

# ENTENDENDO O PCI DSS

PORQUE OS PADRÕES PROMOVIDOS PELO PAYMENT CARD INDUSTRY COUNCIL SÃO BEM MAIS DO QUE UM SIMPLES SNAKE OIL

por Eduardo Vianna de Camargo Neves, CISSP

[eduardo@camargoneves.com](mailto:eduardo@camargoneves.com)

## Muito mais que um padrão Snake Oil

No meio da corrida pelo ouro que movimentou a Califórnia do Século XIX, muitos comerciantes aproveitaram a grande quantidade de moeda circulante para vender um elixir que curava tudo: o *Snake Oil*. De dedo inflamado a dor de cabeça, o remédio tinha propriedades milagrosas. Ou pelo menos era vendido assim. Com o passar do tempo, o termo entrou para o linguajar norte-americano como uma fraude que promete milagres mas é incapaz de fazer mais que um placebo.

O autor, pesquisador e profissional de IT Security, Bruce Schneier, usou o termo em seu [blog](#) ao se referir a forma como alguns produtos de criptografia estavam sendo vendidos. Belas palavras que impressionam um leigo mas ao serem analisadas por um profissional com um mínimo de conhecimento sobre o assunto não passam desta definição: belas palavras.

Os padrões de segurança estabelecidos pelo Payment Card Industry (PCI) Council são referenciados por muitas pessoas desta forma, como um conjunto de regras simplista criado para satisfazer a necessidade de mostrar aos clientes das operadoras de cartão de crédito que seus dados estão sendo protegidos. Esta visão me parece primária e equivocada, pois a adoção de qualquer padrão de segurança pode cair no mesmo erro. Durante a minha carreira já vi empresas de diversos setores implementarem Planos Diretores de Segurança da Informação que deixavam todos os auditores que tinham pouco pouco tempo para fazer o seu trabalho satisfeitos, mas não resistiam a uma análise um pouco mais profunda.

Independente de qual seja o padrão de segurança que a sua empresa adote – ou queira adotar – a forma como o processo é implementado e administrado, importa muito mais do que a quantidade de controles que serão colocados no seu ambiente. Os controles estabelecidos pelo PCI Council tem a vantagem de serem simples, eficazes dentro do escopo ao qual se propõe a abordar e altamente escalonáveis. Este artigo mostra em uma visão geral, como estes padrões nasceram, quais controles são esperados e como a sua empresa pode se alinhar para um processo de certificação.

## As origens do PCI DSS

A popularização da Internet e o conseqüente crescimento do *e-commerce* multiplicaram de forma exponencial a quantidade de transações feitas pela Internet, gerando somente no Brasil, um **crescimento anual** que orbita entre 40% a 60%. Em valores mais palpáveis, este mercado **movimentou R\$ 6,3 bilhões em 2007**, com um *ticket* médio de R\$ 302. E apesar das opções de boleto bancário e débito em conta corrente, o cartão de crédito é a forma de pagamento escolhida pela maioria absoluta dos consumidores.

Um cenário impressionante que cria um motivador para o *cyber* crime em todas as partes do mundo. A fraude mais comum é o furto de dados de um determinado portador de cartão de crédito e o uso para compras e transferência de valores entre contas. A mídia brasileira publica com freqüência a prisão de quadrilhas envolvidas com este tipo de prática, porém um cenário muito mais amplo já está sendo mantido: o comércio de números de cartão de crédito no mercado negro. Uma vez que é muito mais eficaz concentrar a tentativa de furto de dados em um lugar onde exista uma grande quantidade de números de cartão de crédito, para que um *cyber* criminoso irá perder tempo com um único consumidor se ele pode mirar na base de dados de uma empresa de *e-commerce*?

Se cruzarmos esta premissa com a **quantidade de vulnerabilidades que existem em web sites**, está pronta a receita para uma avalanche de fraudes em todo o mundo. E elas estão ocorrendo há quase uma década com números cada vez maiores, uma vez que o crime organizado aprendeu a usar crackers para suportar suas atividades. As fraudes envolvendo informações de portadores de cartão de crédito aumentaram de US\$ 1,5 bilhões em 2000, para US\$ 3,6 bilhões em 2007, e como mesmo período, o percentual de perdas com fraudes on line caiu de 3,6% para 1,4%, os números deixam claro que já algum tempo era preciso fazer algo para interromper a crescente perda de rentabilidade frente as fraudes, uma vez que o comércio on-line não para de crescer.

