



FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Raissa Tadeu

RELAÇÃO ENTRE A ISO/IEC 27001 E PCI DSS

Americana, SP.

2018



FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Raissa Tadeu

RELAÇÃO ENTRE A ISO/IEC 27001 E PCI DSS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação Prof. Me. Benedito Aparecido Cruz.
Área de concentração: Segurança da Informação.

Americana, SP.

**FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte**

T128r TADEU, Raissa

Relação entre a ISO/IEC 27001 e PCI DSS. / Raissa Tadeu. –
Americana, 2018.

51f.

Monografia (Curso de Tecnologia em Segurança da Informação) - -
Faculdade de Tecnologia de Americana – Centro Estadual de Educação
Tecnológica Paula Souza

Orientador: Prof. Ms. Benedito Aparecido Cruz

1 Segurança em sistemas de informação I. CRUZ, Benedito
Aparecido II. Centro Estadual de Educação Tecnológica Paula Souza –
Faculdade de Tecnologia de Americana

CDU:681.518.5

Raissa Tadeu

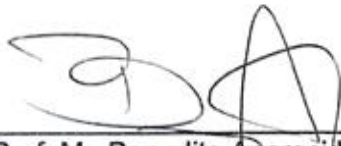
Relação entre a ISO/IEC 27001 e PCI DSS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

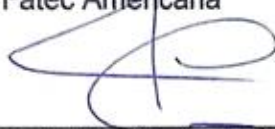
Área de concentração: Segurança da Informação

Americana, 08 de Agosto de 2018.

Banca Examinadora:



Prof. Me Benedito Aparecido Cruz
Fatec Americana



Prof. Ms. Wladimir da Costa
Fatec Americana



Prof. Dr. Renato Kraide Soffner
Fatec Americana

AGRADECIMENTOS

Ao Prof. Benedito Aparecido Cruz pela orientação, compreensão e incentivo dispensado ao desenvolvimento deste trabalho.

Ao Coordenador do curso Wladimir da Costa pelo incentivo e oportunidade.

DEDICATÓRIA

À

Minha Família

Em especial aos meus pais.

RESUMO

Atualmente, um especialista em segurança da informação tem como principal função garantir ao máximo os pilares de segurança da informação, principalmente a confidencialidade, disponibilidade e integridade. O intuito desse trabalho de conclusão de curso é demonstrar a importância da segurança da informação nas empresas que tem como ramo de atividade o comércio eletrônico e que trabalham com a manipulação dos dados dos titulares de cartão, demonstrando os requerimentos de segurança criados pelo *PCI Security Standards Council*, fundado pelas principais bandeiras de cartão American Express, Discover Financial Services, JCB International, MasterCard, e Visa, Inc., denominado PCI DSS e atualmente dividido em 12 requisitos principais. Além dos requisitos estabelecidos pelo PCI DSS, podemos contar com a ajuda da ISO/IEC 27001, norma internacional de gestão de segurança da informação, que possui em grande parte relação direta com o PCI DSS. São confrontadas as principais características dos dois padrões e seus enfoques. Apesar da similaridade dos objetivos, a ISO/IEC 27001 possui uma flexibilidade maior que o PCI DSS devido aos seus controles em alto nível, tornando a sua conformidade mais fácil de ser alcançada. Em relação aos processos, o PCI DSS possui relação direta com 7 cláusulas da ISO/IEC 27001, com notável semelhança nos itens A12 - Segurança nas operações e A13 - Segurança nas comunicações. Analisadas as similaridade entre eles, foi possível relacionar os requisitos e as normas e aplicar o comprovado ciclo de melhoria contínua PDCA (Plan-Do-Check-Act) da ISO/IEC 27001 para auxiliar na conformidade com o PCI DSS, possibilitar a integração de ambas ou utilizar a ISO/IEC 27001 como base para alcançar melhores resultados, tendo em vista que as duas se complementam muito bem.

Palavras Chave: Segurança da Informação; *PCI Security Standards Council*; PCI DSS; ISO/IEC 27001;

ABSTRACT

Nowadays, an information security specialist has as main function to guarantee the maximum of the pillars of information security, mainly confidentiality, availability and integrity. The purpose of this course completion work is to demonstrate the importance of information security in companies that have e-commerce as a branch of activity and that work with the manipulation of cardholder data, demonstrating the security requirements created by PCI Security Standards Council, founded by the leading American Express, Discover Financial Services, JCB International, MasterCard, and Visa, Inc., PCI DSS and currently divided into 12 major requirements. In addition to the requirements established by the PCI DSS, we can count on the help of ISO/IEC 27001, an international information security management standard, which has a direct relationship with the PCI DSS. The main features of the two standards and their approaches are confronted. Despite the similarity of the objectives, ISO/IEC 27001 has greater flexibility than PCI DSS because of its high level controls, making its compliance easier to achieve. Regarding the processes, PCI DSS is directly related to 7 clauses of ISO/IEC 27001, with notable similarity in items A12 - Safety in operations and A13 - Safety in communications. Analyzing the similarities between them, it was possible to relate the requirements and standards and to apply the proven continuous improvement cycle (PDCA) of ISO/IEC 27001 to assist with PCI DSS compliance, to enable the integration of both or use ISO/IEC 27001 as a basis for achieving better results, given that the two complement each other very well.

Keywords: *Information Security; PCI Security Standards Council; PCI DSS; ISO/IEC 27001;*

SUMÁRIO

1. INTRODUÇÃO	9
2. REVISÃO DA LITERATURA	11
2.1 Surgimento do comércio eletrônico	11
2.2 Fraudes envolvendo cartão	14
2.3 Pilares da segurança da informação	18
2.4 Vulnerabilidades	19
3. PCI DSS	22
3.1 PCI SSC	22
3.2 PCI DSS	22
3.3 Os três processos do PCI DSS	23
3.4 Requisitos do PCI DSS	23
3.5 Responsabilidades e Penalidades	28
4. ISO/IEC27001	31
4.1 Estruturas da ISO/IEC 27001	31
4.2 Seções da ISO/IEC 27001	31
4.3 Benefícios ao implantar a ISO/IEC 27001	33
5. RELAÇÃO ENTRE O PCI DSS E A NORMA ISO/IEC 27001	35
5.1 Comparações gerais entre os padrões e seus enfoques	35
5.2 Relação entre os requisitos e normas	37
5.3 Integrações das normas	38
6. CONSIDERAÇÕES FINAIS	42
REFERÊNCIAS BIBLIOGRÁFICAS	44
ANEXO A	47

LISTA DE FIGURAS

Figura 1 - Total de vendas no varejo mundial	12
Figura 2 - Usuários de internet pelo mundo	13
Figura 3 - Tipos de dados em um cartão pagamento.....	16
Figura 4 - Taxas totais de fraude no cartão por país.....	17
Figura 5 - Visão geral de pagamento na própria página	21
Figura 6 - Padrão de segurança de dados do PCI DSS.....	24

LISTA DE TABELAS

Tabela 1 - Lista de multas MasterCard	29
Tabela 2 - Estrutura da norma ISO/IEC 27001.....	31
Tabela 3 - Mapeamento entre PCI DSS e ISO/IEC 27001:2013.....	35
Tabela 4 - Mapeamento de alto nível dos requisitos PCI DSS x ISO/IEC 27001	37
Tabela 5 - Comparação de seções utilizando o Ciclo PDCA.....	39
Tabela 6 - Porcentagem de relação entre processos da ISO/IEC 27001 e requisitos do PCI DSS.....	40

LISTA DE ABREVIATURAS

ISO	<i>International Standardization Organization</i>
PCI	<i>Payment Card Industry</i>
PCI DSS	<i>Payment Card Industry Data Security Standards</i>
PCI SSC	<i>Payment Card Industry Security Standards Council</i>
SGSI	Sistema de Gestão de Segurança da Informação
ABECS	Associação Brasileira das Empresas de Cartões de Crédito

1. INTRODUÇÃO

O comércio eletrônico é um modelo de mercado atrativo e que cresce a ritmos elevados, junto com a democratização do acesso à internet. Por consequência, onde há grande fluxo de informações e transações envolvendo dinheiro, pessoas mal intencionadas procuram brechas a fim de explorar vulnerabilidades e assim obter lucros ilícitos. Algumas empresas tendem a ser mais suscetíveis a exploração destas vulnerabilidades, pois não investem ou simplesmente desconhecem os requisitos de segurança básicos para que possam operar de forma eficiente.

As constantes e numerosas fraudes a partir da utilização do cartão para pagamentos e roubos de identidade, motivaram a criação do PCI DSS – *Payment Card Industry Data Security Standards*, um padrão de requerimentos para todas organizações que transmitem, processem ou armazenem dados sensíveis de cartão com objetivo de promover a privacidade e a confidencialidade destes dados. Atualmente, demonstrar a conformidade com o PCI DSS auxilia no aumento da confiança nas relações comerciais entre empresas e entre empresas e consumidores.

Por outro lado, a ISO/IEC 27001, norma internacional de gestão de segurança da informação, também prevê controles aplicáveis as organizações que necessitam proteger seus dados financeiros e confidenciais.

O objetivo geral deste trabalho é destacar a importância da segurança da informação com foco no ambiente de comércio eletrônico, levantando as normas padrões existentes aplicáveis e recomendados para garantir a confidencialidade, integridade e disponibilidade das informações que transitam nos processos envolvendo pagamento por cartão.

O objetivo específico é realizar uma comparação referente aos padrões ISO/IEC 27001 e PCI DSS e seus enfoques, analisar a relação entre os requisitos e normas destes padrões, e como os dois podem ser utilizados de forma concomitante ou complementares, utilizando alguns processos da ISO/IEC 27001 para atingir a conformidade ao PCI DSS.

O presente trabalho foi estruturado em seis capítulos, organizados da seguinte forma:

O capítulo 2 apresenta uma visão geral do surgimento do comércio eletrônico, as categorias existentes e seu constante crescimento. São descritas as motivações que levam as fraudes especificamente em transações por cartão, apresentando seus dados sensíveis e quais são os fatores suspeitos que podem indicar uma possível fraude. Por fim, traz os conceitos da segurança da informação e das vulnerabilidades, além de exemplificar de acordo com a pesquisa, algumas das vulnerabilidades que expõem e comprometem a segurança da informação relacionadas ao contexto apresentado.

