Conformidade com PCI-DSS - Lições Práticas

Alexandre Correia Pinto

CISSP-ISSAP, CISA, CISM, PCI QSA

SEGURANÇA DA INFORMAÇÃO:
UMA ESPECIALIDADE CIPHER

Agenda

- PCI Data Security Standard
- Mobilize e Conscientize
- Aproxime-se de um QSA
- Conheça seu Escopo
- Reduza seu Escopo
- Parceiros e Prestadores de Serviço
- Planeje a Conformidade Contínua

PCI Data Security Standard

- O PCI é uma organização do mercado de cartões de pagamento:

PCI SSC FOUNDERS

AMERICAN EXPRESS

DISCOVER NETWORK

JCB

MasterCard Worldwide

VISA

PARTICIPATING ORGANIZATIONS

Merchants, banks, processors, developers and point of sale vendors

- Visa criar padrões de operação e segurança, para preservar a infra-estrutura internacional de pagamentos por cartões.

PCI Data Security Standard

- O PCI DSS visa aumentar o nível global de segurança de pagamentos por cartão;

- Alinhamento de iniciativas pré-existentes:
  - MasterCard: Site Data Protection (SDP);
  - Visa USA: Cardholder Information Security Program (CISP);
  - Visa LatAm: Account Information Security (AIS).

- Padrão único evita inconsistências, esforços e custos redundantes - uma única avaliação atende a todos os programas.

PCI Data Security Standard

- Requisitos associados ao PCI DSS se baseiam em dois pilares:
  - Definição de *safe harbor* para *acquirers* e *issuers* no evento de incidentes/fraudes quando eles e seus *merchants* estiverem em *compliance* com os padrões;
  - Multas e outras sanções em caso de *non-compliance*.
- Quem faz o *enforcement* do padrão, estabelecendo as sanções e estímulos a conformidade são as bandeiras e não o PCI Security Standards Council.

PCI Data Security Standard

- Definição de requisitos para *merchants* e *service providers* são definidos por cada organização, mas geralmente envolvem a divisão em níveis de acordo com critérios de risco;

- Os diferentes níveis poderão ser requeridos a realizar uma ou mais das seguintes atividades:
  - Preencher e submeter regularmente um questionário de auto-avaliação de segurança;
  - Realizar varreduras de vulnerabilidades regulares em sua infra-estrutura por um ASV;
  - Sofrer auditorias *on-site* regulares de *compliance* com o PCI DSS realizada por um QSA.

PCI Data Security Standard

	Elemento de Dados	Armazenamento Permitido	Proteção Requerida	PCI DSS Exig 3.4
Dados do portador do cartão	**Número Primário de Conta (PAN)**	**SIM**	**SIM**	**SIM**
	Nome do Portador*	**SIM**	**SIM***	**NÃO**
	Código de Serviço*	**SIM**	**SIM***	**NÃO**
	Data de Expiração*	**SIM**	**SIM***	**NÃO**
Dados Sensíveis de Autenticação **	**Trilha Magnética Completa**	**NÃO**	**N/A**	**N/A**
	CVC2/CVV2/CID	**NÃO**	**N/A**	**N/A**
	PIN/ Bloco do PIN	**NÃO**	**N/A**	**N/A**

* Estes dados devem ser protegidos se armazenados em conjunto com o PAN. Esta proteção deve ser consistente com as exigências do PCI-DSS para o ambiente com dados do portador de cartão. Adicionalmente, outras proteções poderão ser necessárias para conformidade com legislação especifica (ex: Privacidade) se estes dados forem coletados e armazenados devido a necessidades de negócio. No entanto, se o PAN não for armazenado, processado ou transmitido, o PCI-DSS não se aplica.

** Os dados sensíveis de autenticação **não devem** ser armazenados após autorização da transação **em hipótese alguma** , mesmo que criptografados.

PCI Data Security Standard

Fraudador

Proteção física de documentos

Proteção da rede

Proteção de acesso lógico

Criptografia

Mobilize e Conscientize

- O maior pecado que um esforço de *compliance* de PCI DSS pode cometer é ficar restrito à área de TI ou segurança da informação;

- A conformidade com o padrão PCI DSS afetará diversas áreas de negócios de sua organização;
  - Remoção de acessos a dados e sistemas;
  - Mudança de processos e hábitos pré-existentes;
  - Reflexos orçamentários em projetos futuros ou em andamento.

