Glossário de termos de segurança da informação e pagamentos

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

VERSÃO 2.0 | AGOSTO DE 2018

PCI Security Standards Council®

Introdução

Este *Glossário de termos de segurança da informação e pagamentos* é um suplemento ao *Guia para pagamentos seguros*, parte dos Fundamentos da segurança de dados para pequenos comerciantes. Seu objetivo é explicar os termos relevantes de segurança da informação e da Indústria de cartões de pagamento (PCI, Payment Card Industry) de maneira fácil de entender.

As definições dos termos marcados com um asterisco (*) baseiam-se nas, ou são derivadas das, definições do documento *Padrão de segurança de dados (DSS, Data Security Standard) da Indústria de cartão de pagamento (PCI, Payment Card Industry) e Padrão de segurança de dados de aplicativos de pagamento (PA-DSS, Payment Application Data Security Standard): Glossário de termos, abreviações e acrônimos*. A versão mais recente deste glossário é considerada a fonte oficial de termos, por isso as definições atuais e completas do PCI DSS e do PA-DSS devem ser consultadas nesse documento.

Consulte os Fundamentos da segurança de dados para pequenos comerciantes disponíveis em:

RECURSO	URL
Ferramenta de avaliação	https://www.pcisecuritystandards.org/merchants/ Esta ferramenta é disponibilizada apenas para informação do comerciante. Uma opção para os comerciantes é usá-la como um primeiro passo para obter perspectivas sobre práticas de segurança pertinentes à forma com que aceitam pagamentos a fim de lhes propiciar respostas iniciais e lhes permitirem a visualização de seus resultados.
Guia para Pagamentos Seguros	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Perguntas que você deve fazer aos seus 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

Glossário

TERMO	DEFINIÇÃO
Abuso de privilégio	Uso de privilégios de acesso ao sistema computacional de maneira abusiva. Entre os exemplos estão um administrador de sistema que acesse dados de cartões para propósitos mal-intencionados ou alguém que roube e use os privilégios de acesso elevados do administrador para propósitos mal-intencionados.
Aceitação de pagamento móvel	Uso de um dispositivo móvel para aceitar e processar transações de pagamento. O dispositivo móvel geralmente é emparelhado com um acessório leitor de cartão comercialmente disponível.
Acesso remoto*	Acesso a uma rede de computadores a partir um local externo dessa rede. Conexões de acesso remoto podem ser originadas de dentro da rede da empresa ou em um local remoto. Um exemplo de tecnologia para acesso remoto é a de rede privada virtual (VPN). O acesso remoto pode ser interno (por exemplo, suporte de TI) ou externo (por exemplo, prestadores de serviços, agentes de terceiros, integradores/revendedores).
Adquirente*	Consulte *Banco comercial* e *Processador de pagamento*.
Aplicativo de pagamento validado pelo PCI	Aplicativo de software que foi validado de acordo com o padrão de segurança de dados de aplicativos de pagamento do PCI (PA-DSS) e está listado no site do PCI Council.
Aplicativo de pagamento*	Relacionado ao PA-DSS, um aplicativo de software que armazena, processa ou transmite dados do portador do cartão como parte da autorização ou liquidação de transações de pagamento.
Aplicativo*	Programa de software (ou grupo de programas) executado em um PC, smartphone, tablet, servidor interno ou servidor da Web.
Assessor de segurança qualificado (QSA)*	Uma empresa aprovada pelo PCI Security Standards Council para validar a adesão de uma entidade aos requisitos do PCI DSS.
Ataque cibernético	Qualquer ação ofensiva para entrar em um computador ou em um sistema. Ataques cibernéticos englobam a instalação de spyware em um PC, a invasão de um sistema de pagamento para roubar dados de cartão ou a tentativa de danificar algum elemento de infraestrutura essencial, como uma rede de energia elétrica.
Autenticação*	Método para verificar a identidade de pessoa, dispositivo ou processo que está tentando acessar um computador. Para confirmar que a identidade/usuário é válido, um ou mais dos seguintes elementos são informados: • Senha ou frase secreta (algo que o usuário saiba) • Token, smart card ou certificado digital exclusivo do usuário (algo que o usuário tenha) • Identificador biométrico, como uma impressão digital (algo que o usuário seja ou faça)
Autenticação forte	Tipo de autenticação usada para verificar a identidade de um usuário ou dispositivo para garantir a segurança do sistema. O termo autenticação forte refere-se, muitas vezes, a autenticação de múltiplos fatores (MFA, multifactor authentication).

