Setor de cartões de pagamentos (PCI)
Padrão de Segurança de Dados

Questionário de Autoavaliação

Instruções e diretrizes

Versão 3.2.1

Junho de 2018

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 implementar alterações secundárias observadas desde a v1.1 original.
28 de Outubro de 2010	2.0	Para alinhar o conteúdo com o novo PCI DSS v2.0 e esclarecer os tipos de ambiente SAQ e os critérios de qualificação. Adição de SAQ C-VT para comerciantes de terminais virtuais baseados na Web
Junho de 2012	2.1	Adição de SAQ P2PE-HW para comerciantes que processam dados do titular do cartão somente por meio de terminais de hardware de pagamento incluídos em uma solução de criptografia ponto a ponto (P2PE) PCI validada e listada em PCI SSC. Este documento deve ser utilizado com PCI DSS versão 2.0.
Abril de 2015	3.1	Para alinhar o conteúdo com o PCI DSS v3.1, inclusive a inclusão de SAQs A-EP e B-IP, e esclarecer critérios de qualificação para SAQs existentes.
Maio de 2016	3.2	Atualizado para alinhar com o PCI DSS v3.2 e esclarecer os critérios de qualificação para os SAQs existentes.
Junho de 2018	3.2.1	Atualizações secundárias para alinhar com PCI DSS v3.2.1.

TERMO DE RECONHECIMENTO: A versão em inglês deste documento,conforme disponibilizada no site da PCI SSC, para todos os efeitos, é considerada a versão oficial destes documentos e, na medida em que houver ambiguidades ou inconsistências entre a redação do presente texto e do texto em inglês,a versão em inglês disponibilizada no local mencionado prevalecerá.

Sumário

Alterações no documento ..... **i**

Sobre este Documento **1**

Autoavaliação PCI DSS: como tudo se encaixa **2**

Visão geral do SAQ **3**

Por que o PCI DSS é importante **4**

Entenda a diferença entre conformidade e segurança 5

Dicas e estratégias gerais para a conformidade com PCI DSS 5

Como escolher o SAQ e o atestado que melhor se aplicam à sua organização **8**

SAQ A – Comerciantes de cartões não presentes, todas as funções de dados do titular do cartão totalmente terceirizadas 10

SAQ A-EP — Comerciantes de comércio eletrônico parcialmente terceirizados que utilizam sites de terceiros para o processamento de pagamentos 11

SAQ B – Comerciantes com somente máquinas de impressão ou somente terminais autônomos e de discagem. Nenhum armazenamento de dados do titular do cartão eletrônico 12

SAQ B-IP — Comerciantes com terminais de ponto de interação (POI) PTS autônomos e conectados por IP, sem armazenamento de dados de titulares de cartões eletrônicos 13

SAQ C-VT – Comerciantes com terminais virtuais baseados na web, sem armazenamento de dados de titular de cartão eletrônico 14

SAQ C – Comerciantes com sistemas de aplicativos de pagamento conectados à internet, sem armazenamento de dados do titular do cartão eletrônico 16

SAQ P2PE — Comerciantes que usam somente terminais de pagamento de hardware em uma solução P2PE listada no PCI SSC, sem armazenamento de dados de titular de cartão eletrônico 17

SAQ D para Comerciantes – Todos os demais comerciantes qualificados para SAQ 18

SAQ D para provedores de serviços – prestadores de serviços qualificados para SAQ 18

Qual SAQ se aplica melhor ao meu ambiente? **19**

Sobre este Documento

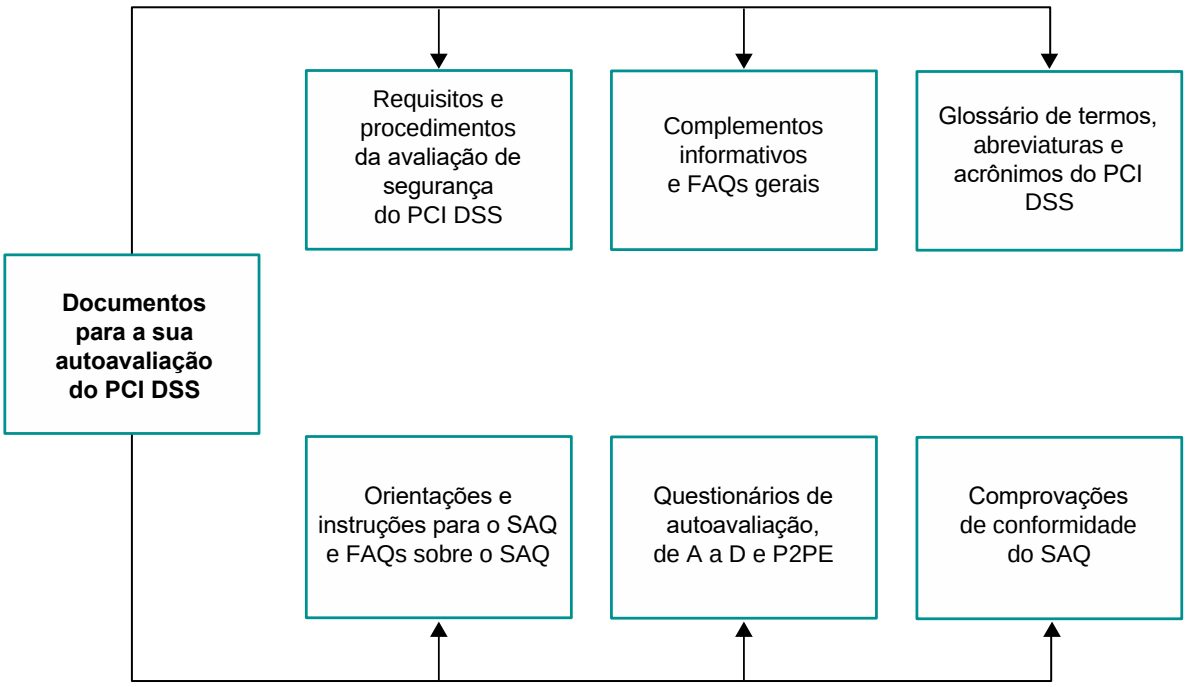
Este documento foi desenvolvido para ajudar comerciantes e prestadores de serviços a entender os Questionários de Autoavaliação (SAQs) do Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS). Para entender por que o PCI DSS é importante para sua organização, quais estratégias ela pode usar para facilitar a validação de conformidade com o PCI DSS e se sua organização está qualificada para concluir um dos SAQs mais curtos, recomendamos que você analise este documento de Instruções e Diretrizes em sua totalidade

