JULIANA MANUELA SEMEÃO DOS REIS

# ESTUDO PRÁTICO SOBRE A COMBINAÇÃO DAS NORMAS ISO 27001 E PCI DSS NOS PROCESSOS DE CARTÃO DE CRÉDITO

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para conclusão do curso de MBA em Tecnologia da Informação.

São Paulo
2011

JULIANA MANUELA SEMEÃO DOS REIS

# ESTUDO PRÁTICO SOBRE A COMBINAÇÃO DAS NORMAS ISO 27001 E PCI DSS NOS PROCESSOS DE CARTÃO DE CRÉDITO

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para a conclusão do curso de MBA em Tecnologia da Informação.

Área de Concentração: Tecnologia da Informação

Orientador: Prof. Dr. Reginaldo Arakaki.

São Paulo
2011

## FICHA CATALOGRÁFICA



Reis, Juliana Manuela Semeão dos

Estudo prático sobre a combinação das normas ISO 27001 e PCI DSS nos processos de cartão de crédito / J.M.S. dos Reis. -- São Paulo, 2011.

57 p.

Monografia (MBA em Tecnologia da Informação) - Escola Politécnica da Universidade de São Paulo. Programa de Educação Continuada em Engenharia.

1. Cartão de crédito 2. Garantia da qualidade 3. Normas técnicas I. Universidade de São Paulo. Escola Politécnica. Programa de Educação Continuada em Engenharia II. .

## AGRADECIMENTOS

Ao meu orientador Prof. Dr. Reginaldo Arakaki pela sua atenção e pelas diretrizes precisas e indispensáveis para elaboração desse trabalho.

Aos meus familiares e amigos pela paciência, apoio e compreensão pelos momentos de ausência.

## RESUMO

Este estudo apresenta a combinação entre as normas de segurança PCI DSS e ISO/IEC 27001, aplicada especificamente em empresas de operação de cartão de crédito. As operações de cartão de crédito são divididas em três partes: consumidor, emissor e adquirente. Esta última será área explorada desse trabalho onde serão apresentados os benefícios dessa combinação e o resultado dessa análise a partir dos principais desafios para manter conformidade de segurança da informação. Considerando a afirmação de vários autores de que em segurança da informação nada é totalmente seguro, muitas das ações para inibir ou evitar o vazamento de informações são decorrentes de melhorias nos processos de tratamento das informações sensíveis nas organizações e também da necessidade de programas de conscientização constantes, pois por mais automatizados que estejam os processos, sempre existirá o elemento humano, manipulando e até mesmo vazando as informações corporativas (Da Silva, 2007). Buscando respaldar este estudo foi realizado um mapeamento dos requisitos das duas normas dentro do cenário proposto, a fim de obter um processo mais completo atingindo a conformidade dos processos de segurança.

## ABSTRACT

This paper presents the combination of the PCI DSS security standards and ISO/IEC 27001, applied specifically to Credit Card Company. The credit card transactions are divided into three parts: consumer, issuer and acquirer. The last one is the area explored in this work that will present the benefits of this combination and the outcome of this analysis from the main challenges to maintain information security compliance. Regarding the statement made by several authors that nothing is completely safe in information security, many of the actions to inhibit or prevent information leaks are a result of improvements in procedures of handling sensitive information in organizations and also the need for constant awareness programs because, even they are automated processes, the human element will always exist, manipulating and even leaking corporate information (Da Silva, 2007). Aiming to back up this paper, the requirements of the two standards within the proposed scenario was mapped, in order to obtain an effective process of reaching compliance security processes.

## LISTA DE ILUSTRAÇÕES

## LISTA DE TABELAS

## LISTA DE ABREVIATURAS E SIGLAS

Adquirente/ Acquirer - é a empresa responsável pela comunicação da transação entre estabelecimento e a bandeira, além de realizar a afiliação, gestão do meio de captura, liquidação de pagamento e antecipação de recebíveis do lojista.

Bandeira - é a empresa que fornece serviços a consumidores e estabelecimentos.

Chargeback – é o cancelamento de uma venda feita com cartão de débito ou crédito, que pode acontecer por dois motivos: um deles é o não reconhecimento da compra por parte do titular do cartão, e o outro pode se dar pelo fato da transação não obedecer às regulamentações previstas nos contratos, termos, aditivos e manuais editados pelas administradoras.

Emissor - é a instituição financeira do portador do cartão e também um membro licenciado pela bandeira.

IST/Switch - é o gerenciador de mensageria financeira de meios eletrônicos de pagamento, atuando entre as pontas (ATMs, POS, PDVs, etc). Gerencia autenticações, autorizações, validações e procedimentos de segurança.

Patch - é um programa para corrigir problemas ou atualizar um programa de computador.

PCI DSS – é um padrão de segurança para proteção de dados de cartão de pagamento.

PCI SSC – é um fórum aberto global para contínuo desenvolvimento, aprimoramento, armazenamento, disseminação e implementação de padrões de segurança para a proteção de dados de cartão.

PED - Pin Entry Devices: é um dispositivo com funcionalidades criptográficas para garantir a segurança sistema de pagamentos eletrônicos.

QSAs – Avaliadores de Segurança Qualificados: as empresas qualificadas pelo conselho PCI para validar a aderência de uma entidade para o PCI DSS.

SAQ – PCI DSS Self-Assessment Questionnaire: ferramenta de validação destinada a auxiliar estabelecimento e prestadores de serviço na auto-avaliação da sua conformidade com o Payment Card Industry Data Security Standard.

SGSI – Sistema de Gerenciamento da Segurança da Informação.

URA – Unidade de resposta audível: trate-se de um aparelho utilizado por empresas de atendimento ao cliente para que possam ser digitadas opções no atendimento eletrônico.

# SUMÁRIO

# 1. INTRODUÇÃO

Na era da inteligência de negócios, as informações corporativas devem estar disponíveis, organizadas e seguras. A informação é um dos ativos mais valiosos da organização e a forma como a informação é transmitida e guardada se transformou com a tecnologia, gerando velocidade e facilidade ao acesso. Até pouco tempo, as informações se encontravam em sua maioria escrita em documentos, livros e guardadas na memória de seus conhecedores. Hoje, nos deparamos com informações armazenadas digitalmente, podendo ser publicadas e acessadas em segundos. As organizações estão conectadas através de redes de dados e os dispositivos de acesso estão cada vez mais modernos, facilitando a utilização por um número cada vez maior de pessoas. Com isso, a informação perdeu barreiras físicas de acesso e ficou disponível a todos que possuem acesso às redes digitais de compartilhamento (Sêmola, 2003).

Dessa mudança, novos riscos surgiram ameaçando a segurança das informações nas organizações, como por exemplo: erros nos sistemas de processamento de dados, fraudes, espionagem, atos de vandalismo eletrônico, vírus de computadores etc.

## 1.1 Motivações

Nos últimos onze anos, houve uma explosão de negócios via Internet, e-commerces, na mesma proporção que aumentou o uso de cartões de crédito para compras em estabelecimentos comerciais e, consequentemente nos sites de internet (Falsarella, 2009). Apesar de todos os esforços das empresas em proteger as informações de clientes, fraudes eletrônicas e roubos de informações tem aumentado drasticamente.

Atualmente, as empresas não se sentem seguras com suas próprias políticas de gestão de risco. De acordo com pesquisa feita pela Symantec (Symantec, 2010), 69 por cento das companhias esperam ter um incidente de TI de pequenas proporções uma vez por mês; 63 por cento esperam uma falha de

grandes proporções pelo menos uma vez por ano; 26 por cento esperam um incidente relacionado a regulamentações, mas não ligado à compliance, pelo menos uma vez por ano e 25 por cento esperam, anualmente, um incidente com perda de dados. A mesma pesquisa, feita com mais de 400 profissionais de TI de todo o mundo, diz que muitas empresas parecem estar falhando ao implementar controles fundamentais para o gerenciamento de risco e segurança da informação.

## 1.2 Objetivo

O objetivo da pesquisa é realizar um estudo prático sobre a combinação de requisitos do PCI DSS (Padrão se Segurança de Dados) com as recomendações da norma ISO/IEC 27001, fortalecendo as melhores práticas e políticas de segurança, e aplicar no processo na indústria financeira, mais especifica em operações de cartão de crédito.

## 1.3 Justificativas

O foco principal do trabalho é ressaltar os requisitos PCI DSS e as recomendações definidos na norma ISO/IEC 27001 para tratar questões de segurança específico em empresas de operações de cartão de crédito.

Nesse trabalho são apresentados os principais benefícios dessa combinação dos padrões de segurança, tendo como base um case de sucesso.

O cenário proposto desse estudo, o adquirente, muitas vezes é esquecido como um negócio de crescimento dinâmico, e que é parte integrante da indústria de cartões de pagamento. O adquirente é um processo composto de muitos processos com vários relacionamentos entre estabelecimentos, bandeiras, bancos e emissor, que irá manter o crescimento e continuará a ser dirigida pela tecnologia.

Alguns estudos confirmam que o PCI DSS não é abrangente e precisa ser apoiado por outras normas de segurança para lidar com leitores de cartões e

softwares aplicativos de pagamento, por não ter uma visão clara de seus objetivos (Blackwell, 2008).

Sobre a combinação das normas, uma pesquisa (Blount, 2010) levantou o resultado de uma análise de falhas de segurança relatado nos últimos cinco anos em organizações com o foco no cliente, ao contrário deste estudo que tem como cenário o adquirente, e compatível com o padrão PCI DSS no momento da infração. Esse estudo evidenciou que as ambas as normas contêm detalhes que completam a outra e ajudam a organização ter o melhor dos dois mundos, além de concluir que a norma com uma arquitetura tão específica como o PCI DSS deve ser usado em conjunto com a ISO / IEC 27001 para alcançar com êxito a criação de um forte sistema de gestão de segurança da informação.

