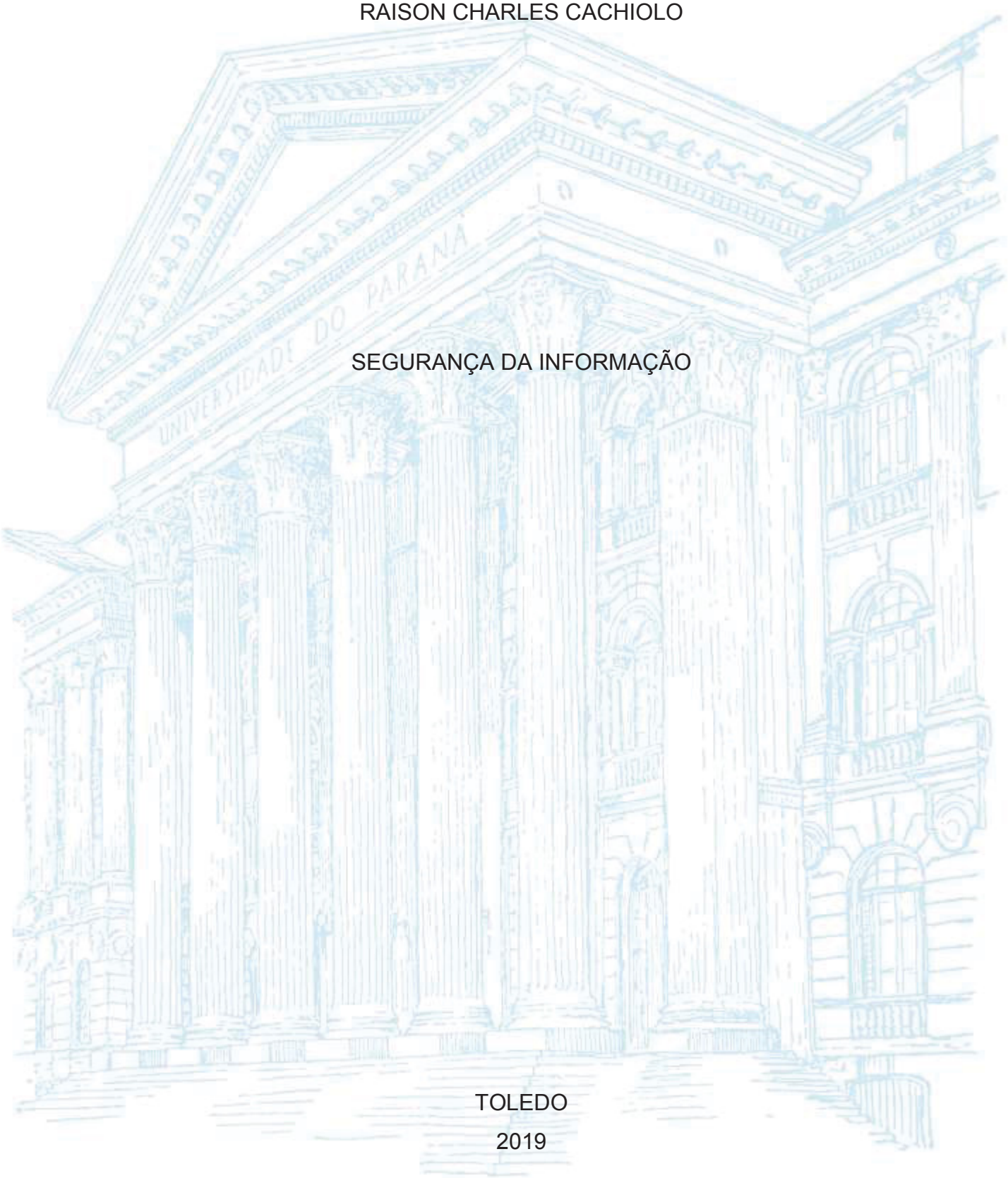
UNIVERSIDADE FEDERAL DO PARANÁ

RAISON CHARLES CACHIOLO



SEGURANÇA DA INFORMAÇÃO

TOLEDO

2019

RAISON CHARLES CACHIOLO

SEGURANÇA DA INFORMAÇÃO

Trabalho de conclusão de curso apresentado ao curso de MBA em Banking para Cooperativas de Crédito, para a Universidade Federal do Paraná, como requisito parcial à obtenção do título de Especialista em Banking.

Orientador(a): Prof(a). Dr(a). Marcos Wagner da Fonseca.

TOLEDO

2019

TERMO DE APROVAÇÃO

RAISON CHARLES CACHIOLO

SEGURANÇA DA INFORMAÇÃO

Trabalho de conclusão de curso apresentado ao curso de MBA em Banking para Cooperativas de Crédito, para a Universidade Federal do Paraná, como requisito parcial à obtenção do título de Especialista em Banking.

_____

Prof(a). Dr(a)./Msc. _____

Orientador(a) – Departamento _____, INSTITUIÇÃO

Toledo, 01 de Maio de 2019.