O capítulo 3 apresenta o padrão PCI DSS, como foi criado e quais seus objetivos em resposta a necessidade de promover um ambiente mais seguro para as organizações que lidam com os dados dos portadores de cartão. São descritos seus doze requisitos principais, as classificações a partir dos níveis de transações, além das responsabilidades e penalidades de acordo com as violações.

O capítulo 4 apresenta a norma ISO/IEC 27001, sua estrutura e seções. São mencionados os benefícios da conformidade à norma.

O capítulo 5 trata da relação entre a ISO/IEC 27001 e o PCI DSS, as comparações gerais entre as normas e seus enfoques. São descritos e contrapostos em alto nível seus requisitos e cláusulas, mostrando a possibilidade da integração e como a ISO/IEC 270001 pode auxiliar na conformidade ao PCI DSS.

Por fim, o capítulo 6 traz a conclusão final deste trabalho, mediante as considerações finais.

2. REVISÃO DA LITERATURA

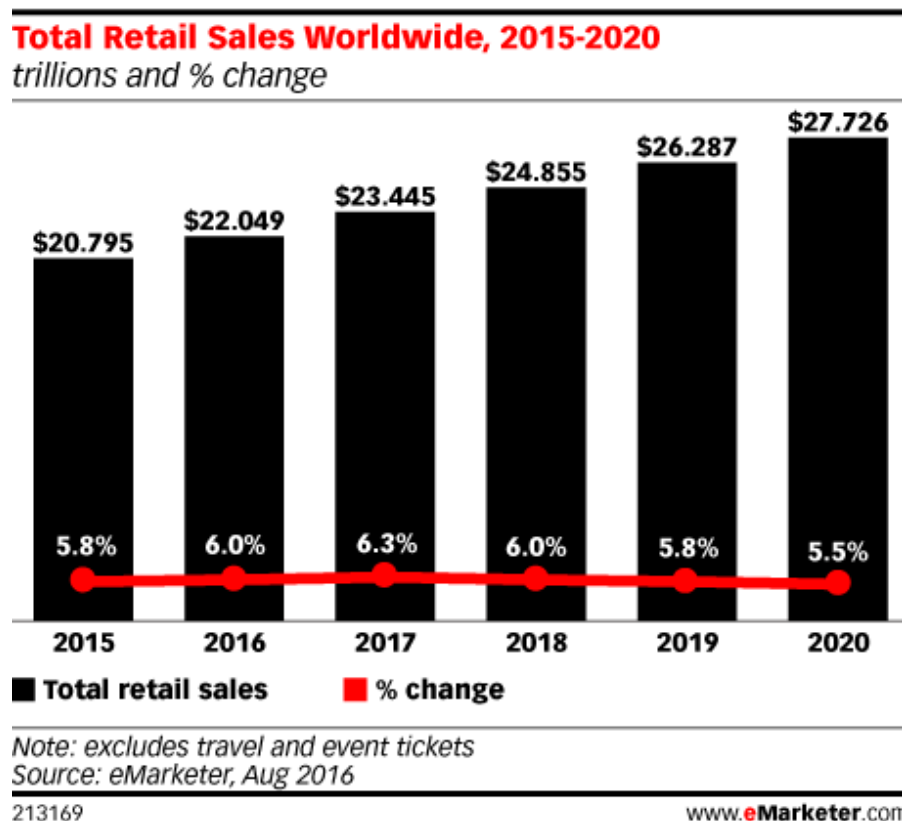
Neste capítulo são apresentados os principais conceitos abordados nesse trabalho, com base na literatura disponível, com objetivo de demonstrar o constante crescimento do comércio eletrônico, a utilização do cartão como forma de pagamento virtual e fatores suspeitos que indicam uma possível fraude, ocasionadas devido ao comprometimento da segurança da informação.

2.1 Surgimento do comércio eletrônico

Segundo Laudon (2011, p. 285), a expressão “comércio eletrônico” se refere às transações comerciais realizadas através da internet e da web, envolvendo saída de dinheiro para aquisição de produtos ou serviços. Seu surgimento deu-se em 1995 através do portal da empresa Netscape com a aceitação de anúncios de grandes corporações, onde a popularização deste tipo de serviço deu oportunidade para que o comércio pela internet pudesse crescer e evoluir de diversas formas.

Atualmente, o comércio eletrônico é a forma de varejo que mais cresce no mundo, segundo estatísticas. Estimativas baseadas em análises de dados, tendências históricas e de receitas relatadas por grandes varejistas (Figura 1) consideram que no ano de 2020 as vendas no varejo mundial cheguem a mais de 27 trilhões de dólares, segundo eMarketer (2017).

Figura 1 - Total de vendas no varejo mundial

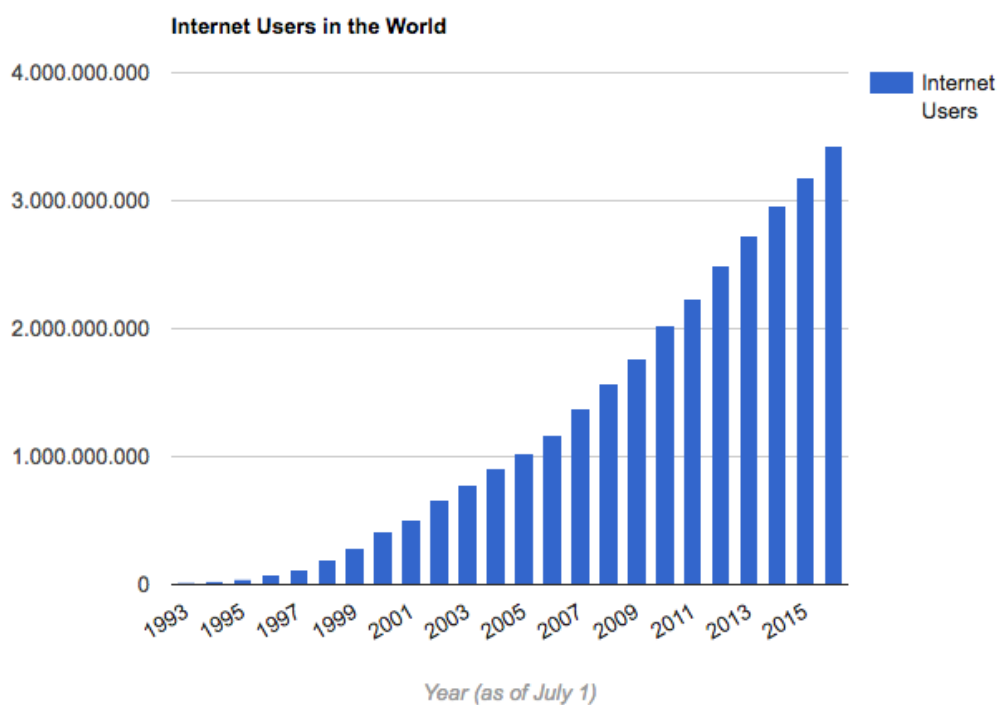


Fonte: eMarketer (2017)

Na visão de Laudon (2011, p. 288), os principais atrativos desta forma de comércio se devem aos custos operacionais reduzidos em comparação ao comércio tradicional, além da ubiquidade, ou seja, a capacidade destas transações serem realizadas além das fronteiras geográficas.

Outros fatores favorecem este crescimento e estão relacionados a popularização da internet, como democratização do acesso à tecnologia, beneficiando o aumento de consumidores e do público geral, cujo crescimento pode ser representado no gráfico a seguir (Figura 2), elaborado pela Internet Live Stats (2017).

Figura 2 - Usuários de internet pelo mundo



Fonte: Internet Live Stats (2017)

Conforme Laudon (2011, p. 295), o comércio eletrônico é classificado de diferentes maneiras de acordo com a natureza dos participantes da transação:

- **Comércio eletrônico empresa-consumidor (B2C):** refere-se a vendas de produtos e serviços diretamente a compradores individuais.
- **Comércio eletrônico empresa-empresa (B2B):** refere-se a vendas de produtos e serviços entre empresas.
- **Comércio eletrônico consumidor-consumidor (C2C):** refere-se a venda eletrônica de bens e serviços por consumidores diretamente a outros consumidores.

2.2 Fraudes envolvendo cartão

De acordo com a Cielo (2018), há alguns anos as fraudes através de cartões de crédito eram mais suscetíveis, isto porque os fraudadores conseguiam copiar as informações da tarja magnética. Após a criação dos cartões com chip a segurança aumentou, reduzindo assim, as fraudes do mundo real. Em meio ao comércio eletrônico, um novo ambiente surgiu e com ele novos desafios, especialmente pelo fato de que as lojas virtuais não conseguem visualizar o cartão e nem seus próprios clientes, e o mais importante, muitas lojas tendem a facilitar as vendas diminuindo os critérios de segurança e validação.

Segundo Tozetto (2015), em matéria para o jornal O Estado de S. Paulo, o cyber crime fez os bancos perderem R\$ 1,8 bilhão. A facilidade ao utilizar dispositivos eletrônicos para realizar pagamentos tem cada vez mais conquistando os clientes dos bancos, porém essa facilidade chamou a atenção também dos cyber criminosos, que descobriram vulnerabilidades nas transações, roubando os dados e até mesmo dinheiro dos clientes.

Para Carrareto (2015) apud Estadão (2015):

“Por mais que os bancos invistam em segurança, ainda há pessoas que caem nesse golpe”, diz o especialista em segurança da informação da Symantec no Brasil, André Carrareto. Cerca de 95% dos ataques virtuais que ocorrem no Brasil tem o objetivo de roubar instituições financeiras locais.”

Um caso famoso de fraude envolvendo cartões de crédito e débito foi organizado por Alberto Gonzalez, um *cracker* de Miami, acusado de premeditar um esquema global para roubar mais de 130 milhões de números de cartões. Através deste esquema, os dados dos cartões roubados foram vendidos *on-line* e utilizados para pagar compras e retiradas bancárias não autorizadas, conforme mostra o estudo de caso abaixo. (Laudon, 2017, p. 224).

O PIOR ROUBO DE DADOS DA HISTORIA

(...) Gonzalez e seus comparsas começaram a realizar seus ataques por *injection* por volta de agosto de 2007. Antes disso, eles invadiram sistemas

corporativos explorando fragilidades de segurança da rede sem fio. Os ladrões dirigiam ao redor dos prédios e varriam as redes sem fio dos varejistas em busca de vulnerabilidades. Em seguida, instalavam *sniffers* que se conectavam as redes de processamento de cartões de crédito, interceptando números de cartões de crédito e débito e números pessoais de identificação.