Autoavaliação PCI DSS: como tudo se encaixa

O PCI DSS e os documentos de suporte representam um conjunto comum de ferramentas do setor para ajudar a garantir o manuseio seguro dos dados do titular do cartão. O padrão em si apresenta uma estrutura acionável para desenvolver um processo de segurança robusto, inclusive prevenção, detecção e reação a incidentes de segurança. Para reduzir o risco de comprometimento e mitigar o impacto, se ocorrer, é importante que todas as organizações que armazenam processos ou transmitem dados do titular do cartão estejam em conformidade.

O gráfico abaixo descreve as ferramentas implementadas para ajudar as organizações com conformidade com PCI DSS e autoavaliação.

Estes e outros documentos relacionados estão disponíveis em www.pcisecuritystandards.org.



** Lembre-se de que os complementos informativos somente oferecem informações e orientação, e que não substituem nem prevalecem sobre nenhum requisito no PCI DSS*

** Observação: os complementos de informações apresentam somente informações complementares e orientação e não substituem nem sobrepõem quaisquer requisitos no PCI DSS.*

Visão geral do SAQ

Os *Questionários de Autoavaliação (SAQs) do PCI DSS* são ferramentas de validação destinadas a auxiliar comerciantes e prestadores de serviços a autoavaliar a conformidade com o PCI DSS. Há várias versões dos SAQs do PCI DSS para atender a vários cenários. Este documento foi desenvolvido para ajudar sua organização a determinar quais SAQs se aplicam melhor ao seu ambiente.

O SAQ do PCI DSS é uma ferramenta de validação para comerciantes e prestadores de serviços, não exigido por seus respectivos adquirentes ou marcas de pagamento para enviar Relatório sobre Conformidade (ROC) PCI DSS. Consulte seu adquirente ou marca de pagamento para obter detalhes sobre os requisitos de validação do PCI DSS.

Cada SAQ do PCI DSS consiste nos seguintes componentes:

1. Perguntas correlacionadas aos requisitos do PCI DSS, conforme apropriado para diversos ambientes: consulte “Como escolher o SAQ e o atestado que melhor se aplicam à sua organização” neste documento. Esta seção contém também uma coluna para “Testes esperados”, que se baseia nos procedimentos de teste no PCI DSS.
2. Atestado de conformidade: o atestado inclui sua declaração de qualificação para responder o SAQ aplicável e os resultados subsequentes de uma autoavaliação do PCI DSS.

Por que o PCI DSS é importante

Os membros fundadores do PCI Security Standards Council (American Express, Discover, JCB, Mastercard e Visa) monitoram constantemente as ocorrências de comprometimento dos dados da conta. Esses comprometimentos cobrem todo o espectro de organizações, dos comerciantes e prestadores de serviços muito pequenos aos muito grandes.

Uma violação de segurança e subsequente comprometimento dos dados do cartão de pagamento têm consequências de longo alcance para as organizações afetadas, incluindo:

1. Requisitos regulamentares de notificação;
2. Perda de reputação;
3. Perda de clientes;
4. Possíveis passivos financeiros (por exemplo, taxas e multas regulamentares e outras), e
5. litígios.

A análise forense de comprometimentos demonstrou que as fraquezas comuns de segurança, que são abordadas pelos controles de PCI DSS, são frequentemente exploradas porque os controles PCI DSS não estavam em vigor ou foram mal implementados quando o comprometimento ocorreu. O PCI DSS foi projetado e contém requisitos detalhados exatamente por esse motivo, para minimizar a chance de comprometimento e seus efeitos, caso isso ocorra.

Alguns exemplos de falhas comuns de controle de PCI DSS:

- Armazenamento de dados de autenticação confidenciais (SAD), como dados de trilha, após a autorização (Requisito 3.2). Muitas entidades comprometidas não sabiam que seus sistemas armazenavam esses dados.
- Controles de acesso inadequados devido a sistemas de ponto de venda (PDV) instalados incorretamente, permitindo que usuários mal-intencionados entrem por meio de caminhos destinados a fornecedores de PDV (Requisitos 7.1, 7.2, 8.2 e 8.3).
- Configurações padrão do sistema e senhas não alteradas quando o sistema foi instalado (Requisito 2.1).
- Serviços desnecessários e não seguros não removidos ou protegidos quando o sistema foi instalado (Requisitos 2.2.2 e 2.2.3).
- Aplicativos da web mal codificados resultando em injeção de SQL e outras vulnerabilidades, que permitem o acesso ao banco de dados que armazena os dados do titular do cartão diretamente no site (Requisito 6.5).
- Correções de segurança ausentes e desatualizadas (Requisito 6.2).
- Ausência de histórico (Requisito 10).
- Falta de monitoramento (por meio de análises de históricos, detecção/prevenção de invasões, verificações trimestrais de vulnerabilidade e mecanismos de detecção de alterações) (Requisitos 10.6, 11.2, 11.4 e 11.5).
- Decisões de escopo inadequadas. Por exemplo, exclusão de parte da rede do escopo do PCI DSS devido à segmentação de rede inadequada que não foi verificada como efetiva (Requisito 11.3.4). Isso faz com que o ambiente de dados do titular do cartão fique inadvertidamente exposto a fraquezas 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 não protegidos e vulnerabilidades introduzidas por e-mail e da navegação na web dos funcionários) (Requisitos 1.2, 1.3 e 1.4).

