Setor de cartões de pagamento (PCI)
Padrão de segurança de dados

Questionário de auto-avaliação

Diretrizes e instruções

Versão 2.0

Outubro de 2010

Alterações no documento

Data	Versão	Descrição
1º de outubro de 2008	1.2	Para alinhar o conteúdo com o novo PCI DSS v1.2 e para implementar alterações menores observadas desde o original v1.1.
28 de outubro de 2010	2.0	Para alinhar o conteúdo com o novo PCI DSS v2.0 e esclarecer os tipos de ambientes e os critérios de qualificação do SAQ. Adição do SAQ C-VT para comerciantes com acesso via terminal virtual baseado na Web.

Índice

Sobre este documento

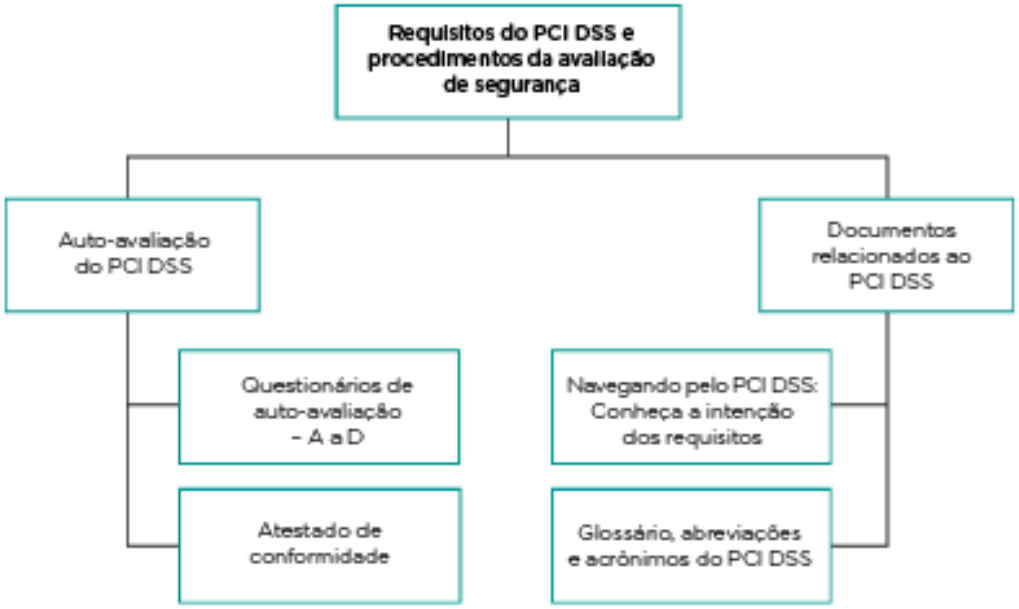
Este documento foi desenvolvido para ajudar comerciantes e prestadores de serviços a entenderem os Questionários de auto-avaliação (SAQ) do Padrão de segurança de dados do setor de cartões de pagamento (PCI DSS). Leia este documento inteiro de Instruções e diretrizes para entender por que o PCI DSS é importante para sua organização, quais estratégias sua organização pode usar para facilitar a validação da conformidade e se sua organização está qualificada para preencher uma das versões resumidas do SAQ. As seções a seguir apresentam as informações necessárias sobre o SAQ do PCI DSS.

- Auto-avaliação do PCI DSS: Como tudo se encaixa
- PCI DSS: Documentos relacionados
- Visão geral do SAQ
- Por que a conformidade com o PCI DSS é importante?
- Dicas e estratégias gerais para se preparar para a validação da conformidade
- Selecionando o SAQ e o Atestado que melhor se aplicam à sua organização
- Orientação para não aplicabilidade de determinados requisitos específicos
- Instruções para preencher o SAQ
- Qual SAQ melhor se aplica ao meu ambiente?