Em julho de 2005, essas técnicas permitiram que o grupo extraísse mais de 40 milhões de números de cartões de crédito e débito da TJX. A equipe de Gonzalez identificou uma rede vulnerável em uma loja de departamentos da Marshalls, em Miami, e utilizou-a para instalar *sniffers* nos computadores da matriz da cadeia, a TJX. O grupo então conseguiu acessar o banco de dados central da empresa, que armazenava transações dos consumidores de lojas como T.J Maxx, Marshalls, HomeGoods e A.J Wright nos Estados Unidos e em Porto Rico, e das lojas HomeSense, no Canadá.

A TJX ainda utilizava o antigo sistema de criptografia WEP (*wired equivalente privacy*), relativamente fácil de ser quebrado por *hackers*. Outras empresas já tinham mudado para o padrão WPA (*wi-fi protected access*), mais seguro e com criptografia mais complexa; mas, na época, a TJX ainda não havia feito a troca. Mais tarde, um auditor descobriu que a empresa também havia negligenciado a instalação de *firewalls* e criptografia de dados na maioria dos computadores que utilizavam rede sem fio, além de não instalar adequadamente outra camada de software de segurança que havia adquirido.

Em um processo da Comissão de Valores Mobiliários, a TJX admitiu ter transmitido dados de cartões de crédito aos bancos sem criptografia, violando as instruções da própria empresa. A TJX também retinha em seus sistemas os dados dos proprietários dos cartões por muito mais tempo que o estipulado pelas regras do setor para armazenamento de tais informações.

Segundo o PCI SSC (2016), as fraudes com cartão são ocasionadas devido ao roubo e utilização indevida das informações críticas, tais como o número da conta principal (PAN), nome do portador do cartão, validade, código de segurança do cartão (Figura 3), com a finalidade de realizar compras de produtos e serviços acarretando prejuízos financeiros aos portadores e entidades envolvidas.

Figura 3 - Tipos de dados em um cartão pagamento



Fonte: PCI SCC (2016)

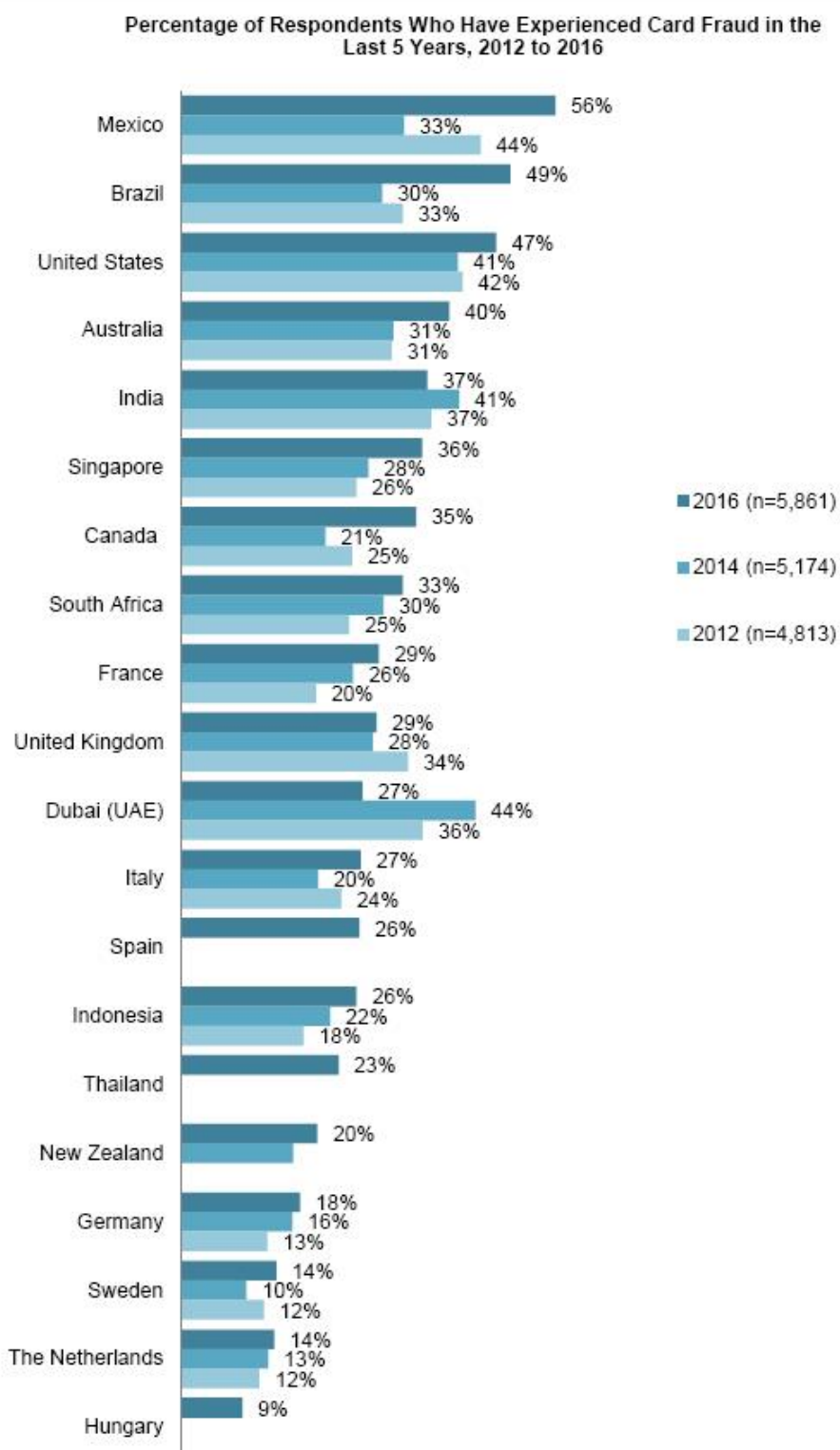
Segundo a Cielo (2018), para os lojistas alguns fatores suspeitos podem ser indicadores de fraudes em transações comerciais eletrônicas, tais como:

- Compras ou tentativas, com cartões diferentes;
- CEP não condiz com a mercadoria comprada;
- Pedidos diferentes para entrega no mesmo endereço;
- Solicitação de quantidades elevadas de um mesmo item;
- Comprador não mostra preocupação com o valor, produto, ou parcelamento do valor.

Segundo a Aite Group (2016), 49% das pessoas no Brasil tiveram alguma experiência com fraudes relacionadas a cartão de crédito, o que coloca o país no segundo lugar do ranking de países, perdendo apenas para o México com 56%, conforme mostra figura a seguir:

Figura 4 - Taxas totais de fraude no cartão por país

Current Total Card Fraud Rates by Country



Fonte: Aite Group (2016)

2.3 Pilares da segurança da informação

Diante ao aumento expressivo no volume de transações comerciais através da internet, aumenta também o interesse de criminosos em buscar meios para que seja possível a prática de seus golpes. Portanto, é necessário que as empresas, aqui representadas por entidades relacionadas a pagamentos por cartão, independentemente de seu porte ou ramo de atividade, estejam devidamente orientadas, conscientizadas e motivadas a manter ambientes preparados contra incidentes de segurança, vulnerabilidades e outras ações que possam afetar ou violar os aspectos básicos da segurança da informação.

Segundo Lyra (2017), ao se referir a segurança da informação, nos referimos a ações para garantir alguns aspectos:

- **Confidencialidade:** capacidade de um sistema de permitir que alguns usuários acessem determinadas informações ao mesmo tempo que impede que outros, não autorizados, a vejam.
- **Integridade:** a informação deve estar correta, ser verdadeira e não estar corrompida.
- **Disponibilidade:** a informação deve estar disponível para todos que precisarem dela para a realização dos objetivos empresariais.
- **Autenticação:** garantir que um usuário é de fato quem alega ser.
- **Não repúdio:** capacidade do sistema de provar que um usuário executou uma determinada ação.
- **Legalidade:** garantir que o sistema esteja aderente a legislação pertinente.
- **Privacidade:** capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações.
- **Auditoria:** capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque.

Todos estes aspectos se referem a segurança do que segundo Lyra (2017), é um bem de grande valor para os processos de negócio. Laudon (2011), define a

informação como dados apresentados em uma forma significativa e útil para os seres humanos, ou seja, mostra em sua própria definição a importância, o valor e a necessidade de proteção e cuidados.

2.4 Vulnerabilidades

Para Semola (2014), vulnerabilidades se tratam de fragilidades à ativos que podem vir a ser exploradas por ameaças, permitindo a ocorrência de incidentes de segurança, comprometendo assim alguns dos princípios da segurança da informação, como a confidencialidade, integridade e disponibilidade. São elementos passivos que, segundo o autor, precisam de agente causador (ameaças) para provocarem um incidente de segurança.

As vulnerabilidades a serem exploradas nas operações do comércio eletrônico podem estar localizadas tanto no computador do comprador, no trânsito das informações, quanto na própria loja virtual, o que engloba seu sistema, infraestrutura e das empresas parceiras. Segundo a ABECS (2012), parte dos ataques contra aplicações web são ocasionadas por brechas de desenvolvimento, vulnerabilidades que expõem a falhas de segurança e entrada de invasores, as quais podem ter origem desde o design até a administração do sistema. São elas:

- **Falhas no design:** São os problemas gerados no planejamento da Aplicação Web, quando estas são desenhadas e desenvolvidas sem que haja uma preocupação adequada com o nível de segurança. Controlar acessos aos aplicativos somente por meio de quais menus cada usuário poderá ver ou as simplificações no acesso a base de dados são exemplos comuns de falhas deste tipo.
- **Falhas na arquitetura:** São as vulnerabilidades associadas à segmentação de redes, implementação de ativos de TI e informações que possam comprometer o ambiente analisado. Manter o banco de dados que suporta um *website* na DMZ possibilitando o acesso remoto externo sem autenticação, é um exemplo comum. É comum ainda a presença de

protocolos de comunicação com falhas que podem ser exploradas para burlar o processo de criptografia estabelecido.

- **Falhas no código:** São as falhas relacionadas à maneira em que as empresas constroem suas aplicações corporativas, frameworks e demais componentes do software. É a camada onde são identificadas as falhas mais comuns.

- **Falhas na administração:** Problemas gerados não pela Aplicação Web em si, mas sim pela forma como ela é administrada onde os conceitos de proteção não são aplicados como esperado. Exemplos comuns ocorrem na remoção de determinados controles previamente planejados, como a mudança de senhas fortes para controles mais fracos a pedido de uma área, para atender a uma necessidade de negócio que não tenha tido o seu nível de risco devidamente avaliado. ABECS (2012).

Segundo o PCI SSC (2016), o comerciante de *e-commerce* que aceita pagamentos na própria página de pagamento e gerencia o próprio site, tem um perfil de risco considerado alto (Figura 5). As vulnerabilidades podem estar no site da loja, mesmo que não capture ou armazene os dados do cartão, em terceiros como hospedagem de *e-commerce*, aplicativos de pagamento, provedor de carrinho de compras, entre outros intermediadores.

Figura 5 - Visão geral de pagamento na própria página



Fonte: PCI SCC (2016)

De acordo com Gasetta (2012):

“Uma organização financeira, por exemplo, tem uma grande preocupação com os riscos associados às fraudes eletrônicas. Estas organizações investem para conhecer estes riscos, avaliar a vulnerabilidade associada a cada um deles e prover medidas para resolvê-los. Uma fraude eletrônica pode comprometer toda a reputação da organização e causar perdas significativas.”

Com intuito de mitigar os riscos que acercam as transações eletrônicas de cartão, alguns padrões de segurança são altamente recomendados e dentro deste contexto, será abordado sobre o PCI DSS no próximo capítulo.

3. PCI DSS

O PCI DSS foi criado para estabelecer o equilíbrio e trazer credibilidade para as informações fornecidas pelos bancos. Neste capítulo são apresentados a fundamentação e os principais fatores que garantem o funcionamento deste processo.

3.1 PCI SSC

O PCI SSC - *Payment Card Industry Security Standards Council* é um fórum aberto global que estabelece o padrão de segurança de dados do setor de cartões de pagamento, denominado PCI DSS - *Payment Card Industry Data Security Standard*. Foi fundado em 2006 pelas principais bandeiras cartão American Express, Discover Financial Services, JCB International, MasterCard, e Visa, Inc. No Brasil, conta atualmente com 15 empresas em seu conselho de engajamento. PCI SSC (2018).

Segundo a ABECS (2012), as principais ações geradas pelo PCI SSC incorporam:

- **Fundamentação Técnica:** Requerimentos para armazenamento, processamento e transmissão segura de dados do portador.
- **Metodologias de Testes:** Procedimentos comuns de auditoria, testes de vulnerabilidades e questionário de autoavaliação.

3.2 PCI DSS

O objetivo principal do PCI DSS é estabelecer as melhores práticas de segurança para a indústria que armazena, processa e transmite dados de portadores de cartão, a partir de 12 requisitos principais. Estes requisitos por sua vez, visam proteger e diminuir brechas no acesso a dados sensíveis de consumidores que conseqüentemente podem acarretar perda de dinheiro, reputação

e confiança dos envolvidos. Atualmente, o PCI DSS está na versão 3.2 lançada em abril de 2016.

3.3 Os três processos do PCI DSS

Segundo o PCI SSC (2016), a conformidade com o PCI DSS é um processo contínuo, realizado em três etapas:

- **Avaliar:** Identificar os dados do portador do cartão, fazer um inventário de ativos de TI e processos de negócios para processamento de cartões de pagamento e analisá-los em busca de vulnerabilidades que possam expor os dados do portador do cartão.
- **Corrigir:** Corrigir vulnerabilidades e eliminar o armazenamento de dados do portador do cartão, a menos que seja absolutamente necessário.
- **Relatar:** Enviando relatórios necessários para o banco adquirente apropriado e marcas de cartões.

3.4 Requisitos do PCI DSS

Segundo o PCI DSS (2016), os requisitos de segurança se aplicam a todos os componentes de sistema, que são definidos como qualquer componente de rede (firewalls, chaves, roteadores, pontos de acesso wireless, mecanismos de rede e outros mecanismos de segurança), servidores (web, aplicativo, banco de dados, autenticação, e-mail, proxy, NTP, DNS) ou aplicativos (adquiridos ou personalizados, internos ou externos) que tenham vínculo ao ambiente de dados do titular do cartão.

Figura 6 - Padrão de segurança de dados do PCI DSS

Padrão de segurança de dados do PCI – Visão geral alto nível	
Construir e manter a segurança de rede e sistemas	<ol style="list-style-type: none"> 1. Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão 2. Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança
Proteger os dados do titular do cartão	<ol style="list-style-type: none"> 3. Proteger os dados armazenados do titular do cartão 4. Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas
Manter um programa de gerenciamento de vulnerabilidades	<ol style="list-style-type: none"> 5. Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus 6. Desenvolver e manter sistemas e aplicativos seguros
Implementar medidas rigorosas de controle de acesso	<ol style="list-style-type: none"> 7. Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio 8. Identificar e autenticar o acesso aos componentes do sistema 9. Restringir o acesso físico aos dados do titular do cartão
Monitorar e testar as redes regularmente	<ol style="list-style-type: none"> 10. Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão 11. Testar regularmente os sistemas e processos de segurança
Manter uma política de segurança de informações	<ol style="list-style-type: none"> 12. Manter uma política que aborde a segurança da informação para todas as equipes

Fonte: PCI DDS v3.2

Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão

Segundo o PCI DSS (2016):

“Um firewall examina todo o tráfego da rede e bloqueia aquelas transmissões que não atendem aos critérios de segurança específicos. Todos os sistemas devem ser protegidos do acesso não autorizado de redes não confiáveis, seja acessando o sistema por meio da internet como e-commerce, acesso à internet através dos navegadores na área de trabalho por parte dos funcionários, acesso via e-mail dos funcionários, conexão dedicada como conexões entre negócios, por meio de redes sem fio ou de outras fontes. Com frequência, trajetos aparentemente insignificantes que direcionam ou partem de redes não confiáveis podem fornecer caminhos não protegidos aos sistemas principais. Os firewalls são um mecanismo de proteção essencial para qualquer rede de computador.”

Requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança

De acordo com o PCI DSS (2016), as senhas e configurações padrão comprometem a segurança pois “são bastante conhecidas pelas comunidades de hackers e facilmente determinadas por meio de informações públicas.”

Requisito 3: Proteger os dados armazenados do titular do cartão

Segundo o PCI DSS (2016):

“Métodos de proteção como criptografia, truncamento, mascaramento e codificação Hash são componentes essenciais para proteção de dados do titular do cartão. Se um invasor burlar outros controles de segurança e obtiver acesso aos dados criptografados, sem as chaves criptográficas adequadas, os dados estarão ilegíveis e inutilizáveis para aquele indivíduo. Outros métodos eficientes de proteção dos dados armazenados também devem ser considerados como oportunidades potenciais de minimização dos riscos. Por exemplo, os métodos para minimizar riscos incluem não armazenar dados do titular do cartão, a menos que seja absolutamente necessário, truncar dados do titular do cartão se o PAN completo não for necessário e não enviar PAN usando tecnologias de mensagens ao usuário final, como e-mails e mensagens instantâneas.”

Requisito 4: Criptografar a transmissão de dados do titular do cartão em redes abertas e públicas

De acordo com o PCI DSS (2016), configurações incorretas em redes wireless, vulnerabilidades na criptografia herdada e nos protocolos de autenticação são exploradas por indivíduos mal-intencionados com objetivo de obter acesso aos ambientes de dados do titular do cartão. Por conta disso, o padrão recomenda uso de protocolos de criptografia e de segurança para a transmissão por redes abertas e públicas.

Requisito 5: Proteja todos os sistemas contra softwares prejudiciais e atualize regularmente programas ou software de antivírus

O padrão PCI DSS tem como requisito número 5 a implementação de softwares antivírus para todos os sistemas que podem ser afetados por *malware*, ou seja, softwares mal intencionados que incluem vírus, *worms*, e cavalos de troia, que podem por sua vez, ter acesso a rede a partir de e-mails e uso da internet, dispositivos móveis e de armazenamento.

Requisito 6: Desenvolver e manter sistemas e aplicativos seguros

A intenção deste requisito segundo o próprio PCI DSS (2016) é que as empresas utilizem os *patches* de segurança de software adequados e recentes disponibilizado pelos fornecedores, de modo estarem protegidos contra a exploração de vulnerabilidades que expõem ou permitem acesso privilegiado aos sistemas por indivíduos sem escrúpulos.

Requisito 7: Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio

Segundo o PCI DSS (2016):

“Para assegurar que os dados críticos possam ser acessados somente por uma equipe autorizada, os sistemas e processos devem estar implementados para limitar o acesso com base na necessidade de divulgação e de acordo com as responsabilidades da função. A “necessidade de divulgação” é quando os direitos de acesso são concedidos somente ao menor número possível de dados e privilégios necessários para realizar um trabalho.”

É necessário ressaltar que neste aspecto, o risco é maior quando a conta de um usuário é utilizada de forma inadequada, por isso recomenda-se que o menor número de pessoas tenha acesso aos dados dos titulares de cartão.

Requisito 8: Identifique e autentique o acesso aos componentes do sistema

Como um complemento ao requisito anterior, o PCI DSS recomenda também que cada pessoa exclusivamente tenha um acesso específico e próprio, o qual será responsabilizado por suas ações, denominado identificação exclusiva (ID). Sendo assim, “uma organização consegue manter a responsabilidade individual pelas ações e uma trilha de auditoria eficaz por funcionário. Isso ajudará a apressar a resolução e a contenção de problemas quando ocorrer mau uso ou tentativa mal-intencionada. (PCI DSS, 2016)”

Requisito 9: Restringir o acesso físico aos dados do titular do cartão

No requisito 9, o PCI DSS aborda sobre os controles de acesso:

“Qualquer acesso físico aos dados ou sistemas que armazenam dados do titular do cartão fornecem a oportunidade para as pessoas acessarem dispositivos ou dados e removerem sistemas ou cópias impressas, e deve ser restrito de forma adequada. Para as finalidades do Requisito 9, "funcionário" refere-se a funcionários que trabalham em período integral e meio-período, funcionários e equipes temporárias, e prestadores de serviços e consultores que atuem com presença física no endereço da entidade. Um "visitante" refere-se a um fornecedor, convidado de um funcionário, equipes de serviço ou qualquer pessoa que precise adentrar as dependências por um breve período, normalmente um dia, no máximo. "Mídia" refere-se a todas as mídias em papel ou eletrônicas que contêm dados do titular do cartão.”

