

FUNDAMENTOS DA SEGURANÇA DE DADOS PARA PEQUENOS COMERCIANTES
UM PRODUTO DA FORÇA-TAREFA DE PEQUENOS COMERCIANTES DA INDÚSTRIA DE CARTÕES DE PAGAMENTO

Guia para Pagamentos Seguros

Versão 2.0 | Agosto de 2018

Fundamentos da segurança de dados para pequenos comerciantes: Guia para pagamentos seguros
Copyright 2018 Conselho dos Padrões de Segurança PCI, LLC. Todos os direitos reservados.

Este Guia para pagamentos seguros é fornecido pelo PCI Security Standards Council (PCI SSC) para informar e instruir comerciantes e outras entidades envolvidas no processamento de cartões de pagamento. Para obter mais informações sobre o PCI SSC e os padrões que gerenciamos, acesse www.pcisecuritystandards.org.

A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre os Padrões do PCI ou seus documentos de apoio.



**COMPREENDENDO
SEU RISCO**

Compreendendo seu risco

Por ser uma pequena empresa, você é alvo de ladrões de dados.

Se seus dados de cartões de pagamento forem violados, as consequências podem aparecer rapidamente. Em situações como essa, seus clientes deixariam de confiar em sua capacidade de proteger informações pessoais. E levariam seus negócios para outros lugares. Poderiam ocorrer sanções financeiras e danos resultantes de ações judiciais, e sua empresa poderia perder a capacidade de aceitar cartões de pagamento. Uma pesquisa com 1.015 pequenas e médias empresas detectou que 60% das empresas que sobrem violações fecham em seis meses. (NCSA)



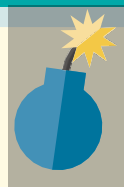
DAS PEQUENAS EMPRESAS
FORAM VIOLADAS NOS
ÚLTIMOS 12 MESES.

(Instituto
Ponemon)



DAS VIOLAÇÕES ATINGIRAM
PEQUENAS EMPRESAS NO ANO
PASSADO, ALTA EM RELAÇÃO
AOS 53% DO ANO ANTERIOR

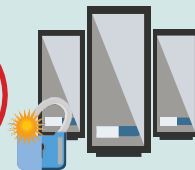
(Verizon 2017)



£ 30 bilhões

FOI O CUSTO DAS VIOLAÇÕES DE
SEGURANÇA CIBERNÉTICA PARA
OS NEGÓCIOS DO REINO UNIDO
EM 2016

(Beaming UK)



DAS PEQUENAS EMPRESAS TINHAM
POLÍTICAS FORMAIS QUE
ABRANGEM RISCOS DE SEGURANÇA
CIBERNÉTICA EM 2017

(Departamento de Cultura, Mídia e Esporte)

O que está em risco?

OS DADOS DO CARTÃO DE SEUS CLIENTES É UMA MINA DE OURO PARA OS CRIMINOSOS. NÃO DEIXE QUE ISSO ACONTEÇA COM VOCÊ!

Siga as ações contidas neste guia para se proteger contra o roubo de dados.

O número da conta principal (PAN) e o código de segurança do cartão de três ou quatro dígitos são exemplos de dados de cartão de pagamento. As setas vermelhas abaixo apontam para os tipos de dados que requerem proteção.

TIPOS DE DADOS EM UM CARTÃO DE PAGAMENTO



O QUE É O PCI DSS?

O Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS) é um conjunto de requisitos de segurança que podem ajudar os pequenos comerciantes a protegerem os dados de cartões de clientes localizados nos cartões de pagamento.

Os pequenos comerciantes podem se familiarizar com a validação de sua conformidade com o PCI DSS por meio de um Questionário de autoavaliação (SAQ).

Para obter mais informações sobre o PCI DSS, consulte Recursos no final deste guia.

Entendendo seu sistema de pagamento: Condições comuns de pagamento

A aceitação presencial de pagamentos em cartão de seus clientes requer equipamentos especiais. Dependendo do país onde você está, o equipamento usado para receber pagamentos é chamado por diferentes nomes. Veja abaixo os tipos que mencionamos neste documento e como são geralmente chamados.



Um **TERMINAL DE PAGAMENTO** é o dispositivo usado para receber pagamentos com cartão do cliente ao passar, inserir, tocar ou introduzir manualmente o número do cartão. Terminal de ponto de venda (POS), máquina de cartão de crédito, terminal PDQ ou terminal EMV/habilitado para chip também são nomes usados para descrever esses dispositivos.



Uma **CAIXA REGISTRADORA ELETRÔNICA** (ou gaveta) registra e calcula transações e pode imprimir recibos, mas não aceita pagamentos com cartão do cliente.



Um **TERMINAL DE PAGAMENTO INTEGRADO** é um terminal de pagamento e uma caixa registradora eletrônica ao mesmo tempo, o que significa que recebe pagamentos, registra e calcula transações e a impressão de recibos/cupons.



Um **BANCO COMERCIAL** é um banco ou uma instituição financeira que processa pagamentos com cartão de crédito e/ou débito em nome de comerciantes. Adquirente, banco adquirente e processador de cartão ou de pagamento também são termos usados para essa entidade.

ENCRIPTAÇÃO (ou criptografia) torna os dados do cartão ilegíveis para pessoas sem informações especiais (chamadas de chave). A criptografia pode ser usada em dados armazenados e dados transmitidos por uma rede. Os terminais de pagamento que fazem parte de uma solução P2PE listada pelo PCI oferece aos comerciantes a melhor garantia de qualidade da encriptação. Com uma solução P2PE listada pelo PCI, os dados do cartão são sempre inseridos diretamente em um terminal de pagamento aprovado pela PCI com algo chamado "leitura e troca de dados seguros (SRED, secure reading and exchange of data)". Essa abordagem minimiza o risco para dados de cartão de texto simples e protege os comerciantes contra invasões dos terminais de pagamento, como um malware de "raspagem de memória". Qualquer encriptação que não seja feita em P2PE listada pelo PCI deve ser discutida com seu fornecedor.



