Payment Card Industry (PCI)

Indústria de Cartões de Pagamento (PCI)

Padrão de Segurança de Dados

Questionário de Auto-avaliação

Instruções e Diretrizes

Versão 1.1

Fevereiro de 2008

Índice

Sobre este Documento 1

Questionário de Auto-avaliação do Padrão de Segurança de Dados PCI: Como Tudo se Encaixa 2

Padrão de Segurança de Dados PCI: Documentos Relacionados 2

Padrão de Segurança de Dados PCI: Documentos Relacionados 3

Visão Geral do SAQ 4

Por que é Importante a Conformidade com o PCI DSS? 5

Sugestões Gerais e Estratégias para se Preparar para uma Validação da Conformidade 6

Selecionando o SAQ e a Declaração Que Melhor se Adapta à sua Organização 9

SAQ de Validação Tipo 1 / SAQ A: Estabelecimentos de Cartão Ausente, Todas as Funções de Dados do Portador de Cartão Executadas por Terceiros 9

SAQ de Validação Tipo 2 / SAQ B: Estabelecimentos Apenas com Máquina de Decalque, Sem Armazenamento Eletrônico dos Dados do Portador de Cartão 10

SAQ de Validação Tipo 3 / SAQ B: Estabelecimentos de Terminal Independente Tipo Dial-up, Sem Armazenamento dos Dados do Portador de Cartão 10

SAQ de Validação Tipo 4 / SAQ C: Estabelecimentos com Sistemas de Aplicativo de Pagamento Conectados à Internet 11

SAQ de Validação Tipo 5 / SAQ D: Todos os Outros Estabelecimentos e Todos os Prestadores de Serviço Definidos por uma Marca de Pagamento como Habilitados para Preencher um SAQ 11

Instruções para Preencher o SAQ 12

Instruções e Diretrizes do SAQ — Qual é o Meu Tipo de Validação? 13

Sobre este Documento

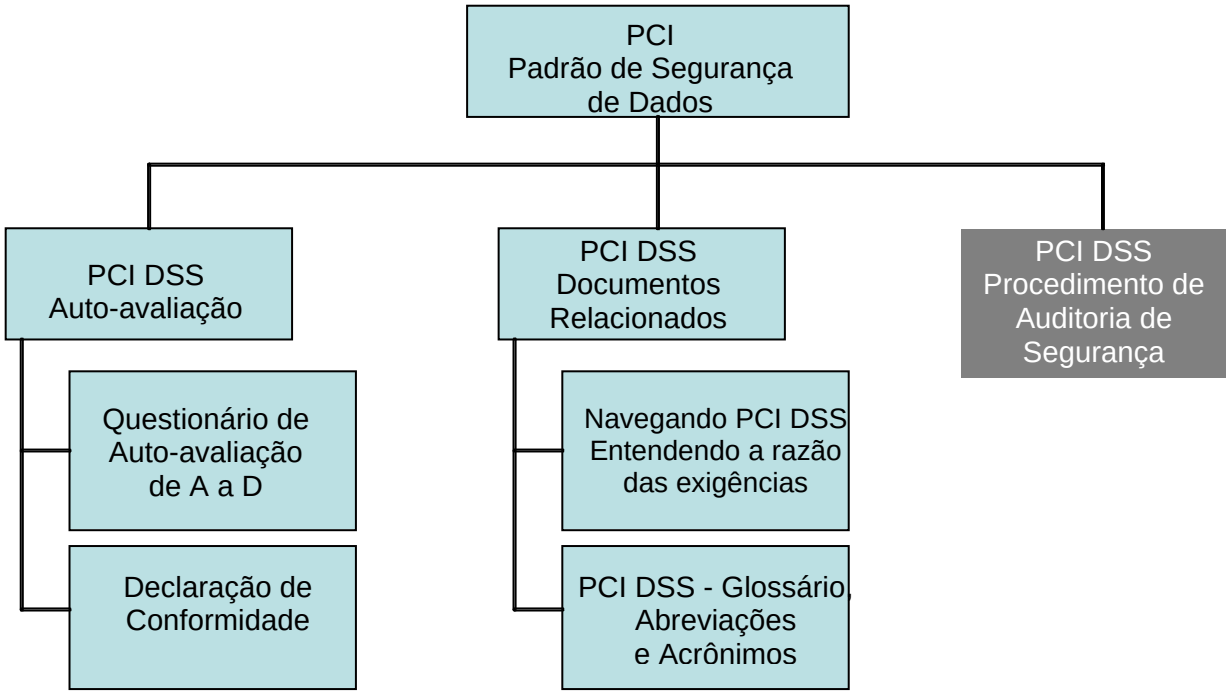
Este documento foi desenvolvido para ajudar os estabelecimentos e prestadores de serviço a compreenderem como funciona o Questionário de Auto-avaliação (Self-Assessment Questionnaire – SAQ em inglês) do Padrão de Segurança de Dados PCI (PCI Data Security Standard – DSS em inglês). Favor ler a totalidade das Instruções e Diretrizes para saber por que o PCI DSS é importante para a sua organização, que estratégias ela pode utilizar para facilitar a validação da conformidade e se a mesma se qualifica para preencher uma das versões curtas do SAQ. Os seguintes capítulos explicam o que você precisa saber sobre o PCI DSS SAQ.