Auto-avaliação do PCI DSS: Como tudo se encaixa

O PCI DSS e os documentos de suporte representam um conjunto em comum das ferramentas e medições do setor para ajudar a garantir o manuseio seguro de informações confidenciais. O padrão fornece uma estrutura litigável para desenvolver um processo robusto de segurança de dados da conta, incluindo prevenção, detecção e reação a incidentes de segurança. Para reduzir o risco de comprometimento e mitigar seus impactos, caso isso ocorra, é importante que todas as entidades que armazenam, processam ou transmitem dados de titulares de cartão cumpram os requisitos. O gráfico abaixo apresenta as ferramentas existentes para ajudar as organizações a cumprirem o PCI DSS e a fazerem a auto-avaliação.

Esse e outros documentos relacionados podem ser encontrados em www.pcisecuritystandards.org.



Padrão de segurança de dados do PCI: Documentos relacionados

Os documentos a seguir foram criados para auxiliar comerciantes e prestadores de serviços a entenderem o PCI DSS e o SAQ do PCI DSS.

Documento	Público
Padrão de segurança de dados do PCI: Requisitos e procedimentos da avaliação de segurança	Todos os comerciantes e prestadores de serviços
Navegando pelo PCI DSS: Entendendo o porquê dos requisitos	Todos os comerciantes e prestadores de serviços
Padrão de segurança de dados do PCI: Diretrizes e instruções de auto-avaliação	Todos os comerciantes e prestadores de serviços
Padrão de segurança de dados do PCI: Questionário A de auto-avaliação e atestado	Comerciantes qualificados[1]
Padrão de segurança de dados do PCI: Questionário B de auto-avaliação e atestado	Comerciantes qualificados[1]
Padrão de segurança de dados do PCI: Questionário C-VT de auto-avaliação e atestado	Comerciantes qualificados[1]
Padrão de segurança de dados do PCI: Questionário C de auto-avaliação e atestado	Comerciantes qualificados[1]
Padrão de segurança de dados do PCI: Questionário D de auto-avaliação e atestado	Comerciantes e prestadores de serviços qualificados[1]
Padrão de segurança de dados do PCI e Padrão de segurança de dados de aplicativos de pagamento: Glossário de termos, abreviações e acrônimos	Todos os comerciantes e prestadores de serviços

[1] Para determinar o Questionário de auto-avaliação apropriado, consulte a seção "Selecionando o SAQ e o Atestado que melhor se aplicam à sua organização" na página 12 deste documento.

Visão geral do SAQ

O *Questionário de auto-avaliação (SAQ) do PCI DSS* é uma ferramenta de validação destinada a auxiliar comerciantes e prestadores de serviços a auto-avaliarem sua conformidade em relação ao Padrão de segurança de dados do setor de cartões de pagamento (PCI DSS). Existem várias versões do SAQ do PCI DSS, que se encaixam em vários cenários. Este documento foi desenvolvido para ajudar as organizações a determinarem qual o SAQ que melhor se aplica a elas.

O SAQ do PCI DSS é uma ferramenta de validação para comerciantes e prestadores de serviços que não são obrigados a apresentar um Relatório de conformidade da avaliação de segurança dos dados no local de acordo com os *Requisitos do PCI DSS e procedimentos da avaliação de segurança* e que pode ser exigido pelo adquirente ou pela bandeira. Consulte o adquirente ou a bandeira para obter detalhes sobre os requisitos de validação do PCI DSS.

O SAQ do PCI DSS é formado pelos seguintes componentes:

1. Perguntas relacionadas aos requisitos do PCI DSS, adequadas para os prestadores de serviços e comerciantes: Consulte a seção "Selecionando o SAQ e o Atestado que melhor se aplicam à sua organização", neste documento.
2. Atestado de conformidade: O atestado é a certificação de que você está qualificado para executar e executou uma auto-avaliação do PCI DSS.

Por que a conformidade com o PCI DSS é importante?

Os membros do PCI Security Standards Council (American Express, Discover, JCB, MasterCard e Visa) monitoram continuamente casos de comprometimento de dados da conta. Esses comprometimentos cobrem o espectro total das organizações, dos menores até os maiores comerciantes e prestadores de serviços.