Um **SISTEMA DE PAGAMENTO** inclui todo o processo de aceitação de pagamentos com cartão. Também chamado de ambiente de dados do titular do cartão (CDE, cardholder data environment), seu sistema de pagamento pode incluir um terminal de pagamento, uma caixa registradora eletrônica, outros dispositivos ou sistemas conectados a um terminal de pagamento (por exemplo, Wi-Fi para conectividade ou um PC para inventário) e conexões com um banco comercial. É importante usar apenas terminais e soluções de pagamento seguros em seu sistema de pagamento. Consulte a [página 21](#) para obter mais informações.

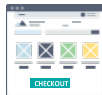


Compreendendo seu sistema de pagamento para e-commerce

Quando você vende produtos ou serviços on-line, você é classificado como um comerciante de e-commerce. Veja alguns termos comuns com os quais você pode se deparar e o que eles significam.



Um **SITE DE E-COMMERCE** armazena e apresenta seu site comercial e suas páginas de compras aos seus clientes. O site pode ser hospedado e gerenciado por você ou por um provedor de hospedagem terceirizado.



Suas **PÁGINAS DE COMPRAS** são páginas da web que mostram seu produto ou seus serviços para seus clientes, permitindo que eles pesquisem e selecionem as compras e informem seus dados pessoais e de entrega. Nenhum dado de cartão de pagamento é solicitado ou capturado nessas páginas.



Sua **PÁGINA DE PAGAMENTO** é uma página ou formulário da web usado para coletar os dados do cartão de pagamento do seu cliente depois que ele decide comprar seu produto ou seus serviços. O tratamento dos dados de cartão pode ser 1) gerenciado exclusivamente pelo comerciante usando um carrinho de compras ou um aplicativo de pagamento, 2) parcialmente gerenciado pelo comerciante com o apoio de um terceirizado usando diversos métodos, ou 3) totalmente feito por um terceirizado. Na maioria das vezes, usar uma empresa terceirizada é a opção mais segura. É importante garantir que seja uma terceirizada validada pelo PCI DSS.



Um **SISTEMA DE PAGAMENTO PARA E-COMMERCE** contempla todo o processo para que um cliente selecione produtos ou serviços e para que o comerciante de e-commerce aceite pagamentos de cartão, incluindo um site com páginas de compras e uma página ou formulário de pagamento, outros dispositivos ou sistemas conectados (por exemplo, Wi-Fi ou PC para inventário) e conexões com o banco comercial (também chamado de prestador de serviços de pagamento ou gateway de pagamento). Dependendo da configuração de pagamento de e-commerce do comerciante, o sistema de pagamento para e-commerce pode ser totalmente terceirizado, parcialmente gerenciado pelo comerciante com suporte terceirizado ou gerenciado exclusivamente pelo comerciante.

Como sua empresa está em risco?

Quanto mais recursos seu sistema de pagamento tiver, mais complexo será para protegê-lo.

Pense cuidadosamente se você realmente precisa de recursos extras como Wi-Fi, software de acesso remoto, câmeras conectadas à internet ou sistemas de gravação de telefonemas para o seu negócio. Se não forem configurados e gerenciados adequadamente, esses recursos podem dar aos criminosos acesso fácil aos dados de cartão de pagamento de seus clientes.

Se você é comerciante de e-commerce, é muito importante compreender se e como os dados de pagamento são capturados em seu site. Na maioria dos casos, a opção mais segura é usar uma empresa terceirizada para capturar e processar pagamentos.

AMBIENTE COMPLEXO



MAIS DIFÍCIL DE REDUZIR O RISCO

AMBIENTE SIMPLES



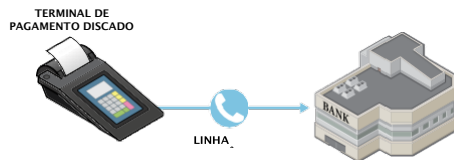
MAIS FÁCIL DE REDUZIR O RISCO

Como você vende suas mercadorias ou serviços? Há três maneiras principais:

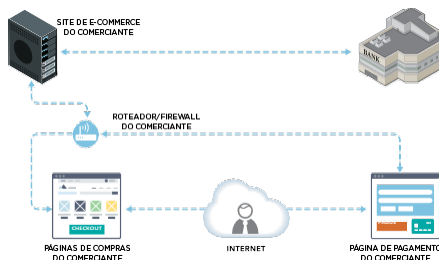
1. Uma pessoa entra em sua loja e faz uma compra usando um cartão.
2. Uma pessoa visita seu site e paga on-line.
3. Uma pessoa liga para sua loja e fornece detalhes do cartão por telefone, ou envia os detalhes por e-mail ou fax.

Entendendo seu risco: Tipos de sistema de pagamento

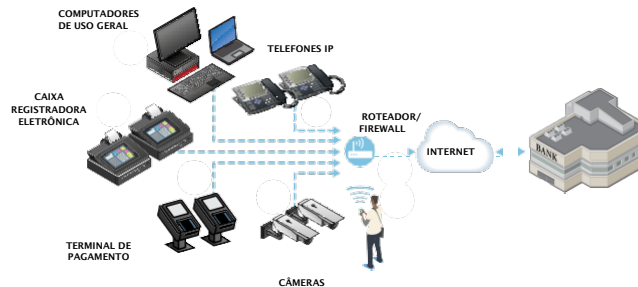
Os riscos de segurança variam muito dependendo da complexidade do sistema de pagamento, seja presencial ou online.



Sistema de pagamento simples para compras em loja



Sistema de pagamento de e-commerce complexo para compras em loja online, no qual o comerciante gerencia seu próprio site e página de pagamento



Sistema de pagamento complexo para compras em loja, com Wi-Fi, câmeras, telefones pela Internet e outros sistemas conectados

Use os [Sistemas comuns de pagamento](#) para ajudá-lo a identificar que tipo de sistema de pagamento você usa, seu risco e as dicas de segurança recomendadas como ponto de partida para as conversas que você precisa ter com seu banco comercial e fornecedores parceiros.



**PROTEJA SEU
NEGÓCIO COM ESTES
PRINCÍPIOS BÁSICOS DE
SEGURANÇA**

Como você protege sua empresa?