Adequar à organização em conformidade ao padrão de segurança é uma tarefa cercada de desafios, a começar pela definição do modelo de gestão a ser implantado e como este processo será conduzido. Este estudo buscou primeiramente identificar quais as melhores práticas adotadas para segurança das informações e os desafios, para posteriormente adaptá-las para operações de adquirente.

Este estudo se justifica, portanto, em poder servir de subsídio para futuros projetos, auxiliando na estratégia de implementação da conformidade de segurança da informação nas operações de cartão de credito, especificamente no adquirente.

## 1.4 Metodologia

Com a definição do tema, objetivo e estrutura do trabalho, o levantamento de informações em livros, artigos, documentações de pesquisa e na Internet foram focados nos temas tratados, sendo avaliados e adaptados quando possível à visão e experiência da autora. A autora valeu-se também do estudo de viabilidade da aplicação em um cenário real e análise dos ganhos pela combinação das normas.

## 1.5 Estrutura do Trabalho

O restante do presente trabalho está estruturado como segue.

Capítulo 1 – Introdução

Neste capitulo é apresentado o objetivo do trabalho, bem como a motivação, justificativa e a metodologia de pesquisa.

Capítulo 2 – Conceitos e fundamentos

Neste capitulo é apresentado uma gama de referenciais teóricas, que foram utilizados para estudar, comparar e analisar a proposta deste trabalho.

Capítulo 3 – Estudo da combinação das referências PCI DSS e ISO/IEC 27001 em operações de cartão de crédito.

Neste capitulo é apresentado o mapeamento de como foi estudo para integrar o PCI DSS com a norma ISO/IEC 27001 seguindo a visão de operações de cartão de crédito.

Capítulo 4 – Aplicação do Estudo

Neste capitulo é apresentado uma análise de como será integrado o PCI DSS com a norma ISO/IEC 27001 em cada um dos objetivos e práticas específicas dos processos de Segurança da informação.

Capítulo 5 – Conclusões

Neste capitulo é apresentado às contribuições do trabalho, a conclusão obtida pela elaboração desse trabalho.

Capítulo 6 – Referências Bibliográficas

Neste capitulo são apresentado todos os artigos, livros e estudos que deram embasamento nesse trabalho.

# 2. CONCEITOS E FUNDAMENTOS

## 2.1 Operações de cartão de crédito

As operações de cartão de crédito são divididas em três partes: consumidor, emissor e adquirente. Para facilitar o entendimento do funcionamento de uma transação, a figura 1 ajuda a compreender o papel do estabelecimento, adquirente, bandeira e emissor.

Uma transação é uma compra que se inicia com o portador do cartão.


**Figura 1 - Processo de transação**

1. O estabelecimento envia a transação ao adquirente para autenticação e aprovação da compra.
2. O Adquirente valida informações do estabelecimento (ponto de venda, numero de parcelas, situação etc.), submete a transação à bandeira e emissor para validação de dados e confirmação de saldo/crédito.
3. Banco emissor identifica cliente e autoriza a compra (concede crédito ou confirma saldo).
4. O portador recebe fatura com seus gastos e efetua pagamento total ou parcial.

5. A Bandeira recebe o valor da taxa de afiliação e valor por quantidade de transações processadas (restante do valor é pago direto aos adquirentes segundo informação da bandeira).
6. O Adquirente recebe valor das compras líquido da tarifa de Intercâmbio e das taxas da Bandeira.
7. O estabelecimento recebe valor da compra já retirado valor do aluguel do meio de captura, taxa administrativa e taxa de conectividade

Bandeira: é a empresa fornece serviços a consumidores e estabelecimentos.

Banco Emissor do Cartão: é a instituição financeira do portador do cartão e também um membro licenciado pela bandeira.

Portador do Cartão: é um consumidor que, ao solicitar um cartão, é analisado e aprovado pelo emissor que estabelece uma linha de crédito para o mesmo e emite o cartão do banco.

Estabelecimento: virtualmente, pode ser qualquer empresa determinada a aceitar os cartões como forma de pagamento e que atinge as qualificações determinadas pela bandeira e um emissor.

Adquirente/adquirente é a empresa responsável pela comunicação da transação entre estabelecimento e a bandeira, além de realizar a afiliação, gestão do meio de captura, liquidação de pagamento e antecipação de recebíveis do lojista. No diagrama abaixo mostra os principais módulos de um sistema adquirente.

Principais módulos de um sistema de adquirente:

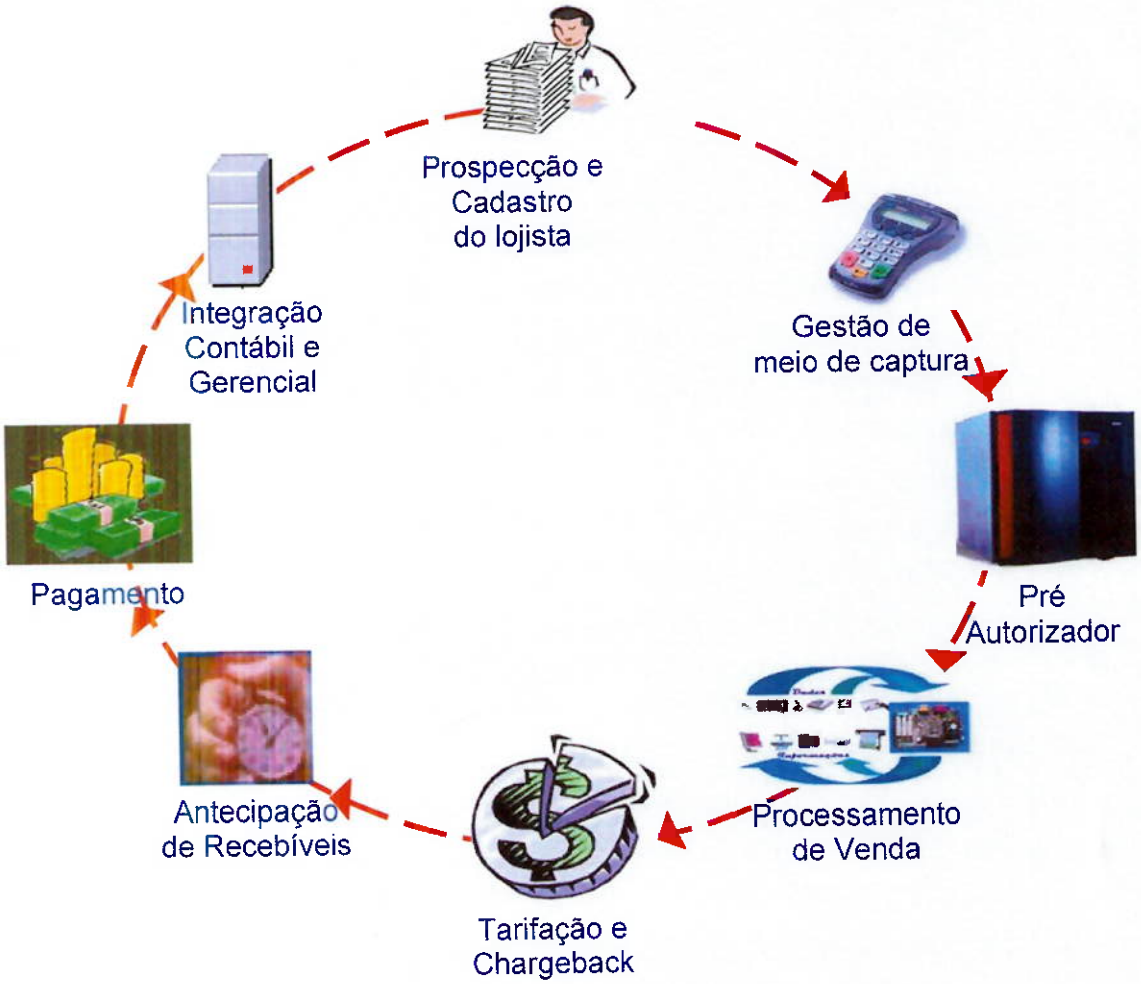


**Figura 2 - Integração entre módulos de um sistema Adquirente**

Prospecção e cadastro de lojista: Esse módulo refere-se parte de credenciamento e manutenção cadastral do lojista, onde são configuradas as condições comerciais do lojista como taxa administrativa por tipo de venda (rotativo e parcelado), aluguel de equipamento ou conexão, forma de pagamento, domicílio bancário, habilitações de redes de captura etc. Dependendo do canal de credenciamento esse processo pode ser feito de forma online ou batch através de troca de arquivos.

Gestão de meio de captura: é o controle do parque de equipamentos por lojista, além de controle de ordem de serviço para instalação, manutenção e retirada. A abertura de ordem de serviço pode ser através de comunicação online com

empresas de prestação de serviço conveniadas, onde trafegam informações do endereço do lojista, o tipo e quantidade de meio de captura.

Pré autorizador: é responsável pela validação das permissões de venda do lojista, como o cadastro, as redes de captura habilitadas, tipo de parcelamento etc. Processo online de trafego de mensageria síncrona com informações de origem e venda do lojista.

Processamento de venda: é processamento da confirmação das vendas enviada pelas bandeiras, transformando a transação em venda para pagamento ao lojista. Esse processo é efetuado por troca de arquivos ou online entre a bandeira e o adquirente.

Tarifação e chargeback: é processo de lançamento das tarifas por meio de captura e/ou conexão de rede, cancelamento de vendas, ajustes a debito e crédito.

Antecipação de recebíveis: é o processo de antecipar o pagamento das vendas do lojista, deduzindo a taxa negociada e os ajustes pendentes para data de pagamento negociada.