RESUMO

Segurança é um atributo muito complexo e difícil de implementar consistentemente em um sistema ou em uma infraestrutura de redes computacionais. A proposta do presente estudo é realizar uma análise do ambiente tecnológico utilizado pela cooperativa de crédito, Uniprime Pioneira do Paraná com sede administrativa na cidade de Toledo-PR. A fim de identificar falhas, riscos tecnológicos, vulnerabilidades virtuais e apresentar possíveis soluções para tais achados. Diante disso, a submissão da cooperativa a este estudo, poderá contribuir na construção efetiva de um ciberespaço mais seguro.

Palavra-chave: Vulnerabilidade. Segurança. Prevenção.

ABSTRACT

Security is a very complex and difficult attribute to implement consistently in a system or in an infrastructure of computational networks. The purpose of the present study is to perform an analysis of the technological environment used by the credit union, Uniprime Pioneira do Paraná, with its administrative headquarters in the city of Toledo-PR. In order to identify failures, technological risks, virtual vulnerabilities and present possible solutions. Faced with this, the submission of the cooperative to this study may contribute to the effective construction of a more secure cyberspace.

Keywords: Vulnerability. Security. Prevention.

LISTA DE ILUSTRAÇÔES

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTO

No início da década de 1980, o termo "computador" cobria todo o espectro do processamento de informações. Hoje, "Tecnologia da Informação" tornou-se a designação mais utilizada para uma gama crescente de equipamentos, aplicações, serviços e tecnologias básicas que se enquadram em três categorias principais: computadores, telecomunicações e dados de multimídia, com literalmente centenas de subcategorias.

É incontestável que a tecnologia da informação é fundamental para a operação de qualquer empresa, assim como a necessidade de se preservar os sistemas dos ataques de hackers, bem como prevenir que informações sejam divulgadas sem a devida autorização.

Os incidentes envolvendo a segurança da informação veem aumentando consideravelmente ao longo dos últimos anos e assumindo as formas mais variadas, ocasionando prejuízo financeiro e transtornos para as organizações.

Destaca-se que Segurança é um atributo muito complexo e difícil de implementar consistentemente em um sistema ou em uma infraestrutura de redes computacionais. Projetar e implementar um ambiente visando segurança significa analisar um conjunto complexo de situações adversas onde o projetista e um oponente elaboram estratégias de modo completamente independente. O resultado desta análise depende fortemente das escolhas e técnicas feitas por cada um dos oponentes.

O setor financeiro possui características próprias que o apontam como um dos que mais se utiliza da informática para sua operacionalização e estratégia competitiva. Nas grandes instituições, essa utilização é, de fato, muito acentuada. Trabalhando com produtos e serviços muito similares, destaca-se a instituição que oferecer melhor nível de

atendimento e uma eficiente prestação de serviços, tanto pessoal como informatizada.

A segurança da informação envolve uma construção multifacetada, e a sua gestão exige que devem ser consideradas questões não apenas técnicas, mas também organizacionais, estruturais, comportamentais e de aspetos sociais.

1.2 PROBLEMA DE PESQUISA

Tendo em vista que a Uniprime Pioneira do Paraná, nunca antes passou por uma consultoria ou auditoria que averiguassem a real situação da segurança do meio virtual, percebi a necessidade de poder contribuir para tal através da realização do estudo, pois atuo na área de T.I. desta cooperativa desde junho de 2010.

Por este motivo caso sejamos vítima de algum golpe ou fraude através de meios virtuais caberá a mim prestar devidas explicações.

1.3 OBJETIVO DA PESQUISA

Portanto o presente estudo tem por objetivo apresentar possíveis vulnerabilidades no ambiente tecnológico, seja físico ou lógico, e apresentar meios de soluções ou até mesmo de prevenções.

1.4 JUSTIFICATIVA

Segundo Castro (1978) justifica-se a escolha do tema, diante de sua originalidade, importância e viabilidade.

Nestes termos, o tema segurança da informação, é substancial no contexto atual, visto que, abarca a confidencialidade, a integridade, a responsabilidade, a honestidade das pessoas, a confiança e a ética. Logo, a informação representa o recurso mais precioso para a organização, assim

sendo, garantir a sua segurança é um dos maiores desafios com que as organizações tem que lidar.

As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, hackers e ataques de *denial of service* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

Desenvolver um conjunto de políticas de segurança da informação é o primeiro e mais importante passo para preparar a organização contra eventuais ataques, quer estes tenham origem interna ou externa.

2 REFERENCIAL TEÓRICO

2.1 SEGURANÇA DA INFORMAÇÃO

Sêmola (2014) define informação como:

> [...]conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos ou transacionais. [...]A informação pode estar presente ou ser manipulada por inúmeros elementos deste processo, chamados ativos, os quais são alvos de proteção da segurança da informação. (SÊMOLA, 2014, p.69)

A informação é gerada, armazenada, tratada e transmitida com o fim de ser comunicada, e a comunicação é eminentemente um processo grupal, seja ela interna ou externa às fronteiras da organização (MARCIANO; MARQUES, 2006).

