ambiente responsável.

Infraestrutura de Tecnologia da Informação (TI) e Gestão de Segurança da Informação

1. **Como é vista a infraestrutura de TI na organização? Há compreensão, dentro da instituição, da influência da infraestrutura de TI no cumprimento da missão?**

   Todos sabem que a infraestrutra de TI é um dos principais pilares para qualquer instituição financeira, pois a maioria dos serviços oferecidos são suportados por sistemas.

2. **A diretoria vê a infra-estrutura de TI como elemento estratégico da instituição? Como a diretoria trata dos investimentos em infra-estrutura de TI pela organização?**

   Sim. Percebemos nas agências a enorme preocupação com a infraestrutura de TI. Sempre estamos recebendo equipamentos e avanços para uma melhor prestação de serviços aos nossos clientes. Nós, funcionários de agência não temos informações a respeito de como a diretoria trata dos investimentos.

3. **A cultura organizacional relaciona a infraestrutura de TI aos riscos da instituição?**

   Sim.

4. **Como as falhas em elementos da infra-estrutura de TI afetam a prestação de serviços e confiabilidade da organização? Qual a relação entre eficiência da instituição e sua infra-estrutura de TI?**

   Somos uma instituição financeira e por isso devemos prestar um serviço de ótima qualidade e com agilidade, o mercado requer isso. Diante deste contexto, a nossa infraestrutra de TI é fundamental para a eficiência no atendimento e realização dos resultados esperados.

5. **O fornecimento de energia elétrica e climatização são vistos como elementos de infra-estrutura de TI?**

   Sim. Fica evidente a forma com que a IFB trabalha estes requisitos.

6. **Quais controles de acesso físico aos ambientes de TI e ambientes de acesso restrito?**

   O acesso é restrito apenas aos funcionários autorizados, através de identificação e supervisão do gerente geral da unidade e o gerente executivo administrativo.

7. **Os equipamentos de uso individual são vistos como ativos da infra-estrutura de TI da organização e elementos necessários à eficiente prestação de serviço pela instituição?**

   Sim.

8. **Como é realizado o processo de armazenamento e recuperação de dados utilizados pela instituição?**

   Ao final de cada expediente é realizado um backup de tudo o que foi realizado na agência, essas informações são replicadas às centrais da IFB e um funcionário monitora este processo até que o mesmo seja totalmente concluído.

9. **O monitoramento do correto funcionamento dos equipamentos da infra-estrutura de TI é feito? Os resultados do monitoramento são usados para melhoria da infra-estrutura de TI?**

   Sim. O monitoramento é feito pelos próprios funcionários das agências e pela central de TI. É possível que a central identifique qualquer falha de comunicação de algum equipamento da rede nas agências.

APÊNDICE B

QUESTIONÁRIO VERIFICADOR DE CONFORMIDADE COM A NORMA ABNT NBR ISO/IEC 17799 e ABNT NBR ISO/IEC 27002

Para a resposta de cada questão o padrão de avaliação utilizado será o seguinte:

0 – Não se aplica.
1 – Resposta – Não.
2 – Solução em Planejamento inicial.
3 – Está planejada a implantação da solução.
4 – Parcialmente implementada. Ainda não confiável.
5 – Está funcionando bem.
6 - Sim

Política de Segurança da informação

1. Existe um documento de política de segurança definindo a filosofia, as diretrizes da organização em relação ao uso e proteção da informação?
   R: 6
2. Existem outros regulamentos que complementam e detalham como os objetivos descritos na política de segurança da informação podem e devem ser alcançados?
   R: 6
3. Existe um processo que garanta a atualidade dos regulamentos de segurança?
   R: 6
4. É garantido que todos os usuários de informação conhecem os regulamentos de segurança de informação existentes?
   R: 1
5. A política de segurança da informação está coerente com o código de ética e demais políticas corporativas?
   R: 6
6. A política de segurança da informação está de acordo com a legislação do país?
   R: 6