Diante deste cenário, as maiores empresas de cartões de crédito – American Express, Discover, MasterCard e Visa – decidiram criar regulamentos para evitar o furto de dados dos portadores de seus produtos e o uso destes em fraudes. O **PCI Data Security Standard (DSS)** foi criado em 2004 e implementado à partir de 30 de junho de 2005.

## Os controles do PCI DSS

Focado em implementar controles de segurança nos componentes da infra estrutura de TI que suportam o fluxo de dados do portador de cartão de crédito, o PCI DSS é formado por um conjunto de práticas que estão presentes na maioria das normas e regulamentações relacionadas à Segurança da Informação. A grande diferença, é que o PCI DSS é focado na proteção de um ativo exclusivo, e foi desenvolvido para impedir a ocorrência de fraudes e outros problemas oriundos do uso inadequado das informações relacionadas ao cartão de crédito. Composto de doze exigências distribuídas em seis linhas de controles, o PCI DSS apresenta controles de segurança técnica básicos, que devem ser entendidos como uma primeira etapa na construção de um ambiente protegido.

### Construa e Mantenha uma Rede Segura

Por mais simples e óbvia que pareça esta prática, uma das maiores portas de entrada para o *cyber* crime é o uso de contas *default* e a exploração de parâmetros de segurança fornecidos pelos prestadores de serviços.

Usando informações que podem ser obtidas pela Internet, ou *exploits* de vulnerabilidades conhecidas, os *crackers* acessam as bases de dados das empresas, capturam a informação e apagam seus rastros.

Nas duas exigências relacionadas a esta linha de controle, o PCI DSS exige que as empresas tenham um firewall protegendo sua rede de dados e nunca caiam no erro apresentado no parágrafo anterior. Os controles se abrem em itens muito específicos descrevendo as configurações mínimas e como proceder na administração das mesmas no dia-a-dia.

### **Proteja os Dados do Portador de Cartão**

Uma vulnerabilidade largamente explorada em tentativas de acesso indevido, é a presença de falhas em bancos de dados decorrentes de configurações inadequadas e falta de cuidado com a modelagem do controle de acesso. A exigência 3 do PCI DSS toca exatamente neste ponto, detalhando como as bases de dados com informações sensíveis – dentro do escopo já citado – devem ser protegidas quando armazenadas. A exigência 4 completa o ponto, especificando como elas devem ser protegidas em trânsito. Nesta vale uma observação, além do fluxo comum pela Internet que deve ser protegido com *Secure Socket Layers* (SSL) e similares, a transmissão a ser cuidada inclui redes nem sempre consideradas, como WiFi e GPRS. Um bom trabalho de casa para as empresas que equipam suas forças de vendas com *smartphones* e similares.

### **Mantenha um Programa de Administração de Vulnerabilidade**

Apesar da exigência 5 determinar algo relativamente comum às empresas, que é o uso e a administração de programas anti vírus, incluindo suas atualizações de assinaturas e modo de implementação, a exigência 6 toca em um aspecto constantemente ignorado: o cuidado no desenvolvimento e manutenção de sistemas operacionais e aplicações. A instalação de *patches* de segurança não é um processo usual, pois mudanças em um ambiente um pouco mais complexo que o padrão considerado pelo fabricante pode simplesmente para um sistema crucial para a empresa.

Como avaliar o que é mais importante em janelas de tempo onde as vendas de uma empresa estão ocorrendo? Parar um servidor para executar a atualização e interromper o processo comercial ou deixar para fazer quando puder? E torcer para esta data existir depois que o *stress* da situação passar? Indo além no mesmo ponto, em quantas empresas existe um *Secure Development Life Cycle* (SDLC) integrado ao processo de desenvolvimento de aplicações internas?

