RECURSOS DE PROTEÇÃO DE PAGAMENTOS PARA PEQUENOS COMERCIANTES

Perguntas que você deve fazer aos seus fornecedores

VERSÃO 1.0 | JUNHO DE 2016

PCI Security Standards Council®

Introdução

Este documento foi elaborado como um auxílio a proprietários e operadores de pequenos negócios. As perguntas sugeridas aqui para fazer aos seus fornecedores e prestadores de serviço foram elaboradas para ajudar você a entender como essas entidades oferecem suporte para a proteção dos dados do cartão dos clientes.

Perguntas que você deve fazer aos seus fornecedores é um documento desenvolvido como um suplemento ao *Guia para pagamentos seguros*, que faz parte dos Recursos de proteção de pagamentos para pequenos comerciantes. Consulte o *Guia para pagamentos seguros* e os outros Recursos de proteção de pagamentos para pequenos comerciantes nos links a seguir.

RECURSO	URL
Guia para pagamentos seguros	https://pt.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Sistemas comuns de pagamento	https://pt.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Glossário de termos de segurança da informação e pagamentos	https://pt.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

Fornecedores e prestadores de serviço e como eles funcionam

Devido ao fato de que, muitas vezes, pequenas empresas e comerciantes entram em contato com diversos fornecedores de pagamento ou prestadores de serviço, é importante que os comerciantes entendam o tipo de fornecedor com o qual estão trabalhando e garantam que o fornecedor tenha tomado as medidas adequadas para proteger os dados de cartões.

A tabela na página 2 descreve os tipos mais comuns de fornecedores de pagamento e prestadores de serviços e informa o que os comerciantes devem verificar em relação a cada fornecedor.

A tabela que começa na página 3 fornece aos comerciantes sugestões de perguntas para fazer aos seus fornecedores ou prestadores de serviços a fim de ajudá-los a entender a função do fornecedor ou do prestador de serviços na proteção dos dados de cartões.

Fornecedores e prestadores de serviço

A tabela abaixo descreve os tipos mais comuns de fornecedores de pagamento e de prestadores de serviços, além de informar o que os comerciantes devem verificar em relação a cada fornecedor.

TIPO DE FORNECEDOR/ PRESTADOR DE SERVIÇO	FUNÇÃO	PADRÃO OU PROGRAMA DO PCI	O QUE VERIFICAR:
Fornecedor do aplicativo de pagamento	Vender e oferecer suporte a aplicativos que armazenam, processam e/ou transmitem dados do portador do cartão.	Padrão de segurança de dados de aplicativos de pagamento (PA-DSS)	O aplicativo está na List of PCI PA-DSS of Validated Payment Applications (Lista do PCI PA-DSS de aplicativos de pagamento validados).
Fornecedor do terminal de pagamento	Vender e oferecer suporte aos dispositivos usados para aceitar pagamentos com cartão (por exemplo, terminal de pagamento).	Segurança de transações com PIN (PTS)	O terminal de pagamento está na List of PCI Approved PTS Devices (Lista de dispositivos PTS aprovados pelo PCI).
Processadores de pagamento, provedores/ processadores de hospedagem de e-commerce	Armazenar, processar ou transmitir dados do portador do cartão em seu nome. Também podem hospedar e gerenciar seu servidor ou site de e-commerce e/ou desenvolver e oferecer suporte ao seu site.	Padrão de Segurança de Dados do PCI (PCI DSS)	Solicite o Atestado de Conformidade do PCI DSS do prestador de serviços e verifique se a avaliação incluiu o serviço que você está usando. Verifique se o prestador de serviços está em uma destas listas: MasterCard's List of Compliant Service Providers (Lista da MasterCard de prestadores de serviços em conformidade) Visa's Global Registry of Service Providers (Registro global de prestadores de serviços Visa) Visa Europe's Registered Member Agents (Agentes de membros registrados da Visa Europa)
Provedores de software como um serviço	Desenvolver, hospedar e/ou gerenciar seu aplicativo da Web ou aplicativo de pagamento baseado na nuvem (por exemplo, aplicativo de emissão de tíquetes ou de reserva online).	PCI DSS	Solicite o Atestado de Conformidade do PCI DSS do prestador de serviços e verifique se a avaliação incluiu o serviço que você está usando. Verifique se o prestador de serviços está em uma destas listas: MasterCard's List of Compliant Service Providers (Lista da MasterCard de prestadores de serviços em conformidade) Visa's Global Registry of Service Providers (Registro global de prestadores de serviços Visa) Visa Europe's Registered Member Agents (Agentes de membros registrados da Visa Europa)
Integradores/revendedores	Instalar os aplicativos de pagamento validados do PA-DSS em seu nome.	Integradores e revendedores qualificados (QIR)	Pergunte se o fornecedor é um integrador ou revendedor qualificado (QIR) do PCI. Verifique se o fornecedor está na List of PCI QIRs (Lista de QIRs do PCI).
Provedores de serviços que atendem ao(s) requisito(s) do PCI DSS	Gerenciar/operar sistemas ou serviços em seu nome (por exemplo, gerenciamento de firewall, patches/serviços antivírus).	PCI DSS	Solicite o Atestado de Conformidade do PCI DSS do prestador de serviços e verifique se a avaliação incluiu o serviço que você está usando. Verifique se o prestador de serviços está em uma destas listas: MasterCard's List of Compliant Service Providers (Lista da MasterCard de prestadores de serviços em conformidade) Visa's Global Registry of Service Providers (Registro global de prestadores de serviços Visa) Visa Europe's Registered Member Agents (Agentes de membros registrados da Visa Europa)

