UNIVERSIDADE FUMEC
Faculdade de Ciências Empresariais - FACE
Mestrado Profissional em Sistemas de Informação e Gestão do Conhecimento

O IMPACTO DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS DE PRESTAÇÃO DE SERVIÇOS BANCÁRIOS: UM ESTUDO EM UMA EMPRESA PERSONALIZADORA DE CARTÕES DE PAGAMENTO BANDEIRADOS

Hudson Oliveira Leite

Belo Horizonte
2017

Hudson Oliveira Leite

O IMPACTO DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS DE PRESTAÇÃO DE SERVIÇOS BANCÁRIOS: UM ESTUDO EM UMA EMPRESA PERSONALIZADORA DE CARTÕES DE PAGAMENTO BANDEIRADOS

Dissertação apresentada ao Curso de Mestrado Profissional em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC, na área de concentração Gestão de Sistemas de Informação e do Conhecimento, na linha de pesquisa Sistemas e Tecnologia da Informação, como requisito parcial para a obtenção do título de mestre em Sistemas de Informação e Gestão do Conhecimento.

Orientador: Prof. Dr. Jersone Tasso Moreira Silva

Belo Horizonte
2017

Leite, Hudson Oliveira.

L533i O impacto da segurança da informação nas empresas de prestação de serviços bancários: um estudo em uma empresa personalizadora de cartões de pagamento bandeirados. / Hudson Oliveira Leite. – Belo Horizonte, 2017.

119 f.: il. (algumas col.) ; 30 cm.

Orientador: Jersone Tasso Moreira Silva.
Dissertação (mestrado) – Universidade FUMEC. Faculdade de Ciências Empresariais.

Inclui bibliografia.

1. Sistemas de informação gerencial – Medidas de segurança 2. Segurança de dados – Estudo de casos. 3. Bancos – Segurança da informação. I. Silva, Jersone Tasso Moreira. II. Universidade FUMEC. Faculdade de Ciências Empresariais. III. Título.

CDU: 65.011:681.3.6

Elaborada por Olívia Soares de Carvalho. CRB/6: 2070

UNIVERSIDADE
FUMEC

Dissertação intitulada "**O impacto da segurança da informação nas empresas de prestação de serviços bancários: um estudo em uma empresa personalizadora de cartões de pagamento bandeirados**" de autoria de Hudson Oliveira Leite, aprovada pela banca examinadora constituída pelos seguintes professores:

Prof. Dr. Jersone Tasso Moreira Silva – Universidade FUMEC
(Orientador)

Prof. Dr. Henrique Cordeiro Martins – Universidade FUMEC
(Examinador Interno)

Profa. Dra. Caíssa Veloso e Sousa – Centro Universitário Unihorizontes
(Examinador Externo)

Cristian Virgílio Roque Reis, Me. – Centro Universitário UNA
(Consultor *Ad Hoc*)

Prof. Dr. Fernando Silva Parreiras
Coordenador do Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC

Belo Horizonte, 24 de maio de 2017.

AGRADECIMENTOS

Agradeço primeiramente a Deus e a nosso senhor Jesus Cristo, pelos milagres que realizou e com fé continuará realizando em minha vida, transformando esse sonho, que muitos consideravam impossível, em realidade.

Ao meu amigo e mentor Alexandre Araújo de Resende, pelos conselhos de imensurável valor, pelos anos de conversas e imensurável apoio, pelos puxões de orelha e pelas orientações que foram fundamentais para formar minha personalidade como homem. Não tenho palavras que descrevam minha gratidão; o Sr. Alexandre é um exemplo de retidão, caridade, dedicação e profissionalismo.

Papai e Mamãe, a vocês um agradecimento especial, de todo coração, pelo companheirismo e amor. Por sempre caminharem ao meu lado e, através de suas simplicidades, trazerem o acalento necessário para eu repousar e me recuperar. Obrigado por me guiarem pelo caminho correto, apontando este trajeto que me proporcionou alcançar mais esta vitória.

Em especial ao meu orientador, professor doutor Jersone Tasso, pelo imensurável apoio que me foi dado em momentos muito difíceis, pelas horas de conversas e ensinamentos que me serviram e servirão de exemplo de profissionalismo, empenho e conhecimento. Obrigado professor, com muito carinho, por ter me surpreendido com tamanha dedicação, atenção e paciência.

Ao Professor Henrique Cordeiro Martins, pela atenção que me foi dada e pelas contribuições que foram de grande importância para a conclusão deste trabalho.

Aos meus grandes amigos Cristiano “Kiko”, Wellington e Gustavo “Lirin”, pessoas que sempre estiveram ao meu lado, apoiando-me em momentos difíceis e compartilhando seu tempo em conversas que traziam paz e orientação.

Finalmente, agradeço especialmente aos meus filhos Geovana e Heitor e à minha sobrinha Maria Eduarda. Anjinhos que, em cada sorriso acalentador, renovaram minhas forças para continuar caminhando; são eles minha a motivação para iniciar e concluir esta caminhada.

RESUMO

Esta dissertação analisou os impactos causados pela adoção e implementação das políticas de segurança da informação em uma empresa produtora e personalizadora de cartões de pagamento bandeirados. Devido à grande utilização e disseminação dos cartões de pagamento ocorrida em 2014, o mercado de cartões movimentou um faturamento de aproximadamente R$ 963 bilhões na economia brasileira. Para atender a essa demanda de fabricação de cartões de plástico, surgiram as personalizadoras de cartões de pagamento e, paralelamente, houve a necessidade de se criar um órgão responsável pelo desenvolvimento, gerenciamento e conscientização sobre os padrões mínimos de segurança lógica adotados mundialmente pela indústria de produção de cartões de pagamento, denominado *Payment Card Industry* (PCI). Com foco nesses padrões de segurança, este trabalho tem o objetivo de identificar os impactos que a segurança da informação pode causar em uma empresa personalizadora de cartões de pagamento bandeirados, identificando e analisando as adequações necessárias na estrutura tecnológica interna, nos aspectos relativos a produtividade e nos reflexos sobre a imagem da empresa no mercado e junto às bandeiras. Foi adotada uma metodologia de estudo de caso com viés qualitativo e, por ser tratar de uma pesquisa exploratória, foi utilizada uma técnica de levantamento bibliográfico e documental. Para refinar a pesquisa e identificar as lacunas sobre o objeto de pesquisa, foi realizada uma entrevista por meio de um roteiro semiestruturado com oito funcionários da empresa, no qual foi possível perceber algumas disparidades entre as informações prestadas pela equipe interna e os principais gestores da empresa. Os impactos da segurança da informação na estrutura tecnológica da empresa são, em sua maior parte, consideráveis e a falta de uma política de segurança da informação ou a sua inconsistência refletem diretamente no processo de homologação junto às bandeiras. Em uma empresa que lida diariamente com informações secretas, o controle de acesso à informação é um fator preponderante. Procedimentos para tratativa de informações, aquisição de servidores e contratação de profissionais qualificados é essencial para a manutenção dos níveis mínimos de segurança lógica. É explícito que em uma personalizadora de cartões de pagamento bandeirados, a segurança da informação tem um importante papel no planejamento estratégico da empresa, impactando diretamente na produtividade, na estrutura tecnológica e, principalmente, nos processo de homologação junto às bandeiras.

PALAVRAS-CHAVE: Segurança da Informação. Cartões de Pagamento. *Payment Card Industry* (PCI). Prestação de serviços bancários.

ABSTRACT

This dissertation has analyzed the impacts caused by adoption and implementation of policies of information safety in a company that produces and personalizes flagged payment cards. Due to the great use and spread of payment cards in 2014, the cards market moved an asset of around R$ 963 billion in the Brazilian economy. To cover this request for plastic cards production, the personalizers of payment cards appeared and, in parallel, there was a necessity to create a department responsible for the development, management and awareness about the minimal standards of logic safety adopted worldwide by the Payment Card Industry (PCI). Focusing on these safety standards, this work aims to identify the impacts that information safety may cause in a flagged payment cards personalizing company, identifying and analyzing the necessary adjustments on the internal technologic structure, on the aspects related to the productivity and on the reflections over the image of the company in the market and within the flags. A methodology of study of cases with qualitative bias was adopted and, being an exploratory research, a technic of documents and bibliography gathering was used. In order to refine the research and identify the gaps over the research project, an interview was conducted through a semi-structured questionnaire with eight company employees, in which it was possible to see some disparities among the information offered by the internal team and the main managers of the company. The impacts of the information safety on the technologic structure of the company are, mostly, considerable and the lack of an information safety policy or its inconsistence reflect directly on the process of homologation within the flags. In a company that deals with secret information daily, the control of access to the information is a preponderant factor. Procedures for the treatment of information, acquisition of servers, and hiring of qualified professionals are essential for the maintenance of the minimum level of logic safety. It is explicit that in a flagged payment cards personalizer, the information safety has an important role in the strategic planning of the company, impacting directly the productivity, the technologic structure, and, mainly, the homologation process within the flags.

KEYWORDS: Information Safety. Payment Cards. Payment Card Industry (PCI). Banking services provision.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

Abecs	Associação Brasileira das Empresas de Cartões de Crédito e Serviços
ACL	*Access Control Lists*
ASV	*Approved Scanner Vendor*
CISO	*Chief Information Security Officer*
COBIT	*Control Objectives for Information and Related Technologies*
DLP	*Data Loss Prevention*
DMZ	*Demilitarized Zone*
Embratel	Empresa Brasileira de Telecomunicações
EMV	*Europay, MasterCard* e *VISA*
Febraban	Federação Brasileira de Bancos
GPO	*Group Policy*
HSA	*High Security Area*
HSM	*Hardware Security Module*
IFAC	Federação Internacional de Contabilistas
IPS	*Intrusion Prevention System*
ISO	*International Organization for Standardization*
ITGI	*Information Technology Governance Institute*
ITIL	*Information Technology Infrastructure Library*
JCB	*Japan Credit Bureau*
LAN	*Local Area Networks*
LDAP	*Lightweight Directory Access Protocol*
LLC	*Limited Liability Companies*
NIDS	*Network Intrusion Detection System*
OSI	*Open Systems Interconnection*
PAN	*Primary Account Number*
PCI	*Payment Card Industry*

PG-SETI	Procedimento de Gestão – Segurança da Tecnologia da Informação
PMI	*Project Management Institute*
PTI	Profissionais de TI
Renpac	Rede Nacional de Comunicação de Dados por Comutação de Pacotes
ROI	*Return on investment*
SLA	*Service Level Agreement*
SSO	*Single Sign-On*
VLANS	*Virtual LANs*
VPN	*Virtual Private Network*

SUMÁRIO

Não importa quanto a vida possa ser ruim, sempre existe algo que você pode fazer, e triunfar.

STEPHEN HAWKING

1. INTRODUÇÃO

A segurança da informação é uma ferramenta fundamental para viabilização, manutenção e homologação da cadeia de serviços das organizações que trabalham diretamente com informações sigilosas.

Requisitos como confidencialidade e integridade são indispensáveis para as empresas que lidam direta ou indiretamente com informações como um bem intangível. No manual de procedimentos do COBIT.5 (2012), a confidencialidade corresponde às metas de qualidade da informação no que diz respeito à restrição ao acesso, e a integridade corresponde às metas de qualidade da informação em sua completude e exatidão. Se a informação estiver íntegra, então ela será exata e completa.

Marciano (2006) argumenta que o grau de valor e de relevância conferido à segurança da informação pela organização deve estar diretamente relacionado ao grau dos mesmos conceitos quando aplicados à informação ou, para ser mais exato, o valor que a informação tem para a empresa deverá ser proporcional aos cuidados que a empresa deverá empenhar em seus sistemas ou processos relacionados à segurança da informação. Anderson (2001) relata que, em muitos casos, quanto maior a utilização de um determinado sistema ou informação, mais valiosa ela se torna, sendo esse valor proporcional ao quadrado do número de usuários que a utilizam, segundo a lei de Metcalfe (1995).

Conforme Bispo (1998), a política de segurança da informação define como será o esquema de acesso à informação, como será a hierarquia de acesso à informação, como será a periodicidade da troca de senhas de acesso e como será o plano de monitoramento ou auditoria de acesso à informação. Tais características garantem que todo o esquema de segurança lógica foi implementado e não está sendo violado. Atender aos requisitos de segurança é uma parte essencial para empresas que prestam serviços para instituições que exigem segurança lógica em todo o processo produtivo.

As empresas entendem que a segurança dos dados é um imperativo da estratégia de negócios e exige uma resposta corporativa, alinhada à questão mais ampla da Segurança da Informação em toda a estrutura (ERNST & YOUNG, 2012).

Anderson (2003) afirma que, embora as grandes empresas e instituições financeiras invistam aproximadamente 2% de seus orçamentos totais em segurança da informação, o ROI (*return on investment*) pretendido é pouco mensurado e, por consequência, considerado tímido, por falta de um aceite na real definição do conceito de segurança da informação.

> No mercado global atual, capacitado pela Internet e tecnologias avançadas, as organizações precisam cumprir um crescente número de exigências legais e regulatórias. Devido a escândalos corporativos e a crises financeiras nos últimos anos, há uma maior conscientização dos membros da alta administração da existência e implicações de leis e regulamentos mais rigorosos. As partes interessadas exigem uma maior garantia de que as organizações estejam atuando conforme as leis e os regulamentos e em conformidade com boas práticas de governança corporativa em seu ambiente de atuação (COBIT.5, 2012).

Para Pemble (2004), a segurança da informação deve ser definida conforme as atribuições dos profissionais que são responsáveis por ela, circundando três esferas de atuação: a esfera operacional, que está ligada à capacidade da organização de sustentar seus processos de negócio; a esfera da reputação, voltada aos incidentes que refletem diretamente no valor da "marca" ou sobre o valor acionário, e a esfera financeira, que está voltada aos custos de um eventual incidente que impacte diretamente no caixa da empresa.

Para Geer Jr., Hoo e Jaquith (2003), o custo relativo a segurança da informação para corrigir eventuais falhas de segurança no desenvolvimento de sistemas demostra que quanto mais tardiamente as falhas são detectadas, maior é o custo para corrigi-las. Por isso, em um processo decisório, é necessário levar em consideração vários fatores pertinentes à tecnologia da informação e aos impactos causados pela segurança da informação no que tange à imagem da empresa em um mercado extremamente competitivo, como exemplo as instituições financeiras bancárias e suas parceiras.

Sanches (2006) deixa claro que o tipo de serviço realizado pelo setor bancário é fortemente alicerçado na manipulação de dados e informações sigilosas e, devido ao surgimento de novas tecnologias que apoiaram a automatização de processos, grande parte das tarefas que antes eram realizadas manualmente, na atualidade, têm, em sua maior parte, o processamento bancário informatizado e os processos automatizados. As facilidades advindas da troca de dados via sistemas eletrônicos e digitais propiciaram que parte dos serviços bancários começassem a ser realizados em outros espaços físicos, dando início à contratação de terceiros para a realização dessas tarefas.

A partir da década de 1990, no Brasil, iniciou-se a terceirização dos serviços bancários, um fenômeno amplamente difundido pelos capitalistas contemporâneos como uma

ferramenta para redução dos custos. A terceirização dos serviços bancários, apoiada no conceito da organização do trabalho, foi responsável pelo surgimento de uma técnica denominada gestão da força do trabalho, na qual a produtividade contribuía diretamente para a alta lucratividade no final dos processos dos setores bancários brasileiros (SANCHES, 2006).

Alicerçadas pelo crescimento do setor de prestação de serviços bancários, surgiram as empresas personalizadoras de cartões de pagamento. A palavra personalizadoras, é um termo utilizado para designar as prestadoras de serviços bancários que atuam no mercado de produção de cartões de pagamento com a preparação e escrita de dados do emissor ou do titular do cartão na faixa magnética ou no circuito integrado no cartão (PCI, 2017). Tais empresas são classificadas como gráficas, editoras ou empresas de impressão de cartões plásticos e lidam diretamente com uma grande quantidade de informações confidenciais e, quando homologadas pelas bandeiras como Visa, Master Card e Elo, passam a ter a permissão para produzir e personalizar os cartões de pagamento bandeirados.

Normalmente, as personalizadoras também atuam na produção de cartões não bandeirados, como cartões de clubes de futebol, cartões de associações, cartões de convênios, cartões de supermercados, cartões funcionais, entre outros, porém, sem a necessidade de certificação das bandeiras, mas, ainda, com uma atenção especial à segurança dos dados contendo informações particulares de seus clientes.

Segundo Gomes e Costa (2015), os cartões de pagamento surgiram a partir do século XX; no Brasil, o crescimento desse mercado aconteceu a partir do ano de 1994 com a estabilização da economia acompanhada pelo Plano Real. Os cartões de pagamento surgiram como uma nova ferramenta de compra a prazo que viabilizou o sistema de aprovação de crédito imediato, com comodidade, segurança, e certa facilidade de utilização. Tanto os varejistas quanto os clientes adotaram rapidamente os cartões de pagamento em suas operações comerciais, tornando-se uma das principais formas de financiamento no varejo.

Dados da Federação Brasileira de Bancos, a Febraban (2016), demonstram que, motivados pela grande divulgação desse serviço, o mercado de cartões de pagamento, em 2014, chegou a 10,2 bilhões em quantidade de transações utilizando os cartões de pagamento, movimentando um faturamento de aproximadamente R$ 963 bilhões na economia brasileira. Segundo levantamento da Abecs (Associação Brasileira das Empresas de Cartões de Crédito e Serviços), em 2014, o Brasil apresentou um crescimento de 14,8% em relação a 2013 em transações com cartões de pagamento. Isso representou cerca de 30% do consumo total das famílias brasileiras.

Alguns fatores contribuíram diretamente para a aceitação e o crescimento dos cartões de pagamento no mercado nacional. Em 1964, os militares tomaram o poder e se empenharam para que o Brasil dispusesse de uma infraestrutura moderna de telecomunicação que propiciasse desenvolvimento, segurança e integração nacional. Em 1976, a Embratel (Empresa Brasileira de Telecomunicações) instalou, em caráter experimental, as primeiras linhas específicas para transmissão digital com circuitos operando com velocidades de até 4800 bps entre o Rio de Janeiro e São Paulo. A partir dos anos 1980, surgiram as primeiras críticas ao modelo monopolista do setor de telecomunicações no Brasil e, em 1997, deu-se início ao processo de privatização das telecomunicações brasileiras (CARVALHO, 2006).

Paralelamente ao crescimento brasileiro dos meios de comunicação e transmissão de dados que influenciou diretamente nas formas de transporte e transmissão de informações, facilitando a troca de dados, especialmente entre os bancos e as personalizadoras, deu-se início à expansão do mercado de cartões de pagamento. A partir daí, tornou-se necessária a criação de regras de segurança lógica para garantir a confidencialidade das informações trafegadas entre as instituições financeiras e as personalizadoras de cartões.

Diante dessa necessidade, foi criado um fórum global aberto, lançado em 2006 e denominado PCI (*Payment Card Industry*). Esse órgão é responsável pelo desenvolvimento, gerenciamento, educação e conscientização sobre os padrões de segurança adotados mundialmente pela indústria de produção de cartões de pagamento. É uma corporação de responsabilidade limitada (LLC – *Limited Liability Companies*) baseada em Delaware, EUA. O PCI *Security Standard Concil* foi fundado pela *American Express, Discover Financial Services, JCB International, Master Card* e *Visa Inc* (PCI, 2016).

Seguindo as normas de segurança da informação ditadas pelo PCI, as bandeiras deram início à adoção de rígidas medidas de segurança lógica direcionadas ao mercado de produção de cartões de pagamento, de maneira que todos os processos que envolvem a personalização de cartões de pagamento pudessem ser auditados durante todos os processos de fabricação, *embossing* e expedição.

Conforme descrito no PCI *Card Prodution* (2017), esses requisitos destinam-se a estabelecer níveis mínimos de segurança com os quais os fornecedores devem cumprir para a codificação de banda magnética e personalização de *chip*.

Conforme descrito em sua página na internet, o *PCI Security Standards Council* (2016) fornece manuais de procedimentos de governança nos quais constam as exigências de segurança lógica impostas pelas bandeiras que têm como objetivo servir como uma base de referência para os processos de auditorias anuais, responsáveis por emitir o parecer de

conformidade para que as bandeiras forneçam os certificados de homologação para empresas que estão inseridas no mercado de produção e personalização dos cartões bandeirados.

As marcas de pagamento ou bandeiras são responsáveis pela definição e gestão de programas de conformidade associados aos requisitos constantes no manual de procedimentos do PCI *Card Prodution* (PCI, 2017).

A documentação relativa à autorização para produção e personalização de cartões de pagamento é renovada anualmente, conforme o contrato de concessão para prestação de serviços de cartões bandeirados. Porém, devido ao sigilo imposto, o contrato entre personalizadoras e bandeiras não foi disponibilizado para análise.

As empresas que se comprometem a produzir os cartões bandeirados, sejam eles de crédito ou débito, são obrigadas a adotar práticas que garantam a segurança e a rastreabilidade do fluxo de informações em todo o processo de personalização, desde a transmissão dos dados confidenciais originados dos clientes, passando pela fabricação dos cartões de plástico até a finalização do processo com o envio dos cartões já personalizados aos destinatários finais (PCI, 2017).

Conforme Freitas (2007), não há nenhum órgão que, pelo menos explicitamente, seja responsável pela regulamentação da indústria de cartões de crédito no Brasil. Por exigência das bandeiras, qualquer empresa que almeje uma autorização para produção de cartões bandeirados, antes precisa ser homologada e submetida aos processos de auditoria anuais realizados por empresas certificadas pelo PCI. Essas auditorias têm a finalidade de garantir que todo fluxo de personalização dos cartões esteja de acordo com normas de segurança estabelecidas no manual de procedimentos do PCI *Card Prodution*.

Uma vez que a segurança da informação se tornou um processo inerente a todo fluxo produtivo das empresas personalizadoras de cartões de pagamento, essas foram obrigadas a se adequar, forçando o corpo diretor e os responsáveis pelos processos decisórios das empresas a considerar em suas reuniões aspectos relacionados ao impacto da segurança da informação em seu ciclo de produção.

> Todos os sistemas e processos de negócios associados com as atividades de segurança lógica relativos a produção de cartões, tais como a preparação de dados, pré-personalização, personalização de cartões, a geração de PIN, e a entrega de cartões, devem cumprir os requisitos descritos neste documento [...]
> Este documento descreve os requisitos de segurança lógica necessários para os produtores que personalizam cartões ou manipulam os dados do cartão durante a preparação dos sistemas de cartões de pagamento (PCI, 2015, p. 1).

A sinergia entre segurança da informação e produtividade tem uma influência direta nos processos de tomada de decisão nas empresas que trabalham com personalização de cartões de pagamento e buscam adequar seus processos internos com a finalidade de melhorar o seu ciclo produtivo, garantindo a continuidade do negócio, minimizando os riscos, maximizando o retorno sobre os investimentos e otimizando as oportunidades de negócio, (ISO 27001, 2013).

No Brasil, as principais empresas que prestam serviços como personalizadoras de cartões de pagamento bandeirados são: a IntelCav, localizada em Barueri, São Paulo, a Thomas Greg & Sons, localizada em São Bernardo do Campo, São Paulo, a Valid, localizada em São Paulo, capital, a Editora Alterosa, localizada em Contagem, Minas Gerais e a Morpho, localizada em Taubaté, São Paulo.

O PCI *Card Prodution* deixa explícito em seu manual de procedimentos que o fornecedor deve designar, por escrito, um gerente sênior com conhecimentos específicos em segurança da informação suficientes para ser nomeado como responsável pela Gestão de Segurança da Informação do fornecedor. Esse profissional é denominado como CISO (*Chief Information Security Officer*) (PCI, 2015).

Essa exigência deixa clara a importância dos requisitos de segurança lógica que devem ser adotados pelas personalizadoras que as obriga a nomear um responsável pela segurança da informação com conhecimentos necessários para garantir que todo o processo produtivo, no que tange à segurança dos dados confidenciais, desde a recepção dos arquivos encaminhados pelos bancos, passando pelo processamento dos dados, personalização dos cartões e expedição, sejam realizados dentro dos padrões e das normas de segurança descritas no manual de procedimentos de segurança lógica do PCI *Card Prodution*, possibilitando a rastreabilidade em qualquer fase do processo sem comprometer a produtividade.

As personalizadoras precisam estar alinhadas e conscientes da importância de estabelecer condições para adequação às exigências mínimas de segurança da informação exigidas pelas bandeiras.

Ter conhecimento dos impactos que a segurança lógica pode causar é essencial para as personalizadoras de cartões de pagamento bandeirados, principalmente no que diz respeito às consequências negativas sobre a imagem das prestadoras de serviços bancários no mercado.

1.1. Problema de pesquisa

Este trabalho tem o propósito de responder ao seguinte problema de pesquisa: qual é o impacto da segurança da informação nas empresas de prestação de serviços bancários, considerando a abordagem em uma empresa personalizadora de cartões de pagamento bandeirados?

1.2. Objetivo geral

O objetivo geral deste trabalho é identificar os impactos da segurança da informação em uma empresa de prestação de serviços bancários que realiza a personalização de cartões de pagamento bandeirados.

1.3. Objetivos específicos

A fim de se alcançar o objetivo geral, foram estabelecidos os seguintes objetivos específicos:

- analisar os impactos da segurança da informação na estrutura tecnológica interna das empresas personalizadoras de cartões de pagamento, obedecendo às recomendações descritas no manual de procedimento do PCI *Card Prodution* para homologação e produção de cartões de pagamento bandeirados;
- analisar os impactos da segurança da informação na produtividade das personalizadoras de cartões de pagamento bandeirados;
- identificar os principais requisitos que impactam na imagem da empresa no mercado de produção de cartões de pagamento bandeirados e na homologação junto às bandeiras *Master Card* e *Visa*.

1.4. Justificativa

O número de fraudes proveniente da utilização não autorizada de dados confidenciais pode ser constatada em vários setores de prestação de serviços, principalmente naqueles em que existe a transmissão e o tratamento de informações sigilosas. O mercado de cartões de pagamento não é o único setor a ter essa peculiaridade.

A quebra de sigilo relativo a informações confidenciais pode trazer grandes transtornos às empresas que lidam diretamente com essas informações. Conforme Anderson (2001), existem casos relatados em que os dados dos clientes de seguradoras de saúde são furtados e vendidos, expondo a privacidade dos pacientes e as vulnerabilidades dos sistemas de segurança lógica dessas empresas.

O *Government Accountability Office* dos Estados Unidos (órgão do congresso americano responsável por questões relativas ao recebimento e pagamento de recursos públicos) informou que as violações de dados federais envolvendo a divulgação não autorizada de informações pessoalmente identificáveis aumentaram 19% entre 2010 e 2011, num salto de 13.000 para 15.500 registros. As vítimas dessas violações passam pelo menos alguns meses sem saber o que está acontecendo. Cerca de 123.000 contribuintes do *Thrift*

Savings Plan (plano de pensão para servidores públicos americanos), cujos dados pessoais foram comprometidos numa violação ocorrida em julho de 2011, só foram avisados sobre o episódio em maio de 2012 (ERNST & YOUNG, 2012).

O mercado de cartões de pagamento está consolidado como uma das principais formas de financiamento apreciada pelos brasileiros no mercado varejista. Impulsionados pela facilidade de utilização e obtenção de crédito imediato, os cartões tiveram uma grande aceitação dos comerciantes e consumidores.

Os procedimentos relativos à segurança dos dados que permeiam os sistemas de informação que, por sua vez, compõem todo o processo de produção dos cartões de pagamento tornam os sistemas de informação e, por consequência, a segurança da informação parte inerente no processo de fabricação dos cartões de pagamento. Surge, então, diante desse cenário, a necessidade de um estudo focado nos impactos causados pela segurança da informação nas empresas envolvidas na indústria de produção e personalização de cartões de pagamento bandeirados.

Conforme relatado pelos principais noticiários, o mercado de cartões de pagamento é um setor muito explorado pelas máfias de cartões de pagamento. Os principais crimes cibernéticos ligados ao furto de informações estão ligados principalmente à clonagem de cartões. O Correio Brasiliense relata em um de seus artigos intitulado *Polícia prende quadrilha especializada em clonagem de chips de cartões* que foi necessária uma megaoperação batizada de *Double Card* para desarticular essa organização criminosa especializada em clonagem de *chip*, na qual a polícia cumpriu quinze mandatos de prisão preventiva (BITTAR, 2015).

O jornal O Tempo publicou uma reportagem em 2009 sobre quadrilhas especializadas em clonagem de cartões de pagamento. No desfecho, três indivíduos foram detidos após a denúncia do gerente de um banco da capital mineira. Segundo a Polícia Militar, esses três homens agiam em todo Brasil aplicando fraudes sem deixar rastros (COSTA, 2009).

Anderson (2003) afirma que após os incidentes em que os números dos cartões de crédito dos clientes foram roubados de um *website* de *E-commerce* por um *hacker* ficou evidente o risco a que muitas empresas estão sujeitas, e como as consequências podem ser desastrosas, uma vez que muitas dessas empresas nunca se recuperaram.

Diante desse cenário que vem sendo noticiado com constantes violações e crimes relacionados ao furto de informações, requisitos como confidencialidade, integridade, continuidade e disponibilidade, tornaram-se requisitos preponderantes para as

empresas que trabalham com os dados confidenciais dos portadores de cartões de pagamento. Assegurar que as políticas de segurança da informação estejam presentes em todo o processo de *embossing* torna-se prioridade para a indústria de cartões de pagamento.

Conforme descrito no PCI *Card Prodution* (2015), a segurança da informação é uma ferramenta imprescindível para as empresas personalizadoras de cartões de pagamento. O PCI é um manual de procedimentos que descreve todo processo ligado a desenvolvimento, fabricação, transporte e personalização dos cartões de pagamento e como a segurança da informação impacta diretamente sobre a estrutura dos sistemas de cartões de pagamento.

Como uma forma de melhorar os dispositivos de segurança dos cartões de pagamentos bandeirados devido à ocorrência de um número significativo de fraudes com cartões magnéticos convencionais, segundo Guimarães Neto e Pessoa (1992) citado por Gomes e Costa (2015), os bancos emissores substituíram sua base de cartões de pagamento que anteriormente utilizavam somente a tarja magnética por cartões com *chip* embarcado (os SmartCards) que são cartões dotados de memória e microprocessador, capazes de tomar decisões, armazenar diversas informações e suportar aplicações com diversas funções.

O crescente número de fraudes utilizando os cartões de pagamento bandeirados forçou os bancos e os prestadores de serviços envolvidos na transmissão de dados dos cartões de pagamento a ter como foco os requisitos exigidos a respeito de segurança da informação, uma vez que os reflexos causados por furto ou vazamento de informações confidenciais dos portadores de cartões de pagamento podem trazer sérios riscos à imagem da empresa, impactando diretamente nos processos licitatórios para prestação de serviços bancários.

Por essa razão, faz-se necessário um estudo focado, dentro de em uma empresa que possuem homologação das bandeiras para produção de cartões de pagamento, demostrando os impactos que a segurança da informação tem nas empresas de prestação de serviços bancários, considerando uma abordagem em uma personalizadora de cartões de pagamento bandeirados, abordando os principais requisitos que precisam ser atendidos para o desempenho dessa atividade de forma ampla e certificada.

1.5. Estrutura da dissertação

Esta dissertação encontra-se estruturada da seguinte maneira: na introdução, capítulo 1, é apresentada a relevância do tema, o problema de pesquisa, os objetivos, a justificativa e a estrutura da dissertação. No capítulo 2, é abordada a revisão da literatura. No capítulo 3, é apresentada a metodologia. Os resultados são descritos no capítulo 4, seguidos da conclusão, no capítulo 5. Finalmente, são apresentadas as referências, que listam toda a bibliografia utilizada para a elaboração deste trabalho, e, por fim, os apêndices, com o levantamento sistemático e o roteiro da entrevista utilizado para colher os dados desta pesquisa.

2. REVISÃO DA LITERATURA

Este capítulo irá abordar os principais conceitos que forneceram subsídios para o desenvolvimento do trabalho. Está divido em dois tópicos: o primeiro relativo à segurança da informação e o segundo relativo ao setor de prestação de serviços bancários, no qual consta um tópico sobre a personalização de cartões de pagamento bandeirados.

2.1. Segurança da informação

Conforme Anderson (2003), a segurança da informação tenta garantir confidencialidade, integridade e disponibilidade dos dados e componentes sistêmicos de um ou muitos computadores. O propósito final da segurança da informação é proporcionar uma sensação de bem informado ou de uma garantia de que os riscos e controles relativos à informação estão em equilíbrio.

