

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

Sistemas comuns de pagamento

Versão 2.0 | Agosto de 2018



Tipos de sistema de pagamento e como protegê-los



TIPOS DE SISTEMA DE PAGAMENTO

Para proteger o seu negócio contra roubo de dados de pagamento, primeiro você precisa entender como você recebe pagamentos em sua loja. Que tipo de equipamento você usa, quem são seus parceiros fornecedores de tecnologia e bancos? Como todos esses elementos se encaixam?

Use esses recursos visuais reais para identificar o tipo de sistema de pagamento que você usa, os tipos de riscos associados ao seu sistema e os passos de segurança que você pode usar para protegê-lo.

Como você usa este recurso?

IDENTIFIQUE QUAL IMAGEM MAIS REPRESENTA O SEU SISTEMA DE PAGAMENTO:

- Este guia, destinado a complementar o [Guia para pagamentos seguros](#), mostra vários diagramas de sistemas comuns de pagamento, começando pelo mais simples e avançando até o mais complexo.
- Cada diagrama do sistema de pagamento inclui quatro visualizações:
 - 1) Visão geral
 - 2) Riscos - onde os dados de cartão estão expostos
 - 3) Ameaças - como os criminosos podem obter os dados de cartões
 - 4) Proteções - maneiras recomendadas de proteger os dados do cartão.
- Encontre o diagrama que representa o seu sistema.

ENTENDA SEUS RISCOS E AMEAÇAS:

- Depois de encontrar as visualizações do sistema de pagamento que mais se aproximam das suas, reveja os dois diagramas a seguir para ver onde os dados de cartões estão em risco para a sua empresa e as formas como sua empresa está vulnerável a ataques.

PROTEJA OS DADOS DE CARTÕES E SUA EMPRESA COM PRINCÍPIOS BÁSICOS DE SEGURANÇA:

- Por último, reveja a quarta visualização do seu tipo de sistema de pagamento, que inclui recomendações básicas de segurança para ajudá-lo a proteger sua empresa.
- Esta visualização inclui links para as recomendações nas áreas do [Guia para pagamentos seguros](#) para ajudá-lo neste processo.
- Consulte também [Perguntas que você deve fazer aos seus fornecedores](#) e o [Glossário de termos de segurança da informação e pagamentos](#).

FAÇA A AVALIAÇÃO DOS FUNDAMENTOS DE SEGURANÇA DE DADOS CASO SEJA INSTRUÍDO POR SEU ADQUIRENTE/MARCA

Opcionalmente, apenas para informações do comerciante, você pode optar por usar este recurso ou [Ferramenta de avaliação dos Fundamentos da segurança de dados](#) para obter percepções sobre as práticas de segurança referentes a sua forma de aceitar pagamentos. Para usar esse recurso, basta:

- Abrir a [Visão geral dos tipos de sistema de pagamento](#)
- Encontrar o diagrama do sistema de pagamento que mais combina com a forma como você aceita pagamentos
- A partir desse diagrama, clique no botão da **Caixa azul** para baixar o Formulário de avaliação
- Apresente suas respostas
- Revise seus resultados
- Imprima ou salve o PDF dos resultados para uso futuro

Observe que esses são resultados preliminares. *Você não consegue enviar a avaliação no site do PCI SSC nem o PCI SSC pode enviá-la em seu nome. Você deve entrar em contato com seu banco comercial e seguir as instruções para o envio.*

O que significam esses

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) que 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 imprime recibos.



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 cartão ou processador de pagamento também são termos para esta 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.

Terminais de pagamento que fazem parte de uma solução

Os P2PE listada pelo PCI oferece aos comerciantes a melhor garantia de qualidade de 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 listado pela PCI deve ser discutida com seu fornecedor.



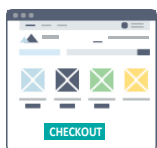
A Um **SISTEMA DE PAGAMENTO** inclui todo o processo para aceitar pagamentos de cartão. Também chamado de ambiente de dados de titular de cartão (CDE, cardholder data environment), seu sistema de pagamento pode incluir um terminal de pagamento, uma caixa registradora eletrônica, outros dispositivos ou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

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.



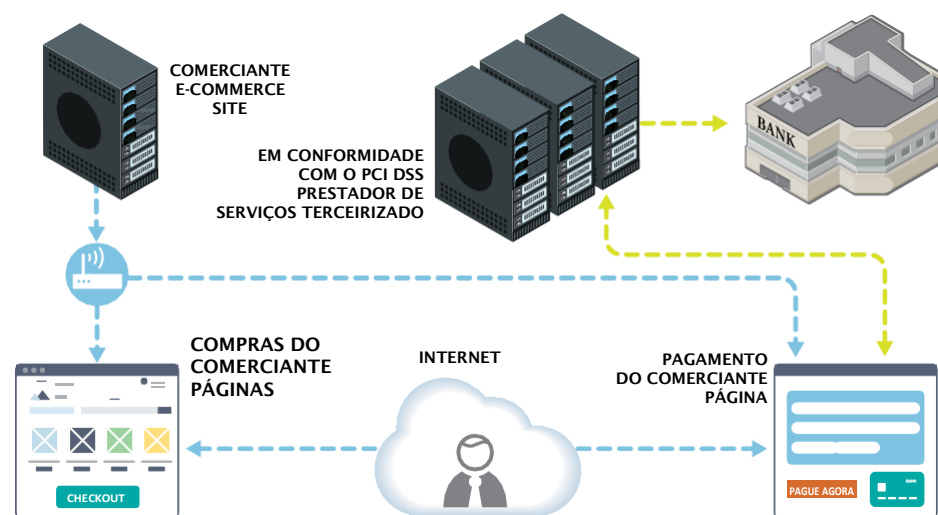
Um **SITE DE E-COMMERCE** armazena e apresenta seu site comercial e suas páginas de compras aos seus clientes. O site pode ser hospedado e gerenciado por você ou por um provedor de hospedagem terceirizado.



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 do 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 e por 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.

Visão geral dos tipos de sistema de pagamento

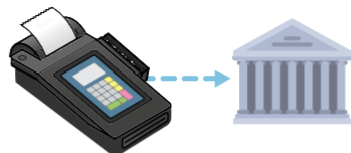
Como você aceita pagamentos?

Revise todos os diagramas de pagamento que se aplicam à forma como seu negócio aceita pagamentos



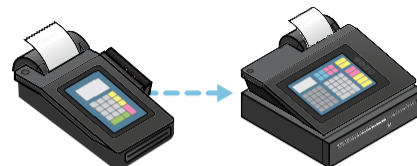
Você aceita pagamentos com um terminal de pagamento por discagem telefônica independente

TIPOS 1, 2



Você aceita pagamentos com um dispositivo de pagamento conectado apenas a um processador

TIPOS 3, 4



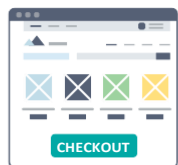
Você aceita pagamentos com um terminal de pagamento conectado a uma gaveta ou caixa registradora eletrônica, e a caixa registradora eletrônica/gaveta fica conectada apenas a um processador

TIPO 5



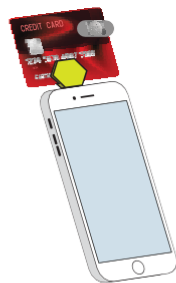
Você aceita pagamentos com um terminal de pagamento conectado a outros sistemas (por exemplo, servidores) em sua rede

TIPOS 6, 7, 8



Você aceita pagamentos via e-commerce

TIPOS 9, 10, 11



Você aceita pagamentos por meio de um SCR (leitor de cartão seguro) listado pelo PCI conectado a um dispositivo móvel

TIPOS 12, 13



Você aceita pagamentos por meio de um terminal virtual

TIPO 14



Você aceita pagamentos por meio de uma solução P2PE listada pelo PCI

TIPO 15

Terminal de pagamento discado. Pagamentos enviados via linha telefônica.



TIPO 1 - VISÃO GERAL

TIPO 1 - RISCOS

TIPO 1 - AMEAÇAS

TIPO 1 - PROTEÇÕES

SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente



Para este cenário, os riscos para os dados de cartões estão presentes em ! acima. Riscos explicados na próxima página.

Terminal de pagamento discado. Pagamentos enviados via linha telefônica.



Onde os dados de cartão estão em risco?



Terminal de pagamento discado. Pagamentos enviados via linha telefônica.



Como os criminosos obtêm os dados de cartão?

Eles roubam recibos ou relatórios em papel que não são protegidos, que são mantidos quando não são mais necessários ou que não são descartados de maneira segura.

Eles roubam dados de cartões por meio de um equipamento de “clonagem” que eles conectam (ou incorporam) ao seu terminal de pagamento.

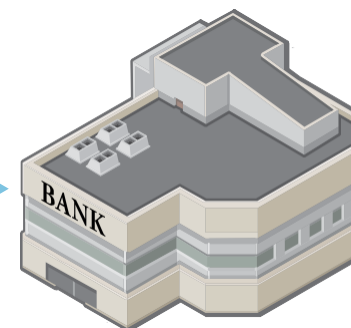
Também podem roubar seu terminal, substituindo-o por um terminal modificado usado para obter dados de cartões.

TERMINAL DE
PAGAMENTO DISCADO



123423487340
981230630736
034603740987
382929293846
262910304826
454900926344
153784

LINHA TELEFÔNICA



Terminal de pagamento discado. Pagamentos enviados via linha telefônica.



Como você pode começar a proteger dados de cartões hoje mesmo?*



Proteja os dados de cartões e armazene apenas o necessário



Inspecione seus terminais de pagamento para ver se há danos ou mudanças



Peça ajuda aos seus parceiros fornecedores, se precisar



Limite o acesso interno aos dados de cartão

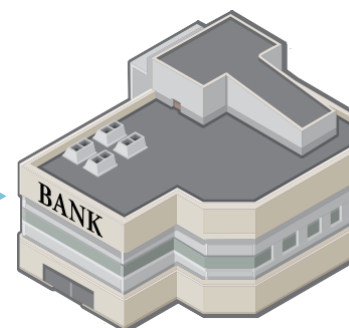
TERMINAL DE
PAGAMENTO DISCADO



123423487340
981230630736
034603740987
382929293846
262910304826
454900926344
153784

TERMINAL

LINHA TELEFÔNICA



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

Terminal de pagamento discado e caixa registradora eletrônica conectada à Internet. Pagamentos enviados via linha telefônica.

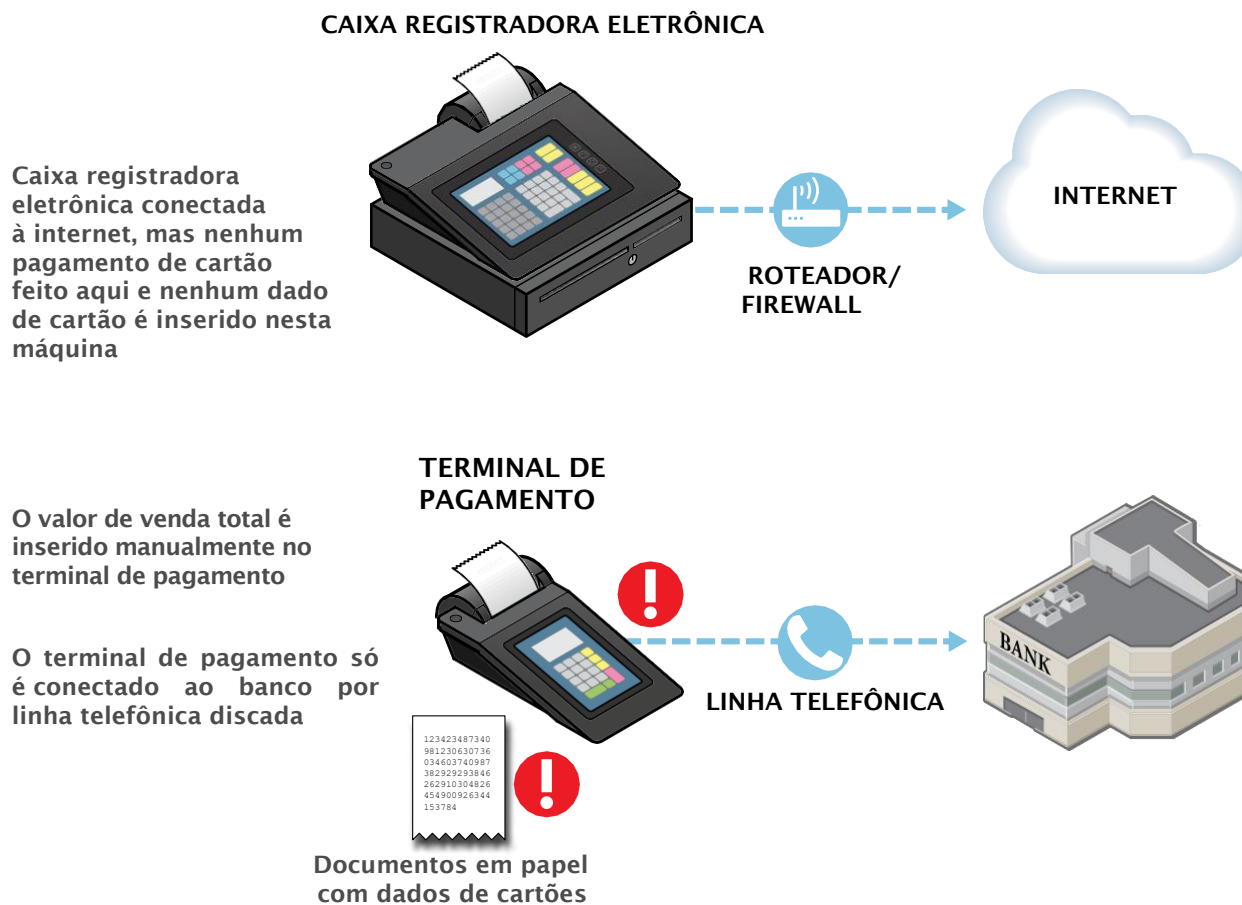


TIPO 2 - VISÃO GERAL

TIPO 2 - RISCOS

TIPO 2 - AMEAÇAS

TIPO 2 - PROTEÇÕES

**SIM**

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

Para este cenário, os riscos para os dados de cartões estão presentes em ! acima. Riscos explicados na próxima página.

Terminal de pagamento discado e caixa registradora eletrônica conectada à Internet. Pagamentos enviados via linha telefônica.



Onde os dados de cartão estão em risco?



Terminal de pagamento discado e caixa registradora eletrônica conectada à Internet. Pagamentos enviados via linha telefônica.



Como os criminosos obtêm os dados de cartão?



Terminal de pagamento discado e caixa registradora eletrônica conectada à Internet. Pagamentos enviados via linha telefônica.



TIPO 2 - VISÃO GERAL

TIPO 2 - RISCOS

TIPO 2 - AMEAÇAS

TIPO 2 - PROTEÇÕES

Como você pode começar a proteger dados de cartões hoje mesmo?*



Proteja os dados do seu cartão e armazene apenas o necessário



Inspeção seus terminais de pagamento para ver se há danos ou mudanças

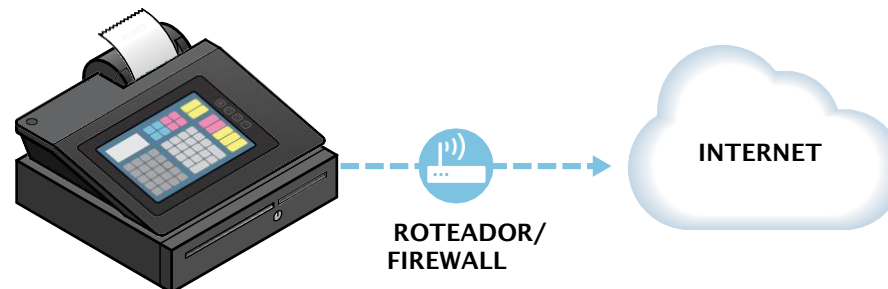


Peça ajuda aos seus parceiros fornecedores, se precisar

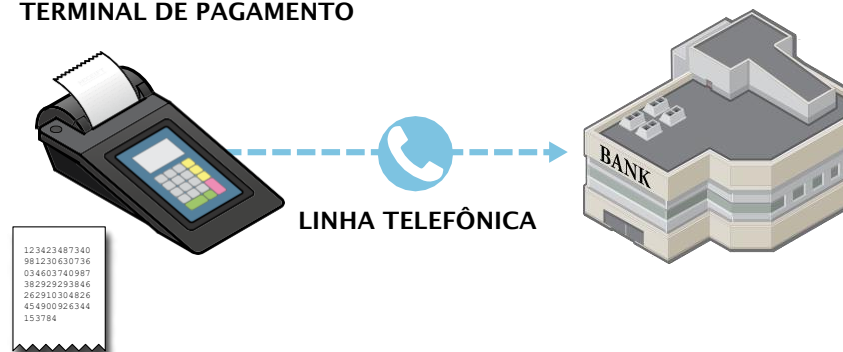


Proteja o acesso interno aos dados de cartão

CAIXA REGISTRADORA ELETRÔNICA



TERMINAL DE PAGAMENTO



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

Terminal de pagamento e caixa registradora eletrônica conectados separadamente à Internet. Pagamentos enviados via Internet por terminal de pagamento.

Os dados do cartão estão criptografados?



SIM



NÃO

TIPO 3 - VISÃO GERAL

TIPO 3 - RISCOS

TIPO 3 - AMEAÇAS

TIPO 3 - PROTEÇÕES

Se você estiver usando uma solução de criptografia ponto a ponto (P2PE) listada pelo PCI, vá para o [Tipo 15](#).

Nenhum outro equipamento conectado aos sistemas de pagamento do comerciante

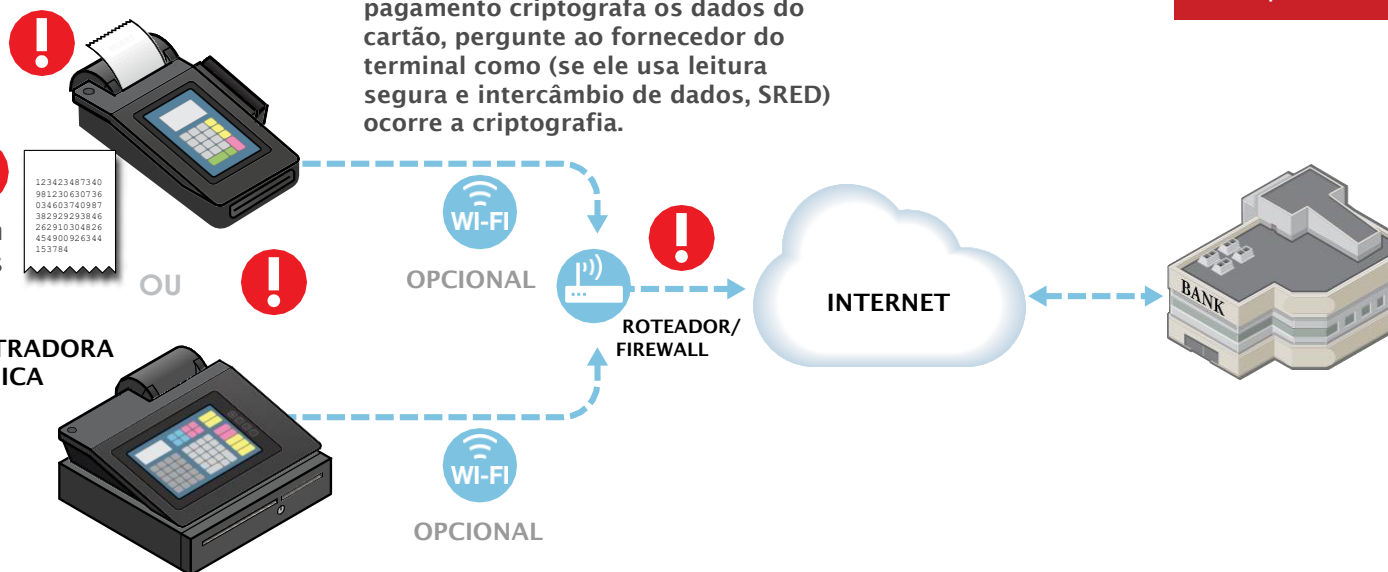
TERMINAL DE PAGAMENTO

A criptografia de dados do cartão reduz seu risco. Se seu terminal de pagamento criptografa os dados do cartão, pergunte ao fornecedor do terminal como (se ele usa leitura segura e intercâmbio de dados, SRED) ocorre a criptografia.

Documentos em papel com dados de cartões

CAIXA REGISTRADORA ELETRÔNICA

Pode haver uma caixa registradora eletrônica. Por exemplo, quando o valor de venda total da caixa registradora eletrônica é inserido manualmente no terminal de pagamento; nenhum pagamento com cartão é aceito na caixa registradora eletrônica



SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

Para este cenário, os riscos para os dados de cartões estão presentes em acima. Riscos explicados na próxima página.

Terminal de pagamento e caixa registradora eletrônica conectados separadamente à Internet. Pagamentos enviados via Internet por terminal de pagamento.