Pagamento: é o processo de efetuar o pagamento ao lojista. Esse processo calcula os débitos, créditos, tarifas, taxas, antecipações e envia para o banco configurado no cadastro do lojista. Processo com comunicação online e/ou batch por troca de arquivos CNAB entre bancos (link direto) para efetuar o pagamento aos lojistas.

Integração contábil e gerencial: é o processo de envio das provisões e efetivações de vendas, antecipações, ajustes, tarifas e taxas do lojista para controle contábil, financeiro e fiscal da instituição. Essas mesmas informações são enviadas para sistema de informações gerenciais para análise e tomadas de decisão da empresa. Devido à quantidade e o formato da informação a integração é de forma batch, através de troca de arquivos.

## 2.2 PCI DSS

O PCI DSS é um padrão de segurança para proteção de dados de cartão de pagamento introduzido em 2006 pelo conselho formado pelas bandeiras VISA, MasterCard, American Express, JCB e Discovery.

O principal objetivo do padrão foi reduzir as fraudes em larga escala com cartão de crédito em ambientes de pagamento eletrônico, tanto via internet quanto em estabelecimento comerciais tradicionais.

Sobre a parte técnica, os requisitos de segurança do PCI DSS se aplicam a todos os componentes do sistema. Os componentes de rede incluem, mas não se limitam a, firewalls, chaves, roteadores, pontos de acesso sem fio, mecanismos de rede e outros mecanismos de segurança. Os tipos de servidores incluem, mas não se limitam: Web, aplicativo, banco de dados, autenticação, e-mail, Proxy, NTP (network time protocol) e DNS (domain name server). Os aplicativos incluem todos os aplicativos adquiridos e personalizados, incluindo os aplicativos internos e externos (Internet).

O PCI DSS é composto por 12 requisitos de segurança:

1. Instale e mantenha uma configuração de firewall para proteger os dados do portador de cartão.
2. Não use as senhas padrões de sistema e outros parâmetros de segurança fornecidos pelos prestadores de serviços.
3. Proteja os dados armazenados do portador de cartão.
4. Codifique a transmissão dos dados do portador de cartão que transitam nas redes publicas abertas.
5. Use e atualize regularmente o software antivírus.
6. Desenvolva e mantenha seguros os sistemas e aplicativos.
7. Restrinja o acesso aos dados do portador de cartão apenas aqueles que necessitem conhecê-los para a execução dos trabalhos.
8. Atribua um ID único para cada pessoa que possua acesso ao computador.
9. Restrinja ao máximo o acesso físico aos dados do portador de cartão.

10. Acompanhe e monitore todo o acesso aos recursos da rede e dados do portador de cartão.
11. Teste regularmente os sistemas e processos de segurança.
12. Mantenha uma política que atenda a segurança da informação.

Dentro dos requisitos do PCI DSS foi criado o Padrão de Segurança de Dados de Aplicativos de Pagamento (PA DSS) que se aplica aos fornecedores de software que armazenam, processam e transmite dados de portador de cartão como parte da autorização.

O escopo da revisão do PA DSS deve incluir:

1. Cobertura de todas as funcionalidades do aplicativo de pagamento, incluindo sem limitações:
    - Funções de pagamento ponta-a-ponta (autorização e acordo);
    - Entrada e saída;
    - Condições de erro;
    - Interfaces e conexões a outros arquivos, sistemas, e/ou aplicativos de pagamento ou componentes desses aplicativos;
    - Todos os fluxos de dados de portadores de cartão;
    - Mecanismos de criptografia;
    - Mecanismos de autenticação.
2. Cobertura da orientação do fornecedor do aplicativo de pagamento esperada pelos clientes e revendedores/integradores para garantir que:
    - O cliente saiba como implementar o aplicativo de pagamento de uma forma compatível com o PCI DSS e;
    - O cliente seja informado claramente que determinados aplicativos de pagamento e configurações de ambiente podem impedir sua conformidade com o PCI DSS. Observe que se espera que o fornecedor do aplicativo de pagamento forneça tal orientação mesmo quando a configuração específica:
        - Não puder ser controlada pelo fornecedor do aplicativo de pagamento assim que o aplicativo for instalado pelo cliente, ou

- For de responsabilidade do cliente e não for fornecedor do aplicativo.

3. Cobertura de todas as plataformas selecionadas para a versão revisada do aplicativo de pagamento (as plataformas incluídas devem ser especificadas).

4. Cobertura das ferramentas utilizadas pelo aplicativo para acessar e/ou visualizar dados do portador do cartão (ferramentas de relatório, de log etc.).

O PCI PED (PIN Entry Device Security Requirements) é para fabricantes de dispositivos de cartão de pagamento usado no ponto de venda (POS). Além de outros requisitos do PCI DSS, os desenvolvedores de software, revendedores e transformadores deve usar apenas dispositivos aprovados em conformidade com a PED.

## 2.3 Norma ISO/IEC 27001

Em contraste com o quadro do PCI, a Norma ISO 27001 é reconhecida internacionalmente como padrão de segurança, que destina a aplicar a uma ampla variedade de organizações em diversas indústrias. É considerado de fato como padrão de segurança da informação por muitas organizações onde a segurança da informação é uma obrigação estrita, embora cumprimento seja voluntário. Muitas organizações que optam por se certificar a esse padrão muitas vezes o fazem para fins de diligência ou a confiança dos parceiros. Quando aplicado corretamente a norma é baseada em um fluxo de informações, que compõe o que o padrão define como um sistema. A organização define os sistemas a serem certificados e configura um Sistema de Gerenciamento da Segurança da Informação em torno da área relevante do negócio, que é então definido como o âmbito de aplicação. Posteriormente, a organização documentada totalmente no âmbito, cria um inventário detalhado de ativos e realiza uma formal avaliação de risco sobre os ativos. Os resultados da avaliação de risco levam a organização para o controle das cláusulas padrão e escolher aqueles que melhor abordam os riscos para o ambiente. Os controles selecionados são então documentados em sua Declaração de

Aplicabilidade (documento que formalizará os objetivos e controles aplicáveis e pertinentes a cada companhia) e mapeados para avaliação dos riscos.

Esta norma especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização.

O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionais para proteger os ativos de informação e propiciar confiança as partes interessadas.

A Norma encoraja que seus usuários enfatizem a importância de:

- Entendimento dos requisitos de segurança da informação e da necessidade de estabelecer uma política e objetivos para a segurança de informação.
- Implementação e operação de controles para gerenciar os riscos de segurança da informação.
- Monitoração e análise crítica do desempenho e eficácia do SGSI.
- Melhoria continua baseada em medições objetivas.

A Norma incorpora vários ciclos Plan-Do-Check-Act (PDCA), por exemplo, os controles de segurança da informação não são apenas especificados e implementados como uma atividade pontual, mas são continuamente revisados e ajustados para levar em conta as alterações de ameaças à segurança, vulnerabilidades e impactos das falhas de segurança da informação, usando atividades de melhoria especificada no sistema de gestão.

Nos próximos capítulos será apresentado como este estudo realiza a combinação das normas dentro do cenário de adquirente.

# 3. ESTUDO DA COMBINAÇÃO DAS REFERÊNCIAS PCI DSS E ISO/IEC 27001 EM OPERAÇÕES DE CARTÃO DE CRÉDITO

O mapeamento correto de um sistema de gestão de segurança da informação (SGSI) pode oferecer uma visão bem profunda dos riscos à organização, além de auxiliar no processo de segurança visando identificar vulnerabilidades e atingir partes profundas da aplicação não cobertas pelos procedimentos de segurança convencionais, como os do PCI DSS. Nesse estudo foi realizada a comparação das duas normas para mapear seus benefícios e pontos de melhoria durante a implementação nas organizações.

Entre as semelhanças das duas normas, destacam-se as verificações de sistemas a fim de mostrar conformidade e execução das melhores práticas na organização. Por outro lado, há muitas diferenças, o padrão PCI DSS é reconhecido principalmente na América e Europa, a adesão é obrigatória, têm níveis de abrangência (comerciantes e prestadores de serviços), todas as normas são necessárias e devem ser atendidas, a alteração nos sistemas é complexa, a flexibilidade é baixa, não há qualquer menção de pré-requisito para o enquadramento de gestão e o PCI DSS é aplicável nas informações de cartão de crédito. Comparativamente, a ISO/IEC 27001 é reconhecida internacionalmente, em conformidade voluntária, é mais flexível em termos de abrangência, controles, conformidade e execução. É projetada para ser aplicada em uma variedade de organizações em todos os setores ao redor do mundo e trabalham com outras normas e regulamentos. Como a norma é voluntária, os controles são mais uma sugestão, e a organização pode decidir quais controles são aplicáveis em específica área. Os controles do PCI DSS são muito mais rigorosos e específicos, as organizações devem cumprir cada um dos requisitos listados na norma. O rigor do PCI DSS é difícil para as organizações se tornarem compatíveis, devido à variedade de funções. A falta de flexibilidade da norma pode ser considerada um obstáculo em empresas de pequeno porte, pelo pouco tempo para adequação das recomendações do PCI DSS.

Uma solução abrangente para preencher as lacunas entre as duas normas é a combinação das normas, pois o PCI DSS é destinado a lidar com dados de segurança de informações de cartão de crédito, portanto, carece de objetivos, escopo, gerenciamento de dados e outras medidas de controle. Usando ISO/IEC 27001, o processo de segurança fica mais completo e abrange todas as entidades de segurança da informação que uma organização pode necessitar, incluindo o ciclo de melhoria contínua (PDCA).

Para facilitar a visão do modelo proposto, foram criadas categorias que separam os requisitos do PCI por objetivos de controle, a fim de facilitar o entendimento e relação com as recomendações da norma ISO 27001. Os requisitos foram agrupados pelos principais conceitos de segurança informação.