Entenda a diferença entre conformidade e segurança

É importante reconhecer a diferença entre estar em conformidade e estar seguro. Estar em conformidade com o PCI DSS em um momento não impede que haja mudanças no seu ambiente, o que, se os controles adequados não forem implementados, pode afetar sua segurança. Portanto, você deve assegurar que os controles de PCI DSS continuem sendo implementados corretamente como parte das atividades de negócios rotineiras (BAU) e conforme definido pela sua estratégia de segurança geral. Isso permitirá que você monitore a eficácia dos controles de segurança da sua organização de forma constante e mantenha seu ambiente compatível com o PCI DSS entre avaliações PCI DSS. Há exemplos de como o PCI DSS deve ser incorporado às atividades de BAU disponíveis na seção “Práticas recomendadas para implementar PCI DSS em processos de negócios rotineiros” no PCI DSS.

Além disso, os requisitos de segurança de PCI DSS destinam-se à proteção dos dados do cartão de pagamento e sua organização pode ter outros dados e ativos confidenciais que precisam de proteção que podem estar fora do escopo do PCI DSS. Portanto, embora a conformidade com o PCI DSS, se devidamente mantida, possa certamente contribuir para a segurança geral, ela não deve ser vista como um substituto para um programa de segurança robusto e em toda a organização.

Dicas e estratégias gerais para a conformidade com PCI DSS

Veja a seguir algumas dicas e estratégias gerais para iniciar seu trabalho de conformidade com o PCI DSS. Essas dicas podem ajudá-lo a eliminar o armazenamento de dados de titulares de cartões de que você não precisa, isolar os dados necessários para áreas centralizadas definidas e controladas e podem permitir que você limite seu esforço de validação de conformidade com o PCI DSS. Por exemplo, ao eliminar os dados de titulares de cartões de que você não precisa e/ou isolar os dados necessários para áreas definidas e controladas, é possível remover sistemas e redes que não armazenam, processam ou transmitem dados de titulares de cartão, e que não se conectam a sistemas que o fazem, do escopo da sua autoavaliação.

1. **Dados de autenticação confidenciais (inclui o conteúdo completo da faixa da fita magnética ou dados equivalentes em um chip, códigos e valores de verificação de cartões, PINs e PIN Blocks):**

   É importante que você ***jamais armazene esses dados*** após a autorização:

2. **Pergunte ao seu fornecedor de PDV sobre a segurança do seu sistema, utilizando as seguintes perguntas sugeridas:**

   a. As configurações e senhas padrão foram alteradas nos sistemas e nos bancos de dados que fazem parte do sistema de PDV?

   b. Você acessa meu sistema de PDV remotamente? Em caso afirmativo, você implementou controles apropriados para impedir que outras pessoas acessem meu sistema de PDV, como usar métodos de acesso remoto seguro e não usar senhas comuns ou padrão? Com que frequência você acessa meu dispositivo de PDV remotamente e por quê? Quem está autorizado a acessar meu PDV remotamente?

   c. Todos os serviços desnecessários e inseguros foram removidos dos sistemas e bancos de dados que fazem parte do sistema de PDV?

   d. Meu software de PDV é validado para o PA-DSS (Payment Application Data Security Standard)? (Consulte a lista de aplicativos de pagamento validados do PCI SSC).

   e. Meu software de PDV armazena dados de autenticação confidenciais, como dados de rastreamento ou blocos de PIN? Em caso afirmativo, esse armazenamento é proibido: com que rapidez você pode me ajudar a removê-lo?

f. Meu software de PDV armazena os números de contas principais (PANs)? Em caso afirmativo, esse armazenamento deve ser protegido: como o PDV protege esses dados?

g. Você documentará a lista de arquivos escritos pelo aplicativo com um resumo do conteúdo de cada arquivo, para verificar se os dados proibidos acima mencionados não estão armazenados?

h. Meu software de PDV impõe senhas complexas e exclusivas para todos os acessos de usuários?

i. Você pode confirmar que não usa senhas comuns ou padrão para acessar meu sistema e outros sistemas de comerciantes aos quais presta suporte?

j. Todos os sistemas e bancos de dados que fazem parte do sistema do PDV foram corrigidos com todas as atualizações de segurança aplicáveis?

k. O recurso de registro está ativado para os sistemas e bancos de dados que fazem parte do sistema de PDV?

l. Se as versões anteriores do meu software de PDV armazenaram dados de autenticação confidenciais, esse recurso foi removido durante as atualizações atuais do software de PDV? Foi utilizado um utilitário de limpeza segura para remover esses dados?

3. Dados de titulares de cartões — se não precisar, não os armazene!

a. As regras de marca de pagamento permitem o armazenamento do número de conta principal (PAN), da data de validade, do nome de titulares de cartões e do código de serviço.

b. Faça uma lista de todos os motivos para armazenar esses dados e os lugares de armazenamento. Se os dados não atenderem a um propósito comercial legítimo, considere a possibilidade de eliminá-los.

c. Analise se o armazenamento desses dados e o processo de negócios que ele apoia compensam o seguinte:

   i. O risco de ter os dados comprometidos.

   ii. Os controles de PCI DSS adicionais que devem ser aplicados para proteger esses dados.