Diante disso, a Norma Brasileira Regulamentadora nº 17799:2005 dispõe:

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectvidade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

Sequencialmente, a norma regulamentora supracitada define seguraça da informação como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

No mesmo sentido Beal (2005, p. 71) leciona que a segurança de informação é “o processo de proteger a informação das ameaças para garantir a sua integridade, disponibilidade e confidencialidade”.

Consoante a isso Pinheiro (2010) salienta:

> 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.(PINHEIRO, 2010, p. 82)

Peixoto (2006) indicou três princípios fundamentais para a segurança da informação: (1) Disponibilidade: propriedade que a informação apresenta, de estar disponível e utilizável em eventual requisição de uma entidade autorizada; (2) Integridade: propriedade que a informação apresenta, de estar completa e fiel ao estado original; (3) Confidencialidade: propriedade que a informação apresenta, de estar disponível apenas para àqueles que estão autorizados a obtê-la.

Oliveira et. al (2012) explicam que a confidencialidade é respeitada quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação, ou seja, a informação no ambiente organizacional requer essa atenção por parte dos gestores da informação em designar as pessoas certas no que diz respeito à guarda das informações para que não haja quebra da confidencialidade.

Já a integridade refere-se a forma como as informações são tratadas pela empresa. Tais informações devem estar corretas e verídicas, não podendo ser alteradas ou excluídas.

> [...] o princípio da integridade é respeitado quando a informação acessada está completa, sem alterações e, portanto, confiável. Ou seja, quando a informação é alterada ou chegada de forma incorreta ao seu destino, isto faz com que a integridade se quebre (OLIVEIRA; MOURO; ARAÚJO, 2012, p. 3).

No que diz respeito à disponibilidade, ainda sob a perspectiva dos autores supracitados, este fator tem como principal finalidade a garantia de que as informações sejam passadas levando a empresa a atingir o nível de segurança adequado ao seu negócio, de forma correta para os usuários, com a participação dos associados na organização.

A informação, os processos de apoio, sistemas e redes são importantes ativos para os negócios. Logo, savalguardar todas essas informações contra acessos não autorizados, alterações, furtos informacionais e danos físicos é premissa da segurança da informação.

> Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as transformações tecnológicas e o uso de computadores de grande porte, a estrutura de segurança já ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda concentrados. (TCU, 2012, p.7)

"Com o constante avanço tecnológico e a facilidade de acesso as informações, o fator humano tornou-se o principal desafio para se ter uma boa e segura conduta de segurança da informação". É o que conclui Araujo (2005, p. 5).

Santos (2007) ratifica ao explicar que as vulnerabilidades existem e não são poucas, contudo as condutas inadequadas e mais comuns envolvem, na maioria das vezes, falta de informação. A ausência de orientações simples aos colaborados, tais como evitar deixar o computador ligado sem bloquear o acesso, o que evitaria que um colaborador mal intencionado realizasse operações não autorizadas, poderiam ser facilmente evitadas se houvesse orientação nesse sentido.

Pemble (2004) citado por Klettenberg (2016, p. 31) buscou parametrizar e compreender a segurança da informação, considerando a atuação dos seus profissionais, e vislumbrou três esferas conceituais.

> A primeira é a esfera operacional, pela qual a segurança da informação está relacionada aos incidentes e as suas consequências no âmbito operacional da organização. A relação entre os incidentes e os seus impactos sob o valor da marca e valor acionário, representam a segunda esfera, denominada de esfera da reputação, enquanto que a terceira é a esfera financeira e envolve os custos advindos de eventuais incidentes. (KLETTENBERG, 2016, p. 31)

Para Mitnick e Simon (2003) a segurança não é problematizada pela tecnologia, mas sim pelas pessoas, consideradas o elo mais fraco da segurança.

Contudo é relevante destacar que não adianta as instituições apenas elaborarem regras se estas não forem devidamente registradas e conhecidas pelas pessoas que trabalham com o tratamento da informação e, também, por aqueles que possuem o direito de acesso a ela. (SFREDDO; FLORES, 2012).

2.2 A SEGURANÇA DE INFORMAÇÃO NAS INSTITUIÇÕES FINANCEIRAS

O setor financeiro é um dos mais afetados pela nova realidade de negócios na era digital. O desenvolvimento de um planejamento de TI tem importância fundamental nos bancos e cooperativas de crédito, pois possui um grande potencial para alavancar as atividades de negócios. Estas instituições implementam novos serviços com o objetivo de aumentar a eficiência dos negócios através da melhoria da administração das transações comercias e das informações geradas por essas transações. Além disso a utilização e o desenvolvimento contínuo em TI proporciona a criancão de novas áreas de negócios e novos produtos.

Segundo Gomes (2001):

> A tecnologia da informação apoia todas as etapas de um processo de inteligência competitiva, desde a fase de identificação das necessidades de informação, passando pela coleta, análise e disseminação, até a avaliação dos produtos entregues. Ela organiza o fluxo de informação e auxilia nos principais objetivos do Sistema de Inteligência competitiva: alerta possíveis oportunidades e ameaças, apoiar o processo de tomada de decisão estratégica, avaliar e monitor os concorrentes, a industria e as tendencias polítcas e sociais e apoiar o planejamento e o processo estratégico. (GOMES, 2001, p. 83)

Os negócios financeiros são arriscados pela sua própria natureza. Entretanto, conhecer os riscos com a maior precisão possível é um dos pilares de um sistema de controles internos eficiente, permitindo uma pronta ação no sentido de evitá-los ou minimizá-los.