Tabela 1 – Categorização dos requisitos do PCI DSS.[1]

| Classificação | Subclassificação | Recomendações PCI DSS |
|---|---|---|
| **A.** Política | A.1 Política de Segurança da informação | A.1.1 Mantenha uma política que atenda a segurança da informação. |
| **B.** Proteção de Dados | B.1 Proteção de dados | B.1.1 Proteja os dados armazenados do portador de cartão.<br><br>B.1.2 Codifique a transmissão dos dados do portador de cartão que transitam nas redes públicas abertas. |
| | B.2 Administração de vulnerabilidade | B.2.1 Use e atualize regularmente o software antivírus.<br><br>B.2.2 Desenvolva e mantenha seguros os sistemas e aplicativos. |

[1] *Especificamente, o capitulo três tem itens enumerados por letra para facilitar o entendimento do modelo proposto.*

| | | |
|---|---|---|
| C. Monitoração | C.1 Medidas rígidas de controle ao acesso | C.1.1 Restrinja o acesso aos dados do portador de cartão apenas aqueles que necessitem conhecê-los para a execução dos trabalhos.<br><br>C.1.2 Atribua um ID único para cada pessoa que possua acesso ao computador.<br><br>C.1.3 Restrinja ao máximo o acesso físico aos dados do portador de cartão. |
| | C.2 Supervisão de teste | C.2.1 Acompanhe e monitore todo o acesso aos recursos da rede e dados do portador de cartão.<br><br>C.2.2 Teste regularmente os sistemas e processos de segurança. |
| | C.3 Rede Segura | C.3.1 Instale e mantenha uma configuração de firewall para proteger os dados do portador de cartão.<br><br>C.3.2 Não use as senhas padrões de sistema e outros parâmetros de segurança fornecidos pelos prestadores de serviços. |

Para cada item recomendado pelo PCI DSS, foram levantados os requisitos da ISO/IEC 27001 que completam e ajudam a melhorar o processo, além de relacionar dentro do cenário proposto, os módulos e/ou áreas do adquirente que se enquadram e que devem ter uma atenção maior.

## A. Política

### A.1 Políticas de Segurança da informação

Conforme mencionado no capítulo dois sobre a estrutura do adquirente, o item principal pra esse requisito são as práticas e políticas do negócio. Exemplo:

antecipação, pagamento a lojista, prospecção e cadastro de lojista etc. Dentro das organizações normalmente é feito troca de dados sensíveis do estabelecimento, como CNPJ, endereço, domicilio bancário, valores de faturamento para estratégias de vendas, porém sem o controle sistêmico desses dados, pode denegrir a imagem da organização, por vazamento de informações confidenciais.

### A.1.1 Mantenha uma política que atenda a segurança da informação.

Uma política de segurança sólida determina o nível 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.

Abaixo, são mencionadas requisitos da ISO 27001, que facilitam a manter uma política de Segurança da Informação.

- Auditorias: A organização deve conduzir auditorias internas para determinar se os objetivos de controle, processos e procedimentos atendem:
  - Aos requisitos do PCI DSS.
    - Atendem aos requisitos de segurança da informação identificados.
    - Estão mantidos e implementados eficazmente e são executados conforme esperado.
- Responsabilidade treinamento, conscientização e competência: A organização deve também assegurar que todo o pessoal pertinente esteja consciente da relevância e importância das suas atividades de segurança da informação e como eles contribuem para o alcance dos objetivos do PCI DSS. Além de fornecer treinamento ou contratar pessoal competente para divulgar as práticas e os processos do PCI DSS, mantendo registros de educação, treinamento, habilidades, experiências e qualificações.
- Melhoria Continua: A organização deve continuamente melhorar a eficácia da política de segurança da informação, objetivos de segurança, resultados de auditorias, analises de eventos monitorados, ações corretivas e preventivas e analise critica pela direção.

- Análise critica do SGSI: Esta análise critica deve ser realizada em intervalos planejados, e precisa incluir a avaliação das oportunidades para melhoria e a necessidade de mudanças do SGSI, incluindo a política de segurança da informação.

## B. Proteção de Dados

### B.1 Proteção de Dados

Dentro da estrutura adquirente, a criptografia pode ser exigida em vários módulos, e é mais evidente a necessidade nos arquivos de conciliação financeira, chargeback, confirmação de venda e pré autorizador devido ao detalhamento do conteúdo, venda a venda.

Seguem os requisitos necessários que ajudam a cumprir o nível de segurança da aplicação:

#### B.1.1 Proteja os dados armazenados do portador de cartão

Métodos de proteção como criptografia, truncamento e mascaramento são componentes essenciais da proteção de dados do portador do cartão. Se um invasor burlar outros controles de segurança da rede 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 devem ser considerados como oportunidades potenciais de minimização dos riscos:

- Executar procedimentos de monitoração e análise crítica para:
  - Prontamente detectar erros nos resultados de processamento.
  - Determinar se as ações tomadas para solucionar uma violação de segurança da informação foram eficazes.

- Melhoria continua: a organização deve executar ações corretivas para eliminar as causas de não conformidade com os requisitos do PCI e ações preventivas para evitar essas causas.

### B.1.2 Codifique a transmissão dos dados do portador de cartão que transitam nas redes públicas abertas.

Redes sem fio configuradas de forma incorreta, vulnerabilidades na criptografia e protocolos de autenticação podem ser alvos contínuos de indivíduos mal intencionados que exploram essas vulnerabilidades para obter acesso privilegiado aos ambientes de dados do portador do cartão.

- Identificar riscos.
- Analisar e avaliar os riscos.
- Implementar os controles para tratamento de riscos, provendo um resumo de decisões relativas ao tratamento de riscos.
- Definir como medir a eficácia dos controles ou grupos de controles de segurança, e especificar como estas medidas devem ser usadas para avaliar a os controles de modo a produzir resultados comparáveis e reproduzíveis.
- Executar procedimentos de monitoração e analise critica para:
  - Prontamente detectar erros nos resultados de processamento;
  - Determinar se as ações tomadas para solucionar uma violação de segurança da informação foram eficazes.
- Comunicar as ações e melhorias a todas as partes interessadas com um nível de detalhe apropriado as circunstâncias.
- Assegurar-se de que as melhorias atinjam os objetivos pretendidos.

### B.2 Administração de vulnerabilidade

Dentro do adquirente, os links online e batch e canais de comunicação com o lojista (site, ftps, URA etc.) são alvo de ataques e precisam de atenção a fim de mitigar riscos.

### B.2.1 Use e atualize regularmente o software antivírus.

Softwares mal-intencionados, normalmente chamados de "malware" (incluindo vírus, worms e cavalos de Tróia) entram na rede durante muitas atividades de negócios aprovadas, incluindo e-mail dos funcionários e uso da Internet, computadores móveis e dispositivos de armazenamento, resultando na exploração das vulnerabilidades do sistema. O software antivírus deve ser usado em todos os sistemas comumente afetados pelo malware para proteger os sistemas de ameaças atuais e potenciais de softwares mal-intencionados.

- Responsabilidade treinamento, conscientização e competência: A organização deve também assegurar que todo o pessoal pertinente esteja consciente da relevância e importância das suas atividades de segurança da informação e como eles contribuem para o alcance dos objetivos do PCI DSS.

### B.2.2 Desenvolva e mantenha seguros os sistemas e aplicativos.

Muitas das vulnerabilidades são solucionadas pelos patches de segurança disponibilizados pelos fornecedores, que devem ser instalados pelas entidades que gerenciam os sistemas. Todos os sistemas críticos devem contar com os patches de software adequados lançados mais recentes para proteger contra a exploração e o comprometimento dos dados do portador do cartão por indivíduos e softwares mal-intencionados.

Aplicação de auditorias facilita a análise dos atuais requisitos de segurança. A melhoria continua facilita a identificação de problemas e reduz as causas de não conformidade.

## C. Monitoração

### C.1 Medidas rígidas de controle ao acesso

Dentro do adquirente, o item principal relacionado a controle de acesso está no pré autorizador, redes para troca de arquivos, sistema core para impedir invasão e intermitência na rede ou até mesmo perda de conectividade.

### C.1.1 Restrinja o acesso aos dados do portador de cartão apenas aqueles que necessitem conhecê-los para a execução dos trabalhos.

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.

- Responsabilidade de treinamento, conscientização e competência: A organização deve também assegurar que todo o pessoal pertinente esteja consciente da relevância e importância das suas atividades de segurança da informação e como eles contribuem para o alcance dos objetivos do PCI DSS.
- Controles de registros: os registros devem ser estabelecidos e mantidos para fornecer evidências de conformidade aos requisitos, ex: os controles necessários para a identificação, armazenamento, proteção, recuperação, tempo de retenção e disposição de registros.

### C.1.2 Atribua um ID único para cada pessoa que possua acesso ao computador.

Atribuir uma identificação exclusiva (ID) a cada pessoa com acesso, assegura que cada indivíduo seja exclusivamente responsável pelas suas ações. Quando tal responsabilidade estiver em vigor, as ações desempenhadas nos dados e sistemas críticos serão realizadas por usuários conhecidos e autorizados.

- Executar procedimentos de monitoração e analise critica para:
  - Prontamente detectar erros nos resultados de processamento;
  - Determinar se as ações tomadas para solucionar uma violação de segurança da informação foram eficazes.
- Melhoria continua: a organização deve executar ações corretivas para eliminar as causas de não conformidade com os requisitos do PCI e ações preventivas para evitar essas causas.