São exigências que devem considerar áreas muito além do escopo definido pelo PCI DSS e exigem investimentos em empresas de qualquer porte – e por isso mesmo, estão entre as mais criticadas pelo mercado – mas não passam de práticas de segurança que devem ser utilizadas em qualquer empresa que queira alcançar um nível mínimo de proteção do seu ambiente de TI.

### **Implemente Medidas Rígidas de Controle ao Acesso**

Estabelecer um processo de segregação de funções e o [Princípio do Menor Privilégio](#), são práticas consagradas de administração de empresas para evitar fraudes e abusos de privilégios como os que resultaram na criação da regulamentação *Sarbanes-Oxley* nos Estados Unidos. A exigência 7 do PCI DSS segue esta linha, estabelecendo que o acesso aos dados do portador de cartão deve ser concedido somente aqueles que necessitam conhecê-lo para a execução de seus trabalhos.

A exigência 8 estabelece a necessidade de atribuir um único ID par cada pessoa que acesse os sistemas, um princípio consagrado de rastreabilidade. Vale olhar com mais cuidado o texto, pois a abertura dos critérios entra em vários tópicos de controle de acesso, como bloqueio de contas, troca de senhas e autenticação de dois fatores. A exigência 9 define as medidas de controle de acesso físico aos dados do portador de cartão, dando uma pequena pincelada em administração de mídias de *backup* e tratamento de descarte de mídias, ainda que não seja muito criteriosa neste último aspecto.

### **Acompanhe e Teste Regularmente Todas as Redes**

As exigências 10 e 11 se completam em um processo de monitoramento contínuo da segurança estabelecida na rede de dados. Enquanto a primeira foca na obrigatoriedade de se acompanhar e monitorar o acesso aos recursos da rede e dados do portador de cartão, a segunda segue na linha de testes regulares de segurança técnica, onde *scans* de vulnerabilidade externa e *penetration tests* fazem a simulação de uma tentativa de *cracking* à partir do ambiente externo. O monitoramento de acesso citado na exigência 10 trata da existência e administração de vários tipos de *logs*, tais como os que registram acessos privilegiados, alteração de objetos, processos de autenticação e outros eventos que podem ser utilizados posteriormente para rastrear uma tentativa de quebra de segurança.

A exigência 11 entra em um dos pontos onde a empresa precisa contar com os serviços especializados de um *Approved Scanning Vendor* (ASV) para executar as atividades de análise externa de vulnerabilidades. Além de ser um ponto de controle onde muitas empresas erram por não manterem uma rotina de testes dessa natureza, é fundamental entender que o processo de *scans* e *pen-tests* é novamente focado no escopo do PCI DSS, e não deve ser entendido como um teste de vulnerabilidades baseado nestas práticas.