Para Dantas (2011), ao se falar de segurança da informação, deve-se levar em conta considerações sobre a qualidade da informação, pois toda ação que comprometer qualquer aspecto da qualidade está atentando contra a sua segurança.

O manual de procedimentos do COBIT.5 (2012) diz que a segurança da informação exige a criação e a adoção de diversas políticas e procedimentos que, por sua vez, exigem a implementação de diversas práticas de segurança. No entanto, se a cultura e a ética da organização e das pessoas não forem apropriadas, os processos e os procedimentos de segurança das informações não serão efetivos.

O COBIT é um modelo que auxilia as organizações a atingirem seus objetivos de governança e gestão de tecnologia, agregando valor por meio da manutenção do equilíbrio entre os benefícios e a otimização dos níveis de riscos no que tange a tecnologia da informação, permitindo que a TI seja gerida de forma holística para toda organização, abrangendo o negócio de ponta a ponta, levando em consideração os interesses internos e externos relacionas a TI COBIT.5 (2012).

Para proteger a informação, é necessário estabelecer de forma consistente os requisitos de segurança como confidencialidade, integridade, continuidade e disponibilidade.

Esses requisitos, corretamente implementados e auditados, propiciam um nível de segurança dos dados eficiente e proativo (DANTAS, 2011).

O ITIL (*Information Technology Infrastructure Library*) é uma biblioteca que oferece ações de boas práticas para atender a grande parte dos processos no que diz respeito a tecnologia da informação, criando um guia que oferece suporte para o gerenciamento, controle e governança dos serviços ligados a TI (DE SOUZA *et al).*

A palavra confidencialidade, em segurança da informação, é um requisito de extrema importância, principalmente se for levada em consideração a peculiaridade das empresas que trabalham com prestação de serviços bancários e que, em sua grande parte, lidam ou processam informações confidenciais em seu cotidiano profissional. O PMI (2013) determina que se as informações a serem comunicadas são sensíveis ou confidenciais, devem ser tomadas medidas adicionais de segurança ou não. Para isso, é necessário determinar se as informações a serem comunicadas são sensíveis ou confidenciais e se devem ser tomadas medidas adicionais de segurança ou não. Para o COBIT.5 (2012), a confidencialidade corresponde às metas de qualidade da informação no que diz respeito à restrição ao acesso. Para o PCI (2015), dados confidenciais são todos os dados de acesso restrito.

Da mesma maneira que o requisito relativo a confidencialidade é de grande importância, os requisitos relativos a integridade também são imprescindíveis no que tange à segurança dos dados confidenciais. Uma informação íntegra é uma informação original. Dantas (2011) descreve a integridade como uma garantia de completeza da informação e dos métodos de processamento de dados. Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização.

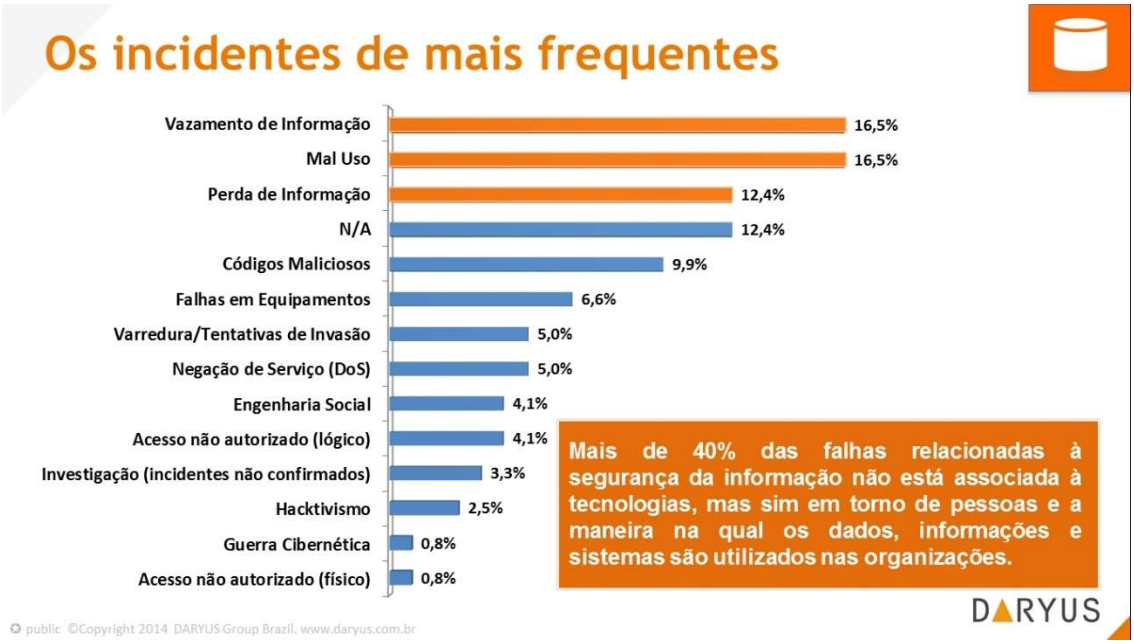

Figura 1 – Incidentes mais frequentes
Fonte: PTI, 2016.

Uma pesquisa nacional sobre segurança da informação divulgada no *site* PTI (profissionais de TI), conforme a Figura 1, afirma que mais de 40% das falhas em segurança da informação associadas a tecnologia estão relacionadas a vazamento, perda e mau uso da informação. A pesquisa foi realizada ente maio e julho de 2014 em parceria com Exin e IT Mídia e deixa evidente que a manipulação incorreta da informação e a falta de uma política de segurança clara e bem definida pode acarretar sérios prejuízos à empresa e à sua imagem no mercado.

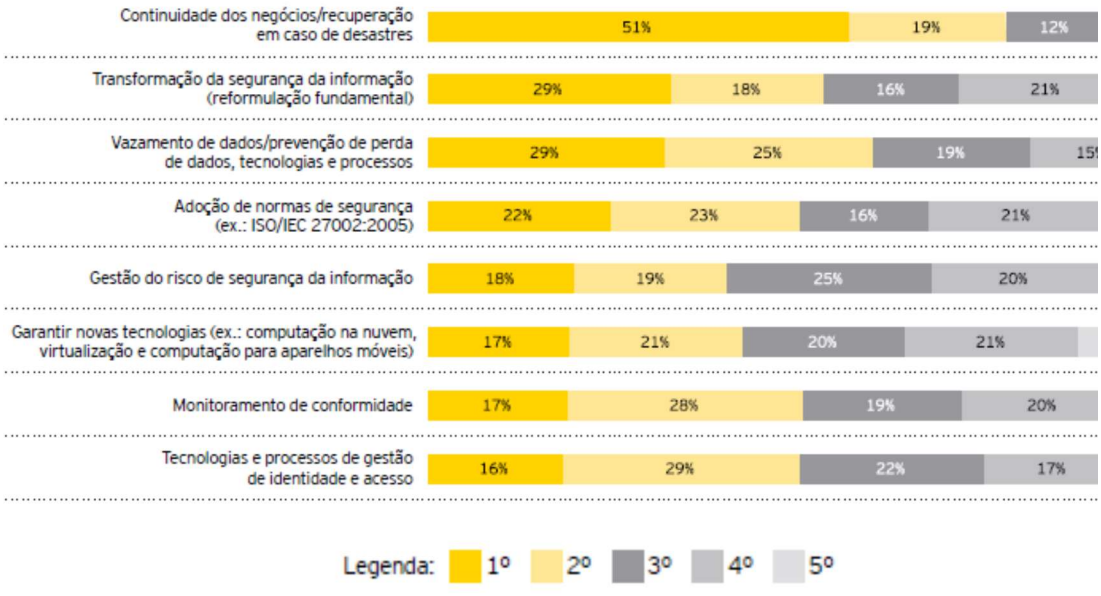

Figura 2 – Prioridades essenciais em SI
Fonte: ERNST & YOUNG, 2012, p. 17.

Em 2012, a Ernst & Young começou uma pesquisa global a respeito dos projetos e investimentos em tecnologia a serem considerados para os próximos doze meses. Conforme a Figura 2, os principais investimentos apontados em TI que foram definidos como prioridades essenciais pelas empresas são os investimentos em continuidade do negócio, em segurança da informação e no vazamento de informações.

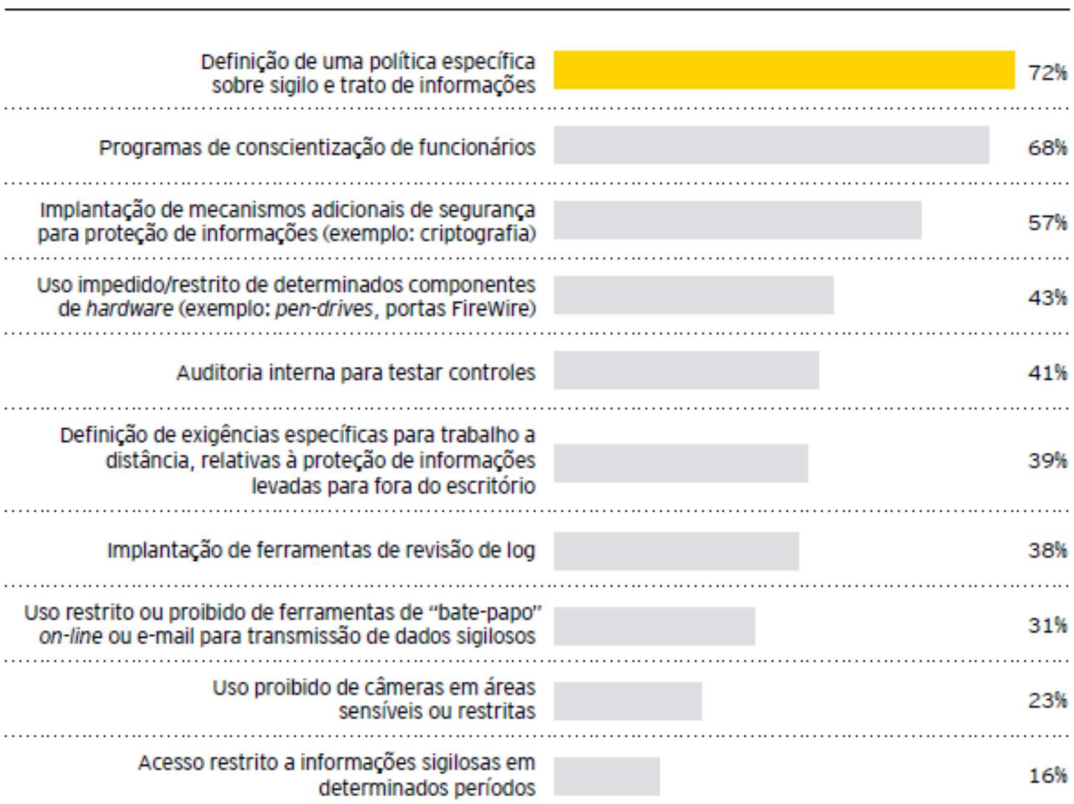

Figura 3 – Principais inciativas para controlar o vazamento de dados sigilosos
Fonte: ERNST & YOUNG, 2012, p. 31.

A Ernst & Young, conforme demostrado na Figura 3, em uma pesquisa realizada em 2012, defende que a definição de políticas específicas para o tratamento de dados sigilosos são as principais iniciativas para combater o vazamento de informações, reduzindo um dos gaps de segurança lógica. Como iniciativa para o tratamento dos dados confidenciais, as empresas adotaram como principais medidas a definição de políticas específicas sobre o sigilo das informações, o treinamento de pessoal e a implantação de mecanismos de criptografia para proteção das informações. Além disso, muitas optaram pela adoção de tecnologias voltadas à

prevenção de perda de dados, como o *Data Loss Prevention* (DLP), embora em um percentual considerado baixo pela Ernst & Young.

Investimentos em treinamento para conscientização dos profissionais ligados aos processos que lidam diretamente com dados confidenciais são essenciais dentro das empresas personalizadoras de cartões de pagamento. Conceitos sobre as técnicas de engenharia social precisam ser abordados de forma direcionada ao produto que a empresa se propõe a entregar. Conforme Long (2013) e Watson, Mason e Ackroyd (2014), os conceitos de engenharia social, quando inseridos no contexto da segurança da informação, podem ser definidos como a arte de extrair informações sensíveis manipulando usuários para realizar ações que resultam no comprometimento de informações sigilosas, uma vez que o fator humano é, muitas vezes, deixado de lado pelas empresas, propiciando a exploração da fragilidade humana.

Para a tratativa e mitigação dos riscos negativos, a utilização de uma ferramenta de gestão de riscos é fundamental. O PMI (2013) descreve que o gerenciamento dos riscos do projeto inclui processos de planejamento, identificação, análise, planejamento de respostas e controle de riscos de um projeto. Os objetivos do gerenciamento dos riscos do projeto são aumentar a probabilidade e o impacto dos eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos no projeto.

O PMI (*Project Management Institute*) é um instituto de gerenciamento de projetos e uma das maiores associações de gestão de projetos no mundo, fica localizada em 14 Campus Boulevard, Newtown Square, Pennsylvania 19073-3299 USA. O PMI é o criador e mantenedor do PMBOOK, um guia que fornece diretrizes para o gerenciamento de projetos individuais e define os conceitos relacionados com o gerenciamento de projetos, descrevendo todo ciclo de vida de projetos e seus respectivos processos (PMI, 2013).

No manual de procedimentos do COBIT.5 (2012), um dos objetivos da governança implica em reconhecimento do risco, avaliação do impacto e da probabilidade daquele risco e desenvolvimento de estratégias para evitar o risco, reduzir o efeito negativo do risco e/ou transferir o risco, para administrá-lo no contexto da organização de inclinação ao risco.

Os riscos existem e sempre permeiam todas as áreas que envolvam tecnologia da informação, principalmente naquelas em que houver recepção, tratamento ou armazenamento de informações confidenciais.

A compreensão do ambiente e das atividades de negócio é outro ponto fundamental no estudo do risco. Dantas (2011) deixa claro que compreender o ambiente de negócios é fundamental para realizar uma análise do cenário da organização. O papel do setor de TI nas organizações, de forma sucinta, é suportar a infraestrutura tecnológica para que as organizações

possam atingir as metas estabelecidas. Dessa forma, torna-se necessário o alinhamento estratégico da tecnologia da informação ao negócio, para que a mesma atue rumo ao atingimento do que foi estabelecido (CORRÊA, 2014).

Dantas (2011) ainda descreve o risco como um cenário de incertezas, ameaças e oportunidades que têm o potencial de produzir perdas ou aumentar os ganhos. Os resultados negativos são oriundos da ausência ou fragilidade da gestão da informação. Seus resultados podem produzir danos e perdas de grandes proporções. Conhecer todos os níveis dos processos produtivos que a empresa realiza é uma premissa básica para o desenvolvimento de ferramentas tecnológicas e processos inovadores que, dentro da corporação, mitigam ao máximo a eminência de ocorrer riscos negativos.

De acordo com COBIT.5 (2012), gerenciar corretamente a segurança da informação contribui para que os objetivos de Tecnologia da Informação estejam em conformidade com o negócio. Conceitos como a disponibilidade, que corresponde às metas de qualidade da informação sob a orientação da acessibilidade e segurança; a confidencialidade, que corresponde às metas de qualidade da informação no que diz respeito à restrição ao acesso; a continuidade, que corresponde à prevenção, à mitigação e à recuperação de incidentes após uma interrupção; e a integridade, que corresponde à exatidão da informação e sua completude, garantindo que a informação não sofreu qualquer interferência ou modificação em qualquer parte do processo. Estes são requisitos indispensáveis na elaboração de uma política de segurança da informação destinada às personalizadoras de cartões de pagamento bandeirados.

Tratar a política de segurança da informação com seriedade, conscientizando todos os membros da empresa sobre sua importância, elucidando quais são suas principais regras a serem seguidas e as consequências do seu não cumprimento, cria um ambiente mais seguro e favorável para o desempenho das funções dentro de uma empresa que trabalha com dados confidenciais.

2.2. Setor de prestação de serviços bancários

Conforme Sanches (2006), a partir dos anos noventa, ocorreu a expansão dos processos de terceirização de diversos setores bancários, principalmente dos serviços classificados como atividades de retaguarda e compensação. Esse cenário de terceirização foi impulsionado pela grande diversidade de serviços oferecidos pelas instituições financeiras, pela

grande massa de funcionários alocados para realização desses trabalhos repetitivos e pela necessidade de automatização desses processos.

O termo terceirização foi diretamente relacionado a otimização de processos e a especialização dos serviços, permitindo a criação de vantagens competitivas entre as empresas, a fim de reduzir os custos de produção e aumentar o lucro por meio do redirecionamento de atividades dispensáveis na realização do produto principal da empresa, reduzindo os custos com mão de obra e infraestrutura (SILVA, 2011).

Para Berry e Parasuraman (1992), a sinergia dos atributos tangíveis com os que são intangíveis constitui um serviço que garante ao cliente os benefícios de um produto diferenciado de alto valor agregado.

Uma vez que as empresas contratadas se propõem a ser especializadas nas atividades realizadas, o ganho em qualidade e rapidez fica evidente. A empresa contratante, por sua vez, tem a possibilidade de voltar seu foco para os processos de melhoria contínua de seus produtos finais, visando diferenciais de atendimento para atrair mais clientes.

A terceirização dos serviços bancários foi facilitada, em sua maior parte, pela expansão tecnológica da comunicação e pelos avanços dos sistemas de informação por meio da interligação de sistemas eletrônicos. Esse crescimento tecnológico viabilizou a conexão entre empresas localizadas em diferentes logradouros, propiciando mais controle dos sistemas centrais dos bancos e suas empresas terceirizadas, garantindo agilidade na troca de dados e nas operacionalizações relativas às atividades bancárias (SANCHES, 2006).

O processo de transmissão de dados, conforme relata Carvalho (2006), iniciou-se em 1965 com a Embratel com a missão de implantar a rede nacional brasileira. Na década de 1970, as instituições, como bancos e companhias de aviação que precisassem comunicar dados, eram obrigadas a recorrer a soluções próprias, usando rede telefônica ou de telex.

Em 1982, a Embratel lançou o Ciranda, um projeto piloto de uma rede de serviços de informações, no qual foram colocados microcomputadores compartilhados para acesso em seus escritórios. Em novembro de 1984, a Embratel lançou a Rede Nacional de Comunicação de Dados por Comutação de Pacotes (Renpac), uma rede pública de transmissão de dados que possuía treze centros de comutação distribuídos pelo território nacional. O próximo passo foi a chegada da internet, no início dos anos 1990, como uma rede de alcance internacional, a disseminação da World Wide Web foi exponencial, expandindo-se por todo o planeta e propiciando a utilização de serviços de transmissão de dados como nunca visto antes (CARVALHO, 2006).

Em 1996, o Brasil possuía o maior e mais complexo sistema financeiro na América Latina, com 234 bancos, 16.484 agências, cerca de 9.229 postos de atendimento adicionais e um total de 497.109 empregados. Com uma atividade caracterizada pela alta lucratividade e favorecidos pelos altos índices inflacionários que ocorreram no final da década de 1980, o sistema financeiro brasileiro chegou a representar 14% do PIB brasileiro. Em consequência da alta lucratividade, verificaram-se grandes investimentos em equipamentos e programas de informática e telecomunicações (US$ 3,8 bilhões em 1993; mais de US$ 4,1 bilhões em 1994). Com extensa difusão do uso da informatização em 1996, 86% das agências bancárias já se encontram conectadas *on-line* e 72% em *real time* (LARANGEIRA, 1997).

Atualmente, os investimentos em tecnologias bancárias não cessaram. Dados da Febraban (2016) demostram que os gastos em tecnologias bancárias ainda apresentam um crescimento considerável, conforme demostrado no Gráfico 1.

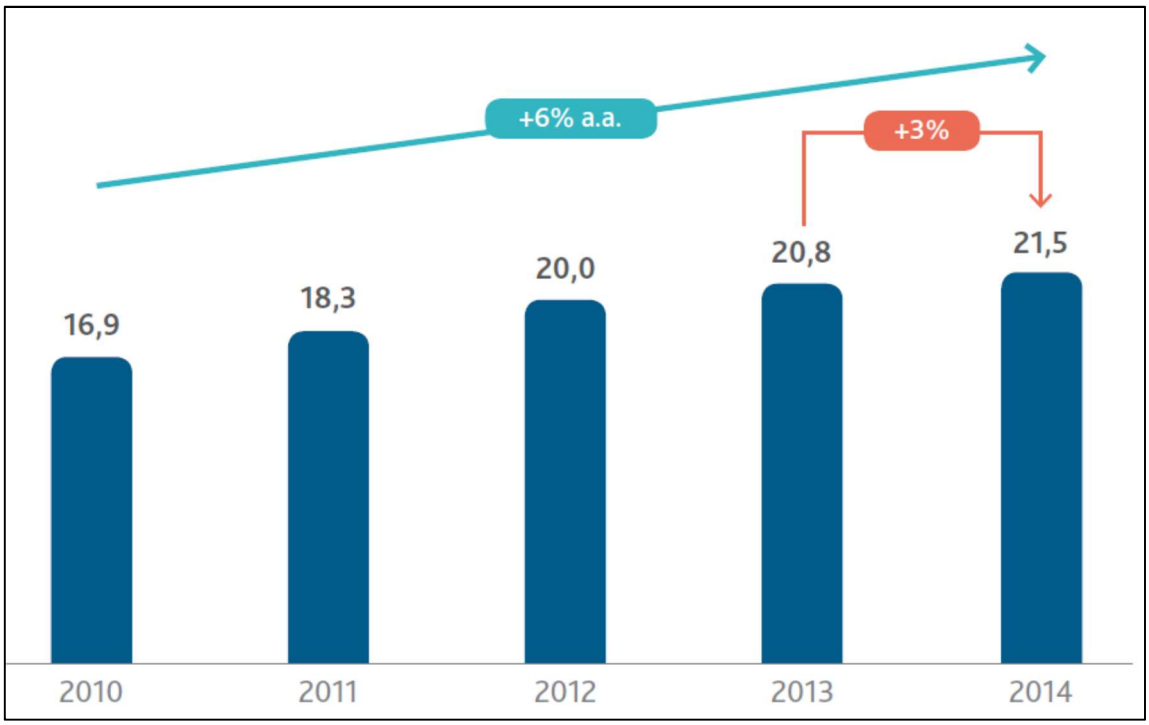

Gráfico 1 – Gastos em tecnologia bancária (em bilhões)
Fonte FEBRABAN, 2014.

O setor bancário brasileiro evoluiu significativamente ao longo das décadas, realizando investimentos em tecnologia em um ritmo considerável, somando R$ 21,5 bilhões em 2014. O total de investimentos em tecnologia da informação realizado pela indústria bancária em 2014 foi equivalente a USD 11.9 bilhões, aproximando-se de países desenvolvidos como França e Alemanha (FEBRABAN, 2016).

Juntamente a esse crescimento, o sistema de cartões de pagamento acompanhou essa tendência, como pode ser visto no Gráfico 2, passando de 628 milhões de cartões em 2010 para mais de 910 milhões em 2014, um crescimento próximo de 45% em quatro anos.

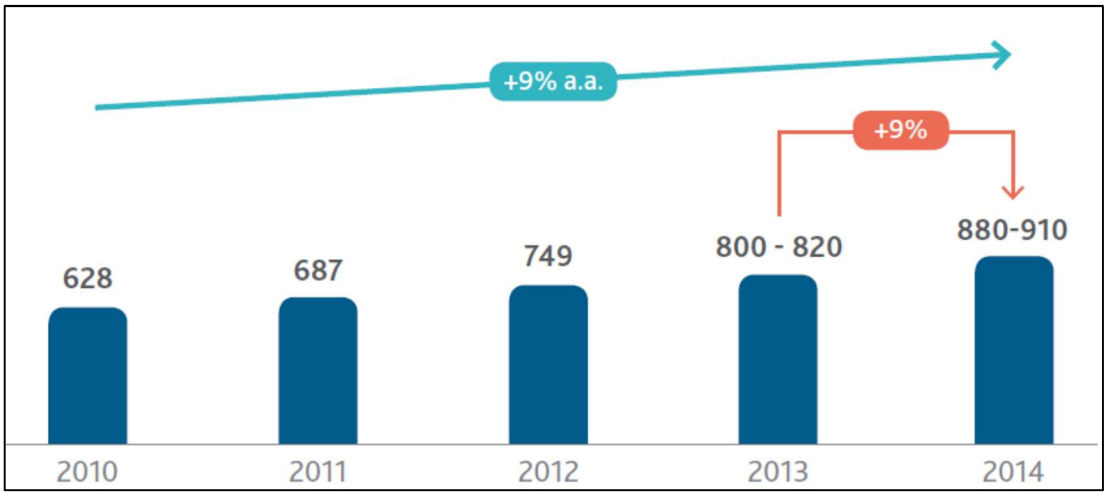

Gráfico 2 – Número de cartões de pagamento (em milhões)
Fonte: FEBRABAN, 2014.

A FEBRABAN (2011) publicou em seu *site* uma nova terminologia, denominada bancarização. Esse termo foi definido como a adoção de métricas universais para medir o acesso aos serviços financeiros e o seu grau de utilização de forma adequada, atendendo às necessidades da população e contribuindo com a qualidade de vida de seus clientes.

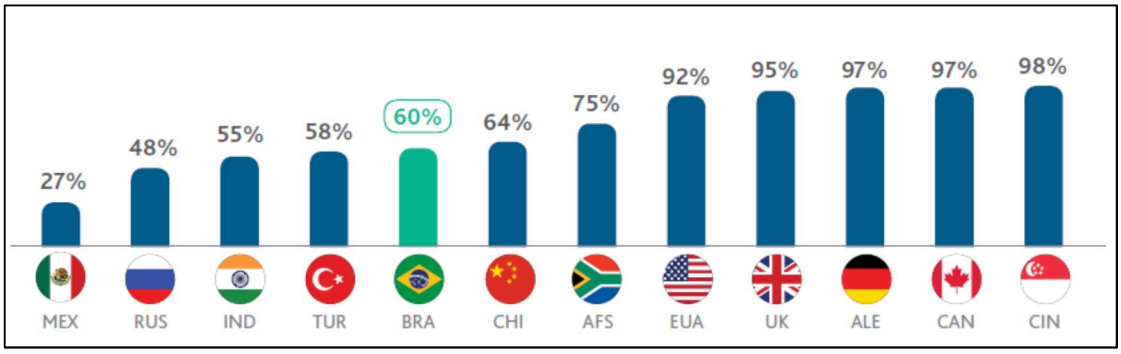

Gráfico 3 – Bancarização dos países em 2014 (% da população adulta)
Fonte: FEBRABAN, 2014.

Conforme o Gráfico 3, no Brasil, apesar do crescimento do setor bancário, a taxa de bancarização ainda é tímida. Estando em apenas 60%, esse valor está alinhado com outras economias emergentes como Índia e Turquia, bem abaixo de economias mais desenvolvidas, como EUA e Alemanha.

A partir da disponibilização e facilitação de acesso a esses serviços, a Febraban (2016) destaca que o número de transações bancárias cresceu em mais de 14 milhões de acessos em um período de quatro anos, chegando a 55.719 milhões em 2010. A rede de atendimento

cresceu 79,8% quando comparamos os números do ano de 2006 e 2010, chegando a 256.998 correspondentes. O número de cartões de pagamento chegou a 628 milhões em 2010.

Em 2014, o montante de transações realizadas com cartões de crédito somou R$ 963 bilhões, como pode ser visto no Gráfico 4. O valor representa elevação de 36,2% na comparação com o valor de 2011, que foi de R$ 614 bilhões.

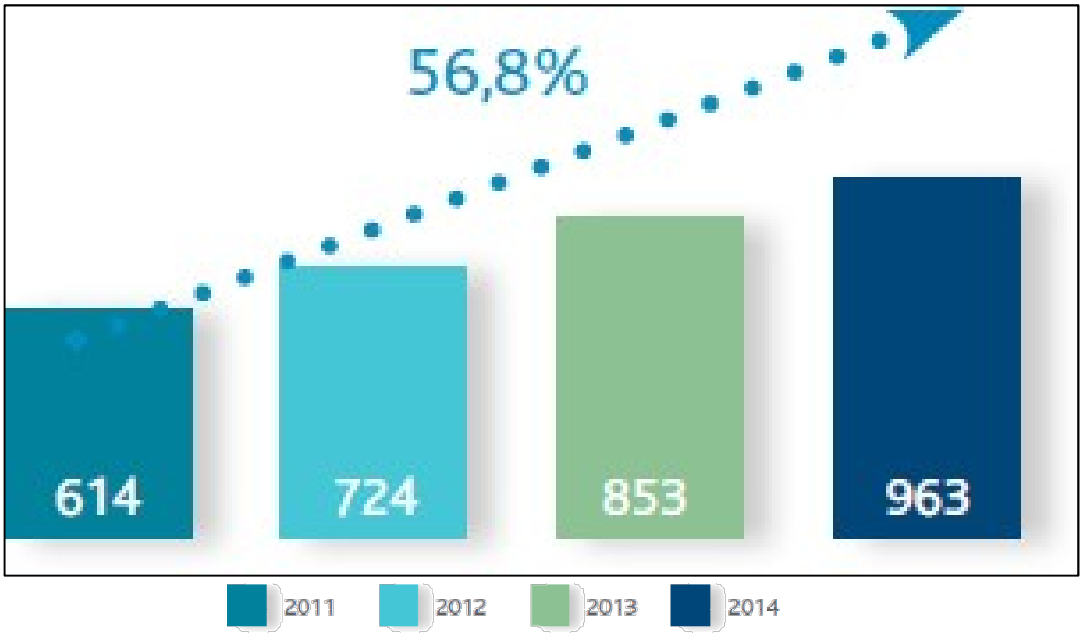

Gráfico 4 – Valor das transações com cartões de crédito (em bilhões)
Fonte: FEBRABAN, 2016.

A evolução dos sistemas informacionais bancários viabilizou meios mais rápidos, especializados e seguros para a criação de produtos e serviços com maior nível de valor agradado.

2.2.1. Personalização de cartões de pagamento bandeirados

A palavra personalização foi um termo designado ao processo de preparação e escrita dos dados do emissor ou do portador de um cartão específico na tarja magnética ou no circuito integrado no cartão (*chip*). O termo utilizado como personalização de cartões inclui preparação de dados confidenciais, codificação da tarja magnética e codificação de *chip*, conforme descrito no manual de procedimentos do PCI *Card Prodution* (PCI, 2017).

O PCI (*Payment Card Industry*) foi criado em 2006 como um fórum global aberto destinado ao desenvolvimento, gerenciamento, educação e conscientização sobre os padrões de segurança adotados pela indústria de produção de cartões de pagamento bandeirados, é uma corporação de responsabilidade limitada (LLC – *Limited Liability Companies*) baseada em Delaware, EUA, fundado pela *American Express, Discover Financial Services, JCB International, Master Card* e *Visa Inc* (PCI, 2016), no qual as marcas de pagamento ou bandeiras são as responsáveis pela definição e gestão dos programas de conformidade associados aos requisitos constantes no manual de procedimentos do PCI *Card Prodution* (PCI, 2017).

Os cartões de pagamento, que incluem cartões de crédito, débito e lojas, desempenham um papel fundamental para a população recém-bancarizada. Para os bancos, surge a possibilidade de não apenas pagamentos em espécie, mas também de novas formas de financiamento, aumentando a oferta de crédito na praça. Os gastos familiares via cartões de pagamento evoluíram oito pontos nos últimos quatro anos, saltando de 23% em 2011 para 31% em 2014 (FEBRABAN, 2016).