- Auto-avaliação do Padrão de Segurança de Dados PCI: Como tudo se encaixa
- Padrão de Segurança de Dados PCI: Documentos relacionados
- Visão geral do SAQ
- Por que é importante a conformidade com o PCI DSS?
- Sugestões gerais e estratégias
- Selecionando o SAQ que melhor se adapta à sua organização
- Orientação para a exclusão de certas exigências específicas
- Como preencher o questionário

Questionário de Auto-avaliação do Padrão de Segurança de Dados PCI: Como Tudo se Encaixa

O Padrão de Segurança de Dados PCI e seus documentos de apoio representam um conjunto de ferramentas e medidas comuns à indústria que ajudam a garantir o manuseio seguro das informações vulneráveis ou confidenciais. O padrão oferece uma estrutura de trabalho para o desenvolvimento de um processo de segurança dos dados das contas — incluindo a prevenção, detecção e reação no caso de incidentes de segurança. Para reduzir o risco de comprometimento e os impactos, caso ocorram tais incidentes, é importante que todas as entidades que armazenam, processam ou transmitem dados do portador de cartão estejam em conformidade. O quadro abaixo destaca as ferramentas existentes para ajudar as organizações a se tornarem em conformidade com o PCI DSS e efetuarem a Auto-avaliação.

Estes e outros documentos podem ser encontrados no www.pcisecuritystandards.org.



Padrão de Segurança de Dados PCI: Documentos Relacionados

Os seguintes documentos foram criados para auxiliar os estabelecimentos e prestadores de serviços a conhecerem melhor o Padrão de Segurança de Dados PCI e o SAQ do PCI DSS.

Documento	Público Alvo
Padrão de Segurança de Dados PCI	Todos os estabelecimentos e prestadores de serviços
Navegando o PCI DSS: Entendendo a Razão das Exigências	Todos os estabelecimentos e prestadores de serviços
Padrão de Segurança de Dados PCI: Instruções e Diretrizes da Auto-avaliação,	Todos os estabelecimentos e prestadores de serviços
Padrão de Segurança de Dados PCI: Questionário de Auto-avaliação A e Declaração	Prestadores de serviços [1]
Padrão de Segurança de Dados PCI: Questionário de Auto-avaliação B e Declaração	Prestadores de serviços [1]
Padrão de Segurança de Dados PCI: Questionário de Auto-avaliação C e Declaração	Prestadores de serviços [1]
Padrão de Segurança de Dados PCI: Questionário de Auto-avaliação A e Declaração	Prestadores de serviços e todos os outros estabelecimentos [1]
Padrão de Segurança de Dados PCI: Glossário, Abreviações e Acrônimos	Todos os estabelecimentos e prestadores de serviços

[1] Para determinar qual é o Questionário de Auto-avaliação adequado, consulte o *Padrão de Segurança de Dados: Instruções e Diretrizes para a Auto-avaliação*, "*Selecionando o SAQ e a Declaração Que Melhor se Adapta à Sua Organização*."

Visão Geral do SAQ

O Questionário de Auto-avaliação do Padrão de Segurança de Dados PCI é uma ferramenta de validação que tem como objetivo auxiliar os estabelecimentos e prestadores de serviços a fazerem uma auto-avaliação da sua conformidade com o Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS). Existem múltiplas versões do PCI DSS SAQ que atendem a vários e diferentes cenários. Este documento foi desenvolvido para auxiliar as organizações a determinarem qual é o SAQ que melhor se adapta a elas.