Uma violação de segurança e o subsequente comprometimento dos dados do cartão de pagamento têm grandes consequências para as organizações afetadas, a saber:

1. Exigências de notificação regulatória,
2. Perda de reputação,
3. Perda de clientes,
4. Possíveis responsabilidades financeiras (como responsabilidades regulatórias e outras taxas e multas), e
5. Processos.

A análise de comprometimento post-mortem demonstrou pontos fracos em comum na segurança que são resolvidos pelo PCI DSS, mas que não estavam implementados nas organizações quando ocorreram os comprometimentos. O PCI DSS foi feito e inclui requisitos detalhados exatamente por isso: minimizar a chance de comprometimento e os efeitos, caso comprometimentos de fato ocorram.

Investigações após comprometimentos mostram sempre violações comuns no PCI DSS, incluindo, mas não de forma exclusiva:

- Armazenamento dos dados da tarja magnética (Requisito 3.2). É importante observar que várias entidades comprometidas não estão cientes de que seus sistemas estão armazenando esses dados.
- Controles de acesso inadequado decorrentes de sistemas de POS instalados inadvertidamente no comerciante, permitindo que hackers entrem por caminhos destinados aos fornecedores do POS (Requisitos 7.1, 7.2, 8.2 e 8.3)
- Configurações e senhas padrão do sistema não alteradas durante a configuração do sistema (Requisito 2.1)
- Serviços desnecessários e inseguros não removidos ou não protegidos durante a configuração do sistema (Requisitos 2.2.2 e 2.2.4)
- Aplicativos da Web mal-codificados, resultando em injeção SQL e outras vulnerabilidades, dando acesso aos bancos de dados que armazenam os dados do titular do cartão a partir do site (Requisito 6.5)
- Patches de segurança ausentes e desatualizados (Requisito 6.1)
- Falta de log (Requisito 10)
- Falta de monitoramento (por análise do log, detecção/prevenção de intrusões, varreduras trimestrais de vulnerabilidades e sistema de monitoramento da integridade dos arquivos) (Requisitos 10.6, 11.2, 11.4 e 11.5)
- Implementação de uma segmentação de rede fraca resultando na exposição involuntária do ambiente de dados do titular do cartão a falhas em outras partes da rede que não foram protegidas de acordo com o PCI DSS (por exemplo: a partir de pontos de acesso sem fio desprotegidos e vulnerabilidades introduzidas através do e-mail do funcionário e da navegação na Web) (Requisitos 1.2, 1.3 e 1.4)

Dicas e estratégias gerais para se preparar para a validação da conformidade

A seguir, são apresentadas algumas dicas e estratégias gerais para o início das suas atividades de validação de conformidade com o PCI DSS. Essas dicas podem ajudá-lo a eliminar os dados que não forem necessários, isolar os dados necessários para áreas centralizadas definidas e controladas e permitir que você limite o escopo das atividades de validação da conformidade com o PCI DSS. Por exemplo: ao eliminar os dados desnecessários e/ou isolar os dados necessários para áreas definidas e controladas, é possível remover sistemas e redes que não armazenam, processam ou transmitem dados do titular do cartão e não se conectam aos sistemas que o fazem, a partir do escopo da sua auto-avaliação.