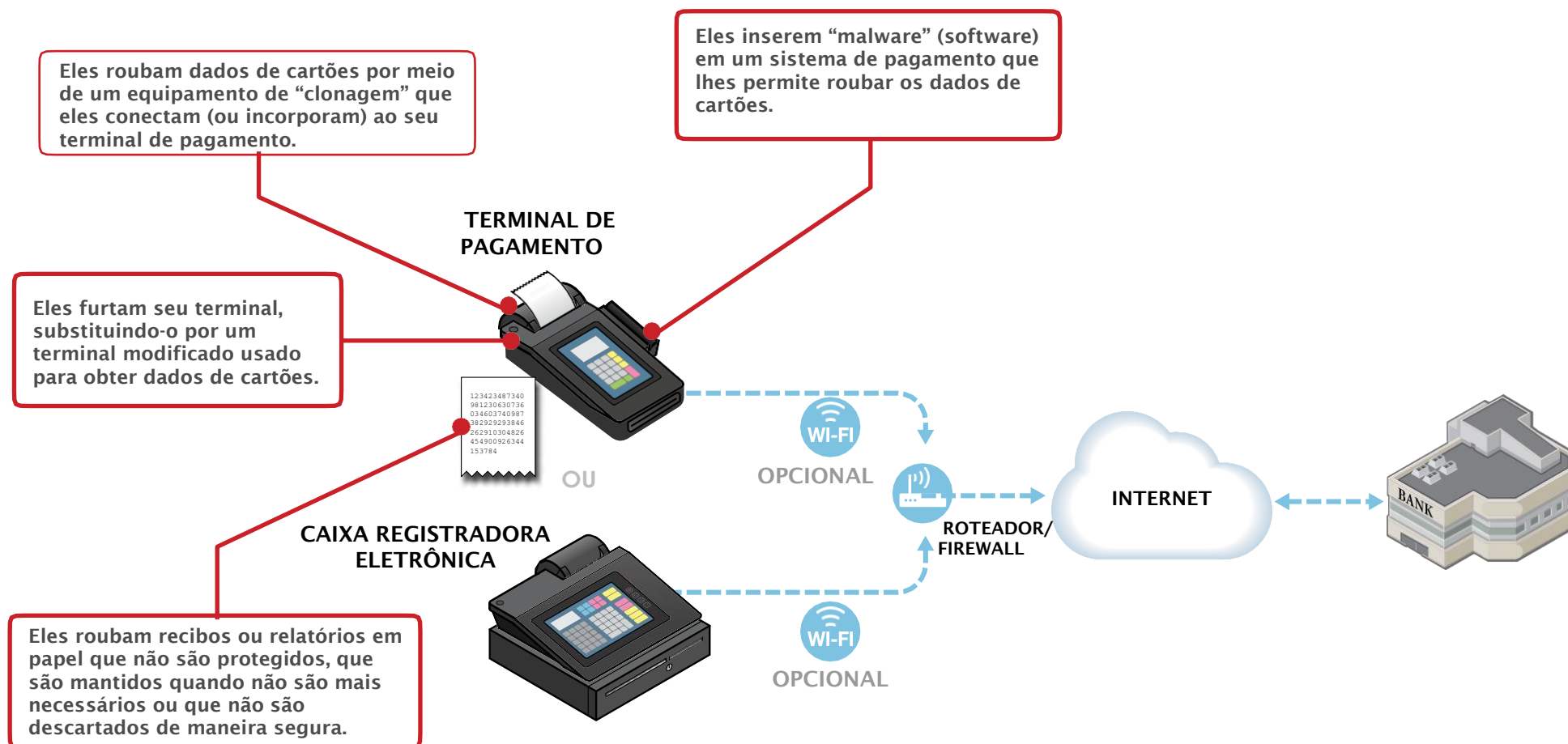
Onde os dados de cartão estão em risco?



Terminal de pagamento e caixa registradora eletrônica conectados separadamente à Internet. Pagamentos enviados via Internet por terminal de pagamento.



Como os criminosos obtêm os dados de cartão?



Terminal de pagamento e caixa registradora eletrônica conectados separadamente à Internet. Pagamentos enviados via Internet por terminal de pagamento.



SIM



NÃO

TIPO 3 - VISÃO GERAL

TIPO 3 - RISCOS

TIPO 3 - AMEAÇAS

TIPO 3 - PROTEÇÕES

Como você pode começar a proteger dados de cartões hoje mesmo?*



Use senhas fortes



Proteja os dados de cartões e armazene apenas o necessário



Inspecione seus terminais de pagamento para ver se há danos ou mudanças



Instale os patches de seu fornecedor de terminal de pagamento



Peça ajuda aos seus parceiros fornecedores, se precisar



Proteja o acesso interno aos dados de cartão



Limite o acesso remoto aos seus parceiros fornecedores: não permita que os hackers tenham acesso fácil



Faça varreduras regulares de vulnerabilidade



Use sistemas de pagamento seguro



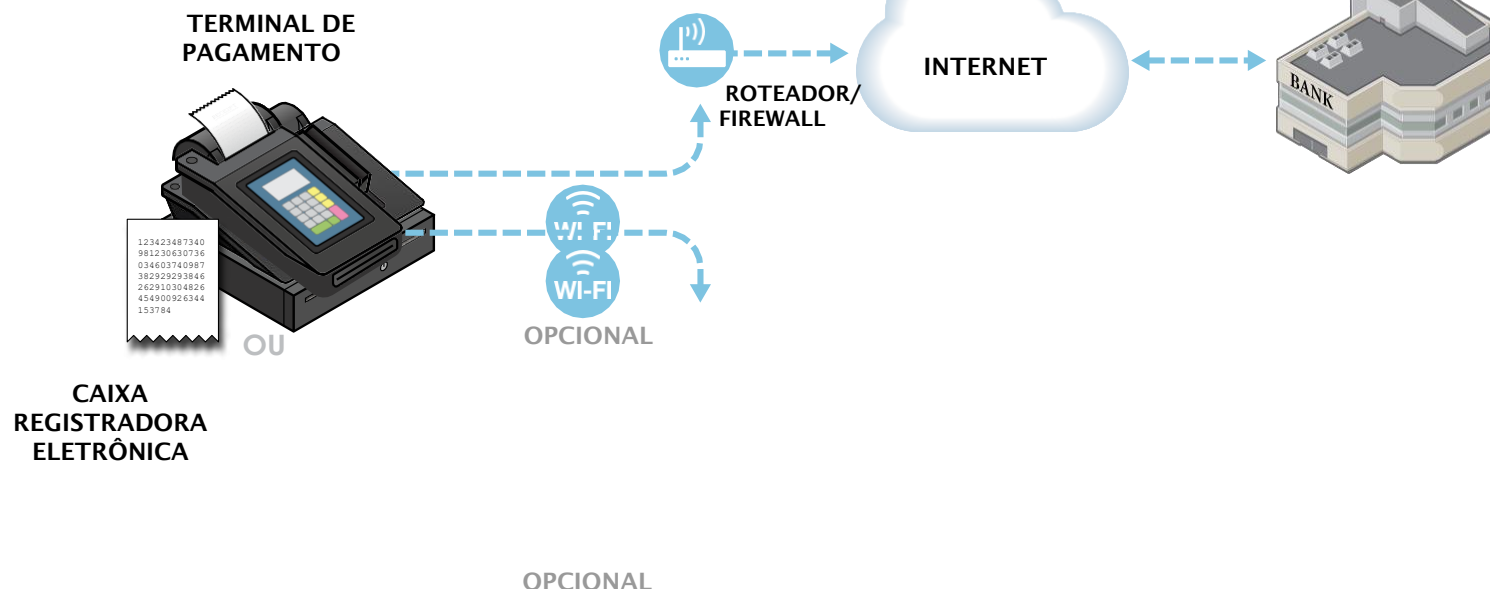
Proteja sua empresa contra vulnerabilidades da Internet



Use software antivírus



Torne os dados do seu cartão inúteis para criminosos



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

TIPO 4

A caixa registradora eletrônica e o terminal de pagamento compartilham dados que não são do cartão. Pagamento enviado via Internet por terminal de pagamento.

PERFIL DE RISCO

Os dados do cartão estão criptografados?



SIM



NÃO

TIPO 4 - VISÃO GERAL

TIPO 4 - RISCOS

TIPO 4 - AMEAÇAS

TIPO 4 - PROTEÇÕES

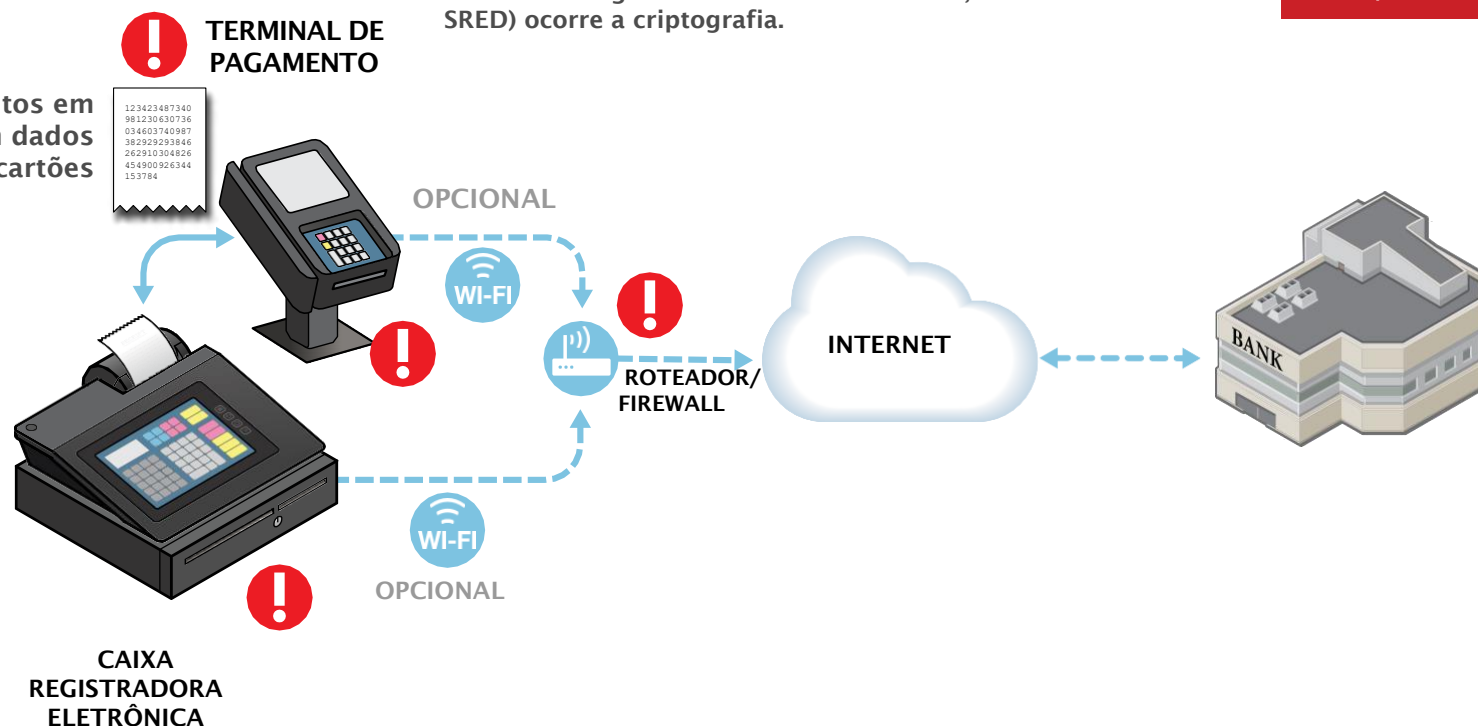
Se você estiver usando uma solução de criptografia ponto a ponto (P2PE) listada pelo PCI, vá para o [Tipo 15](#).

Nenhum outro equipamento conectado a sistemas de pagamento de comerciante, a menos que você tenha um dispositivo de entrada de PIN separado

O terminal de pagamento aceita pagamentos com cartão com base no valor total da venda recebido da caixa registradora eletrônica. Nenhum pagamento de cartão aceito na caixa registradora eletrônica.

Nenhum dado do cartão é compartilhado entre a caixa registradora eletrônica e o terminal de pagamento

A criptografia de dados de cartão reduz seu risco. Se seu terminal de pagamento criptografa os dados de cartão, pergunte ao fornecedor do terminal como (se ele usa leitura segura e intercâmbio de dados, SRED) ocorre a criptografia.



SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

Para este cenário, os riscos para os dados de cartões estão presentes em ! acima. Riscos explicados na próxima página.



SIM



NÃO

Onde os dados de cartão estão em risco?



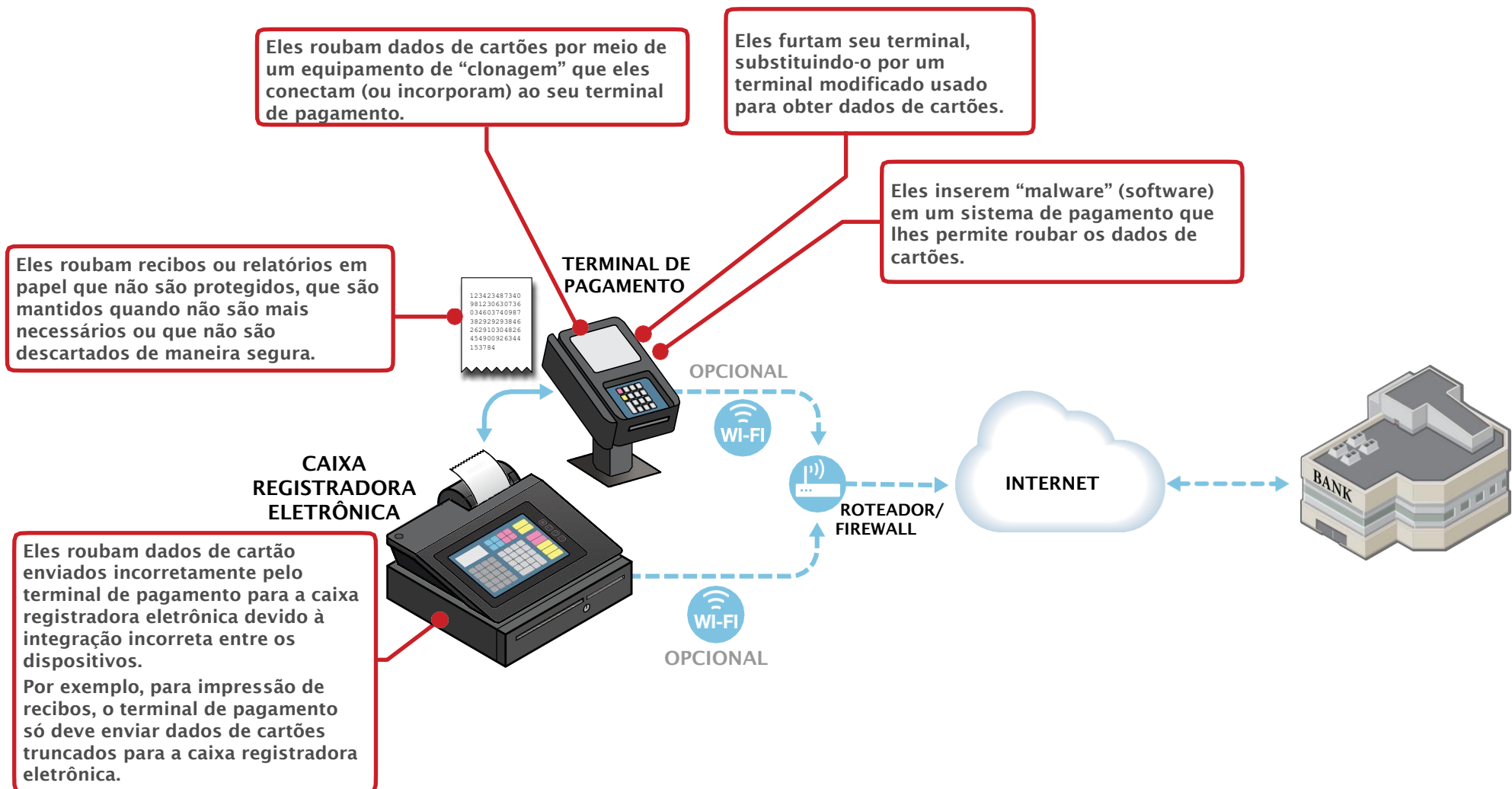


SIM



NÃO

Como os criminosos obtêm os dados de cartão?



A caixa registradora eletrônica e o terminal de pagamento compartilham dados que não são do cartão. Pagamento enviado via Internet por terminal de pagamento.

PERFIL DE RISCO

Os dados do cartão estão criptografados?



SIM



NÃO

TIPO 4 - VISÃO GERAL

TIPO 4 - RISCOS

TIPO 4 - AMEAÇAS

TIPO 4 - PROTEÇÕES

Como você pode começar a proteger dados de cartões hoje mesmo?*



Use senhas fortes



Proteja os dados de cartões e armazene apenas o necessário



Inspeção seus terminais de pagamento para ver se há danos ou mudanças



Instale os patches de seu fornecedor de terminal de pagamento



Peça ajuda aos seus parceiros fornecedores, se precisar



Proteja o acesso interno aos dados de cartão



Limite o acesso remoto aos seus parceiros fornecedores: não permita que os hackers tenham acesso fácil



Faça varreduras regulares de vulnerabilidade



Use sistemas de pagamento seguro



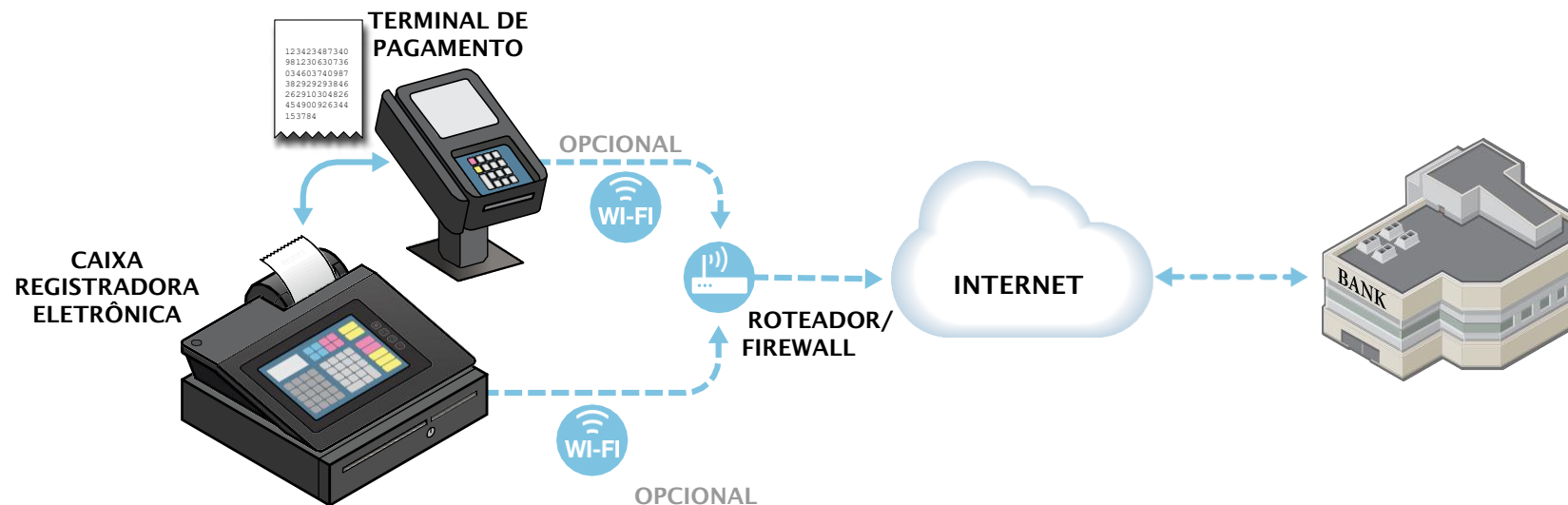
Proteja sua empresa contra vulnerabilidades da Internet



Use software antivírus



Torne os dados do seu cartão inúteis para criminosos



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

Terminal de pagamento conectado a caixa registradora eletrônica. Pagamentos enviados via Internet por caixa registradora eletrônica.



SIM



NÃO

TIPO 5 - VISÃO GERAL

TIPO 5 - RISCOS

TIPO 5 - AMEAÇAS

TIPO 5 - PROTEÇÕES

Se você estiver usando uma solução de criptografia ponto a ponto (P2PE) listada pelo PCI, vá para o [Tipo 15](#).

SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

TERMINAL DE PAGAMENTO

CAIXA REGISTRADORA ELETRÔNICA

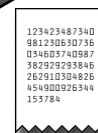
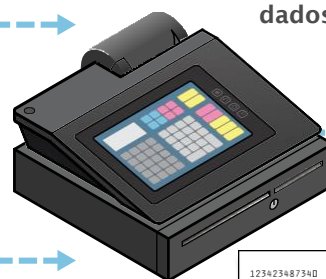
A caixa registradora eletrônica não aceita cartões, mas é usada para enviar dados de cartão para processamento.

A criptografia de dados de cartão reduz seu risco. Se seu terminal de pagamento criptografa os dados de cartão, pergunte ao fornecedor do terminal como (se ele usa leitura segura e intercâmbio de dados, SRED) ocorre a criptografia.

Nenhum outro equipamento conectado aos sistemas de pagamento do comerciante



OU

WI-FI
OPCIONALWI-FI
OPCIONALROTEADOR/
FIREWALL

Documentos em papel com dados de cartões

INTERNET



Dados de cartões enviados para caixa registradora eletrônica

Para este cenário, os riscos para os dados de cartões estão presentes em acima. Riscos explicados na próxima página.

Terminal de pagamento conectado a caixa registradora eletrônica. Pagamentos enviados via Internet por caixa registradora eletrônica.



Onde os dados de cartão estão em risco?



Terminal de pagamento conectado a caixa registradora eletrônica. Pagamentos enviados via Internet por caixa registradora eletrônica.



SIM



NÃO

TIPO 5 - VISÃO GERAL

TIPO 5 - RISCOS

TIPO 5 - AMEAÇAS

TIPO 5 - PROTEÇÕES

Como os criminosos obtêm os dados de cartão?