A boa notícia é que você pode começar a proteger sua empresa hoje com esses princípios básicos de segurança:

 Use senhas fortes e altere as senhas-padrão	 Proteja os dados do seu cartão e armazene apenas o que você precisa	 Inspeione se os terminais de pagamento foram adulterados	 Use parceiros de negócios confiáveis e saiba como contatá-los	 Instale os patches de seus fornecedores	 Proteja o acesso interno aos dados de cartão
Custo 	Custo 	Custo 	Custo 	Custo 	Custo 
Facilidade 	Facilidade 	Facilidade 	Facilidade 	Facilidade 	Facilidade 
Mitigação de riscos 	Mitigação de riscos 	Mitigação de riscos 	Mitigação de riscos 	Mitigação de riscos 	Mitigação de riscos 
 Não permita que os hackers tenham acesso fácil aos seus sistemas	 Use software antivírus	 Verifique se há vulnerabilidades e corrija os problemas	 Use terminais e soluções de pagamento seguros	 Proteja sua empresa contra vulnerabilidades da Internet	 Para ter o máximo de proteção, torne seus dados inúteis para criminosos
Custo 	Custo 	Custo 	Custo 	Custo 	Custo 
Facilidade 	Facilidade 	Facilidade 	Facilidade 	Facilidade 	Facilidade 
Mitigação de riscos 	Mitigação de riscos 	Mitigação de riscos 	Mitigação de riscos 	Mitigação de riscos 	Mitigação de riscos 

Esses princípios básicos de segurança são organizados em ordem, desde os mais fáceis e com implementação menos onerosa, até os mais complexos e com implementação mais cara. A quantidade de redução de risco que cada um oferece aos pequenos comerciantes também é indicada na coluna "Mitigação de riscos".



Use senhas fortes e altere as senhas-padrão

Custo



Facilidade



Mitigação de riscos



Suas senhas são essenciais para a segurança dos dados do computador e dos cartões. Assim como uma trava em sua porta protege a propriedade física, uma senha ajuda a proteger seus dados empresariais. Esteja ciente de que equipamentos de computador e software prontos para uso (inclusive seu terminal de pagamento) geralmente vêm com senhas-padrão (senhas predefinidas) como “senha” ou “admin”. Elas geralmente são conhecidas por hackers, por isso são uma fonte frequente de violações de pequenos comerciantes.

MUDE SUAS SENHAS REGULARMENTE. Trate suas senhas como uma escova de dentes. Não deixe que mais ninguém a use; além disso, altere-a a cada três meses.

CONVERSE COM SEUS PRESTADORES DE SERVIÇOS. Pergunte aos fornecedores ou prestadores de serviços sobre senhas-padrão e como alterá-las. E então altere-as! Além disso, se o seu prestador de serviços gerencia as senhas para seus sistemas, pergunte se ele alterou as senhas padrão do fornecedor.

DIFICULTE A ADIVINHAÇÃO. As senhas mais comuns são “senha” e “123456.” A primeira tentativa dos hackers sempre são senhas fáceis de adivinhar, pois elas são usadas por quase todas as pessoas. Uma senha forte tem sete ou mais caracteres e uma combinação de letras maiúsculas e minúsculas, números e símbolos (como !@#\$%^). Uma frase também pode ser uma senha forte (e pode ser mais fácil de lembrar), como “B1gMac&frieS”.

NÃO COMPARTILHE. Insista para que cada funcionário tenha sua própria ID de login e senha, as quais nunca devem compartilhar!

SENHAS PADRÃO COMUNS QUE DEVEM SER ALTERADAS:

[nenhum]

[nome do produto/fornecedor]

1234 ou 4321

acesso

admin

anônimo

nome da empresa

base de dados

convidado

gerente

pass

password

raiz

as

segredo

sysadmin usuário

65%

das pequenas empresas que têm política de senha não a aplicam rigorosamente

Instituto Ponemon

Para obter mais informações sobre a segurança de senhas, consulte estes recursos no site do PCI Council:



INFOGRÁFICO

It's Time to Change Your Password (É hora de alterar sua senha)



VÍDEO

Learn Password Security in 2 Minutes (Aprenda sobre segurança da senha em 2 minutos)



Proteja os dados de cartões e armazene apenas o que você precisa

Custo



Facilidade



Mitigação de riscos



É impossível proteger os dados do cartão se você não souber onde eles estão.

O que você pode fazer?

Outro lugar que deve ser considerado como possível local de armazenamento de dados de pagamento é os e-mails. Se você receber dados de cartão por e-mail, você pode processar a transação, mas deve excluir o e-mail imediatamente e informar ao remetente como você prefere receber os dados do portador do cartão (e que o e-mail não é a melhor maneira de enviá-los). Não responda usando o e-mail original do seu cliente. Em vez disso, exclua os detalhes do cartão do e-mail de resposta. Caso contrário, você estará expondo ainda mais os dados do cartão através do armazenamento do e-mail original, do e-mail enviado etc.

A tokenização tem um objetivo semelhante à criptografia, mas funciona de maneira diferente. Ela substitui os dados do cartão por dados sem significado (um "token"), que não têm valor para um hacker. Os comerciantes podem usar tokens para enviar transações subsequentes, processar um reembolso etc., sem precisar armazenar os dados do cartão de pagamento. O token é usado pelo seu processador de pagamento para pesquisar os dados do cartão, que a empresa armazena em vez de você.

PERGUNTE A UM ESPECIALISTA. Pergunte ao seu fornecedor de terminal de pagamento, prestador de serviços ou banco comercial onde (se for o caso) seus sistemas armazenam dados e se você pode simplificar o processamento de pagamentos. Pergunte também como conduzir transações específicas (por exemplo, para pagamentos recorrentes) sem armazenar o código de segurança do cartão.

TERCEIRIZE. A melhor maneira de se proteger contra violações de dados é não armazenar dados de cartões de nenhuma forma. Considere terceirizar o processamento do seu cartão para um prestador de serviços em conformidade com o PCI DSS. Consulte Recursos na [página 25](#) para ver listas de prestadores de serviços compatíveis.