Glossário

TERMO	DEFINIÇÃO
Autenticação multifatorial*	Método de autenticação de usuários no qual são verificados dois ou mais fatores. Os fatores incluem algo da posse do usuário (como smart card ou dongle), algo do conhecimento do usuário (como senha, frase de senha ou PIN) ou algo que o usuário seja ou faça (como impressão digital, outras formas de biometria etc.).
Autorização*	Em uma transação com cartão de pagamento, a autorização ocorre quando um comerciante recebe a aprovação de transação após o adquirente validá-la com o emissor/processador.
Banco comercial*	Um banco ou uma instituição financeira que processa pagamentos com cartão de crédito e/ou débito em nome de comerciantes. Também chamado de “adquirente”, “banco adquirente”, “processador de cartões” ou “processador de pagamento”. Consulte também *Processador de pagamento*.
Caixa registradora eletrônica (ECR, Electronic Cash Register)	Um dispositivo que registra e calcula transações e pode imprimir recibos, mas não aceita pagamentos com cartão do cliente. Também chamada de “gaveta”.
Chip	Também conhecido como “chip EMV”. É o microprocessador (ou “chip”) de um cartão de pagamento usado no processamento de transações de acordo com as especificações internacionais para transações EMV.
Chip e assinatura	Um processo de verificação em que um consumidor usa sua assinatura em um terminal de pagamento habilitado para chip EMV ao comprar bens ou serviços.
Chip e PIN	Um processo de verificação em que um consumidor digita seu PIN em um terminal de pagamento habilitado para chip EMV ao comprar bens ou serviços.
Clonagem	Roubo de dados do cartão diretamente do cartão de pagamento do consumidor ou da infraestrutura de pagamento em um estabelecimento comercial, usando, por exemplo, um leitor de cartão portátil não autorizado ou modificações feitas no terminal de pagamento do comerciante. A finalidade desse procedimento é cometer fraudes. A ameaça é séria e pode atingir o ambiente de qualquer comerciante.
Conforme ao PCI DSS	Em conformidade com todos os requisitos aplicáveis do PCI DSS atual, de maneira contínua por meio de uma abordagem de atividades de rotina. A conformidade é avaliada e validada em um único momento; no entanto, cabe a cada comerciante seguir continuamente os requisitos a fim de oferecer uma segurança robusta. Os bancos comerciais e/ou as marcas de pagamento podem ter requisitos para validação formal anual da conformidade com o PCI DSS.
Credencial	Informações usadas para identificar e autenticar um usuário para permitir o acesso a um sistema. Geralmente consistem no nome de usuário e senha. Outras formas de credenciais são impressão digital, verificação de retina ou um número de uso único gerado por um “gerador de token” portátil. Quanto mais credenciais um acesso requer, mas seguro ele é.
Conforme ao PCI DSS	Em conformidade com todos os requisitos aplicáveis do PCI DSS atual, de maneira contínua por meio de uma abordagem de atividades de rotina. A conformidade é avaliada e validada em um único momento; no entanto, cabe a cada comerciante seguir continuamente os requisitos a fim de oferecer uma segurança robusta. Os bancos comerciais e/ou as marcas de pagamento podem ter requisitos para validação formal anual da conformidade com o PCI DSS.