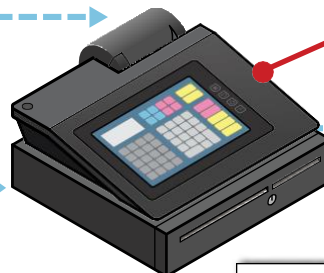
Eles roubam dados de cartões por meio de um equipamento de “clonagem” que eles conectam (ou incorporam) ao seu terminal de pagamento.

TERMINAL DE PAGAMENTO

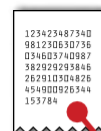


Também podem roubar seu terminal, substituindo-o por um terminal modificado usado para obter dados de cartões.

CAIXA REGISTRADORA ELETRÔNICA



Eles roubam os dados do cartão acessando sua caixa registradora eletrônica, por exemplo, instalando um malware (software) que permite isso.

WI-FI
OPCIONALWI-FI
OPCIONALROTEADOR/
FIREWALL

Eles roubam recibos ou relatórios em papel que não são protegidos, que são mantidos quando não são mais necessários ou que não são descartados de maneira segura.

INTERNET



Terminal de pagamento conectado a caixa registradora eletrônica. Pagamentos enviados via Internet por caixa registradora eletrônica.



SIM



NÃO

TIPO 5 - VISÃO GERAL

TIPO 5 - RISCOS

TIPO 5 - AMEAÇAS

TIPO 5 - PROTEÇÕES

Como você pode começar a proteger dados de cartões hoje mesmo?*



Use senhas fortes



Proteja os dados de cartões e armazene apenas o necessário



Inspeção seus terminais de pagamento para ver se há danos ou mudanças



Instale os patches de seu fornecedor de terminal de pagamento



Peça ajuda aos seus parceiros fornecedores, precisar



Proteja o acesso interno aos dados de cartão



Limite o acesso remoto aos seus parceiros fornecedores: não permita que os hackers tenham acesso fácil



Faça varreduras regulares de vulnerabilidade



Use sistemas de pagam seguro



Proteja sua empresa contra vulnerabilidades da Internet



Use software antivírus



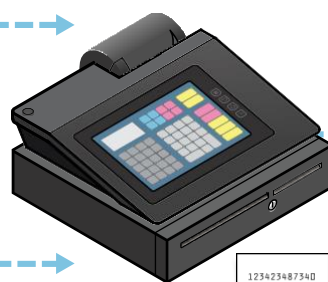
Torne os dados do seu cartão inúteis para criminosos

TERMINAL DE PAGAMENTO

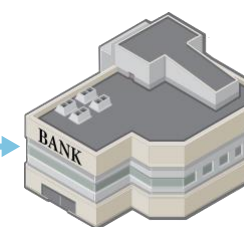
CAIXA REGISTRADORA ELETRÔNICA



OU

WI-FI
OPCIONALWI-FI
OPCIONALROTEADOR/
FIREWALL

INTERNET



1234567890
9876543210
0123456789
9876543210
0123456789
9876543210
0123456789
9876543210
0123456789
9876543210

*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

Terminal de pagamento integrado e middleware de pagamento compartilham dados de cartões. Pagamentos enviados via Internet.



SIM



NÃO

TIPO 6 - VISÃO GERAL

TIPO 6 - RISCOS

TIPO 6 - AMEAÇAS

TIPO 6 - PROTEÇÕES

Se você estiver usando uma solução de criptografia ponto a ponto (P2PE) listada pelo PCI, vá para o [Tipo 15](#).

SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

Terminal de pagamento e caixa registradora eletrônica combinados

O cartão é roubado por um membro da equipe; não é aplicável para cartões com chip

Nenhum dispositivo de entrada de PIN separado

Nenhum outro equipamento conectado ao sistema de pagamento do comerciante

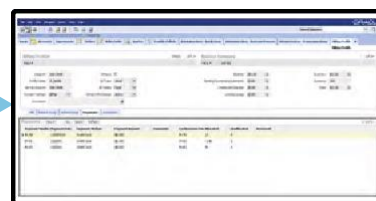
TERMINAL DE PAGAMENTO INTEGRADO



O terminal de pagamento compartilha os dados do cartão com o middleware de pagamento

A criptografia de dados de cartão reduz seu risco. Se seu terminal de pagamento criptografa os dados de cartão, pergunte ao fornecedor do terminal como (se ele usa leitura segura e intercâmbio de dados, SRED) ocorre a criptografia.

MIDDLEWARE DE PAGAMENTO




Software usado como parte da transação de pagamento

ROTEADOR/FIREWALL



INTERNET



Para este cenário, os riscos para os dados de cartões estão presentes em  acima. Riscos explicados na próxima página.

Terminal de pagamento integrado e middleware de pagamento compartilham dados de cartões. Pagamentos enviados via Internet.



SIM



NÃO

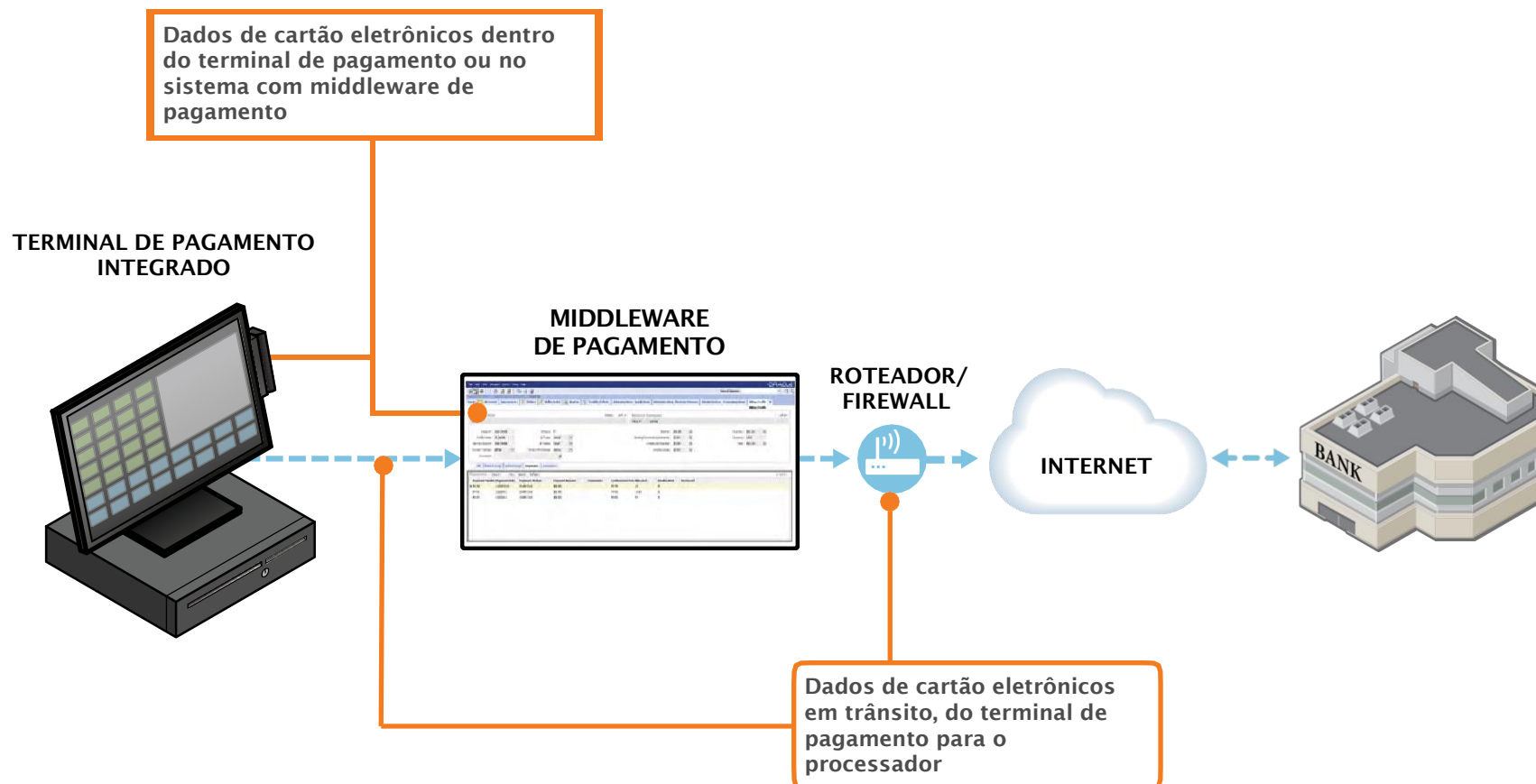
TIPO 6 - VISÃO GERAL

TIPO 6 - RISCOS

TIPO 6 - AMEAÇAS

TIPO 6 - PROTEÇÕES

Onde os dados de cartão estão em risco?



Terminal de pagamento integrado e middleware de pagamento compartilham dados de cartões. Pagamentos enviados via Internet.



SIM



NÃO

TIPO 6 - VISÃO GERAL

TIPO 6 - RISCOS

TIPO 6 - AMEAÇAS

TIPO 6 - PROTEÇÕES

Como os criminosos obtêm os dados de cartão?

Eles roubam dados de cartões por meio de um equipamento de “clonagem” que eles conectam (ou incorporam) ao seu terminal de pagamento.

Eles inserem “malware” (software) em um sistema de pagamento que lhes permite roubar os dados de cartões.

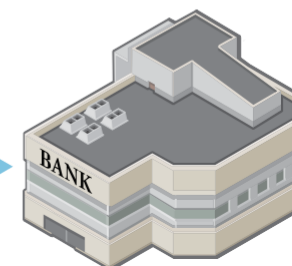
Eles acessam e roubam os dados do cartão do cliente por meio do mesmo software de “acesso remoto” usado por seu fornecedor para oferecer suporte aos seus sistemas de pagamento.

TERMINAL DE PAGAMENTO INTEGRADO

MIDDLEWARE DE PAGAMENTO

ROTEADOR/FIREWALL

INTERNET



Eles furtam seu terminal, substituindo-o por um terminal modificado usado para obter dados de cartões.

Terminal de pagamento integrado e middleware de pagamento compartilham dados de cartões. Pagamentos enviados via Internet.



SIM



NÃO

TIPO 6 - VISÃO GERAL

TIPO 6 - RISCOS

TIPO 6 - AMEAÇAS

TIPO 6 - PROTEÇÕES

Como você pode começar a proteger dados de cartões hoje mesmo?*



Use senhas fortes



Proteja os dados de cartões e armazene apenas o necessário



Inspecione seus terminais de pagamento para ver se há danos ou mudanças



Instale os patches de seu fornecedor de terminal de pagamento



Peça ajuda aos seus parceiros fornecedores, se precisar



Proteja o acesso interno aos dados de cartão



Limite o acesso remoto aos seus parceiros fornecedores: não permita que os hackers tenham acesso fácil



Faça varreduras regulares de vulnerabilidade



Use sistemas de pagamento seguro



Proteja sua empresa contra vulnerabilidades da Internet



Use software antivírus

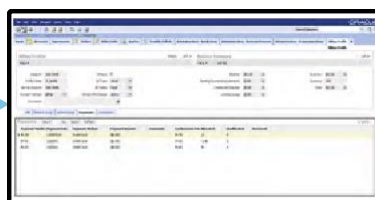


Torne os dados do seu cartão inúteis para criminosos

TERMINAL DE PAGAMENTO INTEGRADO



MIDDLEWARE DE PAGAMENTO



ROTEADOR/FIREWALL



INTERNET



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

Terminal de pagamento sem fio (“pagamento na mesa”) com terminal de pagamento e middleware de pagamento integrados. Pagamentos enviados via Internet.

PERFIL DE RISCO

Os dados do cartão estão criptografados?



SIM



NÃO

TIPO 7 - VISÃO GERAL

TIPO 7 - RISCOS

TIPO 7 - AMEAÇAS

TIPO 7 - PROTEÇÕES

Se você estiver usando uma solução de criptografia ponto a ponto (P2PE) listada pelo PCI, vá para o [Tipo 15](#).

Dados de cartão compartilhados com terminal e middleware

Nenhum outro equipamento conectado aos sistemas de pagamento do comerciante

A criptografia de dados de cartão reduz seu risco. Se o seu terminal de pagamento criptografa os dados dos cartões, pergunte ao fornecedor do terminal como (se ele usa leitura segura e intercâmbio de dados, SRED) ocorre a criptografia.

TERMINAL DE CARTÃO SEM FIO

TERMINAL DE PAGAMENTO INTEGRADO

Terminal de pagamento integrado com leitor de cartão desativado ou sem leitor de cartão

MIDDLEWARE DE PAGAMENTO

ROTEADOR/FIREWALL

INTERNET



Software usado como parte da transação de pagamento

Os pagamentos são efetuados apenas através do terminal de pagamento sem fio na presença do cliente

SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

Para este cenário, os riscos para os dados de cartões estão presentes em acima. Riscos explicados na próxima página.

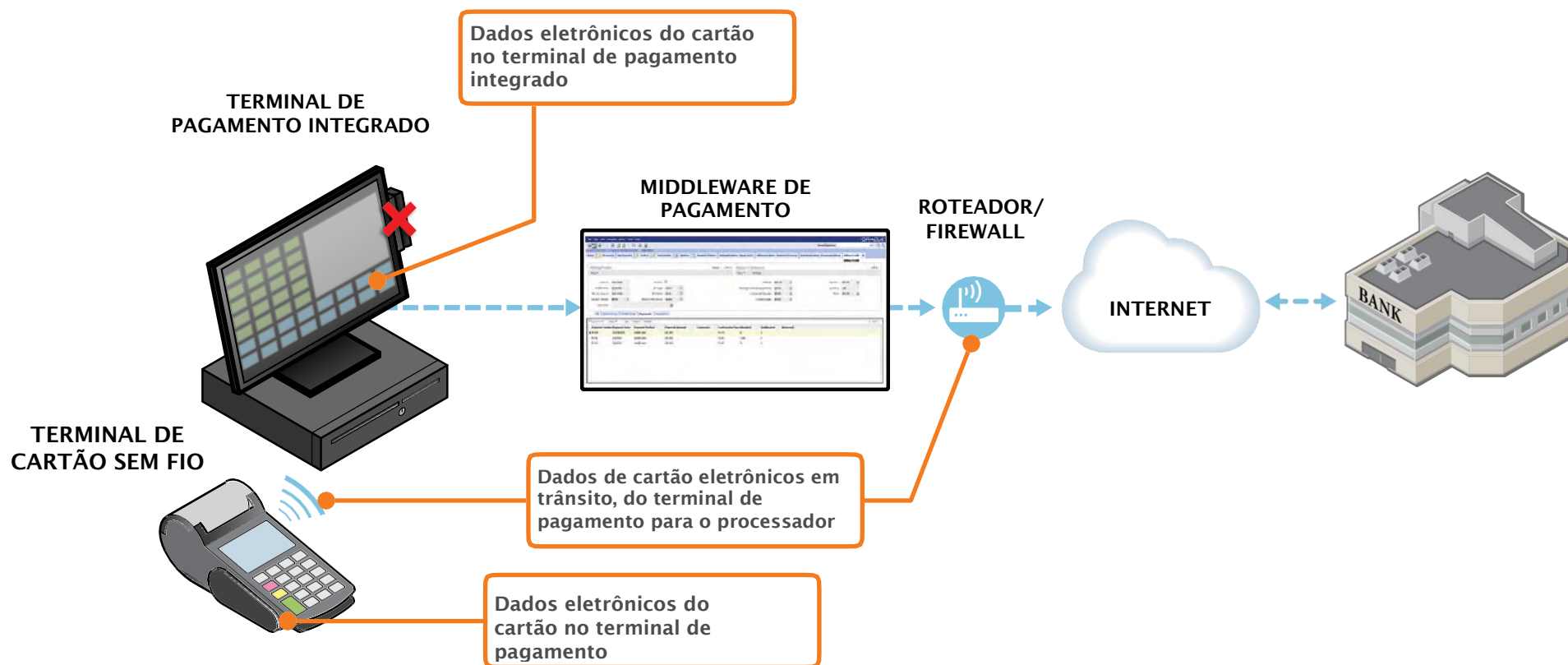


SIM



NÃO

Onde os dados de cartão estão em risco?



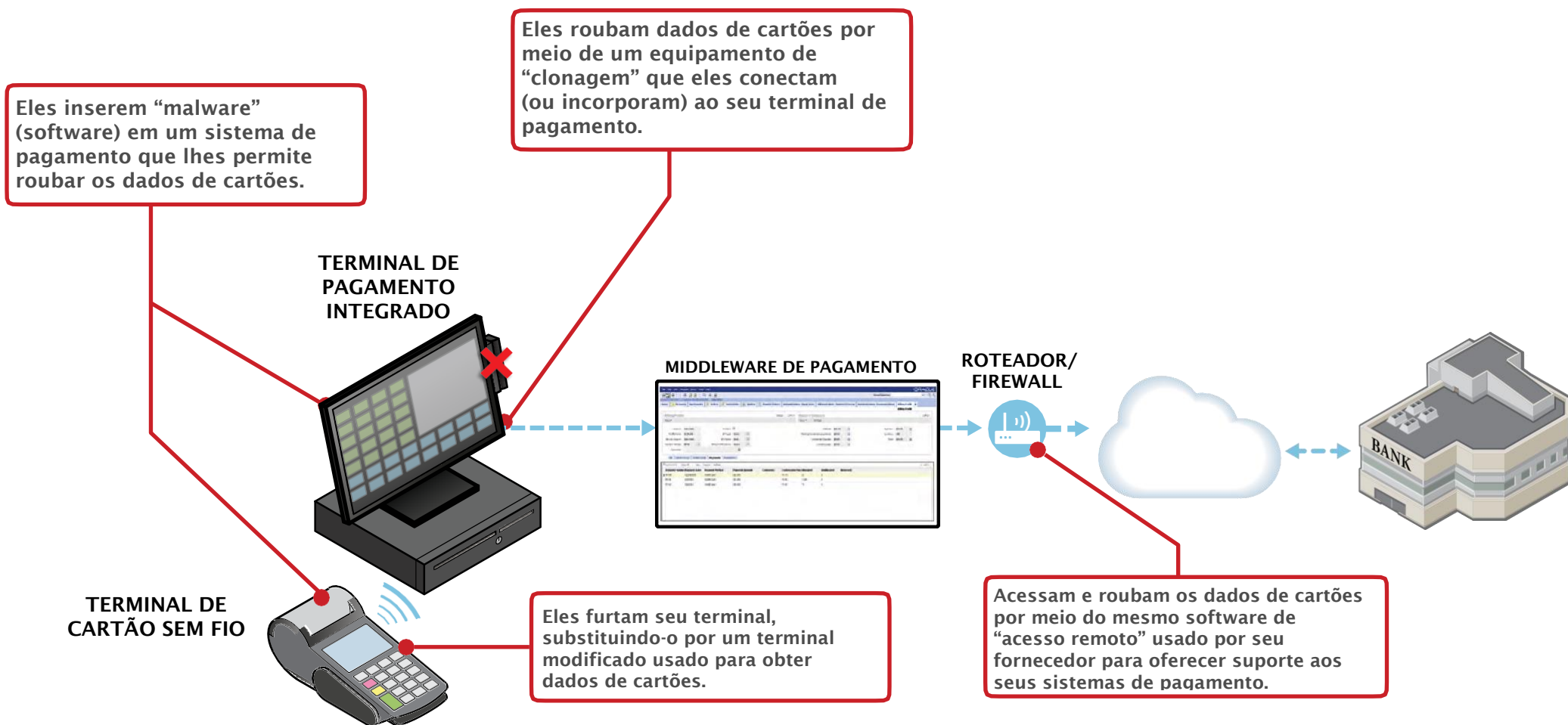


SIM



NÃO

Como os criminosos obtêm os dados de cartão?



Terminal de pagamento sem fio (“pagamento na mesa”) com terminal de pagamento e middleware de pagamento integrados. Pagamentos enviados via Internet.

PERFIL DE RISCO

Os dados do cartão estão criptografados?



SIM



NÃO

TIPO 7 - VISÃO GERAL

TIPO 7 - RISCOS

TIPO 7 - AMEAÇAS

TIPO 7 - PROTEÇÕES

Como você pode começar a proteger dados de cartões hoje mesmo?*



Use senhas fortes



Proteja os dados de cartões e armazene apenas o necessário



Inspeção seus terminais de pagamento para ver se há danos ou mudanças



Instale os patches de seu fornecedor de terminal de pagamento



Peça ajuda aos seus parceiros fornecedores, se precisar



Proteja o acesso interno aos dados de cartão



Limite o acesso remoto aos seus parceiros fornecedores: não permita que os hackers tenham acesso fácil



Faça varreduras regulares de vulnerabilidade



Use sistemas de pagamento seguro



Proteja sua empresa contra vulnerabilidades da Internet

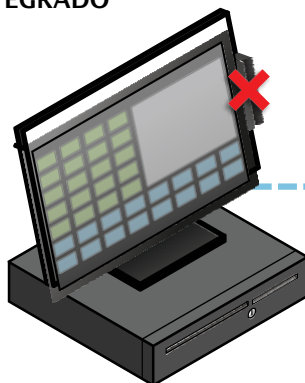


Use software antivírus

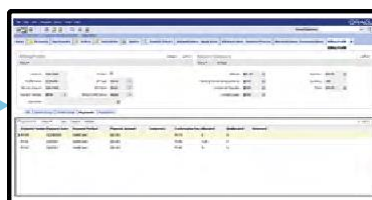


Torne os dados do seu cartão inúteis para criminosos

TERMINAL DE PAGAMENTO INTEGRADO



MIDDLEWARE DE PAGAMENTO



ROTEADOR/FIREWALL



INTERNET



TERMINAL DE CARTÃO SEM FIO



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

O terminal de pagamento conecta-se à caixa registradora eletrônica com equipamento adicional conectado. Pagamentos enviados via Internet.