1. **Dados de autenticação confidenciais (incluindo o conteúdo total da tarja magnética ou do chip, valores e códigos de verificação do cartão, PINs e blocos de PIN):**
   a. Certifique-se de ***nunca armazenar esses dados***.
   b. Se você não tiver certeza, pergunte ao fornecedor do POS se o software e a versão que você utiliza armazenam esses dados. Você também podem pensar em contratar um Assessor de Segurança Qualificado que possa ajudá-lo a determinar se a autenticação confidencial está sendo armazenada, registrada em log ou capturada em algum outro lugar dos seus sistemas.
2. **Se você for comerciante, pergunte ao fornecedor do POS sobre a segurança do sistema. Sugerimos as seguintes perguntas:**
   a. O meu software do POS foi validado pelo Padrão de segurança de dados de aplicativos de pagamento (PA-DSS)? (Consulte a lista do PCI SSC de Aplicativos de pagamento validados.)
   b. O software do meu POS armazena dados da tarja magnética (dados de rastreamento) ou blocos de PIN? Em caso afirmativo, esse armazenamento é proibido. Em quanto tempo vocês conseguem me ajudar a removê-lo?
   c. O meu software do POS armazena números da conta primária (PANs)? Em caso afirmativo, esse armazenamento deve ser protegido. Como o POS está protegendo esses dados?
   d. Vocês documentarão a lista de arquivos gravados pelo aplicativo com um resumo do conteúdo de cada arquivo, a fim de verificar que os dados proibidos supramencionados não estão sendo armazenados?
   e. Seu sistema do POS exige que eu instale um firewall para proteger meus sistemas contra acesso não autorizado?
   f. Eu preciso de senhas complexas e exclusivas para acessar meus sistemas? Você pode confirmar que não usa senhas padrão ou iguais para mim e para os sistemas de comerciantes a quem vocês dão suporte?
   g. As configurações e senhas padrão foram alteradas nos sistemas e bancos de dados que fazem parte do sistema do POS?
   h. Todos os serviços desnecessários e inseguros foram removidos dos sistemas e bancos de dados que fazem parte do sistema do POS?
   i. Você acessa meu sistema do POS remotamente? Em caso positivo, você implementou controles adequados para evitar que outras pessoas acessem meu sistema do POS, como a utilização de métodos de acesso remoto protegidos e a não utilização de senhas iguais ou padrão? Com que frequência você acessa remotamente meu dispositivo de POS? E por quê? Quem está autorizado a acessar remotamente meu POS?

j. Todos os sistemas e bancos de dados que fazem parte do sistema do POS receberam os patches de todas as atualizações de segurança aplicáveis?

k. A capacidade de log foi ativada para os sistemas e bancos de dados que fazem parte do sistema do POS?

l. Se versões anteriores do meu software do POS armazenavam dados de rastreamento, esse recurso foi removido durante as atualizações atuais para o software do POS? Foi utilizado um utilitário de limpeza segura para remover esses dados?

3. Dados do titular do cartão – se você não precisar, não os armazene!

a. As regras da bandeira permitem o armazenamento do número da conta pessoal (PAN), da data de validade, do nome do titular do cartão e do código de serviço.

b. Faça um inventário de todos os motivos e de todos os lugares onde você armazena esses dados. Se os dados não tiverem um bom objetivo corporativo, pense em eliminá-los.

c. Pense se o armazenamento desses dados e do processo de negócios que o suporta valem o seguinte:

i. O risco de comprometer os dados.

ii. As atividades adicionais do PCI DSS que devem ser aplicadas para proteger esses dados.

iii. As atividades de manutenção contínuas para manter o PCI DSS compatível com o tempo.

4. Dados do titular do cartão – se você precisa deles, consolide-os ou isole-os.

É possível limitar o escopo de uma avaliação do PCI DSS consolidando o armazenamento de dados em um ambiente definido e isolando os dados através do uso de uma segmentação de rede adequada. Por exemplo: se seus funcionários navegarem na internet e receberem e-mails na mesma máquina ou segmento de rede dos dados do titular do cartão, pense em segmentar (isolar) os dados do titular do cartão em uma máquina ou segmento de rede exclusivo (por meio de roteadores ou firewalls). Se for possível isolar com eficácia os dados do titular do cartão, será possível concentrar os esforços do PCI DSS somente na parte isolada, ao invés de incluí-los em todas as máquinas.