Perguntas

A tabela abaixo contém várias perguntas que os comerciantes devem fazer aos seus fornecedores/prestadores de serviços para determinar se os controles adequados estão em vigor para proteger os dados de cartões.

PERGUNTA *Do comerciante ao fornecedor*	**RESPOSTA DESEJADA DO FORNECEDOR**	**AÇÃO RECOMENDADA** *Com base na resposta do fornecedor*
QUAL É O NÍVEL DE SEGURANÇA DE SUA SOLUÇÃO OU PRODUTO?		
1. Sua solução ou produto garante a captura e transmissão seguras dos dados do portador do cartão?	**Para transações de pagamento presenciais com cartão presente:** **SIM** • Verifique se o terminal de pagamento é aprovado pelo PCI PTS: List of PCI Approved PTS Devices (Lista de dispositivos PTS aprovados pelo PCI) E/OU • Verifique se o aplicativo de pagamento é validado pelo PCI PA-DSS: List of PCI PA-DSS of Validated Payment Applications (Lista do PCI PA-DSS de aplicativos de pagamento validados) OU • Verifique se a solução de criptografia é validada pelo PCI P2PE: List of PCI P2PE Validated Solutions (Lista de soluções validadas pelo PCI P2PE)	Se a resposta for **NÃO**, faça a Pergunta 2.
	Para transações de pagamento com cartão não presente (inclusive em e-commerce e encomendas por correio e por telefone): **SIM** • Verifique se o aplicativo de pagamento é validado pelo PCI PA-DSS: List of PCI PA-DSS of Validated Payment Applications (Lista do PCI PA-DSS de aplicativos de pagamento validados) OU • Verifique se o prestador de serviços é conforme ao PCI DSS: MasterCard's List of Compliant Service Providers (Lista da MasterCard de prestadores de serviços em conformidade) Visa's Global Registry of Service Providers (Registro global de prestadores de serviços Visa) Visa Europe's Registered Member Agents (Agentes de membros registrados da Visa Europa)	