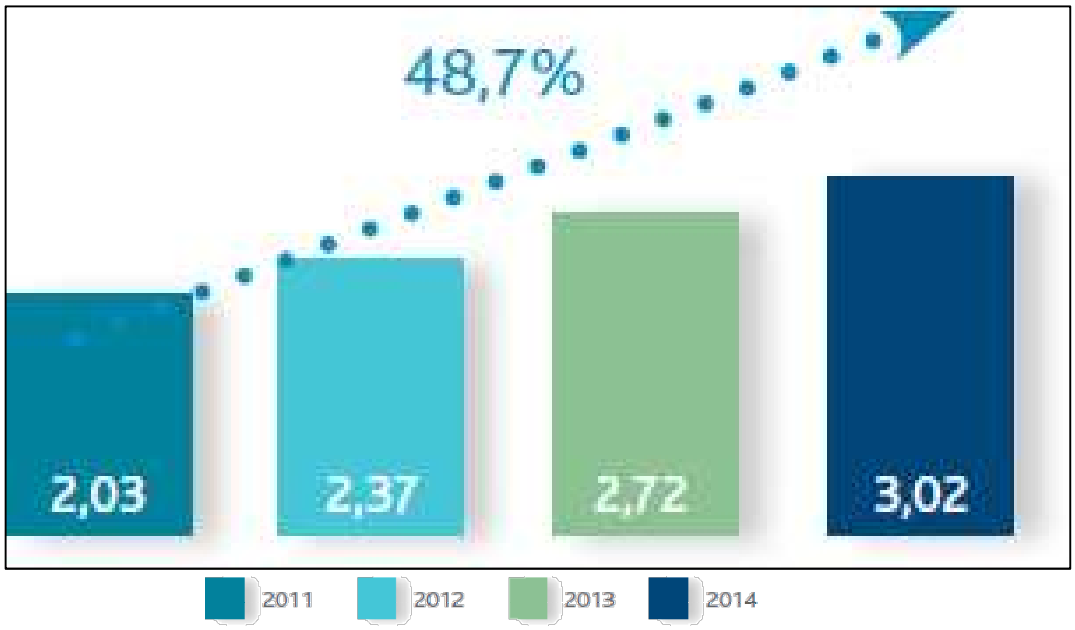

Gráfico 5 – Crescimento do crédito (em trilhões)
Fonte: FEBRABAN, 2016.

O Gráfico 5 demostra que houve um crescimento de 48,7% em relação aos anos de 2011 e 2014 do valor disponibilizado em linhas de crédito no mercado brasileiro, chegando em 2014 a 3,03 trilhões de reais.

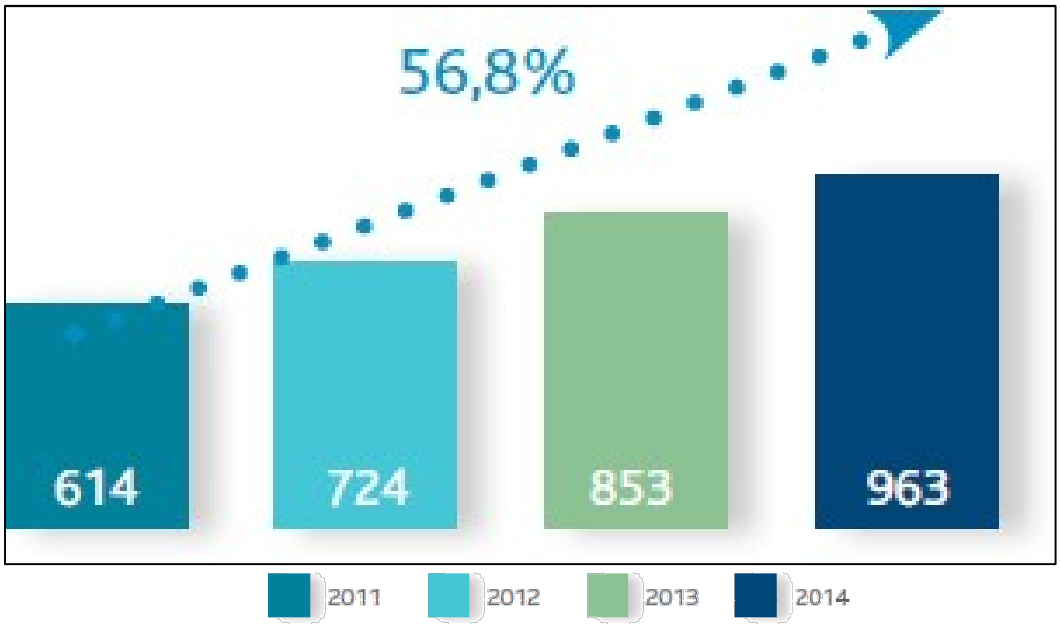

Gráfico 6 – Valor das transações com cartões de crédito (em bilhões)
Fonte: FEBRABAN, 2016.

O número de transações com cartões de pagamento no ano de 2014 chegou a 10,2 bilhões, crescimento de 11,6% em relação ao mesmo período do ano anterior. Conforme demostrado no Gráfico 6, foram R$ 610,2 bilhões em operações de crédito e R$ 353,3 bilhões em transações de débito em 2014, sendo que a alta em comparação com 2013 foi de 13,6% para os valores de crédito e de 17,8% para os de débito (FEBRABAN, 2016).

Essa aceitação demonstrada pelo grande crescimento do sistema de pagamento e financiamento rápido proporcionado pelos cartões de pagamentos bandeirados abriu um grande nicho de mercado para as empresas que se propuseram a trabalhar com a realização de serviços de produção de cartões de plástico. Essas empresas transformaram-se em organizações cada vez mais complexas, hierarquizadas, especializadas e que demandavam supervisão e gerência, por conseguinte, a preocupação passou a ser com autoridade, responsabilidade, planejamento, controle, coordenação e relações no trabalho (MOTTA, 1986).

O conceito cartão de crédito é o mais comum e difundido meio de pagamento eletrônico, seu funcionamento é relativamente simples para o consumidor final, porém requer um grau de investimento e sofisticação elevado por parte das instituições que operam o sistema. Desde a criação dos primeiros cartões de pagamento, as empresas têm buscado novas tecnologias, com o propósito de trazer conforto e maior segurança para as transações por elas acolhidas (GOMES; COSTA, 2015).

A revolução da informação, ancorada pela tecnologia dos computadores, promove novamente uma revolução dos processos organizacionais. Os processos e as atividades

desempenhados sofrem mudanças disruptivas pelo uso de sistemas de computadores, permitindo agilidade e acesso a informação em tempo real e em nível global (CORRÊA, 2014). Toda agilização de processos proporcionados pela informatização agora precisa receber tratamentos voltados aos requisitos relativos a segurança da informação, sem comprometer todo o processo produtivo e a produtividade.

Conforme Bonelli e Fonseca (1998), a produtividade da mão de obra é o mais utilizado indicador parcial do rendimento dos fatores usados na produção. Para De Lima Bezerra e Cacciamali (1997), a produtividade do trabalho é uma medida apenas parcial da eficiência dos fatores no processo produtivo. Nesse caso, nos dá a contribuição do fator mão de obra na produção, supondo estável a participação de todos os demais fatores.

Segundo Simon (1977), administrar é a arte de conseguir realizar coisas, é, fundamentalmente, tomar decisões. Para Zeleny (1982), a tomada de decisão é um processo dinâmico, na qual a busca pela informação é enriquecida pelo *feedback* resultante da análise de todas as consequências possíveis.

3. METODOLOGIA

A metodologia científica, de acordo com Vergara (2005), são os procedimentos utilizados para que os objetivos de pesquisa sejam alcançados. Prodanov e Freitas (2013) descrevem a metodologia aplicada como uma ferramenta que cria condições de examinar, descrever e avaliar métodos e técnicas de pesquisa durante a coleta e o processamento das informações, com o objetivo de resolver um problema ou uma questão de investigação.

O presente estudo analisou os impactos da segurança da informação em uma empresa personalizadoras de cartões de pagamento localizada em Contagem, Minas Gerais. Por questões de confidencialidade, o nome da empresa será preservado, a empresa estudada foi fundada em 1939 como uma editora, em 1990 se especializou na produção de formulários de segurança e chegues e em 2009 se certificou para produção e personalização de cartões de pagamento bandeirados. Atualmente a empresa conta com uma equipe de aproximadamente 450 colaboradores.

Foi adotada uma metodologia de estudo de caso com viés qualitativo, escolhida por ser a melhor estratégia quando o pesquisador tem pouco controle sobre os eventos e quando o foco se encontra em fenômenos contemporâneos inseridos em algum contexto da vida real (YIN, 2001). Segundo Prodanov e Freitas (2013), a análise qualitativa define um processo como uma sequência de atividades que envolve a redução dos dados, sua categorização, interpretação e redação do relatório no momento em que o pesquisador obtém as informações por meio de aplicações de técnicas de pesquisa.

Por ser tratar de uma pesquisa exploratória, foram utilizadas as técnicas de levantamento bibliográfico, utilizando um material já elaborado constituído de livros e artigos científicos, no qual o pesquisador faz o uso de uma gama de fenômenos muito mais amplos do que aquela que poderia pesquisar diretamente, e uma pesquisa documental, na qual são utilizadas as contribuições de diversos autores sobre um assunto pertinente à pesquisa realizada, porém sem uma validação analítica (GIL, 2008). Nessa linha, serão abordados os principais manuais e procedimentos técnicos relativos a segurança da informação que são referência no que tange a políticas direcionadas à situação de pesquisa estudada.

Para refinar as principais lacunas a respeito do objeto de pesquisa, foi realizada uma entrevista com os profissionais ligados às áreas de processamento de dados, tratamento de informações confidenciais, personalização de cartões bandeirados e manuseio de cartões personalizados conforme roteiro descrito no Apêndice B, em uma personalizadora de cartões

de pagamento localizada em Contagem, Minhas Gerais. Através de uma entrevista baseada em um roteiro semiestruturado, é possível obter informações a respeito de um problema ou de uma situação (GUIMARÃES; HAYASHI; BENZE, 2011). Conforme Manzini (1990/1991), a entrevista semiestruturada é elaborada junto a um roteiro de perguntas centrais voltadas a assuntos inerentes ao tema abordado durante a entrevista. Esse método propicia a emersão de informações de forma livre, sem um padrão de respostas aos questionamentos com a interação do informante, a fim de atingir os objetivos pretendidos.

Para compor o universo da amostra utilizada na fase de entrevista deste estudo, o público-alvo são os líderes e os funcionários envolvidos diretamente nos processos produtivos da empresa estudada, os quais, segundo Moresi (2003), compõem uma amostra probabilística que possibilita obter informações representativas a respeito do problema de pesquisa apresentado.

Por questões de confidencialidade e sigilo exigidos pelas bandeiras, os profissionais entrevistados serão identificados como Analista-M (Analista de Segurança da informação), Analista-R (Desenvolvedor), Analista-W (Processamento de dados), Coordenador-D (Setor de Personalização), Coordenador-H (Setor de Manuseio e Expedição), Gestora da Qualidade-S, Superintendente-S (CISO) e o Diretor-C. O roteiro de entrevista está detalhado no Apêndice B deste trabalho.

3.1. Trabalhos relacionados

Conforme descrito no Apêndice A, foi realizada uma pesquisa na base de dados Periódicos Capes dos últimos dez anos, utilizando-se os constructos, Cartões de Pagamento, *Payment Card Industry* (PCI) e Prestação de serviços bancários. E nos últimos quinze anos para o constructo Segurança da Informação.

Para Segurança da Informação, foram encontrados 481 periódicos, sendo 157 revisados por pares nos últimos cinco anos; destes foram filtrados 11 periódicos que contêm assuntos relacionados a esta pesquisa.

Para Cartões de Pagamento, foram encontrados sete periódicos, sendo três revisados por pares nos últimos cinco anos; dentre os três encontrados nenhum apresentou um conteúdo relacionados a esta pesquisa.

Para *Payment Card Industry* foram encontrados 4621 periódicos, sendo 163 revisados por pares nos últimos dois anos; destes foram filtrados 16 periódicos que contêm assuntos relacionados a esta pesquisa. Para esse constructo, foram consideradas as revisões a partir de dois anos, por se tratar um termo diretamente ligado ao manual de procedimentos do PCI que foi atualizado para os processos de auditoria em março de 2015.

Para Prestação de serviços relativos a serviços bancários, foram encontrados oito periódicos, sendo seis revisados por pares nos últimos cinco anos; dentre os seis encontrados, nenhum apresentou um conteúdo relacionado a este projeto de pesquisa.

3.2. Contexto da pesquisa

Este estudo tem o propósito de fornecer informações suficientes para as empresas que atuam diretamente no ramo de produção e, principalmente, de personalização de cartões de pagamento bandeirados, contribuindo diretamente na disseminação do conhecimento para elaboração de projetos técnicos relevantes e direcionados ao tratamento de informações confidenciais recebidas e processadas por empresas de prestação de serviços bancários dessa natureza.

Outro ramo que pode ser beneficiado são as empresas especializadas e certificadas pelo PCI para realização de auditorias de processos para produção de cartões de pagamento. Essas empresas podem usufruir das informações e considerações abordadas, desenvolvidas e analisadas durante a elaboração deste trabalho.

4. ANÁLISE DE RESULTADO E DISCUSSÕES

Para determinar o impacto da segurança da informação nas empresas personalizadoras de cartões de pagamento bandeirados, o presente estudo confrontou as informações técnicas a respeito de segurança da informação, de acordo com normas descritas pelo órgão que regula as normas de segurança lógica para produção de cartões de pagamento, o PCI *Card Prodution,* com as respostas dos profissionais entrevistados que atuam dentro de uma personalizadora de cartões de pagamento bandeirados. Cada um desses profissionais lida diretamente com informações confidenciais em seu cotidiano de trabalho e desempenham funções de gestão dentro de uma empresa personalizadora de cartões de pagamento.

A presente seção irá realizar uma análise comparando os resultados da pesquisa bibliográfica com as respostas fornecidas pelos entrevistados que atuam diretamente nos processos produtivos de uma personalizadora de cartões de pagamento bandeirados, buscando determinar os impactos que a implementação das políticas de segurança da informação tem nos processos e procedimentos internos e os riscos da não adoção das práticas ditadas pela política de segurança da informação.

O principal manual de procedimentos utilizado como referência técnica para a análise dos impactos da segurança da informação nos processos internos de uma personalizadora foi o PCI *Card Prodution and Provisioning – Logical Requeriments,* uma vez que, com base nesse manual, os auditores credenciados e certificados pelo PCI e pelas bandeiras criam o plano de ação que será aplicado durante a auditoria interna anual dentro das personalizadoras.

A adequação a cada um dos tópicos apontados é essencial para a liberação do certificado que homologa a produção dos cartões de pagamento. Sem esse certificado, a empresa fica impedida de produzir e personalizar cartões de pagamento bandeirados.

Foi realizada a entrevista com um dos auditores das bandeiras Visa e Master Card, durante um processo de auditoria anual dentro de uma personalizadora. Todo procedimento de auditoria durou quatro dias e aconteceu no mês de outubro de 2016. O nome do auditor é Steve Wilson, seu cargo é *Senior Auditor* e ele atua na empresa *NCC Group*. A *NCC Group Manchester Technology Centre* é uma empresa certificada PCI e autorizada a realizar as auditorias pelas bandeiras padrão EMV (*Europay, MasterCard* e *VISA*). Sua sede fica localizada em Manchester Technology Centre, Oxford Rd, Manchester M1 7EF, Reino Unido.

Durante a entrevista, o Auditor da *NCC Group* afirmou que não há nenhum tópico do PCI que seja mais ou menos relevante ou que tenha um maior peso nas avalições realizadas pelos auditores para liberação do certificado. De acordo com o Sr. Steve, durante os processos de auditoria são avaliados todos os critérios mínimos exigidos pelo PCI *Card Prodution,* realizando uma espécie de *overview* para que, após uma análise crítica inicial, seja montado um plano de ação focado nas principais lacunas que o auditor entender como importantes. Para isso, a empresa auditada deve responder a um questionário denominado *Card Production Report on Compliance*, que é enviado com vinte dias de antecedência da data inicial do processo de auditoria.

Todo o cronograma de auditoria é baseado nas respostas fornecidas neste questionário. As evidências são apresentadas pela empresa, conforme solicitado pelo auditor durante o processo de auditoria.

Após a conclusão de todo o processo de auditoria, que leva em média três dias, é gerado um relatório para ser encaminhado às bandeiras, contendo o parecer técnico e as análises pessoais do auditor sobre os processos internos identificados dentro da personalizadora. Com base nesse relatório analítico, as bandeiras liberam ou não o certificado de homologação que autoriza a personalização dos cartões de pagamento bandeirados.

Conforme dito durante a entrevista com o Sr. Steve Wilson,

> Geramos o relatório e encaminhamos separadamente a cada uma das bandeiras auditadas para apreciação, considerações e liberação do certificado. O parecer do auditor é extremamente relevante para liberação do certificado que, caso não seja favorável, pode implicar na suspensão de três meses ou na revogação do certificado para produção e personalização dos cartões (AUDITOR STEVE WILSON).

Às empresas que não atenderem às expectativas de uma determinada bandeira, conforme dito pelo Sr. Steve, é proposto um plano de readequação com prazo máximo de três meses para a tratativa das não conformidades apontadas. Após o prazo de três meses, é marcada uma nova auditoria para apresentação dos resultados e averiguação. Durante esse período, a personalizadora fica impedida de produzir os cartões da bandeira na qual foi descredenciada temporariamente, além de ter que arcar com os custos de um novo plano de auditoria, que deverá ser realizado após o comprimento do plano de adequações aprovados pelo auditor.

No Brasil, conforme relatado pelo CISO, não existem empresas credenciadoras, autorizadas a auditar personalizadoras pelo PCI, a realizar auditorias internas em empresas produtoras e personalizadoras de cartões de pagamento Visa, Master e JCB (*Japan Credit Bureau*).

A personalizadora que serviu como base para este estudo não será identificada, porém todos os processos apresentados e os requisitos de segurança da informação abordados neste trabalho podem ser aplicados a qualquer empresa que realiza a prestação de serviços de personalização de cartões de pagamento no mundo, uma vez que o manual de procedimentos do PCI *Card Prodution* é único, e deve ser seguido por qualquer empresa personalizadora de cartões de pagamento bandeirado.

> O PCI Security Standards Council é um fórum global aberto, lançado em 2006, que é responsável pelo desenvolvimento, gerenciamento, educação e conscientização sobre os Padrões de Segurança do PCI, incluindo: os requisitos do Padrão de Segurança de Dados, Padrão de Segurança de Dados de Aplicativo de Pagamento e Dispositivo de Entrada de Pin [...]
> [...] Todas as cinco marcas de pagamentos compartilham igualmente a governança do conselho, colaboram igualmente com o PCI Security Standards Council e compartilham a responsabilidade de realizar o trabalho da organização (PCI, 2016).

A partir da criação e aceitação pela bandeira das regras de segurança estabelecidas pelo PCI, qualquer empresa seja ela multinacional ou nacional, a partir de 2006, foi obrigada a se adequar às normas de governança e segurança ali descritas. Esse fator culminou em estudos para adequação das normas de segurança da informação e investimentos em tecnologia da informação a serem realizados pelas empresas personalizadoras de cartões de pagamento bandeirados.

No Brasil, a produção de cartões de pagamento foi alavancada pela grande facilidade de crédito imediato, o que culminou no aumento da demanda por cartões e, como consequência, na migração de empresas, em sua maior parte multinacionais, personalizadoras de cartões para o mercado brasileiro.

Uma reportagem publicada no *site* Valor Econômico, em dezembro de 2012, relata que a Morpho e-Documents, empresa do grupo Safran, inaugurou uma linha de produção de semicondutores na fábrica que possui em Taubaté. A fábrica recebeu um investimento de 4 milhões de euros e terá capacidade para processar 60 milhões de *chips* por ano.

Em uma outra reportagem publicada em agosto de 2013 pela revista Exame, relata que de abril a junho, a Valid, empresa personalizadora de cartões de pagamento, obteve um lucro líquido de 20,4 milhões de reais, ante 40,3 milhões de reais no mesmo período de 2012.

Ambas as reportagens corroboram que os investimentos mobilizados para fabricação e personalização dos cartões de pagamento tiveram um grande crescimento. Diante desse cenário, fica explícita a necessidade de adotar regras de segurança da informação que garantam o sigilo das informações processadas por essas empresas personalizadoras de cartões de pagamento.

Segundo o ITGI (2006), a Federação Internacional de Contabilistas (IFAC) definiu o objetivo da segurança da informação como a proteção dos interesses daqueles que dependem da informação e dos sistemas de informação e comunicações que fornecem a informação, dos danos resultantes de falhas de disponibilidade e integridade.

O PCI focou em segurança lógica e criou um manual de procedimentos exclusivo para atender a esse requisito. Todo processo que envolve a auditoria anual realizada pelas bandeiras é moroso e tem início quando a personalizadora começa a responder ao questionário denominado *Card Production Report on Compliance.* Em seguida, esse questionário deve ser encaminhado ao auditor com prazo mínimo de vinte dias de antecedência da data da auditoria *in loco*.

O *Card Production Report on Compliance* obriga a empresa auditada a fornecer informações sobre todo seu processo produtivo, detalhando todo o fluxo de recepção, tratativa das informações sensíveis, processo de personalização, responsáveis por cada área de atuação no processo de personalização e pela expedição dos cartões.

Durante a entrevista com o auditor Steve, ficou claro que sua interpretação pessoal é relevante, tendo um impacto direto na liberação do certificado emitido pelas bandeiras. Conforme o auditor relatou, “sou eu quem faz e envia os relatórios sobre a auditoria para as bandeiras, minha palavra é o que autoriza ou descredencia a empresa a produzir cartões” (AUDITOR STEVE WILSON).

Tomando como base essa informação, fica claro que os requisitos de segurança abordados no manual do PCI são relevantes, mas as opiniões pessoais do auditor acerca do que está sendo analisado têm grande peso no processo de certificação da personalizadora.

Outro fator que tem influência direta no processo de certificação das bandeiras e permite que o auditor seja subjetivo em sua análise técnica é que o PCI *Card Production Logical Security Requirements* não é específico em suas abordagens e colocações. O PCI é um guia de procedimentos que deixa margem para interpretações dos especialistas em segurança e tecnologia.

Durante a entrevista com CISO e com os Analistas, eles deixaram claro que, em muitos tópicos, o PCI não é completamente claro. Conforme o Analista-M, há a necessidade de buscar em outros manuais e modelos de referência em segurança lógica informações técnicas e procedimentos para subsidiar a criação da política de segurança da informação.

Essa lacuna fica mais evidente quando realizado o levantamento de requisitos de um determinado assunto relativo a segurança da informação. Essa margem de interpretação, deixa a empresa suscetível da subjetividade do auditor que, muitas vezes, deve ser convencido por meio de argumentos sobre a conformidade de um determinado requisito.

A argumentação que o CISO estabelece com o auditor durante o processo de auditoria dentro da empresa *in loco*, na tentativa de convencê-lo sobre a regularidade de uma não conformidade apontada pode abrir lacunas na segurança lógica, levando em conta que a descrição de um determinado requisito do PCI pode não ser completamente claro.

Casos como este, que abrem margem para uma interpretação pessoal, têm a tendência de culminar em uma discussão entre o CISO e o auditor e pode ser conduzida de forma incoerente ou precipitada em relação a uma não conformidade apontada. A interpretação pessoal sem uma argumentação técnica bem embasada pode ter um grande impacto no que tange à tratativa de dados sigilosos, abrindo uma lacuna na segurança lógica ao ignorar procedimentos ou deixar de discuti-los durante o debate com o auditor.

4.1. Política de segurança da informação

Dantas (2011) enfatiza o quanto é preocupante a segurança da informação e o quanto de trabalho há pela frente para se atingir um padrão eficiente em segurança da informação.

O *PCI Card Prodution and Provisioning – Logical Requeriments*, atualmente em sua versão 2.0 publicada em janeiro de 2017, tem o objetivo de estabelecer níveis mínimos de segurança lógica que as personalizadoras devem cumprir para realização das atividades de codificação da banda magnética e a gravação do *chip* nos cartões de pagamento (PCI, 2017).

A primeira recomendação do PCI é a nomeação de um *CISO* (*Chief Information Security Officer*), um profissional que tem a incumbência de ser um gestor sênior, com conhecimentos adequados para assumir as responsabilidades sobre os requisitos de segurança da informação dentro da empresa.

Durante a entrevista realizada com Diretor-C, ficou clara sua preocupação quanto à nomeação de um CISO com conhecimentos e autoridade suficiente para criar e fazer cumprir as normas de segurança da informação dentro da empresa.

> Existe uma preocupação em cumprir todas as normas internacionais exigidas pelas bandeiras para que a empresa possa estar preparada para desempenhar seu papel na produção de cartões. O CISO é um profissional qualificado e de alta confiança; ele tem a obrigação de cumprir e fazer cumprir todas as normas exigidas internacionalmente dentro da empresa. Nós somos obrigados e fazemos questão de cumprir todas essas recomendações do PCI (DIRETOR-C).

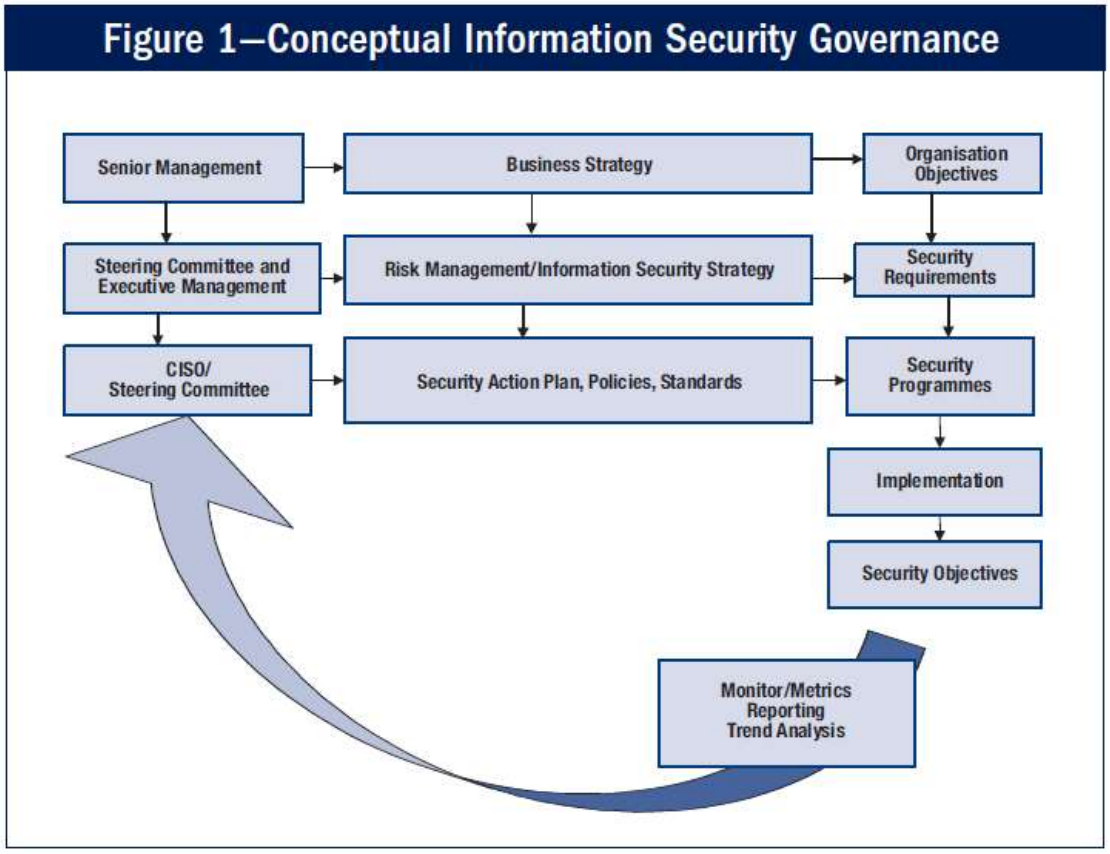

Figura 4 – *Conceptual information security governance*
Fonte: ITGI, 2006, p. 16.

Na Figura 4, o ITGI (2006) demostra que o CISO é um profissional da alta direção e estratégico, designado pela empresa especialmente para ser encarregado da gestão de segurança da informação da organização, garantindo o alinhamento do programa de segurança lógica com os objetivos organizacionais.

É extremamente necessário que o CISO conheça todos os processos inerentes à segurança da informação que permeiam os processos produtivos dentro da empresa. Obviamente isso implica em conhecer profundamente todos os processos que envolvem recepção, processamento, personalização e expedição dos cartões de pagamento bandeirados.

Chan e Reich (2007) ressaltam a alta cúpula estratégica das organizações, reconhecem a necessidade de alinhamento entre as estratégias de TI e as estratégias de negócio da empresa.

Uma das principais atividades desempenhadas pelo CISO é a criação de uma política de segurança da informação alinhada com os objetivos da empresa. O CISO deve ter autoridade suficiente para garantir o cumprimento de todas as normas ditadas na política de segurança da informação, sendo um profissional dedicado a Segurança da Informação e subordinado diretamente ao diretor presidente.

A política de segurança da informação é um documento que deve estar sempre atualizada, descrevendo todos os grupos, funções e responsabilidades relativas aos profissionais envolvidos no processo de personalização de cartões bandeirados (PCI, 2017).

Durante a entrevista realizada com CISO, também denominado Superintendente-S, foi confirmado que a empresa possui uma política de segurança da informação, criada por ele mesmo e baseada nas normas ditadas pelo *PCI Card Prodution and Provisioning – Logical Requeriments.* O CISO afirmou que esse documento é de acesso confidencial e abrange todos os tópicos necessários e relevantes para o cumprimento das regras de segurança lógica da empresa, com a missão de deixá-la em conformidade com os processos de auditoria estabelecidos pelo PCI.

Segundo o CISO, a política de segurança da informação é um documento que serve de base para a criação do manual de procedimentos de gestão de segurança da informação, chamado de PG-SETI (*Procedimento de Gestão – Segurança da Tecnologia da Informação).*

O PG-SETI é um documento que auxilia na aplicação das normas ditadas na política de segurança da informação. Este documento contém, de forma detalhada, todas as normas e os procedimentos ditados na política de segurança, contendo o passo a passo de como realizar uma determinada tarefa, como monitorar um determinado processo que ocorre na personalização, como garantir a rastreabilidade das informações sigilosas que trafegaram na personalizadora, como assegurar que todo o procedimento esteja documentado conforme as recomendações do PCI e como verificar que todo o procedimento de segurança está sendo cumprido conforme a política de segurança da informação.

Na concepção do ITGI (2006), a segurança da informação abrange todos os processos de informação, físicos e eletrônicos, independentemente se envolvem pessoas e tecnologia ou relações com parceiros comerciais, clientes e terceiros. A política deve contemplar todos esses aspectos, levando em conta pessoas, procedimentos e infraestrutura necessária para prover os recursos de tecnologia sem abrir mão dos requisitos de segurança.

Durante a entrevista a respeito de terceiros e sobre os processos e procedimentos internos no que se refere a conscientização sobre a política de segurança da informação, os analistas Analista-M, Analista-W e Analista-R afirmaram que não há um treinamento ou processo de conscientização destinados aos prestadores de serviço. Conforme os analistas, os prestadores de serviço são cadastrados e orientados quanto às normas de acesso ao interior da fábrica de cartões, a HSA (*high security area*), porém não há um procedimento formal de treinamento, destinado a terceiros ou visitantes que necessitem utilizar os recursos tecnológicos internos.

Os analistas demostraram preocupação a respeito da disseminação das regras que constam na política de segurança da informação, principalmente em relação aos prestadores de serviço.

O CISO afirmou que todos os terceiros são conscientizados, mas não informou como e em que momento isso ocorre. Conforme o CISO, “O foco da política é servir de referência para garantir que todos os requisitos de segurança da informação sejam cumpridos em qualquer âmbito da empresa, por qualquer um que esteja dentro dela” (SUPERINTENDENTE-S – CISO). O CISO, afirmou que os terceiros são conscientizados sobre as normas de segurança lógica, mas não foi capaz de dizer como isso acorre ou onde está descrito no PG-SETI.

A segurança da informação trata da proteção, confidencialidade, disponibilidade e integridade da informação ao longo do ciclo de vida da informação e seu uso dentro da organização. Marciano (2006) reforça que é claro que a segurança da informação requer uma atenção especial, uma vez que permeia todo o complexo da informação no ambiente tratado e negligenciá-la pode até inviabilizar a execução das atividades-fim da organização.

Essa divergência de informações fornecidas pelo CISO e pela equipe de analistas deixa evidente que há uma falha na política de segurança da informação, quanto ao treinamento e à conscientização de terceiros sobre segurança lógica. Este é um fator importante e pode acarretar em um sério risco à segurança da informação, uma vez que um terceiro pode propagar um vírus ou ter uma ação que comprometa a integridade dos dados confidenciais. É importante ter rotinas que promovam um treinamento estruturado aos terceiros, de maneira formal e aprovada pelo CISO.

O ITGI (2006) deixa claro que assegurar a eficácia da política de segurança da informação através de revisões e aprovação do comitê diretor é uma prática essencial para manter os níveis adequados de segurança na empresa. O diretor demostrou plena ciência da importância e necessidade de se ter uma política de segurança da informação consolidada, efetiva e atualizada como forma de suporte à homologação da empresa no mercado de personalização de cartões de pagamento.

Conforme informações fornecidas pelo CISO, a política é atualizada anualmente de acordo com as regras ditadas pelo PCI. Depois de realizadas as atualizações, são ministrados treinamentos com a equipe de segurança da informação, para disseminação das regras aos demais setores, garantindo o cumprimento das normas ditadas na política.

Os analistas Analista-M, Analista-W e Analista-R confirmam a importância de estabelecer rotinas de treinamento para alinhamento das informações e novas regras a respeito

da política de segurança da informação, porém não corroboraram as informações do CISO a respeito da rotina de treinamento e não souberam dizer quando foi realizado o último.

Durante a entrevista com a Gestora da Qualidade-S, responsável por padronizar e armazenar todos os documentos da empresa, ela garantiu que tanto a política de segurança da informação quanto o procedimento de segurança da informação são padronizados e disponibilizados na intranet com controle de versão e controle de acesso. Conforme a Gestora, existe uma regra para ministração de treinamentos anuais, direcionada aos profissionais da empresa, mas ela não soube dizer nada quanto ao treinamento direcionado a terceiros.

O impacto ligado a criação e disseminação da Política de Segurança da Informação internamente e a terceiros é dimensionada como muito alta, uma vez que toda a estrutura tecnológica física e lógica, processos produtivos e controle de acessos a informações confidenciais dentro da empresa precisam estar alinhados com essa política e aplicáveis.

Uma empresa personalizadora lida com informações confidenciais em todo seu ciclo produtivo, um plano de treinamento formal, detalhando os principais processos relevantes a cada área interna, principalmente para aquelas que processam ou manuseiam informações sensíveis, e é essencial para garantir o cumprimento dos requisitos de segurança tecnológica que constam na política de segurança da informação.

É recomendado que os processos de treinamento sejam ministrados por um profissional competente e direcionados aos setores ou pessoas que estão recebendo esse treinamento, levando em conta as peculiaridades do setor, identificando os principais processos envolvidos na tratativa de informações confidenciais e os principais cuidados que devem ser tomados para preservar a confidencialidade e integridade das informações, de acordo com a política de segurança da informação.

O não cumprimento desse requisito, a respeito do treinamento e da conscientização no que tange à política de segurança da informação, tem um grande impacto em todas as áreas da empresa e, por consequência, no processo produtivo.

Falhas na segurança que por ventura possam ser identificadas durante o processo de auditoria anual realizado pelas bandeiras podem acarretar em perda do certificado que homologa a personalizadora a produzir cartões. Se a empresa perder a homologação, ela deixa de produzir.

Os impactos por uma política de segurança da informação inconsistente ou não disseminada corretamente tem um reflexo negativo na tratativa de dados confidenciais e, por consequência, em todo processo de segurança lógica. Deixar de treinar, treinar de forma incorreta ou incompleta, ministrar treinamentos não direcionados à realidade de cada setor ou deixar que treinamentos sejam realizados por profissionais não preparados deixam a política de segurança da informação com um *status* ou conceito de um documento irrelevante.

4.2. Segurança dos dados confidenciais

A confidencialidade e integridade são indispensáveis para atender aos requisitos de segurança de dados confidenciais. Dantas (2011) argumenta que a confidencialidade e a integridade dos dados devem ser consideradas, implementadas e auditadas, a fim de propiciar um nível de segurança eficiente e proativo.

O tratamento de dados confidenciais é assunto abordado no Capítulo 4 do PCI *Card Prodution* com foco no sigilo das informações relativas aos portadores de cartões de pagamento.

O PMI (2013) descreve que é necessário determinar se a informação trafegada é sensível ou confidencial e se devem ser tomadas medidas adicionais de segurança ou não para resguardá-las. Inicialmente, é necessário que o CISO determine quais informações serão tratadas como confidenciais e cada tipo de dado ou informação deve ser classificada.

O PCI (2017) recomenda que a informação seja classificada da seguinte forma:

- ***Dados secretos***. Informação que quando conhecida por qualquer indivíduo resultaria no comprometimento generalizado de ativos financeiros, incluindo as informações relativas ao HSM (*Hardware Security Module*) que fazem referência a chaves e criptogramas utilizados no processo de criptografia dos dados dos cartões de pagamento. É uma informação de grande sensibilidade.

- ***Dados confidenciais***. Informações que podem oferecer vantagens competitivas, prejuízo comercial ou exposição desnecessária de informações sigilosas, como, por exemplo, dados dos portadores de cartões de pagamento, tais como as credenciais de acesso às informações gravadas no *chip* e o número PAN (*Primary Account Number*) dos cartões de pagamento. O comprometimento desse tipo de informação pode acarretar em transtornos aos clientes portadores dos cartões de pagamento, incluindo fraudes.
- ***Dados públicos***. Informações que não foram classificadas como confidenciais ou secretas, porém devem ser explicitamente classificadas pelo CISO como públicas. Esse tipo de informação não afeta diretamente os clientes, portadores de cartões de pagamento ou as bandeiras. São informações do cotidiano da empresa, como relatórios e papéis com relatórios e controles internos.

Durante a entrevista realizada com CISO, responsável pela identificação e classificação das informações, quem foi indagado sobre qual a importância da classificação das informações e quais os principais critérios que são levados em conta para a classificação dos dados ou das informações.

> A classificação da informação é pertinente sim e tem por objetivo dar ciência a todos os envolvidos sobre as restrições de divulgação de informações, principalmente quanto às informações que não podem ser divulgadas.
> Os critérios utilizados para classificação obedecem às recomendações do próprio PCI, tudo que é dado ou informações relativas a chaves de criptografia, informações sobre os titulares de cartões é classificada como informação secreta (SUPERINTENDENTE-S).

Ainda conforme o CISO, após estabelecer os níveis de classificação das informações, as tratativas que serão aplicadas a cada um dos níveis são determinadas e, a partir daí, toda informação que trafegue dentro da empresa deve ser classificada antes de ser armazenada ou divulgada.

O padrão de formatação a ser seguido para classificação das informações é ditado pelo setor de controle de qualidade. Esse setor é o responsável pela padronização e pelas adequações dos documentos e informações, com base nas regras de certificação ISO-9001. Conforme entrevista com a Gestora da Qualidade-S, qualquer documento interno, seja ele um contrato, formulário ou relatório, deve ser corretamente classificado e cadastrado para receber sua respectiva marcação relativa ao nível de confidencialidade determinado pelo CISO. O controle dos documentos é realizado através de uma lista mestra, na qual constam todos os

nomes, tipos de documentos, classificação e informações relativas ao tratamento de que este documento precisa receber. A lista mestra deve ser assinada pelo CISO, validando e dando ciência sobre as informações ali presentes.

A Gestora da Qualidade-S demostrou um conhecimento superficial da importância da classificação da informação; ela não foi capaz de exemplificar as possíveis consequências de um vazamento de informações classificadas como secretas ou confidenciais e não soube afirmar se essas diretrizes de classificação de documentos constam na política de segurança da informação.

É importante a conscientização dessa profissional a respeito dos níveis de sigilo que a empresa trabalha. A Gestora da Qualidade-S tem acesso livre a uma gama de informações confidenciais e isso a obriga a ter conhecimento das consequências de uma divulgação não autorizada. Existe um sério risco nesse quesito que pode ser facilmente explorado através de técnicas de engenharia social.

Dantas (2011) diz que pontos de vulnerabilidade apresentados nas pesquisas sobre segurança da informação tem relação com os funcionários e prestadores de serviço. A fuga das informações e sua exposição involuntária ocorrem em momentos simples do dia a dia das empresas, o que torna os recursos humanos uma das maiores preocupações para implementação de políticas e treinamentos voltados à proteção das informações.

O PCI (2017) recomenda que sejam realizados processos de treinamentos anuais com os funcionários envolvidos nos procedimentos de personalização de cartões de pagamento bandeirados.

Dantas (2011) reforça que as vulnerabilidades humanas constituem a maior preocupação dos especialistas, já que o desconhecimento de medidas de segurança é a sua maior vulnerabilidade.

Conforme a Ernst & Young (2012), o volume de perdas não intencionais de dados provocadas pelos funcionários vem crescendo consideravelmente; uma gestão eficiente, treinamento e conscientização podem frear a crescente ocorrência dessas perdas.

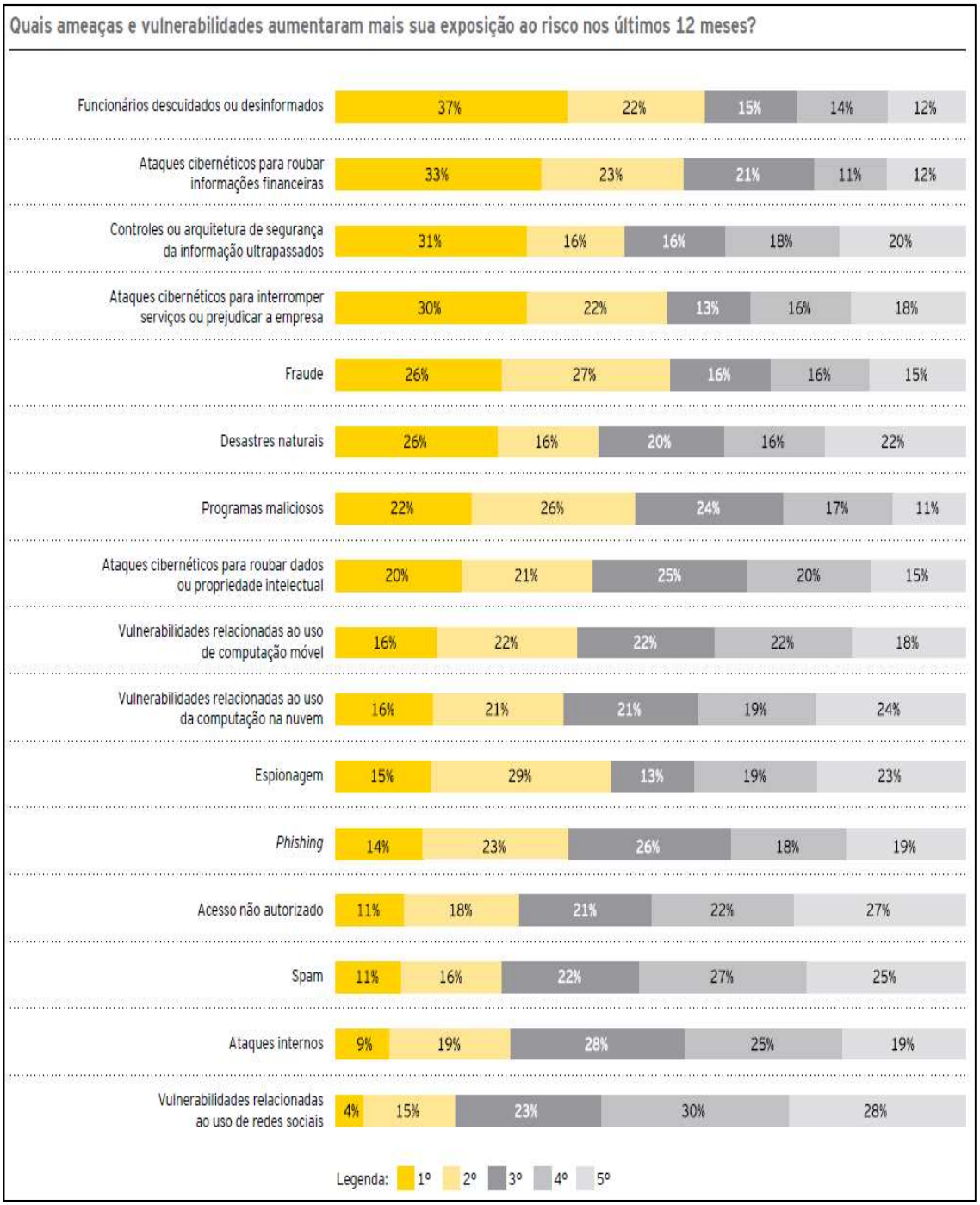

Figura 5 – Exposição ao risco em tecnologia
Fonte: ERNST & YOUNG, 2012, p. 21.

Conforme a Figura 5 demonstra, em uma pesquisa realizada no ano de 2012 pela Ernst & Young, mais de 37% dos entrevistados apontaram os funcionários descuidados ou desinformados como ameaças que mais aumentam a exposição da empresa ao risco. A Ernst & Young (2012) acrescenta que o número de incidentes ligados a funcionários negligentes que causaram perda de dados confidenciais aumentou em 25% ao longo de 2012.

Nakamura (2007) argumenta que a implementação de política de segurança requer verbas para suporte para os programas de conscientização dos usuários e treinamentos, principalmente no que tange a substituição de tecnologias e o estabelecimento de procedimentos adicionais.

Maulais (2016) ressalta que não existe uma tecnologia boa o suficiente para evitar um ataque; é necessário investir em treinamento dos funcionários para eles estejam sempre atualizados e é de vital importância que haja uma política de segurança da informação implementada e divulgada para conscientização de todos de como se proteger e das penalidades em caso de displicência.

Conforme Maulais (2016), o uso consciente e planejado das instruções dadas pela empresa é que faz a diferença, o funcionário deve ser preparado de maneira ampla. O funcionário precisa estar ciente e consciente dos perigos eminentes; ele precisa ter o mínimo de conhecimento necessário para identificar atividades suspeitas de engenharia social.

Quando a Gestora da Qualidade-S foi questionada sobre como é realizado o controle de acesso a essa lista mestra e quais critérios devem ser seguidos para a inserção de informações, no que tange aos documentos classificados como secretos ou confidenciais, ela se sentiu desconfortável para responder, porém disse que tudo é feito conforme orientações do CISO.

Não foi autorizada a divulgação da listra mestra deste trabalho, por questões de confidencialidade e sigilo, mas ela foi exibida durante a entrevista com a Gestora de Qualidade-S e, através dessa apresentação, foi possível identificar que nesse documento constam informações relativas ao local de armazenamento dos documentos, ao período de armazenamento, a informações sobre a classificação dos documentos, às informações sobre os responsáveis por esse documento e ao setor que ele pertence e às informações sobre os processos de descarte desses documentos. A Gestora da Qualidade-S reforça que todas essas informações são registradas conforme as orientações do CISO.

Quando questionada sobre os períodos de treinamento a respeito de segurança da informação, a Gestora de Qualidade-S afirmou que acontecem anualmente, mas que não se lembra dos assuntos abordados a respeito de engenharia social ou classificação de dados sigilosos.

Os impactos negativos causados pelo vazamento de informações confidenciais em uma empresa personalizadora de cartões de pagamento bandeirados, conforme corroborado pelo Diretor-C, têm um reflexo direto na imagem da empresa. A gestão de documentos é fundamental para gerenciar a divulgação ou o controle de acesso a quaisquer informações.

Toda informação classificada como secreta ou confidencial precisa ter critérios bem definidos que contemplem desde a recepção, passando pela transmissão e pelo armazenamento, até o descarte. O PCI (2017) recomenda que esse tipo de informação deve ter todo seu tráfego auditado via *log* de sistema, e os dados devem permanecer cifrados durante todo o processo de transmissão e armazenamento, sendo decifrados pelo menor tempo possível e apenas dentro da área de alta segurança, com a finalidade de garantir a integridade e confidencialidade dos dados. As informações devem ser recebidas ou transmitidas apenas por fontes previamente autorizadas e nunca enviadas ou disponibilizadas publicamente.

O processo de criptografia dos dados classificados como secretos ou confidenciais é um controle exigido durante todo o processo de transmissão e armazenamento dos arquivos. No Capítulo 4, o PCI (2017) faz uma série de exigências quanto ao tamanho das chaves de criptografia utilizadas e o algoritmo adotado, conforme demostrado na Figura 5.

Algorithm	DES	RSA	Elliptic Curve	DSA/D-H	AES
Minimum key size in number of bits:	112	1024	160	1024/160	–
Minimum key size in number of bits:	168	2048	224	2048/224	–
Minimum key size in number of bits:	–	3072	256	3072/256	128
Minimum key size in number of bits:	–	7680	384	7680/384	192
Minimum key size in number of bits:	–	15360	512	15360/512	256

Figura 6 – Tamanhos de chaves mínimos e equivalentes e pontos fortes para algoritmos aprovados
Fonte: PCI, 2017, p. 53.

Durante a entrevista realizada com os analistas, eles garantiram que toda informação relativa a cartões de pagamento bandeirados, recebida e processada pela empresa, é cifrada e armazenada em servidores com controle de acesso, localizados dentro da área de alta segurança. O CISO reafirmou que toda informação enviada para a empresa é recepcionada, cifrada e transmitida para a área de alta segurança para ser processada.

Conforme o CISO, “toda informação relativa aos dados dos portadores dos cartões de pagamento permanecem na empresa pelo menor tempo possível, sendo apagadas assim que acontece a expedição dos cartões” (SUPERINTENDENTE-S - CISO), e garantiu que todo esse processo pode ser constatado e rastreado através de registos de *log* de acesso em cada um dos sistemas e servidores.

O PCI (2017) recomenda que todo esse processo de recepção, processamento e descarte de informações confidenciais deve ser auditado via *log* de sistema, e as informações relativas aos portadores de cartões de pagamento devem ser apagadas de forma irrecuperável. Tanto o CISO quanto a Gestora da Qualidade-S for seguros em afirmar que existe um procedimento formal na política de segurança da informação para tratar dos requisitos a respeito da eliminação de informações confidenciais. De acordo com a Gestora da Qualidade-S, esse processo é auditado trimestralmente e levado ao conhecimento do CISO.

Dantas (2011) argumenta que a informação nasce com a produção, tem um tempo de vida útil, no qual é manuseada, utilizada interna e externamente, transportada por diferentes meios, armazenada, e morre com sua destruição. A identificação das necessidades e dos requisitos é o ponto de partida para o ciclo de vida da informação.

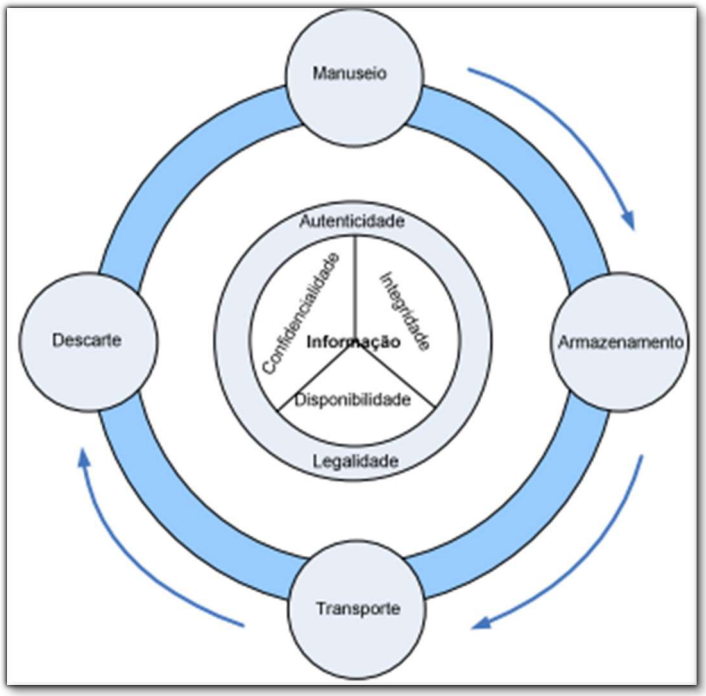

Figura 7 – Ciclo de vida da informação
Fonte: SÊMOLA, 2003.

Na Figura 7, Sêmola (2003) afirma que é necessário mitigar os riscos que envolvem os quatro momentos de vida da informação, sendo eles o manuseio, momento no qual a informação é manipulada, o armazenamento, momento no qual a informação é armazenada, o transporte e o descarte, momentos nos quais a informação é transferida e excluída de forma definitiva.

Os procedimentos de classificação e tratamento de dados secretos e confidenciais são de extrema importância para as personalizadoras de cartões de pagamento bandeirados, uma vez que as informações sigilosas precisam ser identificadas, classificadas e monitoradas durante todo fluxo do processo de personalização de cartões, a fim de garantir se os requisitos como confidencialidade e integridade são efetivos.

Todo procedimento de segurança de dados confidenciais tem início na comunicação entre emissores e personalizadora e deve constar na política de segurança da informação. As equipes envolvidas nesse processo precisam ser treinadas e conscientizadas sobre os níveis de confidencialidade com que estão lidando. Dar conhecimento e preparar os envolvidos nos processos que lidam com informações sigilosas é essencial para manter a segurança das informações.

Conforme entrevista realizada com Diretor-C e CISO, o vazamento de uma informação confidencial traria sérios problemas à imagem da empresa no mercado de personalização de cartões de modo generalizado. O Diretor-C enfatizou que "não se pode imaginar ou cogitar tal situação que exponha a empresa de forma tão pejorativa" (DIRETOR-C).

O CISO foi seguro ao afirmar que todos os cuidados cabíveis quanto a confidencialidade e integridade das informações são assegurados e auditados pela empresa. Não foi respondida a pergunta referente a como esse procedimento é realizado.

Cabe à empresa estabelecer parâmetros ou buscar referências para, obrigatoriamente, atender de forma plena aos requisitos. Independentemente da linha a ser adotada, todas as etapas do ciclo de vida da informação são importantes (DANTAS, 2011).

4.2.1. Fluxo de transmissão dos dados dos titulares dos cartões

Em uma personalizadora de cartões de pagamento bandeirados, dados confidenciais são qualquer informação que possa conceder ao fornecedor uma vantagem competitiva, causando danos comerciais ou exposição legal se a informação for usada ou divulgada sem restrições. Os dados confidenciais são dados restritos a indivíduos autorizados (PCI, 2017).

Toda informação classificada como secreta ou confidencial precisa receber um tratamento específico focado nos requisitos de confidencialidade e integridade. Conforme o ITGI (2006), o equilíbrio entre a segurança da informação e uma boa gestão de tecnologia, está em tomar as ações necessárias para garantir que os riscos inerentes a privacidade e confidencialidade da informação estejam alinhados às necessidades da empresa, garantindo que a informação seja divulgada apenas para aqueles que precisam saber.

O PCI (2017) recomenda que todas as informações confidenciais transmitidas estejam criptografadas e que os aplicativos responsáveis pela transmissão e recepção dos arquivos possuam mecanismos que garantam a identidade e a autenticidade do emissor.

É muito importante que os meios de comunicação e transmissão de dados entre a personalizadora e os emissores sejam seguros. O PCI (2017) exige que essa transmissão aconteça através de links dedicados ou VPN (*Virtual Private Network*) com certificado digital, para garantir que todo o tráfego externo esteja cifrado e direcionado.

É de responsabilidade da personalizadoras, garantir que os dados recebidos sejam de emissores pré-autorizados (PCI, 2017). De acordo com o Analista-M e o Analista-W, todos os emissores são registrados em um procedimento formal para, após a aprovação do CISO, serem cadastrados no *firewall* da empesa, dando acesso exclusivamente ao ambiente dedicado à recepção de arquivos confidenciais.

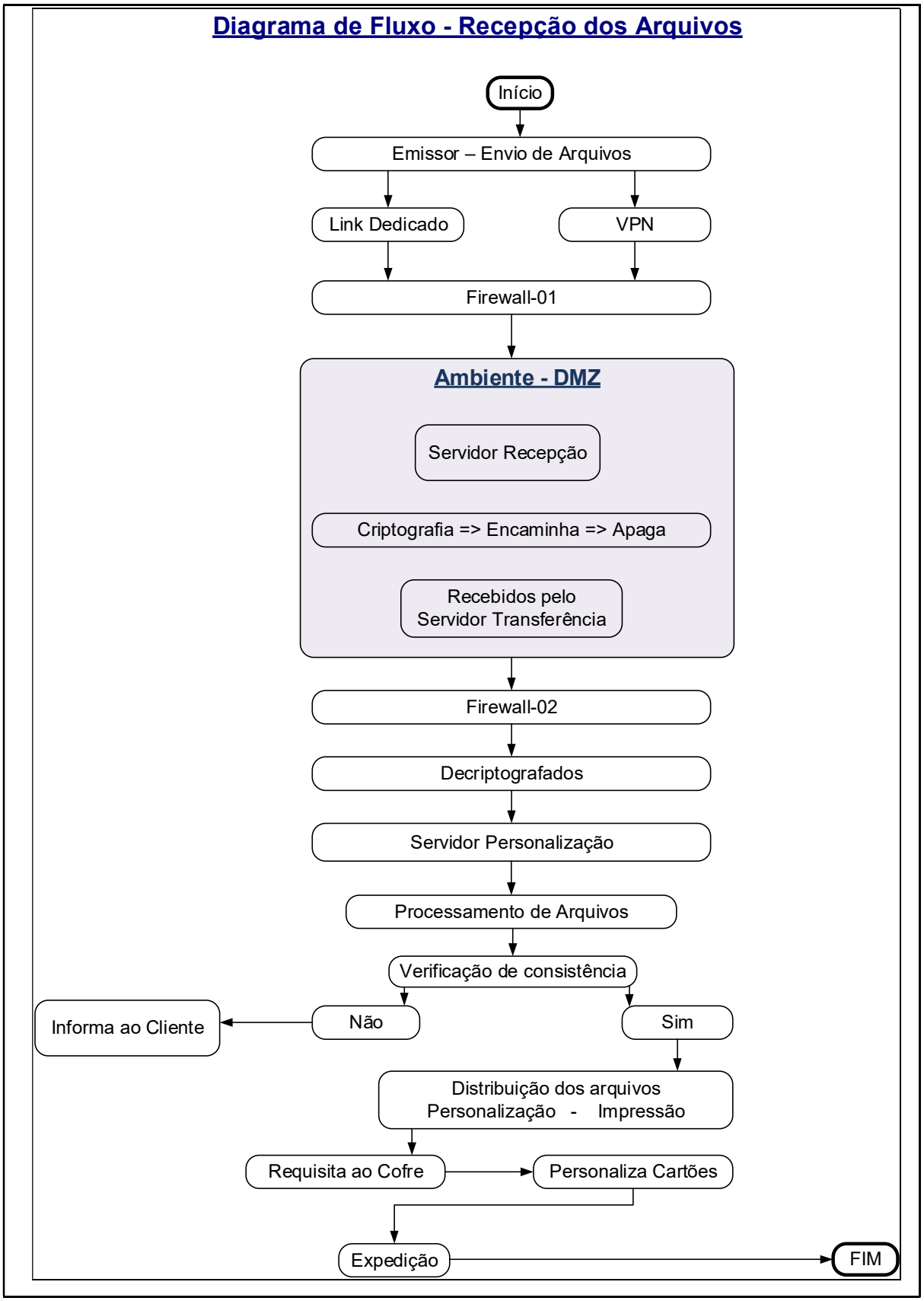

Figura 8 – Fluxo de recepção de arquivos
Fonte: Dados da pesquisa

A Figura 8 é um diagrama criado a partir de informações fornecidas pelos funcionários da empresa e através dos acompanhamentos testemunhados durante este estudo, ele elucida todo fluxo de recepção de arquivos ou dados que contém informações confidenciais dos portadores de cartões de pagamento. É focado na recepção dos arquivos originados dos emissores, a partir do momento em que são recebidos pelos servidores da personalizadora até a expedição do cartão já embossados.

Conforme descrito em entrevista realizada com CISO e corroborada pelo Analista-W, que lida diretamente com a recepção e o processamento de dados, todo o processo tem início no emissor ou cliente. os dados confidenciais são transmitidos por canais de link dedicado ou VPN através de um aplicativo destinado à transferência de informações sensíveis. Após as informações serem recebidas pelos servidores da DMZ, elas são criptografadas por um processo interno, apagadas e transmitidas a um segundo servidor, ainda dentro da DMZ (*Demilitarized Zone*), porém sem acesso externo. Esse procedimento é realizado para garantir a confidencialidade dos dados dentro da empresa. Depois de recebidos e cifrados, os dados ficam à disposição para serem requisitados pelo setor de processamento de dados. Assim que requisitados, eles são transferidos, apagados da origem, decifrados no destino e processados, para, então, dar continuidade nos processos de personalização dos cartões bandeirados. Todo fluxo é auditado, por *log* de aplicativos e as informações nunca ficam decifradas fora da HSA.

Durante a entrevista com o Coordenador-D, responsável pelo setor de personalização, foi afirmado que todas as informações disponibilizadas pelo setor de processamento de dados são automaticamente apagadas, assim que são coletadas pelas máquinas que realizam a personalização dos dados variáveis nos cartões de pagamento, no que tange aos arquivos destinados apenas ao setor de personalização e não aos arquivos enviados pelos clientes. O Coordenador-D enfatizou que os equipamentos que realizam a personalização são, por determinação do PCI, de uma empresa chamada DataCard, também certificada pelo PCI *Card Prodution.* Todos os equipamentos certificados pelo PCI são auditados ainda dentro da fábrica da DataCard e, durante os procedimentos de auditoria anual, dentro da personalizadora.

Não é recomendada a utilização de equipamentos não homologados pelo PCI. Esse procedimento visa garantir que o parque tecnológico de personalização está em conformidade com as normas de segurança exigidas pelas bandeiras, provendo rastreabilidade e correto descarte das informações utilizadas.

Um aspecto importante abordado nos processos de auditoria é quanto à rastreabilidade das informações processadas pelas personalizadoras. O PCI (2017) recomenda que os *logs* de auditoria devem conter pelo menos a identificação do usuário, o tipo de evento, o carimbo de data e hora, a origem do evento, a identificação de sucesso ou falha, os componentes ou o nome dos dados afetados ou manipulados e os níveis de privilégio de acesso.

Esse detalhamento do *log* de eventos precisa estar presente em todas as etapas que compreendem o tráfego de informações confidenciais em todos os aplicativos e softwares utilizados, em todos os servidores envolvidos no processo, em todo fluxo de dados de provisionamento do portador de cartão, desde o recebimento e processamento, até o fim de seu ciclo de vida (PCI, 2017).

De acordo com o Analista-M, responsável pelo *firewall*, e o Analista-R, responsável pelo setor de desenvolvimento das aplicações, todo o processo de auditoria dos registros de *log* é realizado sistematicamente. Qualquer informação trafegada dentro da empresa é registrada, principalmente dentro da área de alta segurança.

As personalizadoras têm a responsabilidade e o dever de restringir o acesso externo, garantindo a proteção das informações em todas as etapas do processamento, além de certificar-se de que todos os componentes que pertencem à rede de personalização estejam fisicamente dentro da HSA. O CISO deve garantir que as configurações de todos os componentes dos sistemas associados a transmissão, armazenamento e personalização de dados confidenciais sejam validadas mensalmente contra configurações não autorizadas (PCI, 2017).

Os impactos relativos à transmissão e ao monitoramento das informações sigilosas são, em sua maioria, processuais, ou seja, com baixo investimento em tecnologia, uma vez que a comunicação entre emissores e personalizadora precisa acontecer. A personalizadora precisa estar atenta e garantir a correta implementação desses meios de transmissão, contemplando todos os requisitos de segurança da informação que garantam a comunicação com os emissores.

Para que essa informação confidencial não seja recepcionada, cifrada, decifrada e processada por uma única pessoa na cadeia de processos, o PCI (2017) exige que a personalizada tenha um esquema de segregação de funções.

Durante a entrevista, o CISO foi questionado sobre a existência da segregação de funções dentro da empresa, requisito exigido pelo PCI, que visa garantir que uma mesma pessoa não realize mais de uma tarefa dentro do processo de personalização dos cartões de pagamento. Em resposta, o CISO afirmou que todas as etapas, desde a recepção até a finalização no setor de manuseio e expedição, são realizadas por profissionais e gestões diferentes.

O CISO detalhou o processo de recepção e mudança de responsabilidade da seguinte forma: o início se dá no setor de processamento, sob a gestão do Coordenador de TI, passando pelo setor de personalização, sob a gestão do Coordenador-D, e é finalizado no setor de manuseio e expedição, sob a Gestão do Coordenador-H. Esse procedimento atende o requisito de separação de funções, conforme recomendações do PCI (2017).

Foi demostrado durante a entrevista que todo o fluxo de informações que trafegam dentro da empresa é auditado e gravado em *log* de sistema. O Analista-M exibiu um dos arquivos de *log* retirado diretamente do servidor de recepção dos arquivos.

Este é um aspecto muito importante no que se refere à rastreabilidade das informações sigilosas dos portadores de cartões de pagamento. Durante o processo de auditoria anual realizado pelo auditor da *NCC Group* ficou clara a preocupação em verificar se os arquivos de *log* gerados em cada uma das etapas do processo de personalização dos cartões estão íntegros e contêm todo o detalhamento exigido pelo PCI.

Não foi identificado um conflito de informações fornecidas entre os profissionais que atuam na recepção, no processamento, na personalização e no desenvolvimento. Todos demostraram uma linha de conhecimento similar às informações que o CISO forneceu.

As adequações necessárias para prover os processos de geração de *log* de forma consistente são praticamente tecnológicas e envolvem a compra de servidores e sua correta configuração. O impacto da adoção dessa exigência na produtividade da empresa é nulo, uma vez que todo esse processo é transparente e não exige nenhuma intervenção humana para seu funcionamento, após configurado.

Há um impacto negativo, relativo à não adequação desse procedimento, levando-se em consideração três pontos bastante relevantes:

(1) O auditor, profissional responsável pelo processo de homologação das bandeiras, exige que esse requisito esteja consistente e validado em todos as auditorias. Para isso, ele solicita a disponibilização do arquivos de *log,* retirados diretamente nos servidores em datas aleatórias, visando certificar-se de que os arquivos estejam íntegros e detalhados.

(2) Caso haja um vazamento de informações sobre o portador de um cartão bandeirado, a trilha de auditoria gerada pelos arquivos *logs* de eventos é uma ferramenta essencial e indispensável para a rastreabilidade das informações.

(3) Caso um determinado banco solicite informações sobre o recebimento ou o processamento de um arquivo ou nome de um portador de cartão, o *log* de registros é a única forma que a personalizadora pode recorrer para apresentar as informações ao solicitante, uma vez que todos os dados do portador do cartão, após serem expedidos, são apagados.

4.2.2. Controle de acesso aos dados confidenciais

O controle de acesso aos dados confidenciais é de suma importância para as empresas que trabalham com dados sigilosos, uma vez que todos os procedimentos de personalização dos cartões de pagamento têm a premissa de preservar a confidencialidade e a integridade das informações recebidas e processadas dentro da HSA. O PCI (2017) deixa explícito que é primordial prevenir todo acesso físico e lógico das informações envolvidas no processo de personalização dos cartões de pagamento bandeirados.

Lento, Da Silva Fraga e Lung (2006) dizem que o controle de acesso é um serviço de segurança e tem como função gerenciar o acesso aos objetos dos sistemas computacionais, limitando as ações de um sujeito, restringindo o que ela pode executar em seu nome.

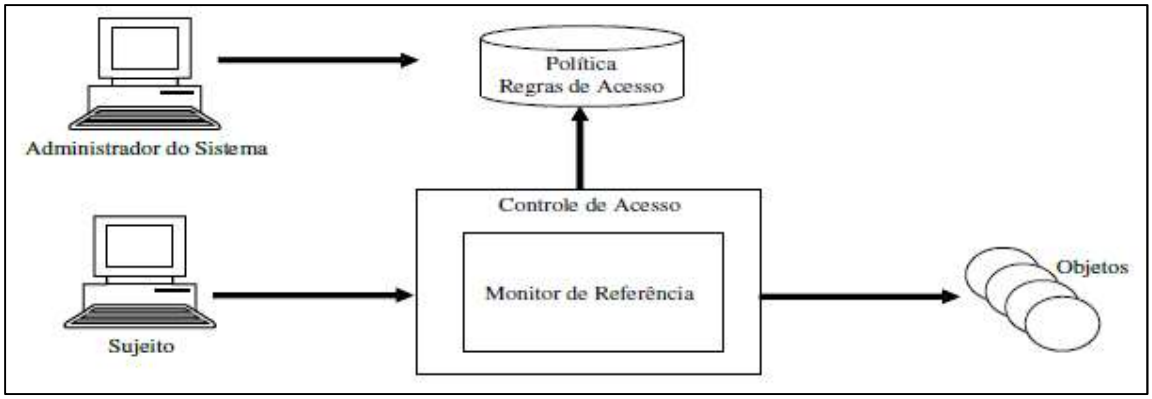

Figura 9 – Controle de acesso a objetos
Fonte: LENTO; DA SILVA FRAGA; LUNG, 2006, p. 5.

A Figura 9 ilustra como se dá o controle de acesso e permissão a um sujeito para acessar um determinado objeto, de acordo com a política de controle de acesso, gerenciada pelo administrador do sistema que monitora e controla quem e quais objetos esse sujeito pode acessar.

Durante a entrevista com o CISO e com os analistas, todos afirmaram que o controle de acesso à informação é gerenciado via sistema e reforçado através de políticas de grupo ou GPO (*Group Policy*). Essas políticas incluem a utilização de mídias de armazenamento externas.

De acordo com o PCI (2017), a empresa deve garantir a proteção das informações contra modificação e deleção não autorizada em qualquer parte do processo, garantindo o acesso às informações apenas por profissionais autorizados.

O CISO garantiu que está claro na política de segurança da informação, em um determinado capítulo que não foi indicado claramente, que há um tópico específico para tratar dos procedimentos de controle de acesso às informações confidenciais.

> Todas as informações confidenciais permanecem dentro da área de alta segurança e caso seja necessário o descarte de qualquer mídia ou dispositivo de armazenamento que pertença à HSA, este é destruído de forma definitiva, conforme ditado pelo PCI. O acesso às informações é monitorado pelos servidores e ninguém pode acessar qualquer informação que não esteja em seu escopo de trabalho (SUPERINTENDENTE-S - CISO).

De acordo com PCI (2017), qualquer mídia utilizada dentro da HSA deve ser destruída de forma definitiva, caso seja necessária sua remoção, em qualquer hipótese, para que as informações não possam mais ser recuperadas de maneira alguma. Esse procedimento de destruição de mídia deve ser acompanhado por, no mínimo, dois profissionais, em um procedimento formal e assinado pelos acompanhantes e pelo CISO.

O CISO informou que, caso haja a necessidade de destruir qualquer mídia de armazenamento que esteja dentro da HSA, é designado um profissional do setor de segurança da informação em conjunto com outro profissional do setor de auditoria interna para realizar o procedimento em conjunto, garantindo que todo esse processo seja registrado e assinado por todos os envolvidos em um documento denominado termo de destruição de mídias. Esse procedimento de destruição de mídias tem a finalidade de garantir que qualquer dispositivo de armazenamento que seja retirado da área de alta segurança seja destruído de forma definitiva, para que não haja qualquer suspeita de vazamento de informações confidenciais.

A entrada e, principalmente, a saída de qualquer dispositivo de armazenamento eletrônico, dentro da HSA, deve ser monitorada de perto. É de responsabilidade do CISO criar políticas claras de acesso à informação, incluindo a utilização de mídias de armazenamento digitais como quem entrou com a mídia, a justificativa para a entrada e para onde se destina a mídia.

A fuga de dados sigilosos através de mídias de armazenamento removíveis é um ponto sensível e que precisar ser levado em consideração com bastante rigor. O impacto do furto de informações tem grande relevância na imagem da empresa.

O PCI (2017) destaca que caso haja qualquer suspeita de comprometimento dos dados confidenciais ou secretos, os clientes e emissores impactados devem ser informados por escrito em um prazo de vinte e quatro horas. As incidências confirmadas devem ser comunicadas imediatamente aos impactados, juntamente com os procedimentos de aplicação das leis vigentes.

O Coordenador-D, os analistas de TI e o Coordenador-H confirmaram que qualquer suspeita de comprometimento ou vazamento de informações confidenciais é imediatamente comunicada ao CISO formalmente.

O CISO afirmou que, no caso de suspeita de comprometimento de informações sensíveis, o plano de comunicação é iniciado imediatamente, dando conhecimento à equipe interna de tecnologia e ao Diretor-C. Todas as áreas envolvidas são comunicadas, e o procedimento de averiguação e análise do ocorrido é imediatamente iniciado.

O PCI (2017) exige que todos os indícios de irregularidade que envolvam o comprometimento de dados sensíveis sejam preservados para subsidiar evidências futuras durante a apuração das investigações e todas as leis cabíveis sejam aplicadas aos responsáveis pelo vazamento.

Conforme informações fornecidas pelo Analista-W e pelo Analista-M, as evidências, quando identificado qualquer incidente envolvendo os dados confidenciais, são preservadas e o CISO imediatamente informado.

Todos os procedimentos que envolvem a tratativa de informações confidenciais devem ser considerados como críticos em uma empresa personalizadora de cartões de pagamento, uma vez que o cerne da empresa é lidar com informações sigilosas, e os requisitos de segurança de tecnologia como confidencialidade e integridade são a base para garantir que nenhuma informação está sendo divulgada publicamente.

Os impactos relativos ao vazamento de informações confidenciais refletem diretamente na imagem da empresa de forma extremamente negativa, como reforçado na entrevista realizada com Diretor-C.

O PCI reforça a importância da confidencialidade dos dados dos portadores de cartões de pagamento bandeirados em vários trechos de seu manual de procedimentos. Conforme afirmado pelo CISO, pelo Coordenador-D e pelo Coordenador-H, os procedimentos descritos na política de segurança da informação para tratativa das informações confidenciais burocratizam os processos produtivos, podendo, em alguns momentos, atrasar o fluxo de produção e a personalização de cartões, porém são necessários e até mesmo imprescindíveis para garantir os requisitos de segurança e rastreabilidade.

Conforme o Analista-M, a segurança nos acessos aos dados confidenciais é provida através de um servidor que provê o serviço com protocolo LDAP (*Lightweight Directory Access Protocol*), no qual todos os grupos de acesso são cadastrados e gerenciados, concedendo permissão exclusivamente ao que é necessário para o desempenho das funções. O CISO não soube afirmar quais grupos têm acesso direto aos diretórios contendo dados confidenciais, mas garantiu que apenas os profissionais que lidam diretamente com a personalização têm esse acesso.

Listar os grupos, determinar o nível de acesso de cada grupo, monitorar e validar os acessos pelo menos trimestralmente seria uma boa prática para garantir a confidencialidade das informações. O PCI (2017) recomenda que a validação das permissões de acesso seja feita trimestralmente. Esse procedimento minimiza a probabilidade de um acesso indevido.

4.3. Segurança da rede de dados

No Capítulo 5 do PCI (2017), estão descritos os requisitos de segurança de rede que devem ser adotados pelas empresas personalizadoras de cartões de pagamento bandeirados. Os principais tópicos abordados são:

- Topologia e diagrama da rede física.
- Criação de uma rede destinada â recepção dos arquivos enviados pelos emissores, denominada DMZ (*demilitarized zone*) e a criação de uma rede destinada à personalização de cartões, ambas totalmente separadas por *firewall*.

- Registro e controle de todos os dispositivos de rede como roteadores e dispositivos de armazenamento que pertençam a uma das redes de personalização e DMZ.
- Aquisição e configuração de pelo menos dois *firewalls* dedicados e destinados a regular o tráfego, tanto de origem interna quanto de origem externa, impedindo o vazamento de informações a pessoas não autorizadas.
- Aquisição e configuração de sistemas de antivírus coorporativo com atualização diária, emissão de alertas e que abranja todos os sistemas operacionais utilizados dentro da empresa.

> A segurança em redes é definida como proteção das redes e dos serviços por ela prestados contra modificação sem autorização, destruição ou revelação, garantindo-se a execução das suas funções críticas corretamente sem a ocorrência de efeitos colaterais prejudiciais.
> [...] A ameaça à integridade é a adulteração das informações e a ameaça à disponibilidade consubstancia-se na recusa ao atendimento de uma solicitação legítima da informação, comumente caracteriza pela negativa na prestação de um serviço de rede (MEDEIROS, 2005, p. 7).

O PCI (2017) recomenda a criação de um diagrama que reflita resumidamente como é realizada a comunicação entre as personalizadoras e os emissores ou bancos.

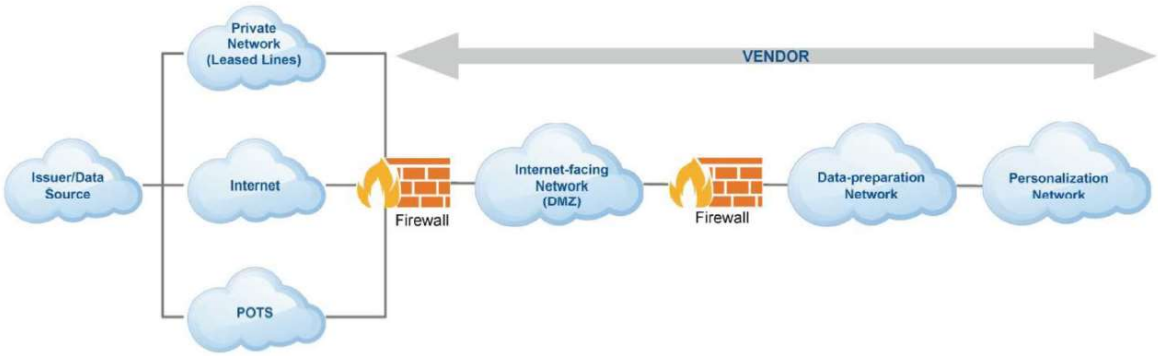

Figura 10 – Diagrama padrão para rede de personalização
Fonte: PCI, 2017, p. 11.

A Figura 10 é exemplo de um diagrama de redes fornecido no próprio manual do PCI *Card Prodution*, no qual pode ser identificada claramente a segregação entre as redes de maneira física, utilizando aparelhos de *firewall* coorporativo para separar os ambientes externos, denominados *Issuer/Data Source,* da rede DMZ e um segundo aparelho de *firewall* destinado à segregação das redes de *Data-preparation e personalização.*

Conforme Nakamura (2007), o estabelecimento de uma DMZ é essencial para proteção da rede interna; seu propósito é isolar os servidores que proveem serviços externos dos servidores que ficam localizados dentro da rede interna, ou seja, os acessos externos ficam confinados nessa rede desmilitarizada.

Essa separação é complexa, por isso deve ser analisada e realizada seguindo os critérios recomendados pelo PCI por um profissional com conhecimento em segurança de redes, formação e capacitação para essa atividade. Nakamura (2007) corrobora que a implantação de um ambiente cooperativo eficiente é complexa, e a segurança necessária a ser implementada é igualmente complexa.

Este é um dos pontos mais abordados durante o processo de auditoria anual realizado pelas bandeiras. Durante a entrevista com o auditor Steve, ele deixou clara a importância em se ter um diagrama de rede atualizado, ressaltando que grande parte do processo de auditoria é conduzido de acordo com as informações que constam nesse diagrama. Se houver uma grande quantidade de dúvidas ou informações inconsistentes, o processo de auditoria será bem mais apurado.

Durante a entrevista realizada com CISO, ficou clara a importância de manter o diagrama de rede atualizado. O CISO afirmou que o auditor se embasa nesse diagrama para fazer suas análises e observações iniciais a respeito dos requisitos de segurança relativos à transmissão de arquivos.

> Mantemos o diagrama sempre atualizado e assinado por mim e pelo Analista de segurança da informação. É a partir desse diagrama que o auditor da Visa e Master faz a análise do ambiente; se houver algo que ele não entende ou concorda ele, começa a questionar. Buscamos assegurar que esteja tudo em conformidade para que a auditoria transcorra normalmente (SUPERINTENDENTE-S - CISO).

Oliveira (2015) argumenta que nas organizações a informação e os sistemas de informação estão envolvidos em vários tipos de riscos em resultado designadamente do crescente nível de complexidade como, por exemplo, a ligação a redes externas cada vez mais sofisticadas. O desenho de um diagrama que transpareça a realidade da rede de dados da empresa auxilia diretamente os analistas de segurança da informação na formatação de soluções e na mitigação de vulnerabilidades advindas de um possível erro da estrutura da topologia lógica da rede.

É recomendado que o diagrama esteja sempre atualizado, revisado e assinado por um profissional competente e capacitado, capaz de compreender, julgar e criticar pontos que considerar relevantes no que diz respeito a vulnerabilidades que podem afetar a rede de alta segurança da empresa. Em uma personalizadora, essa incumbência cabe ao CISO.

O Analista-M, responsável pelos *firewalls* da personalizadora, garantiu que o diagrama é atualizado periodicamente ou caso haja qualquer modificação significativa na topologia de rede. De acordo com o analista, o diagrama é apenas um esboço da topologia de rede, e a compreensão da estrutura de rede interna leva em conta outros aspectos de rede LAN (*Local Area Networks*) e segurança que não estão explícitos no diagrama.

Quando questionado sobre o processo de auditoria anual e a colocação feita pelo CISO sobre as observações do auditor, no que tange à observância do diagrama para conduzir o processo de auditoria, o Analista-M afirmou que, por experiência pessoal, alguns auditores focam na estrutura de rede e em seus requisitos de segurança, outros focam em processos e no fluxo de recebimento das informações.

O Analista-M deixou claro seu descontentamento com a subjetividade dos auditores durante a interpretação do diagrama de rede.

> O auditor fala o que acha ser correto. Já passamos por auditores que realmente compreendem as regras de segurança, como as regras de firewall, NAT, filtros de conteúdo, IPS/IDS, mas a maioria não tem conhecimento suficiente para analisar e essa falta de conhecimento leva o auditor a fazer perguntas sem sentindo e fazer apontamento de não conformidades que são meramente interpretativos. Muitas vezes temos que mostrar o firewall fisicamente para que ele entenda que não existem V-Lans na empresa e, mesmo assim, continuam questionando sobre a existência delas (ANALISTA-M).

O PCI deixa de mencionar ou deixa de ser objetivo em suas colocações em vários aspectos, faltando clareza, que deixa margem para subjetividade.

Os aparelhos de *firewalls* são essenciais para a empresa, uma vez que através deles é feita a segregação das redes de alta segurança.

O PCI (2017) não considera o método de criação de VLANS (*Virtual Local Area Networks*) como segregação de redes. Essa separação deve ser realizada por *firewalls* físicos. Nakamura (2007) corrobora essa informação, afirmando que VLANS não podem ser considerados mecanismos de segurança como segmentação de redes, uma vez que é possível que quadros injetados em uma VLAN sejam direcionados a outras VLANS.

Seguindo tal recomendação, as personalizadoras precisam se adequar e realizar a segregação, utilizando dispositivos de *firewall* dedicados. A documentação relativa à configuração dos *firewalls* é um procedimento que auxilia na comprovação da segregação das

redes e deixa mais explícito o fluxo de recepção das informações sigilosas aos auditores das bandeiras.

O Analista-M garantiu que todas as redes são segregadas por *firewall* e não existe qualquer VLAN dentro da personalizadora, porém ele informou que não existe um documento formal com a configuração inicial para ser confrontado com a configuração atual dos *firewalls*.

Para o PCI (2017), os *firewalls* têm como função primordial segregar fisicamente e proteger as redes localizadas dentro da HSA (*High Security Area*), denominadas *Data-preparation* e personalização.

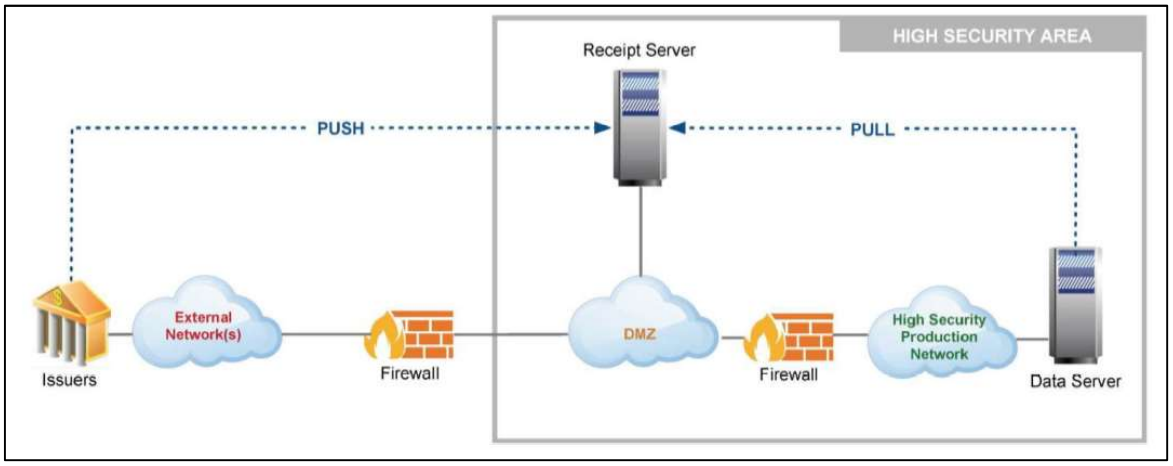

Figura 11 – Diagrama de *firewall*
Fonte: PCI, 2017, p. 12.

A Figura 11 é um diagrama que exemplifica a maneira recomendada de posicionamento dos *firewalls* para garantir a separação correta entre a área de alta segurança (*HSA – High Security Area*) e as demais redes da corporação. Há uma preocupação especial em garantir a separação física, também por *firewall*, entre a rede DMZ e as redes dentro da HSA.

Al-Shaer e Hamed (2004) afirmam que o *firewall* é a defesa de fronteira adotada pelas empresas, atuando como um filtro de rede do tráfego não autorizado em direção à rede segura.

Garantir a separação física da rede de personalização é essencial para manter os níveis adequados de segurança dos dados confidenciais. As restrições de acesso externo e a liberação apenas de serviços e portas indispensáveis para realização das atividades diárias são essenciais para o controle de tráfego nas redes de alta segurança. Esse é um requisito essencial para garantir a confidencialidade e a integridade das informações secretas.

Conforme o Analista-M, responsável pelo gerenciamento dos *firewalls* da personalizadora, esses equipamentos estão configurados para emitir alertas enviando e-mails a coordenação de TI e a ele, contendo informações sobre os incidentes mais relevantes como os

eventos de IPS (*Intrusion Prevention System*), as tentativas de *login* nos equipamentos de *firewall* que não são autorizados e as possíveis ameaças de vírus detectados na camada de rede do modelo OSI.

Nakamura (2007) destaca o *firewall* como um dos principais e mais conhecidos componentes de segurança dentro de um sistema de segurança da informação, a partir do qual é possível controlar e autenticar o tráfego, além de registrar através de *logs* todo tráfego da rede.

Manter um documento formal, atualizado trimestralmente com assinatura do CISO, contendo todas as regras de todos os *firewalls* com a respectiva justificativa para tais regras é uma prática recomenda pelo PCI (2017).

De acordo com o Analista-M, os *firewalls* foram implementados incialmente por uma terceirizada que não documentou os processos de criação de regras. O CISO corrobora as argumentações do Analista-M e também não soube dizer o motivo pelo qual as regras dos *firewalls* não foram documentadas durante a implantação.

Essa falta de controle relativa às regras do *firewall* não são benéficas para a empresa, uma vez que esses dispositivos são muito sensíveis e responsáveis por toda segurança de informação no perímetro da empresa. Alterações realizadas sem análise e aprovação do CISO podem trazer sérias consequências para a empresa.

Conforme o CISO, as alterações nas regras dos *firewalls* são solicitadas via ordem de serviço. Após recebida e classificada, a solicitação gera um formulário próprio para alteração de *firewall*, destinado à aprovação do CISO. Esse formulário contém o detalhamento de todas as modificações propostas e suas justificativas para serem aprovadas e liberadas.

De acordo com PCI (2017), o acesso ao *firewall* deve ser restrito a apenas profissionais autorizados e designados pelo CISO para essa função. Nenhum outro profissional, mesmo que seja da equipe de tecnologia, deve ter acesso físico ou às configurações dos *firewalls*.

Uma típica empresa em grande escala pode envolver centenas de regras de *firewall* que podem ser escritas por diferentes administradores em vários momentos. Isso implica em um aumento no potencial de ocorrência de anomalia na política de segurança do *firewall*, colocando em risco a segurança da rede protegida (AL-SHAER; HAMED, 2004).

Durante o processo de auditoria das bandeiras, normalmente os auditores solicitam os documentos contendo as informações de configuração inicial e atual vigente no *firewall*. A partir dessa comparação, o auditor emite seu parecer (CISO).

Este é um ponto que pode culminar em uma não conformidade de difícil solução, uma vez que não existe um documento que deveria ter sido gerado inicialmente. Conforme o

CISO, neste caso, o auditor abre um debate, pede esclarecimentos e propõe um plano de ação para resolver a não conformidade.

Fica claro que a subjetividade do auditor é um fator preponderante durante o processo de auditoria, já que o PCI não cobre essas lacunas ou não contém propostas consistentes para a solução de não conformidades.

Os investimentos necessários para a segregação física às redes de uma personalizadora ficam a cargo da aquisição de aparelhos destinados aos *firewalls* corporativos e da contratação de mão de obra especializada.

A administração desses aparelhos de *firewall* precisa ser realizada por um profissional bem capacitado e com formação acadêmica. Os impactos negativos que podem ser gerados pelo conforto de uma falsa proteção irão comprometer muito a segurança tecnológica.

Todas as regras dos *firewalls* precisam estar justificadas, e toda justificativa precisa ser ponderada e aprovada pelo CISO. O documento contendo as informações de configuração de regras precisa ser analisado com cuidado por um profissional competente.

O PCI (2017) deixa claro que o ambiente de rede de dados de uma personalizadora deve ser cuidadosamente analisado, visando o completo isolamento da rede de alta segurança em que se encontra a rede de personalização de cartões de pagamento bandeirados.

Conforme conversa com o auditor Steve, a segregação de redes é um ponto culminante para iniciar o processo de auditoria; se não for constatado esse procedimento, a auditoria não terá início.

A política de segurança da informação precisa contemplar todas as normas e todos os procedimentos no que diz respeito ao acesso físico e lógico aos *firewalls* da empresa, ao detalhamento dos procedimentos de alteração de regras dos *firewalls* e a como deverá ser feito o fluxo de aprovação das modificações propostas, bem como as medidas a serem tomadas caso seja identificada qualquer modificação não aprovada.

Nakamura (2007) afirma que um *firewall* é tão seguro quanto a política de segurança que ele suporta.

O PCI (2017) traz uma série de recomendações sobre os *firewalls*, como, por exemplo, o acesso individualizado aos equipamentos, a aquisição de equipamentos dedicados e exclusivos à função de *firewalls*, a implementação de mecanismos que garantam a não violação das configurações e que mantenham a integridade dos *firewalls* e a criação de um documento formal para a autorização explícita do tráfego de entrada e saída através dos *firewalls*, negando qualquer outro tráfego através desses dispositivos.

Esses equipamentos de *firewall* têm grande relevância na política de segurança da informação. Conforme afirmado pelo CISO, os auditores não começam o processo de auditoria, caso não seja identificada a utilização de pelo menos dois *firewalls* separando a rede de personalização da internet.

Os impactos da não utilização dos *firewalls* para criação de uma DMZ, conforme as orientações do PCI (2017), refletem diretamente no processo de homologação para produção dos cartões.

A criação de um ambiente denominado DMZ, destinado exclusivamente ao acesso dos emissores para o envio de dados relativos aos portadores de cartões, desde que previamente cadastrados e autorizados formalmente pela personalizadora, devem levar em conta todos os aspectos de segurança lógica exigidos pelo PCI e constantes na política de segurança da informação.

Sistemas e tecnologias como *intrusion prevention system* e *intrusion detection system*, conversão de endereçamentos via *network address translation*, antivírus em camada três do modelo OSI (*Open Systems Interconnection*), entre outros, precisam ser implementados e monitorados rotineiramente (PCI, 2017).

O modelo OSI, conforme Pinheiro (2004), é a base para a implantação de qualquer tipo de rede de dados; a camada três ou camada de rede tem a função de controlar as operações de rede, roteando os pacotes e contabilizando o tráfego em números de bytes.

No *site* da SonicWall, uma empresa de segurança e fabricante de dispositivos *firewalls*, em sua *website* acessada pelo endereço www.sonicwall.com/br-pt/products/sonicwall-enforced-anti-virus, é esclarecido que a tecnologia de antivírus capaz de atuar na camada três do modelo OSI garante um nível de proteção avançada, agindo antes de o pacote chegar ao perímetro de rede local. Todos esses aspectos garantem que a criação de um ambiente de DMZ seja feita de forma gerenciada, segura e aprovada pelo PCI.

A DMZ tem o propósito de ser um ambiente destinado à comunicação externa, porém, no caso específico das personalizadoras, esse ambiente é destinado à comunicação com os emissores e não com a *web*, uma vez que a rede de personalização não pode ter qualquer contato com redes externas (PCI, 2017). Essa é uma peculiaridade da DMZ nas personalizadoras de cartões de pagamento bandeirados.

Temponi (2010) enfatiza que os cuidados que devem ser considerados no que tange ao controle de segurança de rede precisam enfatizar que uma invasão ou a concessão de acesso a terceiros pode levar à divulgação de boa parte de informações privilegiadas multiplicando os riscos relativos a confidencialidade, integridade e disponibilidade da informação.

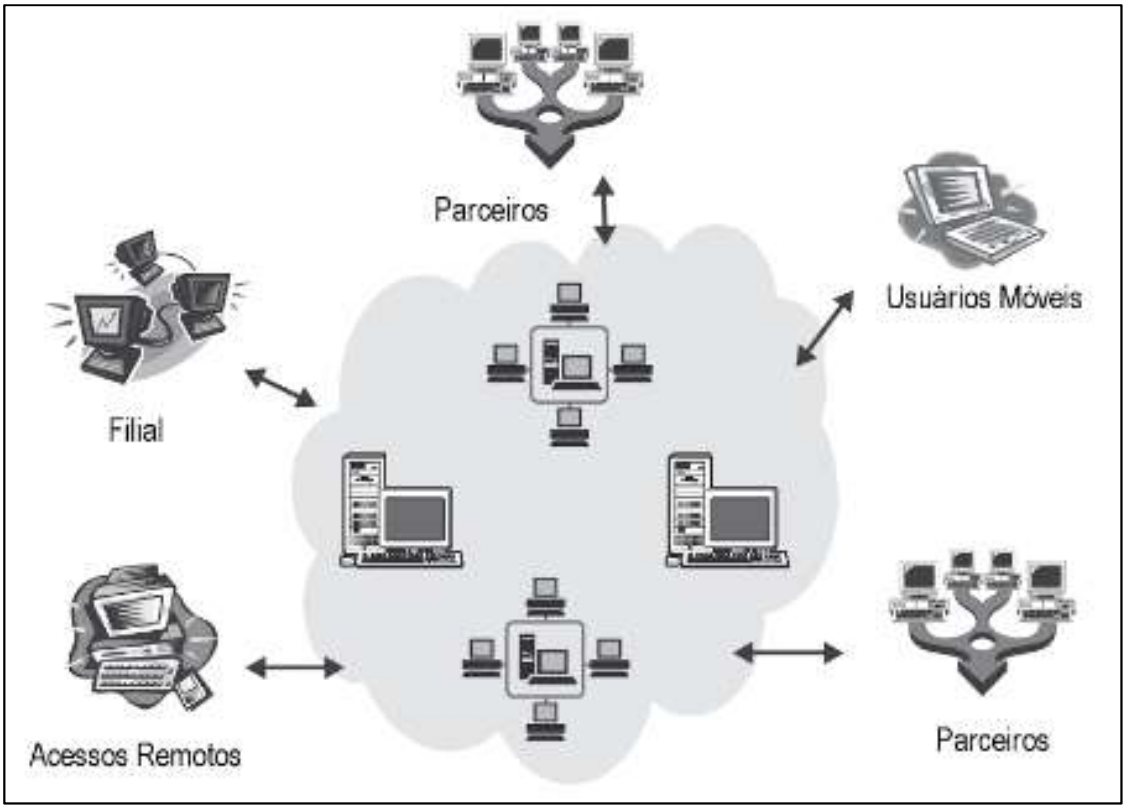

Figura 12 – Ambiente cooperativo – Diversidade de conexões
Fonte: NAKAMURA, 2007.

Conforme exemplificado na Figura 12, em uma rede interna, existe a cooperação entre diversos tipos de parceiros e usuários que, embora proporcione velocidade e eficiência de processos, também trazem riscos que precisam ser mitigados através da segregação das redes.

Conforme o Analista-W, responsável pela recepção e pelo processamento dos arquivos provenientes dos emissores, esses arquivos são recebidos em um ambiente totalmente apartado da rede administrativa.

> Todo o processo de recebimento dos arquivos enviados pelos clientes acontece dentro da rede de DMZ.
> Os profissionais que têm acesso a essa rede são exclusivamente da equipe de tecnologia da informação, e cada cliente tem um ambiente separado e um aplicativo destinado à recepção dos arquivos sigilosos, como, por exemplo, o IMB-ConnectDirect (ANALISTA-W).

Oliveira (2015) aponta que as características de segurança de uma rede corporativa devem levar em consideração os seguintes aspectos: ser de responsabilidade do departamento de tecnologia da informação, não permitir a ligação de modens a qualquer computador sem avaliação prévia e aprovação do CISO, serem utilizado apenas aplicativos autorizados, ter um procedimento disciplinar junto ao departamento de recursos humanos para disciplinar quem

viole as regras estabelecidas na política de segurança da informação, ter um plano de contingência para situações de emergência, serem realizadas auditorias anuais internas com plano de ação corretiva para as não conformidades identificadas.

Fica evidente a necessidade de que a política de segurança da informação descreva as regras, de maneira bem clara, quanto à concessão de acessos tanto físicos quanto lógicos, e o processo de autorização para instalação de aplicativos em qualquer ambiente da empresa, principalmente aqueles que lidam diretamente com dados sigilosos.

Conforme Marciano (2006), com a ampla utilização da rede mundial de computadores, os problemas se multiplicaram de forma avassaladora. As empresas precisam criar métodos e procedimentos para se adequar a essa crescente utilização.

O PCI (2017) exige a instalação e configuração de um sistema de antivírus corporativo com atualizações automáticas e que garanta a proteção em toda rede de alta segurança. Os analistas de segurança da informação que atuam em uma personalizadora devem ficar atentos aos cuidados em relação à comunicação externa e entre as redes da empresa. A rede de personalização e a DMZ precisam ter acesso restrito e não é permitido qualquer acesso direto à internet, mesmo com a finalidade de atualização dos pacotes de segurança.

O Analista-W, responsável pelo sistema de antivírus, afirmou que o aplicativo adquirido pela empresa está sempre atualizado e é auditado semanalmente.

Conforme Medeiros (2005), os vírus atuam modificando ou substituindo um outro arquivo executável, sendo capazes de alterar até o setor de inicialização do sistema operacional dos computadores. Uma vez ativo, o vírus passa a propagar-se através de uma rede local.

A ação de um vírus em uma rede de personalização é extremamente danosa, uma vez que nessa rede trafega uma grande quantidade de informações confidenciais.

O s*oftware* antivírus é o responsável pela detecção, identificação e possível remoção do código malicioso, podendo utilizar métodos heurísticos para identificar comportamentos suspeitos e disparando ações defensivas a fim de evitar que alguma ação danosa seja realizada no sistema (MEDEIROS, 2005).

A eleição de um aplicativo de antivírus robusto, administrado por um profissional capacitado, é de vital importância para que uma rede classificada como sensível permaneça íntegra. Um sistema de antivírus que permita a atualização via rede local, utilizando um servidor como repositório, é, sem dúvida, a melhor solução para uma rede sem acesso externo ou à internet.

Sem atualização, o *software de antivírus* torna-se ineficiente na detecção e no tratamento dos códigos maliciosos (MEDEIROS, 2005).

De acordo com o Analista-W, o antivírus implementado na personalizadora é robusto e possui todas as tecnologias exigidas pelo PCI como, por exemplo, antivírus, *antispyware*, NIDS (*Network Intrusion Detection System*), detecção de computadores ou máquinas sem antivírus, alertas de emergência e controle de dispositivos.

O PCI (2017) recomenda que mensalmente seja reportado ao CISO e à diretoria, todos os eventos relativos à segurança de rede da empresa. O Analista-W não confirmou a geração de relatórios para serem encaminhados ao CISO a respeito de alertas de incidência de vírus e outros.

Esse envio de relatórios periódicos ao CISO é uma prática recomendada e importante para dar ciência ao responsável pela segurança de rede da empresa.

Toda adequação da estrutura física da rede de dados tem um impacto considerável nos requisitos de segurança da informação. A não implementação desses requisitos, como criação de uma DMZ, aquisição de dispositivos de *firewalls* coorporativos e aquisição e implementação de um sistema de antivírus coorporativo e robusto criam pontos de vulnerabilidades consideráveis, principalmente em uma rede de alta segurança. O PCI (2017) exige e audita a implementação de tais tecnologias.

O impacto da adequação desses processos pode ser descrito de três maneiras:

- Nos investimentos em equipamentos, softwares, adequações físicas e contratação de mão de obra especializada, que pode ter um reflexo financeiro negativo, no que tange aos gastos desprendidos, e um reflexo financeiro positivo, no que tange à segurança das informações e mitigação dos furtos ou fraudes.
- Na produtividade da empresa, que pode ser considerada irrisória, levando-se em conta que essas adequações são transparentes aos profissionais que lidam diretamente na linha de produção.
- Sobre a imagem da empresa, uma vez que são requisitos exigidos durante o processo de auditora para homologação junto às bandeiras e extremamente necessárias para prover níveis adequados de segurança.

O não cumprimento dessas adequações pode acarretar, com toda certeza, na perda da homologação para produção de cartões bandeirados ou na não homologação para personalização dos cartões.

4.3.1. Segurança dos sistemas

A segurança dos sistemas consiste em uma série de exigências ligadas à gestão de aplicativos e sua liberação ou disponibilização para rede de personalização e para rede de DMZ. O PCI (2017) deixa explícito que qualquer sistema utilizado no processo de personalização de cartões deve ser usado somente para essa finalidade, e todo processo de desenvolvimento e liberação para o ambiente de produção, na rede de personalização e DMZ, deve ser documentado e validado.

Buscando cumprir essa exigência relativa à documentação de aplicativos desenvolvidos internamente e para auxiliar nos processos de desenvolvimento e documentação de *softwares* desenvolvidos dentro da empresa e que se destinam aos ambientes de personalização e recepção de arquivos é recomendada a utilização de aplicativos que auxiliem na geração automática de documentação a partir dos códigos fonte.

É importante para a equipe de desenvolvimento de aplicativos internos direcionados às redes de personalização e DMZ a adoção de aplicativo controlador de versão. Essa ferramenta auxilia diretamente no controle gradativo das modificações realizadas diretamente nos códigos fonte pela equipe de desenvolvimento, datando e mantendo um histórico de modificações e atualização de aplicativos.

Essas ferramentas são essenciais para o gerenciamento e acompanhamento dos processos de desenvolvimento que são gerenciados pelo CISO. Os impactos relativos à aquisição de aplicativos para esse tipo de gerenciamento são irrelevantes; no que tange às questões financeiras, muitos aplicativos com essa finalidade podem ser encontrados gratuitamente ou com preço muito baixo. No que diz respeito à adequação tecnológica e mão de obra, o impacto também é irrisório; por serem de fácil implementação e utilização, não há a necessidade de aquisições de grande ou médio porte para viabilizar esses recursos. Os impactos na produtividade podem ser considerados altos, uma vez que a liberação de uma versão com problemas e sem um plano de *roolback* definido e documentado, pode acarretar em atrasos e erros na produção, refletindo diretamente no cliente ou no SLA (*Service Level Agreement*) da empresa.

O Analista-R, responsável pelo setor de desenvolvimento de aplicativos da personalizadora, deixou claro que todos os procedimentos relativos a documentação e controle de versão são realizados e acompanhados de perto por ele mesmo e pelo coordenador de TI. Todos os profissionais ligados ao setor de desenvolvimento estão cientes dessas obrigações. Porém, o Analista-R não soube apontar como são feitos o treinamento e a conscientização dos profissionais de desenvolvimento após serem admitidos.

O CISO não soube responder às perguntas sobre o controle de aplicativos desenvolvidos internamente como, por exemplo, o controle de versão e a geração de documentação relativa ao desenvolvimento. Ele não se sentiu confortável para falar sobre o assunto e, por essa questão, encerramos este assunto.

É importante para a organização manter um plano de treinamento direcionado aos profissionais de desenvolvimento, conscientizando-os sobre as políticas de segurança, no que tange ao desenvolvimento de aplicações de maneira segura, informando aos novos funcionários sobre os principais aplicativos que são utilizados na gestão de desenvolvimento e a maneira com que são utilizados.

O PCI (2017) exige que todos os aplicativos desenvolvidos internamente sejam capazes de gerar *logs* de auditoria dos processos ou tarefas realizadas, bem como ter uma rigorosa política de controle de acesso por usuário, exigindo as credenciais de acesso sempre

que forem iniciados ou reiniciados. Os aplicativos utilizados dentro da rede de personalização devem garantir que o PAN nunca seja exibido por completo durante qualquer etapa da personalização ou manuseio de cartões, como maneira de garantir o sigilo dessa informação em qualquer etapa da produção.

O Analista-R garantiu que todos os aspectos de segurança, como a exibição do PAN e o acesso aos códigos-fonte, estão de acordo com as regras determinas no PCI e concomitante com a política de segurança da informação. O CISO corroborou as afirmações do Analista-R e garantiu que todo o processo de desenvolvimento obedece aos critérios de geração de *logs*, conforme solicitado pelo PCI, e que nenhum profissional da área de desenvolvimento instala ou implementa diretamente qualquer aplicativo ou atualização de aplicativos no ambiente de produção. Conforme o CISO, existe um procedimento de transferência de responsabilidade que é encaminhado à equipe de segurança da informação que irá proceder com a instalação ou atualização de aplicativos no ambiente de produção.

De acordo com PCI (2017), os procedimentos de atualização dos aplicativos utilizados dentro da rede de personalização devem ser bem definidos e documentados. Esses procedimentos visam garantir que as correções de falhas e as atualizações de segurança sejam corretamente implementadas e autorizadas formalmente pelo CISO, antes de serem liberadas.

O Analista-R afirmou que existe um procedimento de transferência de responsabilidade, no qual um aplicativo criado ou atualizado é disponibilizado à equipe de segurança da informação para ser analisado e transferido para o ambiente de produção. Este documento é assinado pelo analista desenvolvedor, pelo supervisor de desenvolvimento e pelo analista de segurança que irá realizar a transferência do aplicativo para o ambiente de produção.

O nível de detalhamento do procedimento de desenvolvimento e liberação dos aplicativos desenvolvidos internamente, direcionados ao ambiente de recepção e produção, ficou a cargo do Analista-R. O CISO não foi capaz de fazer algumas afirmações ou ditar alguns procedimentos.

A sinergia entre as equipes de tecnologia e o gestor de tecnologia e segurança da informação é de suma importância para que a política de segurança da informação seja consistente e corretamente obedecida. O não conhecimento de algum processo implica em um processo não documentado ou falho, e os impactos na segurança da informação podem ser altos. O CISO precisa conhecer todos os processos, incluindo o desenvolvimento, para que as políticas direcionadas a esse setor sejam adequadas e façam cumprir os requisitos mínimos de segurança da informação.

Outro ponto apontado pelo PCI (2017) exige que todos os aplicativos desenvolvidos internamente ou adquiridos de terceiros sejam testados fora do ambiente de produção, a fim de garantir que suas funcionalidades não irão prejudicar ou impactar negativamente o processo produtivo.

O Analista-R afirmou que existe um ambiente virtualizado, denominado Ambiente de Homologação para atender a esta exigência do PCI. De acordo com o analista, este ambiente foi criado para simular o ambiente de produção; nele são aplicados todos os pacotes de correção e testes de entrada e saída dos sistemas desenvolvidos internamente. Todo erro é corrigido, e somente após ser analisado neste ambiente, o aplicativo é liberado para produção.

De acordo com Analista-R, todo esse procedimento consta na política de segurança da informação. O Coordenador-H corroborou as informações relativas ao Ambiente de Homologação; ele foi claro ao afirmar que os aplicativos são testados e acompanhados por um de seus profissionais, ligados diretamente à produção, para, após validados, serem direcionados a fábrica.

Os impactos advindos da adoção de uma metodologia de desenvolvimento de softwares e aplicativos seguros são, em sua maior parte, positivos, uma vez que os aplicativos destinados à manipulação de dados confidenciais precisam ser gerenciados e ter ferramentas de controle que auxiliem no apontamento de uma não conformidade, no que tange à segurança da informação.

Os impactos financeiros são mínimos, uma vez que tais ferramentas de controle podem ser adquiridas gratuitamente.

Os impactos ligados à produtividade são sempre positivos, uma vez que esses *softwares* desenvolvidos pela equipe interna são personalizados e direcionados a atender as necessidades da empresa, propiciando a otimização de recursos, a agilização de processos internos e a geração de relatórios para acompanhamento de produção. As melhorias nos níveis assertividade das tarefas realizadas na produção e os recursos tecnológicos, como geração de relatórios gerenciais e alertas de erros, auxiliam muito os gestores ligados à produção.

Não foi identificado um impacto negativo na produtividade da empresa, uma vez que o procedimento de desenvolvimento seguro é transparente para as equipes de produção e personalização de cartões.

O desenvolvimento seguro agrega valor e confiabilidade nos requisitos de entrada e saída "*input/output*" dos sistemas utilizados. Todo esse processo exigido é auditado pelos auditores do PCI.

A não implementação dos requisitos de desenvolvimento seguro podem acarretar em processamento de informações de maneira incorreta e principalmente na fragilidade dos requisitos de segurança, propiciando o vazamento de informações confidenciais ou a adulteração de dados sigilosos.

Qualquer informação confidencial divulgada tem um grande impacto negativo sobre imagem da empresa no mercado de produção e personalização de cartões de pagamento bandeirados. Esse tipo de incidente deve ser mitigado a qualquer custo, conforme corroborado pelo Diretor-C.

4.3.2. Gerenciamento de usuários e sistemas de controle de acesso

Nakamura (2007) diz que a identificação e autenticação possui um papel fundamental para a segurança dos sistemas, ao validar a identidade dos usuários, concedendo-lhes a autorização para acessar os recursos pertinentes às suas atividades.

As políticas de gerenciamento de autenticação dos usuários são tratadas pelo PCI (2017) com a finalidade de estabelecer parâmetros de segurança na identificação dos usuários e no controle de acesso. Existe a preocupação em garantir que todos os acessos concedidos às informações dos portadores de cartões de pagamento sejam estritamente restritos ao mínimo necessário para o desempenho das funções.

O CISO assegurou que todos os usuários têm um único identificador de acesso, conforme recomendado na política de segurança da informação, e que todos os usuários são conscientizados sobre as políticas de concessão de acessos.

O Analista-M esclareceu que todo procedimento de autenticação dos usuários consta no documento PG-SETI e está de acordo com todas as exigências do PCI como: identificação única, requisitos de complexidade de senha, tamanho mínimo de senha, período de expiração de senha e número máximo de tentativas para validação do *login*. O analista afirmou que todo acesso é concedido conforme solicitações da chefia imediata, considerando o mínimo de privilégios necessários para que o colaborador desempenhe suas funções profissionais. Todas as exceções são tratadas diretamente pelo CISO e reportadas ao Analista-M para providências.

O Analista-M relatou que todo esse processo de identificação, autenticação e concessão de acesso é realizado via protocolo LDAP *(Lightweight Directory Access Protocol)*, por meio de servidores Microsoft, e que todos os sistemas atuantes na rede de personalização estão integrados a um controlador de domínio, dentro da empresa que provê a tecnologia de segurança de autenticação com um único ponto de acesso.

Este procedimento de integração de *logins* é nominado s*ingle sign-on,* e tem a função de prover um ponto único de autenticação aos usuários de uma determinada rede ou sistema. “Os serviços de segurança visam a garantir a correta identificação e autenticação dos usuários e processos da rede, o controle de acessos aos recursos, a integridade, confidencialidade e disponibilidade dos dados, o não repúdio e a criação de trilhas de auditoria” (MEDEIROS, 2005).

Nakamura (2007) argumenta que durante o processo de identificação o usuário declara uma determinada identidade ao sistema; durante a autenticação, o sistema valida essa identidade, após validada a identidade, a segurança depende das concessões permitidas de acesso.

Os controles de acesso de usuários listados pelo PCI (2017) têm como objetivo: restringir e autorizar os níveis de acesso concedido às equipes que lidam com dados confidenciais, garantido o mínimo de privilégios de acesso necessários para desempenhar as funções; assegurar que todos os funcionários tenham uma identificação única com *login* e senha; garantir que todo nível de acesso, em nível de administrador de sistemas, tenha sido liberado formalmente pelo CISO, com a respectiva justificativa; detalhar a política de geração, uso, renovação e distribuição de senhas de acesso aos sistemas da personalização; garantir a implementação de mecanismos que assegurem a exigência de critérios para criação de senhas fortes para os usuários, com a finalidade de dificultar a ação de mecanismos de força bruta.

Tanto o Analista-M quanto o CISO explicitaram suas preocupações na adoção de ferramentas que garantem a utilização de credenciais de acesso aos usuários e com os níveis de acesso concedido.

O Analista-M foi enfático em afirmar que os cuidados para controlar os níveis mínimos de acesso aos usuários são de grande importância para a segurança da informação, porém deve haver um cuidado especial para que essas políticas não prejudiquem o desempenho das atividades diárias dos profissionais. Conforme o Analista-M, encontrar um nível de acesso adequado é uma tarefa complexa e de grande importância no que tange aos requisitos de segurança.

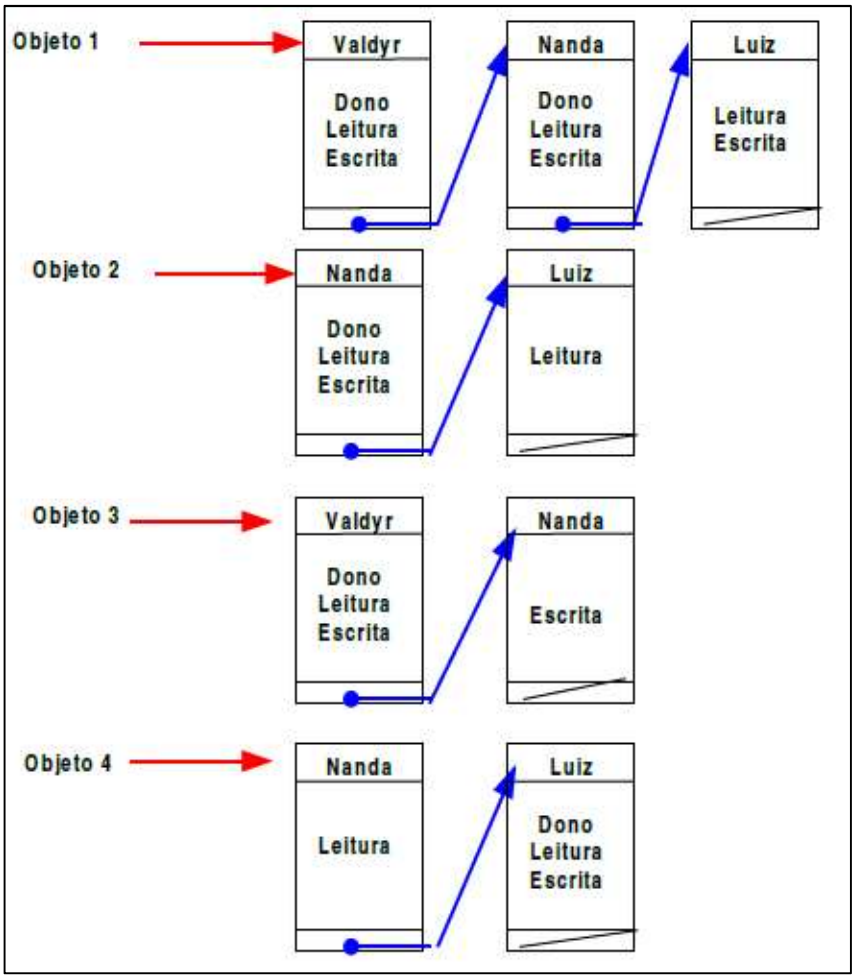

Figura 13 – Lista de controle de acesso
Fonte: LENTO; DA SILVA FRAGA; LUNG, 2006, p. 9.

A Figura 13 demostra a complexidade de administração de um controle de acesso a usuários. Conforme Lento, Da Silva Fraga; Lung (2006), cada objeto é associado a uma ACL (*Access Control Lists*), que indica os sujeitos no sistema e seus respectivos acessos autorizados. Essa administração é difícil, normalmente utilizada em níveis mais altos na administração de sistemas.

As regras de níveis de acesso devem estar claras na política de segurança da informação, conforme recomendações do PCI (2017). A implementação deve ser realizada por um profissional capacitado, a fim de propiciar os níveis de acessos necessários sem comprometer suas tarefas diárias. Todo esse processo deve ser validado pelo CISO formalmente, garantindo que não haja nenhum acesso concedido de forma equivocada ou superdimensionada.

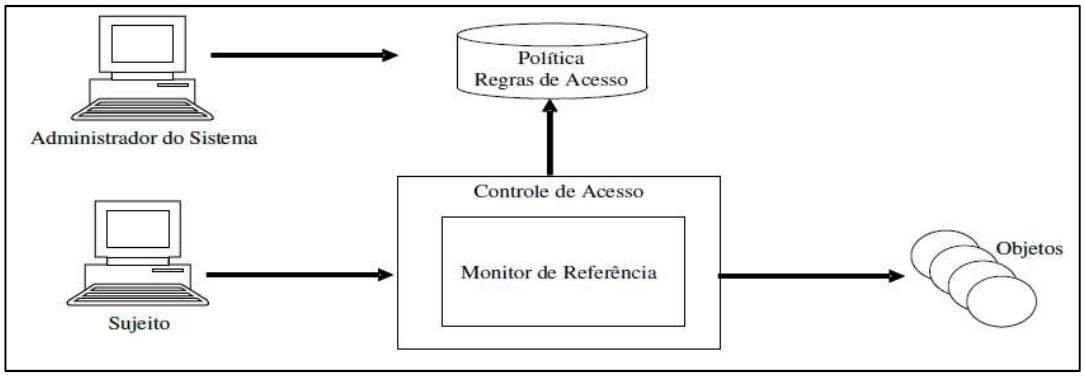

Figura 14 – Controle de acesso
Fonte: LENTO; DA SILVA FRAGA; LUNG, 2006, p. 5.

A Figura 14 demonstra como o controle de acesso limita as ações dos usuários de um determinado sistema e restringir diretamente a maneira com que ele pode operar o sistema.

Normalmente, em uma empresa, existem vários sistemas e isso acarretaria em várias credenciais de acesso. Tecnologias como o SSO (*Single Sign-On*), trazem grandes vantagens de usabilidade para os usuários e facilidades para os analistas de segurança da informação nas empresas; através dessa tecnologia, o usuário pode acessar diversas aplicações, incluindo o sistema operacional do computador, através de um único *login* e senha de acesso (NAKAMURA, 2007).

O SSO permite que a administração de senhas de *login* e a concessão de acessos sejam centralizadas, facilitando o controle e o gerenciamento das políticas de segurança de acesso da empresa. O SSO permite a integração direta com aplicativos desenvolvidos internamente e de terceiros, através de um protocolo com alto nível de segurança, além de proporcionar mais facilidade na administração de *login* e senhas pelos usuários.

Durante a entrevista, quando questionado a respeito da usabilidade dos usuários no que diz respeito aos sistemas disponibilizados dentro da fábrica de cartões, o Analista-M afirmou que existe uma necessidade de estabelecer um cronograma de treinamento anual, voltado a todos os funcionários da empresa, principalmente aqueles que lidam diretamente com os sistemas internos, para disseminar ou atualizar os conceitos exigidos pelo PCI a respeito dos procedimentos de *login* e senha de acesso.

De acordo com o Analista-M, os funcionários não têm os conceitos básicos de segurança da informação e até mesmo de tecnologia. Ele citou como exemplo a consciência por parte dos funcionários a respeito das consequências da divulgação de suas credenciais de *login* e senha a outros profissionais e as punições que isso pode acarretar.

Marciano (2006) enfatiza que deve existir uma preocupação com a usabilidade dos sistemas, tornando-os mais amigáveis, com a finalidade de facilitar a identificação por parte dos usuários. Quanto às formas de se realizar o acesso, os programadores devem considerar esse requisito como uma meta no desenvolvimento de sistemas seguros.

É de fundamental importância que a política de segurança da informação contemple um cronograma de treinamento anual, divulgando informações sobre os critérios de *login* exigidos pela empresa, determinando a periodicidade com que esses treinamentos acontecerão e o cronograma para as equipes ou setores da empresa se prepararem.

Embora os profissionais do setor de tecnologia que lidam diretamente com a recepção das informações provenientes dos emissores de cartão bandeirados tenham demonstrado bons conhecimentos a respeito dos conceitos de segurança, os demais funcionários da empresa, de acordo com o Analista-M e o Analista-W, não têm nenhuma preparação ou treinamento quanto à utilização de senhas ou sobre as consequências do comprometimento dessas credenciais de acesso.

O impacto de um comprometimento de credenciais dos usuários internos que participam diretamente na personalização dos cartões de pagamento bandeirados traria um aspecto de vulnerabilidade considerável a todo o ambiente tecnológico da empresa, uma vez que esse tipo de invasão ou acesso não autorizado, utilizando credencias internas, dificilmente seria identificado pela equipe de segurança de tecnologia e daria ao invasor pleno acesso a todo o ambiente de trabalho que a credencial permitir, podendo incluir acesso aos dados confidenciais.

Isso traria grandes problemas para a empresa e uma árdua tarefa para a equipe de segurança da informação.

Os impactos na estrutura tecnológica ligados à implementação de ferramentas destinadas ao controle de acesso com segurança são consideráveis e envolvem a aquisição de servidores, a implementação de ferramentas e a capacitação de profissionais com conhecimentos necessários para a utilização dessas ferramentas.

Os impactos à produtividade da empresa são mínimos ou até mesmo transparentes, uma vez que a única modificação apresentada aos usuários será a utilização de suas credenciais de acesso.

Os impactos da não adoção desses procedimentos de validação de credenciais de acesso e controle de acesso aos usuários ligados diretamente à personalização dos cartões de pagamento são consideráveis, uma vez que durante um processo de auditoria anual realizado pelas bandeiras, com certeza, se for identificado o não cumprimento desse requisito, isso

acarretará na suspensão do certificado para produção dos cartões de pagamento bandeirados. Em entrevista com Sr. Steve, ele deixou claro que a primeira coisa a ser observada durante a avaliação dos aplicativos utilizados na HSA é a validação das credenciais de acesso de cada usuário.

> Faço isso por amostragem, a tela tem que exigir as credenciais; quando o usuário se ausentar ou quando ele iniciar suas atividades, ele tem que digitar uma senha grande, se for pequena, já liga o alerta de que tem algo errado. Cada usuário tem que estar utilizando um *login* específico, é fácil ver isso. Esse é um requisito de grande peso, sem ele, não continuo, eu mando parar a auditoria (AUDITOR STEVE WILSON).

4.3.3. Gestão de Mudanças

O PCI (2017) possui um tópico em seu manual de procedimentos de segurança lógica destinado exclusivamente ao plano de gestão de mudanças. Esse tópico tem a finalidade de assegurar que todas as mudanças necessárias sejam autorizadas por um gestor competente e que cumpram todos os requisitos mínimos necessários para assegurar a continuidade da produção, sem deixar de lado os aspectos relativos a segurança da informação.

De acordo com o PCI (2017), o plano de gestão de mudanças descreve como deve ser documentado todo procedimento que envolva modificações tecnológicas dentro da área de alta segurança, a HSA, garantindo que essas modificações estejam em conformidade com os processos de auditoria e com a política de segurança da informação.

Durante a entrevista, o CISO confirmou a existência de um plano de gestão de mudanças implementado conforme as exigências do PCI. Ele destacou que esse procedimento é mencionado na política de segurança da informação e é detalhando no PG-SETI.

De acordo com CISO, o PCI exige a criação de um plano de mudanças detalhado que envolva: um plano de comunicação formal com a assinatura dos responsáveis pelas principais áreas afetadas; uma aprovação direta do CISO, autorizando a realização das mudanças; um detalhamento das tarefas realizadas, com a validação passo a passo das atividades; a determinação de uma data prevista de conclusão da mudança proposta; e um pano de *rollback*, caso o plano de mudanças não tenha o resultado esperado ou apresente falhas que inviabilize.

O documento foi exposto pelo CISO durante a entrevista, mas por conter informações confidenciais a respeito da rede de personalização e a identificação da empresa, não foi autorizada sua publicação neste trabalho acadêmico.

O plano de gestão de mudanças apresentado cumpre todas as exigências do PCI (2017); nele consta, inclusive, um plano de mudanças emergenciais não mencionado na entrevista com o CISO, que permite o registro e a realização de uma mudança não planejada em caráter emergencial. O documento apresentado estava assinado pelos principais envolvidos de cada área afetada e validado pelo CISO, autorizando a realização das tarefas.

Assegurar a criação e implementação de um plano de gestão de mudanças conforme o PCI consiste em documentar todo o processo de mudança, planejando e detalhando o passo a passo de cada modificação necessária para cumprir o plano, além de comunicar formalmente cada setor envolvido, coletando assinaturas que certificam a ciência de cada um dos gestores.

Outro aspecto importante em um plano de gestão de mudanças, seguindo as recomendações do PCI (2017), é determinar as datas de conclusão para execução de cada uma das etapas listadas no documento, registrando a conclusão de cada uma delas até a finalização do plano e validação do CISO.

Conforme Sallé (2004), o ITIL (*Information Technology Infrastructure Library*) descreve que o objetivo do processo de gestão de mudanças é assegurar que as técnicas utilizadas sejam padronizadas, utilizando métodos eficientes, minimizando os incidentes relacionados às mudanças propostas. O plano de gestão de mudanças tem o propósito de assegurar que as atividades sejam realizadas de forma controlada que sejam avaliadas, priorizadas, planejadas, testadas, implantadas e documentadas.

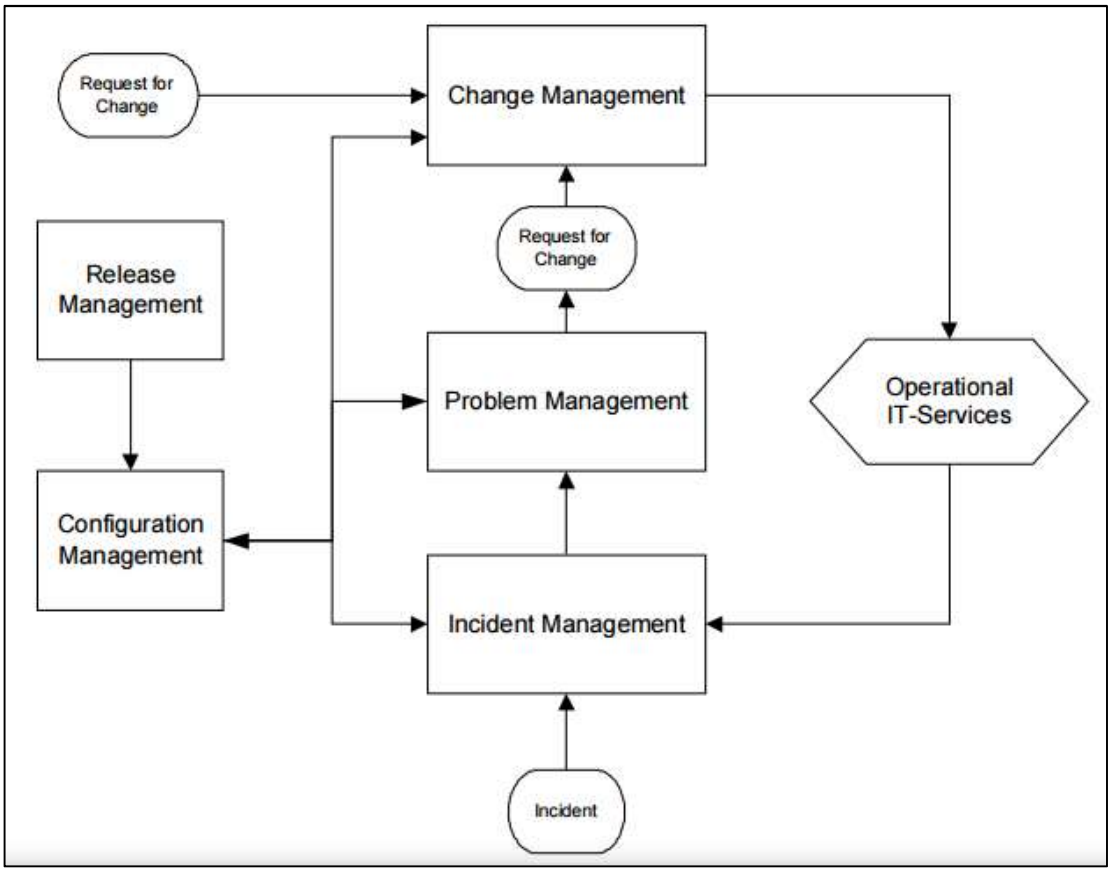

Figura 15 – Relacionamento entre processos – ITIL
Fonte: SALLÉ, 2004, p. 11.

Conforme a Figura 15, todos os processos ditados pelo ITIL são interligados e cooperam entre si; o processo de gestão de mudanças tem um impacto direto nos serviços operacionais e na tratativa de incidentes que porventura possam ocorrer durante o procedimento de mudança.

Para que o plano de mudanças seja efetivo e os impactos negativos, mitigados, é necessária a criação de rotinas de *Backup/Roolback*. Esses procedimentos irão assegurar a recuperação, praticamente imediata, a um nível aceitável, do ambiente afetado pelas mudanças em caso de falha. Sêmola (2003) reforça que um plano de continuidade de negócios deve ser desenvolvido com o claro objetivo de reparar incidentes de segurança que não puderam ser evitados.

Os analistas Analista_R, Analista-W e Analista-M têm ciência da existência de um procedimento de plano de mudança dentro da empresa. Todos confirmaram que este plano é utilizado e o consideram muito importante.

O Analista-W mencionou que esta é a única maneira de estabelecer um controle e acompanhar as mudanças realizadas, comunicando todos os envolvidos e criando um subsídio, caso ocorra a alegação por qualquer uma das partes envolvidas quanto ao desconhecimento das mudanças realizadas.

Conforme Moraes (2007), dependendo do objetivo da organização, a falta de uma informação pode resultar em dificuldades administrativas e até na paralização de serviços essenciais, caso ocorra perda de dados.

Um plano de mudança bem estruturado, com processos bem definidos, é essencial para o sucesso das ações que precisam ser realizadas de forma programada. Foi relatado pelo CISO que em todos os processos de auditoria interna realizados pelas bandeiras, o auditor solicita a apresentação dos documentos relativos aos planos de mudança ocorridos no último ano.

Qualquer procedimento realizado dentro de uma personalizadora precisa ser planejado levando-se em conta todos os aspectos possíveis relativos à segurança da informação. Uma análise criteriosa da mudança proposta deve ser realizada pela equipe de segurança da informação e validada pelo CISO antes de qualquer intervenção.

Os impactos na produtividade, na estrutura tecnológica da empresa e na estrutura financeira são irrisórios. O plano de gestão de mudanças não carece de qualquer investimento em tecnologias; é uma metodologia de trabalho que dever ser corretamente implementada e gerenciada por um CISO.

O impacto de uma mudança realizada sem planejamento pode afetar em sério prejuízo financeiro, tendo em vista que uma mudança sem sucesso pode paralisar toda produção, atrasar todos os prazos e compromissos com os clientes e manchar a imagem da empresa, além de gerar pesadas multas contratuais por atrasos na produção e entrega dos cartões.

Vale ressaltar que conforme informações do CISO, em um processo de auditoria anual, a falta de evidências de que a empresa possui um plano de gestão de mudanças efetivo é uma não conformidade.

Outro importante aspecto que precisa ser observado pela não realização de um correto plano de mudanças diz respeito diretamente aos requisitos de segurança da informação. Os impactos em segurança lógica podem refletir diretamente nos processos internos da empresa, abrindo lacunas de segurança, comprometendo o desempenho dos servidores e aplicativos, propiciando a violação ou o furto de informações confidenciais.

4.4. Plano de análise de risco

Dantas (2011) afirma que o estudo do risco assume um importante papel nas corporações do mundo moderno proporcionando-lhes um processo de gerenciamento baseado nos riscos, para serem compreendidos como algo que cria oportunidades ou produz perdas com relação à segurança lógica. Os riscos são condições que criam ou aumentam principalmente o potencial de danos para as corporações.

Um dos principais objetivos da segurança da informação é reduzir os impactos negativos dos riscos sobre a organização para um nível aceitável, gerenciando e buscando maneiras de mitigar os potenciais *gaps* de segurança da informação (ITGI, 2006).

Marciano (2006) afirma que o risco deve ser adequadamente medido e avaliado, possibilitando a criação de medidas preventivas voltadas à sua diminuição.

No guia de segurança da informação e governança do ITGI (2006), são recomendadas medidas que a equipe de segurança da informação deve levar em conta para estabelecer um plano de mitigação dos riscos. São eles: proteger todos os ativos de TI contra acesso indevido ou remoção não autorizada, realizar regularmente avaliações da probabilidade de riscos à segurança da informação, realizar avaliações regulares da equipe de monitoramento de risco, restringir ao mínimo necessário o acesso a informações sensíveis, monitorar, identificar e relatar vulnerabilidades e incidentes de segurança ao CISO que deve, por sua vez, manter um plano de continuidade efetivo e testado.

Para o COBIT.5 (2012), a gestão de riscos implica o reconhecimento do risco, a avaliação do impacto e da probabilidade daquele risco ocorrer, para que seja desenvolvido um plano estratégico com a finalidade de evitar os riscos.

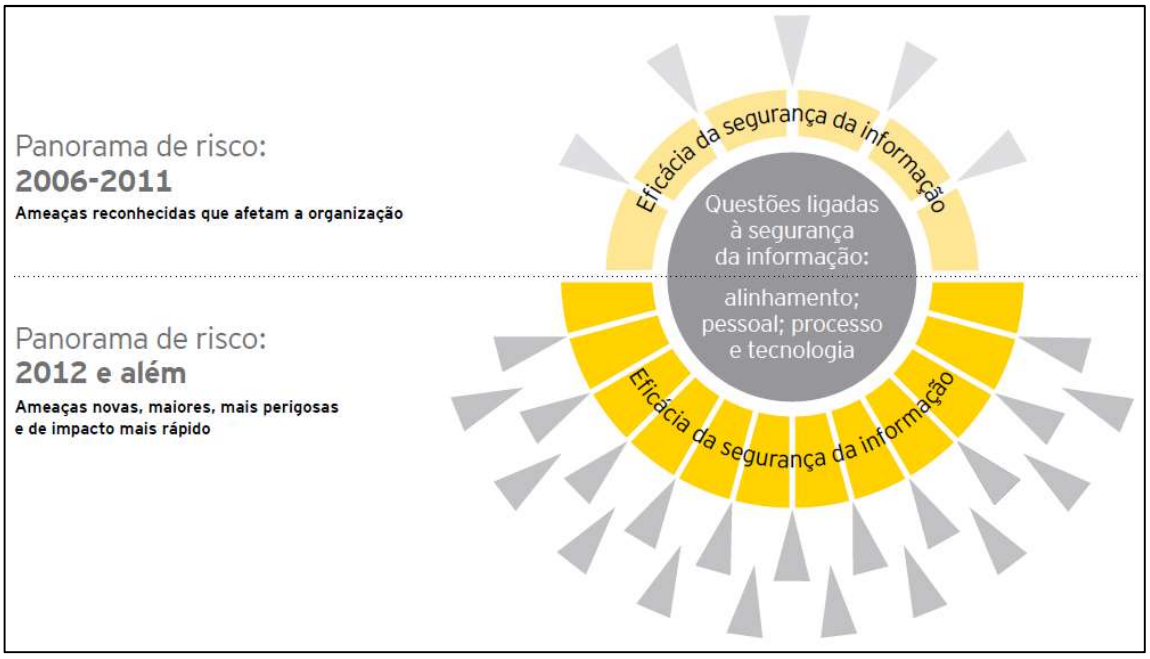

Figura 16 – Panorama de riscos – Análise de *gaps* em segurança da informação
Fonte: ERNST & YOUNG, 2012, p. 11.

A Figura 16 demostra, em um panorama de riscos, que o *gap* em segurança da informação não é fruto de uma só questão; o resultado compreende uma gama de fatores relacionados ao alinhamento estratégico organizacional, envolvendo pessoas, processos e tecnologias. Para criar um plano estratégico de segurança voltado à redução dos riscos de forma eficaz, é preciso, primeiramente, entender todo o processo de negócio da empresa e funcionar em uníssono com diversas áreas dentro da corporação (ERNST & YOUNG, 2012).

É muito importante determinar as ferramentas, os processos e os métodos adequados para monitorar ameaças, medir o desempenho e identificar *gaps* de cobertura dentro da empresa. A designação de um profissional competente representado pelo CISO é de fundamental importância para a criação de um plano de segurança da informação eficiente e voltado às necessidades da empresa (ERNST & YOUNG, 2012).

A eleição de um CISO com autoridade suficiente para criar uma política de segurança da informação eficiente e efetiva, baseada nas necessidades tecnológicas da empresa e focada na redução dos riscos, é muito importante para empresas que lidam com informações confidenciais em seu cotidiano.

A criação de uma matriz de riscos, conforme Dantas (2011) propõe, fornece uma base para determinar a criticidade e aceitabilidade pela organização, escolhendo cuidadosamente os parâmetros para o estudo e a classificação dos riscos, alinhados com a realidade da empresa e levando em consideração as atividades de negócio e seu contexto.

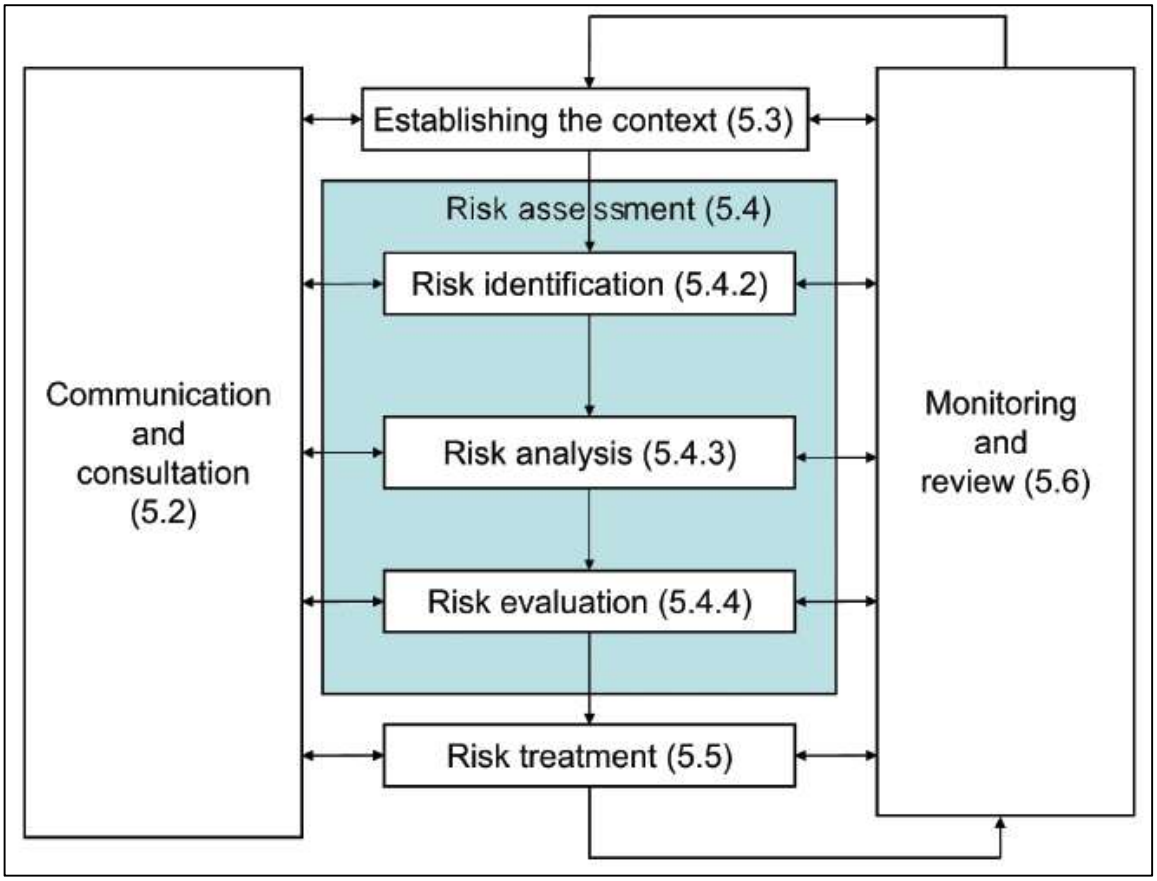

Figura 17 – Processo de gestão de risco
Fonte: INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2009.

Como demostrado na Figura 17, um processo de gestão de riscos precisa monitorar, identificar, analisar, avaliar, tratar e comunicar, estabelecendo a integração entre as partes, e adequando os processos de negócio às necessidades da empresa.

Conforme a ISO 31000 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2009), a compreensão do contexto externo também é importante para garantir que os objetivos e as preocupações das partes interessadas sejam completamente atendidos e resguardados ao identificar os principais critérios de risco. Entender o contexto da organização e detalhes específicos das exigências legais é importante para fechar o escopo do processo de gerenciamento de risco de forma adequada e efetivo, dentro da corporação.

O PCI (2017) recomenda às personalizadoras de cartões bandeirados que façam a realização periódica de testes de vulnerabilidades e penetração interna e externa em suas empresas. Os testes de vulnerabilidades externas devem ser realizados trimestralmente ou quando houver qualquer modificação significativa na estrutura de rede lógica da empresa. Esses

testes devem ser realizados apenas por empresas qualificadas pelo PCI ASV – *Approved Scanner Vendor* (PCI, 2017).

Os testes de vulnerabilidades internas também devem ser trimestrais, porém podem ser realizados pela equipe interna da personalizadora, desde que sejam utilizadas as ferramentas adequadas (PCI, 2017).

Conforme o CISO, responsável pela contratação, pelo monitoramento e pela realização dos planos para tratativa das não conformidades apontadas durante os testes de vulnerabilidades e penetração, existe uma certa dificuldade em encontrar empresas certificadas ASV, principalmente no Brasil. O valor cobrado por essas empresas, geralmente em libras esterlinas, é consideravelmente alto.

Conforme o PCI (2017), os testes internos podem ser realizados pela própria equipe de segurança da informação da personalizadora. Conforme o Analista-M, a empresa utiliza o *Retina Guided UI*, uma ferramenta destinada exclusivamente a testes de varredura de vulnerabilidades que gera relatórios em conformidade com o PCI e que é atualizada diariamente.

Conforme o CISO, o *Retina Guided UI* tem um elevado custo de manutenção anual necessário para atualização de seus pacotes e definições de segurança; porém, mesmo com esse custo elevado, ainda é mais vantajoso para a personalizadora custear essas atualizações do que contratar um terceiro para realização dos testes. O CISO estimou que os gastos com terceiros seriam de aproximadamente 130% do valor de uma atualização anual, por teste, sendo necessários pelo menos quatro testes anuais.

Conforme o Analista-M, esse procedimento de verificação é realizado conforme as solicitações do PCI, e a partir dos resultados é gerado um formulário contendo as não conformidades identificadas, que deverão ser tratadas, e o plano de tratativa evidenciado nas auditorias anuais, juntamente com um relatório confirmando a resolução daquele risco apontado.

Conforme o PCI (2017), esses testes consistem em procedimentos de varredura em busca de possíveis vulnerabilidades que possam ser exploradas por *hackers* ou aplicativos maliciosos. Após a realização dos testes, deve ser emitido um relatório, conforme os padrões PCI, com as vulnerabilidades encontradas. A partir desse relatório, inicia-se um plano de correção das vulnerabilidades apontadas, para que sejam corrigidas através de um plano de ação definido pelo CISO, em um prazo máximo de dois dias.

Feitas as correções das ameaças encontradas pela ferramenta, é gerado um novo relatório para comprovar que o plano de ação foi efetivo.

O PCI (2017) recomenda que todas as evidências, fruto das tratativas das ameaças encontradas, e o processo de remediação dessas vulnerabilidades sejam preservadas para serem apresentadas nos processos de auditoria anual, caso solicitado.

Já os testes de penetração externos devem ser realizados anualmente, conforme as recomendações do PCI (2017); esses testes podem ser realizados remotamente e não necessariamente por uma empresa certificada ASV.

Os testes de penetração internos não podem ser realizados remotamente e devem incluir os testes voltados para detecção de *Injection flaws, Buffer overflow, Insecure cryptographic storage, Improper error handling* e outras vulnerabilidades de redes (PCI, 2017).

Conforme o CISO, a empresa não possui uma ferramenta que possibilite a realização dos testes de penetração. Normalmente, eles são realizados por empresas contratadas e acompanhados pela equipe interna de segurança da informação.

Conforme o PCI (2017), a personalizadora precisa assegurar que todas as ações corretivas foram realizadas e iniciadas em, no máximo, dois dias após o apontamento, com a autorização formal do CISO. Todas as evidências do sucesso na correção e remediação das não conformidades devem ser preservadas para serem apresentadas nos processos de auditoria.

Conforme o Analista-M, o Analista-W e o Analista-R, esses planos de ação mobilizam toda a equipe de tecnologia. O CISO não soube detalhar como é realizado o plano de ação para tratativa das não conformidades, ele se limitou a dizer que todas são tratadas e as evidências, preservadas, conforme solicitado pelo PCI.

Conforme Nakamura (2007), em um ambiente corporativo, diferentes tipos de acessos devem ser dados a diferentes tipos de bolsões de segurança. Essa diferenciação é prudente e deve ser tratada com cautela, garantindo a segurança interna. A exploração de vulnerabilidades é comum e podem ocorrer através de *bugs* na implementação ou construção de aplicativos.

Esses procedimentos de varredura de vulnerabilidades e testes de penetração têm um impacto significativo nas personalizadoras de cartões de pagamentos bandeirados.

Há um impacto direto na produtividade, uma vez que, durante a realização dos testes, acontece uma sobrecarga de processamento nos servidores e periféricos de rede, causando lentidão e atrasos nos processamentos. Isso reflete diretamente na capacidade de escoamento da produção, uma vez que todo o sistema de fechamento e expedição de cartões é informatizado.

Existe o impacto financeiro, uma vez que esses testes são realizados trimestral e anualmente, tanto pela equipe interna, fazendo a utilização de um aplicativo específico com

atualizações anuais, quanto por terceiros, neste caso, por empresas cadastradas e certificadas ASV.

Os custos que envolvem os terceiros certificados PCI, geralmente são faturados em libras esterlinas ou em euro e consideravelmente altos, conforme corroborado pelo CISO.

Os testes de penetração utilizam ferramentas bem específicas, e o custo de aquisição dessas ferramentas, que também envolve manutenção e atualização anual, são elevados, além de ser necessária uma equipe técnica muito bem capacitada e especializada para realização desses testes.

O PCI (2017) não aceita que os relatórios emitidos, relativos aos testes de vulnerabilidades e penetração, sejam gerados por aplicações de código aberto.

Esse processo de testes de penetração, testes de varredura e plano de ação para correção dos riscos é moroso e pode afetar toda estrutura tecnológica da empresa, paralisando a produção e comprometendo a produtividade. É recomendado que tudo seja planejado e realizado conforme descrito e aprovado pelo CISO.

O não cumprimento desses requisitos tem um impacto direto no plano de homologação da personalizadora junto às bandeiras. Conforme o CISO, se esses procedimentos de varredura de vulnerabilidades e testes de penetração, que certificam se a estrutura tecnológica da empresa atende ou não aos requisitos mínimos de segurança da informação recomendados pelo PCI, não forem realizados ou se o plano de correção das ameaças encontradas não for cumprido, durante o processo de auditoria anual, o auditor suspende a empresa da produção de cartões de pagamento bandeirados até que sejam apresentadas as evidências relativas à correção das não conformidades apontadas na auditoria.

5. CONSIDERAÇÕES FINAIS

Uma empresa que se propõe a personalizar cartões de pagamento bandeirados tem a obrigação de adotar práticas que garantam segurança e rastreabilidade durante todo o processo, desde o recebimento das informações relativas aos portadores de cartões até os procedimentos de personalização e expedição dos cartões personalizados.

A informação é um dos ativos mais valiosos em uma empresa que lida diariamente com informações confidenciais. O furto ou a violação de qualquer informação classificada como secreta pode acarretar sérios prejuízos à empresa, afetando, inclusive, sua imagem no mercado.

Requisitos como a confidencialidade e a integridade das informações são muito relevantes dentro de uma personalizadora. A adoção de práticas mundialmente aceitas e com foco nas recomendações do *PCI Card Prodution and Provisioning – Logical Requeriments* são exigências das principais bandeiras de cartões de pagamento para personalização de cartões. No que tange à segurança da informação, o PCI fornece um manual de procedimentos, a fim de mitigar as lacunas de segurança lógica dentro das personalizadoras, proporcionando um ambiente mais seguro e estruturado para tratativa de informações sigilosas.

Ter ciência dos impactos que a segurança da informação pode causar dentro de uma empresa personalizadora de cartões de pagamento bandeirados é um fator preponderante, principalmente no que diz respeito às consequências negativas sobre a imagem das prestadoras de serviços bancários no mercado de cartões.

Este estudo realizou uma entrevista a partir de um roteiro semiestruturado para identificar as principais lacunas ou disparidades de informações a respeito de procedimentos adotados e descritos na política de segurança da informação dentro de uma personalizadora.

Durante as entrevistas, foram observadas divergências nas informações fornecidas entre o CISO, responsável por criar e fazer cumprir todos os procedimentos de segurança lógica constantes na política de segurança da informação, e a equipe interna da empresa, composta por analistas de tecnologia, coordenadores de produção, gestores de qualidade e a diretoria.

Por se tratar de um assunto delicado, principalmente dentro de uma personalizadora de cartões de pagamento bandeirados, alguns entrevistados demonstraram insegurança e receio de fornecer informações em sua completude ou argumentar de forma mais clara, quando indagados sobre os processos que envolvem a tratativa de dados confidenciais.

Durante a análise de resultados, foram identificados os principais impactos que a segurança da informação causa em uma empresa personalizadora de cartões de pagamento bandeirados.

Na primeira análise realizada, uma lacuna foi imediatamente identificada no que diz respeito à segurança da informação: a grande margem de interpretação subjetiva que os auditores, certificados pelo PCI e homologados pelas bandeiras, impõem durante os processos de auditoria realizados dentro das personalizadoras. Essa interpretação pessoal pode trazer problemas de segurança lógica, uma vez que essas discussões a respeito de uma determinada não conformidade apontada pelo auditor não estão claras no manual de procedimentos do *PCI Card Prodution and Provisioning – Logical Requeriments.*

As discussões entre o CISO e o auditor que acontecem durante as auditorias anuais, em sua maior parte, são incoerentes em relação à não conformidade apontada e culminam na impugnação de uma tarefa direcionada à personalizadora em virtude da falta de um embasamento técnico apropriado no manual de procedimentos do PCI.

As auditorias anuais são a maneira de garantir o cumprimento mínimo dos requisitos de segurança lógica dentro das personalizadoras. A determinação de um órgão regulador e fiscalizador homologado pelas bandeiras obriga as personalizadoras a adotarem procedimentos e padrões de segurança da informação, como, por exemplo, a criação de uma política de segurança da informação efetiva e atualizada.

Os impactos da falta de uma política de segurança da informação ou da sua inconsistência refletem diretamente no processo de homologação das personalizadoras para produzir cartões de pagamento bandeirados. Ter uma política de segurança da informação formal e validada por um profissional competente é um requisito obrigatório para iniciar o processo de homologação junto às bandeiras. A política de segurança da informação tem o dever de primar pelos requisitos de confidencialidade e integridade das informações relativas aos portadores de cartões de pagamento.

Os impactos causados pela divulgação ou violação de informações sigilosas dentro de uma personalizadora estão ligados diretamente à imagem da empresa no mercado de produção e personalização de cartões de pagamento. Ficou evidente, durante as entrevistas, a preocupação da diretoria e do CISO em preservar as informações confidenciais e, respectivamente, a imagem da empresa no mercado. Em uma personalizadora de cartões, a segurança da informação é uma parte estratégica da corporação e, como tal, precisa ser tratada com a devida importância, envolvendo todos os principais gestores e a diretoria da empresa.

É de responsabilidade do CISO manter um diagrama de fluxo de transmissão de dados e informações atualizado e validado, bem como ter esse fluxo de informações monitorado. Esse é um requisito importante no que tange à rastreabilidade dos dados recebidos e processados pelas personalizadoras. O impacto da adequação desse requisito na produtividade da empresa é irrelevante, uma vez que ele é transparente para os usuários e não reflete nos processos produtivos.

Os impactos financeiros para criar e monitorar o fluxo de informações ficam a cargo da aquisição e configuração de servidores e da contratação de mão de obra especializada para essa finalidade. Manter o monitoramento do fluxo de informações de forma adequada é um requisito importante, no que se refere à rastreabilidade das informações sigilosas dos portadores de cartões de pagamento dentro das personalizadoras.

A não adequação desse procedimento tem um impacto negativo durante os processos de auditoria e homologação junto às bandeiras. Este é um requisito exigido e verificado pelos auditores sistematicamente em todos os processos de auditoria; sua falta pode acarretar na perda do certificado de homologação para produção de cartões bandeirados.

O monitoramento do fluxo de dados é um procedimento essencial para fornecer informações sobre qualquer incidente ocorrido dentro da personalizadora a respeito do tráfego de informações ou para atender às solicitações dos bancos em relação à recepção de arquivos confidenciais. Uma falha no monitoramento do fluxo de informações tem um impacto direto na imagem da empresa junto aos emissores e aos bancos. É de responsabilidade da personalizadora garantir que as informações sobre todo o fluxo que envolve, desde a recepção, passando pelo processamento de dados, personalização e expedição dos cartões de pagamento bandeirados, sejam verídicas e completas.

Qualquer procedimento que envolva a tratativa de informações confidenciais e o controle de acesso a essas informações é considerado crítico. Manter a segurança da rede de dados, o gerenciamento dos sistemas desenvolvidos internamente e o controle de acesso dos usuários é importante para garantir que os serviços relativos à personalização de cartões sejam

prestados com assertividade e segurança. Os impactos na produtividade são considerados baixos, uma vez que, após a equipe de produção e tecnologia estarem treinadas e cientes dos procedimentos, o fluxo de produção transcorre normalmente, sem gerar atrasos ou percalços. Os impactos financeiros estão ligados diretamente à aquisição de ferramentas para o controle e o pagamento de mão de obra especializada, porém sem grande expressividade.

Os impactos da segurança da informação na estrutura tecnológica da empresa são, em sua maior parte, consideráveis. A aquisição de servidores dedicados para atender às especificações de segurança do PCI, a disponibilização de uma sala para adequação física desses servidores e a contratação de profissionais com formação e conhecimentos adequados é inevitável para manter o padrão de segurança na rede de dados.

A falsa sensação de segurança decorrente de uma má estruturação da rede de dados pode acarretar na dificuldade de identificação de uma suposta invasão, podendo afetar diretamente as redes de alta segurança, como a personalização e a DMZ. Outro impacto considerável seria na produtividade da empresa: uma falha da estruturação da rede pode comprometer o desempenho dos servidores e todo o fluxo de informações secretas, incluindo o acesso não autorizado. Esse tipo de incidente traz sérios problemas para uma personalizadora; seu impacto vai além da produtividade, resultando, talvez, na suspenção da licença para produção de cartões.

Um planejamento adequado, tanto na estruturação do ambiente tecnológico quanto na manutenção dos requisitos de segurança, é primordial para se ter uma estrutura lógica segura.

Os impactos causados por uma modificação malsucedida, realizada sem planejamento, sem um plano de comunicação formal e sem a autorização do CISO, podem impactar diretamente na produtividade, paralisando toda a linha de produção que inclui o processamento e a personalização dos cartões.

Fica evidente a necessidade de se ter um plano de gestão de tecnologia detalhado, focado em segurança da informação e direcionado para as empresas que lidam diretamente com informações sigilosas na composição de seu processo produtivo. Uma falha em um dos procedimentos que envolvem a recepção dos arquivos ou a falta de comunicação entre emissores e personalizadoras é considerado um complicador em todo o processo produtivo, comprometendo o SLA. Um plano de gestão de mudanças bem elaborado tem um impacto positivo na linha de produção de uma personalizadora. Os impactos financeiros para a adoção desse plano são ínfimos, por se tratar exclusivamente da adequação de um procedimento para o alinhamento das tarefas junto à equipe de tecnologia. Os impactos na estrutura tecnológica

são praticamente inexistentes, por ser procedural, além de auxiliar no acompanhamento dos resultados e possíveis riscos.

Quanto à gestão de riscos, o impacto financeiro relativo à manutenção de um plano de análise de riscos homologados pelo PCI é consideravelmente alta. Os procedimentos necessários para cumprir este requisito são indispensáveis para a obtenção dos certificados emitidos pelas bandeiras e precisam ser apresentados nos processos de auditoria anual. Esses procedimentos devem ser realizados trimestralmente, conforme o PCI.

Os impactos relativos à adoção de um plano de gestão de riscos na produtividade são consideráveis, uma vez que os testes de varredura interna sobrecarregam a rede de dados e os principais servidores da empresa. Porém, como mencionado anteriormente, o não cumprimento desse requisito, deixa a personalizadora inapta para a produção dos cartões bandeirados.

Fica claro que os assuntos relativos a segurança da informação têm chegado ao alto escalão das empresas personalizadoras de cartões de pagamento bandeirados. A necessidade de atuação direta dos profissionais de segurança da informação nos controles internos para adequação aos procedimentos para atender aos processos de auditorias anuais das bandeiras é inquestionável. O alinhamento entre CISO e diretoria é um fator determinante para garantir um plano de conformidade em acordo com as exigências constantes no manual do PCI *Card Production and Provisioning Logical Security Requirements*.

Infere-se, neste estudo, que, embora haja exceções por se tratar de um assunto muito amplo, a segurança da informação tem um impacto direto na construção da estrutura tecnológica, na produtividade e na imagem da empresa no mercado de produção e personalização de cartões. O tema segurança da informação é muito extenso e permeia todos os processos internos nas empresas contemporâneas, principalmente naquelas que lidam diretamente com informações confidenciais, como as personalizadoras de cartões de pagamento bandeirados.

Marciano (2006) afirma que, naturalmente, a segurança da informação tem custos, contudo, sua ausência tem um custo ainda maior, seja econômico, seja social, na figura de uma imagem negativa perante o público, por isso manter uma política de segurança atualizada é primordial em uma personalizadora de cartões.

5.1. Limitações

Por se tratar de um seguimento que lida em sua completude com informações confidenciais, o acesso a determinadas informações é completamente vetado, como por exemplo:

- O acesso aos contratos de concessão e prestação serviços entre a personalizadora e as bandeiras (documento inacessível).
- O acesso a documentos e relatórios relativos a produção, com a finalidade de medir e identificar gargalos produtivos, falhas de comunicação e erros de processamento de dados. Nenhum documento pode ser fornecido e algumas perguntas da entrevista foram retiradas.
- O acesso aos profissionais que lidam diretamente nos processos produtivos foi moroso e complicado. Todos os profissionais têm receio de se manifestar e poder comprometer os requisitos de segurança da informação. Ficou claro durante as entrevistas, que esses profissionais, muitas vezes, deram respostas resumidas, com receio de fornecer informações sigilosas ou até mesmo de estarem sendo abordados com perguntas que possivelmente tragam vulnerabilidades a respeito da segurança lógica da empresa, conhecido como técnicas de engenharia social.

Houveram, também, dificuldades em identificar outros artigos que argumentem sobre as empresas personalizadoras de cartões de pagamento. Por se referir a um assunto tratado com sigilo, tanto pelos bancos quanto pelas personalizadoras, e por ser realizado por pocas empresas no Brasil, o acesso à informação é moroso, tendo em vista que confidencialidade das informações sobre as atividades das personalizadoras é uma das exigências a serem cumpridas no manual do PCI.

Além disso, foi difícil ter acesso a outras empresas que prestam serviços de personalização de cartões de pagamento bandeirados. Mesmo com a justificativa de ser um trabalho acadêmico, as empresas se negam a fornecer qualquer tipo de informações a terceiros.

5.2. Sugestões para estudos futuros

O PCI *Card Prodution* é um manual de regras que se limita a auditar apenas as redes de alta segurança ou, especificamente, as redes em que trafegam os dados confidenciais, como a DMZ e a rede de personalização. Seria conveniente, levando-se em conta os aspectos de segurança da informação, que toda a rede da empresa fosse contemplada, realizando um levantamento de todo o parque tecnológico empresarial, com informações de todas as redes da empresa e o plano de segregação efetivo. Assim, ficaria claro para o auditor a estrutura e a topologia tecnológica da empresa, possibilitando uma análise mais criteriosa a respeito da segregação física e dos possíveis pontos que podem comprometer a segurança das redes de alta segurança que precisam ficar dentro da HSA.

O PCI não é exato sem suas colocações constantes no PCI *Card Production and Provisioning Logical Security Requirements,* permitindo que os auditores, conforme relatado em entrevista pelo Sr. Steve, explicitem suas opiniões pessoais e considerações, com margem para interpretações e julgamentos, muitas vezes, contestáveis.

Outro aspecto importante faz menção aos processos de auditoria anual. Esses deveriam ser mais criteriosos, determinando pesos ou notas nas não conformidades ou requisitos apontados, facilitando e deixando claro se uma empresa atende às exigências mínimas ou não de produzir os cartões de crédito bandeirados. Esse procedimento deixaria o processo de auditoria mais claro, reduzindo também a interpretação pessoal dos auditores que, muitas vezes, são errôneas, no que tange aos quesitos de segurança lógica das personalizadoras.