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

4. Dados de titulares de cartões — se você precisar, consolide-os e isole-os.

É possível limitar o escopo de uma avaliação de PCI DSS consolidando o armazenamento de dados em um ambiente definido e isolando os dados por meio de uma segmentação de rede adequada. Por exemplo, se os seus funcionários navegarem na internet e receberem e-mails na mesma máquina ou segmento de rede que os dados de titulares de cartões, considere a possibilidade de segmentar (isolar) os dados de titulares de cartões em sua própria máquina ou segmento de rede (por exemplo, por meio de roteadores ou firewalls). Se você puder isolar os dados de titulares de cartões de forma eficaz, será possível concentrar seus esforços de PCI DSS somente na parte isolada, em vez de incluir todas as suas máquinas.

5. Controles de compensação

Podem-se considerar controles de compensação para a maioria dos requisitos do PCI DSS se uma organização não puder atender à especificação técnica de um requisito, mas tiver atenuado suficientemente o risco associado por meio de controles alternativos. Se a sua organização não tiver o controle exato especificado no PCI DSS, mas tiver outros controles em vigor que satisfaçam a definição de PCI DSS de controles compensadores (consulte "Controles de Compensação" no Apêndice B do *PCI DSS e também no Glossário de Termos, Abreviações e Siglas do PCI DSS e PA-DSS*), ela deverá fazer o seguinte:

a. Seguir os procedimentos de controles compensatórios, conforme descrito no Apêndice B do PCI DSS.

b. Para todos os requisitos que foram atendidos com a assistência de um controle compensatório, responda à pergunta do SAQ marcando a coluna "SIM com CCW".

c. Documentar cada controle compensatório preenchendo uma Planilha de Controles Compensatórios no Apêndice B do SAQ.

   Deve-se preencher uma Planilha de Controles Compensatórios para cada requisito que for atendido com um controle compensatório.

d. Envie todas as Planilhas de Controles Compensatórios concluídas junto com o SAQ e/ou o Atestado de Conformidade preenchidos, de acordo com as instruções do seu adquirente ou da bandeira de pagamento.

6. Assistência profissional e formação

a. Se você quiser contratar um profissional de segurança para ter ajuda em sua autoavaliação, recomendamos que considere a possibilidade de entrar em contato com um Assessor de Segurança Qualificado (QSA). Os QSAs foram treinados pelo PCI SSC para realizar avaliações do PCI DSS e estão listados no site do PCI SSC.

b. O site do PCI SSC é uma fonte primária para recursos adicionais, incluindo:

   - O *Glossário de termos, abreviações e siglas do PCI DSS*
   - Dúvidas frequentes (FAQs)
   - Webinários
   - Suplementos de informações e diretrizes
   - Formulários de SAQ e atestados de conformidade

Observações: *os Suplementos de Informações complementam o PCI DSS e identificam considerações e recomendações adicionais para atender aos requisitos do PCI DSS — eles não alteram, eliminam nem substituem o PCI DSS ou qualquer um de seus requisitos.*

c. O PCI SSC apresenta também uma série de programas de treinamento para ajudar a aumentar a conscientização do pessoal de uma organização. Os exemplos incluem o PCI Awareness, o programa PCI Professional (PCIP) e o programa Internal Security Assessor (ISA).

   Consulte www.pcisecuritystandards.org para mais informações.

d. Pode também haver disponíveis programas de treinamento e recursos relacionados a pagamentos nas bandeiras de pagamento e/ou no seu adquirente comerciante.

Como escolher o SAQ e o atestado que melhor se aplicam à sua organização

Todos os comerciantes e prestadores de serviços são obrigados a cumprir o PCI DSS, conforme aplicável aos seus ambientes em todos os momentos. Há uma série de tipos de SAQ, apresentados brevemente na tabela abaixo e descritos com mais detalhes nas páginas a seguir. Use a tabela para ajudar a determinar qual SAQ se aplica à sua organização e, em seguida, revise as descrições detalhadas para garantir que você atenda a todos os requisitos para esse SAQ.

Observação para todos os SAQs, exceto SAQ D: esses SAQs contêm perguntas que se aplicam a um tipo específico de ambiente de comerciante, conforme definido nos critérios de qualificação de SAQ relacionados. Se houver requisitos PCI DSS aplicáveis ao seu ambiente que não estiverem cobertos em um determinado SAQ, isso poderá ser uma indicação de que esse SAQ não é adequado para o seu ambiente. Além disso, você deve cumprir todos os requisitos aplicáveis do PCI DSS para ser compatível com PCI DSS.

SAQ	Descrição
A	Comerciantes de cartão não presente (comércio eletrônico ou pedido por correio/telefone), que terceirizaram totalmente todas as funções de dados do titular do cartão para prestadores de serviços terceirizados compatíveis com PCI DSS , sem armazenamento eletrônico, processamento ou transmissão de dados do titular do cartão nos sistemas ou instalações do cliente. *Não se aplica aos canais presenciais.*
A-EP	Comerciantes de comércio eletrônico que terceirizam todo o processamento de pagamentos para terceiros, validados pelo PCI DSS, e que têm sites que não recebem diretamente dados dos titulares de cartões, mas que podem afetar a segurança da transação de pagamento. Não há processamento, transmissão ou armazenamento eletrônico de dados de titulares de cartões nos sistemas ou nas instalações do comerciante. *Aplicável somente a canais de e-commerce.*
B	Comerciantes que utilizam somente: ▪ Máquinas de impressão sem armazenamento de dados de titulares de cartões eletrônicos e/ou ▪ Terminais autônomos de discagem sem armazenamento de dados de titulares de cartões eletrônicos. *Não se aplica aos canais de e-commerce.*
B-IP	Comerciantes que usam somente terminais de pagamento independentes aprovados pelo PTS, com uma conexão IP ao processador de pagamento, sem armazenamento de dados de titulares de cartões eletrônicos. *Não se aplica aos canais de e-commerce.*
C-VT	Comerciantes que inserem manualmente uma única transação por vez, por meio de teclado, em uma solução de terminal de pagamento virtual baseada na internet fornecida e hospedada por um provedor de serviços terceirizado e validado pelo PCI DSS. Não há armazenamento de dados de titulares de cartões eletrônicos. *Não se aplica aos canais de e-commerce.*