PERFIL DE RISCO

Os dados do cartão estão criptografados?



SIM



NÃO

TIPO 8 - VISÃO GERAL

TIPO 8 - RISCOS

TIPO 8 - AMEAÇAS

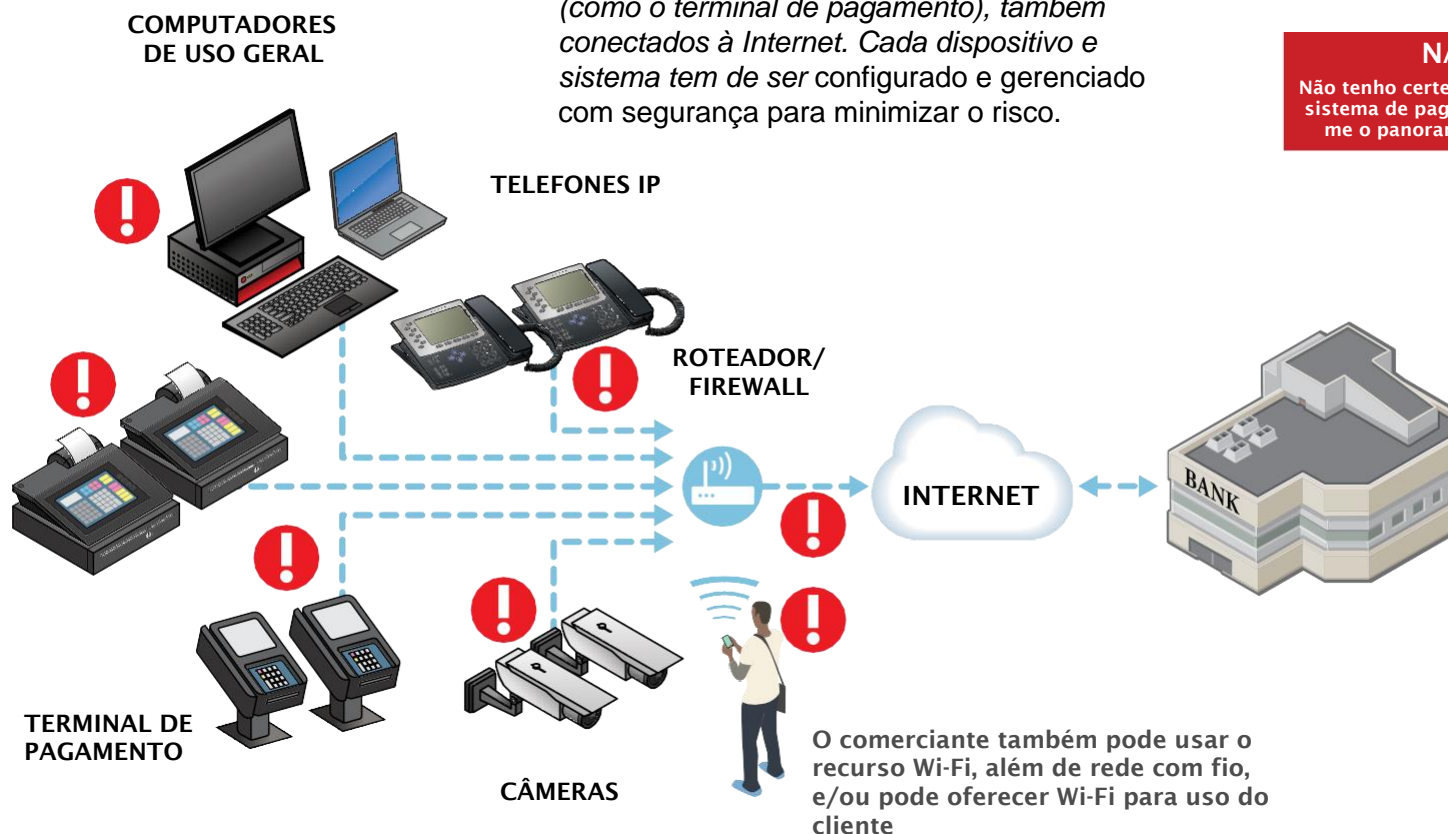
TIPO 8 - PROTEÇÕES

Se você estiver usando uma solução de criptografia ponto a ponto (P2PE) listada pelo PCI, vá para o [Tipo 15](#).

Há muitos pontos de risco aqui devido aos equipamentos adicionais na mesma rede (como o terminal de pagamento), também conectados à Internet. Cada dispositivo e sistema tem de ser configurado e gerenciado com segurança para minimizar o risco.

A criptografia de dados de cartão reduz seu risco. Se seu terminal de pagamento criptografa os dados de cartão, pergunte ao fornecedor do terminal como (se ele usa leitura segura e intercâmbio de dados, SRED) ocorre a criptografia.

Os dados de cartão podem ser inseridos em caixa registradora eletrônica ou terminal de pagamento



SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

Para este cenário, os riscos para os dados de cartões estão presentes em ! acima. Riscos explicados na próxima página.

O terminal de pagamento conecta-se à caixa registradora eletrônica com equipamento adicional conectado. Pagamentos enviados via Internet.

PERFIL DE RISCO

Os dados do cartão estão criptografados?



SIM



NÃO

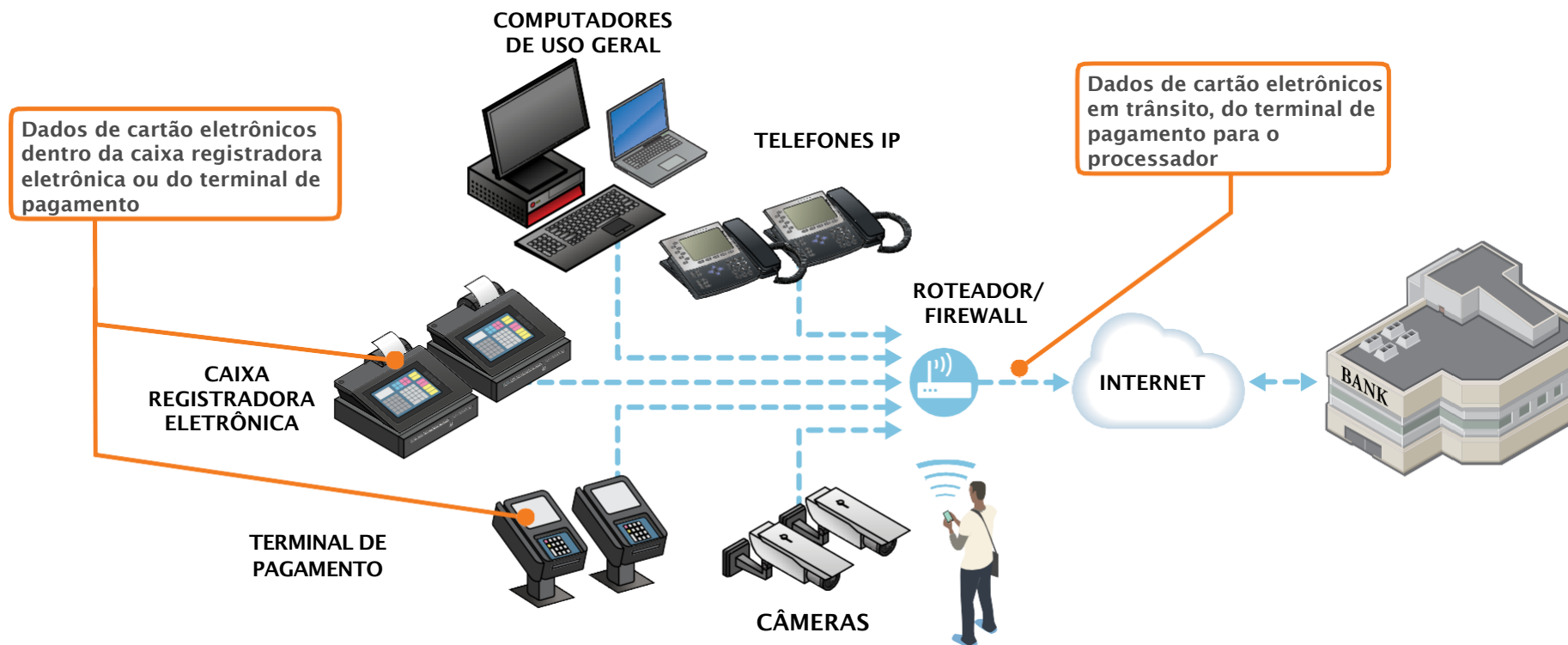
TIPO 8 - VISÃO GERAL

TIPO 8 - RISCOS

TIPO 8 - AMEAÇAS

TIPO 8 - PROTEÇÕES

Onde os dados de cartão estão em risco?



O terminal de pagamento conecta-se à caixa registradora eletrônica com equipamento adicional conectado. Pagamentos enviados via Internet.

PERFIL DE RISCO

Os dados do cartão estão criptografados?



SIM



NÃO

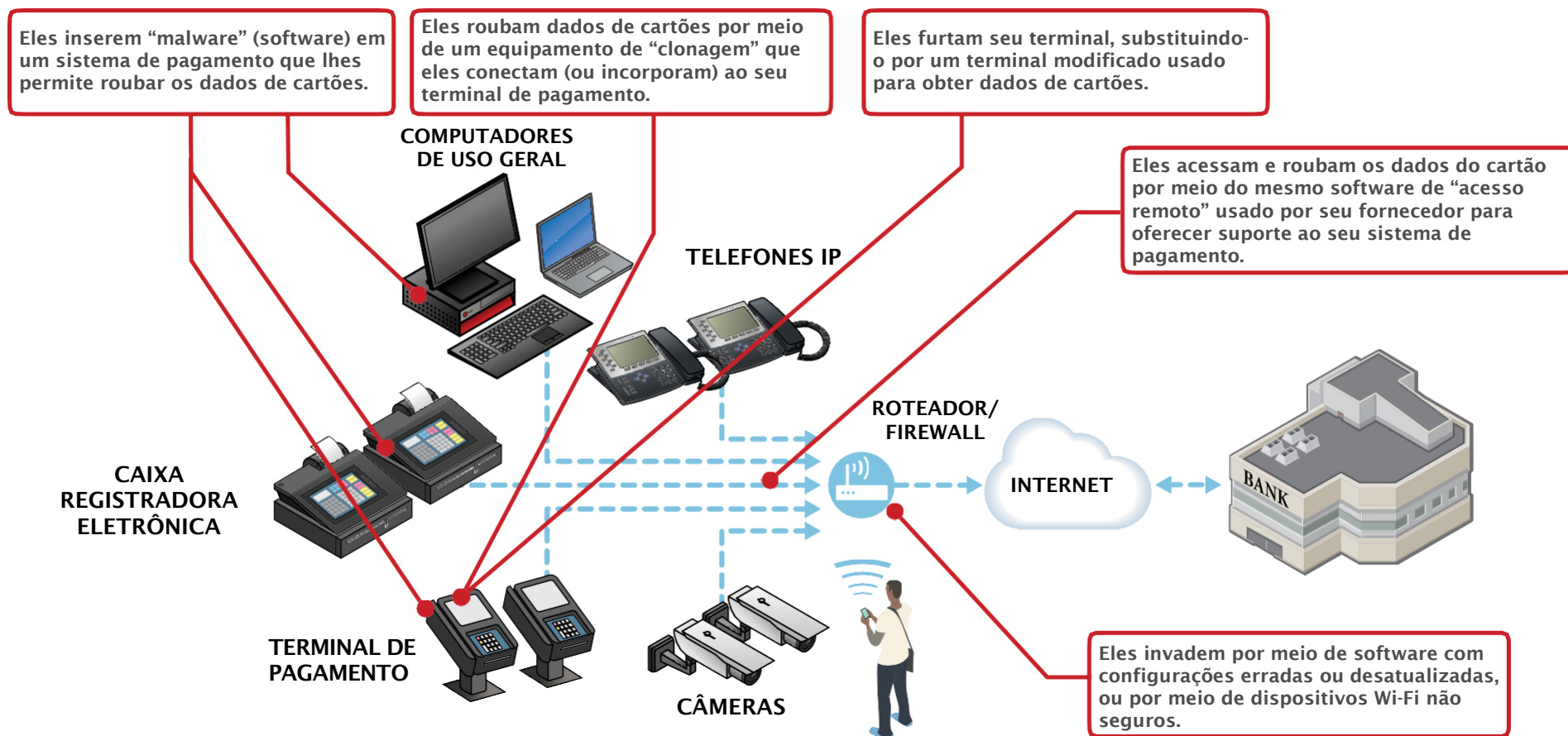
TIPO 8 - VISÃO GERAL

TIPO 8 - RISCOS

TIPO 8 - AMEAÇAS

TIPO 8 - PROTEÇÕES

Como os criminosos obtêm os dados de cartão?



O terminal de pagamento conecta-se à caixa registradora eletrônica com equipamento adicional conectado. Pagamentos enviados via Internet.

PERFIL DE RISCO

Os dados do cartão estão criptografados?



SIM



NÃO

TIPO 8 - VISÃO GERAL

TIPO 8 - RISCOS

TIPO 8 - AMEAÇAS

TIPO 8 - PROTEÇÕES

Como você pode começar a proteger dados de cartões hoje mesmo?*



Use senhas fortes



Proteja os dados de cartões e armazene apenas o necessário



Inspeção seus terminais de pagamento para ver se há danos ou mudanças



Instale os patches de seu fornecedor de terminal de pagamento



Peça ajuda aos seus parceiros fornecedores, se precisar



Proteja o acesso interno aos dados de cartão



Limite o acesso remoto aos seus parceiros fornecedores: não permita que os hackers tenham acesso fácil



Faça varreduras regulares de vulnerabilidade



Use sistemas de pagamento seguro



Proteja sua empresa contra vulnerabilidades da Internet



Use software antivírus



Torne os dados do seu cartão inúteis para criminosos



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

Comerciante de e-commerce com página/formulário de pagamento totalmente terceirizado. Pagamentos enviados pelo prestador de serviços terceirizado em conformidade com o DSS da PCI.



TIPO 9 - VISÃO GERAL

TIPO 9 - RISCOS

TIPO 9 - AMEAÇAS

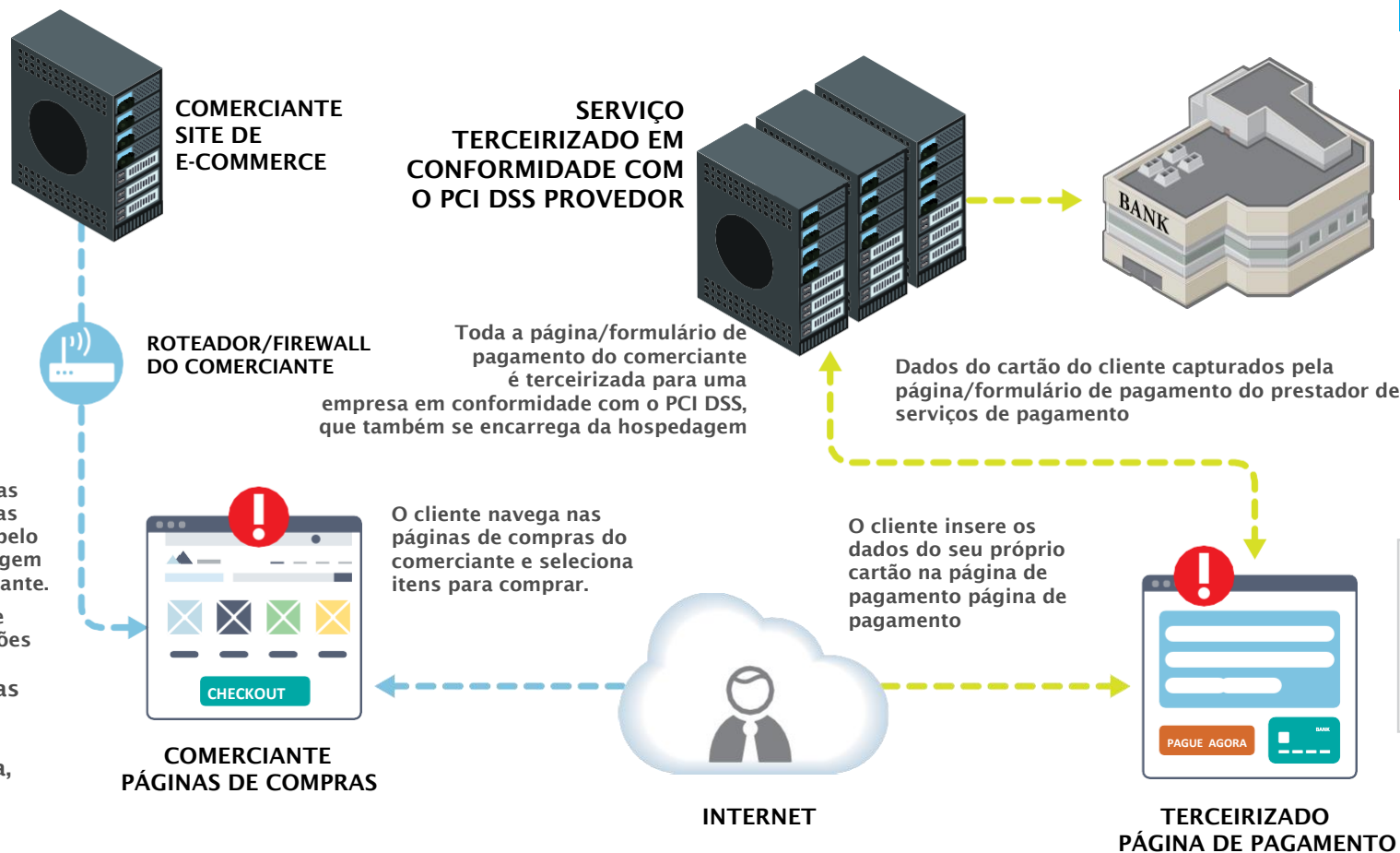
TIPO 9 - PROTEÇÕES

OU: Site do comerciante implementa redirecionamento de URL para enviar o navegador do cliente para a página de pagamento do prestador de serviço terceirizado (conforme mostrado)

OU: O site do comerciante implementa um quadro embutido (IFrame) para exibir o formulário de pagamento do prestador de serviços terceirizado incorporado na página do comerciante (não mostrado)

O site do comerciante pode ser hospedado e gerenciado pelo comerciante ou por um provedor de hospedagem terceirizado em nome do comerciante. De qualquer forma, o comerciante não tem acesso à página de pagamento.

As páginas de compras podem ser hospedadas pelo comerciante ou pelo provedor de hospedagem da página do comerciante. O site do comerciante tem apenas informações sobre o produto (páginas de compras etc.) disponíveis. Comerciante nunca tem acesso a, ou capacidade de, controlar qualquer dado de cartão.



SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

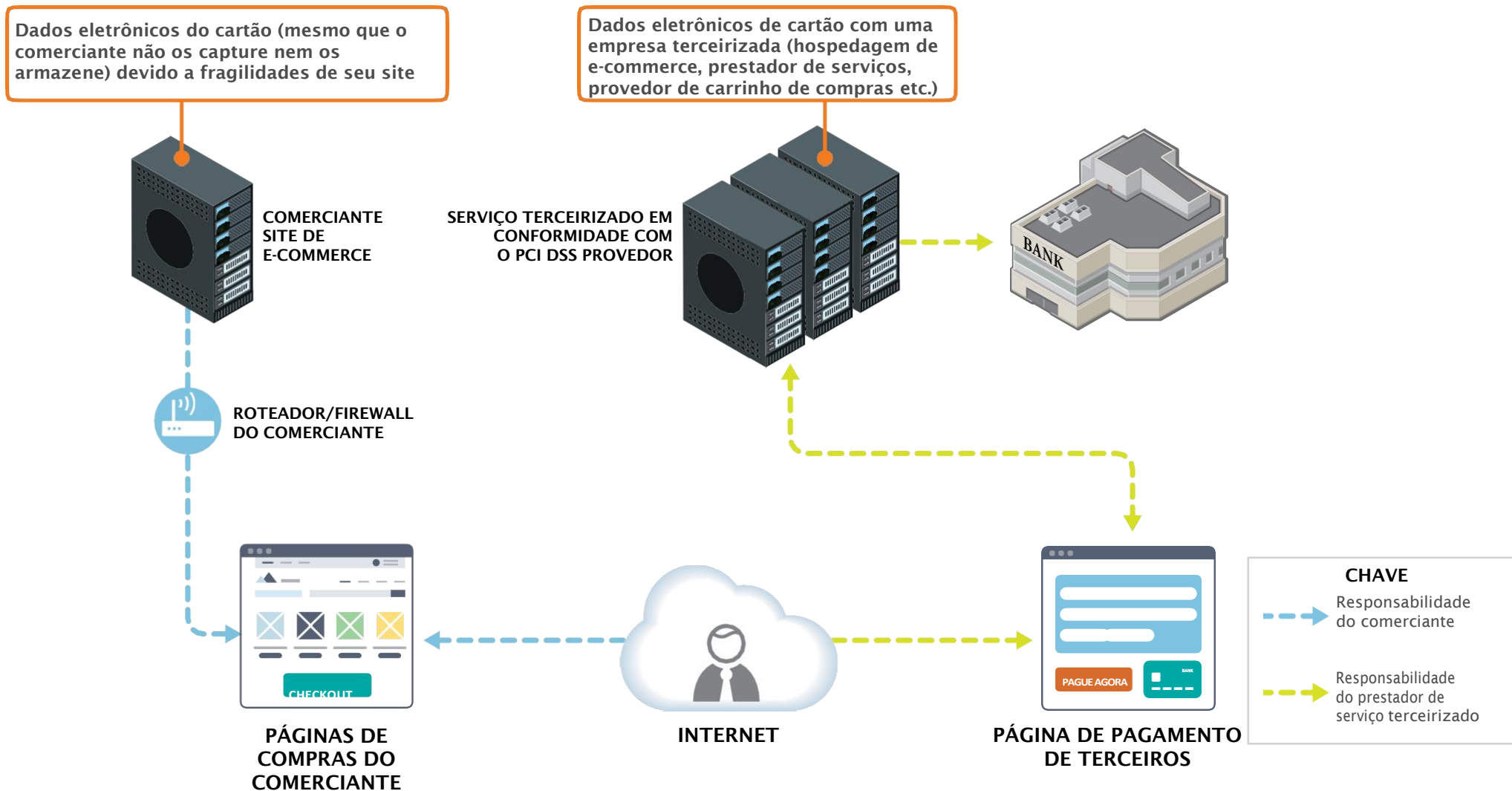
CHAVE

--- Responsabilidade do comerciante

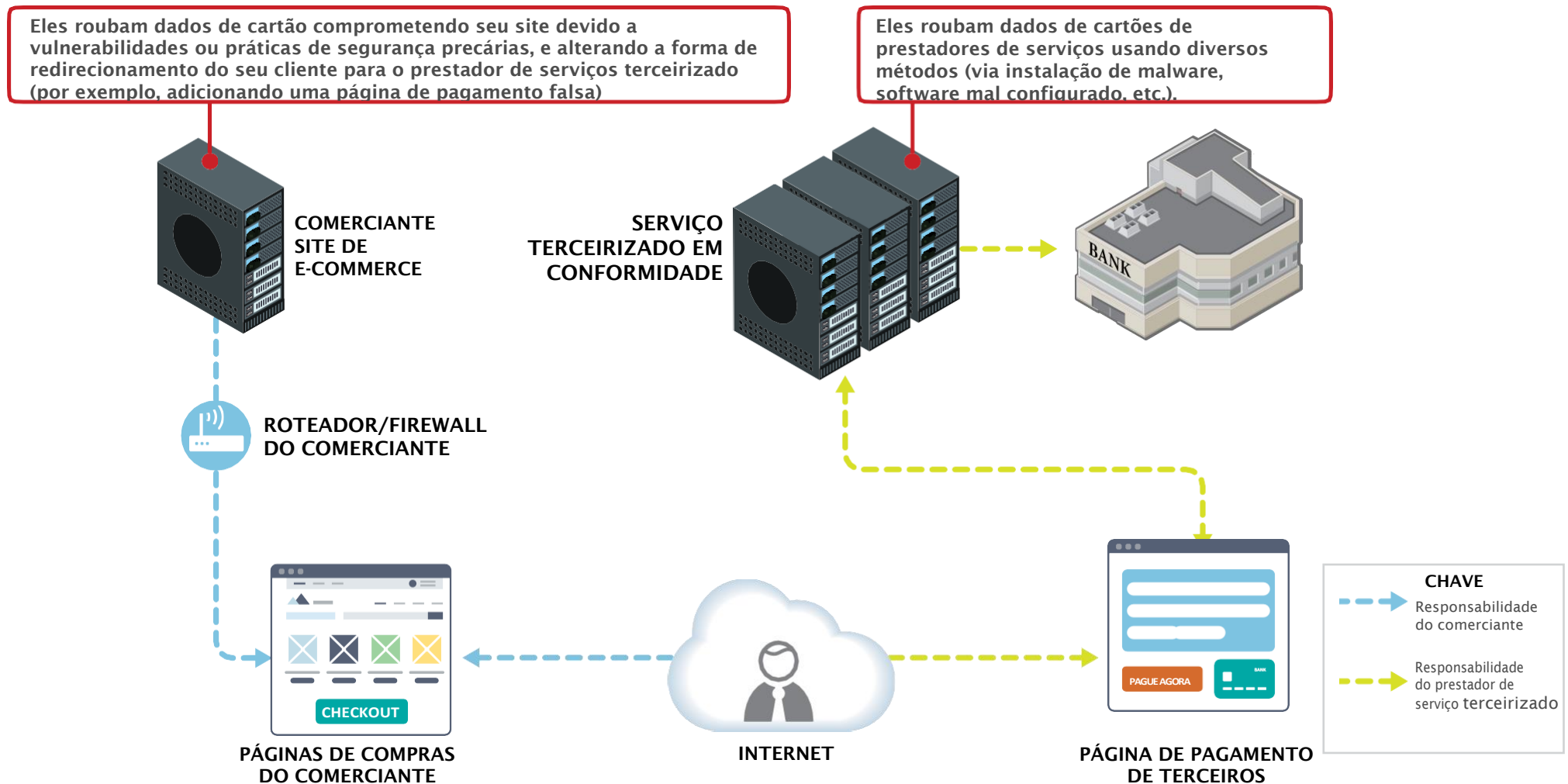
--- Responsabilidade do prestador de serviço terceirizado

Para este cenário, os riscos para os dados de cartões estão presentes em ! acima. Riscos explicados na próxima página.

Onde os dados de cartão estão em risco?



Como os criminosos obtêm os dados de cartão?



Como você pode começar a proteger dados de cartões hoje mesmo?*



Use senhas fortes



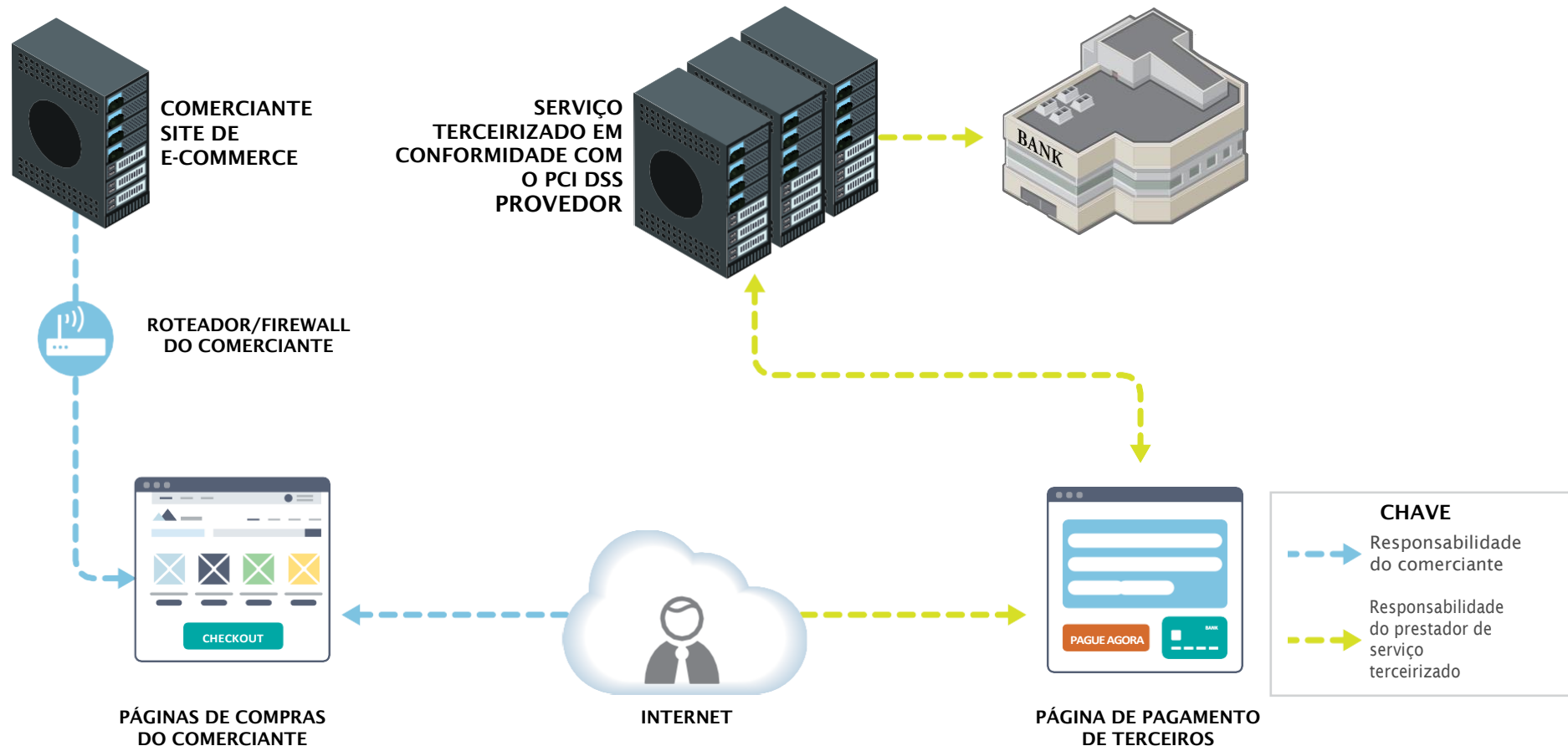
Proteja os dados de cartões e armazene apenas o necessário



Peça ajuda aos seus parceiros fornecedores, se precisar



Proteja o acesso interno aos dados de cartão



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

O comerciante de e-commerce apresenta total ou parcialmente a página de pagamento aos clientes. Pagamentos enviados do navegador do cliente diretamente para o prestador de serviços terceirizado em conformidade com o PCI DSS.



ALTO

TIPO 10 - VISÃO GERAL

TIPO 10 - RISCOS

TIPO 10 - AMEAÇAS

TIPO 10 - PROTEÇÕES

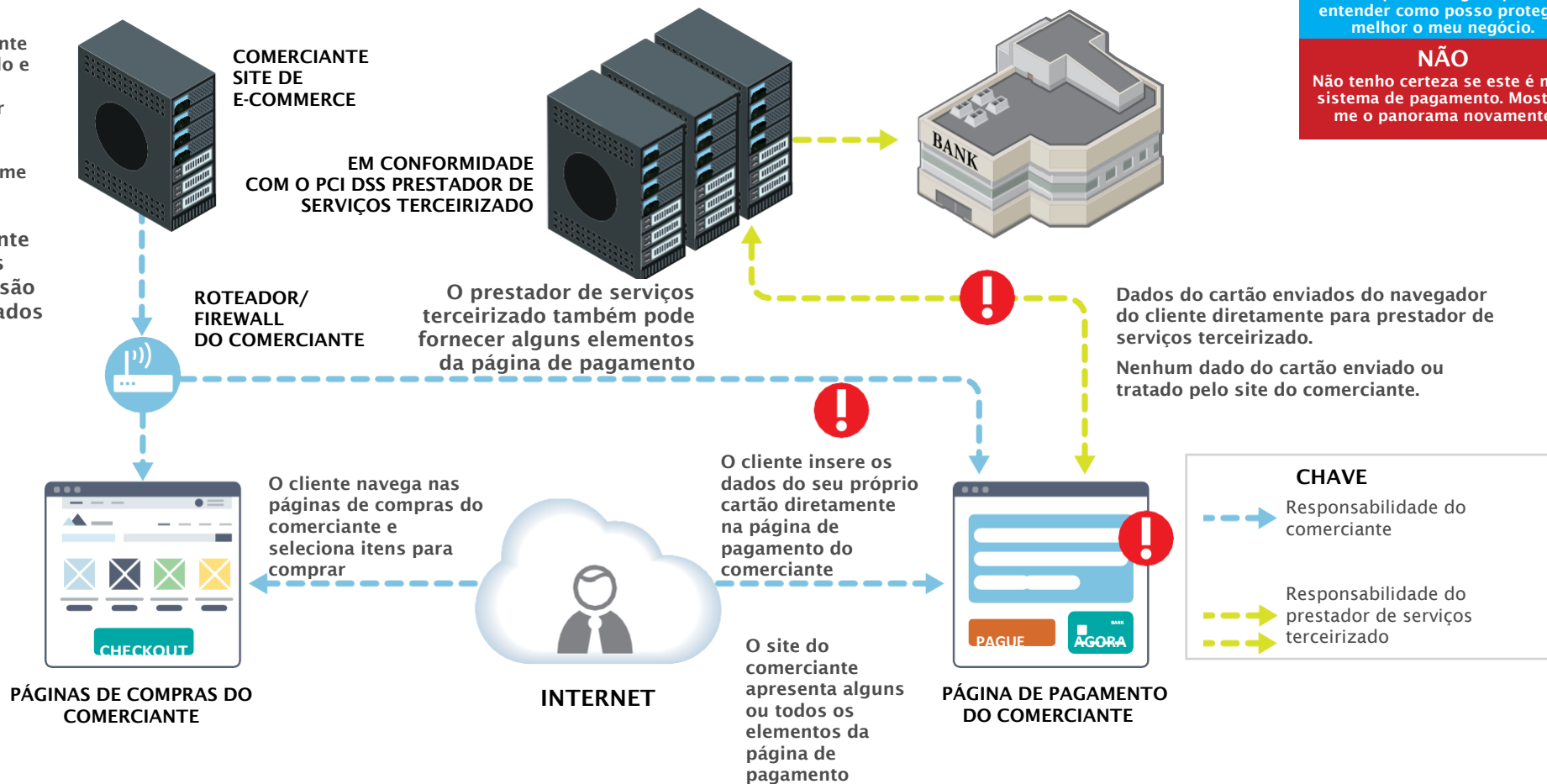
OU: O site do comerciante cria toda a página de pagamento e usa o Método de Envio Direto para enviar dados de cartão (conforme mostrado).

OU: O site do comerciante cria toda a página de pagamento e solicita que o navegador do cliente crie o pagamento a partir do código Javascript executado a partir do prestador de serviços terceirizado (não exibido).

Em ambos os casos, os dados do cartão são enviados diretamente do navegador do cliente para o prestador de serviços terceirizado.

O site do comerciante pode ser hospedado e gerenciado pelo comerciante ou por um provedor de hospedagem terceirizado em nome do comerciante.

Site do comerciante controla como os dados do cartão são coletados e enviados ao terceiro.



SIM

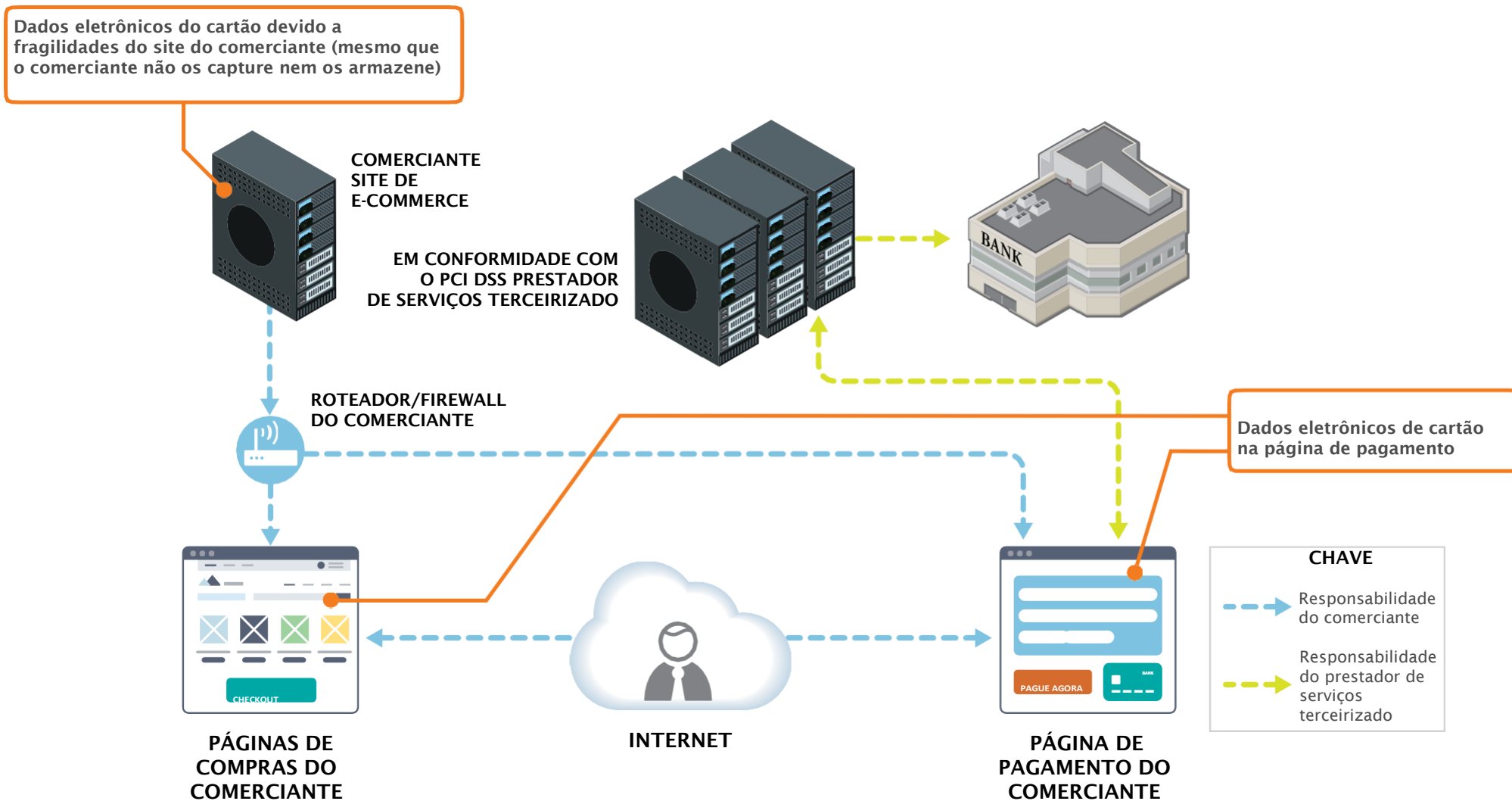
Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

Para este cenário, os riscos para os dados de cartões estão presentes em **!** acima. Riscos explicados na próxima página.

Onde os dados de cartão estão em risco?

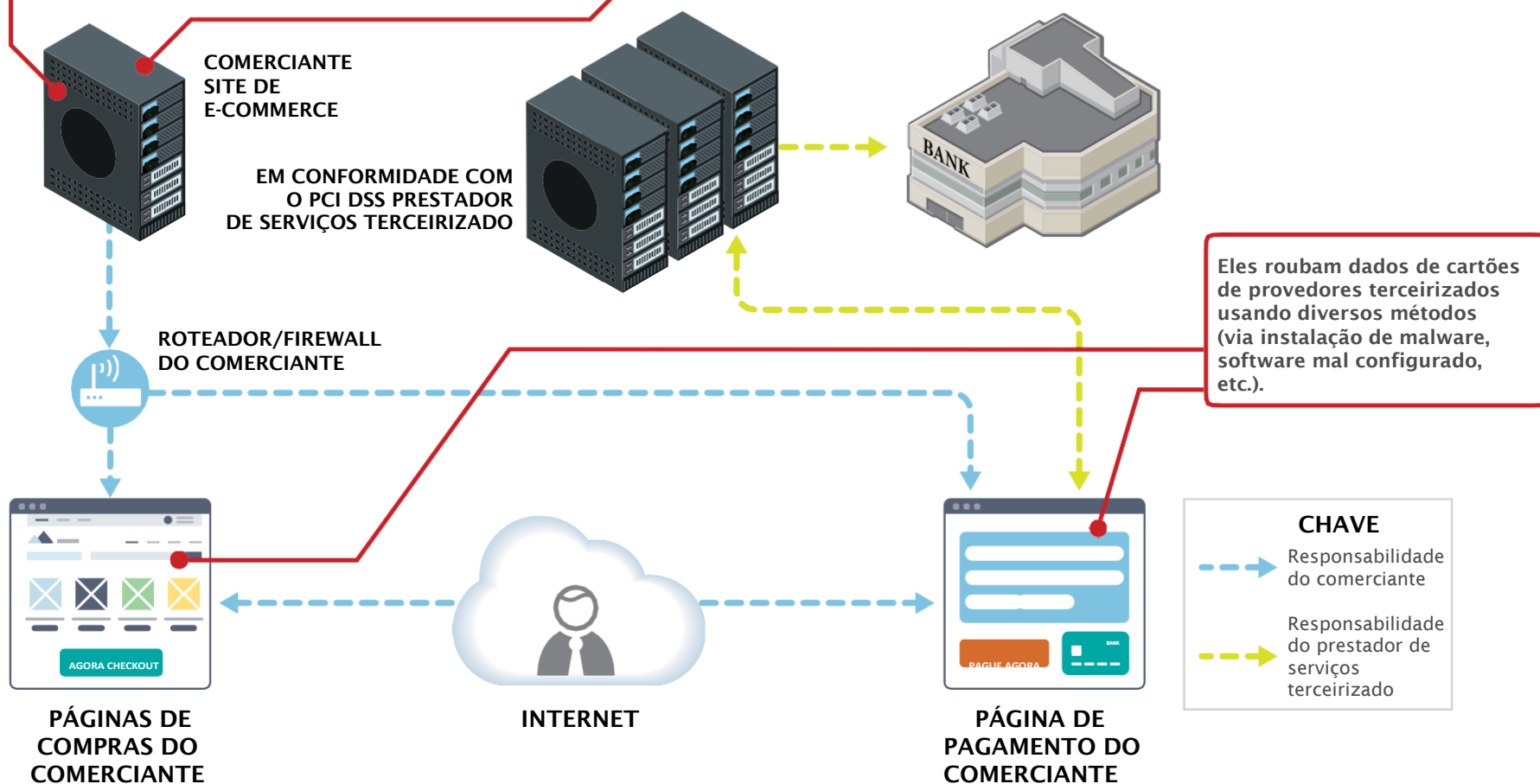




Como os criminosos obtêm os dados de cartão?