- É fundamental conseguir apoio da direção da organização antes de seguir com as atividades de planejamento e conformidade.

Mobilize e Conscientize

- Envolva as bandeiras, adquirentes e QSA se possível no seu esforço de conscientização interno;
- Estabeleça um fórum / comitê de acompanhamento das iniciativas de conformidade em PCI DSS com as principais áreas envolvidas;
- Não caia na armadilha da venda negativa – conformidade não serve apenas para evitar sanções:
  - Diferencial competitivo;
  - Redução de fraudes;
  - Preservação de imagem de marca.

... mas crie expectativas realistas quanto à conformidade – PCI DSS é *baseline* -> conformidade não é invulnerabilidade.

Mobilize e Conscientize

- Não faça uma caça às bruxas – foco na obtenção da conformidade e não no levantamento de culpados pela não-conformidade.
  - Padrão é novidade para maioria;
  - Informe ao invés de criticar.

- Seu primeiro investimento de conformidade deve ser um programa formal de treinamento e conscientização organizacional sobre PCI DSS.

Aproxime-se de um QSA

- Qualified Security Assessors são empresas autorizadas pelo PCI SSC a conduzir avaliações oficiais frente ao PCI DSS;

- QSAs não têm o papel usual de uma auditoria:
  - Podem ter papel consultivo no esforço de conformidade das organizações que avaliam;
  - Relação deve estar devidamente documentada no ROC, contudo.

- É fundamental estar apoiado por empresa formalmente qualificada no padrão:
  - Interpretação adequada dos requisitos;
  - Experiência na avaliação de alternativas válidas de controles;
  - Parceria continuada facilitada internalização de conhecimento pela organização.

Conheça seu Escopo

- Um dos erros mais comuns das organizações que buscam *compliance* com PCI DSS é desconhecer o escopo real de conformidade;

- Estão no escopo todos os sistemas, redes e ativos no ambiente de armazenamento, processamento ou tráfego de dados de portadores de cartões de pagamento;
  - É necessário mapear todo o ciclo de vida dos dados de portadores de cartão na organização;
  - Parece fácil...

- Antes do PCI DSS, dados de portadores de cartão eram tratados como qualquer outro dado na organização, muitas vezes replicados desnecessariamente e sem controle;

Conheça seu Escopo

- Alguns locais óbvios são sistemas de TEF, caixas / PDV e sistemas de e-Commerce;

- Alguns locais menos óbvios:
  - Infra-estrutura de e-mail corporativo;
  - Infra-estrutura lógica e mídias de *backup*;
  - Documentos em estações de trabalho e servidores de arquivos:
    - *Call-center*;
    - Áreas de detecção e prevenção a fraudes;
    - Financeiro / Contábil (reconciliação);
    - Administradores de sistemas e DBAs.
  - Sistemas não relacionados diretamente ao fluxo de autorização:
    - ERP;
    - BI / DW.
  - Arquivos de logs de sistemas acima;
  - Relatórios em papel.

Conheça seu Escopo

- Alguns locais muito perigosos mas não menos comuns:
  - Computadores, *pen-drives* ou outras mídias de funcionários ou terceiros;
  - Contas de e-mail pessoais de funcionários ou terceiros;
  - Servidores e ambientes de rede de parceiros e prestadores de serviço;
  - *Shadow IT*.

Conheça seu Escopo

- Siga os dados de cartão:
  - Para cada sistema sabidamente no escopo:
    - Identifique suas interfaces com usuários e outros sistemas;
      - Analise as interfaces e identifique quais lidam com dados de portadores de cartão;
      - Inclua a outra ponta da interface no escopo.
    - Identifique os perfis que podem ter acesso a dados de portadores de cartão;
      - Identifique os usuários neste perfil;
      - Adicione suas áreas ao escopo.
  - Para cada área sabidamente no escopo:
    - Identifique todos os repositórios de arquivos acessíveis a membros da área (incluindo as próprias estações);
      - Valide se contém dados de portadores de cartão;
      - Identifique os demais usuários que têm acesso aos mesmos repositórios;
      - Adicione suas áreas ao escopo.
  - Identifique os responsáveis pelos ativos no escopo.