Fatores críticos de sucesso

1. Quando do planejamento das ações de negócio da organização existe o envolvimento da área de segurança da informação?
   R: 6
2. O executivo da área de segurança da informação participa de comitê que analisa os requisitos necessários para a implementação dos futuros produtos e serviços da organização?
   R: 6
3. Existe definido o orçamento e demais recursos para o processo de gestão da segurança da informação?
   R: 6
4. A direção da organização valida periodicamente o direcionamento e prioridades da implementação dos controles de segurança da informação?
   R: 6

Infraestrutura de segurança da informação

1. Existe uma estrutura organizacional com a responsabilidade de coordenar o processo de segurança da informação?
   R: 6
2. Foi dado conhecimento a todos os usuários da informação da existência da área responsável pelo processo de segurança da informação?
   R: 6
3. A área de segurança da informação tem definido formalmente suas responsabilidades, escopo de atuação, estrutura de recursos e plano de ação?
   R: 4

Gestão de Ativos

1. Existe uma política de classificação da informação que define os níveis de sigilo e indica para cada um deles como deve ser tratada a informação?
   R: 4
2. O gestor da informação é o responsável pela liberação do acesso à informação pelo usuário?
   R: 6
3. Existe procedimento definido para o descarte de equipamentos garantindo que as informações será devidamente apagadas antes do ativo ser liberado?
   R: 6

Segurança em recursos humanos

1. Existe um processo de conscientização e treinamento de usuários em segurança da informação?
   R: 6
2. Todo tipo de usuário participa do treinamento em segurança da informação?
   R: 1
3. Todo usuário antes de iniciar suas atividades profissionais na organização recebe orientações em relação à segurança da informação e toma conhecimento dos regulamentos existentes?
   R: 1
4. Cada usuário formaliza o seu conhecimento dos regulamentos através de assinatura de um documento?
   R: 1

Segurança física e do ambiente

1. Cada pessoa tem autorização de acesso físico apenas aos ambientes que necessita acessar para desempenhar as funções profissionais na organização?
   R: 5
2. O acesso físico das áreas é controlado, impedindo que pessoas não autorizadas acessem ambientes em que não estão autorizadas?
   R: 5
3. O acesso físico de cada pessoa fica registrada, permitindo uma auditoria?
   R: 5
4. Existe o monitoramento e gravação de imagens dos principais pontos de acesso ao ambiente físico, pontos de vigilância e do perímetro do terreno?
   R: 5
5. As imagens são armazenadas durante um período previamente estabelecido, podendo ser recuperadas neste período?
   R: 5
6. As imagens são guardadas em um local protegido adequadamente de forma que não seja possível o roubo delas com o objetivo de desaparecimento de provas?
   R: 5
7. As pessoas são avisadas de que o ambiente é monitorado e gravado?
   R: 6

8. Existe um processo contínuo garantindo a efetividade das medidas de controles existentes?
   R: 5
9. Existe um controle de para a saída e entrada de material?
   R: 5
10. Sempre que possível é utilizado material retardante a fogo, que dificulta o início e a propagação do incêndio?
    R: 5
11. Existe sinalização de emergência indicando as saídas e saídas de emergência?
    R: 6

Gerenciamento das operações e comunicações

1. Existe documentação dos processos e procedimento relativos aos recursos de informação?
   R: 5
2. Foi analisada a questão da segregação de função e está garantido que este controle está implementado?
   R: 5
3. É proibida a execução no ambiente de produção de programas em teste ou em situação de homologação?
   R: 4
4. Antes da passagem de programas para a produção é feito um processo de teste e homologação para garantir que o que será implantado em agências possui uma qualidade e uma efetividade adequada?
   R: 5
5. Todo o processo de passagem de programa para o ambiente de produção pode ser auditado?
   R: 6
6. Os serviços prestados por terceiros são monitorados e gerenciados de maneira que possa ser feita uma avaliação desse prestador de serviço?
   R: 5

Controle de acesso

1. A identificação do usuário é única e individual para qualquer tipo de usuário?
   R: 6
2. Existe a garantia da não existência de identificações genéricas?