Requisito 10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão

Para o PCI DSS (2016):

“Mecanismos de registro e a capacidade de monitorar as atividades dos usuários são fundamentais na prevenção, detecção ou minimização do impacto do comprometimento dos dados. A presença de registros em todos os ambientes permite o monitoramento, o alerta e a análise completa quando algo dá errado. Determinar a causa de um comprometimento é muito difícil, se não impossível, sem registros das atividades do sistema.”

O padrão recomenda que sejam implementadas trilhas de auditoria com o objetivo de vincular todos os acessos dos usuários efetuados aos componentes do sistema.

Requisito 11: Testar regularmente os sistemas e processos de segurança

De acordo com o PCI DSS (2016):

“As vulnerabilidades estão sendo continuamente descobertas por indivíduos mal-intencionados e pesquisadores, e são apresentadas por novos softwares. Os componentes do sistema, processos e softwares personalizados devem ser testados com frequência para assegurar que os controles de segurança continuem refletindo um ambiente em

transformação.”

Neste requisito, são recomendações do PCI DSS a implementação de procedimentos a resposta de incidentes caso haja a detecção de pontos de acesso sem fio não autorizados, pois “a implementação e/ou exploração de tecnologia sem fio dentro de uma rede é um dos caminhos mais comuns para usuários mal-intencionados obterem acesso a rede e aos dados do titular do cartão.” PCI DSS (2016).

Requisito 12: Manter uma política que aborde a segurança das informações para todas as equipes.

De acordo com o PCI DSS (2016):

“Uma política de segurança sólida determina o tom da segurança para toda a empresa e informa aos funcionários o que é esperado deles. Todos os funcionários devem estar cientes da confidencialidade dos dados e de suas responsabilidades para protegê-los [...]”

3.5 Responsabilidades e Penalidades

Para Shier (2014), pequenos comerciantes são os principais alvos de ladrões de dados, e o dever de proteger os dados do portador do cartão é de sua responsabilidade. Se os dados do titular do cartão forem roubados, há chances de multas, penalidades, mesmo extinção do direito de aceitar cartões de pagamento em seu comércio, além de custos de substituição do cartão, auditorias forenses, danos à marca, a revogação de privilégios e outras penalidades. A seguir está uma tabela que representa a lista de multas da MasterCard:

Tabela 1 - Lista de multas MasterCard

Lista de multas MasterCard		
Violação	Comerciantes Nível 1 e 2	Comerciantes Nível 3 e 4
Primeira violação	Valor da multa: até US \$ 25.000	Valor da multa: até US \$ 10.000
Segunda violação	Valor da multa: até US \$ 50.000	Valor da multa: até US \$ 20.000
Terceira violação	Valor da multa: até US \$ 100.000	Valor da multa: até \$ 40.000
Quarta violação	Valor da multa: até US \$ 200.000	Valor da multa: Até \$ 80.000

Fonte: Próprio autor apud. Shier, 2014

De acordo com Rouse (2015), a classificação dos comerciantes é realizada a partir de níveis (de 1 a 4), que determina o risco e nível apropriado de segurança para seus negócios. Especificamente, os níveis do comerciante determinam a quantidade de avaliação e validação de segurança necessária para o comerciante aprovar a avaliação do PCI DSS.

Nível 1: Qualquer comerciante, independentemente do canal de aceitação, processando mais de 6.000.000 de transações por ano.

Nível 2: 1 milhão - 6 milhões de transações Visa ou MasterCard anualmente (todos os canais).

Nível 3: Comerciantes que processam 20.000 a 1 milhão de transações de comércio eletrônico Visa ou MasterCard anualmente.

Nível 4: Menos de 20.000 transações de e-commerce Visa ou MasterCard anualmente e todos os outros comerciantes processando até 1 milhão de transações Visa ou MasterCard anualmente. (Rouse, 2015).

Para Shier (2014), com um pouco de esforço inicial e custo, aplicar os processos e andar em conformidade com o PCI pode ajudar a reduzir os riscos. As

multas não irão eliminar as vulnerabilidades por completo, porém vão motivar os comerciantes a adotar o padrão, principalmente para aqueles que não podem se dar ao luxo de pagar multas e custos associados ao processo.

Para Blount (2010), à medida que a tecnologia avança, os criminosos também avançam e encontram maneiras de contornar os sistemas de segurança e obter acesso não autorizado às informações confidenciais. No entanto, o PCI DSS dificulta a sua ação e ajuda a reduzir o risco para as empresas. À medida que o padrão evolui, as organizações também terão que evoluir e ajustar-se para garantir que seus sistemas e controles sejam seguros o suficiente para processar transações e manter os dados do cliente em segurança.

4. ISO/IEC27001

A ISO/IEC27001 é a norma internacional de gestão de segurança da informação, descrevendo como colocar em prática um sistema de gestão de segurança da informação (SGSI) avaliado e certificado de forma independente. Isso permite que as organizações protejam seus dados financeiros e confidenciais de maneira mais eficiente, minimizando os riscos e vulnerabilidades, conforme BSI - *British Standards Institution* (2018).

4.1 Estruturas da ISO/IEC 27001

De acordo com a norma ISO/IEC 27001 (2013), sua estrutura é dividida em 11 seções e Anexo A, onde as seções de 0 a 3 são introdutórias (e não são obrigatórias para a implementação), enquanto as seções de 4 a 10 são obrigatórias.

Tabela 2 - Estrutura da norma ISO/IEC 27001

ESTRUTURA DA NORMA	
ISO/IEC 27001:2013	
P	4 - Contexto da Organização
	5 - Liderança
	6 - Planejamento
D	7 - Suporte
	8 - Operação
C	9 - Avaliação do Desempenho
A	10 - Melhoria

Fonte: Próprio Autor *apud* ISO/IEC 27001

4.2 Seções da ISO/IEC 27001

Seção 0: Introdução - propósito e compatibilidade com outras normas de gestão.

Seção 1: Escopo - aplicável a qualquer tipo de organização.

Seção 2: Referência normativa – refere-se a ISO / IEC 27000 como uma norma onde termos e definições são dadas.

Seção 3: Termos e definições – novamente, refere-se a ISO / IEC 27000.

Seção 4: Contexto da organização – é parte da etapa de planejamento (Plan) do ciclo PDCA e define requisitos para o entendimento de assuntos externos e internos, partes interessadas e seus requisitos, e a definição do escopo do SGSI.

Seção 5: Liderança – também é parte do planejamento (Plan) do ciclo PDCA e define as responsabilidades da Alta Direção, estabelecendo papéis e responsabilidades.

Seção 6: Planejamento – (Plan) do ciclo PDCA, define requisitos para a avaliação de risco, tratamento de risco, plano de tratamento de risco, e define os objetivos de segurança da informação.

Seção 7: Suporte – esta seção é parte da etapa de execução (Do) do ciclo PDCA e define requisitos de disponibilidade de recursos, competências, conscientização, comunicação e controle de documentos e registros.

Seção 8: Operação – esta seção também é parte da etapa execução (Do) do ciclo PDCA e define a avaliação e tratamento de risco, além de controle e processos para garantir a segurança.

Seção 9: Avaliação do Desempenho – esta seção é parte da etapa verificação (Check) do ciclo PDCA e define requisitos para o monitoramento, medição, análise, avaliação, auditoria interna e análise crítica.

Seção 10: Melhoria – esta seção é parte da etapa de atuação (Act) do ciclo PDCA e define requisitos para não conformidades, ações corretivas e melhoria contínua.

Anexo A – Disponibiliza um catálogo de 114 controles (salvaguardas) distribuídos em 14 seções. (Anexo A). LEAL (2017) *apud* ISO/IEC 27001 (2013).

4.3 Benefícios ao implantar a ISO/IEC 27001

Para Leal (2017), existem inúmeros benefícios de negócio que uma organização pode atingir com a implementação desta norma de segurança da informação:

- **Conformidade com requisitos legais** – existem cada vez mais leis, regulamentações e requisitos contratuais relacionados a segurança da informação que podem ser resolvidas com a implementação da ISO/IEC 27001.
- **Reduzir custos** – a principal filosofia da ISO/IEC 27001 é prevenir incidentes de segurança de ocorrerem; e cada incidente, sendo este grande ou pequeno custa dinheiro.
- **Melhor organização** - Encoraja as organizações a escrever seus principais processos possibilitando a elas reduzir a perda de tempo de seus empregados, auxiliando nos processos o que precisa ser feito, quando e por quem. (Leal, 2017)

O padrão tem sido amplamente percebido como referência em excelência em segurança da informação e uma estrutura de processos para governança de segurança da informação. A norma ISO/IEC 27001 é aplicável a uma ampla variedade de sistemas de informação, identificando controles de segurança de maneira genérica (independente de tecnologia) e definindo um processo baseado em risco para a seleção sistemática de controles de segurança que são baseados no resultado de processos de avaliação de risco e gerenciamento de risco. Provavelmente, o ponto mais importante na implementação da ISO/IEC 27001 é a definição de escopo que representa parte do negócio que é realmente o assunto de certificação. Uma empresa pode licenciar processos, sistemas ou organização, dependendo de suas necessidades.

Para Kosutic (2017), a ISO/IEC 27001 dá uma visão geral perfeita de quais controles as organizações podem aplicar, dando flexibilidade para as organizações escolherem quais requisitos e controles são aplicáveis e trarão benefícios a organização, (em muitos casos, até 90% dos controles são aplicáveis); os demais são declarados não aplicáveis.