### C.1.3 Restrinja ao máximo o acesso físico aos dados do portador de cartão.

Qualquer acesso físico aos dados ou sistemas que armazenam dados do portador do cartão fornece a oportunidade para as pessoas acessarem dispositivos ou dados e removerem sistemas ou cópias impressas, e deve ser restrito de forma adequada.

- Analisar e avaliar os riscos
  - Avaliar a probabilidade real da ocorrência de falhas de segurança.
  - Identificar e avaliar as opções para tratamento de riscos.
- Formular um plano de tratamento de riscos que identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades para a gestão dos riscos de segurança.
- Melhoria continua: a organização deve executar ações corretivas para eliminar as causas de não conformidade com os requisitos do PCI e ações preventivas para evitar essas causas.

### C.2 Supervisão de teste

Dentro do adquirente, os itens principais para esse requisito são os processos de contingência, planos de teste integrado, ambiente de teste, processo de homologação para cada mudança realizada, a fim de garantir disponibilidade.

### C.2.1 Acompanhe e monitore todo o acesso aos recursos da rede e dados do portador de cartão.

Mecanismos de registro e a capacidade de monitorar as atividades dos usuários são fundamentais na prevenção, detecção ou redução 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 sem registros das atividades do sistema.

- Auditorias: A organização deve conduzir auditorias internas para determinar se os objetivos de controle, processos e procedimentos atendem:
  - Aos requisitos do PCI DSS.
  - Atendem aos requisitos de segurança da informação identificados.
  - Estão mantidos e implementados eficazmente e são executados conforme esperado.
- Controles de registros: os registros devem ser estabelecidos e mantidos para fornecer evidencias de conformidade aos requisitos, ex: os controles necessários para a identificação, armazenamento, proteção, recuperação, tempo de retenção e disposição de registros.
- Melhoria continua: a organização deve executar ações corretivas para eliminar as causas de não conformidade com os requisitos do PCI e ações preventivas para evitar essas causas.
- Executar procedimentos de monitoração e analise critica para:
  - Prontamente detectar erros nos resultados de processamento;
  - Determinar se as ações tomadas para solucionar uma violação de segurança da informação foram eficazes.

### C.2.2 Teste regularmente os sistemas e processos de segurança.

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 freqüência para assegurar que os controles de segurança continuem refletindo um ambiente em transformação.

- Auditorias: A organização deve conduzir auditorias internas para determinar se os objetivos de controle, processos e procedimentos atendem:
  - Aos requisitos do PCI DSS.
  - Atendem aos requisitos de segurança da informação identificados.
  - Estão mantidos e implementados eficazmente e são executados conforme esperado.
- Melhoria Continua: A organização deve continuamente melhorar a eficácia da política de segurança da informação, objetivos de segurança, resultados de auditorias, analises de eventos monitorados, ações corretivas e preventivas e analise critica pela direção.

### C.3 Rede Segura

Dentro do adquirente, é necessário ter uma boa infraestrutra nos módulos online e de comunicação com redes externas, como os pré autorizadores, redes vans e aplicativos para troca de arquivos.

### C.3.1 Instale e mantenha uma configuração de firewall para proteger os dados do portador de cartão.

O ambiente que trafega informações de dados do portador do cartão é um exemplo de uma área mais sensível dentro da rede confiável de uma organização. 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.

- Identificar riscos.
- Identificar e avaliar as opções para tratamento de riscos.
- Formular um plano de tratamento de riscos que identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades para a gestão dos riscos de segurança.

**C.3.2 Não use as senhas padrões de sistema e outros parâmetros de segurança fornecidos pelos prestadores de serviços.**

Indivíduos mal-intencionados (dentro e fora de uma empresa) com freqüência usam senhas padrão do fornecedor e outras configurações padrão do fornecedor para comprometer os sistemas. Essas senhas e configurações são bastante conhecidas pelas comunidades de hackers e facilmente determinadas por meio de informações públicas.

- Executar procedimentos de monitoração e análise crítica para:
  - Prontamente detectar erros nos resultados de processamento.
  - Determinar se as ações tomadas para solucionar uma violação de segurança da informação foram eficazes.
- Melhoria continua: a organização deve executar ações corretivas para eliminar as causas de não conformidade com os requisitos do PCI e ações preventivas para evitar essas causas.

Com a combinação entre as normas passada nesse capítulo, adquirimos um modelo mais completo para implantação do processo de conformidade na estrutura adquirente. Usando a norma ISO 27001 como um meio para cumprir as metas de conformidade pode ser considerada como uma metodologia adequada para atender aos requisitos do quadro PCI, destacando as melhores práticas e definindo o escopo que precisa ser registrado e monitorado em um alto nível de detalhe.

Segue a tabela com o mapeamento completo das duas normas por item e por classificação:

Tabela 2 – Mapeamento dos requisitos do PCI, ISO 27001 e as operações do adquirente.

| A. Política | | |
|---|---|---|
| A.1 Política de Segurança da Informação | | |
| **Requisitos do PCI DSS** | **Recomendações da ISO 27001** | **Operações do Adquirente** |
| A.1.1 Mantenha uma política que atenda a segurança da informação. | Documentação dos procedimentos de operação | Práticas e políticas do negócio, ex.:<br>- antecipação<br>- pagamento a lojista<br>- prospecção e cadastro de lojista. |
| | Monitoramento | |
| | Gerenciamento de serviços terceirizados | |
| | Políticas e procedimentos para troca de informações | |
| | Política de controle de acesso | |
| | Política de mesa limpa e tela limpa | |
| | Política de uso dos serviços de rede | |
| | Identificação de equipamento em redes | |
| | Identificação e autenticação de usuário | |
| | Desconexão de terminal por inatividade | |
| | Computação móvel e trabalho remoto | |
| | Política para o uso de controles criptográficos | |
| | Gestão de incidentes de segurança da informação | |
| | Continuidade de negócios e análise/avaliação de risco | |
| | Conformidade com normas e políticas de segurança da informação e conformidade técnica | |
| | Política de segurança da informação | |
| | Atribuição de responsabilidades para a segurança da informação | |
| | Acordos de confidencialidade | |
| | Identificação segurança da informação nos acordos com terceiros | |
| | Responsabilidade pelos ativos | |
| | Papéis e responsabilidades | |
| | Conscientização e treinamento em segurança da informação. | |

| B. Proteção de dados | | |
|---|---|---|
| B.1 Proteção de dados | | |
| **Requisitos do PCI DSS** | **Recomendações da ISO 27001** | **Operações do Adquirente** |
| B.1.1 Proteja os dados armazenados do portador de cartão.<br><br>B.1.2 Codifique a transmissão dos dados do portador de cartão que transitam nas redes públicas abertas | Procedimentos e responsabilidades operacionais | Criptografia de dados sensíveis em:<br>- Arquivos de conciliação financeira<br>- Chargeback<br>- Confirmação de venda (base 2)<br>- Pré autorizador |
| | Manuseio de mídias | |
| | Mensagens eletrônicas | |
| | Autenticação para conexão externa do usuário | |
| | Gerenciamento de chaves | |
| | Procedimentos para controle de mudanças | |

| B.2 Administração de vulnerabilidade | | |
|---|---|---|
| **Requisitos do PCI DSS** | **Recomendações da ISO 27001** | **Operações do Adquirente** |
| B.2.1 Use e atualize regularmente o software antivírus.<br><br>B.2.2 Desenvolva e mantenha seguros os sistemas e aplicativos. | Procedimentos e responsabilidades operacionais | - Links online e batch.<br>- Canais de comunicação com o lojista (site, URA etc.). |
| | Monitoramento | |
| | Proteção contra códigos maliciosos e códigos móveis | |
| | Requisitos de negócio para controle de acesso | |
| | Gerenciamento de senha do usuário | |
| | Controle de acesso à rede | |
| | Requisitos de segurança de sistemas de informação | |
| | Validação dos dados de entrada | |
| | Controle do processamento interno | |
| | Segurança dos arquivos do sistema | |

| | | |
|---|---|---|
| | Análise crítica técnica das aplicações após mudanças no sistema operacional | |
| | Restrições sobre mudanças em pacotes de software | |
| | Vazamento de informações | |
| | Gestão de vulnerabilidades técnicas | |
| | Contato com grupos especiais | |

| C. Monitoração | | |
|---|---|---|
| C.1 Medidas rígidas de controle ao acesso | | |
| **Requisitos do PCI DSS** | **Recomendações da ISO 27001** | **Operações do Adquirente** |
| C.1.1 Restrinja o acesso aos dados do portador de cartão apenas aqueles que necessitem conhecê-los para a execução dos trabalhos.<br><br>C.1.2 Atribua um ID único para cada pessoa que possua acesso ao computador.<br><br>C.1.3 Restrinja ao máximo o acesso físico aos dados do portador de cartão. | Documentação dos procedimentos de operação | - Pré autorizadores.<br>- Redes para troca de arquivos.<br>- Sistema core. |
| | Registros de auditoria | |
| | Cópias de segurança | |
| | Manuseio de mídias | |
| | Mídias em trânsito | |
| | Gerenciamento de acesso do usuário | |
| | Controle de conexão de rede | |
| | Procedimentos seguros de entrada no sistema (logon) | |
| | Sistema de gerenciamento de senha | |
| | Desconexão de terminal por inatividade | |
| | Controle de acesso à aplicação e à informação | |
| | Termos e condições de contratação | |
| | Áreas seguras | |
| | Instalação e proteção do equipamento. | |