### **Mantenha uma Política de Segurança da Informação**

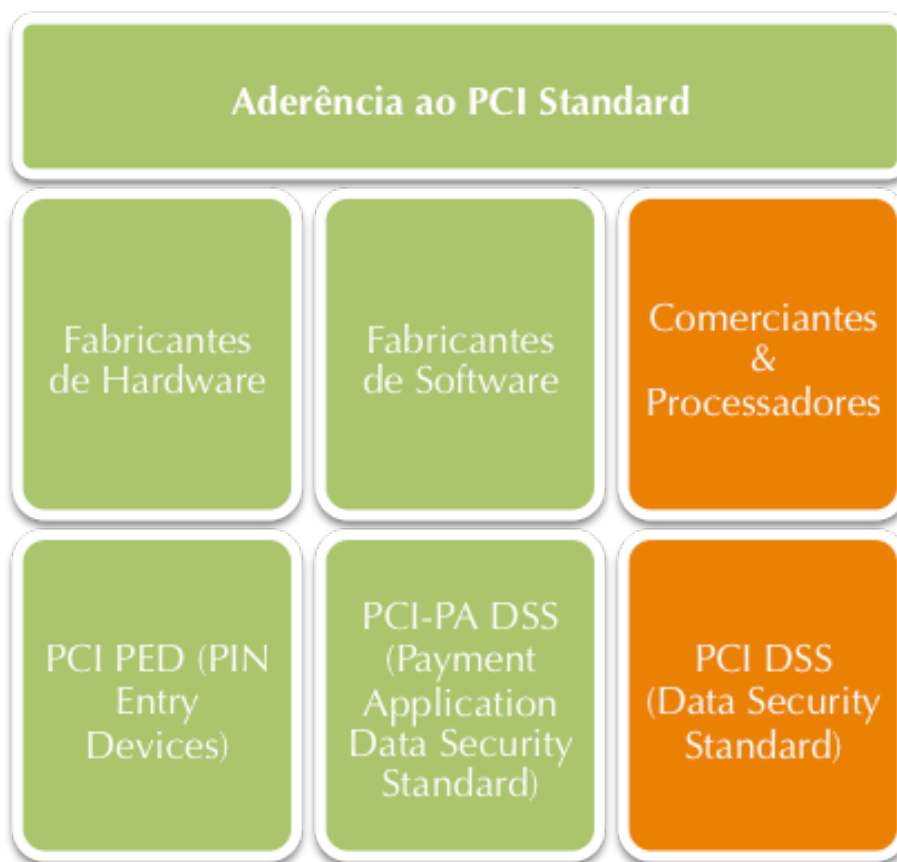
A exigência 12 é a única componente desta parte, mas é desdobrada em dez tópicos complementares que especificam exatamente o que é esperado pelo PCI DSS em uma Política de Segurança. Os controles são completamente voltados para Segurança Técnica dentro do escopo pretendido pelo padrão, e assim como a prática anterior, não deve ser confundidos com o desenvolvimento e implementação de um *Information Security Management System* (ISMS) da ISO 27001. Um ponto extremamente relevante nesta exigência, é a obrigação dos prestadores de serviços de hosting (ex. Data Center) em aderir a algumas das regras estabelecidas pelo PCI DSS.

O texto do padrão é muito claro em informar que “o prestador de serviço de *hosting* deve atender a todas essas exigências (citadas), assim como todas as outras seções relevantes do PCI DSS...”, isto abre margem a interpretação de que o padrão deve ser aplicado em qualquer local onde os dados do portador do cartão estejam sendo armazenados e/ou transmitidos, e estende a responsabilidade pela proteção a todas as partes envolvidas.

### **Como Funciona a Aderência ao PCI DSS**

A primeira questão a ser respondida é: o quão aderente a empresa precisa estar? O PCI DSS deve ser aplicado a qualquer organização que armazene, processe ou transmita os dados do portador de cartão, desde que o *Primary Account Number* (PAN) esteja dentro deste escopo. E ele normalmente está.

É necessário então classificar em qual nível de aderência a empresa deve ser incluída, o que irá determinar o tipo de trabalho de adequação necessário e as medidas de manutenção da aderência ao decorrer do tempo. O gráfico abaixo mostra o eco sistema estabelecido pelo PCI Council, onde irei abordar somente o processo de certificação com o PCI DSS.



#### A Classificação dos Comerciantes e Processadoras

O PCI DSS define cinco modelos de validação<sup>1</sup> para a aderência ao PCI DSS, baseados em como a empresa utiliza os dados do cartão de crédito. Para cada modelo, um *Self Assessment Questionnaire* (SAQ) é mantido e deve ser utilizado para a validação da necessidade de aderência, onde os controles podem ser melhor entendidos, avaliados e sua aplicabilidade verificada.

- SAQ 1: Estabelecimentos de cartão ausente (*e-commerce* ou transações pelo correio ou telefone), todas as funções de dados de portador de cartão executadas por terceiros. Esta categoria nunca se aplica a estabelecimentos com vendas frente a frente.
- SAQ 2: Estabelecimentos apenas com máquina de decalque e sem armazenamento dos dados do portador de cartão.
- SAQ 3: Estabelecimentos de terminal independente tipo *dial-up*, sem armazenamento dos dados do portador de cartão.

<sup>1</sup> Conforme apresentado no documento *Questionário de Auto-avaliação, Instruções e Diretrizes, Versão 1.1, Fevereiro de 2008*

- SAQ 4: Estabelecimentos com sistemas de aplicativo de pagamento conectados à Internet, sem armazenamento dos dados do portador de cartão.
- SAQ 5: Todos os outros estabelecimentos e todos os prestadores de serviço definidos por uma marca de pagamento como sujeitos a preencher um SAQ.