SAQ	Descrição
C	Comerciantes com sistemas de aplicativos de pagamento conectados à internet, sem armazenamento de dados de titulares de cartões eletrônicos. *Não se aplica aos canais de e-commerce.*
P2PE	Comerciantes que usam somente terminais de pagamento de hardware incluídos e gerenciados por meio de uma solução de criptografia ponto a ponto (P2PE), validada e listada no PCI SSC, sem armazenamento de dados de titulares de cartões eletrônicos. *Não se aplica aos canais de e-commerce.*
D	***SAQ D para Comerciantes:*** todos os comerciantes não incluídos nas descrições dos tipos de SAQ acima.
	SAQ D para Prestadores de Serviços: todos os prestadores de serviços definidos por uma bandeira de pagamento como qualificados para concluir um SAQ.

SAQ A – Comerciantes de cartões não presentes, todas as funções de dados do titular do cartão totalmente terceirizadas

O SAQ A foi desenvolvido para atender aos requisitos aplicáveis aos comerciantes cujas funções de dados de titulares de cartões são completamente terceirizadas a terceiros validados, onde o comerciante retém somente relatórios ou recibos em papel com dados de titulares de cartões.

Para obter um guia gráfico e escolher seu tipo de SAQ, consulte "Qual SAQ melhor se aplica ao meu ambiente?" na página 19.

Os comerciantes da categoria SAQ A podem ser tanto de comércio eletrônico como pedidos por correio/telefone (cartão não presente) e não armazenam, processam nem transmitem quaisquer dados dos titulares de cartões em formato eletrônico em seus sistemas ou instalações.

Os comerciantes da categoria SAQ A confirmarão que atendem aos seguintes critérios de qualificação para esse canal de pagamento:

- Sua empresa aceita somente transações de cartão não presente (e-commerce ou pedidos por correio/telefone);
- Todo o processamento de dados de titulares de cartões é inteiramente terceirizado para prestadores de serviços terceirizados validados pelo PCI DSS;
- Sua empresa não armazena, processa ou transmite eletronicamente quaisquer dados de titulares de cartões em seus sistemas ou instalações, mas depende inteiramente de terceiros para lidar com todas essas funções;
- Sua empresa confirmou que todos os terceiros que lidam com armazenamento, processamento e/ou transmissão de dados de titulares de cartões estão em conformidade com o PCI DSS; **e**
- Os dados de titulares de cartões retidos pela sua empresa estão em papel (por exemplo, relatórios ou recibos impressos) e esses documentos não são recebidos eletronicamente.

Além disso, para canais de e-commerce:

- Todos os elementos de todas as páginas de pagamento entregues ao navegador do consumidor são originários somente e diretamente de um prestador de serviços terceirizado validado pelo PCI DSS.

Este SAQ não se aplica a canais presenciais.

SAQ A-EP — Comerciantes de comércio eletrônico parcialmente terceirizados que utilizam sites de terceiros para o processamento de pagamentos

O SAQ A-EP foi desenvolvido para atender aos requisitos aplicáveis aos comerciantes de comércio eletrônico com sites que não recebem dados de titulares de cartões, mas que afetam a segurança da transação de pagamento e/ou a integridade da página que aceita os dados de titulares de cartões de consumidores.

Os comerciantes SAQ A-EP são comerciantes de comércio eletrônico que terceirizam parcialmente seu canal de pagamento de comércio eletrônico para terceiros validados pelo PCI DSS e não armazenam, processam ou transmitem dados de titulares de cartões em seus sistemas ou instalações.

Para ver um guia gráfico e escolher seu tipo de SAQ, consulte "Qual SAQ melhor se aplica ao meu ambiente?" na página 19.

Os comerciantes da categoria SAQ A-EP confirmarão que atendem aos seguintes critérios de qualificação para esse canal de pagamento:

- Sua empresa aceita somente transações de comércio eletrônico;
- Todo o processamento dos dados de titulares de cartões, com exceção da página de pagamento, é inteiramente terceirizado para um processador de pagamento terceirizado validado pelo PCI DSS;
- Seu site de comércio eletrônico não recebe dados de titulares de cartões, mas controla como os consumidores ou os dados de titulares de cartões são redirecionados para um processador de pagamento terceirizado validado pelo PCI DSS;
- Se o site do comerciante for hospedado por um provedor terceirizado, o provedor será validado para todos os requisitos aplicáveis do PCI DSS (por exemplo, incluindo o Apêndice A do PCI DSS se o provedor for do tipo de hospedagem compartilhada);
- Cada elemento das páginas de pagamento entregue ao navegador do consumidor é originário do site do comerciante ou de um prestador de serviços compatível com PCI DSS;
- Sua empresa não armazena, processa ou transmite eletronicamente quaisquer dados de titulares de cartões em seus sistemas ou instalações, mas depende inteiramente de terceiros para lidar com todas essas funções;
- Sua empresa confirmou que todos os terceiros que lidam com armazenamento, processamento e/ou transmissão de dados de titulares de cartões estão em conformidade com o PCI DSS; **e**
- Os dados de titulares de cartões retidos pela sua empresa estão em papel (por exemplo, relatórios ou recibos impressos) e esses documentos não são recebidos eletronicamente.

Este SAQ aplica-se somente aos canais de comércio eletrônico.

Observação: *para efeitos do SAQ A-EP, os requisitos do PCI DSS que se referem ao "ambiente de dados de titulares de cartões" aplicam-se aos sites do comerciante. Isso ocorre porque o site do comerciante afeta diretamente a forma como os dados dos cartões de pagamento são transmitidos, mesmo que o próprio site não receba dados de titulares de cartões.*

SAQ B – Comerciantes com somente máquinas de impressão ou somente terminais autônomos e de discagem. Nenhum armazenamento de dados do titular do cartão eletrônico

O SAQ B foi desenvolvido para atender aos requisitos que se aplicam aos comerciantes que processam dados de titulares de cartões somente por meio de máquinas de impressão ou terminais de discagem autônomos.