A expressão risco, engloba inúmeras incertezas, é qualquer evento que possa afetar os objetivos das organizações. conforme evidencia Damodaran (2009), pode-se analisar o risco como oportunidade, pois o risco pode propiciar retorno positivo quando bem administrado. O autor afirma que o risco oferece oportunidades ao mesmo tempo em que nos expõe a resultados talvez indesejáveis.

No que se refere à gestão de riscos, o Comitê de Supervisão Bancária da Basileia, no seu material de Princípios Fundamentais para uma Supervisão Bancária Efetiva (2006), considera que a inadequada avaliação de riscos

contribuiu decisivamente para os problemas de controles internos de algumas organizações bancárias e às perdas relacionadas.

Portanto, o resultado da avaliação dos riscos dos sistemas de controles internos de uma entidade é componente significativo no processo de determinação da natureza, época e extensão dos testes de auditoria por serem aplicados pelo autor independente de demonstrações contábeis.

Em que pese as instituições financeiras e cooperativas de crédito sempre despenderam atenção majoritária para dos riscos de mercado, contudo a globalização e a dependência das novas tecnologias, deixaram o sistema financeiro notoriamente exposto ao risco operacional (MOOSA, 2007).

Crouchy, Galai e Mark (1998) definem risco operacional como eventos externos, ou deficiências em controlos internos ou sistemas de informação resultando numa perda, quer seja antecipada ou completamente inesperada.

Como origem dos eventos de risco operacional, Santos (2011) aponta o ser humano como a principal ameaça a qualquer tipo de informação, visto que o seu processamento se inicia e se finaliza no usuário do sistema informacional.

Brink (2002) lista os erros mais comuns cometidos pelas pessoas que compromentem a seguraça da informação: equívoco, omissão, distração ou negligência de funcionários ou terceiros contratados e de comportamentos fraudulentos (adulterações de controles, descumprimento intencional das normas, vazamento de informações privilegiadas, desvio de valores, divulgação de informações erradas).

Contudo ressalta-se que todos os envolvidos no processo são responsáveis pela segurança da informação, se tratando do aspecto pessoal, a responsabilidade é dos colaboradores da instituição bem como dos úsuários.

Nesse sentido Canongia (2009) leciona:

> Pois, de nada vale a melhor capacitação técnica senão conscientizar o usuário, o profissional, o cidadão, destas tecnologias, e de que a segurança da informação é consequentemente, a segurança cibernética, é um problema de todos. Assim sendo, esta conscientização deve ser iniciada desde o ensino fundamental, criando uma cultura orientada a esta abordagem, pois é inegável que a cada dia a iniciação digital se dá em idades mais precoces.(CANONGIA, 2009, p. 46).

Sêmola (2006) destaca ainda como fator de risco as vulnerabilidades físicas como as barreiras de controle de acesso, por exemplo, bem como as vulnerabilidades técnologicas, vindas de configurações ou parametrizações inadequadas de sistemas ou firewall.

Consoante a isso Brink (2002), destaca que os riscos decorrentes do sistema, originam-se da descontinuidade das atividades apoiadas por serviços tecnológicos, salientando a sobrecarga de sistemas de processamento de dados (risco de overloads), incapacidade dos sistemas de prover informações confiáveis e suficientes, incompatibilidade e/ou indisponibilidade de informações, falta de meios seguros de acesso aos sistemas, obsolescência dos sistemas e equipamentos, falhas de hardware, ausências de backup e de legalização do software, inadequação de sistemas operacionais/aplicativos e outros.

Neto e Silveira (2017) enfatizam que a segurança da informação envolve cumulativamente a segurança física, que está voltada aos locais nos quais se encontram as informações, ou seja, refere-se a necessidade de proteger equipamentos e programas dentro de um local adequado a eles, bem como a segurança lógica que baseia-se na forma de utilização dos recursos nas diversas atividades cotidianas da instituição que se encontra de posse deles, e por fim a segurança humana, pois todos esses recursos são utilizados por pessoas, de modo que elas devem entender seu papel na manutenção das informações dentro de parâmetros de segurança e confiabilidade.

Entretanto Rocha (2008) destaca a necessidade de mudança na cultura empresarial do Brasil. A segurança da informação somente será efetivada quando se compreender que as informações constituem o patrimônio da empresa.

As inovações tecnológicas, proporcionaram além das trocas informacionais de conhecimentos, na comercialização eletrônica de bens e serviços e ainda na transmissão de dados sensíveis.

Diante dos novos cenários que a tecnologia proporciona, a preocupação da cooperativa, está pautada em atender as necessidades e preferências dos cooperados, criando canais confiáveis que melhorem a vida e o dia a dia das pessoas.