Glossário

TERMO	DEFINIÇÃO
Credencial	Informações usadas para identificar e autenticar um usuário para permitir o acesso a um sistema. Geralmente consistem no nome de usuário e senha. Outras formas de credenciais são impressão digital, verificação de retina ou um número de uso único gerado por um "gerador de token" portátil. Quanto mais credenciais um acesso requer, mas seguro ele é.
Criptografia	A criptografia é o método usado para proteger dados tornando-os ininteligíveis para um humano ou um computador. A criptografia só é útil quando o destinatário pretendido consegue reagrupar os dados em um formato legível usando um método conhecido apenas pelo remetente e pelo receptor. Consulte também *Encriptação*.
Dados de autenticação confidenciais*	Informações relacionadas à segurança usadas para autenticar portadores de cartões e/ou autorizar transações de cartões de pagamento, armazenadas na faixa magnética ou no chip do cartão.
Dados do cartão/dados do cartão do cliente*	Os dados de cartões incluem, no mínimo, o número da conta principal (PAN), e também podem incluir o nome do portador do cartão e a data de validade. O PAN está visível na parte frontal do cartão e é codificado na faixa magnética do cartão e/ou no chip incorporado. Também conhecidos como dados do portador do cartão. Consulte *Dados de autenticação confidenciais* para saber sobre elementos de dados adicionais que podem fazer parte de uma transação de pagamento, mas que não devem ser armazenados após a autorização da transação.
Dados não criptografados	Quaisquer dados que sejam legíveis sem a necessidade de descriptografia. Também chamados de dados de "texto sem formatação" e "texto simples".
Dispositivo de clonagem	Dispositivo físico, geralmente integrado a um dispositivo de leitura de cartão, projetado para capturar ilegitimamente as transações e/ou armazenar informações de um cartão de crédito. Também chamado de "clonador de cartão".
Dispositivo móvel	Dispositivos como smartphones e tablets pequenos que são portáteis e capazes de se conectar a redes de computadores sem fio.
Encriptação	Processo de utilização de criptografia para converter matematicamente informações em um formato inutilizável, exceto para detentores de uma chave digital específica. O uso da criptografia protege as informações as eliminar seu valor para os criminosos. Consulte também *Criptografia*.
Firewall	Hardware e/ou software que protege os recursos de rede contra acesso não autorizado. Um firewall permite ou nega a comunicação entre computadores ou redes com diferentes níveis de segurança com base em um conjunto de regras e outros critérios.
Fornecedor	Uma entidade de negócios que fornece a um comerciante um produto ou serviço necessário para o curso dos negócios. Quando são oferecidos serviços, o fornecedor pode ser considerado um prestador de serviços e pode exigir acesso a locais físicos ou sistemas computacionais dentro do ambiente do comerciante que podem afetar a segurança dos dados de cartões. Consulte também *Prestador de serviços*.

Glossário

TERMO	DEFINIÇÃO
Fornecedor de Varredura Aprovado (ASV)	Empresa aprovada pelo Conselho dos Padrões de Segurança PCI para conduzir serviços de verificação de vulnerabilidades externas para identificar deficiências comuns na configuração do sistema.
Fornecedor do aplicativo de pagamento	Fornecedor que vende aplicativos que armazenam, processam e/ou transmitem dados de cartões durante transações de pagamento.
Fornecedor do sistema de pagamento	Um fornecedor que vende, licencia ou distribui uma solução de pagamento completa para um comerciante. A solução abrange o hardware e o software necessários para lidar com pagamentos dentro da loja e fornece um método para se conectar a um processador de pagamento.
Fundamentos da segurança de dados (DSE, Data Security Essentials)	Fundamentos da segurança de dados para pequenos comerciantes é um conjunto de recursos educacionais e uma ferramenta de avaliação usada para ajudar os comerciantes a simplificar sua segurança e a reduzir seus riscos. O DSE destina-se a uma abordagem alternativa aos Questionários de autoavaliação (SAQs, Self-Assessment Questionnaires) do PCI DSS para os comerciantes considerados elegíveis pelas marcas de pagamento e seus adquirentes (bancos comerciais).
Gaveta	Consulte *Caixa registradora eletrônica*.
Hacker	Uma pessoa ou organização que tenta contornar medidas de segurança de sistemas computacionais para obter controle e acesso. Normalmente, isso é feito com o intuito de roubar dados de cartões.
Integrador/revendedor	Integrador/revendedor é uma empresa com a qual os comerciantes trabalham para ajudar na configuração de seu sistema de pagamento. Podem estar incluídos instalação, configuração e suporte. Essas empresas também podem vender os dispositivos ou aplicativos de pagamento como parte de seu serviço. Consulte também *Integrador e revendedor qualificado (QIR, Qualified Integrator Reseller)*.
Investigador forense	Investigadores forenses do PCI (PFIs) são empresas aprovadas pelo PCI Council para ajudar a determinar quando e como ocorreu uma violação de dados de cartões. Eles realizam investigações dentro do setor financeiro usando metodologias e ferramentas de investigação comprovadas. Também trabalham em conjunto com agências de cumprimento da lei para apoiar as partes interessadas com quaisquer investigações criminais resultantes.
Leitor de cartão seguro (SCR)	Um dispositivo aprovado por PTS que se conecta a um telefone celular ou tablet para aceitar cartões de pagamento com segurança. SCRs aprovados pelo PCI PTS protegem e criptografam os dados de cartões via SRED. Consulte também *SRED*.
Log*	Um arquivo criado automaticamente quando determinados eventos predefinidos (geralmente relacionados à segurança) ocorrem em um sistema computacional ou rede. Os dados de logs incluem carimbo de data/hora, descrição do evento e informações exclusivas do evento. Esses arquivos são úteis para solução de problemas técnicos ou para investigações de violação de dados. O log também é chamado de “log de auditoria” ou “trilha de auditoria”.
Malware*	Software malicioso projetado para infiltrar um sistema computacional com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans (ou cavalos de Troia), spyware, adware e rootkits.