5. Controles de compensação

Os controles de compensação podem ser considerados para a maioria dos requisitos do PCI DSS quando a organização não conseguir atender a especificação técnica de um requisito, mas mitigar com eficiência o risco associado através de controles alternativos. Se sua empresa não possuir o controle exato especificado no PCI DSS mas possuir outros controles em vigor que satisfazem a definição do PCI DSS dos controles de compensação (consulte a seção "Controles de compensação" no Anexo do SAQ aplicável e o documento *Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS* no endereço www.pcisecuritystandards.org), sua empresa deverá executar as seguintes ações:

a. Responder "SIM" à pergunta do SAQ e, na coluna "Especial", anotar o uso de cada controle de compensação usado para atender um requisito.

b. Analisar a seção "Controles de compensação" no Anexo B e documentar o uso dos controles de compensação preenchendo a Planilha dos controles de compensação no Anexo C do SAQ.

c. Preencher uma Planilha dos controles de compensação para cada requisito que for cumprido com um controle de compensação.

d. Enviar todas as Planilhas dos controles de compensação junto com o Atestado e/ou SAQ preenchido segundo as instruções do adquirente ou da bandeira.

6. Treinamento e ajuda profissional

a. Se você quiser ter orientação de um profissional de segurança para obter a conformidade e preencher o SAQ, tem o nosso incentivo. Reconheça que, apesar de você ser livre para usar qualquer profissional de segurança de sua escolha, somente aqueles incluídos na lista do PCI SSC de Assessores de Segurança Qualificados (QSAs) são reconhecidos como QSAs e treinados pelo PCI SSC. Essa lista está disponível no endereço https://www.pcisecuritystandards.org.

b. O PCI Security Standards Council (SSC) fornece uma variedade de recursos educacionais para promover a conscientização de segurança no setor de cartões de pagamento. Esses recursos incluem treinamento do PCI DSS para Assessores de segurança interna (ISAs) e Treinamento de padrões. O site do PCI SSC também é uma fonte primária de recursos adicionais, incluindo:

- O guia *Navegando pelo PCI DSS*
- O *Glossário de termos, abreviações e acrônimos do PCI DSS*
- Perguntas frequentes (FAQs)
- Webinars
- Suplementos informativos e orientações
- Atestado de conformidade

Consulte o site www.pcisecuritystandards.org para obter mais informações.

Observação: *Os Suplementos informativos complementam o PCI DSS e identificam considerações adicionais e recomendações para atender aos requisitos do PCI DSS - eles não alteram, eliminam ou sobrepõem o PCI DSS ou qualquer de seus requisitos*.

Consulte a seção "Selecionando o SAQ e o Atestado que melhor se aplicam à sua organização", neste documento.

Segundo as regras da bandeira, todos os comerciantes e prestadores de serviços precisam obedecer integralmente ao PCI DSS. Existem cinco categorias do SAQ, exibidas brevemente na tabela abaixo e descritas com mais detalhes nos parágrafos seguintes. Use a tabela para determinar qual SAQ se aplica à sua organização e, em seguida, analise as descrições detalhadas para garantir que você esteja cumprindo todos os requisitos desse SAQ.

SAQ	Descrição
A	Comerciantes do tipo cartão não presente (comércio eletrônico ou pedidos por correio/telefone), todas as funções dos dados do titular do cartão são terceirizadas. *Isso nunca se aplica a comerciantes presenciais.*
B	Comerciantes com máquinas de carbono, sem armazenamento eletrônico dos dados do titular do cartão, ou comerciantes com terminais de discagem independentes, sem armazenamento eletrônico dos dados do titular do cartão
C-VT	Comerciantes que usam somente terminais virtuais baseados na Web, sem armazenamento eletrônico dos dados do titular do cartão
C	Comerciantes com sistemas de aplicativos de pagamento conectados à Internet, sem armazenamento eletrônico dos dados do titular do cartão
D	Todos os outros comerciantes não incluídos nas descrições dos SAQs A a C acima e **todos** os **prestadores de serviços** definidos por uma bandeira como qualificados para preencherem um SAQ.

SAQ A – Comerciantes do tipo cartão não presente, todas as funções dos dados do titular do cartão são terceirizadas

O SAQ A foi desenvolvido para resolver os requisitos aplicáveis aos comerciantes que retêm somente relatórios em papel ou recibos com os dados do titular do cartão, que não armazenam os dados do titular do cartão em formato eletrônico e que não processam nem transmitem dados do titular do cartão em suas instalações.

Se você preferir usar um guia visual para selecionar o seu tipo de SAQ, consulte a seção "Qual SAQ melhor se aplica ao meu ambiente?" na página 17.