O PCI DSS SAQ é uma ferramenta de validação para os estabelecimentos e prestadores de serviços que não são obrigados a passar por um levantamento da segurança dos dados em suas próprias instalações através dos Procedimentos de Auditoria de Segurança PCI DSS que pode vir a ser solicitado pelo seu adquirente ou marca de pagamento. Favor consultar o seu adquirente ou marca de pagamento para obter maiores detalhes sobre as exigências de validação do PCI DSS.

O PCI DSS SAQ é composto pelos seguintes componentes:

1. Questões correlacionadas às exigências do PCI DSS, apropriadas para os prestadores de serviços e estabelecimentos: Favor consultar "*Selecionando o SAQ e a Declaração Que Melhor se Adapta à Sua Organização*" adiante neste documento.
2. Declaração de Conformidade: A Declaração é a sua comprovação de que está capacitado a executar e executou a devida Auto-avaliação.

Por que é Importante a Conformidade com o PCI DSS?

Os membros do PCI Security Standards Council (American Express, Discover, JCB, MasterCard e Visa) acompanham continuamente os casos de comprometimento das contas. Estes comprometimentos ocorrem na totalidade das organizações, desde as menores até os gigantescos estabelecimentos e prestadores de serviços.

Uma quebra de segurança e o subseqüente comprometimento dos dados de um cartão de pagamento trazem profundas conseqüências para as organizações afetadas, incluindo:

1. Exigência de notificação regulamentar,
2. Perda da boa reputação,
3. Perda de clientes,
4. Possíveis responsabilidades financeiras (ex: multas regulamentares e outras taxas e encargos), e
5. Processo judicial.

As análises em casos de comprometimentos passados têm demonstrado a existência de debilidades comuns de segurança que são corrigidas pelo PCI DSS, porém o mesmo não se encontrava instalado nas organizações na ocasião em que o comprometimento ocorreu. O PCI DSS foi desenvolvido e inclui exigências detalhadas exatamente por esta razão — para minimizar a chance de comprometimento e dos seus efeitos caso ocorra uma quebra de segurança.

As investigações após o comprometimento mostraram de forma consistente uma série de violações das regras comuns do PCI DSS, incluindo mas não limitadas a:

- Armazenamento dos dados da tarja magnética (Exigência 3.2). É importante notar que muitas das entidades comprometidas não estão conscientes de que os seus sistemas estejam armazenando estes dados.
- Controles de acesso inadequados em decorrência de sistemas de POS de estabelecimentos instalados de forma imprópria, permitindo a penetração de *hachers* nas vias destinadas aos POS dos mesmos (Exigências 7.1, 7.2, 8.2 e 8.3)
- Características padrão (*default*) do sistema e senhas não modificadas quando o sistema foi instalado (Exigência 2.1)
- Existência de serviços desnecessários e vulneráveis não removidos ou reparados quando o sistema foi instalado (Exigência 2.2.2)
- Aplicações da web contando com codificação inadequada ou fraca resultando em injeção de SQL e outras vulnerabilidades, as quais permitem o acesso ao banco de dados que armazena os dados do portador de cartão, diretamente a partir do web site (Exigência 6.5)
- Falta de *patches* de segurança ou versões ultrapassadas (Exigência 6.1)
- Falta da exigência de fazer o *logging* para obter acesso (Exigência 10)
- Falta de acompanhamento (via revisão dos registros, detecção e/ou prevenção de intrusos, *scans* trimestrais de vulnerabilidade e sistemas de acompanhamento da integridade de sistemas) (Exigências 10.6, 11.2, 11.4 e 11.5)
- Falta de segmentação em uma rede, fazendo com que os dados do portador de cartão sejam facilmente acessíveis através de uma debilidade em outras partes remotas da rede (ex: a partir de pontos de acesso *wireless*, e-mail de funcionário e paginador da web) (Exigências 1.3 e 1.4)

Sugestões Gerais e Estratégias para se Preparar para uma Validação da Conformidade

São dadas a seguir algumas sugestões de caráter geral e estratégias para iniciar o processo de validação da conformidade do seu PCI DSS. Estas sugestões podem ajudá-lo a eliminar os dados que não são necessários, isolar e restringir os dados que **são** necessários a determinadas áreas controladas e centralizadas, e podem permitir que você limite o âmbito dos seus esforços de validação da conformidade do seu PCI DSS. Por exemplo, através da eliminação de dados que você não necessita e/ou isolando estes dados em áreas definidas e controladas, você pode eliminar do âmbito da sua Auto-avaliação, aqueles sistemas e redes que não mais armazenam, processam ou transmitem os dados dos portadores de cartão.