| C.2 Supervisão de Teste | | |
|---|---|---|
| **Requisitos do PCI DSS** | **Recomendações da ISO 27001** | **Operações do Adquirente** |
| C.2.1 Acompanhe e monitore todo o acesso aos recursos da rede e dados do portador de cartão.<br><br>C.2.2 Teste regularmente os sistemas e processos de segurança. | Documentação dos procedimentos de operação | - Processos de contingência<br>- Planos de teste integrado<br>- Ambiente de teste<br>- Processo de homologação |
| | Registros de auditoria | |
| | Monitoramento do uso do sistema | |
| | Proteção das informações dos registros (logs) | |
| | Registros (logs) de administrador e operador | |
| | Registros (logs) de falhas | |
| | Sincronização dos relógios | |
| | Segurança dos serviços de rede | |
| | Procedimentos seguros de entrada no sistema (logon) | |
| | Análise crítica técnica das aplicações após mudanças no sistema operacional | |
| | Gestão de vulnerabilidades técnicas | |

| C.3 Rede Segura | | |
|---|---|---|
| **Requisitos do PCI DSS** | **Recomendações da ISO 27001** | **Operações do Adquirente** |
| C.3.1 Instale e mantenha uma configuração de firewall para proteger os dados do portador de cartão.<br><br>C.3.2 Não use as senhas padrões de sistema e | Documentação dos procedimentos de operação | - Pré autorizadores.<br>- Redes vans.<br>- Aplicativos para troca de arquivos. |
| | Gestão de mudanças | |
| | Registros de auditoria | |
| | Gerenciamento da segurança em redes | |
| | Requisitos de negócio para controle de acesso | |
| | Gerenciamento de senha do usuário | |
| | Política de uso dos serviços de rede | |

| | | |
|---|---|---|
| outros parâmetros de segurança fornecidos pelos prestadores de serviços. | Proteção e configuração de portas de diagnóstico remotas | |
| | Segregação de redes | |
| | Controle de conexão de rede | |
| | Controle de roteamento de redes | |
| | Procedimentos seguros de entrada no sistema (logon) | |
| | Identificação e autenticação de usuário | |
| | Uso de utilitários de sistema | |
| | Isolamento de sistemas sensíveis | |
| | Segurança dos arquivos do sistema | |

# 4. APLICAÇÃO DO ESTUDO

De acordo com empresas especialistas em oferecer serviços relacionados à segurança da informação, a razão para as organizações falharem na implementação do PCI está no desenho da infraestrutura. Por exemplo:

- Proteção de dados insuficiente;
- Inadequado teste de sistemas e processos de segurança;
- Insuficientes controles de acesso;
- Isolamento de rede wireless;
- Firewall/VPN mal configurados.

O primeiro ponto a ser analisado nesse estudo é identificar o quão aderente a organização precisa estar no PCI. Em qualquer organização com o foco em operações de cartão de crédito, seja emissor ou adquirente, precisa avaliar a aderência através de um SAQ - Questionário de auto-avaliação que é mantido e deve ser utilizado para a validação da necessidade de aderência, onde os controles podem ser mais bem entendidos, avaliados e sua aplicabilidade verificada, baseados em como a organização utiliza os dados do cartão de crédito. Também é necessário classificar em qual nível de aderência a organização deve ser incluído, o que irá determinar o tipo de trabalho de adequação necessário e as medidas de manutenção da aderência no decorrer do tempo, conforme a figura 3 e tabela 2.

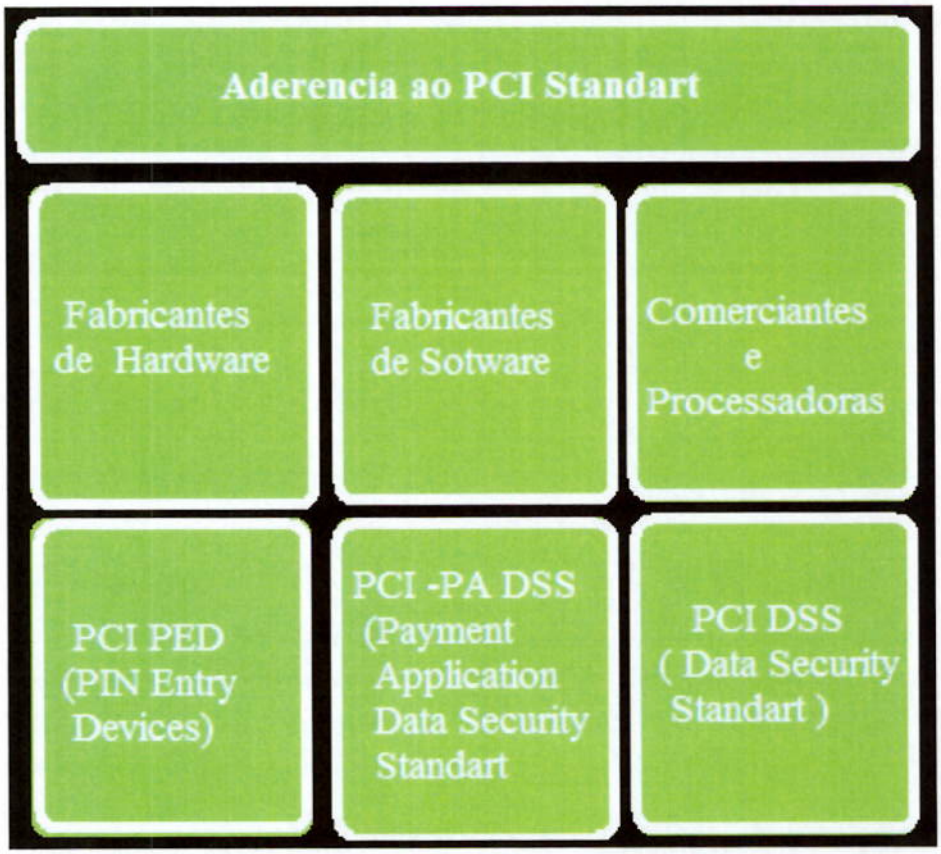


**Figura 3 - Classificação do tipo de aderência**

O processo de validação de controles pode ser iniciado através da análise de atendimento a cada um dos requisitos estabelecidos pelo PCI DSS. Algo que é interessante para as organizações neste cenário, é aproveitar este momento para entender o seu nível de classificação dentro dos critérios de quantidade de transações estabelecido pelo PCI DSS, e estimar o custo de manutenção da aderência para curto, médio e longo prazo. Estes níveis seguem os critérios estabelecidos pela VISA e MasterCard na classificação de seus clientes pela quantidade de transações efetuadas em um período de 12 meses, e também são aplicáveis às empresas provedoras de serviço (organizações que armazenam, processam ou transmitem dados do portador do cartão em nome dos membros de cartões, comerciantes ou prestadores de serviços).

Tabela 3 – Nível de classificação de transação por estabelecimentos.

| Nível | Definição do estabelecimento | Definição do Adquirente |
|---|---|---|
| 1 | Mais de seis milhões de transações anuais em todos os canais de venda. | Todas as empresas adquirentes e payment gateways, que são as empresas que fazem a transmissão dos dados desde o comerciante até as operadoras de cartão. |
| 2 | Entre 1.000.000 e 5.999.999 transações anuais em todos os canais de venda. | Todos as processadoras que não estejam classificados no Nível 1 e transmitam mais de 1.000.000 de transações anuais. |
| 3 | Entre 20.000 e 1.000.000 transações anuais em todos os canais de vendas. | Todos os adquirentes que não estejam classificados no Nível 1 e transmitam menos de 1.000.000 de transações anuais |
| 4 | Menos de 20.000 transações anuais em todos os canais de venda | Não se aplica. |

Após avaliar em qual nível de atendimento aos requisitos a organização está inclusa, o processo de aderência pode ser iniciado. Existem diversas formas de começar este trabalho, e possivelmente uma empresa especializada poderá ajudar.

Neste ponto, começa a necessidade da utilização da norma ISO 27001 para auxiliar na implementação da conformidade. Para implementar o PCI dentro dos processos do adquirente, primeiramente precisa ser levantado os pré requisitos, os módulos que devem estar em conformidade, e por fim o plano de implantação.

Abaixo, o levantamento dos pré requisitos, de acordo com as recomendações do PCI DSS.

- **Realizar uma segmentação da rede**

A segmentação da rede ou o isolamento do ambiente adquirente do restante da rede corporativa não é um requisito do PCI DSS. Entretanto, ela é recomendada como um método que pode reduzir:

- O escopo da avaliação do PCI DSS;
- O custo da avaliação do PCI DSS;
- O custo e a dificuldade de implementar e manter controles do PCI DSS;
- O risco de uma empresa (reduzido pela consolidação dos dados do portador do cartão em locais mais controlados e que totalizam um número menor).

Sem a segmentação adequada da rede, toda a rede corporativa estará no escopo da avaliação do PCI DSS.

- **Análise da tecnologia de rede sem fio**

Se uma tecnologia sem fio for usada para armazenar, processar ou transmitir dados do portador do cartão ou se uma LAN (local area network) sem fio estiver conectada ao ambiente adquirente ou a parte dele (por exemplo, não separado claramente por um firewall), os requisitos do PCI DSS e os procedimentos de teste para ambientes sem fio se aplicarão e também deverão ser realizados. Antes da tecnologia sem fio ser implementada, uma empresa deve avaliar cuidadosamente a necessidade da tecnologia com relação ao risco. Considere a implementação da tecnologia sem fio somente para a transmissão de dados não confidenciais.

- **Monitoração dos Terceiros**

Para prestadores de serviços que devem realizar uma avaliação *in loco* anual, a validação da conformidade deve ser desempenhada em todos os componentes do sistema nos quais os dados do portador do cartão estão armazenados, processados ou transmitidos.

Para aquelas entidades que terceirizam o armazenamento, o processamento ou a transmissão dos dados do portador do cartão para prestadores de serviços terceirizados, o Relatório sobre a conformidade (ROC) deve registrar a função de cada prestador de serviços, identificando claramente quais requisitos se aplicam à entidade analisada e quais se aplicam ao prestador de serviços. Além disso, os estabelecimentos comerciais e prestadores de serviços devem gerenciar e monitorar a conformidade do PCI DSS de todos os terceiros associados quanto ao acesso aos dados do portador do cartão.