Perguntas

PERGUNTA *Do comerciante ao fornecedor*	RESPOSTA DESEJADA DO FORNECEDOR	AÇÃO RECOMENDADA *Com base na resposta do fornecedor*
QUAL É O NÍVEL DE SEGURANÇA DE SUA SOLUÇÃO OU PRODUTO? *(continuação)*		
2. Nosso acordo com você (o fornecedor) inclui cláusulas que afirmam que você manterá seu produto ou serviço em conformidade com o PCI DSS (ou que ele será validado pelo PCI DSS)?	**SIM** Fornecedores que ofereçam produtos ou soluções que estão ou ficarão em conformidade com o PCI DSS devem estar dispostos a concordar com que essa situação seja incluída em um contrato por escrito. Para obter informações adicionais sobre evidências a serem verificadas em relação a produtos e soluções em conformidade com o PCI DSS, consulte a Pergunta 1 acima.	Se a resposta for **NÃO**, considere buscar outro fornecedor ou solução.
3. Seu produto ou solução armazena as informações de cartão de pagamento localmente (no meu estabelecimento)?	**NÃO** Em caso afirmativo, os comerciantes podem considerar apostar em uma solução de tokenização ou criptografia para proteger melhor os dados de cartões. Consulte o *Guia para pagamentos seguros* para obter mais informações sobre criptografia e tokenização.	Se a resposta for **SIM**, o comerciante deve confirmar com o fornecedor que os dados estão armazenados de acordo com os requisitos do PCI DSS. Em caso negativo, considere buscar outro fornecedor.
4. Seu produto ou solução protege as informações de cartão de pagamento com criptografia forte?	**SIM** A criptografia é uma maneira de proteger as informações de modo a diminuir a probabilidade de roubo. Se você puder, selecione uma solução da List of PCI P2PE Validated Solutions (Lista de soluções validadas pelo PCI P2PE), nas quais os dados do cartão são protegidos assim que são recebidos e permanecem protegidos enquanto percorrem a rede.	Se a resposta for **NÃO**, considere buscar outro fornecedor ou solução.

Perguntas

PERGUNTA *Do comerciante ao fornecedor*	**RESPOSTA DESEJADA DO FORNECEDOR**	**AÇÃO RECOMENDADA** *Com base na resposta do fornecedor*
QUAL É O NÍVEL DE SEGURANÇA DA INSTALAÇÃO DO MEU PRODUTO?		
5. Se o fornecedor for instalar um aplicativo de pagamento da Lista de aplicativos de pagamento validados do PCI Council, pergunte: Você é um integrador ou revendedor qualificado (QIR) do PCI?	**SIM** Os QIRs são treinados e qualificados pelo Council para instalar e integrar aplicativos de pagamento PA-DSS, e suas instalações atestam que o aplicativo de pagamento do PA-DSS foi implementado de modo a suportar a conformidade com o PCI DSS. Verifique se o fornecedor consta na lista: List of PCI QIRs (Lista de QIRs do PCI).	Se a resposta for **NÃO**, faça as perguntas de acompanhamento à esquerda.
Perguntas de acompanhamento se a resposta acima for NÃO: Se o aplicativo que o fornecedor instalará não for validado pelo PCI SSC, ou se o fornecedor não for um QIR, pergunte: • Você oferece suporte durante a instalação para garantir que nossa implementação atenda aos requisitos do PCI DSS? • Você oferece um guia de implementação? • Você oferece orientação durante a instalação sobre como garantir que os dados do cartão estejam protegidos onde quer que sejam armazenados, processados ou transmitidos?	**SIM** O fornecedor deve ter processos definidos para ajudá-lo com a instalação da solução em conformidade com os requisitos do PCI DSS. A instalação inadequada pode deixar a solução vulnerável e comprometer a segurança dos dados. O objetivo é que o fornecedor explique como ele ajuda a garantir que os requisitos do PCI DSS são ou podem ser atendidos pelo produto ou solução.	Se a resposta for **NÃO**, considere buscar outro fornecedor.