Os comerciantes do SAQ A não armazenam dados do titular do cartão em formato eletrônico nem processam nem transmitem dados do titular do cartão em suas instalações, e validam a conformidade ao preencherem o SAQ A e o Atestado de conformidade associado, confirmando que:

- Sua empresa aceita somente transações sem a presença do cartão (comércio eletrônico ou pedidos por correio/telefone);
- Sua empresa não armazena, processa ou transmite nenhum dado do titular do cartão nos seus sistemas e nas suas instalações, mas confia totalmente em uma empresa terceirizada para lidar com essas funções;
- Sua empresa confirmou que os terceiros que lidam com armazenamento, processamento e/ou transmissão dos dados do titular do cartão são compatível com o PCI DSS;

- Sua empresa retém somente relatórios ou recibos em papel com os dados do titular do cartão e esses documentos não são recebidos eletronicamente; **e**
- Sua empresa não armazena dados do titular do cartão em formato eletrônico.

Essa opção nunca se aplica a comerciantes com um ambiente de POS presencial.

SAQ B – Comerciantes que usam somente máquinas de carbono ou somente terminais de discagem independentes. Sem armazenamento eletrônico dos dados do titular do cartão.

O SAQ B foi desenvolvido para abordar requisitos aplicáveis aos comerciantes que processam os dados do titular do cartão somente em máquinas de carbono ou terminais de discagem independentes.

Se você preferir usar um guia visual para selecionar o seu tipo de SAQ, consulte a seção "Qual SAQ melhor se aplica ao meu ambiente?" na página 17.

Os comerciantes do SAQ B só processam os dados do titular do cartão por meio de máquinas de carbono ou terminais de discagem independentes, podendo ser do tipo real (cartão presente) ou comércio eletrônico ou pedidos por correio/telefone (cartão não presente). Esses comerciantes validam a conformidade ao preencherem o SAQ B e o Atestado de conformidade associado, confirmando que:

- Sua empresa usa somente máquinas de carbono e/ou terminais de discagem independentes (conectados por uma linha telefônica ao processador) para pegar as informações do cartão de pagamento dos clientes;
- Os terminais de discagem independentes não estão conectados a nenhum outro sistema dentro do seu ambiente;
- Os terminais de discagem independentes não estão conectados à Internet;
- Sua empresa não transmite os dados do titular do cartão pela rede (rede interna ou Internet);
- Sua empresa retém somente relatórios ou cópias em papel dos recibos com os dados do titular do cartão e esses documentos não são recebidos eletronicamente; **e**
- Sua empresa não armazena dados do titular do cartão em formato eletrônico.

SAQ C-VT – Comerciantes com terminais virtuais baseados na Web, sem armazenamento eletrônico dos dados do titular do cartão

O SAQ C-VT foi desenvolvido para abordar requisitos aplicáveis aos comerciantes que processam os dados do titular do cartão somente através de terminais virtuais isolados em computadores pessoais conectados à Internet.

Se você preferir usar um guia visual para selecionar o seu tipo de SAQ, consulte a seção "Qual SAQ melhor se aplica ao meu ambiente?" na página 17.

Um terminal virtual é um acesso baseado no navegador da Web ao site do adquirente, processador ou prestador de serviços terceirizado para autorização de transações com cartões de pagamento, no qual o comerciante insere manualmente os dados do cartão de pagamento através de navegador da Web seguramente conectado. Diferentes dos terminais físicos, os terminais virtuais não leem dados diretamente do cartão de pagamento. Como as transações com o cartão de pagamento são inseridas manualmente, os terminais virtuais são usados ao invés de terminais físicos normalmente em ambientes comerciais com volumes de transação baixos.

Esses comerciantes processam os dados do titular do cartão somente através de um terminal virtual e não armazenam os dados do titular do cartão em nenhum sistema de computador. Esses terminais

virtuais estão conectados à Internet para acessar terceiros que hospedam as funções de processamento do pagamento do terminal virtual. Esse terceiro pode ser um processador, um adquirente ou qualquer prestador de serviços terceirizado que armazena, processa e/ou transmite dados do titular do cartão para autorizar e/ou estabelecer transações de pagamento do terminal virtual dos comerciantes.