Reduza seu Escopo

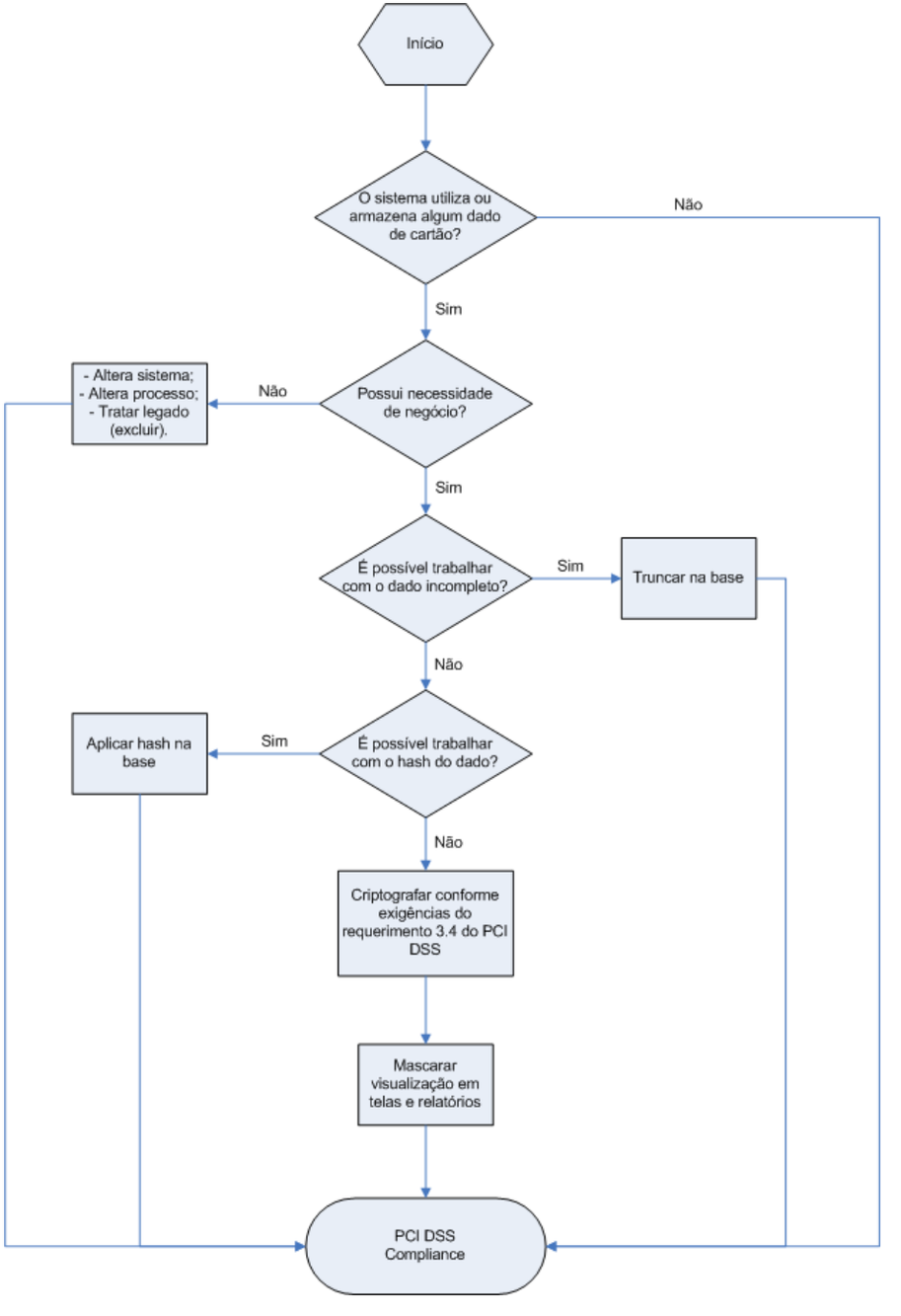
- O custo da conformidade é diretamente proporcional ao escopo:
  - Quantidade de controles que precisam ser aplicados;
  - Quantidade de ativos nos quais estes controles precisam ser aplicados.

- Estas são as principais variáveis de redução de custo e tempo para obter a conformidade;

- Grande parte do custo e complexidade da conformidade advém da exigência 3, que trata da criptografia de dados armazenados.
  - Sistemas que armazenam dados de cartão trazem mais custo do que os que apenas os processam.