R: 6

3. Quando a autenticação é feita através de senha, essa senha é secreta e de conhecimento exclusivamente do usuário?
   R: 6
4. É declarado nas políticas que o usuário é responsável pelo acesso realizado com a sua identificação e autenticação?
   R: 6
5. Todo acesso realizado ou tentativa, ao ambiente computacional é gravado e guardado durante um tempo definido pela segurança da informação?
   R: 6
6. A informação é apenas liberada para o usuário após a autorização do gestor da informação?
   R: 6
7. O processo de liberação de acesso da informação para o usuário é formalizado e registrado, permitindo auditoria?
   R: 5
8. Existe um processo automático que retire os acessos do usuário quando ele é transferido para outra área da organização?
   R: 6
9. Existe um processo automático que retire a identificação do usuário quando ele encerra seu relacionamento profissional com a organização?
   R: 6
10. Quando do uso de senhas, o arquivo de senhas é criptografado?
    R: 6

Aquisição, desenvolvimento e manutenção de sistemas

1. É utilizada uma metodologia de desenvolvimento de sistemas, e essa metodologia é de conhecimento de todos os desenvolvedores (funcionários e terceiros)?
   R: 4
2. Existe na metodologia desenvolvimento de sistemas uma etapa para a especificação dos requisitos de segurança da informação antes do desenho lógico da solução?
   R: 6

3. Existem pelo menos três ambientes computacionais: de desenvolvimento, de teste e produção?
   R: 1
4. Quando da aquisição de sistemas são considerados vários aspectos da solução, inclusive o grau de certeza da continuidade do fornecedor no mercado de tecnologia?
   R: 4
5. Existem cópias de segurança suficientes para recuperação do ambiente de desenvolvimento de sistemas?
   R: 0

Gestão de incidentes de segurança

1. Existe um processo estruturado para o tratamento de incidentes de segurança da informação?
   R: 6
2. A prioridade de ações a ser feita em conseqüência de ocorrência de incidentes de segurança da informação considera o negócio da organização?
   R: 5
3. O processo de tratamento de incidentes de segurança da informação gera informações que possibilitam um melhor planejamento para a proteção do ambiente de tecnologia?
   R: 5
4. Existe um canal de comunicação entre o usuário possa registrar a ocorrência de um incidente, além de acompanhar a pesquisa destes incidentes e conclusões definidas pela organização?
   R: 5

Gestão da continuidade do negócio

1. Existe um plano de continuidade de negócio para ser seguido quando da ocorrência de um desastre que indisponibilize recursos de informação?
   R: 5
2. É realizada periodicamente uma avaliação de risco com foco nas ameaças que podem indisponibilizar recursos de informação e podem parar ou degradar em muito o desempenho da realização do negócio?
   R: 4

3. Existe um manual atualizado que define os procedimentos a serem feitos quando da ocorrência de uma situação de contingência?
   R: 5
4. Todos os envolvidos foram treinados considerando as orientações formalizadas no manual do plano de continuidade de negócio?
   R: 5
5. São realizados testes periódicos para a utilização do plano de continuidade de negócio?
   R: 5
6. Existem cópias de segurança considerando aspectos de operação, de auditoria, guardadas de forma segura, suficientes para uma recuperação da informação?
   R: 5

Conformidade

1. Existe de forma explícita o conjunto de legislação, regulamentos de segmentos de negócio e requisitos éticos que a organização é obrigada a seguir?
   R: 6
2. Esse conjunto de requisitos é de conhecimento dos usuários que tratam a informação da organização para desenvolver sistemas, proteger a mesma e definir procedimentos de recuperação dos recursos da informação?
   R: 4
3. A área jurídica interage fortemente com a área de segurança da informação com a área de tecnologia da informação, com o objetivo de garantir a conformidade da organização com a legislação e demais regulamentos?
   R: 1
4. Existe processo que defina e formalize os requisitos necessários para que possam ser realizados procedimentos de auditoria e de performance computacional?
   R: 5