Essa opção do SAQ aplica-se somente aos comerciantes que inserem manualmente uma única transação por vez através de um teclado em uma solução de terminal virtual baseada na Internet.

Os comerciantes do SAQ C-VT processam os dados do titular do cartão através de terminais virtuais em computadores pessoais conectados à Internet, não armazenam os dados do titular do cartão em nenhum sistema de computador e podem ser do tipo real (cartão presente) ou de pedidos por correio/telefone (cartão não presente). Esses comerciantes validam a conformidade ao preencherem o SAQ C -VT e o Atestado de conformidade associado, confirmando que:

- O processamento do pagamento da sua empresa somente é feito através de um terminal virtual acessado por um navegador da Web conectado à Internet;
- A solução de terminal virtual da sua empresa é fornecida e hospedada por um prestador de serviços terceirizado validado pelo PCI DSS;
- Sua empresa acessa a solução de terminal virtual compatível com o PCI DSS através de um computador isolado em um único local, que não está conectado a outros locais ou sistemas no seu ambiente (isso pode ser obtido através da segmentação do firewall ou da rede para isolar o computador de outros sistemas);
- O computador da sua empresa não possui softwares instalados que armazenam os dados do titular do cartão (por exemplo: não possui software para processamento em lote ou armazenamento e encaminhamento);
- O computador da sua empresa não possui nenhum dispositivo de hardware conectado para capturar e armazenar dados do titular do cartão (como leitores de cartão conectados);
- Sua empresa não recebe ou transmite eletronicamente, de nenhuma outra forma, dados do titular do cartão através de nenhum canal (por exemplo: através de uma rede interna ou através da Internet);
- Sua empresa retém somente relatórios ou cópias em papel dos recibos; **e**
- Sua empresa não armazena dados do titular do cartão em formato eletrônico.

Essa opção nunca se aplica aos comerciantes de comércio eletrônico.

SAQ C – Comerciantes com sistemas de aplicativos de pagamento conectados à Internet, sem armazenamento eletrônico dos dados do titular do cartão

O SAQ C foi desenvolvido para abordar os requisitos aplicáveis aos comerciantes cujos sistemas de aplicação do pagamento (como os sistemas de POS) estão conectados à Internet (via conexão DSL, modem a cabo, etc.) por que:

1. *O sistema do aplicativo de pagamento está em um computador pessoal que está conectado à Internet (por exemplo: para envio de e-mails ou navegação) ou*
2. *O sistema do aplicativo de pagamento está conectado à Internet para transmitir os dados do titular do cartão.*

Se você preferir usar um guia visual para selecionar o seu tipo de SAQ, consulte a seção "Qual SAQ melhor se aplica ao meu ambiente?" na página 17.

Os comerciantes do SAQ C processam os dados do titular do cartão por meio de máquinas de POS ou outros sistemas de aplicativo de pagamento conectados à Internet e não armazenam os dados do titular do cartão em nenhum sistema de computadores, podendo ser do tipo real (cartão presente) ou comércio eletrônico ou pedidos por correio/telefone (cartão não presente). Os comerciantes do SAQ C validam a conformidade ao preencherem o SAQ C e o Atestado de conformidade associado, confirmando que:

- Sua empresa possui um sistema de aplicativo de pagamento e uma conexão com à Internet no mesmo dispositivo e/ou na mesma rede local (LAN);
- O sistema de aplicativo de pagamento/dispositivo de Internet não está conectado a nenhum outro sistema no ambiente (isso pode ser feito através de segmentação da rede para isolar o sistema de aplicativo de pagamento/dispositivo de Internet de todos os outros sistemas);
- O armazenamento da empresa não está conectado a nenhum outro local de armazenamento e todas as LANs são somente para armazenamento exclusivo;
- Sua empresa retém somente relatórios ou cópias em papel dos recibos;
- Sua empresa não armazena dados do titular do cartão em formato eletrônico; **e**
- O fornecedor do software do aplicativo de pagamento da sua empresa usa técnicas seguras para fornecer suporte remoto ao seu sistema seguro de aplicativos de pagamento.