- **Avaliação de áreas de negócio e componentes do sistema.**

O avaliador pode selecionar casos que representem áreas de negócios e componentes do sistema para avaliar os requisitos do PCI DSS. Ao selecionar exemplos de áreas de negócios e componentes de sistema, os avaliados devem considerar o seguinte:

- Se houver mais de um tipo de processo padrão implementado (por exemplo, para diferentes tipos de componentes de sistema ou áreas).
- Se não houver processos de PCI DSS padrão implementado e cada área for responsável pelos seus próprios processos.

- **Controles de compensação**

Anualmente, qualquer controle de compensação devem ser registrado, analisado e validado pelo auditor e incluído no envio do relatório sobre conformidade, controle de compensação e planilha dos controle de compensação.

## 4.1 Requisitos do PCI com menor eficácia em sua implementação

O modulo adquirente tem a premissa de garantir que todo o processo operacional de venda com cartão crédito de um estabelecimento comercial seja seguro, desde seu credenciamento até a ordem de pagamento. Todo esse processo precisa estar em conformidade com o PCI para evitar fraudes, violações e perdas financeiras que prejudiquem a imagem de todos os envolvidos nesse ciclo.

Nesse estudo foram levantados os principais desafios do adquirente em se adequar a conformidade PCI DSS, e quais recomendações da Norma ISO/IEC 27001 ajudam na implementação.

### 4.1.1 Escopo do PCI DSS muito abrangente

Ao implementar o PCI dentro dos processos adquirente, a organização deve analisar a conformidade focando em dois objetivos interligados: redução do risco e escopo. Quando se discute a redução do escopo, é natural que considere a palavra escopo se referindo a requisitos de conformidade. Para o PCI, escopo refere-se a dados sensíveis (dados do portador do cartão). Em relação ao risco, quanto menos dados sensíveis a organização mantém, menor o risco está associado à organização.

Na maioria dos módulos adquirente que precisam cumprir com os objetivos do PCI, os dados do portador do cartão, inicialmente parece estar em toda parte. É no ponto de venda (POS) e nas vendas do estabelecimento, em sistemas de relatórios financeiros, prevenção a fraude, sistemas, registros de investigação, arquivos de conciliação onde constam detalhes da venda, recibos, e-mails etc., a lista é interminável. As organizações geralmente perguntam "Como é que vamos cumprir com o PCI levando em consideração todos esses pontos?" Em vez disso, as organizações devem se perguntar: "Onde é que podemos eliminar o uso desses dados?". Ao eliminar números de cartões de crédito, todos os mecanismos de armazenamento onde estes números não devem residir, a organização ganha vários benefícios importantes. O primeiro é uma redução drástica no escopo associada à conformidade e o risco. O ideal é que números de cartões devem residir em apenas

um sistema central, como o sistema do Emissor. Todas as outras funções, como extratos de vendas, conciliação financeira, prevenção a fraude, podem exigir o número do cartão, ocasionalmente pode ser impulsionado em grande parte pelo uso de mecanismos alternativos, tais como a utilização criptografias em vez de números reais da conta para pesquisas de transação. Além disso, os benefícios de passar pelo exercício de redução de escopo podem ser ainda melhor porque a redução do escopo pode fazer toda a empresa muito mais adequada em lidar com seus ativos.

Para facilitar o que realmente é o escopo para atender as recomendações do PCI, é recomendado utilizar os requisitos do Sistema de gestão de segurança da informação (SGSI) conforme a norma ISO 27001, que ressalta a necessidade da organização em definir escopo e os limites dentro das características do negócio, a organização, sua localização, seus ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo. Por fim, recomenda-se identificar todos os fluxos de dados do portador do cartão e sistemas de armazenamento antes de olhar para o PCI DSS, e depois eliminar o maior número possível de itens.

Na tabela 4, os módulos e processos do adquirente que precisam ser avaliados a necessidade de utilização do numero do cartão de credito.

Tabela 4 – Módulos adquirente avaliados pelo PCI DSS

| Processos Adquirente | |
|---|---|
| **Módulo/Fluxos** | **Descrição** |
| Gestão de Meio de Captura | POS, PDV, GPRS, mensageria de redes van entre Bandeira e Adquirente etc. |
| Conciliação Financeira | Informações de vendas, ajustes, tarifas, taxas etc. |
| Informações Gerenciais | Informações detalhadas de venda, pagamento a lojista, antecipações etc. |
| Prevenção a Fraude | Datamarts, relatórios detalhadas de venda para avaliar comportamento do lojista e cliente. |

### 4.1.2 Falha de automação

Quando uma organização tem o certificado de segurança e é surpreendido por uma falha de segurança, a Bandeira envia um auditor, com objetivo de refutar o não cumprimento das recomendações do PCI no momento da infração. O auditor também analisa a conformidade com base em uma amostra de evidência, baseado em todo o período de tempo: antes e depois da violação. É fácil imaginar que o auditor encontrará controle que não foi cumprido de um ponto ou outro, ou simplesmente não encontre qualquer evidência que justifique a falha de segurança. A conclusão para o auditor é que a organização não está compatível com o PCI DSS, independentemente de sua avaliação anterior que garantiu sua certificação. Esta conclusão encadeia para uma série de obrigações, incluindo multas e outras sanções, dependendo da gravidade da infração.

O detalhamento dos requisitos do PCI, não deixa claro como manter a rastreabilidade nos controles de segurança, e uma maneira de facilitar essa manutenção é a prática da ISO 27001, que sugere o uso de análise critica do SGSI em intervalos planejados, para possibilitar a oportunidade de melhoria e mudança, eliminar erros nos resultados de processamento, rastrear novas vulnerabilidades e ameaças não contempladas e criar ações preventivas e corretivas através de ferramentas que geram automaticamente evidências (logs), para cada ação. Esse requisito da ISO 27001 gera significativos benefícios operacionais, incluindo detecção precoce de falhas, um fator importante para mitigar o risco e principalmente provar que a organização está dentro da conformidade de segurança exigida pelo PCI.

Como o PCI tem muitos controles de requisitos, é praticamente impossível manter a conformidade sem ferramentas apropriadas. Esse requisito também gera benefícios secundários, tais como captura de alterações não autorizadas, detectando problemas de confiabilidade e desempenho, ou simplesmente indicando configurações de qualidade inferior em sistemas operacionais. Note que o cumprimento, por si só não pode parar uma violação de acontecer, apesar de ter controles de segurança no local, mas aumenta a detecção de falhas de semana e meses para minutos e horas. Isso é poderoso. No entanto, essa prática da ISO

27001 em conjunto com as recomendações do PCI, é essencialmente um conjunto de melhores práticas de segurança, e podem contribuir significativamente para a postura de segurança da organização como um todo. O plano de investir tanto em automação e centralização, proporcionará a melhor cobertura na sequência de uma violação, e também irá proporcionar significativos benefícios operacionais.

Na tabela 5, os módulos e processos do adquirente que precisam ter rastreabilidade para mitigar riscos e ameaças:

Tabela 5 – Módulos adquirente que precisam de rastreabilidade

| Processos Adquirente | |
|---|---|
| **Módulo/Fluxos** | **Descrição** |
| Pré Autorizador | Roteador IST, Links de comunicação com as Bandeiras e Emissor, arquivo de base 2 etc. |
| Conciliação Financeira | Informações de vendas, ajustes, tarifas, taxas etc. enviadas por canais de comunicação direto com o estabelecimento. |
| Prevenção a Fraude | Sistemas de monitoração online de comportamento de vendas |

### 4.1.3 Processo de auditoria

Uma questão a parte que as organizações enfrentam para cumprimento do PCI é um processo de auditoria. Embora uma avaliação do PCI se assemelhe a uma auditoria de regulamentação em um determinado nível, as organizações não devem tratá-lo como tal por várias razões: Primeiro, porque o PCI não é uma lei, mas sim uma indústria privada, o nível de risco associado à conformidade com o PCI é diferente de um regulamento controlado por empresas governamentais. Em segundo lugar, as avaliações PCI funcionam mais como um check list do que uma auditoria sistêmica. Na verdade, o PCI é totalmente binário em dois sentidos: todos os controles têm o mesmo peso, e todos eles devem ser cumpridos a fim de garantir a conformidade. Em compensação os controles podem ser classificados e aprovados, não há nenhuma porcentagem, limite de adesão que pode ser atravessado, ou seja, a organização está em conformidade, ou não está.

Em terceiro lugar, os avaliadores não têm um padrão de auditoria rígido a ser seguido pela qual eles são julgados, cada um pode se aproximar do processo de avaliação de forma diferente, desde que satisfaçam os critérios específicos de teste técnico definido dentro da norma. Esta falta de avaliação uniforme provavelmente contribui significativamente para a crença comum de que mais de um PCI Qualified Security Assessor (QSA) provavelmente dará um resultado diferente e conclusões diferentes na avaliação da mesma organização. Por fim, os QSAs normalmente trabalham como consultores, em vez de auditores independentes, que normalmente querem avaliar organizações e ao mesmo tempo, ajudá-la a tornar-se complacente ao PCI. Esta situação cria um conflito inerente de interesses poderosos e resulta em prováveis impactos de avaliação.

Na tentativa de solucionar esse problema, pode ser usado o programa de auditoria de acordo com a ISO 27001, que deve ser planejado levando em consideração a situação, a importância dos processos e áreas a serem auditadas, bem como os resultados de auditorias anteriores. Os critérios da auditoria, escopo, freqüência e métodos devem ser definidos. A seleção dos auditores e a execução das auditorias devem assegurar objetividade e imparcialidade do processo de auditoria. Os auditores não devem auditar seu próprio trabalho. As responsabilidades, os requisitos para planejamento e para execução de auditorias, o relato dos resultados e a manutenção dos registros devem ser definidos em um procedimento documentado.

O responsável pela área a ser auditada deve assegurar que as ações sejam executadas, sem demora indevida, para eliminar as não-conformidades detectadas e suas causas. As atividades de acompanhamento devem incluir a verificação das ações executadas e o relato dos resultados de verificação.

Na tabela 6, os módulos e processos do adquirente com índice maior de auditoria:

Tabela 6 – Módulos adquirente elegíveis a auditoria.

| Processo Adquirente | |
|---|---|
| Módulo/Fluxos | Descrição |
| Contabilidade | Informações de vendas, ajustes, tarifa, saldo a receber, saldo devedor, valores de comissão etc. |
| Conciliação Financeira/ Pagamento a lojista/ Antecipações | Informações de vendas, ajustes, tarifas, taxas, pagamento a lojista, valores de antecipação etc. |
| Informações Gerenciais | Informações detalhadas de venda, pagamento a lojista, antecipações. |
| Pré Autorizador | Logs de transações, logs de conectividade e monitoração. |

## 4.2 Resultados alcançados com a combinação das normas

Para cada item do PCI DSS com menor eficácia de sua implementação, foram levantadas as recomendações da norma ISO 27001 necessárias para tornar-se um processo mais eficaz.

Dentro de um escopo muito abrangente, considere sete requisitos do PCI a serem implantados, e com o estabelecimento de SGSI facilitará a implantação na organização de maneira mais eficaz, facilitando o mapeamento do escopo e limites, o resultado da análise/avaliação de riscos, a seleção de controles e os objetivos de controle.

Com relação às falhas de automação, dentro dos requisitos do PCI não deixa claro como manter a monitoração dos controles de segurança, por isso a sugestão de utilizar a monitoração e analise critica do SGSI que facilita a detecção de erros previamente e possibilita um SGSI mais eficaz, reduzindo falhas e mitigando riscos.

Em vários requisitos do PCI são mencionados os registros de auditoria, mas em nenhum item detalha como deve ser uma auditoria dentro do processo e da organização. Na ISO 27001, a auditoria é um item a ser implantado dentro do SGSI, porque além de gerar um diagnóstico detalhado dos reais problemas em atingir os

itens de conformidade na organização, permite a correção de procedimentos e redução dos riscos associados à execução das atividades.

Em resumo, a norma ISO 27001 agrega ao PCI métodos de criar um Sistema de Gerenciamento da Segurança da Informação, por adotar análise crítica, um processo mais completo de auditoria etc. que facilita a implementação e o gerenciamento do escopo de segurança de uma organização, oferecendo um sistema de segurança mais eficaz e robusto, garantindo que os objetivos sejam alcançados como planejado, reduzindo custo, tempo e escopo.

# 5. CONCLUSÕES

## 5.1 Objetivo atingido

Os 12 requisitos do PCI DSS não são triviais de implementar devido à sua complexidade, tanto em termos técnicos como organizacionais.

Conforme mencionado nos capítulos três e quatro, o PCI DSS é destinado a lidar com dados de segurança de informações de cartão de crédito e a ISO/IEC 27001 abrange todas as entidades de segurança da informação que uma organização pode necessitar, incluindo o ciclo de melhoria contínua (PDCA).

O objetivo desse estudo é a mostrar como a combinação das duas normas de segurança da informação aplicada em um segmento especifico, no caso operações do adquirente, pode trazer benefícios e reduzir algumas das lacunas apresentada na norma PCI DSS.

## 5.2 Próximos passos

Com a combinação entre as normas passada nesse estudo, adquirimos uma sugestão de modelo mais completo para implantação do processo de conformidade na estrutura adquirente. Usando a norma ISO 27001 como um meio para cumprir as metas de conformidade através de uma metodologia adequada para atender aos requisitos do quadro PCI, destacando as melhores práticas, definindo um escopo mais mensurável e a monitoração em um alto nível de detalhe.

## 5.3 Considerações

Implementar todos os requisitos do PCI em operações do adquirente requer uma significativa quantidade de esforço e competência técnica, devido ao foco constantemente ser das operações do cartão de credito (visão cliente) e a falta

do domínio no processo, a probabilidade de gerar falhas na implementação dessa conformidade pode ser grande.

Ao detalhar o processo PCI e aplicar no processo adquirente, muitas subjetividades e dificuldades na implementação dos requisitos são levantadas, ainda mais porque PCI DSS tem uma visão muito mais do processo Emissor (cliente) do que do estabelecimento. Esse estudo identifica alguns dos principais desafios e sugere a combinação com uma norma de segurança mais abrangente, a fim de garantir a implantação com robustez do modelo de segurança da informação.

Para empresas adquirentes a combinação dessas normas facilita para obter um SGSI mais eficiente e mais completo, pelo detalhamento e aplicação das melhores práticas utilizadas na ISO 27001, além de atender as recomendações conforme definido pelo PCI Council.

Vários desafios poderão ser encontrados ao aplicar essa combinação nas organizações, começando pela mudança da cultura na empresa, a conscientização dos funcionários sobre as novas políticas de segurança da informação, as restrições de acesso em determinadas informações, sobre como divulgar dados e limitações de troca de informações entre áreas, empresas e fornecedores.

Como trabalhos futuros, pode se criar um estudo sobre a necessidade de criar um padrão de segurança específico para as operações do adquirente, considerando todos os módulos, a fim de reduzir o escopo e eliminar itens sem aplicação nesse cenário.

# 6. REFERÊNCIAS BIBLIOGRÁFICAS

BARBATO, Luiz Gustavo C.; MONTES, Antonio; VIJAYKUMAR, N. L. Metodologia de análise de código em aplicações de pagamento com cartões de crédito. Laboratório Associado de Computação e Matemática Aplicada (LAC) - Instituto Nacional de Pesquisas Espaciais (INPE) -Campinas – SP, 2007.

BARBATO, Luiz Gustavo C.; MONTES, Antonio; VIJAYKUMAR, N. L. Metodologia de Identificação de Vulnerabilidades em Aplicações de Pagamento. . Laboratório Associado de Computação e Matemática Aplicada (LAC) - Instituto Nacional de Pesquisas Espaciais (INPE) -Campinas – SP, 2007.

BLACKWELL, Clive. The Management of Online Credit Card Data using the Payment Card. IEEE Information Security Group Royal Holloway, University of London, 2008.

BLOUNT, Monika. Compliance Standards in Data Security. Masters of Science in Information Security Practicum Project. Georgia Institute of Technology College of Computing & eFortresses Inc, publicado em Abril de 2010.

BOEHMER, Wolfgang. Appraisal of the effectiveness and efficiency of Information Security management system based on ISO 27001. IEEE The Second International Conference on Emerging Security Information, Systems and Technologies, 2008.

CAMINHA, Jean; LEAL, Rhandsaissem Tavares; MARQUES JUNIOR, Rodrigo Otávio Pires Cabral; NASCIMENTO, Miguel Grimm. Implantação da Gestão da Segurança das informações em um Instituto de Pesquisa Tecnológica. Fundação Centro de Análise, Pesquisa e Inovação Tecnológica (FUCAPI).

Challenges and Opportunities of PCI. Five Challenges to Continuous PCI DSS Compliance.

DA SILVA, Antônio Everardo Nunes, SOUZA, Felipe Nascimento. O vazamento de informações corporativas – Disponível em: http://www.fraudes.org/externos/TCC_Everardo_Nunes_04122007.pdf. Acesso em 17 de Novembro de 2010.

FALSARELLA, Douglas. PCI-DSS: Entenda como funciona a norma de segurança de transações eletrônicas. Disponível em: http://imasters.com.br/artigo/12196/seguranca/pci-dss_entenda_como_funciona_a_norma_de_seguranca_de_transacoes_eletronicas. Acesso em 01 de Dezembro de 2010.

ISO/IEC 27001 - Information technology — Security techniques — Information security management systems — Requirements.

IT Risk Management Report 2: Myths and Realities – 2007. Sysmantec, publicado em janeiro de 2008.

KJOS, Ann. The Merchant-Acquiring Side of the Payment Card Industry: Structure, Operations, and Challenges. Outubro de 2007.

LIU, Jing; XIAO, Yang; CHEN, Hui; OZDEMIR, Suat; DDLE, Srinivas and SINGH, Vikas. A Survey of Payment Card Industry Data Security Standart
IEEE Communications Surveys & Tutorials, Vol. 12, No. 3, Third Quarter 2010.

NEVES, Eduardo Vianna de Camargo. Entendendo o PCI DSS, Porque Os Padrões Promovidos Pelo Payment Card Industry Council São Bem Mais Do Que Um Simples Snake Oil. publicado em Agosto de 2008.

OWASP (2007), TOP Ten 2007. Disponível: http://www.owasp.org/index.php/Application_Security_News. Acesso em 01 de Novembro de 2010.

PCI Security Standard Council. - "Payment Card Industry Data Security Standard". Disponível: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf. Acesso em 01 de Outubro de 2010.

PCI Security Standard Council - "Payment Card Industry Data Security Standard". Disponível: https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf. Acesso em 01 de Outubro de 2010.

Relatório Symantec 2010 sobre Segurança da Informação nas Empresas mostra aumento de ataques cibernéticos contra empresas de todo mundo. Disponível: http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20100224_01. Acesso em 27 de Novembro de 2010.

SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma visão executiva. 1ª. Ed. Rio de Janeiro: Campus, 2003.

WRIGHT, Steve. Using ISO 27001 for PCI DSS Compliance. Siemens Insight Consulting.