1. **Autenticação de Dados Vulneráveis (inclui o conteúdo total da tarja magnética, valores e códigos de validação e blocos de PIN):**
   a. Certifique-se de que ***estes dados nunca serão armazenados***.
   b. Se você não estiver seguro a respeito, pergunte ao seu fornecedor de POS se o software do produto e a versão usada armazenam estes dados. Alternativamente, considere a contratação de um Assessor de Segurança Qualificado que possa ajudá-lo a determinar se os dados vulneráveis de autenticação estão sendo armazenados, registrados ou capturados em algum lugar do seu sistema.

2. **Se você for um estabelecimento, indague ao seu fornecedor de POS sobre a segurança do seu sistema, fazendo as seguintes perguntas sugeridas:**
   a. O software do meu POS armazena apenas os dados da tarja magnética (dado da trilha) ou blocos de PIN? Em caso afirmativo, esta armazenagem é proibida, portanto pergunte em quanto tempo ele pode ajudá-lo a removê-los?
   b. Você pode documentar uma lista dos arquivos escritos pelo aplicativo com o resumo do conteúdo de cada um, para verificar se os dados proibidos acima mencionados não estão sendo armazenados?
   c. O sistema do seu POS requer a instalação de um *firewall* para proteger os meus sistemas contra o acesso não autorizado?
   d. São necessárias senhas complexas e únicas para que os meus sistemas possam ser acessados? Você pode me confirmar de que não são usadas senhas padrão para os meus sistemas bem como de outros estabelecimentos que você provê suporte?
   e. As senhas e parâmetros padrão foram mudados, por ocasião da instalação, no sistema e banco de dados que fazem parte do sistema de POS?
   f. Todos os serviços desnecessários e não seguros foram removidos do sistema e banco de dados que fazem parte do sistema de POS?
   g. Você pode acessar o meu POS remotamente? Em caso afirmativo, foram implementados os controles apropriados para evitar que outros possam ter acesso ao meu sistema de POS, através de métodos de acesso remoto seguro e não utilizando de senhas comuns ou padrão? Com que freqüência você acessa remotamente o meu dispositivo de POS e por quê? Quem está autorizado a acessar remotamente o meu POS?
   h. Todos os sistemas e bancos de dados que fazem parte do sistema de POS receberam um *patch* com todas as atualizações de segurança aplicáveis?
   i. A função de *logging* está habilitada para os sistemas e bancos de dados que fazem parte do sistema de POS?

j. Se as versões anteriores do meu software de POS armazenavam dados, esta capacidade foi removida durante as atualizações do software atual? Estes dados foram removidos de forma segura por um aplicativo adequado?

3. Dados do portador de cartão — se você não precisa deles, não os armazene!

a. As regras das marcas de cartão permitem o armazenamento do *Personal Account Number (PAN*), data de vencimento, nome do portador de cartão e código de serviço.

b. Faça um inventário de todas as razões e locais onde os dados são armazenados. Se os dados não são utilizados para um importante propósito de negócio, considere a sua eliminação.

c. Considere se a armazenagem destes dados e processos de negócio que eles suportam vale o seguinte:

i. O risco do comprometimento destes dados.

ii. O esforço adicional de PCI DSS que devem ser aplicados para proteger estes dados.

iii. Os contínuos esforços de manutenção para continuar em conformidade com o PCI DSS ao longo do tempo.

4. Dados do portador de cartão — se você necessita deles, faça a sua consolidação e os isole.

a. Você pode limitar o escopo de uma auditoria de PCI DSS através da consolidação da armazenagem de dados em um ambiente definido, isolando estes dados através do uso da segmentação apropriada da rede. Por exemplo, se os seus funcionários consultam a Internet e recebem e-mails no mesmo segmento de máquina ou rede que os dados do portador de cartão, considere segmentar (isolando) os dados do portador de cartão dentro da sua própria máquina ou segmento de rede (via *routers* ou *firewalls*). Se você puder isolar os dados do portador de cartão de forma eficiente, você pode ser capaz de focalizar os seus esforços de PCI DSS apenas na parte isolada ao invés de incluir todas as máquinas.