5. RELAÇÃO ENTRE O PCI DSS E A NORMA ISO/IEC 27001

5.1 Comparações gerais entre os padrões e seus enfoques

O principal objetivo do padrão PCI DSS, é definir requerimentos de segurança para as entidades que armazenam, processam ou transmitam dados dos titulares de cartão e que tem por finalidade reduzir os riscos de ataques, comprometimento das informações e fraudes. Por outro lado a ISO/IEC 27001, um padrão internacional também com objetivo de definir um conjunto de diretrizes, processos e controles relacionados a segurança da informação, em busca de mitigar e gerir os riscos da organização. Apesar da semelhante busca pela segurança da informação, várias diferenças são inicialmente notadas comparando os dois padrões, como mostra a tabela a seguir:

Tabela 3 - Mapeamento entre PCI DSS e ISO/IEC 27001:2013

Mapeamento entre PCI DSS e ISO/IEC 27001:2013		
Parâmetro	ISO/IEC 27001	PCI DSS
Criador	ISO	PCI Council
Flexibilidade	Alta	Baixa
Escopo	Depende da companhia	Informações dos titulares de cartão
Aplicação dos controles	Flexível	Não flexível
Controles	Alto-nível	Baixo nível
Tipo de controle	Sugestivos	Obrigatórios
Conformidade	Fácil	Difícil
Numero de controles	114	224
Auditoria	Auditoria em ciclos de três anos e small-scope a cada ano	Quatro auditorias de varredura de rede e uma auditoria no local para o nível 1
Certificação	Pode ser benéfica para várias empresas	Qualquer empresa que lide com processos críticos de pagamento
Nível de conformidade	Não existe	Existe

Fonte: Próprio autor apud. Mataracioglu (2016).

Para Mataracioglu (2016), a ISO/IEC 27001 é mais flexível em relação ao PCI DSS pois os controles foram escritos em alto nível. Realizando uma comparação inicial em relação ao escopo dos dois padrões, o autor descreve que na ISO/IEC 27001 a seleção do escopo é escolhida a partir de cada empresa, já no PCI DSS, o

escopo será sempre as informações do titular do cartão, com a diferença que seus controles são obrigatórios e não somente recomendações.

Para Gorge (2009), com o PCI DSS, a indústria de pagamentos mapeou os riscos em torno do processamento, transmissão e armazenamento de transações de pagamentos e dados associados. Embora cada organização tenha sua própria infraestrutura e os desafios de segurança associados, os riscos podem ser categorizados com auxílio de controles presentes na ISO/IEC 27001. Alguns controles do PCI DSS são bem específicos, porém na grande maioria, a norma ISO/IEC 27001 abrange todo escopo, direcionando de forma geral as melhores práticas de segurança.

Para Mataracioglu (2016) apud Brecht e Nowey (2012), comparando os custos, estabelecer um sistema de gerenciamento de segurança da informação (SGSI), contemplando todo o ciclo PDCA (nativo na norma ISO/IEC 27001) custa aproximadamente US\$ 150,000 em uma organização típica. O custo de um ciclo típico de PDCA inclui:

- Os custos que são causados por incidentes de segurança da informação
- Os custos de gerenciamento da segurança da informação
- Os custos relacionados a medidas de segurança da informação
- Os custos de capital induzidos pelo risco de segurança da informação

No entanto, o custo de conformidade com o PCI DSS é de aproximadamente US\$ 120,000 a US \$ 700,000 por tratar-se de requisitos mais específicos. Toda via, para empresas que estão iniciando um plano estratégico de certificação PCI DSS, utilizar o ciclo PDCA estabelecido pelas seções da norma ISO/IEC 27001 como plano de melhoria contínua pode trazer grandes ganhos a um baixo custo. Mataracioglu (2016).

5.2 Relação entre os requisitos e normas

Mataracioglu (2016) realizou um mapeamento em alto nível dos 12 requisitos do PCI DSS, em relação aos processos similares existentes nas normas da ISO/IEC 27001:2013, como mostra a tabela a seguir:

Tabela 4 - Mapeamento de alto nível dos requisitos PCI DSS x ISO/IEC 27001

Mapeamento de alto nível dos requisitos PCI DSS para ISO/IEC 27001	
Requisitos PCI DSS	Cláusulas ISO/IEC 27001
1. Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão	A.12 Segurança nas operações A.13 Segurança nas comunicações
2. Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança	A.12 Segurança nas operações A.13 Segurança nas comunicações
3. Proteger os dados armazenados do titular do cartão	A.12 Segurança nas operações A.13 Segurança nas comunicações
4. Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas	A.14 Aquisição, desenvolvimento e manutenção de sistemas
5. Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus	A.14 Aquisição, desenvolvimento e manutenção de sistemas
6. Desenvolver e manter sistemas e aplicativos seguros	A.14 Aquisição, desenvolvimento e manutenção de sistemas
7. Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio	A.12 Segurança nas operações A.13 Segurança nas comunicações
8. Identificar e autenticar o acesso aos componentes do sistema	A.12 Segurança nas operações A.13 Segurança nas comunicações
9. Restringir o acesso físico aos dados do titular do cartão	A.11 Segurança física e do ambiente
10. Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão	A.12 Segurança nas operações A.13 Segurança nas comunicações
11. Testar regularmente os sistemas e processos de segurança	A.14 Aquisição, desenvolvimento e manutenção de sistemas A.6 Organização da Segurança da Informação A.18 Conformidade
12. Manter uma política que aborde a segurança da informação para todas as equipes	A.5 Políticas de Segurança da Informação
Fonte: Tolga Mataracioglu	

Fonte: Mataracioglu (2016).

Nota-se a relação direta entre os requisitos do PCI DSS e 7 cláusulas da ISO/IEC 27001, sendo estas: A12 Segurança nas operações, A13 Segurança nas comunicações, A14 Aquisição, desenvolvimento e manutenção de sistemas, A11 Segurança física e do ambiente, A6 Organização da Segurança da Informação, A18 Conformidade e por fim, A5 Políticas de Segurança da Informação.

Para Blount (2010), os requisitos mais aplicáveis da ISO/IEC 27001 ao PCI DSS são aqueles relacionados a comunicações, gerenciamento de operações, controle de acesso e aquisição de sistemas de informação, desenvolvimento e manutenção.

5.3 Integrações das normas

Para Blount (2010), um padrão com um design específico como o PCI DSS deve ser usado em conjunto com um padrão de segurança, como a ISO/IEC 27001 para obter com sucesso um Sistema de Gerenciamento de Segurança da Informação (SGSI) forte e efetivo que ofereça facilidade em quais controles estão em vigor e sendo gerenciados. Além disso, o grande ganho é garantir a melhoria contínua eficaz comprovada no ciclo PDCA (Plan-Do-Check-Act) existente na ISO/IEC 27001.

De acordo com Segovia (2015):

“Uma das coisas mais importantes que a ISO/IEC 27001 possui, e a PCI-DSS não, é o PDCA (Plan, Do, Check, Act), que é estabelecido em qualquer sistema de gestão baseado na ISO. Assim, tenha em mente que a ISO/IEC 27001 é melhor para aquelas organizações onde já existe um Sistema de gestão, e que querem complementá-lo com a segurança da informação (ou não possuem um sistema de gestão e o querem para proteger a informação), enquanto a PCI-DSS é mais adequada, e obrigatória, para aquelas organizações que trabalham com cartões de crédito.”

Para Segovia (2015), é possível implementar a ISO/IEC 27001 e PCI-DSS na mesma organização sem nenhum problema. Integrar ambas as normas pode trazer grandes ganhos, consolidar um sistema de gestão com controles de segurança genéricos, e também controles específicos para ambientes de cartões de crédito. Desta forma, uma vez que os controles de ambas as normas são similares, a integração fica mais acessível. As seções e requisitos entre as duas normas podem se relacionar de acordo com o ciclo PDCA a seguir:

Tabela 5 - Comparação de seções utilizando o Ciclo PDCA

Ciclo	ESTRUTURA DA NORMA	ESTRUTURA DA NORMA
	ISO 27001:2013	PCI DSS 3.2
P	Seção 4 - Contexto da Organização	Construir e Manter a segurança de rede e sistemas. Requisitos 1 e 2
	Seção 5 – Liderança	Proteger os dados do titular do cartão. Requisitos 3 e 4
	Seção 6 - Planejamento	
D	Seção 7 - Suporte	Manter um programa de gerenciamento de vulnerabilidades Requisitos 5 e 6
	Seção 8 - Operação	Programar medidas rigorosas de controle de acesso Requisitos 7, 8 e 9
C	Seção 9 - Avaliação do Desempenho	Monitorar e testar as redes regularmente Requisitos 10 e 11
A	Seção 10 - Melhoria	Manter uma política de Segurança da Informação Requisito 12

Fonte: Próprio Autor

Segundo o PCI DSS (2016), um programa formal de conformidade com o PCI DSS deve estar no local para incluir definição de atividades para manutenção e monitorar a conformidade geral do PCI DSS, incluindo atividades de negócio, além disso, processos anuais de avaliação e validação contínua de requisitos (por exemplo: diariamente, semanalmente, trimestralmente, etc. conforme aplicável por exigência). O programa de conformidade com o PCI DSS pode ser um programa dedicado ou abrangente, e deve incluir uma metodologia bem definida que demonstra avaliação consistente e eficaz, como exemplo a ISO/IEC 27001.

De acordo com Srivastav (2014), o padrão ISO/IEC 27001 é uma referência para a excelência em segurança da informação e estrutura de processo para governança. A norma é aplicável a uma gama muito ampla de sistemas de informação, identificando os controles de segurança de maneira genérica (independente de tecnologia) e definindo um processo baseados no resultado da avaliação de risco e gestão de risco. Processos e escopo são os pontos mais importantes na implementação da ISO/IEC 27001, as normas contribuem para nível de maturidade de segurança da informação, e para uma empresa que possui um

tipo de serviço de *e-commerce* em sua carteira de serviços, é recomendado utilizar os processos da norma ISO/IEC 27001 para alcançar a conformidade em PCI DSS.

Conforme Froud (2013), a porcentagem de relação entre os processos da ISO/IEC 27001 e os requisitos do PCI DSS podem ser expressados na tabela abaixo:

Tabela 6 - Porcentagem de relação entre processos da ISO/IEC 27001 e requisitos do PCI DSS

Controle ISO/IEC 27001:2013	Porcentagem de relação com o PCI DSS V3.2
A.5 Políticas de Segurança da Informação	100%
A.6 Organização da Segurança da Informação	51%
A.7 Segurança dos Recursos Humanos	37%
A.8 Gerenciamento de Ativos	40%
A.9 Controle de Acesso	73%
A.10 Criptografia	50%
A.11 Segurança Física e Ambiental	28%
A.12 Segurança de Operações	59%
A.13 Segurança de comunicações	43%
A.14 Aquisição, Desenvolvimento e Manutenção de Sistemas	51%
A.15 Relacionamentos com fornecedores	24%
A.16 Gerenciamento de Incidentes de Segurança da Informação	46%
A.17 Aspectos de segurança da informação do gerenciamento de continuidade de negócios	15%
A.18 Conformidade	43%

Fonte: Próprio autor Apud Froud (2013).