Os comerciantes da categoria SAQ B podem ser comerciantes lojas físicas (cartão presente) ou de pedidos por correio ou telefone (cartão não presente) e não armazenam dados de titulares de cartões em qualquer sistema informático. Os comerciantes da categoria SAQ B confirmarão que atendem aos seguintes critérios de qualificação para esse canal de pagamento:

Para obter um guia gráfico e escolher seu tipo de SAQ, consulte "Qual SAQ melhor se aplica ao meu ambiente?" na página 19.

- Sua empresa usa somente uma máquina de impressão e/ou usa somente terminais de discagem autônomos (conectados por uma linha telefônica ao seu processador) para levar as informações de cartões de pagamento dos seus clientes;
- Os terminais autônomos de discagem não estão conectados a nenhum outro sistema dentro do seu ambiente;
- Os terminais autônomos de discagem não estão conectados à internet;
- A sua empresa não transmite dados de titulares de cartões através de uma rede (seja uma rede interna ou pela internet);
- Os dados de titulares de cartões retidos pela sua empresa estão em papel (por exemplo, relatórios ou recibos impressos) e esses documentos não são recebidos eletronicamente; **e**
- Sua empresa não armazena dados de titulares de cartões em formato eletrônico.

Este SAQ não se aplica a canais de comércio eletrônico.

SAQ B-IP — Comerciantes com terminais de ponto de interação (POI) PTS autônomos e conectados por IP, sem armazenamento de dados de titulares de cartões eletrônicos

O SAQ B-IP foi desenvolvido para atender aos requisitos que se aplicam aos comerciantes que processam dados de titulares de cartões somente por meio de dispositivos de ponto de interação (POI) autônomos e aprovados pelo PTS com uma conexão IP ao processador de pagamento.

Para ver um guia gráfico e escolher seu tipo de SAQ, consulte "Qual SAQ melhor se aplica ao meu ambiente?" na página 19.

Os comerciantes da categoria SAQ B-IP podem ser comerciantes lojas físicas (cartão presente) ou de pedidos por correio ou telefone (cartão não presente) e não armazenam dados de titulares de cartões em qualquer sistema informático.

Os comerciantes da categoria SAQ B-IP confirmarão que atendem aos seguintes critérios de qualificação para esse canal de pagamento:

- Sua empresa usa somente dispositivos de ponto de interação (POI) autônomos aprovados pelo PTS (exclui SCRs) conectados por IP ao processador de pagamento para levar as informações de cartões de pagamento dos seus clientes;
- Os dispositivos POI autônomos conectados por IP são validados para o programa PTS POI conforme listado no site do PCI SSC (exclui SCRs);
- Os dispositivos POI autônomos conectados por IP não estão conectados a nenhum outro sistema dentro do seu ambiente (isso pode ser realizado por meio da segmentação de rede para isolar dispositivos POI de outros sistemas);
- A única transmissão de dados de titulares de cartões é dos dispositivos POI aprovados pelo PTS para o processador de pagamentos;
- O dispositivo POI não depende de nenhum outro dispositivo (por exemplo, computador, celular, tablet etc.) para conectar-se ao processador de pagamento;
- Os dados de titulares de cartões retidos pela sua empresa estão em papel (por exemplo, relatórios ou recibos impressos) e esses documentos não são recebidos eletronicamente; **e**
- Sua empresa não armazena dados de titulares de cartões em formato eletrônico.

Este SAQ não se aplica a canais de comércio eletrônico.

SAQ C-VT – Comerciantes com terminais virtuais baseados na web, sem armazenamento de dados de titular de cartão eletrônico

O SAQ C-VT foi desenvolvido para atender aos requisitos que se aplicam aos comerciantes que processam dados de titulares de cartões somente por meio de terminais de pagamento virtuais isolados em um computador pessoal conectado à internet.

Para obter um guia gráfico e escolher seu tipo de SAQ, consulte "Qual SAQ melhor se aplica ao meu ambiente?" na página 19.

Um terminal de pagamento virtual é o acesso baseado em navegador da web a um adquirente, processador ou site de prestador de serviços de terceiros, para autorizar transações com cartões de pagamento, onde o comerciante insere manualmente os dados do cartão de pagamento por meio de um navegador da web conectado com segurança. Ao contrário dos terminais físicos, os terminais de pagamento virtuais não leem dados diretamente de um cartão de pagamento. As transações com cartões de pagamento são inseridas manualmente.

Os comerciantes da categoria SAQ C-VT processam os dados de titulares de cartões somente por meio de um terminal de pagamento virtual e não armazenam dados de titulares de cartões em nenhum sistema informático. Esses terminais virtuais são conectados à internet para acessar um terceiro, que hospeda a função de processamento de pagamento de terminal virtual. Esse terceiro pode ser um processador, adquirente ou outro prestador de serviços terceirizado, que armazena, processa e/ou transmite dados de titulares de cartões para autorizar e/ou liquidar transações de pagamento de terminais virtuais dos comerciantes.

Esta opção SAQ destina-se a ser aplicada somente aos comerciantes que inserem manualmente uma única transação por vez por meio de um teclado em uma solução de terminal virtual baseada na Internet. Os comerciantes SAQ C-VT podem ser comerciantes de estabelecimentos físicos (cartão presente) ou de pedidos por correio/telefone (cartão não presente).

Os comerciantes da categoria SAQ C-VT confirmarão que atendem aos seguintes critérios de qualificação para esse canal de pagamento:

- O único processamento de pagamento da sua empresa ocorre por meio de um terminal de pagamento virtual, acessado por um navegador da web conectado à internet;
- A solução de terminal de pagamento virtual da sua empresa é fornecida e hospedada por um provedor de serviços terceirizado validado pelo PCI DSS;
- Sua empresa acessa a solução de terminal de pagamento virtual compatível com PCI DSS por meio de um computador isolado em um único local e que não esteja conectado a outros locais ou sistemas dentro do seu ambiente (isso pode ser conseguido por meio de um firewall ou uma segmentação de rede para isolar o computador de outros sistemas);
- O computador da sua empresa não conta com software instalado que faça com que os dados de titulares de cartões sejam armazenados (por exemplo, não há software para processamento em lote ou armazenamento e encaminhamento);
- O computador da sua empresa não possui dispositivos de hardware integrados que sejam usados para capturar ou armazenar dados de titulares de cartões (por exemplo, não há leitores de cartões integrados);
- A sua empresa não recebe ou transmite dados de titulares de cartões eletronicamente por meio de nenhum canal (por exemplo, por meio de uma rede interna ou da internet);

- Os dados de titulares de cartões retidos pela sua empresa estão em papel (por exemplo, relatórios ou recibos impressos) e esses documentos não são recebidos eletronicamente; **e**
- Sua empresa não armazena dados de titulares de cartões em formato eletrônico.

Este SAQ não é aplicável a canais de comércio eletrônico.

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

O SAQ C foi desenvolvido para atender aos requisitos que se aplicam aos comerciantes cujos sistemas de aplicativos de pagamento (por exemplo, sistemas de ponto de venda) estão conectados à internet (por exemplo, por DSL, modem a cabo etc.).

Os comerciantes da categoria SAQ C processam os dados de titulares de cartões por meio de um sistema de ponto de venda (PDV) ou outros sistemas de aplicativos de pagamento conectados à internet, não armazenam dados de titulares de cartões em qualquer sistema informático e podem ser comerciantes de estabelecimentos físicos (cartão presente) ou de pedidos por correio/telefone (cartão não presente).

Para obter um guia gráfico e escolher seu tipo de SAQ, consulte "Qual SAQ melhor se aplica ao meu ambiente?" na página 19.

Os comerciantes da categoria SAQ C confirmarão que atendem aos seguintes critérios de qualificação para esse canal de pagamento:

- Sua empresa possui um sistema de aplicativos de pagamento e uma conexão à internet no mesmo dispositivo e/ou na mesma rede local (LAN);
- O sistema de aplicativos de pagamento/dispositivo de internet não está conectado a nenhum outro sistema dentro do seu ambiente (isso pode ser realizado por meio de segmentação de rede para isolar o sistema de aplicativos de pagamento/dispositivo de internet de todos os outros sistemas);
- A localização física do ambiente do PDV não está conectada a outras instalações ou locais, e qualquer LAN atende somente a uma única loja;
- Os dados de titulares de cartões retidos pela sua empresa estão em papel (por exemplo, relatórios ou recibos impressos) e esses documentos não são recebidos eletronicamente; **e**
- Sua empresa não armazena dados de titulares de cartões em formato eletrônico.

Este SAQ não se aplica a canais de comércio eletrônico.

SAQ P2PE — Comerciantes que usam somente terminais de pagamento de hardware em uma solução P2PE listada no PCI SSC, sem armazenamento de dados de titular de cartão eletrônico

O SAQ P2PE foi desenvolvido para atender aos requisitos que se aplicam aos comerciantes que processam dados de titulares de cartões somente por meio de terminais de pagamento, incluídos em uma solução de criptografia ponto a ponto (P2PE) validada e listada pelo PCI SSC.

Para obter um guia gráfico e escolher seu tipo de SAQ, consulte "Qual SAQ melhor se aplica ao meu ambiente?" na página 19.

Os comerciantes da categoria SAQ P2PE não têm acesso a dados de contas em texto claro em qualquer sistema de computador e somente inserem os dados da conta através de terminais de pagamento de hardware a partir de uma solução P2PE aprovada pelo PCI SSC. Os comerciantes da categoria SAQ P2PE podem ser comerciantes de estabelecimentos físicos (cartão presente) ou de pedidos por correio/telefone (cartão não presente). Por exemplo, um comerciante de pedidos por correio/telefone pode estar qualificado para o SAQ P2PE se receber dados de titulares de cartões em papel ou por telefone e inseri-los diretamente e somente em um dispositivo de hardware P2PE validado.

Os comerciantes da categoria P2PE confirmarão que atendem aos seguintes critérios de qualificação para esse canal de pagamento:

- Todo o processamento de pagamentos ocorre por meio de uma solução PCI P2PE validada e aprovada e listada pelo PCI SSC;
- Os únicos sistemas no ambiente do comerciante que armazenam, processam ou transmitem dados de conta são os dispositivos de Ponto de Interação (POI) que são aprovados para uso com a solução P2PE validada e listada pelo PCI;
- Sua empresa não recebe ou transmite dados de titulares de cartões eletronicamente.
- Não há armazenamento legado de dados de titulares de cartões eletrônicos no ambiente;
- Os dados de titulares de cartões retidos pela sua empresa estão em papel (por exemplo, relatórios ou recibos impressos) e esses documentos não são recebidos eletronicamente; e
- Sua empresa implementou todos os controles no *Manual de Instruções P2PE (PIM)* fornecido pelo provedor de soluções P2PE.

Este SAQ não se aplica a canais de comércio eletrônico.

SAQ D para Comerciantes – Todos os demais comerciantes qualificados para SAQ

O SAQ D para Comerciantes aplica-se a comerciantes qualificados para o SAQ que não cumpram os critérios de qualquer outro tipo de SAQ.