5. Considere os Controles de Compensação (aplicáveis apenas ao SAQ D)

a. Os Controles de Compensação podem ser considerados para a maioria das exigências do PCI DSS quando uma organização não pode satisfazer à especificação técnica de uma exigência, mas diminuiu de forma suficiente o risco associado. Se a sua organização não possui o exato controle especificado no PCI DSS, mas tem outros controles instalados que satisfazem a definição de controles de compensação do PCI DSS (ver o Anexo ao SAQ D e o documento *PCI DSS, Glossário, Abreviações e Acrônimos* no www.pcisecuritystandards.org), a sua organização deve fazer o seguinte:

i. Na coluna de controles de compensação do SAQ, anote o uso de cada controle de compensação usado para satisfazer uma exigência.

ii. Reveja os "*Controles de Compensação*" no Anexo e documente o uso dos mesmos através do preenchimento da Planilha de Controles de Compensação.

a) Complete uma Planilha de Controles de Compensação para cada exigência que seja atendida por um controle de compensação.

iii. Submeta todas as Planilhas de Controles de Compensação, junto com o seu SAQ preenchido e/ou Declaração, de acordo com as instruções do seu adquirente ou marca de pagamento.

6. Assistência Profissional

a. Se você desejar ter a assistência de um profissional de segurança para estabelecer a conformidade e completar o SAQ, você está incentivado a fazê-lo, mas favor compreender que, embora sua organização tenha a liberdade de utilizar o profissional de segurança da sua escolha, apenas aqueles incluídos na lista de Assessores de Segurança Qualificados (QSAs) do PCI SSC são reconhecidos como QSAs e foram treinados pelo PCI SSC. Esta lista encontra-se disponível no https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm.

Selecionando o SAQ e a Declaração Que Melhor se Adapta à sua Organização

De acordo com as regras da marca de pagamento, todos os estabelecimentos e prestadores de serviço devem estar totalmente em conformidade com o Padrão de Segurança de Dados PCI. Existem cinco categorias de SAQ de Validação, mostrados resumidamente na tabela abaixo e descritos em maiores detalhes nos parágrafos seguintes. Use esta tabela para decidir qual SAQ se aplica à sua organização e então leia as descrições detalhadas para assegurar-se de que atende a todas as exigências para aquele SAQ.

Tipo de SAQ de Validação	Descrição	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*	A
2	Estabelecimentos apenas com máquina de decalque e sem armazenamento dos dados do portador de cartão	B
3	Estabelecimentos de terminal independente tipo *dial-up*, sem armazenamento dos dados do portador de cartão	B
4	Estabelecimentos com sistemas de aplicativo de pagamento conectados à Internet, sem armazenamento dos dados do portador de cartão	C
5	Todos os outros estabelecimentos (não incluídos nas descrições dos SAQs de A a C acima) e **todos** os prestadores de serviço definidos por uma marca de pagamento como sujeitos a preencher um SAQ.	D

SAQ de Validação Tipo 1 / SAQ A: Estabelecimentos de Cartão Ausente, Todas as Funções de Dados do Portador de Cartão Executadas por Terceiros

O SAQ A foi desenvolvido para atender às exigências aplicáveis aos estabelecimentos que retêm apenas comprovantes de papel ou recibos com os dados do portador de cartão, não armazenam estes dados em formato eletrônico e não processam ou transmitem qualquer dado do cliente nas suas instalações.

Os estabelecimentos com Validação Tipo 1 não armazenam os dados do portador de cartão em formato eletrônico e não os processam ou transmitem em suas instalações e devem validar a sua conformidade preenchendo o SAQ A e a Declaração de Conformidade associada, confirmando que**:**

Para ver um guia gráfico da escolha do seu tipo de validação, favor consultar as "Instruções e Diretrizes do SAQ — Qual é o meu Tipo de Validação" na página 13.

- A sua organização manuseia apenas as transações com cartões ausentes (*e-commerce* ou transações pelo correio ou telefone);
- A sua organização não armazena, processa ou transmite quaisquer dados do portador de cartão em suas instalações, mas confia totalmente em um prestador de serviço externo para executar estas funções;
- A sua organização confirmou que o prestador de serviço que executa o armazenamento, processamento e/ou transmissão dos dados do portador de cartão encontra-se em conformidade

com o PCI DSS;

- A sua organização retém apenas os comprovantes ou recibo de papel com os dados do portador de cartão e que estes documentos não são recebidos eletronicamente; **e**
- A sua organização não armazena nenhum dado do portador de cartão em formato eletrônico.