SAQ D – Todos os outros comerciantes e prestadores de serviços definidos por uma bandeira como qualificados para preencherem um SAQ

O SAQ D foi desenvolvido para todos os prestadores de serviços definidos por uma bandeira como qualificados para preencherem um SAQ e também para todos os comerciantes qualificados para preencherem o SAQ não incluídos nas descrições dos SAQs A a C acima.

Os prestadores de serviços e comerciantes do SAQ D validam a conformidade ao preencherem o SAQ D e o Atestado de conformidade associado.

Apesar de várias organizações que preenchem o SAQ D precisarem validar a conformidade com todos os requisitos do PCI DSS, algumas organizações com modelos de negócio bastante específicos podem descobrir que alguns requisitos não se aplicam. Por exemplo: não se espera que uma empresa que não usa tecnologia sem fio de forma alguma valide a conformidade com as seções do PCI DSS que são específicas da tecnologia sem fio. Consulte a orientação abaixo para obter informações sobre a exclusão da tecnologia sem fio e de outros requisitos específicos.

Orientação para não aplicabilidade de determinados requisitos específicos

Exclusão: Se você precisar responder o SAQ C ou D para validar sua conformidade com o PCI DSS, as seguintes exceções podem ser consideradas. Consulte a seção "Não aplicabilidade" abaixo para obter uma resposta adequada do SAQ.

- Requisitos 1.2.3, 2.1.1 e 4.1.1 (SAQs C e D): As perguntas específicas relacionadas a dispositivos sem fio só precisarão ser respondidas se houver dispositivos sem fio em algum lugar da sua rede Observe que o Requisito 11.1 (uso de um processo para identificar pontos de acesso sem fio não autorizados) deverá ser respondido, mesmo que o dispositivo sem fio não esteja na sua rede, pois o analisador detecta intrusos ou dispositivos não autorizados que possam ter sido adicionados sem seu conhecimento.
- Requisitos 6.3 e 6.5 (SAQ D): Essas questões são específicas para aplicativos e códigos personalizados e só precisarão ser respondidas se sua organização desenvolver seus próprios aplicativos da Web.
- Requisitos 9.1 a 9.4 (SAQ D): Essas perguntas só precisarão ser respondidas para instalações com "áreas confidenciais", conforme definido aqui. "Áreas confidenciais" referem-se a qualquer central de dados, sala de servidores ou qualquer área que contenha sistemas que armazenem, processem ou transmitam dados do titular do cartão. Isso exclui as áreas que possuem somente terminais de pontos de vendas, como as áreas dos caixas em uma loja de varejo, mas inclui salas de servidores de back-office de lojas de varejo que armazenam dados do titular do cartão e áreas de armazenamento para grandes quantidades de dados do titular do cartão.

Não aplicabilidade: Para todos os SAQs, estes e outros requisitos considerados não aplicáveis ao seu ambiente deverão ser indicados com "N/A" na coluna "Especial" do SAQ. Da mesma forma, preencha a planilha "Explicação de não aplicabilidade", no Anexo do SAQ, para cada entrada "N/A".

Instruções para preencher o SAQ

1. Use as diretrizes contidas neste documento para determinar qual SAQ é adequado para sua empresa.
2. Use o documento*Navegando pelo PCI DSS: Entendendo o porquê dos requisitos* para entender por que e como os requisitos são relevantes para sua organização.
3. Avalie seu ambiente quanto à conformidade com o PCI DSS.
4. Use o Questionário de auto-avaliação adequado como ferramenta para validar a conformidade com o PCI DSS.
5. Siga as instruções no Questionário de auto-avaliação adequado em "Conformidade do PCI DSS – Etapas para preenchimento" e forneça toda a documentação necessária para seu adquirente ou bandeira, conforme adequado.

Qual SAQ melhor se aplica ao meu ambiente?