Eles roubam os dados de cartão comprometendo seu site devido a vulnerabilidades ou práticas de segurança precárias, e alterando sua página de pagamento para pegar cópias dos dados de cartão de seus clientes à medida que as vendas são processadas

Eles roubam dados comprometendo seu aplicativo de internet para alterar seu processo de checkout ou suas páginas de pagamento



Como você pode começar a proteger dados de cartões hoje mesmo?*



Use senhas fortes



Proteja os dados de cartões e armazene apenas o necessário



Instale os patches de seu fornecedor de terminal de pagamento



Peça ajuda aos seus parceiros fornecedores, se precisar



Proteja o acesso interno aos dados de cartão



Limite o acesso remoto aos seus parceiros fornecedores: não permita que os hackers tenham acesso fácil



Use software antivírus



Faça varreduras regulares de vulnerabilidade



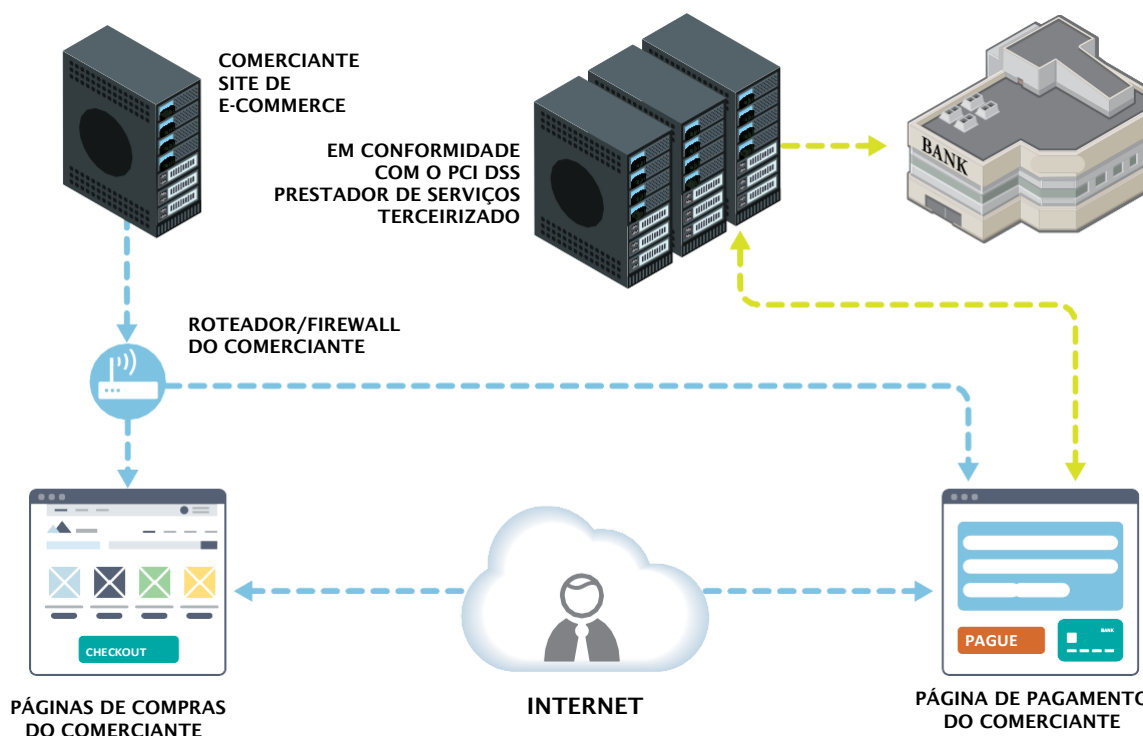
Use sistemas de pagamento seguro



Proteja sua empresa contra vulnerabilidades da Internet



Torne os dados do seu cartão inúteis para criminosos



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

CHAVE

- Responsabilidade do comerciante
- Responsabilidade do prestador de serviços terceirizado

O comerciante de e-commerce aceita dados de cartão usando a página de pagamento apresentada aos clientes a partir de seu próprio site. Pagamentos enviados pelo site do comerciante.



TIPO 11 - VISÃO GERAL

TIPO 11 - RISCOS

TIPO 11 - AMEAÇAS

TIPO 11 - PROTEÇÕES

SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

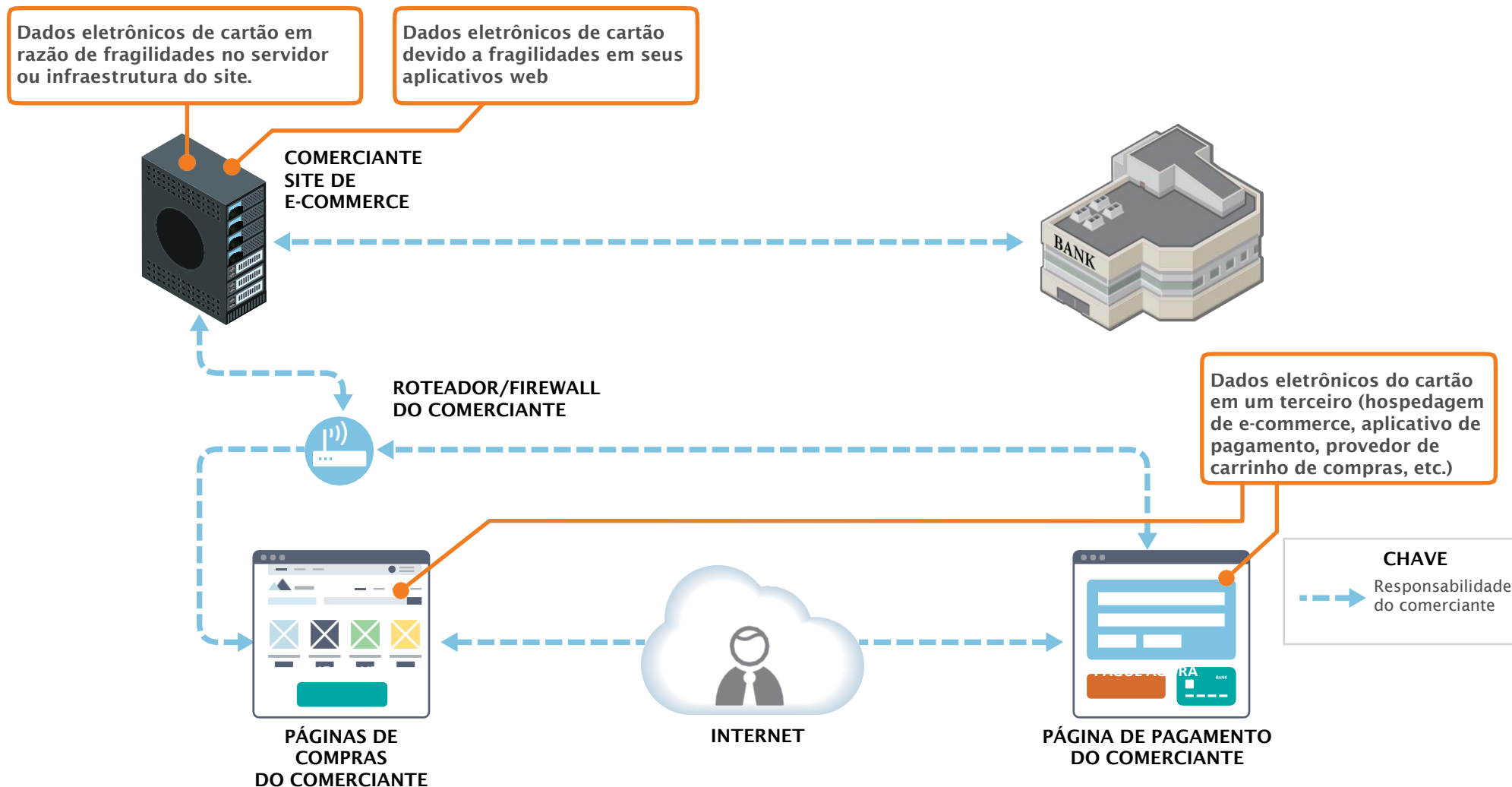


Para este cenário, os riscos para os dados de cartões estão presentes em ! acima. Riscos explicados na próxima página.

O comerciante de e-commerce aceita dados de cartão usando a página de pagamento apresentada aos clientes a partir de seu próprio site. Pagamentos enviados pelo site do comerciante.



Onde os dados de cartão estão em risco?



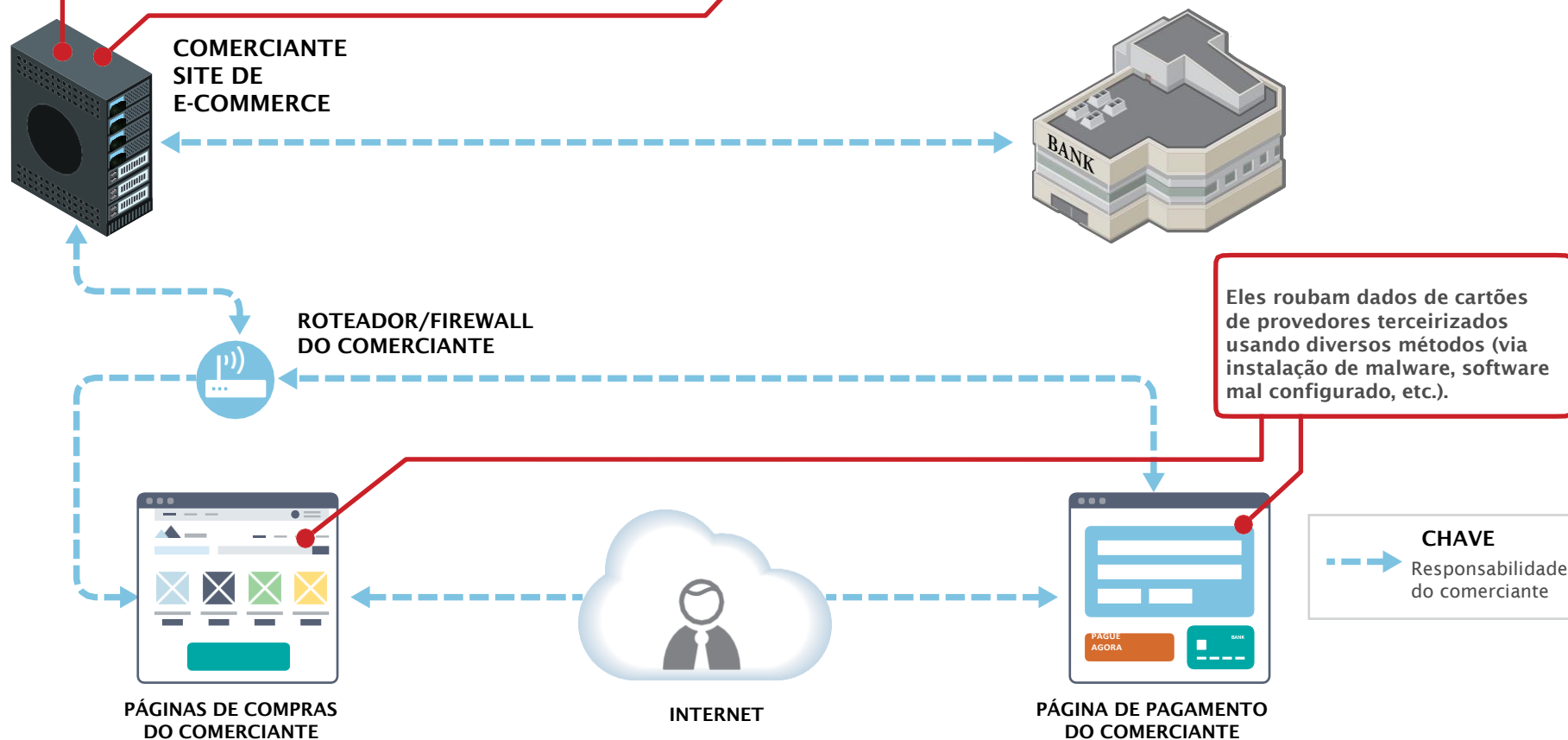
O comerciante de e-commerce aceita dados de cartão usando a página de pagamento apresentada aos clientes a partir de seu próprio site. Pagamentos enviados pelo site do comerciante.



Como os criminosos obtêm os dados de cartão?

Eles roubam dados de cartões aproveitando-se de seu site em razão de vulnerabilidades ou práticas de segurança precárias. Por exemplo, a injeção SQL é uma técnica comum usada para roubar dados de sites.

Eles roubam dados comprometendo seu aplicativo da internet para alterar seu processo de checkout ou suas páginas de pagamento.



O comerciante de e-commerce aceita dados de cartão usando a página de pagamento apresentada aos clientes a partir de seu próprio site. Pagamentos enviados pelo site do comerciante.



TIPO 11 - VISÃO GERAL

TIPO 11 - RISCOS

TIPO 11 - AMEAÇAS

TIPO 11 - PROTEÇÕES

Como você pode começar a proteger dados de cartões hoje mesmo?*



Use senhas fortes



Proteja os dados de cartões e armazene apenas o necessário



Instale os patches de seu fornecedor de terminal de pagamento



Peça ajuda aos seus parceiros fornecedores, se precisar



Proteja o acesso interno aos dados de cartão



Limite o acesso remoto aos seus parceiros fornecedores: não permita que os hackers tenham acesso fácil



Use software antivírus



Faça varreduras regulares de vulnerabilidade



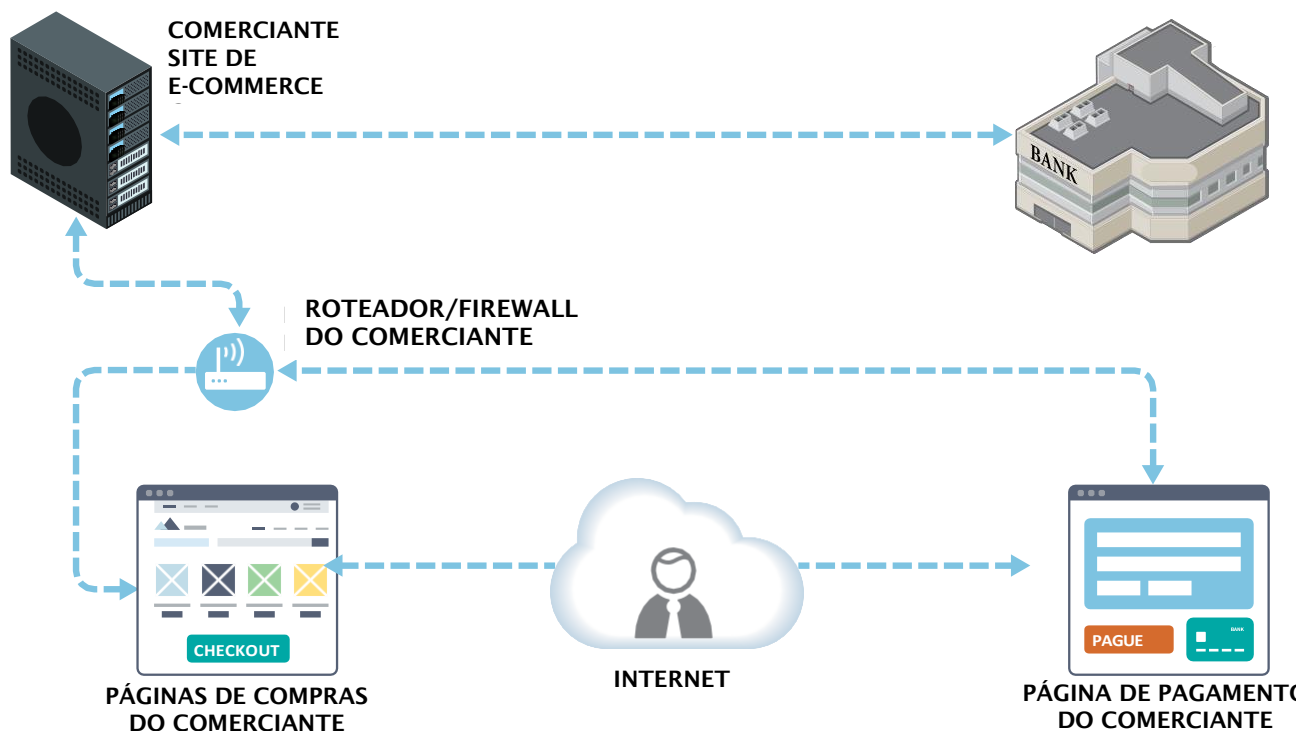
Use sistemas de pagamento seguro



Proteja sua empresa contra vulnerabilidades da Internet



Torne os dados do seu cartão inúteis para criminosos



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

Leitor de cartão seguro de criptografia e terminal de pagamento móvel listados pelo PCI. Pagamentos enviados somente via rede celular.



TIPO 12 - VISÃO GERAL

TIPO 12 - RISCOS

TIPO 12 - AMEAÇAS

TIPO 12 - PROTEÇÕES

Se você estiver usando uma solução de criptografia ponto a ponto (P2PE) listada pelo PCI, vá para o [Tipo 15](#).

O terminal de pagamento móvel só se conecta à Internet pela rede celular e não usa Wi-Fi

Para comerciantes quando não têm local fixo (feiras, exposições, etc.)

O leitor de cartão seguro está listado no site do PCI SSC como um SCR aprovado. Pergunte ao seu fornecedor ou verifique aqui para confirmar (selecione SCR em “tipo de dispositivo”):

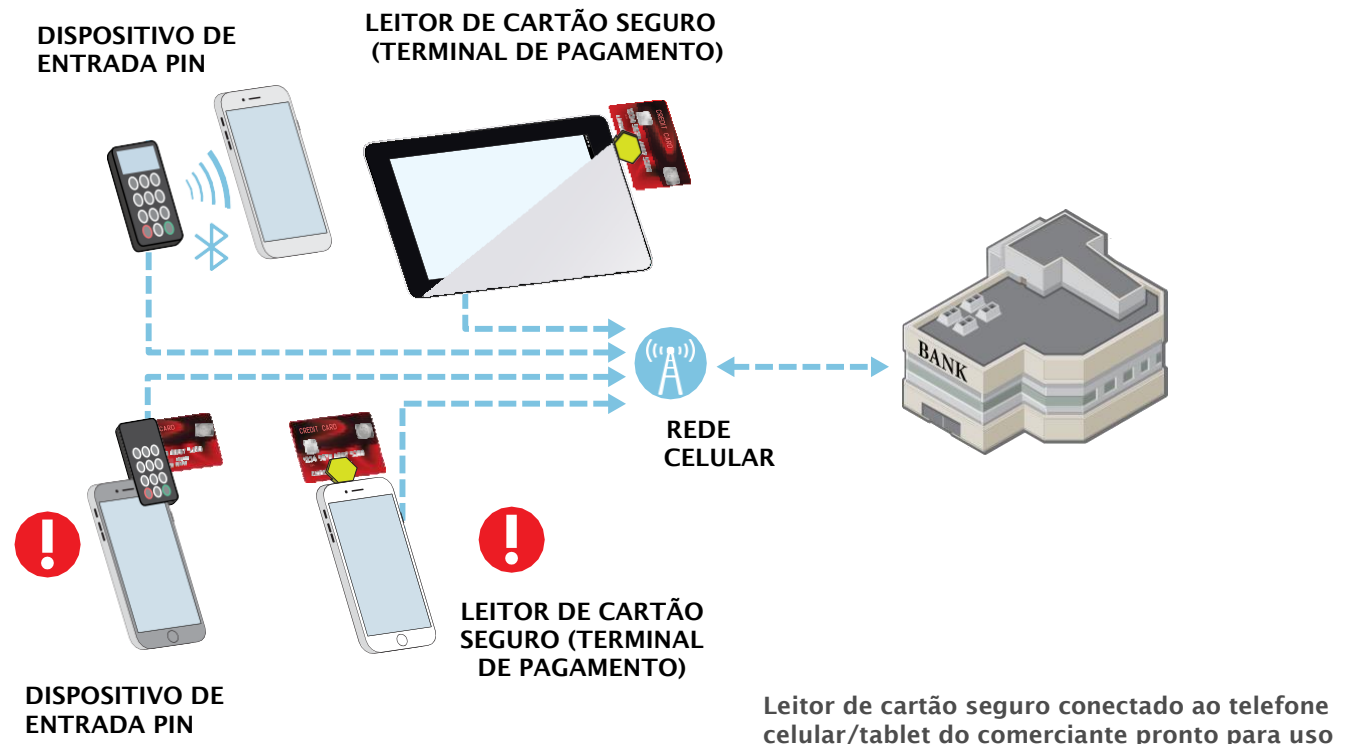
[Dispositivos PTS listados pelo PCI](#).

Os dados de cartões e de PIN são criptografados no leitor de cartões seguro e no dispositivo de digitação do PIN antes do envio para o telefone/tablet; o telefone/tablet só tem acesso aos dados criptografados do cartão

O comerciante não tem capacidade de inserir os dados de cartões manualmente.

O comerciante confirma que o terminal de pagamento móvel não foi adulterado de nenhuma forma e que os aplicativos só podem ser baixados a partir das lojas de aplicativo do fornecedor.