SE VOCÊ NÃO PRECISA DOS DADOS DO CARTÃO, NÃO OS ARMAZENE. Destrua/rasgue os dados do cartão dos quais você não precisa. Se você precisar manter documentos em papel que contenham dados confidenciais de cartões, passe um marcador preto e espesso sobre esses dados até que fiquem ilegíveis e guarde o documento em uma gaveta trancada com trava ou em um cofre ao qual apenas algumas pessoas tenham acesso.

LIMITE O RISCO. Em vez de aceitar os detalhes do pagamento por e-mail, peça que os clientes os forneçam por telefone, fax ou correio normal.

TOKENIZE OU CRIPTOGRAFE. Pergunte ao seu banco comercial se você REALMENTE precisa armazenar os dados do cartão. Se você precisar, pergunte ao seu banco comercial ou prestador de serviços sobre as tecnologias de criptografia ou tokenização que inutilizam os dados do cartão mesmo se eles forem roubados.



CONSULTE
PÁGINA 23

GUIA SOBRE CRIPTOGRAFIA

A criptografia usa uma fórmula matemática para fazer com que textos não criptografados se tornem ilegíveis a pessoas sem conhecimento especial (chamado de chave). A criptografia é aplicada aos dados armazenados, bem como aos dados transmitidos por uma rede.

A **CRIPTOGRAFIA** transforma o texto não criptografado em texto cifrado.

A **DESENCRIPTAÇÃO** parte do texto cifrado e transforma-o novamente em texto não criptografado.

Por exemplo:

This is secret stuff

CHAVE DE CRIPTOGRAFIA

5a0 (k\$H0Q%...

CHAVE DE DESENCRIPTAÇÃO

This is secret stuff



Inspeção se os terminais de pagamento foram adulterados

Custo



Facilidade



Mitigação de riscos



“Dispositivos de clonagem” varrem os dados do cartão quando o cliente o insere em um terminal de pagamento. É essencial que você e sua equipe saibam identificar um dispositivo de clonagem, como é a estética dos seus terminais de pagamento e quantos deles você tem. Você precisa verificar regularmente seus terminais de pagamento para se certificar de que não tenham sido adulterados. Caso haja qualquer suspeita de que um terminal tenha sido adulterado, **NÃO** O USE e informe imediatamente ao seu banco comercial e/ou seu fornecedor do terminal.

Consulte o [guia do PCI Council: Prevenção contra clonagem – Visão geral das melhores práticas para comerciantes](#)

Esteja atento e siga as recomendações abaixo:

FAÇA UMA LISTA de todos os terminais de pagamento e tire fotos (parte frontal e posterior, cabos e conexões) para que saiba futuramente como eles devem estar sempre.

PROCURE SINAIS ÓBVIOS de adulteração, como vedações quebradas em portas ou parafusos de acesso, cabeamento estranho/diferente e dispositivos ou recursos novos que você não reconhece. O guia do PCI Council (mencionado abaixo) pode ajudar.

PROTEJA OS TERMINAIS. Mantenha-os fora do alcance dos clientes quando não estiverem em uso e limite o campo visual de suas telas pelo público. Certifique-se de que seus terminais de pagamento estejam seguros antes de fechar a loja ao final do dia, inclusive quaisquer dispositivos que leiam cartões de pagamento de seus clientes ou aceitem seus números de identificação pessoal (PINs).

REPAROS DOS CONTROLES. Permita reparos de terminais de pagamento somente por pessoal de reparo autorizado e com agendamento. Diga a sua equipe para fazerem o mesmo. Monitore os terceiros com acesso físico aos seus terminais de pagamento, mesmo se estiverem lá por outro motivo, para garantir que eles não modifiquem os terminais.

LIGUE imediatamente para o fornecedor de seu terminal de pagamento ou para o banco comercial se suspeitar de alguma coisa!



Use parceiros entrar em contato com eles confiáveis e saiba como

Use provedores externos para serviços, dispositivos e aplicativos relacionados a pagamentos. Você também pode ter prestadores de serviços com os quais compartilha dados de cartão, que suportam ou gerenciam seus sistemas de pagamento ou que dão acesso aos dados do cartão. Você pode chamá-los de processadores, fornecedores, terceiros ou prestadores de serviços. Eles afetam sua capacidade de proteger seus dados de cartão, portanto é fundamental que você saiba quem eles são e quais perguntas de segurança deve fazer a eles.

SAIBA PARA QUEM LIGAR. Quem é o seu banco comercial? Quem mais o ajuda a processar pagamentos? De quem você comprou seu dispositivo ou software de pagamento e quem o instalou para você? Quem são seus prestadores de serviços?

DEIXE UMA LISTA PRONTA. Agora que você sabe para quem ligar, guarde os nomes das empresas e dos contatos, números de telefone, endereços de sites e outros detalhes de contato pelos quais você possa encontrá-los facilmente no caso de uma emergência.

CONFIRME SE SEUS PRESTADORES DE SERVIÇOS SÃO SEGUROS.

Seu prestador de serviços está cumprindo os requisitos do PCI DSS? Para comerciantes de e-commerce, é importante que seu prestador de serviços de pagamento esteja em conformidade como PCI DSS também! Consulte Recursos na [página 25](#) para ver as listas de prestadores de serviços compatíveis.

FAÇA PERGUNTAS. Quando você souber quem são seus provedores externos e o que eles fazem por você, converse com eles para entender como protegem os dados de cartões. Use o documento [Perguntas que você deve fazer aos seus fornecedores](#) para saber o que perguntar.

CONHEÇA OS TIPOS COMUNS DE FORNECEDORES. Revise a barra lateral à direita para entender os tipos comuns de fornecedores ou prestadores de serviços com os quais você pode trabalhar.