Para Froud (2013), há uma relação direta entre os requisitos específicos do PCI DSS e a norma ISO/IEC 27001, que por sua vez é mais abrangente. As organizações que possuem conformidade a ISO/IEC 27001 conseguem atender em alto nível os requisitos do PCI DSS, mesmo que não em sua totalidade devido as especificações relacionadas as transações eletrônicas e processos de pagamento por cartão.

De acordo com o PCI DSS (2016), um conjunto mínimo de requisitos para proteger os dados do portador do cartão pode ser aperfeiçoado por controles e práticas adicionais para amenizar ainda mais os riscos, como exemplo a ISO/IEC 27001, leis locais, regionais e do setor. Além disso, os requisitos legais ou regulatórios podem exigir proteção específica de informações dos usuários, como exemplo dados pessoais. Os controles gerais das normas e os específicos do PCI DSS se aplicam a todas as entidades envolvidas nos processos de pagamento do cartão.

6. CONSIDERAÇÕES FINAIS

Com o aumento exponencial do comércio através da internet é indispensável o entendimento dos riscos das organizações e a conscientização da importância da segurança da informação. A internet transformou as relações de consumo, abrindo portas para um novo mercado onde grandes volumes de informações pessoais transitam diariamente e chamam a atenção de criminosos, especialmente quando estes dados são de pagamentos por cartão.

Em 2006, foi fundado o PCI DSS, um padrão de segurança de dados para a indústria de pagamentos por cartões, com o intuito de promover 12 requisitos técnicos e operacionais que abrangem desde a configuração de firewalls, instruções para armazenamento e criptografia de dados, políticas de segurança entre outras metodologias, incluindo ferramentas de testes de vulnerabilidades e avaliação da segurança.

Devido a alta complexidade em atender as conformidades do padrão PCI DSS em sua totalidade, por definir diretrizes bem específicas dos processos técnicos e operacionais relacionados as transações eletrônicas de pagamento por cartão, foi realizado um estudo em comparação com as normas da ISO/IEC 27001, padrão reconhecido internacionalmente também responsável por promover diretrizes relacionadas a segurança da informação em sistemas de gerenciamento.

Foram levantadas algumas diferenças principais nos tipos de controles e aplicação dos requisitos, onde no PCI DSS estes são específicos e obrigatórios, e na ISO/IEC 27001 são abrangentes e flexíveis. Essa diferença torna a ISO/IEC 27001 mais adaptável para as empresas que estão iniciando um processo de conformidade relacionado a segurança da informação.

Em comparação aos requisitos do PCI DSS e as normas da ISO/IEC 27001, o PCI DSS possui relação à 7 cláusulas da ISO/IEC 27001, sendo estas: A12 - Segurança nas operações, A13 - Segurança nas comunicações, A14 - Aquisição, desenvolvimento e manutenção de sistemas, A11 - Segurança física e do ambiente, A6 - Organização da Segurança da Informação, A18 - Conformidade e por fim, A5 -

Políticas de Segurança da Informação, sendo que grande parte destas cláusulas possuem mais de 50% de relação direta. Os requisitos que mais se aproximam se referem a segurança nas operações, segurança nas comunicações, controle de acesso e política de segurança da informação.

Por conta da notável semelhança, muitas organizações podem trabalhar utilizando ambas as normas de forma concomitante, o que ajudará a entender melhor seus riscos e ameaças e oferecer um ambiente com mais segurança para que não sofra as penalidades impostas ou que tenha as relações de confiança abaladas devido a fraudes e incidentes. Portanto, as duas normas podem ser utilizadas em conjunto para obter maior êxito nos controles e seu gerenciamento. Aplicar o ciclo de melhoria contínua PDCA (Plan-Do-Check-Act) da ISO/IEC 27001 para auxiliar na conformidade com o PCI DSS, torna os processos objetivos, estabelecendo padrões na entrega e avaliação dos resultados com maior clareza.

Embora o PCI DSS e a ISO/IEC 27001 tenham controles gerais e específicos, cada organização pode adaptar seus processos de forma que garanta a segurança e proteção dos dados sensíveis dos clientes utilizando como base os requerimentos estabelecidos por ambas as normas.

REFERÊNCIAS BIBLIOGRÁFICAS

ABECS – ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE CARTÕES DE CREDITO E SERVIÇOS. 2012, **Guia de boas práticas de segurança para e-commerce**. Disponível em:

<http://www.abecs.org.br/app/webroot/files/media/c/f/2/e365deca93d1f6e7dfaa9317f9a28.pdf>. Acesso em: 21 de março de 2017.

AITE GROUP, **2016 Global Consumer Card Fraud: Where Card Fraud Is Coming From**, Gráfico das Fraudes, 2016, Disponível em: <https://www.aciworldwide.com/-/media/files/collateral/trends/2016-global-consumer-card-fraud-where-card-fraud-is-coming-from.pdf>

BLOUNT, Monika, **Compliance Standards in Data Security**, 2010, Georgia Institute of Technology College of Computing & eFortresses Inc.

BRECHT e NOWEY, 2012, **A Closer Look at Information Security Costs, working paper, The Workshop on the Economics of Information Security**, www.econinfosec.org/archive/weis2012/papers/Brecht_WEIS2012.pdf

BSI, British Standards Institution, **ISO-IEC-27001-Seguranca-da-Informacao**, 2018, Disponível em: <https://www.bsigroup.com/pt-BR/ISO-IEC-27001-Seguranca-da-Informacao/> Acessado em 08 em julho de 2018.

CARRARETO, André, Jornal O Estado de S. Paulo, 2015, **Cibercrime faz bancos perderem R\$ 1,8 bilhão**, Disponível em: <http://link.estadao.com.br/noticias/cultura-digital,cibercrime-faz-bancos-perderem-r-18-bilhao,10000028721> Acessado em 08 em julho de 2018.

CIELO, 2018, **Dicas preventivas para vendas mais seguras**. Disponível em: https://cieloecommerce.cielo.com.br/Backoffice/Areas/Merchant/Content/documents/Dicas_preventivas_para_vendas_mais_seguras.pdf. Acesso em: 10 de julho de 2018

EMARKETER, 2017, **Total Retail Sales Worldwide, 2015-2020 (trillions and % change)**. Disponível em: <https://www.emarketer.com/Chart/Total-Retail-Sales-Worldwide-2015-2020-trillions-change/194243>>. Acessado em: 28 de maio de 2017.

FROUD, David, 2013, **PCI DSS vs ISO27001**. Disponível em: http://www.davidfroud.com/wp-content/uploads/2013/06/PCI-DSS-v3.2-vs-ISO-27001-2013_160729.xlsx Acessado em: 20 de julho de 2018.

GASETA, Edson Roberto. **Fundamentos de governança de TI**. Pág 8, 1° ed. Rio de Janeiro. Brasil. Rede nacional de ensino RNP. 2012.

GORGE, Mathieu, **Does using ISO 27000 to comply with PCI DSS make for better security?**, 2009, Disponível em: <https://searchcompliance.techtarget.com/tip/Does-using-ISO-27000-to-comply-with-PCI-DSS-make-for-better-security/> Acessado em 15/07/2018.

INTERNET LIVE STATS. 2017, **Internet Users**. Disponível em: <http://www.internetlivestats.com/internet-users/>. Acesso em: 04 de junho de 2017.

ISO 27001, **O que é a norma ISO 27001?**, 2013, Disponível em: <https://www.27001.pt/index.html> Acessado em 08 em julho de 2018.

ISO/IEC 27001:2013, **International Organization for Standardization**, 2013.

KOSUTIC, Dejan, **Visão geral do anexo A da ISO 27001**. 2018, Disponível em: <https://advisera.com/27001academy/pt-br/knowledgebase/visao-geral-do-anexo-a-da-iso-270012013/> Acessado em 09 em julho de 2018.

LAUDON, Kenneth. **Sistemas de Informação Gerenciais**. 9ª edição. São Paulo: Editora Pearson, 2011.

LEAL, Rhand, **O que é a iso 27001**, 2018, Disponível em: <https://advisera.com/27001academy/pt-br/o-que-e-a-iso-27001/> Acessado em 08 em julho de 2018.

LYRA, Mauricio Rocha. **Segurança e Auditoria e Sistemas de Informação**. 2ª edição. Rio de Janeiro: Editora Ciência Moderna, 2017.

MATARACIOGLU, Tolga, 2016, **Comparison of PCI DSS and ISO IEC 27001** Disponível em: https://www.isaca.org/Journal/archives/2016/Volume-1/Documents/Comparison-of-PCI-DSS-and-ISO-IEC-27001-Standards_joa_Eng_0116.pdf Acessado em: 10 de julho de 2018.

PCI DSS. Payment Card Industry, 2016. **A Abordagem Priorizada para Buscar a Conformidade do PCI DSS**, Versão 3.2.1. Disponível em: https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2_ptBR.pdf. Acessado em: 29 de abril de 2018.

PCI DSS. Payment Card Industry, 2016. **Data Security Standard – Requirements and Security Assessment Procedures**, Versão 3.2.1. Disponível em: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_3_pt-BR.pdf. Acesso em: Maio de 2018.

PCI SSC, 2016 **Guia para pagamentos seguros – Recursos de proteção de pagamentos para pequenos comerciantes. Versão 1.0.**, Disponível em:

https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments-GEN_ptBR.pdf. Acessado em: 10 de julho de 2018.

PCI SSC, 2018 **PCI SSC Brazil Regional Engagement Board**, Disponível em: https://pt.pcisecuritystandards.org/get_involved/regional_engagement_board. Acessado em: 10 de julho de 2018.

ROUSE, Margaret, 2015, **PCI DSS merchant levels**, Disponível em: <https://searchsecurity.techtarget.com/definition/PCI-DSS-merchant-levels> Acessado em 07/07/2018.

SEGOVIA, Antonio Jose, 2015, **PCI-DSS vs. ISO 27001 Parte 1 e 2 – Similaridades e Diferenças** - Advisera Expert Solution, disponível em: <https://advisera.com/27001academy/pt-br/knowledgebase/pci-dss-vs-iso-27001-parte-1-similaridades-e-diferencas/?icn=free-knowledgebase-27001&ici=top-pci-dss-vs-iso-27001-parte-1-similaridades-e-diferencas-txt> Acessado em 08/07/2018

SEMOLA, Marcos. **Gestão da Segurança da Informação**. 2ª edição. Rio de Janeiro - RJ: Elsevier Brasil, 2014.