Glossário

TERMO	DEFINIÇÃO
Middleware de pagamento	Um termo geral para software que conecta dois ou mais aplicativos de pagamento, talvez não relacionados. Por exemplo, ele pode passar os dados de cartões entre um aplicativo em um terminal de pagamento e outros sistemas de comerciante que enviam dados de cartões para um processador.
Necessidade empresarial de conhecer	Princípio que consiste em conceder o acesso a sistemas ou dados com base na necessidade empresarial do usuário, ou seja, considerando somente o que é necessário para a função do cargo de um usuário.
Número da conta primária (PAN)*	Número exclusivo para cartões de crédito e débito que identifica a conta do portador do cartão.
Número de identificação bancária (BIN)	Os seis primeiros dígitos (ou mais) de um número de cartão de pagamento usados para identificar a instituição financeira que emitiu o cartão de pagamento para o portador do cartão.
P2PE	Acrônimo do padrão de encriptação de ponto a ponto do Conselho dos Padrões de Segurança da PCI. Consulte os detalhes em www.pcisecuritystandards.org.
PA-DSS*	Acrônimo de “Payment Application Data Security Standard” (padrão de segurança de dados de aplicativos de pagamento) do Conselho dos Padrões de Segurança da PCI. Consulte os detalhes em www.pcisecuritystandards.org.
Pagamento recorrente	Um método de faturamento em que os comerciantes faturam seus clientes repetidamente ao longo do tempo; é o caso, por exemplo, de associações ou assinaturas mensais. Uma maneira segura de fazer isso é exigir que o adquirente/processador use tokens para os dados do cartão, o que garante proteção desses dados e isenta o comerciante dessa responsabilidade.
Patch*	Atualização de software existente que agrega uma funcionalidade ou corrige um defeito (ou “bug”).
PCI DSS*	Acrônimo de “Payment Card Industry Data Security Standard” (padrão de segurança de dados da indústria de cartão de pagamento) do PCI Council. Consulte os detalhes em www.pcisecuritystandards.org.
PCI*	Acrônimo de “Payment Card Industry” (indústria de cartão de pagamento).
PED*	Acrônimo de “PIN Entry Device” (dispositivo de entrada de PIN). Teclado em que o cliente digita seu PIN. Também chamado de “teclado de PIN”.
Pequeno comerciante	Um pequeno comerciante é normalmente um negócio de propriedade e operação independentes com um único ou poucos estabelecimentos, com orçamento de TI limitado ou até mesmo ausente, muitas vezes sem equipe de TI. A necessidade de conformidade do pequeno comerciante com a PCI é determinada pela marca de pagamento ou pelo adquirente (banco comercial).
PIN*	Acrônimo de “Personal Identification Number” (número de identificação pessoal). Um número exclusivo conhecido somente pelo usuário e pelo sistema para a autenticação do usuário no sistema. PINs comuns são usados em caixas automáticos para transações de adiantamento em dinheiro ou para cartões com chip EMV para substituir a assinatura de um portador de cartão. Os PINs ajudam a determinar se um portador de cartão está autorizado a usar o cartão, além disso, ajuda a impedir o uso não autorizado se o cartão for roubado.

Glossário

TERMO	DEFINIÇÃO
Prestador de serviços*	Uma entidade comercial que fornece vários serviços aos comerciantes. Geralmente, essas entidades armazenam, processam ou transmitem dados de cartões em nome de outra entidade (como um comerciante) OU são prestadores de serviços gerenciados que fornecem firewalls gerenciados, detecção de intrusão, hospedagem e outros serviços relacionados a TI. Também chamado de "fornecedor".
Processador de pagamento*	Entidade engajada por comerciantes para lidar com transações de cartão de pagamento como representante deles. Embora normalmente ofereçam serviços de aquisição, os processadores de pagamento não são considerados adquirentes (bancos comerciais), a menos que definidos como tal pela marca do cartão de pagamento. Também chamado de "aplicativo de pagamento" ou "prestador de serviços de pagamento" (PSP). Consulte também *Banco comercial*.
Provedor de hospedagem*	Oferece vários serviços aos comerciantes e outros prestadores de serviços, nos quais os dados de seus clientes estão "hospedados" ou residentes nos servidores do prestador. Dentre os serviços comuns, estão o espaço compartilhado para vários comerciantes em um servidor, o fornecimento de um servidor dedicado para um comerciante ou aplicativos da Web, como um site com opções de "carrinho de compras".
PTS*	Acrônimo de "PIN Transaction Security" (padrão de segurança de transação com PIN) do PCI Council. O PTS é um conjunto de requisitos de avaliação modular para terminais de ponto de interação (POI) de aceitação de PIN. Consulte os detalhes em www.pcisecuritystandards.org.
QIR*	Acrônimo de "Qualified Integrator or Reseller" (integrador ou revendedor qualificado). Os QIRs são integradores e revendedores especialmente treinados pelo Conselho dos Padrões de Segurança PCI para abordar controles críticos de segurança ao instalar sistemas de pagamento de comerciantes. Consulte os detalhes em www.pcisecuritystandards.org.
Questionário de autoavaliação (SAQ)*	Questionário que abrange um conjunto de requisitos do PCI DSS que é seguido pela própria organização a fim de se confirmar o cumprimento desses requisitos.
Rede privada virtual (VPN)*	Software que cria um canal seguro e privado para troca de dados e realização de chamadas telefônicas pela internet.
Rede*	Dois ou mais computadores conectados por meio de meios físicos ou sem fio.
Revendedor/integrador*	Entidade que vende e/ou integra aplicativos de pagamento, mas não os desenvolve.
Roteador*	Hardware ou software que conecta duas ou mais redes de computadores internas ou externas para "encaminhar" ou guiar dados através de uma rede e para garantir que os dados fluam corretamente entre essas redes. O roteador também pode proporcionar mais segurança ao permitir somente tráfego aprovado e impedir tráfego não aprovado.
Senha*	Uma palavra, frase ou sequência de caracteres usada para autenticar um usuário. Quando combinada com o nome de usuário, a senha é usada para provar a identidade do usuário, permitindo que ele acesse os recursos computacionais.

Glossário

TERMO	DEFINIÇÃO
Senha-padrão	Uma senha simples fornecida com software ou hardware novo. Senhas-padrão (como “admin”, “senha” ou “123456”) são fáceis de adivinhar e normalmente estão disponíveis por meio de pesquisa online. Elas são apenas espaços reservados para senhas personalizadas futuras, por isso não oferecem segurança real e devem ser alteradas para uma senha mais forte após a instalação de um novo software ou hardware.
Sistema de pagamento	Abrange todo o processo de aceitação de pagamentos de cartão em um estabelecimento de varejo comercial (incluindo lojas físicas e lojas de comércio eletrônico) e pode incluir terminal de pagamento, caixa registradora eletrônica, outros dispositivos ou sistemas conectados ao terminal de pagamento (por exemplo, Wi-Fi para conectividade ou um PC usado para inventário), servidores com componentes de e-commerce, como páginas de pagamento, e as conexões com um banco comercial.
Sistema operacional*	Software em um sistema de computador que fornece gerenciamento e coordenação geral das atividades do computador. Entre os exemplos estão Microsoft Windows, Apple OSX, iOS, Android, Linux e UNIX.
Software antivírus*	Programa de software que detecta, remove e protege contra softwares mal-intencionados (também chamados de “malware”), inclusive vírus, worms, cavalos de Troia, spyware, adware e rootkits. Também chamado de “software antimalware”.
Solução de criptografia de ponto a ponto listada pelo PCI	Solução de criptografia validada de acordo com o padrão de criptografia de ponto a ponto do PCI (P2PE) e listada no site do PCI Council.
SRED	Acrônimo de “Secure Reading and Exchange of Data” (leitura segura e intercâmbio de dados). Um conjunto de requisitos do PCI PTS projetados para proteger e criptografar os dados de cartões em terminais de pagamento. Soluções de criptografia de ponto a ponto listada pelo PCI Council (P2PE) devem usar um terminal de pagamento aprovado e listado pelo PTS com SRED habilitado e que esteja executando ativamente criptografia de dados de cartões.
Terminal de pagamento	Dispositivo de hardware usado para aceitar pagamentos com cartão de cliente ao deslizar, dobrar, inserir ou tocar. Também chamado de “terminal de ponto de venda (POS)”, “máquina de cartão de crédito” ou “terminal PDQ”.
Terminal de pagamento aprovado pelo PCI	Terminal de pagamento aprovado de acordo com o padrão de segurança de transação com PIN do PCI (PTS) e listado no site do PCI Council.
Terminal de pagamento integrado	Um terminal de pagamento e uma caixa registradora eletrônica em um dispositivo que recebe pagamentos, registra e calcula transações e imprime recibos.
Terminal de pagamento sem fio	Terminal de pagamento que se conecta à Internet usando qualquer uma das várias tecnologias sem fio.
Terminal de pagamento virtual*	Acesso baseado no navegador da Web ao site de um adquirente, processador ou prestador de serviços terceirizado para autorizar transações com cartão de pagamento. Diferentemente dos terminais físicos, os terminais virtuais não leem dados diretamente do cartão de pagamento. O comerciante insere manualmente os dados do cartão de pagamento no navegador da Web conectado com segurança. Como as transações com o cartão de pagamento são inseridas manualmente, os terminais de pagamento virtual são usados em vez de terminais físicos em ambientes comerciais com volumes de transação baixos.

Glossário

TERMO	DEFINIÇÃO
Terminal independente	Um terminal de pagamento que não depende de conexão com nenhum outro dispositivo dentro do ambiente do comerciante e não executa outras funções. A única exigência para sua operação é uma conexão com o processador através de uma conexão com a internet ou de uma linha telefônica. Se o terminal exigir conexão com uma caixa registadora eletrônica computorizada ou se for multifuncional (como um dispositivo móvel), ele não é um terminal independente.
Tokenização	Processo pelo qual o número da conta principal (PAN, primary account number) é substituído por um valor alternativo chamado de token. Tokens podem ser usados no lugar do PAN original para executar funções quando o cartão está ausente, como para anulações, reembolsos ou faturamento recorrente. Tokens também fornecem mais segurança no caso de roubo porque são inutilizáveis, portanto não têm valor para criminosos.
Validado pelo PCI DSS	Elementos que fornecem comprovação de que todos os requisitos aplicáveis do PCI DSS foram atendidos em um único momento. Dependendo dos requisitos específicos do banco comercial e/ou da bandeira de pagamento, a validação pode ser alcançada por meio do respectivo Questionário de autoavaliação do PCI DSS ou por um Relatório de conformidade resultante de uma avaliação no local.
Varredura de vulnerabilidades	Uma ferramenta de software que detecta e classifica possíveis pontos fracos (vulnerabilidades) em um computador ou uma rede. Deve-se executar uma varredura trimestral de vulnerabilidades externas de acordo com o Requisito 11.2.2 do PCI DSS por um fornecedor de varredura aprovado. Outras varreduras de vulnerabilidades (como varreduras internas e aquelas realizadas após alterações na rede) podem ser feitas por equipes qualificadas do departamento de TI da organização ou por um prestador de serviços de segurança (como um Fornecedor de varredura aprovado). Consulte também *Fornecedor de Varredura Aprovado (ASV).*
Violação de dados	Uma violação de dados é um incidente no qual dados confidenciais podem ter sido visualizados, roubados ou usados por uma pessoa não autorizada. Violações de dados podem envolver dados de cartões, informações pessoais de saúde (PHI), informações de identificação pessoal (PII), segredos comerciais, propriedade intelectual, etc.
Vírus	Malware que replica cópias de si mesmo para outro software ou arquivos de dados em um computador “infectado”. Após a replicação, o vírus pode executar uma ação mal-intencionada, como excluir todos os dados do computador. Um vírus pode permanecer latente e executar sua carga mais tarde, ou pode nunca desencadear uma ação mal-intencionada. O vírus que se replica reenviando-se como anexo de e-mail ou como parte de uma mensagem de rede é chamado de “worm”.
Vulnerabilidade*	Falha ou fraqueza que, se utilizada, pode resultar em comprometimento intencional ou não intencional do sistema.
Wi-Fi*	Rede sem fio que conecta computadores sem uma conexão física com fios.