Custo



Facilidade



Mitigação de riscos



FORNECEDORES COMUNS

Consulte a tabela no documento [Perguntas que você deve fazer aos seus fornecedores](#) para obter mais detalhes sobre estes fornecedores comuns:

- Fornecedores de terminais de pagamento
- Fornecedores de aplicativos de pagamento
- Instaladores de sistemas de pagamento (chamados de integradores/revendedores)
- Prestadores de serviços que fazem processamento de pagamento ou hospedagem ou processamento de e-commerce
- Prestadores de serviços que ajudam você a cumprir os requisitos do PCI DSS (fornecendo serviços de firewall ou antivírus, por exemplo)
- Provedores de software como serviço



Instale os patches de seus fornecedores

Custo



Facilidade



Mitigação de riscos



O software pode ter falhas que são descobertas após o lançamento causadas por erros cometidos por programadores quando escreveram o código. Essas falhas são também chamadas de brechas de segurança, bugs ou vulnerabilidades. Os hackers exploram esses erros a fim de invadir o seu computador e roubar os dados de sua conta. Proteja seus sistemas aplicando patches disponibilizados pelo fornecedor para corrigir erros de codificação. A instalação pontual dos patches de segurança é essencial!

É importante saber como seu software está sendo regularmente atualizado com patches e quem é o responsável (pode ser você!). Além disso, alguns patches são instalados automaticamente assim que são disponibilizados. Se você não tiver certeza sobre como os patches são adicionados ou quem é o responsável por eles, pergunte ao seu fornecedor.

PERGUNTE ao seu fornecedor ou prestador de serviços como ele o notifica sobre novos patches de segurança. Sempre leia essas notificações.

QUAIS FORNECEDORES ENVIAM PATCHES? Você pode obter patches de fornecedores de seu terminal de pagamento, aplicativos de pagamento, outros sistemas de pagamento (gavetas, caixas registradoras, PCs, etc.), sistemas operacionais (Android, Windows, iOS, etc.), software aplicativo (inclusive navegador da Web) e software de negócios.

CERTIFIQUE-SE de que seus fornecedores atualizam os seus terminais de pagamento, sistemas operacionais, etc., para que possam suportar os patches de segurança mais recentes. Pergunte a eles.

COMERCIANTES DE E-COMMERCE. Instalar patches o mais rápido possível é muito importante para você também. Também fique atento a patches do seu prestador de serviços de pagamento. Pergunte ao seu provedor de hospedagem de e-commerce se eles corrigem o seu sistema (e com que frequência). Certifique-se de que eles atualizam o sistema operacional, a plataforma de e-commerce e/ou o aplicativo da Web para que possam suportar os patches mais recentes.

SIGA as instruções do seu fornecedor ou prestador de serviços e instale esses patches assim que possível.



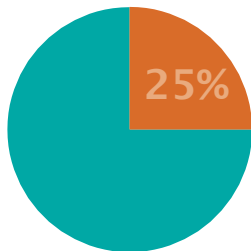
Proteja o acesso interno aos seus dados

Custo	
Facilidade	
Mitigação de riscos	

Abuso de privilégio significa uma pessoa usando...

Informações e dados de outra pessoa para obter acesso a sistemas ou dados aos quais essa pessoa não está autorizada a ter acesso.

25% DAS VIOLAÇÕES ENVOLVEM ATORES INTERNOS.



Verizon 2017

O CONTROLE DE ACESSO É MUITO IMPORTANTE. Configure seu sistema para conceder acesso somente com base na necessidade empresarial de conhecer a informação. Como proprietário, você tem acesso a tudo. Mas a maioria dos funcionários consegue trabalhar com acesso apenas a um subconjunto de dados, aplicativos e funções.

LIMITE O ACESSO a sistemas de pagamento, dados não criptografados de cartões, aplicativos e funções apenas aos funcionários que precisam de acesso e apenas o suficiente para fazerem seu trabalho.

MANTENHA UM REGISTRO. Acompanhe todos os visitantes que entrarem em contato com os processos internos de seu estabelecimento. Inclua nome, motivo da visita e nome do funcionário que autorizou o acesso do visitante. Guarde o registro por pelo menos um ano.

DESCARTE DISPOSITIVOS COM SEGURANÇA. Pergunte ao fornecedor do seu sistema de pagamento ou prestador de serviços sobre a maneira ideal de remover os dados de cartões com segurança antes de vender ou descartar dispositivos de pagamento (para que os dados não possam ser recuperados).

COMPARTILHE ESSAS INFORMAÇÕES. Disponibilize este guia aos seus funcionários, parceiros comerciais e prestadores de serviços terceirizados (como provedores de hospedagem de e-commerce) para que eles saibam o que é esperado deles.

AS IDS DE USUÁRIO DEVEM SER ÚNICAS para cada pessoa com acesso ao seu sistema de pagamento, sempre que possível. Isso ajudará você a acompanhar quem faz login e quando e as mudanças que essas pessoas venham a fazer.

Considere dar acesso aos funcionários para que recebam pagamentos, mas não para que processem reembolsos, ou para que recebam novas reservas e pedidos, mas não para que acessem dados de cartões de pagamento relacionados a reservas e pedidos existentes. Alguns funcionários não devem ter nenhum acesso.



Não permita que os hackers tenham acesso fácil aos seus sistemas

Custo



Facilidade



Mitigação de riscos



HACKERS = AMEAÇAS

Uma das maneiras mais fáceis que os hackers usam para entrar em um sistema é usando pessoas em quem o dono confia. Você precisa saber como seus fornecedores estão acessando seu sistema para se certificar de que eles não estejam deixando brechas para os hackers.

A autenticação de múltiplos fatores usa um nome de usuário e uma senha além de pelo menos um outro fator (como um cartão inteligente, um dongle* ou um código de acesso único).

*Um dispositivo útil que se conecta a um computador para permitir acesso a recursos de software sem fio, etc.

DESCUBRA. Pergunte ao fornecedor do sistema de pagamento ou ao prestador de serviços se ele usa acesso remoto para oferecer suporte ou acessar seus sistemas.

PERGUNTE COMO LIMITAR O USO DO ACESSO REMOTO. Muitos programas de acesso remoto ficam sempre ativos ou sempre disponíveis por padrão, o que significa que o fornecedor pode acessar seus sistemas remotamente o tempo todo (isso também significa que os hackers podem acessar seus sistemas também, pois muitos fornecedores usam senhas comuns para fazer o acesso remoto). Reduza seu risco: pergunte ao fornecedor como desabilitar o acesso remoto quando seu uso não for necessário e como habilitá-lo quando o fornecedor ou prestador de serviços solicitar.

DESATIVE-O QUANDO A ATIVIDADE DESEJADA ESTIVER FINALIZADA.

Para proteger sua empresa, é importante que você participe da gestão de como e quando seus fornecedores podem acessar seus sistemas.

USE AUTENTICAÇÃO FORTE. Se você precisar permitir o acesso remoto, solicite autenticação de múltiplos fatores e criptografia forte.

CERTIFIQUE-SE DE QUE OS PRESTADORES DE SERVIÇOS USAM

CREDENCIAIS EXCLUSIVAS. Cada um deve usar credenciais de acesso remoto que sejam exclusivas para sua empresa e que não sejam as mesmas usadas para outros clientes.

PEÇA AJUDA. Peça ajuda ao seu fornecedor ou prestador de serviços para desativar o acesso remoto ou (se seu fornecedor ou prestador de serviço precisar do acesso remoto) para configurar a autenticação multifatores. Consulte [Perguntas que você deve fazer aos seus fornecedores](#) para saber exatamente o que perguntar.

Se o fornecedor suportar ou solucionar problemas no seu sistema de pagamento trabalhando no escritório dele (e não no seu estabelecimento), quer dizer que ele estará usando a Internet e um software de acesso remoto para fazer isso.

VNC e LogMeIn são alguns exemplos de produtos que o fornecedor pode instalar no seu terminal e usar para suporte remotamente.



Use software anti vírus

Os hackers criam vírus e outros códigos mal-intencionados para explorar recursos de software e erros de codificação, para que possam entrar em seus sistemas e roubar dados do cartão. O uso de software antivírus atualizado (também chamado de antimalware) ajuda a proteger seus sistemas.

INSTALE SOFTWARE ANTIVÍRUS PARA PROTEGER SEU SISTEMA

DE PAGAMENTO. É fácil de instalar e pode ser obtido em sua loja de suprimentos de escritório local ou varejista de TI.

DEFINA A CONFIGURAÇÃO DE “ATUALIZAÇÃO AUTOMÁTICA” DO SOFTWARE para que você sempre tenha a proteção mais recente disponível.

OBTENHA ACONSELHAMENTO. Pergunte ao seu varejista de TI sobre os produtos que eles recomendam para proteção antivírus/antimalware.

FAÇA VERIFICAÇÕES AUTOMÁTICAS. Execute regularmente verificações completas do sistema, pois seus sistemas podem ter sido infectados por um novo malware que foi lançado antes que seu software antivírus pudesse detectá-lo.

COMERCIANTES DE E-COMMERCE. A instalação de software antivírus também é muito importante para você. Pergunte ao(s) seu(s) prestador(es) de serviços se foi feita a instalação de software antivírus em seu sistema (e com que frequência ele é atualizado). Certifique-se de que eles mantenham o software antivírus atualizado e verifique regularmente seu sistema em busca de malware.

Custo	
Facilidade	
Mitigação de riscos	



Verifique se há vulnerabilidades e corrija os problemas

Custo



Facilidade



Mitigação de riscos



Novas vulnerabilidades, brechas de segurança e bugs são descobertos todos os dias. É muito importante fazer com que seus sistemas que usam a internet sejam testados regularmente a fim de identificar esses novos riscos e tratá-los assim que possível. Seus sistemas que usam a Internet (como muitos sistemas de pagamento) são os mais vulneráveis porque podem ser facilmente explorados por criminosos, permitindo que se infiltrem em seus sistemas.

OBTENHA ACONSELHAMENTO. Pergunte ao seu banco comercial se ele possui parcerias com fornecedores de verificação aprovados pelo PCI, ou ASV (Fornecedor de Varredura Aprovado). Faça a mesma pergunta aos seus fornecedores e prestadores de serviços.

CONVERSE COM UM ASV DO PCI. Esses fornecedores podem ajudá-lo com ferramentas que identificam automaticamente vulnerabilidades e configurações inadequadas em seus sistemas de pagamento com internet, site de e-commerce e/ou redes e fornecem um relatório se, por exemplo, você precisar aplicar um patch. A lista do PCI Council (disponível à esquerda) pode ajudá-lo a encontrar um fornecedor de verificação.

SELECIONE UM PROGRAMA DE VARREDURA. Entre em contato com vários ASVs do PCI para encontrar um fornecedor que use um programa adequado para sua pequena empresa.

TRATE AS VULNERABILIDADES. Peça ao seu ASV, fornecedor de sistema de pagamento, prestador de serviços ou banco comercial ajuda para corrigir os problemas encontrados pela varredura.

Os fornecedores de verificação aprovados pelo PCI Council executam verificações de vulnerabilidade e relatórios externos. Consulte a [Lista de fornecedores de verificação aprovados pelo PCI](#)



Use terminais e soluções de pagamento seguros

Custo	
Facilidade	
Mitigação de riscos	

Uma maneira segura de proteger melhor sua empresa é usar soluções de pagamento seguras e profissionais treinados para ajudá-lo. Veja como escolher produtos seguros e certificar-se de que estejam configurados com segurança.

Para os terminais de pagamento do PCI e leitores de cartões seguros que criptografam os dados de cartões, consulte a [página 23](#).



USE TERMINAIS DE PAGAMENTO E DISPOSITIVOS DE DIGITAÇÃO DE PIN QUE SEJAM SEGUROS. O PCI Council aprova os terminais de pagamento que protegem dados de PIN. Certifique-se de que o terminal ou dispositivo de pagamento esteja na [Lista de dispositivos PTS aprovados pelo PCI](#) para equipamentos que oferecem a melhor segurança e suportam “chip EMV”.

USE SOFTWARE SEGURO. Certifique-se de que o software de pagamento esteja na [Lista de aplicativos de pagamento validados pelo PCI](#).

USE PROFISSIONAIS QUALIFICADOS. Certifique-se de que a pessoa que está instalando seu sistema de pagamento o faz de forma correta e segura. Faça sua escolha na [Lista de QIRs do PCI](#). Peça ao seu banco comercial para ajudá-lo a fazer a seleção.

USE PRESTADORES DE SERVIÇOS DE PAGAMENTO PARA E-COMMERCE SEGUROS. Se você ainda não tiver feito isso, considere usar um prestador de serviços de reclamações do PCI DSS para ajudá-lo a processar com segurança suas transações de pagamento de e-commerce e/ou gerenciar seu site de e-commerce.

PROCURE PRESTADORES DE SERVIÇOS EM CONFORMIDADE COM O PCI DSS. Certifique-se de que seu prestador de serviços de pagamento está em conformidade com o PCI DSS. Verifique as listas da Mastercard e da Visa para confirmar se ele está nas listas: Lista da MasterCard de prestadores de serviços em conformidade Registro global de prestadores de serviços da Visa Agentes registrados da Visa Europa

CONSULTE ESTA LISTA DE PERGUNTAS DO FORNECEDOR. Use as Perguntas que você deve fazer aos seus fornecedores para saber o que perguntar aos seus fornecedores e prestadores de serviços.

Seus clientes digitam os números de identificação pessoal (PINs) para seus cartões de pagamento em seu terminal de pagamento ou dispositivo de digitação de PIN. É importante usar dispositivos seguros para proteger os dados de PIN dos seus clientes.



Proteja sua empresa contra vulnerabilidades da Internet

Custo	
Facilidade	
Mitigação de riscos	

A Internet é a principal via utilizada pelos ladrões de dados para atacar e roubar os dados dos seus clientes. Por isso, se sua empresa está na Internet, qualquer coisa que você usa para pagamentos com cartão precisa de proteção extra.

Firewall é um equipamento ou software que fica entre seu sistema de pagamento e a internet. Ele atua como uma barreira para manter o tráfego fora de sua rede e dos sistemas que você não quer e não autorizou. Os firewalls são configurados (em hardware, software ou ambos) com critérios específicos para bloquear ou impedir acesso não autorizado a uma rede. Os firewalls são muitas vezes embutidos no roteador fornecido pelo seu provedor de internet.

ISOLE O USO. Não use o dispositivo ou o sistema com o qual você recebe pagamentos para nenhuma outra finalidade. Por exemplo, não navegue na internet nem acesse e-mails ou mídia social no mesmo dispositivo ou computador que você usa para transações de pagamento. Quando for necessário usar a Internet para negócios (por exemplo, atualizar a página na mídia social da sua empresa), use outro computador, e não seu dispositivo de pagamento.

PROTEJA SEU “TERMINAL VIRTUAL”. Se você inserir pagamentos de clientes por meio de um terminal virtual (uma página da Web que você acessa com um computador ou tablet), não conecte um leitor de cartão externo; isso minimiza seu risco.

PROTEJA O WI-FI. Se sua loja oferecer Wi-Fi gratuito para seus clientes, use outra rede para seu sistema de pagamento (isso é chamado de “segmentação de rede”). Peça que o instalador de rede ajude com a configuração segura do Wi-Fi.

USE UM FIREWALL. Um firewall configurado corretamente atua como um buffer para impedir que hackers e softwares mal-intencionados obtenham acesso a seus sistemas de pagamento, seu site de e-commerce e seus dados de cartão. Verifique com seu fornecedor de terminal de pagamento ou prestador de serviços se você tem um firewall e solicite ajuda para configurá-lo corretamente.

USE SOFTWARE FIREWALL PESSOAL OU EQUIVALENTE quando os sistemas de pagamento não estiverem protegidos por seu firewall corporativo (por exemplo, quando conectado a Wi-Fi público).

Para obter dicas simples sobre como configurar seu firewall, consulte Noções básicas de firewall do PCI



Para ter o máximo de proteção, torne seus dados inúteis para criminosos

Custo	
Facilidade	
Mitigação de riscos	

Seus dados ficam vulneráveis quando se deslocam para seu banco comercial e quando são mantidos ou armazenados em seus computadores e dispositivos. A melhor maneira de mantê-los seguros é inutilizá-los, mesmo que sejam roubados, criptografando-os sempre que você os armazenar ou enviar, e removendo-os completamente quando não forem mais necessários. Embora isso possa ser mais complexo de ser implementado, em longo prazo, pode facilitar muito o gerenciamento da segurança.

O que é tokenização?
Consulte a [página 13](#) para obter uma explicação.

TRABALHE COM O FORNECEDOR DE PAGAMENTO OU PRESTADOR DE SERVIÇOS. Você deve criptografar todos os dados de cartão armazenados ou enviados. Certifique-se de que seu sistema de pagamento esteja usando tecnologia de criptografia e/ou tokenização. Se não tiver certeza, pergunte.

USE DISPOSITIVOS PCI QUE CRIPTOGRAFEM OS DADOS DOS CARTÕES. O PCI Council aprova os terminais de pagamento que protegem dados de PIN e terminais de pagamento e “protegem leitores de cartões” que criptografam ainda mais os dados. Consulte a [Lista de dispositivos PTS aprovados pelo PCI](#).



CONSULTE
PÁGINA 21

USE SOLUÇÕES DE CRIPTOGRAFIA SEGURAS DO PCI. Pergunte se a criptografia do seu terminal de pagamento é feita por uma solução de criptografia de ponto a ponto que está na [Lista de soluções validadas pelo PCI P2PE do PCI Council](#).

VOCÊ É UM COMERCIANTE QUE ESTÁ MUDANDO AGORA PARA TERMINAIS COM CHIP EMV? É uma ótima oportunidade para fazer um investimento em um terminal que suporte EMV e também ofereça a segurança adicional de criptografia e tokenização.

ATUALIZE SUA SOLUÇÃO. Reduza seu risco: considere obter um novo terminal de pagamento que use tecnologia de criptografia e de tokenização para remover o valor dos dados do cartão para hackers.

PERGUNTE. Consulte Perguntas que você deve fazer aos seus fornecedores para obter ajuda em relação a perguntas que você deve fazer a seu fornecedor ou prestador de serviços.