Esta opção nunca se aplica aos estabelecimentos com um ambiente de POS frente a frente.

SAQ de Validação Tipo 2 / SAQ B: Estabelecimentos Apenas com Máquina de Decalque, Sem Armazenamento Eletrônico dos Dados do Portador de Cartão

O SAQ B foi desenvolvido para atender às exigências aplicáveis aos estabelecimentos que processam os dados do portador de cartão apenas via máquinas de decalque ou terminais independentes (*stand-alone*) tipo *dial-up*.

Os estabelecimentos com Validação Tipo 2 processam os dados do portador de cartão apenas via máquina de decalques e devem validar a sua conformidade através do preenchimento do SAQ B e da Declaração de Conformidade associada, confirmando que:

- A sua organização se utiliza apenas de máquinas de decalque para obter a informação do cartão de pagamento do seu cliente;
- A sua organização não transmite os dados do portador de cartão através de linha telefônica ou pela Internet;
- A sua organização retém apenas cópias em papel dos recibos; e
- A sua organização não armazena os dados do portador de cartão em formato eletrônico.

Para ver um guia gráfico da escolha do seu tipo de validação, favor consultar as "Instruções e Diretrizes do SAQ — Qual é o meu Tipo de Validação" na página 13.

SAQ de Validação Tipo 3 / SAQ B: Estabelecimentos de Terminal Independente Tipo Dial-up, Sem Armazenamento dos Dados do Portador de Cartão

O SAQ B foi desenvolvido para atender às exigências aplicáveis aos estabelecimentos que processam os dados do portador de cartão apenas por intermédio de máquinas de decalque ou terminais independentes do tipo *dial-up*.

Os estabelecimentos com Validação Tipo 3 processam os dados do portador de cartão através de terminais independentes do tipo *dial-up* e podem ser estabelecimentos normais de rua (cartão presente) ou de *e-commerce*, transações feitas pelo correio ou telefone (cartão ausente). Os estabelecimentos com Validação Tipo 3 devem dar validade à sua conformidade através do preenchimento do SAQ B e da Declaração de Conformidade associada, confirmando que:

- A sua organização usa apenas terminais independentes do tipo *dial-up* (conectados ao seu processador através de uma linha telefônica);
- Os terminais independentes tipo *dial-up* não estão conectados a nenhum outro sistema dentro do seu ambiente;
- Os terminais independentes tipo *dial-up* não se encontram conectados à Internet;
- A sua organização mantém apenas relatórios em papel ou cópia dos recibos em papel; e
- A sua organização não armazena os dados do portador de cartão em formato eletrônico.

SAQ de Validação Tipo 4 / SAQ C: Estabelecimentos com Sistemas de Aplicativo de Pagamento Conectados à Internet

O SAQ C foi desenvolvido para atender às exigências aplicáveis aos estabelecimentos cujos sistemas de aplicativo de pagamento (por exemplo, sistemas de ponto de venda ou carrinho de compras) estão conectados via Internet (via conexão de alta velocidade, DSL, *modem* de cabo de alta velocidade, etc.) seja porque:

1. O sistema de aplicativo de pagamento se encontra em um computador pessoal que está ligado à Internet (por exemplo, para e-mail ou *web browsing*), ou
2. O sistema de aplicativo de pagamento está conectado à Internet para transmitir os dados do portador de cartão.

Os estabelecimentos com Validação Tipo 4 processam os dados do portador de cartão através de sistemas de aplicativos de pagamento conectados à Internet, não armazenam estes dados em nenhum sistema de computador e podem ser tanto um estabelecimento tradicional com transação de cartão presente ou *e-commerce* ou transações feitas pelo correio ou telefone (cartão ausente). Os estabelecimentos com Validação Tipo 4 devem dar validade à sua conformidade através do preenchimento do SAQ C e da Declaração de Conformidade associada, confirmando que:

- A sua organização possui um sistema de aplicativo de pagamento e uma conexão com a Internet no mesmo dispositivo;
- O sistema de aplicativo de pagamento e o dispositivo de Internet não se encontram conectados a nenhum outro sistema dentro do seu ambiente;
- A sua organização retêm apenas os relatórios em papel e as cópias dos recibos de papel;
- A sua organização não armazena os dados do portador de cartão em formato eletrônico; e
- O fornecedor do software de aplicativo de pagamento da sua organização usa técnicas seguras para prestar suporte remoto ao seu sistema de aplicativo de pagamento.