Perguntas

PERGUNTA *Do comerciante ao fornecedor*	RESPOSTA DESEJADA DO FORNECEDOR	AÇÃO RECOMENDADA *Com base na resposta do fornecedor*
VOCÊ OFERECE SUPORTE E MANUTENÇÃO CONTÍNUOS PARA SEU PRODUTO OU SOLUÇÃO? SE SIM, COMO?		
6. Seu produto ou solução precisa ser instalado em minha rede ou em meus sistemas?	**SIM** O fornecedor deve fornecer manutenção e suporte contínuos para atualizações de software e patches de segurança. Além disso, deve fornecer versões futuras e suporte a elas. É importante ter vendedores ou fornecedores que ofereçam suporte total aos seus produtos e ajudem com instalações e patches para garantir que as mudanças feitas no sistema se alinhem aos requisitos do PCI.	Se a resposta for **SIM**, veja as perguntas de acompanhamento à esquerda. Se a resposta for **NÃO**, vá para a Pergunta 7.
Perguntas de acompanhamento se a resposta acima for SIM: • Você instala patches e atualizações no sistema ou solução? • Você faz isso de maneira alinhada aos requisitos do PCI DSS? • Como você realiza as notificações e disponibiliza os patches? E que suporte você oferece?	**SIM** Se a solução nunca for atualizada, ela pode ficar vulnerável e acarretar comprometimento futuro.	Se a resposta for **NÃO**, considere buscar outro fornecedor.
7. A solução é instalada em sistemas pertencentes ao prestador de serviços e mantidos (hospedados) por ele?	**SIM** Isso é considerado um serviço gerenciado. Se o prestador de serviços for hospedar a solução, solicite o Atestado de Conformidade do PCI DSS do prestador de serviços e verifique se a avaliação incluiu o serviço que você está usando.	Se a resposta for **SIM**, faça a pergunta de acompanhamento à esquerda. Se a resposta for **NÃO** (o serviço gerenciado não é conforme ao PCI DSS) considere buscar outra solução.
Pergunta de acompanhamento se a resposta acima for **SIM**: O ambiente do prestador de serviços é conforme ao PCI DSS?	Verifique se o prestador de serviços está em uma destas listas: MasterCard's List of Compliant Service Providers (Lista da MasterCard de prestadores de serviços em conformidade) Visa's Global Registry of Service Providers (Registro global de prestadores de serviços Visa) Visa Europe's Registered Member Agents (Agentes de membros registrados da Visa Europa)	

Perguntas

PERGUNTA *Do comerciante ao fornecedor*	RESPOSTA DESEJADA DO FORNECEDOR	AÇÃO RECOMENDADA *Com base na resposta do fornecedor*
VOCÊ OFERECE SUPORTE E MANUTENÇÃO CONTÍNUOS PARA SEU PRODUTO OU SOLUÇÃO? *(continuação)*		
8. Você precisa ter acesso remoto ao meu sistema ou solução de pagamento para prestar suporte?	**NÃO** O acesso remoto costuma ser utilizado para realizar violações de dados de pagamento. A funcionalidade de acesso remoto deve ser limitada ao uso periódico breve e deve ser desativada sempre que não estiver em uso.	Se a resposta for **NÃO**, vá para a Pergunta 9. Se a resposta for **SIM**, faça as perguntas de acompanhamento à esquerda.
Perguntas de acompanhamento se a resposta acima for SIM: • Você precisa de acesso remoto para estar sempre ativo?	**NÃO** A funcionalidade de acesso remoto deve ser limitada ao uso periódico breve e deve ser desativada sempre que não estiver em uso.	Se a resposta for **SIM** (se o acesso remoto precisar estar sempre ativo), considere buscar outro fornecedor ou solução.
• Que passos você executa para proteger as conexões durante o acesso remoto?	**Seu fornecedor deve usar autenticação de múltiplos fatores e um nome de usuário e senha diferentes para cada cliente que ele acessa remotamente.** As conexões de acesso remoto podem ser protegidas por meio de IDs de usuário e senhas exclusivas para cada pessoa que usar o sistema. Além disso, devem ser usadas várias formas de verificar a identidade da pessoa que acessa o sistema (autenticação de múltiplos fatores). Os fornecedores que usam um nome de usuário e senha exclusivos para cada um de seus clientes evitam que o comprometimento de segurança de um de seus clientes afete muitos dos outros clientes ou mesmo todos eles.	Se o produto ou solução não oferecer autenticação de múltiplos fatores para acesso remoto, considere buscar outra solução.
9. A solução ou o produto precisa se integrar com meus outros sistemas, como terminais de pagamento, controle de contas a receber ou outros sistemas que contenham dados do portador do cartão?	**NÃO** Um terminal de pagamento autônomo é mais simples de proteger do que um sistema de pagamento mais complexo com vários sistemas conectados. Nos casos em que a solução exigir integração com outros sistemas, é preciso considerar se ela simplificará o seu ambiente de processamento e agregará valor à sua empresa. Você só deve trabalhar com essa condição se a integração for realmente necessária para sua empresa, pois o uso de uma solução integrada aumenta o escopo do PCI DSS, uma vez que torna o ambiente de dados do portador do cartão maior e mais complexo. MasterCard's List of Compliant Service Providers (Lista da MasterCard de prestadores de serviços em conformidade)	Se a resposta for **SIM**, considere buscar outro fornecedor ou produto, a menos que seja realmente necessário ter uma solução mais sofisticada com conexões com outros sistemas.

Perguntas

PERGUNTA *Do comerciante ao fornecedor*	**RESPOSTA DESEJADA DO FORNECEDOR**	**AÇÃO RECOMENDADA** *Com base na resposta do fornecedor*
O QUE ACONTECERÁ SE HOUVER UMA VIOLAÇÃO DE DADOS?		
10. Caso haja uma violação de dados e seu produto ou solução estiver envolvido: • Se eu for penalizado, você oferece suporte e proteção? • Como e quando você me notificará se houver uma violação? • Que monitoramento para violações de dados e atividades suspeitas você fornece?	**SIM** O fornecedor ou prestador de serviços deve fornecer suporte no caso de uma violação de dados do portador do cartão. O fornecedor ou prestador de serviços deve concordar em cooperar com um investigador forense se houver dúvidas sobre o serviço ou solução gerenciada que ele oferece. O fornecedor ou prestador de serviços deve indenizar o comerciante por multas incorridas no caso de uma violação e se for determinado que a solução do fornecedor foi a causa principal.	Se a resposta for **NÃO**, considere buscar outro fornecedor ou solução.
11. O fornecedor ou prestador de serviços possui seguro para cobrir as violações de dados relacionadas ao seu produto ou solução?	**SIM** Ter um seguro demonstra que o fornecedor ou prestador de serviços pensou em sua responsabilidade em relação a violações de dados de cartões. Se a resposta for **SIM**, pergunte sobre o escopo da cobertura e se sua implementação será coberta.	Se a resposta for **NÃO** (se o vendedor não tiver seguro ou não estiver disposto a ele próprio fazer reservas para contingências desse tipo), considere obter o seu próprio seguro ou buscar outro fornecedor.
12. O fornecedor ou prestador de serviços auxiliará na notificação de meus clientes caso ocorra uma violação de dados e a solução de produto desse fornecedor ou prestador de serviços seja a causa principal?	**SIM** Os fornecedores ou prestadores de serviços devem estar dispostos a ajudar os comerciantes com notificação sobre violação quando seu sistema de pagamento for a causa principal da violação.	Se a resposta for **SIM**, faça as perguntas de acompanhamento à esquerda. Se a resposta for **NÃO** (se o fornecedor não auxiliar na notificação), você deve desenvolver um plano para notificação e/ou considerar buscar outro fornecedor.
Se a resposta for **SIM**, até que ponto você ajuda com a notificação? • Você cobre o custo? • Você envia as notificações? • Você fornece monitoramento de crédito para os clientes afetados?		