Reduza seu Escopo

- Minimize os dados de cartão em seu ambiente:
  - Quanto menos repositórios diferentes de dados de cartão, melhor;
  - Quanto menos dados de cartão houver em cada repositório remanescente, melhor;
  - Quanto menos sistemas tiverem contato com dados de cartão, melhor.



Reduza seu Escopo

- Use a definição a seu favor:
  - PAN criptografado é dado de portador de cartão;
  - PAN truncado e *hash* de PAN não são dados de portador de cartão.

- Se realmente tiver que armazenar dados de cartão de forma reversível:
  - Centralize-os em base única e prepare-a para a Exigência 3;
  - Altere sistemas para consultar base central sob demanda;
  - Use um identificador alternativo (não derivável) para substituir PAN em outros sistemas e crie tabela DE/PARA na base principal.

Reduza seu Escopo

- Segmente a sua rede entre as que lidam ou não com dados de cartão:
  - Qualquer ativo em um segmento de rede onde passam dados de cartão faz parte do escopo;
  - Se sua rede interna for monolítica, TUDO estará no escopo;
  - Use um *firewall* interno ou alternativas similares para separar o ambiente de processamento de cartões do restante da sua organização;
- Controle a comunicação entre os segmentos de rede:
  - Deve ter filtragem de pacotes;
  - Deve também ter controle de acesso e trilha de auditoria adequados;
  - Não pode permitir passagem de dados de cartão ou demais redes entrarão no escopo.

Parceiros e Fornecedores

- A organização moderna faz parte de um ecossistema de parceiros e prestadores de serviço envolvidos em processos críticos;

- É muito comum que organizações tenham parceiros ou prestadores de serviço em contato com seus dados de portadores de cartão, como:
  - *Payment gateways*;
  - Processadoras;
  - Embossadoras;
  - Armazenadoras de mídias de *backup* ou documentos;
  - Provedores de serviço em modelo ASP;
  - Administradores de ativos de TI no escopo;
  - Desenvolvedores de sistemas no escopo.

Parceiros e Fornecedores

- A organização tem duas opções:
  - Ou exige contratualmente dos parceiros e prestadores que se sujeitem aos requisitos de conformidade e comprovação de conformidade e os remove de seu próprio escopo;
  - Ou terá os parceiros e prestadores considerados como parte integrante de seu próprio esforço de conformidade e comprovação de conformidade.

- A primeira opção é geralmente a mais vantajosa para as organizações, e deve ser exercitada sempre que possível;
  - PCI DSS se torna um componente viral no mercado;
  - Evita que prestadores sejam avaliados várias vezes (uma para cada cliente) e poupa custos.

- Decisão pode ser tomada por fornecedor.

Parceiros e Fornecedores

- Mesmo quando existe compromisso de conformidade do parceiro ou fornecedor, ainda é necessário:
  - Manter acompanhamento e controle formal da comprovação de conformidade dos parceiros;
  - Atentar para as interações entre a organização e seus parceiros – a responsabilidade é de ambos.
    - Interfaces entre redes e sistemas;
    - Trocas de e-mails;
    - Envio de relatórios e documentos.

