SEGURANÇA DAINFORMAÇÃO: A GESTÃO DE PESSOAS UTILIZANDO TECNOLOGIA EM INSTITUIÇÕES FINANCEIRAS

Enéias Heleno da Silva[1]

[1]*Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco - DEaD/IFPE, e-mail:eneiasheleno@gmail.com*

Resumo
Este trabalho apresenta um estudo de caso sobre a gestão da segurança da informação em instituições financeiras, 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.
Palavras Chave: Gestão de Pessoas; Processos tecnológico; Tecnologia da informação
Introdução.

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, onde a informação se caracteriza como um dos bens mais importantes da organização. Há algumas décadas, a informação mais crítica da empresa poderia ser guardada dentro de uma gaveta, mas, nos moldes das empresas modernas, a proteção da informação deve ser uma das preocupações dos executivos e proprietários. Neste sentido, 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.

O estudo justifica-se, pela relevância e valor agregado da informação para uma instituição financeira, pois, se faz necessário tratá-los e protegê-los devidamente para garantir a segurança deste ativo, fator essencial para o sucesso de uma instituição desta natureza. Desta forma, os recursos computacionais, ferramentas básicas para agilizar negócios e mostrar confiabilidade a clientes e parceiros se caracterizam como de fundamental importância, para evitar, não apenas a perda de produtividade dos colaboradores, mas também, o congestionamento na rede e o risco de divulgação de informações sigilosas, entre outros prejuízos que podem causar uma má imagem da organização ou ao próprio colaborador.

Problema de pesquisa

Quais as melhores práticas de segurança da informação devem ser adotadas em uma instituição financeira pela necessidade do alto nível de proteção de sua informação?

Objetivo Geral

Analisar o processo de gestão de uma instituição financeira a partir da segurança da informação tendo como foco a política de segurança da informação e infraestrutura de Tecnologia da Informação.

Objetivos Específicos

- Analisar controles de segurança da informação utilizados na instituição financeira relativos à política de segurança da informação e infraestrutura de Tecnologia da Informação;
- Elaborar um estudo de caso em uma instituição financeira (Banco), observando à gestão e as práticas da segurança da informação adotadas.

Fundamentação Teórica

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.

Tais propósitos têm como os dois tópicos que seguem, ou seja: política de segurança da informação e infraestrutura 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. Neste sentido, 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.

A Segurança da informação e seus aspectos relacionados a Gestão de Pessoas

Neste momento serão demonstrados alguns dos princípios e conceitos acerca da segurança da informação, bem como, aspectos relacionados a este assunto que influenciam nas questões de segurança e proteção 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 (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.

Assim, pode-se entender o conceito do Direito Digital como sendo uma evolução necessária, por ter como objetivo 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.

Os princípios e a gestão da 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).

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 à tecnologia. Vulnerabilidades existem e não são poucas, até mesmo muito desconhecidas e despercebidas dentro de qualquer organização, seja ela de TI ou não.

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 eutilizável numa eventual solicitação de uma entidade autorizada ABNT (2011).
- **Integridade** – propriedade que a informação apresenta, de estar completa e fielao estado original ABNT (2011).
- **Confidencialidade** – propriedade que a informação apresenta, de estardisponível apenas para àqueles que estão autorizados a obtê-la ABNT (2011).

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. Conforme 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 exploradas por ameaças e possam trazer consequências 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 especializada em segurança para tratar de outros aspectos tais como, humanos, organizacionais e estratégicos.

Fontes ainda aponta que 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. 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:

i) definição da segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação.

ii) declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhadas ao negócio.

iii) Estrutura para estabelecer os objetivos de controle e os controles, incluindo uma estrutura de gerenciamento de risco.

iv) 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.

Análise, avaliação e tratamento de risco

O conceito de risco é definido como sendo a probabilidade que as vulnerabilidades sejam exploradas pelas ameaças existentes, danificando ou ocasionando perdas aos ativos e acarretando prejuízos aos negócios.

Conforme a CERT. BR, Espera-se que as análises/avaliações de riscos verifique e descubra 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 themanagement of TI security*).

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 seu tratamento deve ser tomada e entre 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.

Os riscos aceitos, que necessitam de tratamento e aplicações de controles apropriados, devem assegurar 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;

Assim, a 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 estar alinhada ao negócio da organização.

Metodologia

A metodologia adota neste trabalho teve uma abordagem qualitativa, exploratória de forma descritiva. Qualitativa por levar o pesquisador a uma análise mais específica dos fenômenos estudados, ou seja, ações das pessoas, grupos ou organizações em seu ambiente social (OLIVEIRA, 2008). Oliveira ainda aponta que uma pesquisa se caracteriza como exploratória de forma descritiva, por fornecer a descrição dos fatos a partir das análises. Vale salientar que elaborar uma metodologia de implementação para um projeto de segurança da informação é uma tarefa complexa devido ao nível de detalhamento que inclui todos os tópicos, itens e aspectos, tanto os técnicos quanto os de caráter gerencial, portanto estar completamente fora do escopo deste artigo detalhes técnicos para atender às necessidades específicas de cada organização. O estudo foi desenvolvido a partir deum estudo de caso de 5 (cinco) instituições, onde nas análises buscou-se diferentes conceituações e informações a respeito do tema em questão. Os procedimentos metodológicos adotados nesta pesquisa foram desenvolvidos a partir de 4 (quatro momentos. No primeiro, foram abordados alguns aspectos importantes sobre o valor dos ativos de informação de uma instituição financeira. No segundo foi abordada a **s**egurança da informação e seus aspectos relacionados a gestão de pessoas. No terceiro momento os princípios e a gestão da segurança da informação. No quarto foi realizada uma análise, avaliação e tratamento dos riscos, para se buscar um melhor entendimento da definição da pesquisa. O desenvolvimento do estudo tomando-se como escopo tais procedimentos, contribuiu de forma significativa, para uma melhor percepção da implantação e acompanhamento dos Sistemas de Gestão da Segurança da Informação em organizações.

Considerações Finais e Conclusão

No estudo, foi analisado o cenário de gestão da segurança da informação em várias instituições.

Os dados foram levantados por meio de estudo de caso. Em estudos de caso semelhante ao realizado neste trabalho relativo à gestão da segurança da informação nas instituições, pode ser observado que alguns trabalhos foram utilizados para preparar e orientar organizações, para que elas se elas se adequassem aos requisitos das políticas de segurança da informação aos quais estão sujeitas. Por meio deste trabalho, foi possível realizar uma avaliação sobre como funciona a segurança da informação na gestão de pessoas, observando seus controles e funcionamentos.

Foi possível também perceber, que a gestão da segurança da informação pode ser bem resolvida, inclusive se 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. A informação é algo a ser 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 muitas dificuldades. No estudo foi detectado também que existe a 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 à rede. Portanto, a partir de tais percepções, ficou caracterizado que se pode utilizar pesquisas com tal propósito, como forma de preparação para auditorias, com o intuito de identificar eventuais falhas e adequações necessárias.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR14724: informação e documentação: trabalhos acadêmicos: apresentação. Rio de Janeiro, 2011.

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 Segurançano Brasil**.Estatísticas dos Incidentes Reportados ao CERT**.** 2017.

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

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

OLIVEIRA, Maria Marly de. **Como fazer projetos, relatórios, monografias, dissertações e teses.** 4. Ed. Rio de Janeiro: Elsevier, 2008.

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