Seria, portanto, interessante a realização de um estudo para identificar e padronizar uma ferramenta que futuramente seja homologada pelo PCI, para atuar diretamente na geração de relatórios a respeito de eventos de segurança. O principal objetivo dessa ferramenta seria fornecer informações padronizadas, inalteradas e periódicas, para serem enviadas aos auditores para análise do fluxo de informações dentro das personalizadoras, detalhando como as informações confidenciais são tratadas ao longo do processo de personalização, trazendo mais credibilidade nos processos de auditoria anual, evitando que as personalizadoras façam uso de soluções de contorno ou omitam de fatos críticos.

Esta dissertação não teve a pretensão de esgotar o tema; por essa razão faz-se necessária a indicação de sugestões que possam auxiliar na continuidade deste estudo. Conforme Casanas e Machado (2001), por mais que se trabalhe nesse objetivo, dificilmente se conseguirá cobrir todas as lacunas que esta área proporciona.

REFERÊNCIAS

ABECS - Associação Brasileira das Empresas de Cartões de Crédito e Serviços. **Cartões somam quase R$ 1 trilhão em compras e mais de 10 bilhões de transações em 2014**. Disponível em: <www.abecs.org.br>. Acesso em: 25 maio 2016.

AL-SHAER, Ehab S.; HAMED, Hazem H. Discovery of policy anomalies in distributed firewalls. **INFOCOM 2004**. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies. IEEE, 2004. p. 2605-2616.

ANDERSON, Ross. **Why Information Security is Hard** - An Economic Perspective. University of Cambridge - Computer Laboratory. 30 Jan. 2001. Disponível em: <https://www.acsac.org/2001/papers/110.pdf>. Acesso em: 26 set. 2016.

ANDERSON, James M. Why we need a new definition of information security. **Computers & Security**, v. 22, n. 4, p. 308-313, 2003. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167404803004073>. Acesso em: 26 set. 2016.

BERRY, L.; PARASURAMAN, A. **Serviços de Marketing**: Competindo Através da Qualidade. São Paulo: Maltese, 1992.

BISPO, Carlos Alberto Ferreira. **Uma análise da nova geração de sistemas de apoio à decisão**. 1998. 174 f. Dissertação (Mestrado em Engenharia da Produção) – Universidade de São Paulo, São Paulo, 1998. Disponível em: <http://www.teses.usp.br/teses/disponiveis/18/18140/tde-04042004-152849/en.php>. Acesso em: 08 jun. 2016.

BITTAR, Bernardo. Polícia prende quadrilha especializada em clonagem de chips de cartões. **Correio Brasiliense**. 2015. Disponível em: <http://www.correiobraziliense.com.br/app/noticia/cidades/2015/10/06/interna_cidadesdf,501403/policia-busca-quadrilha-especializada-em-clonagem-de-chips-de-cartoes.shtml>. Acesso em: 09 jun. 2016.

BONELLI, Regis; FONSECA, Renato. **Ganhos de produtividade e de eficiência**: novos resultados para a economia brasileira. 1998. Disponível em: <http://repositorio.ipea.gov.br/handle/11058/2383>. Acesso em: 09 out. 2016.

BONTIS, N.; KEOW, W. C. C.; RICHARDSON, S. Intellectual capital and business performance in Malaysian industries. **Journal of Intellectual Capital**, v. 1, n. 1, 2000, p. 85-100.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. 2006. 261 f. Dissertação (Mestrado em ciências de engenharia de sistemas de computação) – Universidade Federal do Rio de Janeiro – COPPE, Rio de Janeiro, 2006. Disponível em: <https://www.researchgate.net/profile/Marcelo_Carvalho17/publication/268809917_A_TRAJETRIA_DA_INTERNET_NO_BRASIL_DO_SURGIMENTO_DAS_REDES_DE_COMPUTADORES__INSTITUIO_DOS_MECANISMOS_DE_GOVERNANA/links/54774a430cf2a961e4825bd4.pdf>. Acesso em: 08 jun. 2016.

CASANAS, Alex Delgado Gonçalves; MACHADO, César de Souza. O impacto da implementação da norma nbr iso/iec 17799–código de prática para a gestão da segurança da informação-nas empresas. **Anais** em CDROM do XXI Encontro Nacional de Engenharia de Produção, Salvador-BA, 2001.

CERVO, A. L.; ERVIAN, P. A. **Metodologia científica**. 5. ed. São Paulo: Pearson Prentice Hall, 2004.

CHAN, Yolande E.; REICH, Blaize Horner. IT alignment: what have we learned?. **Journal of Information technology**, v. 22, n. 4, p. 297-315, 2007.

CHOO, C. W. The management of uncertainty: organizations as decision-making systems. In: **The knowing organizations: how organizations use information to construct meaning, create knowledge, and make decisions**. New York: Oxford University, 1998. p. 155- 205.

COBIT 5: **Modelo Corporativo para Governança e Gestão de TI da Organização** - ISBN 978-1-60420-284-7. 2012. Disponível em: <www.isaca.org/cobit>. Acesso em: 19 jul. 2016.

COHEN, David. Você sabe tomar decisão? **Revista Exame**. São Paulo: Ed. Abril, 2001. Disponível em: <http://exame.abril.com.br/revista-exame/edicoes/746/noticias/voce-sabe-tomar-decisao-m0047648>. Acesso em: 03 jul. 2016.

CORRÊA, Fábio. **Gestão do conhecimento aplicada ao setor de tecnologia da informação**: proposição de um modelo. 2014. 173 f. Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento) – Universidade FUMEC, Belo Horizonte, 2014. Disponível em: <http://www.fumec.br/revistas/sigc/article/view/2553/1624>. Acesso em: 27 ago. 2016.

COSTA, Fernando. Quadrilha especializada em clonagem de cartão e que agia em todo Brasil é presa em BH. **Jornal O Tempo**. 2009. Disponível em: <http://www.otempo.com.br/cidades/quadrilha-especializada-em-clonagem-de-cart%C3%A3o-e-que-agia-em-todo-o-brasil-%C3%A9-presa-em-bh-1.506058>. Acesso em: 09 jun. 2016.

DANTAS, Marcus Leal. **Segurança da informação**: uma abordagem focada em gestão de riscos. Olinda: Ed. Livro Rápido, 2011.

DE SOUZA, Thiago Vieira; DE SOUSA, Marta Alves; DA COSTA, Helder Rodrigues. Boas Práticas ITIL: Estudo de Caso na Implantação das Boas Práticas no Gerenciamento de Mudança.

DELGADO, Maurício Godinho. **Curso de direito do trabalho**. São Paulo: LTR, 2002. Disponível em: <https://pt.scribd.com/doc/75335050/CURSO-DE-DIREITO-DO-TRABALHO-Mauricio-Godinho-Delgado-Completo>. Acesso em: 27 jul. 2016.

DE LIMA BEZERRA, Lindemberg; CACCIAMALI, Maria Cristina. Produtividade e emprego industrial no Brasil. **Revista Brasileira de Economia**, v. 51, n. 1, p. 77-92, 1997. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/rbe/article/view/687/8044>. Acesso em: 09 out. 2016.

ERNST & YOUNG. **O desafio da redução dos gaps de Segurança da Informação - Ideias e informações sobre o risco de TI.** Pesquisa Global de Segurança da Informação. nov. 2012.

FEBRABAN – Federação Brasileira de Bancos. **Destaques de 2014**. Disponível em: <http://relatorioanual.febraban.org.br/pt/03.htm>. Acesso em: 19 maio 2016.

FEBRABAN – Federação Brasileira de Bancos. **Pesquisa FEBRABAN de Tecnologia Bancária 2014**. 2014. Disponível em: <https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20FEBRABAN%20de%20Tecnologia%20Bancaria%202014.pdf>. Acesso em: 08 out. 2016.

FEBRABAN – Federação Brasileira de Bancos. **Bancarização e Inclusão Financeira no Brasil -** FELABAN. Jul. 2011. Disponível em: <https://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/BANCARIZACAO%20-%20III%20Congresso%20Latino%20Americano%20de%20bancarizacao%20e%20Microfinancas%20-%20FELABAN%20-%20JUNHO%202011%20-%20FINAL.pdf>. Acesso em: 19 maio 2016.

FREITAS, Paulo Springer de. Mercado de Cartões de Crédito no Brasil: problemas de regulação e oportunidades de aperfeiçoamento da legislação. **Revista Consultoria Legislativa do Senado Federal**, Brasília, 2007. Disponível em: <http://www2.senado.leg.br/bdsf/bitstream/handle/id/94272/Texto%20p%20discussao%2037.pdf?sequence=5>. Acesso em: 02 jul. 2016.

GEER JR.; HOO, D., K. S.; JAQUITH, A. Information security: why the future belongs to the quants. **IEEE Security & Privacy**, v. 1, n. 4, p. 24-32, Jul/Ago. 2003.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas. 2002.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas. 2008.

GOMES, Carlos F. S.; COSTA, Helder G. C. Aplicação de métodos multicritério ao problema de escolha de modelos de pagamento eletrônico por cartão de crédito. **Produção**, Rio de Janeiro, v. 25, n. 1, p. 54-68, jan/mar. 2015. Disponível em: <http://www.scielo.br/pdf/prod/v25n1/0103-6513-prod-0103-6513-2014-056412.pdf>. Acesso em: 05 maio 2016.

GUIMARÃES, Vera Ap. Lui; HAYASHI, Maria Cristina Piumbato Innocentini; BENZE, Benedito Galvão. Estratégias metodológicas da pesquisa sobre comunicação científica no campo dos estudos sociais da ciência. **Revista Brasileira de Ciência, Tecnologia e Sociedade**, v. 2, n. 1, p. 120-134, jan. 2011.

GUIMARÃES NETO; PESSOA. 1992. In: GOMES, Carlos F. S.; COSTA, Helder G. C. Aplicação de métodos multicritério ao problema de escolha de modelos de pagamento eletrônico por cartão de crédito. **Produção**, Rio de Janeiro, v. 25, n. 1, p. 54-68, jan/mar. 2015. Disponível em: <http://www.scielo.br/pdf/prod/v25n1/0103-6513-prod-0103-6513-2014-056412.pdf>. Acesso em: 05 maio 2016.

HARVEY, D. **A condição pós-moderna**. São Paulo: Loyola, 1992.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION [ISO]. (2009). ISO 31000: **Risk management – Principles and guidelines**. Superseding AS/NZS 4360:2004. Committee OB-007, New Zealand.

ISO 27001. ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação. **Técnicas de segurança** – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2013.

ITGI: Information security gobernance: **Guidance for boards of directors and executive management**. 2. ed., 2006. Disponível em: <http://www.isaca.org/knowledge-center/research/documents/information-security-govenance-for-board-of-directors-and-executive-management_res_eng_0510.pdf>. Acesso em: 20 fev. 2017.

KAPLAN, R. S.; NORTON, D. P. **A estratégia em ação** – balanced scorecard. 4. ed. Rio de Janeiro: Campus, 1997.

LARANGEIRA, Sônia M. G. Reestruturação produtiva no setor bancário: a realidade dos anos 90. **Educação & Sociedade**, v. 18, n. 61, p. 110-138, 1997.

LENTO, Luiz Otávio Botelho; DA SILVA FRAGA, Joni; LUNG, Lau Cheuk. **A nova geração de modelos de controle de acesso em sistemas computacionais**. SBSeg, p. 151-201, 2006.

LONG, Rebecca M. **Using phishing to test social engineering awareness of financial employees**. EWU Masters Thesis Collection. 2013. Disponível em: <http://dc.ewu.edu/theses/156>. Acesso em: 19 jan. 2017.

MANZINI, E. J. A entrevista na pesquisa social. **Didática**, São Paulo, v. 26/27, p. 149-158, 1990/1991.

MARCIANO, João Luiz Pereira. **Segurança da Informação** - uma abordagem social. 2006. 212 f. Tese (Doutorado em Ciência da Informação) - Universidade de Brasília – CID/FACE-UNB, Brasília, 2006.

MAULAIS, Claudio Nunes dos Santos. **Engenharia Social**: Técnica de ataque e defesa em empresas de micro, média e grande porte. 2016. 133f. Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento) - Universidade FUMEC, Belo Horizonte, 2016.

MEDEIROS, Teobaldo Adelino Dantas de. **Utilização do Linux como ferramenta antivírus em redes corporativas**. 2005. 153f. Dissertação de Mestrado. Universidade Federal do Rio Grande do Norte, Natal, 2005.

METCALFE, Bob. Metcalfe's law: A network becomes more valuable as it reaches more users. **Infoworld**, v. 17, n. 40, p. 53-54, 1995.

MORAES, E. M. **Planejamento de Backup de Dados**. 2007. Dissertação (Mestrado em Gestão e Desenvolvimento Regional do Departamento de Economia, Contabilidade e Administração) - Universidade de Taubaté. Taubaté. 2007.

MORESI, Eduardo *et al*. Metodologia da pesquisa. Universidade Católica de Brasília, p. 21, 2003.

MORESI, Eduardo. **Metodologia da Pesquisa**. 2003. Universidade Católica de Brasília – UCB, Pró-Reitoria de Pós-Graduação – PRPG Programa de Pós-Graduação Stricto Sensu Em Gestão do Conhecimento e Tecnologia da Informação. Brasília. Disponível em: <http://s3.amazonaws.com/academia.edu.documents/34168313/MetodologiaPesquisa-Moresi2003.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1494532602&Signature=3AvDI1lQhM33ZeXXD9FXVT3PeOk%3D&response-content-disposition=inline%3B%20filename%3DMetodologia_da_Pesquisa_PRO-REITORIA_DE.pdf >. Acesso em: 09 ago. 2016.

MOTTA, F. C. P. **Teoria das organizações**: evolução e crítica. São Paulo: Pioneira, 1986. p. 112.

NAKAMURA, Emilio Tissato; DE GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos**. Campinas: Novatec Editora, 2007.

NUTT, Paul. C. Formulation tactics and the success of organization decision making. **Decision Sciences**, 1992. Disponível em: <https://www.researchgate.net/publication/229712315_Formulation_Tactics_and_the_Success_of_Organizational_Decision_Making>. Acesso em: 01 jul. 2016.

NUTT, Paul. C. Why decidion fail – avoiding the blunders and traps that lead to debacles. São Francisco – CA, **Berrett-Koehler Publishers**, Inc., 2002. Disponível em: <http://www.bkconnection.com/static/Why_Decisions_Fail_EXCERPT.pdf>. Acesso em: 01 jul. 2016.

OLIVEIRA, Djalma de Pinho Rebouças. **O executivo estadista**: uma abordagem evolutiva para o executivo estrategista e empreendedor. São Paulo: Atlas, 1991.

OLIVEIRA, Rui Manuel Campos. **Contribuição para a estruturação do Sistema Integrado de Gestão do Grupo Cooprofar-Medlog com integração da Gestão de Segurança da Informação**. 2015. 122f. Dissertação (Mestrado em Engenharia e Gestão Industrial) – Universidade Lusíada – Norte, Vila Nova de Famalicão, 2015.

PCI Security Standards Council. Payment Card Industry (PCI) Card Production. **Logical Security Requirements**. v. 1.1. Mar. 2015.

PCI Security Standards Council. PCI Card Production and Provisioning. **Logical Security Requirements**, v 2.0. Jan. 2017.

PCI Security Standards Council. **Sobre o PCI Security Standards Council**. Disponível em: <https://pt.pcisecuritystandards.org/minisite/en/about.php>. Acesso em: 28 jun. 2016.

PEMBLE, Matthew. What do we mean by “information security”?. **Computer fraud & security**, v. 2004, n. 5, p. 17-19, maio 2004.

PINHEIRO, J. M. S. **Projeto de Redes**. 2004. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_modelo_osi.php>. Acesso em: 22 mar. 2017.

PMI – PROJECT MANAGEMENT INSTITUTE. **Um Guia do Conhecimento em Gerenciamento de Projetos**: Guia PMBOK, 5. ed. Pennsylvania. 2013. Disponível em: <www.PMI.org>. Acesso em: 10 jul. 2016.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. 2. ed. Novo Hamburgo, Rio Grande do Sul: Universidade Feevale, 2013.

PTI - Profissionais TI. **Pesquisa Nacional de Segurança da Informação**: Divulgação dos resultados! Disponível em: <https://www.profissionaisti.com.br/2014/11/pesquisa-nacional-de-seguranca-da-informacao-divulgacao-dos-resultados>Acesso em: 09 out. 2016.

RODOV, I.; LELIAERT. P. Fimiam. Financial Method of Intangible Assets Measurement. **Jounal of Intellectual Capital**, v. 3, n. 3, p. 323-336, 2002.

SALLÉ, Mathias. **IT Service Management and IT Governance: review, comparative analysis and their impact on utility computing**. Hewlett-Packard Company, p. 8-17, 2004. Disponível em: <https://pdfs.semanticscholar.org/ddfd/4cb9e0b68b42bfc4600ff4a9454f0f283401.pdf>. Acesso em: 11 abr. 2016.

SANCHES, Ana Tercia. A terceirização diante da noção de trabalhador coletivo em Marx. In: SIMPÓSIO LUTAS SOCIAIS NA AMÉRICA LATINA, v. 3, 2008.

SANCHES, Ana Tercia. **Terceirização e terceirizados no setor bancário**: Relações de emprego, condições de trabalho e ação sindical. 2006. 155 f. Dissertação (Mestrado em ciências Sociais) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2006.

SILVA, Rogerio Geraldo da. A terceirização no Brasil e a Súmula 331 do TST. **Âmbito Jurídico**. Rio Grande, XIV, n. 92, 2011.

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

SIMON, H. A. **The new science of management decision**. New Jersey: Preentice-Hall, 1977.

TARAPANOFF, Kira. **Técnicas para tomada de decisão nos sistemas de informação**. 2 ed. Brasília: Thesaurus, 1995.

TEMPONI, Francisco Paulo. **O comportamento do nível de maturidade em governança de segurança da informação**. 2010. 97 f. Dissertação (Mestrado em administração) - Universidade FUMEC, Belo Horizonte, 2010.

VAN DEN BERG, H. Models of IC valuation: A comparative evaluation. 24th McMaster WORD CONGRESS MANAGEMENT OF INTELLECTUAL CAPITAL AND INNOVATION. 2003.

VERGARA, Sylvia Constant. **Métodos de pesquisa em administração**. São Paulo: Atlas, 2005.

WATSON, Gavin; MASON, Andrew; ACKROYD, Richard. **Social engineering penetration testing: executing social engineering pen tests, assessments and defense**. Syngress, 2014.

YIN, R. **Estudo de caso**: planejamento e métodos. Trad. Daniel Grassi. 2. ed. Porto Alegre: Bookman. 2001.

ZELENY, M. **Multiple criteria decision making**. New York: McGraw-Hill. 1982.

APÊNDICE A – LEVANTAMENTO SISTEMÁTICO

Revisão sistemática: Artigos relacionados à Segurança da Informação, *Payment Card Industry* e Prestação de Serviços Bancários.

Tabela de Revisão sistemática

Autores	Títulos	Relação com o tema abordado
Bispo (1998)	UMA ANÁLISE DA NOVA GERAÇÃO DE SISTEMAS DE APOIO À DECISÃO	Segurança da Informação
Anderson (2001)	WHY WE NEED A NEW DEFINITION OF INFORMATION SECURITY	Segurança da Informação
Anderson, James M. (2003)	WHY WE NEED A NEW DEFINITION OF INFORMATION SECURITY	Segurança da Informação
Geer Jr, Hoo e Jaquith, (2003)	INFORMATION SECURITY: WHY THE FUTURE BELONGS TO THE QUANTS	Segurança da Informação
Pemble (2004)	WHAT DO WE MEAN BY "INFORMATION SECURITY"?.	Segurança da Informação
Marciano, João Luiz Pereira (2006)	SEGURANÇA DA INFORMAÇÃO – UMA ABORDAGEM SOCIAL	Segurança da Informação
Sanches (2006)	TERCEIRIZAÇÃO E TERCEIRIZADOS NO SETOR BANCÁRIO: RELAÇÕES DE EMPREGO, CONDIÇÕES DE TRABALHO E AÇÃO SINDICAL	Segurança da Informação
Temponi, Francisco Paulo (2010)	O COMPORTAMENTO DO NÍVEL DE MATURIDADE EM GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO	Segurança da Informação
Cortez, Igor Siqueira; Kubota, Luis Claudio (2011)	CONTRAMEDIDAS EM SEGURANÇA DA INFORMAÇÃO E VULNERABILIDADE CIBERNÉTICA: EVIDÊNCIA EMPÍRICA DE EMPRESAS BRASILEIRAS	Segurança da Informação
Knorst, André Marcelo; Vanti, Adolfo Alberto; Andrade, Rafael Alejandro Espín; Johann, Silvio Luiz (2011)	ALIGNING INFORMATION SECURITY WITH THE IMAGE OF THE ORGANIZATION AND PRIORITIZATION BASED ON FUZZY	Segurança da Informação

	LOGIC FOR THE INDUSTRIAL AUTOMATION SECTOR	
Riccio, E.L., Sakata, M. C., Valente, N. T. Z. (2011)	RESULTADOS DO 8º CONTECSI – CONGRESSO INTERNACIONAL DE GESTÃO DA TECNOLOGIA E SISTEMAS DE INFORMAÇÃO	Segurança da Informação
Dantas, Marcus Leal (2011)	SEGURANÇA DA INFORMAÇÃO: UMA ABORDAGEM FOCADA EM GESTÃO DE RISCOS	Segurança da Informação
Alencar, Gliner Dias; Anderson, Apolonio Lira Queiroz; Queiroz, Ruy José Guerra Barretto de (2013)	INSIDERS: ANÁLISE E POSSIBILIDADES DE MITIGAÇÃO DE AMEAÇAS INTERNAS	Segurança da Informação
Antonelli, Ricardo Adriano; Almeida, Lauro Brito de; Espejo, Márcia Maria dos Santos Bortolocci; Longhi, Fernanda Luiza (2013)	BUSINESS PROFESSIONALS' PERCEPTIONS RELATED TO THE INFLUENCE OF INFORMATION TECHNOLOGY IN INDIVIDUAL WORK	Segurança da Informação
Wiedenhöft, Guilherme; Klein, Rodrigo Hickmann (2013)	IDENTIFICAÇÃO DE MECANISMOS PARA ATENDER OS OBJETIVOS E PRINCÍPIOS DE GOVERNANÇA DE TI NA VISÃO DE PROFISSIONAIS DA ÁREA	Segurança da Informação
Riccio, Edson Luiz; Gramacho Sakata, Marici Cristine; Zubek Valente, Nelma Terezinha; Capobianco, Ligia (2014)	RESULTADOS DO 11º CONTECSI USP – CONGRESSO INTERNACIONAL DE GESTÃO DA TECNOLOGIA E SISTEMAS DE INFORMAÇÃO	Segurança da Informação
Correia. José Carlos; Joia.Luiz Antonio (2014)	A REPRESENTAÇÃO SOCIAL DAS COMPETÊNCIAS ESSENCIAIS AOS CIOS SOB A PERSPECTIVA DOS PROFISSIONAIS DE TI	Segurança da Informação
Vianna, Eduardo Wallier; Fernandes, Jorge Henrique Cabral (2014)	O GESTOR DA SEGURANÇA DA INFORMAÇÃO NO ESPAÇO CIBERNÉTICO GOVERNAMENTAL: GRANDES DESAFIOS, NOVOS PERFIS E PROCEDIMENTOS	Segurança da Informação

Klumb, Rosangela; Azevedo, Beatriz Marcondes de (2014)	A PERCEPÇÃO DOS GESTORES OPERACIONAIS SOBRE OS IMPACTOS GERADOS NOS PROCESSOS DE TRABALHO APÓS A IMPLEMENTAÇÃO DAS MELHORES PRÁTICAS DE GOVERNANÇA DE TI NO TRE/SC	Segurança da Informação
Oliveira, Rui Manuel Campos (2015)	CONTRIBUIÇÃO PARA A ESTRUTURAÇÃO DO SISTEMA INTEGRADO DE GESTÃO DO GRUPO COOPROFAR-MEDLOG COM INTEGRAÇÃO DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO	Segurança da Informação
Carvalho (2006)	A TRAJETÓRIA DA INTERNET NO BRASIL: DO SURGIMENTO DAS REDES DE COMPUTADORES À INSTITUIÇÃO DOS MECANISMOS DE GOVERNANÇA.	Payment Card Industry
Freitas (2007)	MERCADO DE CARTÕES DE CRÉDITO NO BRASIL: PROBLEMAS DE REGULAÇÃO E OPORTUNIDADES DE APERFEIÇOAMENTO DA LEGISLAÇÃO	Payment Card Industry
Aileen G., Bacudio; Xiaohong Yuan; Bei-Tseng Bill Chu; Monique Jones (2011)	AN OVERVIEW OF PENETRATION TESTING	Payment Card Industry
Chul Ho Lee; Xianjun Geng; Srinivasan Raghunathan (2012)	MANDATORY STANDARDS AND ORGANIZATIONAL INFORMATION SECURITY	Payment Card Industry
Harbauer, Patrick (2013)	DO YOU DUE DILIGENCE WITH THE CLOUD ADN PCI	Payment Card Industry
Rechtman, Yigal; Gabriele. Guido (2013)	TECHNOLOGY, RISK MANAGEMENT, AND THE AUDIT PROCESS MANAGING NEW ACQUISITIONS IN THE RESTARTED ECONOMY	Payment Card Industry
Allassani, William (2014)	DETERMINING FACTORS OF BANK EMPLOYEE READING HABITS OF INFORMATION SECURITY POLICIES	Payment Card Industry

Lincke, Joseph Johnson and Susan J.; Imhof, Ralf; Lim. Charles (2014)	A COMPARISON OF INTERNATIONAL INFORMATION SECURITY REGULATIONS	Payment Card Industry
PCI (2014)	PCI DATA SECURITY STANDARD (PCI DSS)	Payment Card Industry
Santiago, Sandra Dıaz; Henrıquez, Lil Marıa Rodrıguez; Chakraborty, Debrup (2014)	A CRYPTOGRAPHIC STUDY OF TOKENIZATION SYSTEMS	Payment Card Industry
Gomes e Costa (2015)	APLICAÇÃO DE MÉTODOS MULTICRITÉRIO AO PROBLEMA DE ESCOLHA DE MODELOS DE PAGAMENTO ELETRÔNICO POR CARTÃO DE CRÉDITO	Payment Card Industry
Martínez, Josefina Gutiérrez; Gaona, Marco Antonio Núñez; Meneses, Heriberto Aguirre (2015)	BUSINESS MODEL FOR THE SECURITY OF A LARGE-SCALE PACS, COMPLIANCE WITH ISO/27002:2013 STANDARD	Payment Card Industry
PCI (2015)	PAYMENT CARD INDUSTRY (PCI) CARD PRODUCTION. LOGICAL SECURITY REQUIREMENTS	Payment Card Industry
PCI (2017)	PAYMENT CARD INDUSTRY (PCI) CARD PRODUCTION. LOGICAL SECURITY REQUIREMENTS	Payment Card Industry
Clapper, Danial; Richmond, William (2016)	SMALL BUSINESS COMPLIANCE WITH PCI DSS	Payment Card Industry
Such, Jose M.; Gouglidis, Antonios; Knowles, William; Misra, Gaurav; Rashid, Awais (2016)	INFORMATION ASSURANCE TECHNIQUES: PERCEIVED COST EFFECTIVENESS	Payment Card Industry
laranjeira, Sônia M.G. (1997)	REESTRUTURAÇÃO PRODUTIVA NO SETOR BANCÁRIO: A REALIDADE DOS ANOS 90	Prestação de Serviços
Sanches. Ana Tercia (2006)	TERCEIRIZAÇÃO E TERCEIRIZADOS NO SETOR BANCÁRIO: RELAÇÕES DE EMPREGO, CONDIÇÕES DE TRABALHO E AÇÃO SINDICAL	Prestação de Serviços
Sanches, Ana Tercia (2008)	A TERCEIRIZAÇÃO DIANTE DA NOÇÃO DE TRABALHADOR COLETIVO EM MARX	Prestação de Serviços

Luciano, Edimara Mezzomo; Testa, Mauricio Gregianin (2011)	CONTROLES DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO PARA A TERCEIRIZAÇÃO DE PROCESSOS DE NEGÓCIO: UMA PROPOSTA A PARTIR DO COBIT	Prestação de Serviços
Rigolon, Guilherme Jacob; Silveira, Marco Antonio Pinheiro da (2012)	PARTICIPAÇÃO DE TERCEIROS EM EQUIPES DE PROJETOS TI: CONFLITOS E INFLUÊNCIAS NOS RESULTADOS	Prestação de Serviços

APÊNDICE B – ROTEIRO DA ENTREVISTA

A IDENTIFICAÇÃO DOS RESPONDENTES SERÁ PRESERVADA POR QUESTÕES DE SIGILO, CONFORME AS NORMAS DITADAS PELO PCI.

Os profissionais entrevistados serão identificados como Analista-M (Analista de Segurança da informação), Analista-R (Desenvolvedor), Analista-W (Processamento de dados), Coordenador-D (Setor de Personalização), Coordenador-H (Setor de Manuseio e Expedição), Gestora da Qualidade-S, Superintendente-S (CISO) e Diretor-C. Cada um desses profissionais está ligado diretamente às atividades que envolvem o processamento, o manuseio e a personalização dos cartões de pagamento.

A função de CISO é desempenhada pelo Superintendente-S.

Os cargos dos entrevistados estão diretamente ligados à sua nomenclatura de identificação. Todos os entrevistados fazem o uso de recursos tecnológicos para desempenhar suas funções diárias.

No questionário apresentado, serão realizadas perguntas semiestruturadas a respeito de assuntos pertinentes a segurança da informação, tratamento e manuseio de dados confidenciais e a respeito dos processos internos ligados ao setor em que o profissional está inserido. As respostas foram gravadas em áudio para serem analisadas, com autorização dos entrevistados.

As informações providas são absolutamente confidenciais e serão utilizadas exclusivamente para fins desta pesquisa.

É solicitado ao respondente que responda às perguntas da forma mais precisa e sincera possível.

Sobre Segurança da Informação
Você tem conhecimento de que a empresa segue uma série de normas de segurança da informação ditadas por um órgão internacional denominado PCI?
A empresa possui uma política de segurança da informação?
A seu ver, a diretoria entende a importância da criação de uma política de segurança da informação e do cumprimento de suas normas?
A sensibilização sobre as políticas de segurança da informação é promovida pela alta gestão?
A equipe de segurança da informação tem autonomia para atuar em seu escopo de trabalho?

As regras ditadas pela política de segurança da informação são cumpridas?
Prestadores de serviços e terceiros estão cientes e incluídos na política de segurança da informação?
Existe uma programação para treinamentos específicos a respeito dos conceitos e da política de segurança da informação?
Você tem conhecimento de quem é o CISO e de suas responsabilidades?
Você considera necessária a nomeação de um CISO, com autoridade suficiente para criar e fazer cumprir todos os requisitos de segurança lógica da empresa?
Você conhece os conceitos de Engenharia Social no âmbito da Segurança da informação?
A empresa possui um *firewall*?
Existe um plano de revisão e alteração de regras de *firewall* formal?
Sobre Tratamento e manuseio de dados confidenciais
Existe um procedimento para classificação das informações de forma criteriosa?
Você considera o procedimento de classificação das informações pertinente à empresa?
Existem políticas destinadas ao controle de acesso aos dados confidenciais? Como são gerenciados?
Sob o seu ponto de vista, as informações confidenciais recebidas e processadas pela empresa são tratadas conforme a política de segurança da informação?
Você tem conhecimento se a empresa já sofreu algum tipo de fraude eletrônica?
A alta direção é informada sobre qualquer incidente ou comprometimento que envolva as informações confidenciais?
Sobre Processos internos
Você tem conhecimento de todos os processos que envolvem a personalização dos cartões de pagamento?
Como é o fluxo de recebimento e tratamento das informações confidenciais?
Os processos e controles implementados pela segurança da informação têm um impacto direto na produtividade da empresa?

A empresa adotou algum padrão para o desenvolvimento de sistemas?
O CISO acompanha o desenvolvimento, os testes de segurança em códigos fontes e a liberação de aplicativos?
Existe uma preocupação com desenvolvimento seguro de aplicativos?
Qual é a ferramenta utilizada na análise de fontes desenvolvidas internamente? Ela é eficiente?
Existe um plano de treinamento e atualização da equipe de tecnologia?
Os procedimentos e processos internos são padronizados e documentados?
Os procedimentos e processos são revisados periodicamente?
Os documentos relativos aos processos e procedimentos são classificados e publicados conforme as normas de controle de acesso?
Sob seu ponto de vista, qual seria o impacto que um vazamento de informações confidenciais teria sobre a imagem da empresa no mercado em que atua?
A empresa está empenhada em atender a todos os requisitos de segurança da informação exigidos pelas bandeiras?