Para ver um guia gráfico da escolha do seu tipo de validação, favor consultar as "Instruções e Diretrizes do SAQ — Qual é o meu Tipo de Validação" na página 13.

SAQ de Validação Tipo 5 / SAQ D: Todos os Outros Estabelecimentos e Todos os Prestadores de Serviço Definidos por uma Marca de Pagamento como Habilitados para Preencher um SAQ

O SAQ D foi desenvolvido para atender às exigências aplicáveis a todos os prestadores de serviço definidos por uma marca de pagamento como habilitados a preencherem um SAQ e aqueles estabelecimentos que não se enquadram na Validação do Tipo 1 a 4 acima.

Os prestadores de serviço e estabelecimentos que se enquadram na Validação Tipo 5 devem dar validade à sua conformidade através do preenchimento do SAQ D e da Declaração de Conformidade associada.

Embora muitas das organizações que preenchem o SAQ D tenham a necessidade de validar a conformidade referente a cada exigência PCI DSS, algumas possuidoras de modelos de negócio muito específicos podem concluir que algumas das exigências não se aplicam. Por exemplo, uma empresa que não se utiliza da tecnologia *wireless* em qualquer das suas formas não poderá validar a conformidade para com as seções do PCI DSS que são específicas da tecnologia *wireless*. Favor consultar as instruções a seguir sobre a exclusão da tecnologia *wireless* e algumas outras exigências específicas.

Instrução para a Exclusão de Determinadas Exigências Específicas

Se for determinado que você deve responder ao SAQ D para validar a sua conformidade ao PCI DSS, as seguintes exceções poderão ser consideradas (você puder marcar estas exigências com um "N/A" se elas não se aplicarem ao seu ambiente):

- As perguntas específicas sobre *wireless* precisam apenas ser respondidas se a tecnologia *wireless* estiver presente em qualquer parte da sua rede (Exigências 1.3.8, 2.1.1 e 4.1.1). Favor notar que a Exigência 11.1 (uso de um analisador de *wireless*) deve ser respondida mesmo que não haja um dispositivo *wireless* em sua rede, visto que o analisador detecta qualquer dispositivo mal intencionado ou não autorizado que possa ter sido adicionado sem o seu conhecimento.
- As perguntas específicas a respeito de aplicativos customizados e códigos (Exigências 6.3 a 6.5) necessitam ser respondidas apenas se a sua organização desenvolver seus próprios aplicativos customizados de rede.
- As perguntas específicas para os centros de processamento de dados (Exigências 9.1 a 9.4), devem ser respondidas apenas se você possuir um centro de dados ou ambiente de servidor dedicado. Um centro de dados é definido pelo PCI SSC como uma sala ou estrutura dedicada e fisicamente segura onde a infra-estrutura de tecnologia da informação (servidores de aplicativos, servidores de banco de dados, servidores de rede e/ou dispositivos de rede) encontra-se centralmente instalada, e cujo propósito principal é a armazenagem, processamento ou transmissão dos dados do portador de cartão. Central de dados ou "*data center*" pode ser sinônimo de sala do servidor, centro de operação de rede ou "*network operations center* "– *NOC* em inglês ou instalações em um ISP ou provedor de hosting.

Instruções para Preencher o SAQ

1. Use as diretrizes aqui contidas para determinar qual SAQ é apropriado para a sua organização.
2. Use o "*Navegando o PCI DSS: Entendendo a Razão das Exigências"* para entender como e porque as exigências são relevantes para a sua organização.
3. Use o Questionário de Auto-avaliação apropriado como uma ferramenta para validar a sua conformidade com o PCI DSS.
4. Siga as instruções do Questionário de Auto-avaliação apropriado no Conformidade com o PCI DSS – Etapas para o Preenchimento, e entregue toda a documentação requerida ao seu adquirente ou marca de pagamento conforme apropriado.

Instruções e Diretrizes do SAQ — Qual é o Meu Tipo de Validação?