Atualmente todo cooperado pode gerenciar sua vida financeira com apenas poucos cliques. A grande maioria das instituições financeiras e cooperativas de crédito, permitem que seus clientes tenham acesso a empréstimos, financiamentos, aplicações financeiras, pagamentos de boletos e transações financeiras por meio de um aplicativo instalado em seus smartphones, ou pelo acesso via Internet Banking.

Referente a isso Gonzalez (2006) enfatiza:

> [...] aumenta o grau de liberdade com que os homens podem atuar no mundo social e material. Permitem executar largas cadeias de processamento, a partir de diversos inputse obtendo um número indefinido de produtos. Sendo sociais em sua produção, permite que desde um único ponto se possa intervir em uma vasta rede com múltiplas consequências no mundo social e material (GONZALEZ, 2006, p. 52).

No mundo conectado, segurança dever ser um pilar estratégico. A segurança da informação dever ser uma das maiores preocupações das empresas, especialmente nesse ramo, vez que a perda de dados pode compreter seus lucros, seus resultados, sua confiabilidade no mercado. (TORRES, 2014).

As instituições que atuam no ramo financeiro, tem em seu patrimônio informações privilegiadas, e caso haja alguma falha de segurança, esses dados poderão ser apropriados de forma indevida. Portanto não se pode esquecer que embora á segurança da informação tenha sofrido avanços expressivos nos últimos anos, a especialização dos invadores também aumentou. Desta forma a preocupação com a segurança da informação deve ser priorizada e requer acompanhamento contínuo.

A segurança da informação, por muitos, é vista como a proteção de dados oferecidos ou recebidos por alguém, porém, é preciso compreender que esta significa muito mais do que isso, pois engloba o desenvolvimento de medidas e práticas que façam com que esses dados sejam resguardados mesmo dentro da empresa, já que mesmo ali existem usuários não autorizados a utilizar essas informações e, caso tenham acesso a elas, poderão fazer um uso inadequado, fornecendo-as a quem não tenha direito a isso. (OLIVEIRA; MOURO; ARAÚJO, 2012).

Uma ferramenta muito eficaz são as consultorias, realizadas por empresas especializadas, que podem auxiliar na identificação e prevenção de fatores de riscos.

A consultoria de TI é responsável por fazer uma checagem e avaliação dos riscos do ambiente de trabalho dos sistemas de informação que suportam os processos de negócio. A atividade tem como intuito ajudar a organização por meio da identificação e avaliação de exposições ao risco que sejam significativas, bem como contribuir para o avanço dos mecanismos de gestão de risco e de controle dos sistemas de informação(ISACA, 2010).

Dentro da realidade apresentada pela cooperativa de crédito, uma auditoria poderia ocorrer em duas áreas distitnas conforme leciona Neto e Solonca (2007). Auditoria de segurança de informações e auditoria de aplicativos.

Os referidos autores explicam que uma auditoria da segurança da informação visa mitigar vulnerabilidades em ambientes informatizados, ela avalia a política de segurança da informação e também os controles relacionados a aspectos de segurança e de controles que influenciam o bom funcionamento dos sistemas da organização. Tais controles estão listados a seguir:

- Avaliação da política de segurança;
- Controles de acesso lógico;
- Controles de acesso físico;
- Controles ambientais;
- Plano de contingência e continuidade de serviços;
- Controles organizacionais;
- Controles de mudanças;
- Controle de operação dos sistemas;
- Backups dos bancos de dados;
- Controles sobre computadores;
- Controles sobre ambiente cliente-servidor.

Já uma auditoria de aplicativos, está direcionada para a segurança e o controle de aplicativos específicos, incluindo aspectos que fazem parte da área que o aplicativo atende. A auditoria de aplicativos compreende:

- Controles sobre o desenvolvimento de sistemas e aplicativos;

- Controles de entrada, processamento e saída de dados;
- Controles sobre o conteúdo e funcionamento do aplicativo com relação à área por ele atendida.

De acordo com o Tribunal de Contas da União a segurança da informação é obtida:

I. Estabelecendo requisitos de segurança: É fundamental que a organização identifique seus requisitos de segurança.
    - Fontes principais:
        - Análise de Risco dos Ativos de Informação.
        - Normas internas (PSI, classificação da informação).
        - Legislação vigente, estatutos, regulamentação e cláusulas contratuais (requisitos legais).
        - Conjunto particular (no contexto da organização) de princípios, objetivos e requisitos para o processamento da informação (objetivos de negócio).

II. Estabelecendo controles: Uma vez identificado os requisitos de segurança, podem ser selecionados e implementados controles que visam satisfazer esses requisitos.

    Existirão situações onde a implementação de controles não será capaz de eliminar as vulnerabilidades identificadas, contudo poderá ser suficiente para reduzir os seus respectivos impactos ou probabilidade de ocorrência a um nível de risco aceitável.

    Controles compensatórios também devem ser identificados. Exemplo: funções devem ser segregadas para evitar fraudes e erros, contudo isso pode não ser possível para organizações pequenas e, nesse caso, outra maneira de se alcançar o mesmo objetivo de controle poderá ser necessário (ex.: utilização de trilhas de auditoria para monitoramento de acessos e atividades por outra pessoa).
    - Implementação de controles por meio de:
        - Políticas.
        - Práticas.
        - Procedimentos.
        - Pessoas.
        - Estruturas organizacionais.