Após [entender como a empresa deve avaliar sua necessidade de aderência](#), o processo de validação de controles pode ser iniciado através da análise de atendimento a cada um dos requerimentos estabelecidos pelo PCI DSS. Algo que é interessante para as empresas neste cenário, é aproveitar este momento para entender o seu nível de classificação dentro dos critérios de quantidade de transações estabelecido pelo PCI Council, 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 Processadoras:

NÍVEL	DEFINIÇÃO DO COMERCIANTE	DEFINIÇÃO DA PROCESSADORA
1	Mais de 6 milhões de transações anuais em todos os canais de vendas.	Todos as processadoras da VisaNet 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 vendas.	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 as processadoras 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 vendas.	N/A

### Da Análise de Aderência ao ROC

Após avaliar em qual nível de atendimento aos requerimentos a empresa 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 de estimar até onde uma empresa precisa de ajuda externa para estar aderente ao PCI DSS. As consultorias especializadas são autorizadas pelo PCI Council a atuarem em dois escopos diferentes:

- **Qualified Security Assessor (QSA):** São empresas autorizadas a prestar serviços de auditoria na aderência ao PCI DSS – chamados no jargão relacionado de *On-Site Data Security Assessments* – processos de *Gap Analysis* com o padrão e demais serviços de consultoria relacionados.
- **Approved Scanning Vendor (ASV):** São empresas autorizadas a prestar serviços de *application vulnerability scans* e *penetration tests* no escopo do PCI.

Ao considerar o suporte destes dois modelos de trabalho especializado na obtenção da aderência ao padrão, as empresas devem avaliar alguns pontos de custo/benefício que irão variar de acordo com cada mercado, tipo de empresa e tamanho do escopo onde o PCI DSS é aplicável.

### **Primeiro Passo: A Análise de Aderência**

O processo de comparação dos controles existentes com os requerimentos do PCI DSS é conhecido como *gap analysis* e pode ser feito por qualquer pessoa que tenha um conhecimento mínimo de segurança. O que deve ser feito é fazer o [download do PCI DSS](#), entender os controles estabelecidos e mapear o quão aderente a empresa está. Os próprios documentos disponíveis no web site do PCI Council podem ser usados neste processo. Além do padrão estar disponível em várias línguas, existe um [FAQ bastante completo](#), e [documentos de suporte](#) para diversas atividades.

Eu recomendo que ao fazer um *gap analysis*, a empresa use o [mesmo documento](#) considerado para o *On-Site Data Security Assessment*. Este documento apresenta os controles em uma matriz de aderência bastante útil, simplificando o processo e ajudando a não esquecer nenhum dos controles apresentados. Usar uma empresa especializada em Segurança da Informação – seja um QSA ou não – para ajudar neste processo é uma questão de avaliar se a equipe da empresa tem as competência, a experiência e o tempo para esta atividade.

As maiores vantagens de ter o suporte de alguém com experiência neste tipo de atividade, é não repetir os erros ocorridos em outras empresas e poder contar com o conhecimento necessário para fazer o que é recomendado por todas as consultorias da área: reduzir o fluxo dos dados do portador do cartão ao mínimo possível. Isso permite que a aderência ao PCI DSS seja menos custosa e a manutenção dos controles mais simples, barata e eficaz. Especialmente para empresas de médio e pequeno porte, esta recomendação pode fazer uma grande diferença.

### **Segundo Passo: Implementando os Controles**

Como defendi no início deste artigo, o PCI DSS tem a vantagem de manter controles simples, eficazes dentro do escopo ao qual se propõe a abordar e altamente escalonáveis. Quando se tem o resultado do *gap analysis*, é possível analisar não só as necessidades de implementação de controles, como ainda ter uma boa perspectiva das deficiências da empresa em relação à Segurança da Informação.

Como os controles estabelecidos pelo PCI DSS podem ser aplicados a toda a empresa, é bem possível que as atividades para atender a necessidade de aderência caiam em uma das falhas mais comuns em qualquer empresa. A solução recomendada é corrigir as vulnerabilidades existentes e desenvolver os controles exigidos pelo padrão em toda a organização. Claro que isso custa dinheiro e requer um esforço que talvez não esteja disponível, e é aí que a escalonabilidade do PCI DSS pode ajudar.

Quando a aderência é o motivador para o desenvolvimento dos controles, é possível trabalhar dentro do escopo requerido pelo PCI DSS e posteriormente ampliar a aplicabilidade para os demais componentes da empresa. Especialmente quando se fala de Controle de Acesso e Política de Segurança, é muito provável que seja necessário implementar em quase toda a empresa para atender aos requerimentos do padrão, o que pode ser usado para elevar o nível de segurança de uma forma geral.

### **Terceiro Passo: A Auditoria**

Depois de implementar os controles ausentes e atender aos requisitos do PCI DSS, é necessário fazer uma auditoria que ateste a presença e eficácia dos mesmos na proteção dos dados do portador de cartão. O processo novamente depende do posicionamento da empresa dentro das categorias definidas pelo PCI Council.

Os Comerciantes classificados nos Níveis 2, 3 e 4 e as Processadoras classificadas no Nível 3, podem fazer a auditoria através do [PCI Self-Assessment Questionnaire](#), o que não requer nenhuma ajuda externa e pode ser feito pela equipe da própria empresa nos mesmos moldes apresentados para o gap analysis. Os Comerciantes classificados no Nível 1 e as Processadoras classificadas nos Níveis 1 e 2, precisam obrigatoriamente contratar um QSA para fazer a auditoria. Existem algumas discussões em andamento, na qual é defendida a posição de um grupo de auditoria interna da empresa ter a “autorização” para fazer o On-Site Data Security Assessment. Em caso de dúvidas nesta questão, a melhor coisa é [questionar diretamente o PCI Council](#).

Ao final, tendo todos os controles presentes, é necessário enviar para a bandeira de cartão de crédito ou o banco emissor – varia caso a caso, país a país, mercado a mercado – uma cópia do *PCI Self-Assessment Questionnaire* ou do *Report on Compliance (ROC)* para assegurar o atendimento aos requerimentos e a certificação de aderência.

### **Quarto Passo: A Manutenção**

Em qualquer processo de aderência a um determinado padrão – seja de segurança, qualidade ou qualquer outro mercado – a manutenção é a parte mais complicada. Além de ser necessário inserir na rotina da empresa os controles requeridos, existe toda uma dinâmica de negócios que pode ameaçar a manutenção da aderência em decisões difíceis de serem tomadas.

No caso do PCI DSS, este processo me parece o mesmo independente do nível de classificação do Comerciante ou Processadora, uma vez que a manutenção dos controles é o desafio, e provar para o PCI Council, bandeiras de cartão e bancos emissores que a empresa está aderente, é só mais um processo. Os modelos estabelecidos são:

- *On-Site Data Security Assessment* uma vez por ano e *Network Scans* a cada trimestre para os Comerciantes no Nível 1 e Processadoras nos Níveis 1 e 2.
- *PCI Self-Assessment Questionnaire* uma vez por ano *Network Scans* a cada trimestre para os Comerciantes nos Níveis 2, 3 e 4 e as Processadoras no Nível 3.

A justificativa do PCI Council para os dois modelos, está no tamanho da estrutura dos Comerciantes e Processadoras, e na divisão da análise dos controles em uma perspectiva interna (a auditoria ou o *self-assessment*) e externa (os *network scans*).

É comum ouvir críticas sobre a eficiência deste processo, e elas são muito relevantes. Certamente uma auditoria baseada em repostas a um questionário e requisição de evidências a um cliente, não mostra de forma completa como está a segurança dos controles e processos de um ambiente. Muito menos um *network scan* ou *penetration test* por si só são as ferramenta ideais para analisar as vulnerabilidades que podem ser exploradas à partir de um acesso pela Internet.

Como na aderência a qualquer padrão, a qualidade e eficiência dos controles vai depender de como a empresa se porta em relação à Segurança da Informação como um todo. Existem motivadores financeiros para isso, como os casos da [TJX](#), Bank of America, Morgan Stanley e Citibank exaustivamente citados como exemplos de falta de aderência ao PCI DSS com resultados desastrosos.

## **A Questão da Obrigatoriedade**

O PCI Council estabelece alguns prazos para que os Comerciantes e Processadoras adotem o PCI DSS, porém a obrigatoriedade depende de como as bandeiras de cartão tratam o assunto, o que também varia de acordo com cada mercado. Em alguns países existem leis que estabelecem regras de proteção para os dados de consumidores e privacidade em geral, e o PCI DSS acaba sendo somente mais um padrão a ser seguido. Em outros, as bandeiras de cartões e bancos obrigam os comerciantes a cumprirem os requerimentos ou serem multados e até perder o contrato comercial que garante o uso desta forma de pagamento. Tudo é uma questão de como o mercado se comporta.

Porém, manter a empresa aderente ao PCI DSS é parte do bom senso de proteger as informações dos portadores de cartão e evitar todos os impactos decorrentes de um acesso e uso indevido destes dados. Pessoalmente, eu vejo no mínimo quatro motivos básicos para uma empresa adotar este padrão:

- Permite que as vulnerabilidades e possibilidades de melhoria mais simples sejam identificadas, um modelo básico de segurança implementado à partir deste resultado e posteriormente ampliado para estabelecer uma estratégia de proteção integrada aos demais dados e informações considerados importantes;
- Permite proteger as informações dos clientes, o que além de evitar uma exposição desnecessária da empresa em caso de vazamentos – e os consequentes processos que podem ser movidos na maioria dos países – pode ser usado como ferramenta de marketing para diferenciar a empresa de seus concorrentes, e
- É simples e escalonável, o que o torna muito mais fácil de ser vendido internamente em uma empresa que a aderência a processos e padrões mais complexos como os da família ISO 27000.

## **Conclusão**

Como citei no começo deste artigo, a aderência ao PCI DSS pode ser considerada um snake oil por alguns setores, mas se olhada com um ponto de vista mais otimista, é o primeiro passo no aumento da proteção a qualquer ambiente. Os controles são simples, altamente escalonáveis e podem ser usados por praticamente empresas de qualquer porte e mercado. O que sempre irá determinar o nível de proteção é o quanto a gerência da empresa dá importância para isso. Sempre existirá uma queda de braço entre a Segurança da Informação e o atendimento às necessidades de negócio da empresa, e o grande desafio não muda: é equilibrar como estes dois pontos devem ser tratados.

O mesmo se aplica ao PCI DSS, a implementação deve ser equilibrada e atender ao que a empresa quer como produto final dos seus negócios (lucro, correto?) ao invés de ser colocado como mais um custo que “tem que ser endereçado” pois é uma “exigência” do mercado. A aderência ao PCI DSS é uma excelente escolha quando a empresa não tem um padrão de segurança implementado e precisa de algo para começar a proteger seu ambiente. Para aquelas que já possuem aderência a uma linha de controles, é uma oportunidade de alinhar o que está implementado com o que pode ser melhorado. As empresas ganham das duas formas.

## Sites Relacionados

Alguns dos sites abaixo relacionados são mantidos por empresas que prestam serviços relacionados aos requerimentos do PCI Council, e podem ter um forte apelo comercial. De qualquer forma, todos apresentam informação de qualidade sobre o padrão e facilitam o entendimento do processo de uma forma geral.

- [American Express Data Security](#)
- [Discover Information Security & Compliance](#)
- [JCB International Security](#)
- [MasterCard Site Data Protection Program](#)
- [PCI Standards Overview](#)
- [Visa Cardholder Information Security Program](#)
- [PCI Standard.com](#)
- [PCI Compliance Guide](#)
- [PCI Answers](#)

## Sobre o Autor

Eduardo Vianna de Camargo Neves, CISSP, está no mercado de Segurança da Informação desde 1997, onde trabalhou como auditor, consultor e gestor em uma empresa Fortune 500 do mercado de bens de consumo. É fundador e sócio da Conviso IT Security, onde atua como Gerente de Operações, responsável pela administração da empresa, gestão de parcerias e desenvolvimento de negócios internacionais. Pode ser contatado através do e-mail [eduardo@camargoneves.com](mailto:eduardo@camargoneves.com).