Estes são alguns dos exemplos de ambientes de comerciantes que usariam SAQ D:

- Comerciantes de comércio eletrônico que aceitam dados de titulares de cartões no site;
- Comerciantes com armazenamento eletrônico de dados de titulares de cartões;
- Comerciantes que não armazenam dados de titulares de cartões eletronicamente, mas que não atendem aos critérios de outro tipo de SAQ;
- Comerciantes com ambientes que possam atender aos critérios de outro tipo SAQ, mas que possuem requisitos PCI DSS adicionais que se aplicam ao seu ambiente.

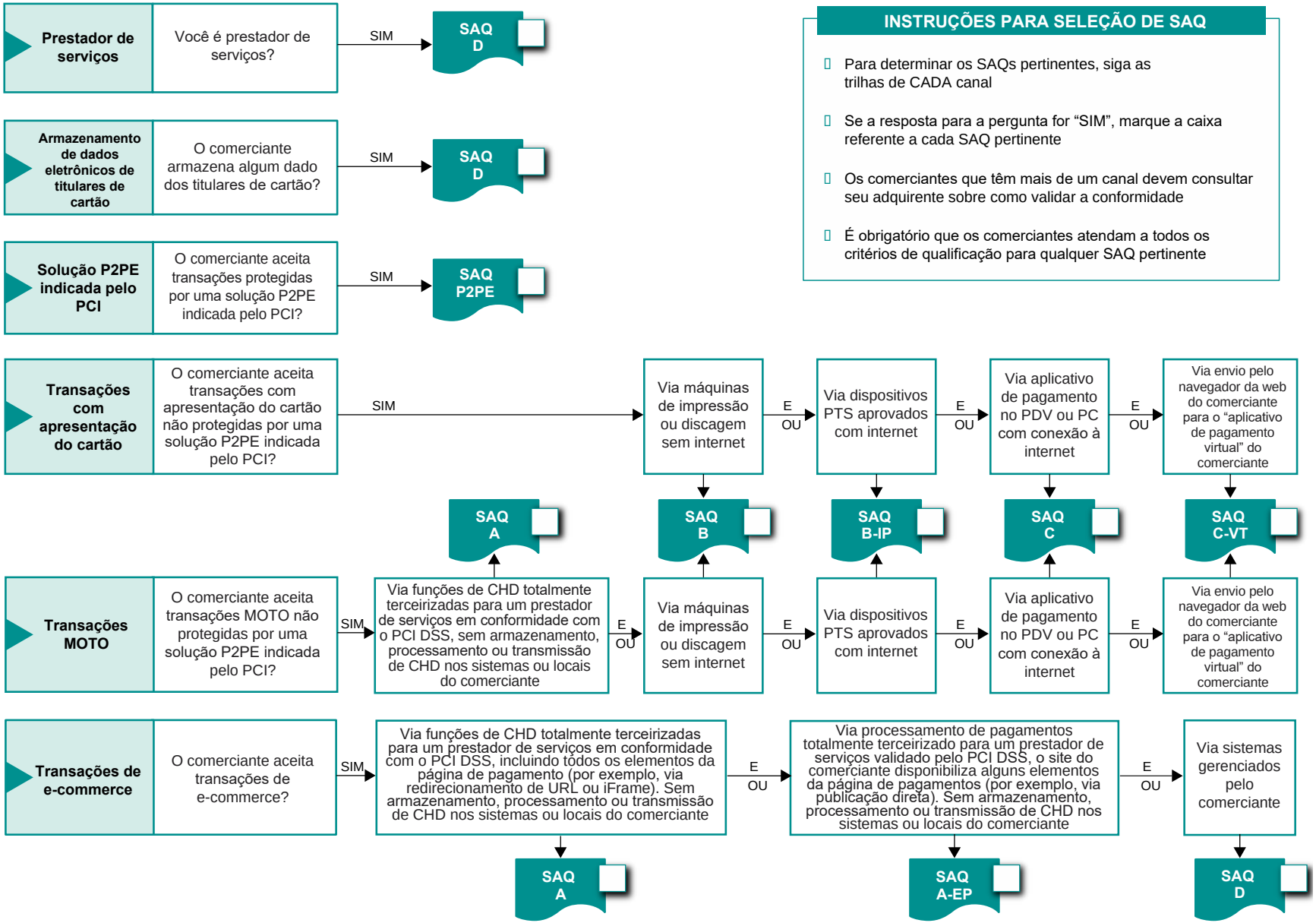
SAQ D para provedores de serviços – prestadores de serviços qualificados para SAQ

O SAQ D para Prestadores de Serviços aplica-se a todos os prestadores de serviços definidos por uma bandeira de pagamento como qualificados para SAQ.

Observação para SAQ D para Comerciantes e SAQ D Prestadores de Serviços: embora muitas organizações que completem o SAQ D precisem validar a conformidade com todos os requisitos do PCI DSS, algumas organizações com modelos de negócios muito específicos podem achar que alguns requisitos não se aplicam. Por exemplo, uma empresa que não utiliza tecnologia sem fio em qualquer capacidade não esperaria precisar fazer a validação de conformidade com as seções do PCI DSS, específicas para gerenciar tecnologias sem fio. Consulte as orientações específicas no respectivo SAQ D para obter informações sobre a exclusão de outros requisitos específicos.

Para obter um guia gráfico e escolher seu tipo de SAQ, consulte "Qual SAQ melhor se aplica ao meu ambiente?" na página 19.

Qual SAQ se aplica melhor ao meu ambiente?



INSTRUÇÕES PARA SELEÇÃO DE SAQ

- Para determinar os SAQs pertinentes, siga as trilhas de CADA canal
- Se a resposta para a pergunta for "SIM", marque a caixa referente a cada SAQ pertinente
- Os comerciantes que têm mais de um canal devem consultar seu adquirente sobre como validar a conformidade
- É obrigatório que os comerciantes atendam a todos os critérios de qualificação para qualquer SAQ pertinente