- Ferramentas de software.

III. Política de Segurança da Informação (PSI): tem por objetivo prover à administração uma direção e apoio para a segurança da informação, bem como estabelecer os princípios adotados pela organização para a distribuição, proteção, administração e supervisão dos recursos de informação.

O grande pilar de sustentação do ambiente informatizado, é preservar os princípios básicos de segurança: integridade, disponibilidade, confidencialidade.

Segundo Almeida et. al (2013, p. 181) para se construir um comportamento de segurança da informação em uma organização, será preciso interagir os elementos pertinentes à Ciência da Informação, e que esses elementos alimentam uma trajetória que se inicia com a necessidade de informação, passa pela busca informacional e termina com o comportamento informacional.

3 METODOLOGIA

Para o estudo foi realizado uma análise da infraestrutura da rede de computadores, bem como uma varredura em microcomputadores afim de encontrar possíveis vulnerabilidades que comprometem a segurança da informação.

Formam analisados 70 microcomputadores na Uniprime, entre o período de 01.04.2019 a 30.04.2019, afim de identificar possíveis vulnerabilidades na segurança de informação.

Os riscos identificados fazem parte de vulnerabilidades internas sendo objeto da análise os fatores de riscos presentes na atividade profissional diária, bem como na estrutura física ou lógica da tecnologia da informação.

Para análise da rede de computadores foram verificadas configurações já estabelecidas de equipamentos que a compõe como: switch's, modems, roteadores e access points. Sobre microcomputadores realizou-se uma conferência lógica no painel de controle, em softwares, em contas de usuários, browsers, configurações de IPv4, checagem de proxy, DNS e em possíveis compartilhamentos lógicos de cada estação abrangendo também caixas eletrônicos (ATMs).

O meio físico também foi inspecionado (Hardware), verificado portas USB's, Leitores de CD\DVDs e lacres em gabinetes.

4 ESTUDO DE CASO NA COOPERATIVA DE CRÉDITO - UNIPRIME

A Uniprime Pioneira do Paraná iniciou suas atividades em 15 de outubro de 1996, com 2 funcionários e 20 sócios-fundadores, sendo a primeira cooperativa do Sistema a ser aberta no Paraná, por isso recebeu o nome “Pioneira”. Oferecer crédito e serviços de forma mais simples e vantajosa, por meio de um atendimento personalizado, moldado às necessidades dos profissionais e empresários da área de saúde. Este vem sendo o propósito da Uniprime Pioneira do Paraná em suas duas décadas de trajetória.

Atualmente conta com 8 mil cooperados 80 colaboradores divididos em 9 postos de atendimentos pelas cidades do estado do Paraná sendo: Ubiratã, Goioerê, Medianeria, Marechal C. Rondon, Assis Chateaubriand, Palotina, Guaíra, Santa-Helena e Toledo. A Cidade de Toledo comporta a sede admisnitrativa\regional da instituição, a qual tem o dever em prestar auxílio, suporte para os postos quando necessário.

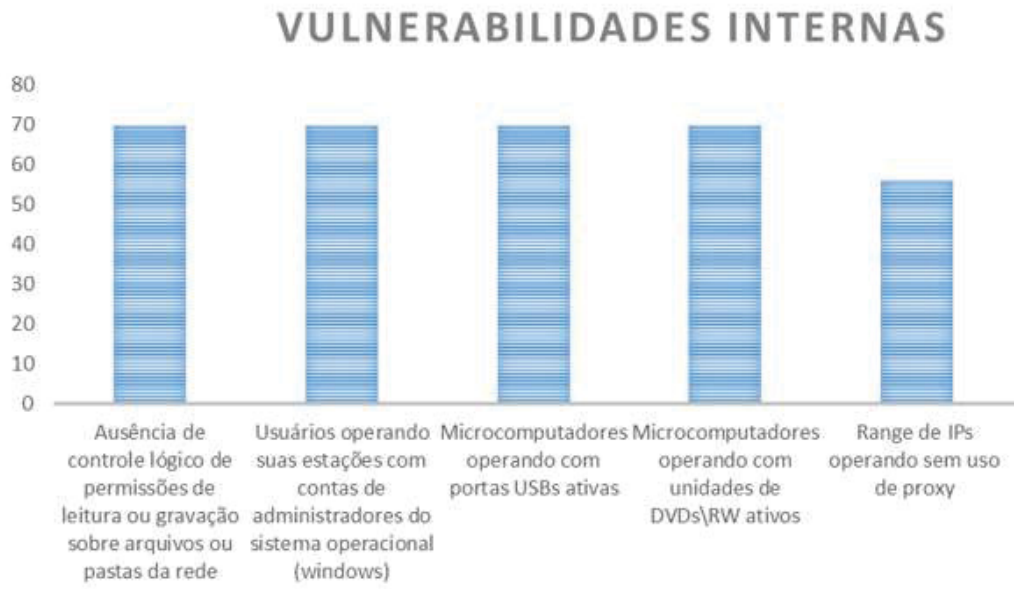
4.1 DISCUSSÃO E RESULTADOS

Ao analisar 70 microcumputadores da cooperativa, foram identificados inúmeros riscos, contudo destacam-se a: ausência de controle lógico de permissões de leitura ou gravação sobre arquivos ou pastas da rede, operação das estações com com contas de administradores do sistema operacional (windows), o que permite remover ou instalar quaisquer softwares e alterar as configurações junto ao painel de controle.

Além disso, todos os microcomputadores operam com portas USBs ativas, podendo um usuário infestar a máquina com vírus através de um pendrive; o que se repete com relação a unidades de DVDs\RW ativos, que permitem ao usuário a gravação de mídias.

Na mesma pesquisa, indentificou-se que 20 dos microcumputadores possuem acesso a navegação web sem uso de proxy (notebooks gerentes).

GRÁFICO 1 – VULNERABILIDADES INTERNAS



Fonte: O Autor(2019)

Além desses, foram apontados ainda como vulnerabilidades:

- O "Sequestro" de sessão de software.
- A disponibilização de dados sensíveis dos usuários.
- Engenharia social.
- Endereçamento DHCP ativo. *Dynamic Host Configuration Protocol*. Trata-se de um protocolo utilizado em redes de computadores que permite a estes obterem um endereço IP automaticamente, assim podendo facilmente um terceiro ingressar na rede de computadores.
- Ausência de contingência do servidor de arquivos.

Ressalto também que a cooperativa faz uso de SMS e WhatsApp para comunicação com cooperados. Essa situação inquestionavelmente aumenta a possibilidade de um golpe no qual o remetente se passaria pela instituição, enviando links mal intencionados a fim de roubo de informações.

Além disso, outro fato de risco emergente é a ausência de duplo fator de autenticação de transação financeira quando eletrônica (Token), e a grande maioria, senão, a totalidade dos cooperados já realizaram alguma transação financeira por meio de seus smartphones ou computadores.

Além das “brechas” apresentadas acima, também formam identificados como aspectos que tornam a segurança da informação vulneraveis:

- Link principal encaminhado via Wi-Fi.

- Instalações que deixam à mostra pontos e cabos de rede.
- Mesas de atendimento muito próximas umas das outras, podendo gerar vazamento de informações no ato das negociações.

5 SOLUÇÃO

Diante do cenário apresentado, algumas medidas que podem ser adotadas a fim de minimizar os riscos:

- Constante trocas de senhas.
- Curto tempo de sessão inativa, evitando roubo de sessão e utilização indevida.
- Utilização de Token para duplu faturo de autenticação.
- Coleta de registros de LOGs que permitam identificar modificações realizadas em arquivos.
- Definição de níveis de permissão de acesso.

Inclusive, é aconselhável submeter a instituição a uma auditoria\consultoria externa, esta poderá auxiliar, executando ferramentas que simulam vários tipos de ataques a softwares que permitem validar se a aplicação possui tais vulnerabilidades, elas também indicam as formas de solucionar estas vulnerabilidades apontadas, definindo políticas de segurança que envolva, por exemplo, uma rede de alçadas de aprovações, onde a hierarquia indica as operações que podem ser executadas por cada pessoa, criando políticas de controle e renovação de senhas, realizando atualização de softwares constantemente, com orientações baseadas nos golpes que são aplicadas, como identificar e prevenir.

6 CONCLUSÃO

Diante o exposto, é inquestionável que a atuação dentro do sistema financeiro, o gerencimento do crescente volume informacional, torna-se um desafio para as instituições garantirem a segurança desse patrimônio. Desta forma, a submissão da cooperativa a uma auditoria externa, pode contribuir para uma construção mais efetiva de um ciberespaço seguro.

Consoante a isso, os resultados oriundos da consultoria/auditoria auxiliarão no desenvolvimento de um Programa de Segurança de Informação, que inclui a capacitação de colaboradores, cooperados e demais clientes, bem como na adoção de medidas estratégicas de prevenção a segurança física do patrimônio de informações.

A grande maioria dos ataques bem-sucedidos explora sensibilidades conhecidas. É importante que as equipes de segurança combatam as vulnerabilidades existentes e garantam uma proteção básica eficaz.

São incontáveis os perigos em potencial da automação quando o assunto são incidentes reais de segurança. Contudo as organizações precisam estar preparadas para um futuro cada vez mais complexo e conectado.

REFERÊNCIAS

ALMEIDA, M.B., CARNEIRO, Luciana Emirena Santos. Gestão da Informação e do Conhecimento no âmbito das práticas de Segurança da Informação: O fator humano nas organizações. **Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação**, Florianópolis, v. 18, n. 37, p. 175-202, 2013.

ANTUNES, Jerônimo. **Modelo de Avaliação de Risco de Controle Utilizando a Lógica Nebulosa**. 2004, 162 f. (Tese de Doutorado em Contabilidade e Controladoria) – Faculdade de Economia, Administração e Contabilidade – Universidade de São Paulo, 2004.

ARAUJO, Eduardo. **A Vulnerabilidade Humana na Segurança da Informação**. 95 f. Trabalho de graduação (Bacharelado em Sistemas da Informação) - UNIMINAS, Uberlândia, 2005.

BEAL, Adriana, **Segurança da Informação:** Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. 1. ed. São Paulo: Atlas, 2005.

BRINK,G. J. **Operational risk:** the new challenge for bank. 1. Ed. Nova York: Palgrave, 2002.

CAMPELLO, Rafael Saldanha et. Al. **Técnicas de Segurança da Informação:** da Teoria Folna, Paulo Rogério. IN: Lyra, Mauricio Rocha. Governança da Segurança da Informação/ Edição do Autor – Brasília, 2015, p.10.

CANONGIA, Claudia; MANDARINO, Rafael. Segurança Cibernética: o desafio da nova sociedade da informação. **Parcerias estratégicas**, Brasília, v.14, n.29, jul. /dez. 2009, p.21-46.

ISACA, Information Systems Audit and Control Association. **ISACA Introduces Portuguese Edition of COBIT 4.1 (Portuguese).** Disponível em http://www.isaca.org/About-ISACA/Press-room/News-Releases/Portuguese/Pages/ISACA-Introduces-Portuguese-Edition-of-COBIT-4-1-Portuguese.aspx.

LIMA, Telma Cristiane Sasso de; MIOTO, Regina Célia Tamoso. Procedimentos metodológicos na construção do conhecimento científico: a pesquisa bibliográfica. **Rev. Katálysis**. Florianópolis v. 10 n. esp. p. 37-45, 2007.

MARCIANO, João Luiz; MARQUES, Mamede Lima. O enfoque social da segurança da informação. **Ciência da Informação**, Brasília, v. 35, n. 3, p. 89-98, set./dez. 2006. Disponível em: http://www.scielo.br/pdf/ci/v35n3/v35n3a09.

MATTAR, F. N. **Pesquisa de marketing, metodologia e planejamento.** São Paulo: atlas 2001.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar:** Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

MOOSA, I. A. Operational Risk: A Survey. New York University Salomnn Center, **Financial Markets, Institutions & Instruments**, v. 16, n.4, p.167-200, 2007.

NETO, Abílio Bueno; SOLONCA, Davi. **Auditoria de Sistemas Informatizados.** 3ª edição; Palhoça: Unisul Virtual, 2007

NETTO, Abner da Silva; SILVEIRA, Marco Antônio Pereira da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Revista de Gestão da Tecnologia e Sistemas de Informação.** Vol. 4, No. 3, 2007, p. 375-397. Disponível em: <http://www.redalyc.org/html/2032/203219581007/

OLIVEIRA, Gabriella Domingos de; MOURA, Rafaela Caroline Gaudêncio de; ARAÚJO, Francisco de Assis Norberto Galdino de. Gestão da segurança da informação: perspectivas baseadas na tecnologia da informação. In: Encontro Regional de Estudantes de Biblioteconomia, Documentação, Ciência e Gestão da Informação, 15, 2012, Juazeiro do Norte. **Anais...** Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/moci/article/viewFile/2111/1311

PIMENTA, A.M.S., Quaresma, R.F.C. A segurança dos sistemas de informação e o comportamento dos usuários. **JISTEM - Journal of Information Systems and Technology Management Revista de Gestão da Tecnologia e Sistemas de Informação**. Vol. 13, No. 3, Set/Dez., 2016, p. 535

PINHEIRO, Patrícia Peck. **Direito Digital.** 6. ed. São Paulo: Saraiva, 2010.

RAZZIOTIN, Carlos Augusto. **Controles Internos e Gestão de Riscos em instituições financeiras.** 2002, 75 f. Dissertação (Mestrado em Economia com ênfase em Controladoria) – Curso de Pós-Graduação em Economia da Faculdade de Ciências Econômicas da UFRGS, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2002.

ROECH, S. M. A. **Projetos de estágio e de pesquisa em administração.** 3 ed. São Paulo: Atlas, 2005.

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

SCHNEIDER, Juliane; Souza, Angela Rozane Leal de. A importância da Segurança da Informação e dos Controles Internos na Prevenção de Riscos à Estabilidade Financeira de uma Instituição Bancária. **Pensar Contábil**. Rio de Janeiro, v. 19, n. 69, p. 30-39, 2017.

SFREDDO, Josiane A.; FLORES, Daniel. Segurança da informação arquivista: o controle de acesso em arquivos públicos estaduais. **Revista Perspectivas em Ciência da Informação.** Minas Gerais, v. 17, n.2, p. 158-178, abr./jun. 2012

SILVA, Sanderlene Goulart da Silva. **Uso da Tecnologia da informação no setor bancário: um diagnóstico do uso da intranet no Banco do Brasil, Agência Príncipe de Joinville.** 2007. 64 p. (Trabalho de Conclusão de curso de especialização em Gestão de Negócios Financeiros) – Programa de pós-graduação em Administração – Universidade Federal do Rio Grande do Sul, 2007.

TCU. **Boas Práticas em Segurança da Informação**. 4. ed. Brasília: TCU, 2012