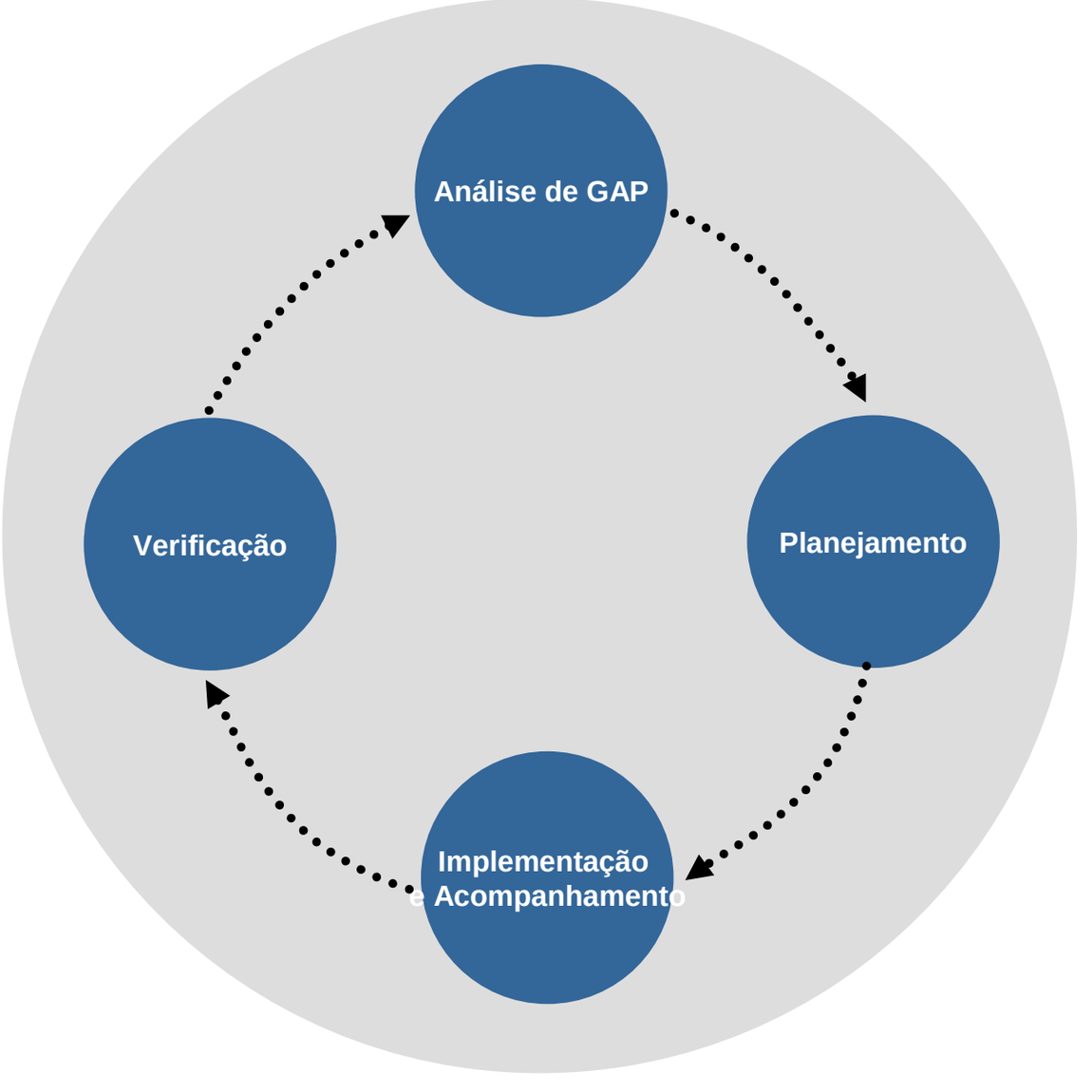
- É importante lembrar que todos os fornecedores e parceiros devem ser considerados:
  - Aqueles que não deveriam ter acesso a dados de cartão devem ter cláusulas contratuais exigindo isto;
  - Utilize segregação de rede e controle de acesso para garantir isso.

Planeje a Conformidade Contínua

- Conformidade com PCI DSS não é um projeto!
  - Segundo o PMBoK, projeto é um “esforço temporário”;
  - Conformidade com o PCI DSS deve ser mantida continuamente por prazo indeterminado, exigindo esforços contínuos.

- Lembre-se da máxima de Bruce Schneier: “Segurança é um processo e não um produto”;
  - Apesar de comprovar conformidade anualmente, as organizações devem estar em conformidade todo o tempo;
  - Desenhe controles para evitar que novos projetos, alterações aos ambientes, sistemas ou processos levem a não-conformidades;

Planeje a Conformidade Contínua



Planeje a Conformidade Contínua

- Incorpore fases de identificação de requisitos não-funcionais ligados a PCI DSS no processos de criação de projetos, desenvolvimento e aquisição de sistemas;
- Incorpore a avaliação de controles de segurança pedidos no PCI DSS e PCI PA-DSS nos modelos de RFP e contratos de produtos e serviços;
- Adicione treinamento e conscientização sobre PCI DSS na orientação de novos funcionários;
- Faça com que requisitos do PCI DSS sejam incorporados ao trabalho da Auditoria Interna.

CIPHER

Obrigado,

Alexandre Correia Pinto
CISSP-ISSAP, CISA, CISM, PCI QSA

alexandre.pinto@ciphersec.com.br