SHIER, John, 2014, **PCI DSS - Why It Works** - Site <https://nakedsecurity.sophos.com/pt/2014/04/23/pci-dss-why-it-works/> Acessado em 08/07/2018.

SRIVASTAV, Abhishek e col, 2014, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), **A Simple Prototype for Implementing PCI DSS by Using ISO 27001 Frameworks**, Disponível em: <http://www.ijarcsse.com/> Acessado em 15/07/2018.

TOZETTO, Claudia, jornal O Estado de S. Paulo, 2015, **Cibercrime faz bancos perderem R\$ 1,8 bilhão**, Disponível em: <http://link.estadao.com.br/noticias/cultura-digital,cibercrime-faz-bancos-perderem-r-18-bilhao,10000028721> Acessado em 08 em julho de 2018.

ANEXO A

Controles

A.5 Políticas de Segurança da Informação

A.5.1 Direção de gerenciamento para segurança da informação

A.5.1.1 Políticas para segurança da informação

A.5.1.2 Revisão das políticas de segurança da informação

A.6 Organização da Segurança da Informação

A.6.1 Organização Interna

A.6.1.1 Funções e responsabilidades de segurança da informação

A.6.1.2 Segregação de deveres

A.6.1.3 Contato com as autoridades

A.6.1.4 Contato com grupos de interesse especiais

A.6.1.5 Segurança da informação no gerenciamento de projetos

A.6.2 Dispositivos Móveis e Teletrabalho

A.6.2.1 Política de dispositivo móvel

A.6.2.2 Teletrabalho

A.7 Segurança dos Recursos Humanos

A.7.1 Antes do Emprego

A.7.1.1 Triagem

A.7.1.2 Termos e condições de emprego

A.7.2 durante o emprego

A.7.2.1 Responsabilidades de gestão

A.7.2.2 Conscientização, educação e treinamento em segurança da informação

A.7.2.3 Processo disciplinar

A.7.3 Rescisão e mudança de emprego

A.7.3.1 Rescisão ou mudança de responsabilidades de emprego

A.8 Gerenciamento de Ativos

A.8.1 Responsabilidade pelos Ativos

A.8.1.1 Inventário de ativos

A.8.1.2 Propriedade de ativos

A.8.1.3 Uso aceitável de ativos

A.8.1.4 Devolução de ativos

A.8.2 Classificação da Informação

A.8.2.1 Classificação da informação

A.8.2.2 Rotulagem da informação

- A.8.2.3 Movimentação de ativos
- A.8.3 Manuseio de Mídia
 - A.8.3.1 Gerenciamento de mídia removível
 - A.8.3.2 Descarte de mídia
 - A.8.3.3 Transferência de mídia física

A.9 Controle de Acesso

- A.9.1 Requisitos comerciais do controle de acesso
 - A.9.1.1 Política de controle de acesso
 - A.9.1.2 Acesso a redes e serviços de rede
- A.9.2 Gerenciamento de acesso do usuário
 - A.9.2.1 Registro do usuário e cancelamento de registro
 - A.9.2.2 Provisionamento de acesso do usuário
 - A.9.2.3 Gestão de direitos de acesso privilegiado
 - A.9.2.4 Gerenciamento de informações de autenticação secreta de usuários
 - A.9.2.5 Revisão dos direitos de acesso do usuário
 - A.9.2.6 Remoção ou ajuste de direitos de acesso
- A.9.3 Responsabilidades do usuário
 - A.9.3.1 Uso de informações de autenticação secreta
- A.9.4 Sistema e Controle de Acesso ao Aplicativo
 - A.9.4.1 Restrição de acesso à informação
 - A.9.4.2 Procedimentos seguros de logon
 - A.9.4.3 Sistema de gerenciamento de senhas
 - A.9.4.4 Uso de programas utilitários privilegiados
 - A.9.4.5 Controle de acesso ao código-fonte do programa

A.10 Criptografia

- A.10.1 Controles Criptográficos
 - A.10.1.1 Política sobre o uso de controles criptográficos
 - A.10.1.2 Gerenciamento de chaves

A.11 Segurança Física e Ambiental

- A.11.1 Áreas Seguras
 - A.11.1.1 perímetro de segurança física
 - A.11.1.2 Controles de entrada física
 - A.11.1.3 Protegendo escritórios, salas e instalações
 - A.11.1.4 Protegendo contra ameaças externas e ambientais
 - A.11.1.5 Trabalhando em áreas seguras
 - A.11.1.6 Áreas de entrega e carregamento
- A.11.2 Equipamento

- A.11.2.1 Localização e proteção do equipamento
- A.11.2.2 Utilitários de suporte
- A.11.2.3 Segurança de cabeamento
- A.11.2.4 Manutenção de equipamentos
- A.11.2.5 Remoção de ativos
- A.11.2.6 Segurança de equipamentos e ativos fora da premissa
- A.11.2.7 Descarte seguro ou reutilização de equipamentos
- A.11.2.8 Equipamento de usuário desacompanhado
- A.11.2.9 Limpar a política de mesa e limpar a tela

A.12 Segurança de Operações

- A.12.1 Procedimentos Operacionais e Responsabilidades
 - A.12.1.1 Procedimentos operacionais documentados
 - A.12.1.2 Gerenciamento de mudanças
 - A.12.1.3 Gerenciamento de capacidade
 - A.12.1.4 Separação de ambientes de desenvolvimento, teste e operação
- A.12.2 Proteção contra Malware
 - A.12.2.1 Controles contra malware
- A.12.3 Backup
 - A.12.3.1 Backup de informações
- A.12.4 Logging and Monitoring
 - A.12.4.1 Registro de Eventos
 - A.12.4.2 Proteção de informações de log
 - A.12.4.3 Registros de administrador e operador
 - A.12.4.4 Sincronização do relógio
- A.12.5 Controle de Software Operacional
 - A.12.5.1 Instalação de software em sistemas operacionais
- A.12.6 Gerenciamento Técnico de Vulnerabilidades
 - A.12.6.1 Gerenciamento de vulnerabilidades técnicas
 - A.12.6.2 Restrições à instalação de software
- A.12.7 Considerações sobre Auditoria de Sistemas de Informação
 - A.12.7.1 Controles de auditoria de sistemas de informação

A.13 Segurança de comunicações

- A.13.1 Gerenciamento de segurança de rede
 - A.13.1.1 Controles de rede
 - A.13.1.2 Segurança de serviços de rede
 - A.13.1.3 Segregação em redes
- A.13.2 Transferência de Informações
 - A.13.2.1 Políticas e procedimentos de transferência de informações

- A.13.2.2 Acordos sobre transferência de informação
- A.13.2.3 Mensagens eletrônicas
- A.13.2.4 Acordos de confidencialidade ou não divulgação

A.14 Aquisição, Desenvolvimento e Manutenção de Sistemas

- A.14.1 Requisitos de segurança dos sistemas de informação
 - A.14.1.1 Análise e especificação de requisitos de segurança da informação
 - A.14.1.2 Protegendo serviços de aplicativos em redes públicas
 - A.14.1.3 Protegendo transações de serviços de aplicativos
- A.14.2 Segurança em processos de desenvolvimento e suporte
 - A.14.2.1 Política de desenvolvimento segura
 - A.14.2.2 Procedimentos de controle de mudança do sistema
 - A.14.2.3 Revisão técnica de aplicativos após mudanças na plataforma operacional
 - A.14.2.4 Restrições às mudanças nos pacotes de software
 - A.14.2.5 Princípios seguros de engenharia de sistemas
 - A.14.2.6 Ambiente de desenvolvimento seguro
 - A.14.2.7 Desenvolvimento terceirizado
 - A.14.2.8 Teste de segurança do sistema
 - A.14.2.9 Teste de aceitação do sistema
- A.14.3 Dados de Teste
 - A.14.3.1 Proteção de dados de teste

A.15 Relacionamentos com fornecedores

- A.15.1 Segurança da Informação nas Relações com Fornecedores
 - A.15.1.1 Política de segurança da informação para relacionamentos com fornecedores
 - A.15.1.2 Abordar a segurança dentro dos acordos com fornecedores
 - A.15.1.3 Cadeia de suprimentos de tecnologia da informação e comunicação
- A.15.2 Gerenciamento de entrega de serviços de fornecedores
 - A.15.2.1 Monitoramento e revisão de serviços de fornecedores
 - A.15.2.2 Gerenciando mudanças nos serviços do fornecedor.

A.16 Gerenciamento de Incidentes de Segurança da Informação

- A.16.1 Gerenciamento de informações Incidentes de segurança e melhorias
 - A.16.1.1 Responsabilidades e procedimentos
 - A.16.1.2 Relatando eventos de segurança da informação
 - A.16.1.3 Relatando Fraquezas da Segurança da Informação
 - A.16.1.4 Avaliação e decisão sobre eventos de segurança da informação
 - A.16.1.5 Resposta a incidentes de segurança da informação
 - A.16.1.6 Aprendendo com incidentes de segurança da informação
 - A.16.1.7 Recolha de provas

A.17 Aspectos de segurança da informação do gerenciamento de continuidade de negócios

A.17.1 Continuidade da Segurança da Informação

A.17.1.1 Planejando a continuidade da segurança das informações

A.17.1.2 Implementação da continuidade da segurança da informação

A.17.1.3 Verificar, revisar e avaliar a continuidade da segurança das informações

A.17.2 Redundancies

A.17.2.1 Disponibilidade de facilidades de processamento de informação

A.18 Conformidade

A.18.1 Conformidade com os requisitos legais e contratuais

A.18.1.1 Identificação da legislação aplicável e requisitos contratuais

A.18.1.2 Direitos de propriedade intelectual

A.18.1.3 Proteção de registros

A.18.1.4 Privacidade e proteção de informações pessoalmente identificáveis

A.18.1.5 Regulamentação de controles criptográficos

A.18.2 Revisões de Segurança da Informação

A.18.2.1 Revisão independente da segurança da informação

A.18.2.2 Conformidade com políticas e padrões de segurança

A.18.2.3 Revisão de conformidade técnica