Leitores de cartões seguros e terminais de pagamento aprovados pelo PCI que criptografam os dados dos cartões fazem isso usando uma tecnologia chamada “Leitura e troca segura de dados” (SRED, Secure Reading and Exchange of Data). Pergunte a seu fornecedor se seu terminal de pagamento criptografa os dados de cartão com SRED.

Os sites de e-commerce devem criptografar os dados de cartão enviados pela internet, por exemplo, usando algo chamado “Segurança de camada de transporte” (TLS). Pergunte ao seu prestador de serviços como ele criptografa seus dados de cartão.



ONDE OBTER AJUDA

Recursos

Listagens do PCI Council

Recurso	URL
Lista de aplicativos de pagamento validados	https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement
Lista de dispositivos PTS aprovados	https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
Lista de fornecedores de verificação aprovados	https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
Lista de integradores/revendedores qualificados	https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers
Lista de soluções validadas P2PE	https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

Listas de bandeiras de pagamento

Recurso	URL
Listas de prestadores de serviços em conformidade	Lista da MasterCard de prestadores de serviços em conformidade https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html
	Registro global de prestadores de serviços Visa http://www.visa.com/splisting/
	Agentes de comerciantes registrados da Visa Europa https://www.visaeurope.com/receiving-payments/security/downloads-and-resources

PCI DSS e orientação relacionada

Recurso	URL
Mais informações sobre o PCI DSS	https://www.pcisecuritystandards.org/pci_security/how
Questionários de autoavaliação do PCI DSS	https://www.pcisecuritystandards.org/pci_security/completing_self_assessment
Guia: Prevenção contra clonagem: Visão geral das melhores práticas para comerciantes	https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf

Recursos

Infográficos e vídeos

Recurso	URL
Infográfico: It's Time to Change Your Password (É hora de alterar sua senha)	https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf
Infográfico: Fight Cybercrime by Making Stolen Data Worthless to Thieves (Combater o crime cibernético, deixando os dados roubados sem valor para os ladrões)	https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf
Vídeo: Domine segurança para senhas em 2 minutos	https://www.youtube.com/watch?v=FsRoxqZKa7U
Vídeo: Senhas	https://www.youtube.com/watch?v=dNVQk65KL8g
Infográfico: Senhas	https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Strong-Passwords.pdf
Vídeo: Patches	https://www.youtube.com/watch?v=0NGz1mGO3Jg
Infográfico: Patches	https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Patching.pdf
Vídeo: Acesso remoto	https://www.youtube.com/watch?v=MxgSNFqvAVc
Infográfico: Acesso remoto	https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Secure-Remote-Access.pdf

Fundamentos da segurança de dados para pequenos comerciantes do PCI e respectivas orientações

Recurso	URL
Sistemas comuns de pagamento	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Pequenos comerciantes - Perguntas para fornecedores	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf
Glossário para pequenos comerciantes	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_SecurityTerms.pdf
Infográfico: Noções básicas de firewall do PCI	https://www.pcisecuritystandards.org/pdfs/Small-Merchant-Firewall-Basics.pdf
Ferramenta de avaliação: Visão geral do adquirente	https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Acquirers.pdf
Ferramenta de avaliação: Visão geral do pequeno comerciante	https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Small-Merchants.pdf

Fontes e referências úteis

Dept. de Mídia, Cultura e Esporte – *Pesquisa sobre violações de segurança cibernética 2017*

Instituto Ponemon – *Estado da segurança cibernética em 2016 nas pequenas e médias empresas*
(Patrocinado pela Keeper Security), junho de 2016

Centro Nacional de Segurança Cibernética – *Guia de segurança cibernética para pequenas empresas*, 2017

Beaming UK – *Violações de segurança cibernética custam às empresas britânicas quase 30 bilhões de libras em 2016, março de 2017*

Verizon 2017 – *Relatório de investigações sobre violações de dados da Verizon*

Sobre o PCI Security Standards Council

O [Conselho dos Padrões de Segurança PCI](https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Partnering_for_Global_Payment_Security.pdf) é um fórum global de união do setor para desenvolver, melhorar, disseminar e auxiliar na compreensão dos padrões de segurança para a segurança de contas de pagamento. Leia mais sobre a Iniciativa global de envolvimento em segurança de pagamentos do PCI SSC em www.pcisecuritystandards.org/pdfs/PCI_SSC_Partnering_for_Global_Payment_Security.pdf

O PCI Council mantém, desenvolve e promove os padrões de segurança da Indústria de cartão de pagamento. Ele também fornece as ferramentas essenciais necessárias para a implementação dos padrões, como qualificações de avaliação e de verificação, questionários de autoavaliação, treinamentos e programas de certificação de produtos.

Os membros fundadores do Conselho, American Express, Discover, Financial Services, JCB International, MasterCard e Visa Inc., concordaram em incorporar o Padrão de Segurança de Dados do PCI (PCI DSS) como parte dos requisitos técnicos para cada um dos seus programas de conformidade de segurança de dados. Cada membro fundador também reconhece os avaliadores de segurança qualificados e os fornecedores de varredura aprovados qualificados pelo Conselho dos Padrões de Segurança PCI.

As bandeiras de pagamento, juntamente com os membros estratégicos, compartilham igualmente a governança do PCI Council, têm participação igualitária no Conselho dos Padrões de Segurança PCI e compartilham a responsabilidade pela realização do trabalho da organização. Outras partes interessadas da indústria são incentivadas a aderir ao PCI Council como membros estratégicos ou afiliados e organizações participantes para revisar adições ou modificações propostas aos padrões. Dentre as organizações participantes estão comerciantes, bancos, processadores, desenvolvedores de hardware e de software e fornecedores de pontos de venda.

Este guia fornece informações suplementares, que não substituem nem prevalecem sobre os Padrões de Segurança do PCI SSC ou seus documentos de apoio.

FUNDADORES DO PCI SSC



ORGANIZAÇÕES PARTICIPANTES

Comerciantes, bancos, processadores, desenvolvedores de hardware e de software e fornecedores de pontos de venda