Diferentes dispositivos são usados para ler os dados de cartões com faixa magnética, inserir o número de identificação pessoal (PIN) e ler os dados de cartões com chip



SIM

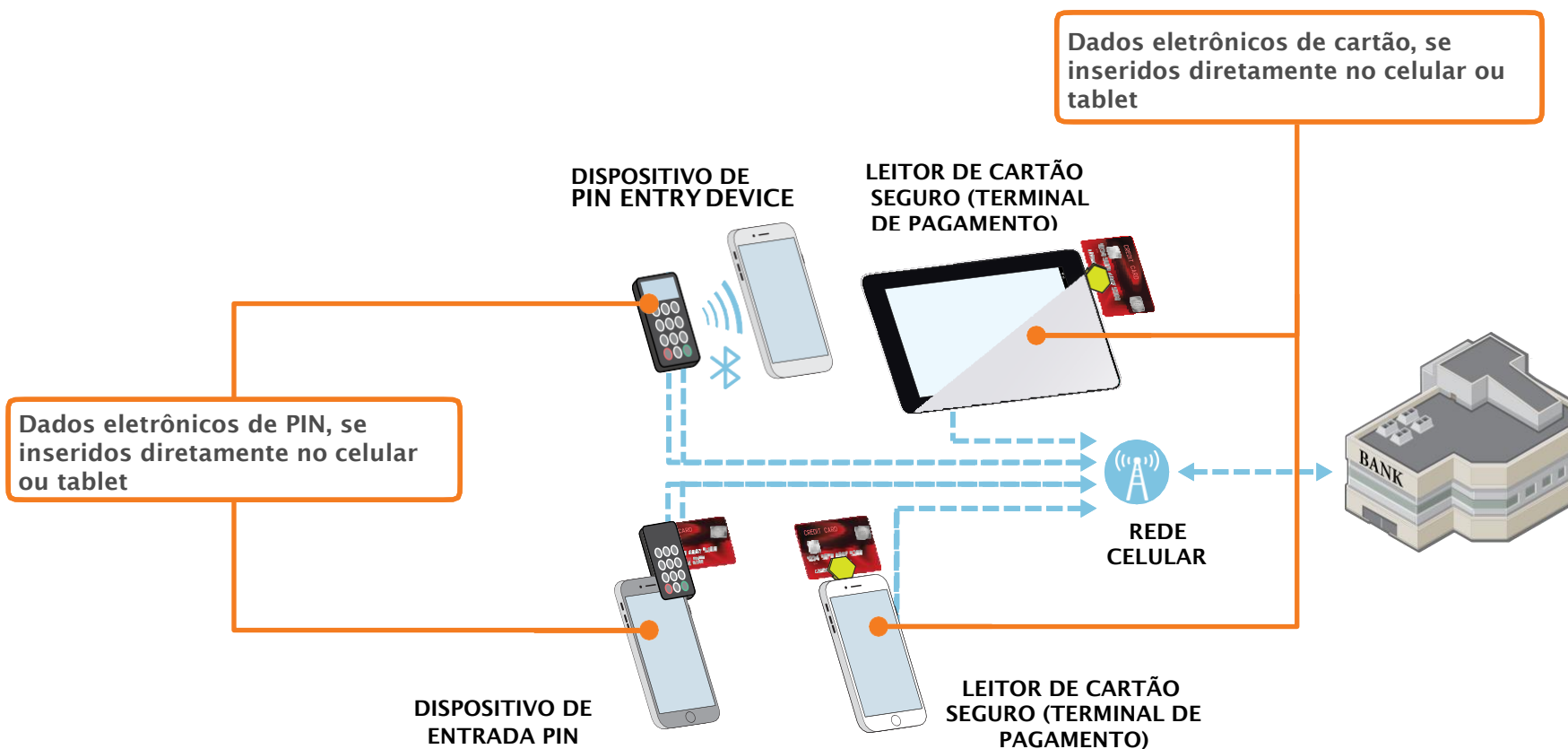
Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

Para este cenário, os riscos para os dados de cartões estão presentes em acima. Riscos explicados na próxima página.

Onde os dados de cartão estão em risco?

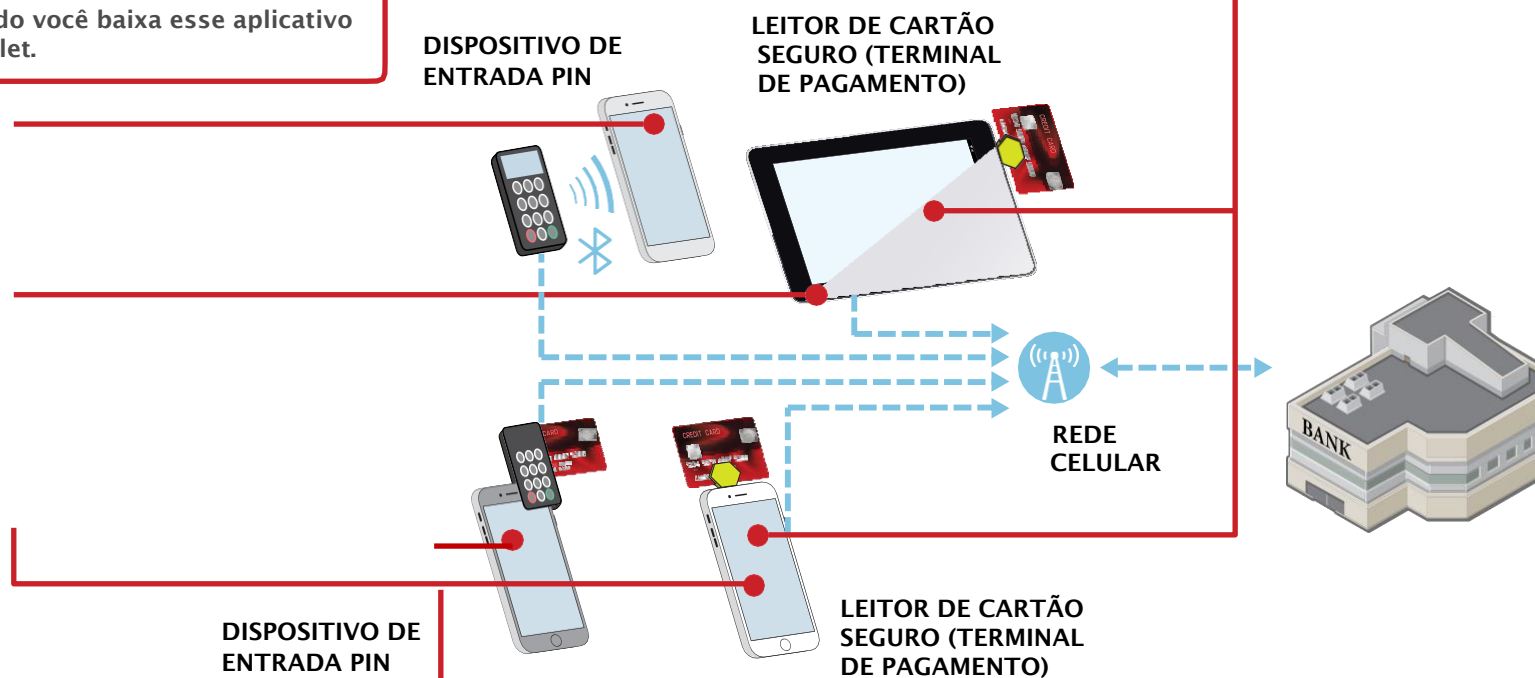


Como os criminosos obtêm os dados de cartão?

Eles invadem o telefone/tablet e inserem o “malware” (software) que lhes permite fazer um desvio do leitor seguro de cartões e roubar dados de cartões ou dados de PIN em telefones celulares/tablets.

Eles usam aplicativos da “loja de aplicativos” que lhes permitem fazer um desvio do leitor seguro de cartões e roubar dados de cartões ou de PIN quando você baixa esse aplicativo no telefone/tablet.

Eles roubam os dados de cartões trocando o leitor de cartão seguro por um que tenha sido modificado para incluir um dispositivo de clonagem.





Como você pode começar a proteger dados de cartões hoje mesmo?*



Inspecione seus leitores de cartões seguros e dispositivos de digitação de PIN para ver se há danos ou mudanças



Instale os patches de seus fornecedores



Peça ajuda aos seus parceiros fornecedores, se precisar



Proteja sua empresa contra vulnerabilidades da Internet



Use um leitor de cartão seguro e um dispositivo de digitação de PIN



Torne os dados do seu cartão inúteis para criminosos



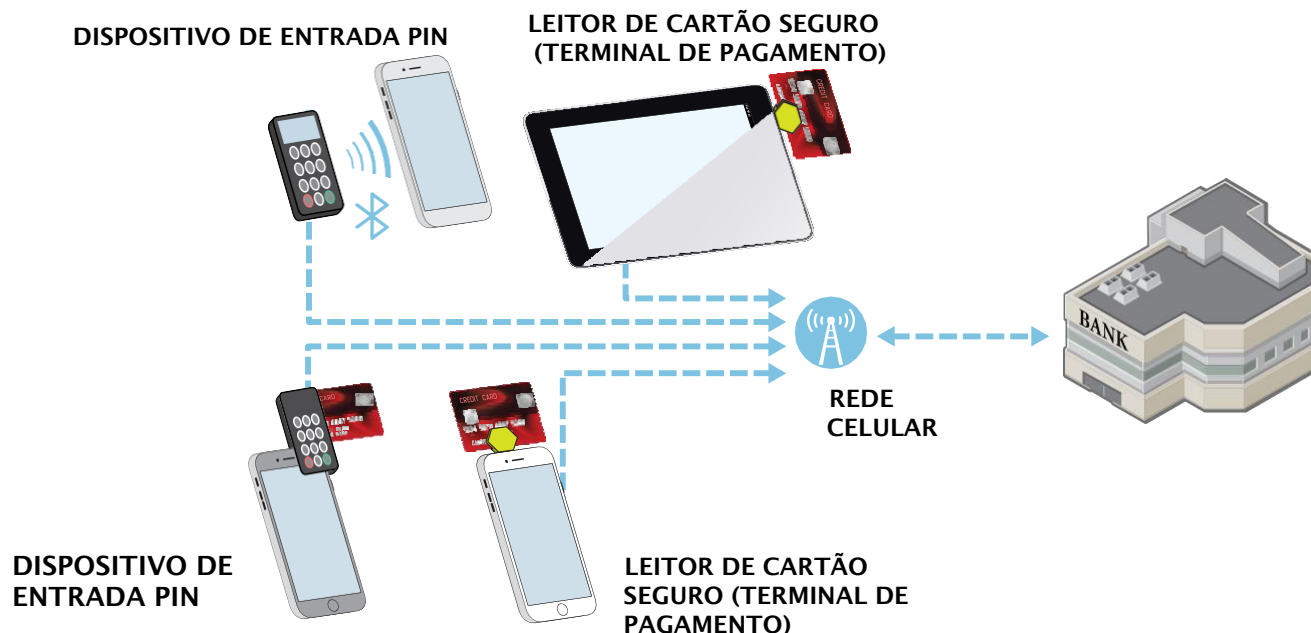
Proteja os dados de cartões e armazene apenas o necessário



Proteja o acesso interno aos dados de cartão



Limite o acesso remoto aos seus parceiros fornecedores: não permita que os hackers tenham acesso fácil



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

Leitor de cartão seguro de criptografia e terminal de pagamento móvel listados pelo PCI. Pagamentos enviados via rede celular ou Wi-Fi.



TIPO 13 - VISÃO GERAL

TIPO 13 - RISCOS

TIPO 13 - AMEAÇAS

TIPO 13 - PROTEÇÕES

Se você estiver usando uma solução de criptografia ponto a ponto (P2PE) listada pelo PCI, vá para o [Tipo 15](#).

Conecta-se à Internet pela rede celular e/ou Wi-Fi.

Para comerciantes quando não têm local fixo (feiras, exposições, etc.)

O leitor de cartão seguro está listado no site do PCI SSC como um SCR aprovado. Pergunte ao seu fornecedor ou verifique aqui para confirmar (selecione SCR em “tipo de dispositivo”): [Dispositivos PTS listados pelo PCI](#).

Os dados de cartões e de PIN são criptografados no leitor de cartões seguro e no dispositivo de digitação do PIN antes do envio para o telefone/tablet; o telefone/tablet só tem acesso aos dados criptografados do cartão

O comerciante não tem capacidade de inserir os dados de cartões manualmente

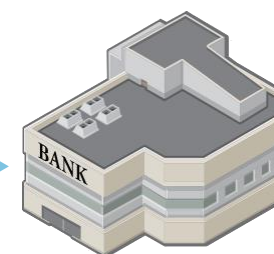
O comerciante confirma que o terminal de pagamento móvel não foi adulterado de nenhuma forma e que os aplicativos só podem ser baixados a partir das lojas de aplicativo do fornecedor.

DISPOSITIVO DE ENTRADA PIN

LEITOR DE CARTÃO SEGURO (TERMINAL DE PAGAMENTO)

Diferentes dispositivos são usados para ler os dados de cartões com faixa magnética, inserir o número de identificação pessoal (PIN) e ler os dados de cartões com chip


WI-FI OU REDE CELULAR



DISPOSITIVO DE ENTRADA PIN

LEITOR DE CARTÃO SEGURO (TERMINAL DE PAGAMENTO)

Leitor de cartão seguro conectado ao telefone celular/tablet do comerciante pronto para uso

Para este cenário, os riscos para os dados de cartões estão presentes em  acima. Riscos explicados na próxima página.

SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

Leitor de cartão seguro de criptografia e terminal de pagamento móvel listados pelo PCI. Pagamentos enviados via rede celular ou Wi-Fi.



Onde os dados de cartão estão em risco?



Leitor de cartão seguro de criptografia e terminal de pagamento móvel listados pelo PCI. Pagamentos enviados via rede celular ou Wi-Fi.

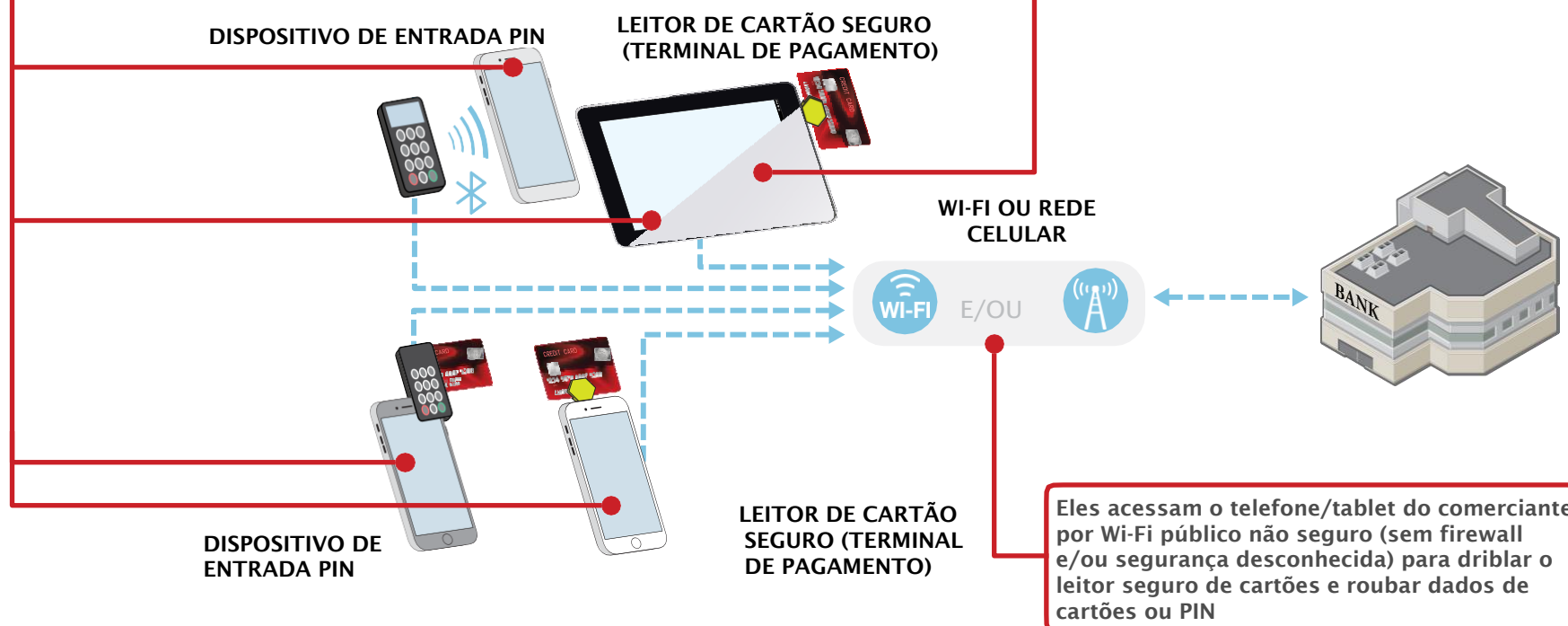


Como os criminosos obtêm os dados de cartão?

Eles invadem o telefone/tablet e inserem o "malware" (software) que lhes permite fazer um desvio do leitor seguro de cartões e roubar dados de cartões ou dados de PIN em telefones celulares/tablets.

Eles usam aplicativos da "loja de aplicativos" para roubar dados de cartões ou de PIN quando você baixa esse aplicativo no telefone/tablet.

Eles roubam os dados de cartões trocando o leitor de cartão seguro por um que tenha sido modificado para incluir um dispositivo de clonagem.



Leitor de cartão seguro de criptografia e terminal de pagamento móvel listados pelo PCI. Pagamentos enviados via rede celular ou Wi-Fi.



TIPO 13 - VISÃO GERAL

TIPO 13 - RISCOS

TIPO 13 - AMEAÇAS

TIPO 13 - PROTEÇÕES

Como você pode começar a proteger dados de cartões hoje mesmo?*



Proteja o acesso interno aos dados de cartão



Inspeção seus leitores de cartões seguros e dispositivos de digitação de PIN para ver se há danos ou mudanças



Instale os patches de seu fornecedor de terminal de pagamento



Peça ajuda aos seus parceiros fornecedores, se precisar



Proteja sua empresa contra vulnerabilidades da Internet



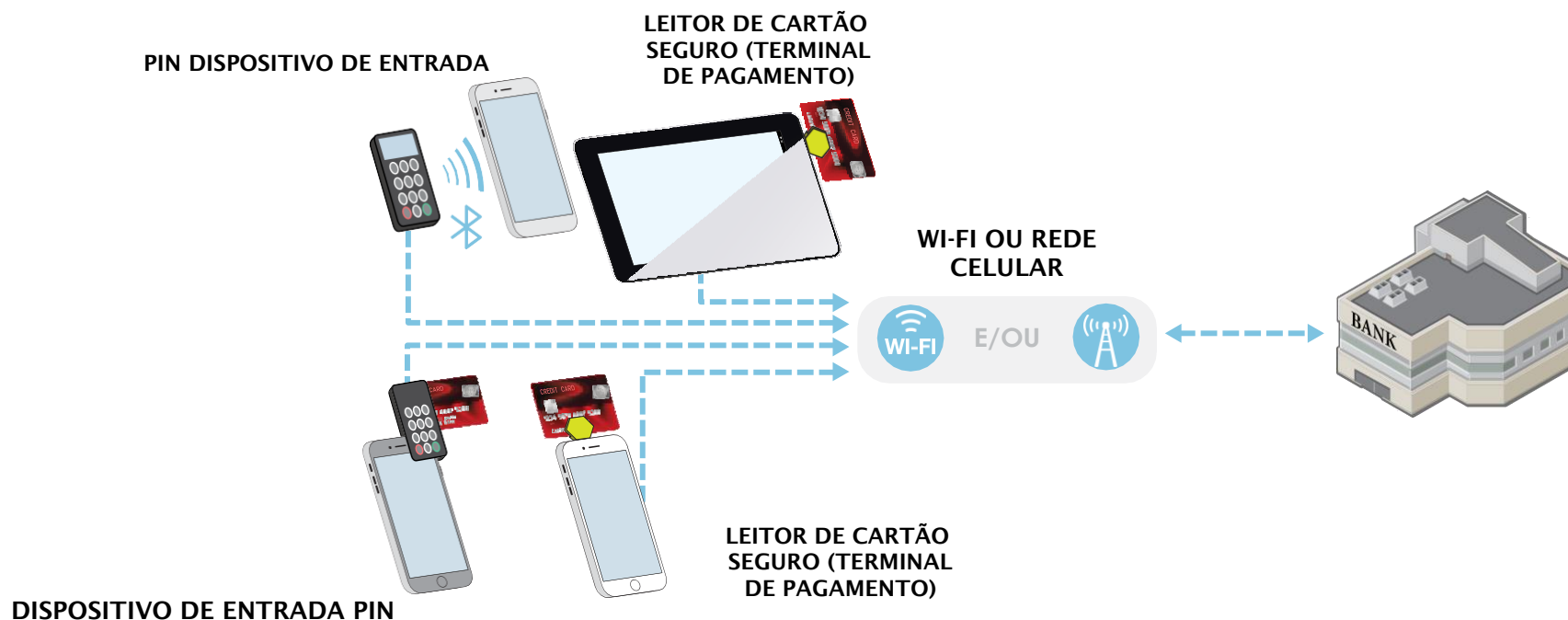
Limite o acesso remoto aos seus parceiros fornecedores: não permita que os hackers tenham acesso fácil



Torne os dados do seu cartão inúteis para criminosos



Use um leitor de cartão seguro e um dispositivo de digitação de PIN



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

Observe que há um risco ainda maior se a aceitação do pagamento móvel for feita por uma rede Wi-Fi pública desprotegida pois os criminosos conseguem roubar seus dados de cartão por meio de redes sem segurança.

SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

Um “terminal virtual” é uma página da Web acessada pelo comerciante, usando, por exemplo, um computador ou um tablet

O comerciante insere manualmente os dados de cartões no navegador da Web no terminal virtual

Para comerciantes sem um terminal de pagamento tradicional. Eles inserem as transações manualmente, uma a uma, e geralmente têm baixo volume de transações de pagamento (por exemplo, aqueles que fazem vendas desde casa)

PC DO COMERCIANTE



Não há leitores de cartões ou terminais conectados ao dispositivo ou rede do comerciante

TELEFONE/TABLET DO COMERCIANTE



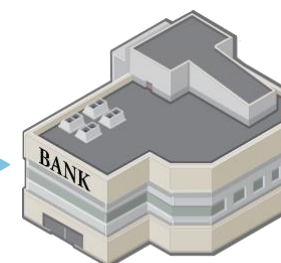
ROTEADOR/FIREWALL



TERMINAL VIRTUAL DE UM PROCESSADOR DE PAGAMENTO EM CONFORMIDADE COM O PCI DSS




O adquirente ou o processador de pagamento de terceiros fornece o serviço de pagamento virtual



INTERNET

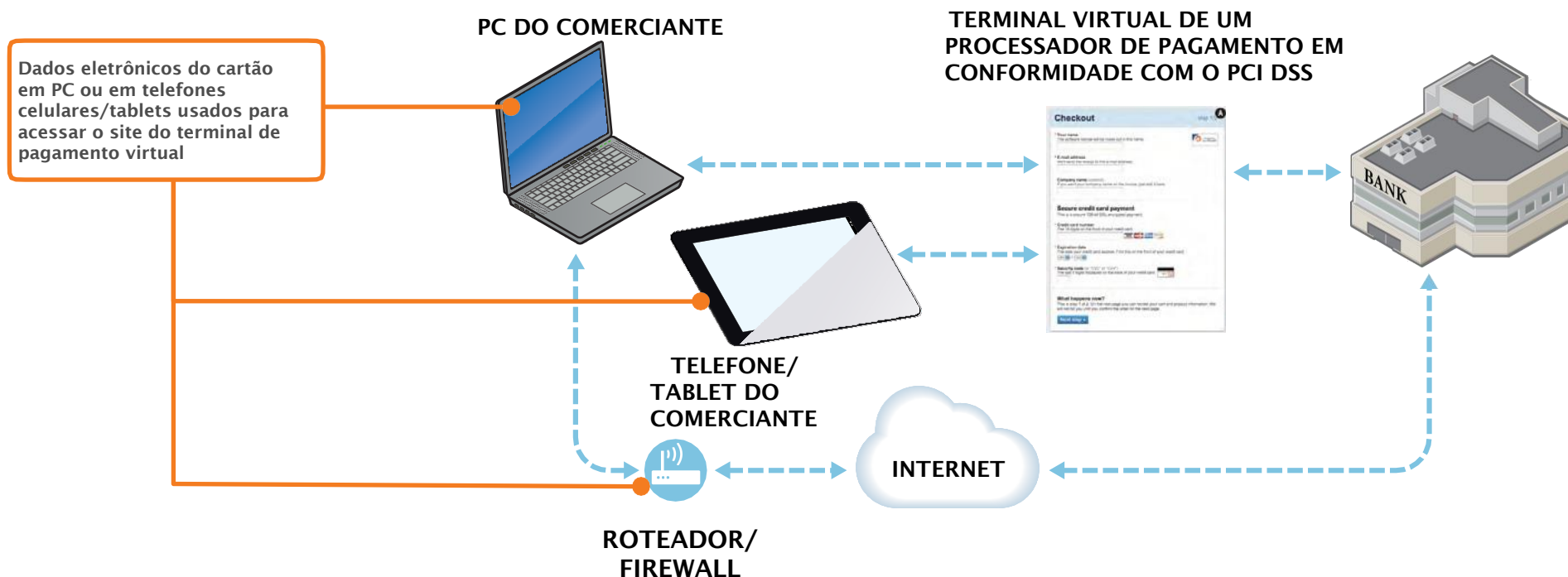


Para este cenário, os riscos para os dados de cartões estão presentes em  acima. Riscos explicados na próxima página.

Terminal de pagamento virtual acessado via navegador da Internet do comerciante. Pagamentos enviados via Internet.



Onde os dados de cartão estão em risco?



Terminal de pagamento virtual acessado via navegador da Internet do comerciante. Pagamentos enviados via Internet.



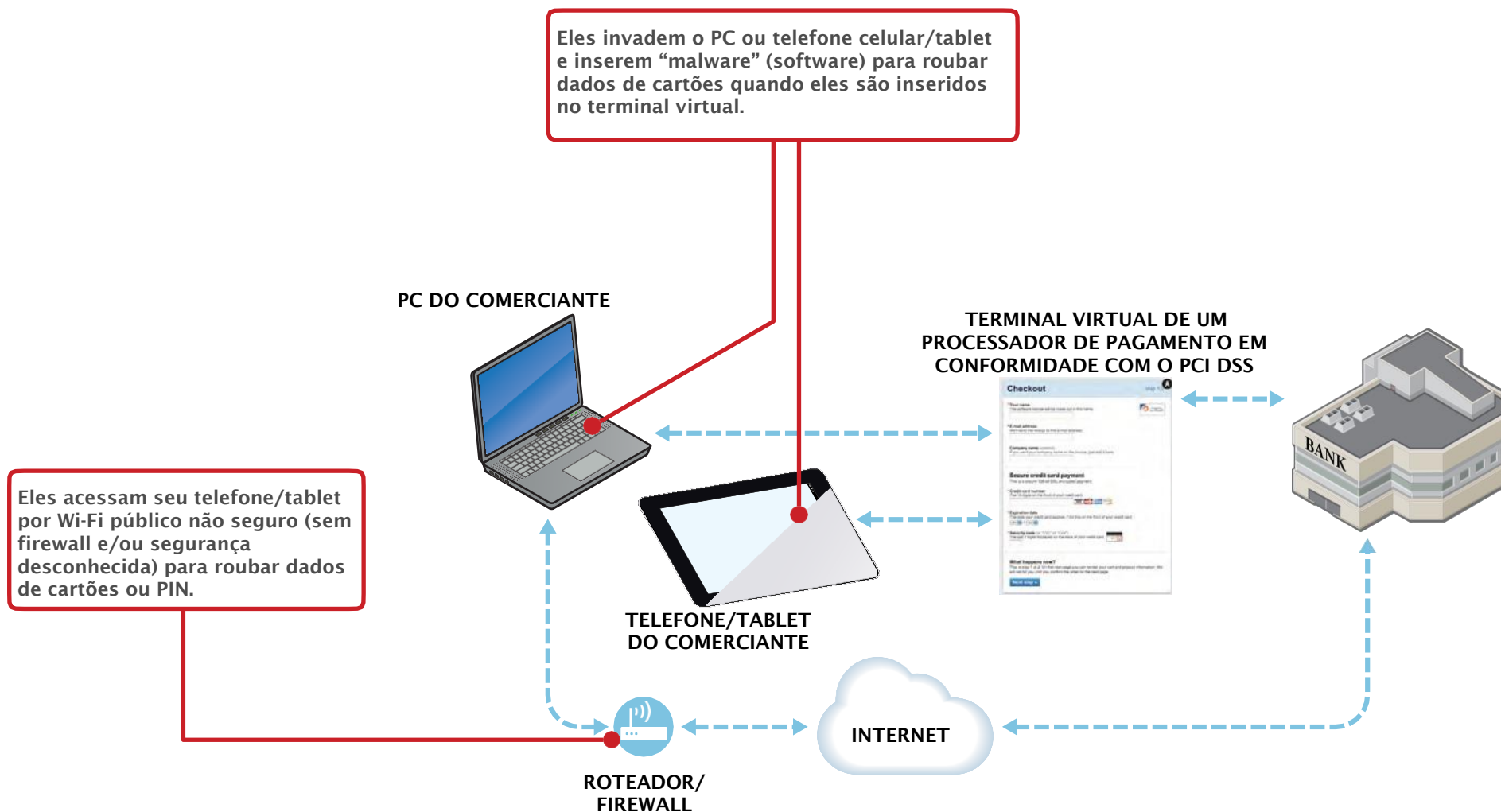
TIPO 14 - VISÃO GERAL

TIPO 14 - RISCOS

TIPO 14 - AMEAÇAS

TIPO 14 - PROTEÇÕES

Como os criminosos obtêm os dados de cartão?



Terminal de pagamento virtual acessado via navegador da Internet do comerciante. Pagamentos enviados via Internet.



TIPO 14 - VISÃO GERAL

TIPO 14 - RISCOS

TIPO 14 - AMEAÇAS

TIPO 14 - PROTEÇÕES

Como você pode começar a proteger dados de cartões hoje mesmo?*



Use senhas fortes



Instale os patches de seu fornecedor de terminal de pagamento



Peça ajuda aos seus parceiros fornecedores, se precisar



Limite o acesso remoto aos seus parceiros fornecedores: não permita que os hackers tenham acesso fácil



Use software antivírus



Faça varreduras regulares de vulnerabilidade



Use um firewall (ou software de firewall pessoal se estiver usando Wi-Fi público)

PC DO COMERCIANTE



TERMINAL VIRTUAL DE UM PROCESSADOR DE PAGAMENTO EM CONFORMIDADE COM O PCI DSS



TELEFONE/TABLET DO COMERCIANTE



INTERNET

ROTEADOR/
FIREWALL

*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

A solução está incluída na Lista de soluções P2PE validadas pelo PCI (dica: consulte o manual de instruções P2PE do provedor de soluções em busca do nome da solução).

O comerciante implementa todos os controles no Manual de instrução P2PE (PIM) fornecido pelo provedor de solução P2PE

Todo o armazenamento, processamento ou transmissão de dados de cartão para este canal fica dentro do terminal de pagamento aprovado pelo PCI.

MANUAL DE INSTRUÇÕES P2PE (PIM)
(FORNECIDO PELO PROVEDOR DE SOLUÇÕES P2PE)



TERMINAL DE PAGAMENTO
(FORNECIDO PELO PROVEDOR DE SOLUÇÕES P2PE)



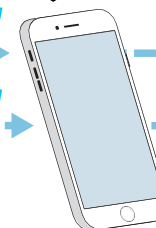
DISPOSITIVO DE DIGITAÇÃO DE PIN E/OU LEITORES SEGUROS DE CARTÕES
(FORNECIDO PELO PROVEDOR DE SOLUÇÕES P2PE)



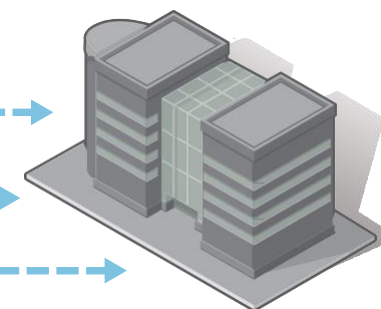
O ambiente de pagamento do comerciante pode incluir outras caixas/gavetas registradoras eletrônicas etc.

Dados criptografados da conta

Dados criptografados da conta



CELULAR OU TABLET



PROVEDOR DE SOLUÇÕES P2PE LISTADO NO SITE DO PCI SSC

RESPONSABILIDADE DO COMERCIANTE

SIM

Este é o meu sistema de pagamento e eu analisei as abas de Riscos, Ameaças e Proteções. Estou pronto para baixar o formulário de avaliação no meu computador agora para entender como posso proteger melhor o meu negócio.

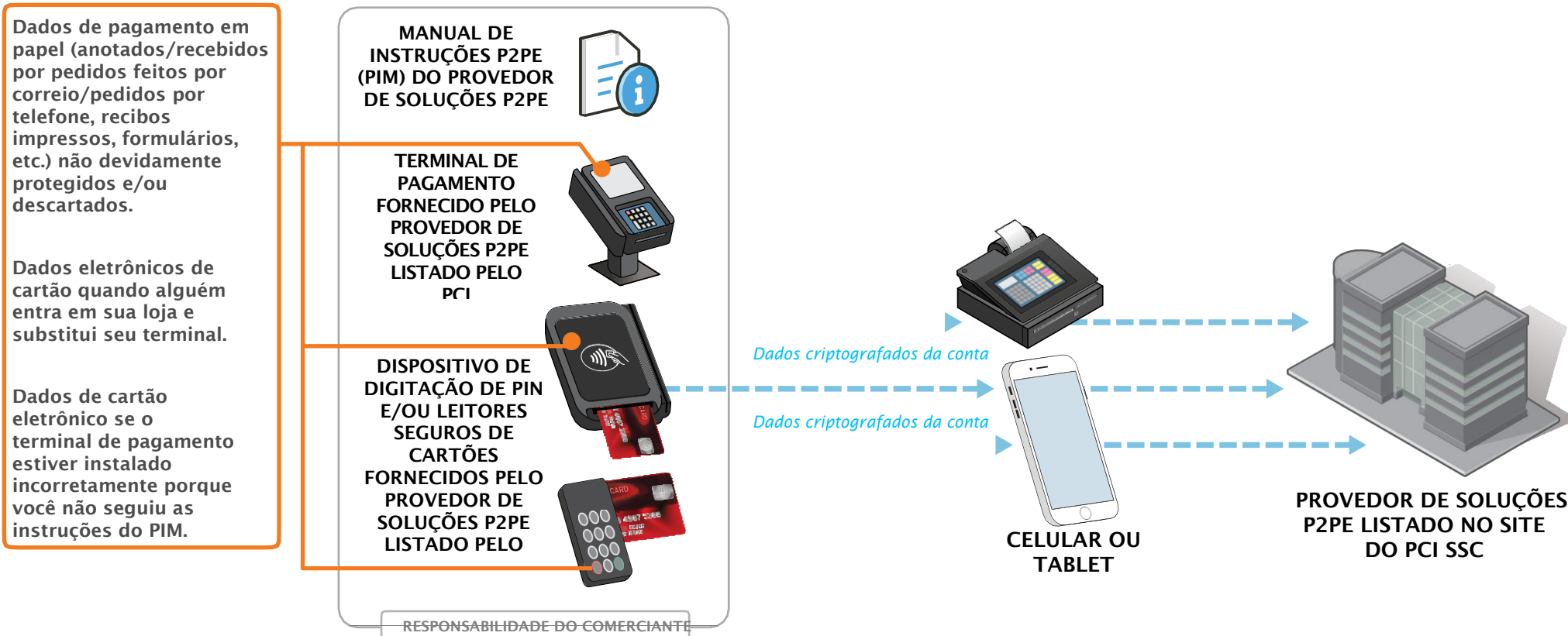
NÃO

Não tenho certeza se este é meu sistema de pagamento. Mostre-me o panorama novamente

Para este cenário, os riscos para os dados de cartões estão presentes em ! acima. Riscos explicados na próxima página.



Onde os dados de cartão estão em risco?



Como os criminosos obtêm os dados de cartão?

Eles roubam os dados do cartão registrados em papel (anotados/recebidos de pedidos feitos pelo correio/pedidos por telefone, recibos impressos, formulários, etc.)

Eles furtam seu terminal, substituindo-o por um terminal modificado usado para obter seus dados de cartões.

Eles roubam seus dados de cartão por meio de fragilidades existentes porque você não seguiu o manual de instruções P2PE

MANUAL DE INSTRUÇÕES P2PE (PIM) DO PROVEDOR DE SOLUÇÕES P2PE



TERMINAL DE PAGAMENTO FORNECIDO PELO PROVEDOR DE SOLUÇÕES P2PE LISTADO PELO PCI



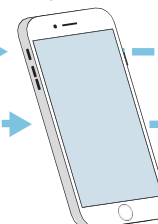
DISPOSITIVO DE DIGITAÇÃO DE PIN E/OU LEITORES SEGUROS DE CARTÕES FORNECIDOS PELO PROVEDOR DE SOLUÇÕES P2PE LISTADO PELO PCI



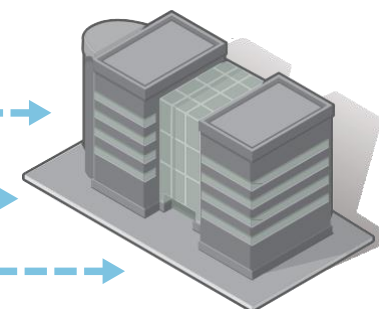
RESPONSABILIDADE DO COMERCIANTE

Dados criptografados da conta

Dados criptografados da conta








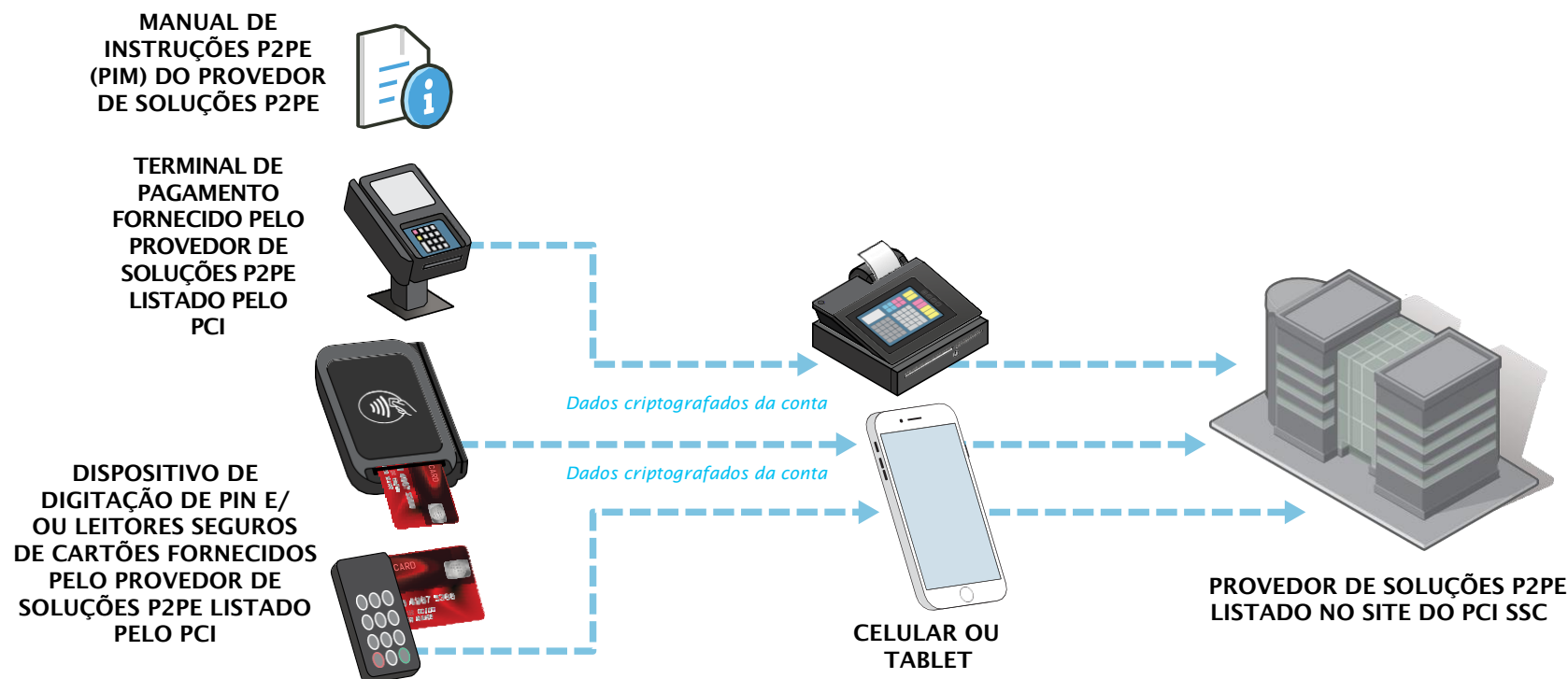
CELULAR OU TABLET



PROVEDOR DE SOLUÇÕES P2PE LISTADO NO SITE DO PCI SSC

Como você pode começar a proteger dados de cartões hoje mesmo?*

-  Proteja os dados de cartões e armazene apenas o necessário
-  Inspeção seus terminais de pagamento para ver se há danos ou mudanças
-  Peça ajuda aos seus parceiros fornecedores, se precisar
-  Proteja o acesso interno aos dados de cartão
-  Torne os dados do seu cartão inúteis para criminosos



*Clique nos ícones acima para ser direcionado ao [Guia para pagamentos seguros](#) e obter informações sobre esses princípios básicos de segurança. Para definições simples dos termos de pagamento e segurança, consulte nosso Glossário.

Recursos

Infográficos e vídeos

Recurso	Link	URL
Infográfico: Acesso remoto	https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Secure-Remote-Access.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	
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: Noções básicas de firewall do PCI	https://www.pcisecuritystandards.org/pdfs/Small-Merchant-Firewall-Basics.pdf	
Infográfico: Patches	https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Patching.pdf	
Infográfico: Senhas	https://www.pcisecuritystandards.org/documents/Payment-Data-Security-Essential-Strong-Passwords.pdf	
Vídeo: Acesso remoto	https://www.youtube.com/watch?v=MxgSNFqvAVc	
Vídeo: Learn Password Security in 2 Minutes (Aprenda sobre segurança da senha em 2 minutos)	https://www.youtube.com/watch?v=FsrOXgZKa7U	
Vídeo: Patches	https://www.youtube.com/watch?v=0NGz1mGO3Jg	
Vídeo: Senhas	https://www.youtube.com/watch?v=dNVQk65KL8g	

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

Recurso	Link	URL
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	
Glossário para pequenos comerciantes	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf	
Pequenos comerciantes - Perguntas para fornecedores	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf	
Sistemas comuns de pagamento	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf	