

Indústria de cartões de pagamento (PCI) Padrão de segurança de dados (DSS) e Padrão de segurança de dados de aplicativos de pagamento (PA-DSS)

Glossário de termos, abreviações e acrônimos

Versão 3.2

Abril de 2016

TERMO DE RECONHECIMENTO:

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

Termo	Definição
AAA	Acrônimo de “autenticação, autorização e contabilidade” (authentication, authorization, accounting, no inglês). Protocolo para autenticar um usuário com base em sua identidade verificável, autorizando-o com base nos direitos do usuário e levando em consideração o seu consumo dos recursos de rede.
Controle de acesso	Mecanismos que limitam a disponibilidade de informação ou recursos de processamento de informação apenas para pessoas ou aplicativos autorizados.
Dados contábeis	Dados contábeis consistem em dados do titular do cartão e/ou dados de autenticação confidenciais. Consulte <i>Dados do titular do cartão</i> e <i>Dados de autenticação confidenciais</i> .
Número da conta	Consulte o <i>Número de conta principal (PAN)</i> .
Adquirente	Também chamado de “banco do comerciante”, “banco adquirente” ou “instituição financeira adquirente”. Entidade, normalmente uma instituição financeira, que processa transações em cartão de pagamento para comerciantes, a qual é definida por uma marca de pagamento como adquirente. Os adquirentes estão sujeitos às normas da marca de pagamento e aos procedimentos concernentes à conformidade do comerciante. Ver também <i>Processador de pagamento</i> .
Acesso administrativo	Aumento de privilégios em qualidade e quantidade concedidos a uma conta, para que a conta gere sistemas, redes e/ou aplicativos. O acesso administrativo pode ser atribuído a contas individuais ou a contas incorporadas pelo sistema. Contas com acesso administrativo são muitas vezes referidas como “super-usuário”, “raiz”, “administrador”, “admin”, “sysadmin” ou “supervisor-status”, a depender do sistema operacional específico e da estrutura organizacional.
Adware	Tipo de software malicioso que, quando instalado, força o computador a exibir automaticamente ou fazer download de anúncios.
AES	Abreviação de “Advanced Encryption Standard”. Cifrador de bloco usado na criptografia de chave simétrica adotada pelo NIST em novembro de 2001 como U.S. FIPS PUB 197 (ou “FIPS 197”). Consulte <i>Criptografia robusta</i> .
ANSI	Acrônimo de “American National Standards Institute”. Organização privada sem fins lucrativos que administra e coordena o sistema de avaliação de conformidade e a padronização voluntária nos Estados Unidos.
Antivírus	Programa ou software capaz de detectar, remover e proteger de diversas formas de softwares maliciosos (também chamado de “malware”), incluindo vírus, worms, Trojans ou cavalos de Troia, spyware, adware e rootkits.

Termo	Definição
AOC	Acrônimo de “atestado de conformidade” (attestation of compliance, no inglês). O AOC é um modo pelo qual os comerciantes e prestadores de serviço atestam os resultados de uma avaliação do PCI DSS, conforme documentado no Questionário de autoavaliação ou Relatório de conformidade.
AOV	Acrônimo de “atestado de validação” (attestation of validation, no inglês). O AOV é o modo pelo qual os PA-QSAs atestam os resultados de uma avaliação de PA-DSS, conforme documentado no Relatório PA-DSS de validação.
Aplicativo	Inclui todos os programas ou grupos de programas comprados e de software personalizado, incluindo aplicativos internos e externos (por exemplo, Web).
ASV	Acrônimo de “fornecedor de varredura aprovado” (Approved Scanning Vendor, no inglês). Empresa aprovada pelo PCI SSC para conduzir serviços externos de rastreamento de vulnerabilidade.
Log de auditoria	Também chamado de “trilha de auditoria”. Registro cronológico das atividades do sistema. Fornece uma trilha independentemente verificável o suficiente para permitir a reconstrução, a revisão e o exame de sequência de ambientes e atividades que têm relação ou que levam à operação, procedimento ou evento em uma transação da origem aos resultados finais.
Trilha de auditoria	Consulte <i>Log de auditoria</i> .
Autenticação	Processo de verificação de identidade de um indivíduo, dispositivo ou processo. A autenticação normalmente ocorre por meio do uso de um ou mais fatores de autenticação, por exemplo: <ul style="list-style-type: none"> ▪ Algo que você sabe, como uma senha ou frase de senha ▪ Algo que você tem, como um dispositivo de token ou um smart card ▪ Algo que você é, como a biométrica
Credenciais de autenticação	Combinação da ID de usuário ou ID de conta com os fatores de autenticação usados para autenticar um indivíduo, dispositivo ou processo.
Autorização	No contexto do controle de acesso, a autorização é a concessão de acesso ou outros direitos a um usuário, programa ou processo. A autorização define o que determinado programa ou usuário pode fazer após ser autenticado com êxito. Para os propósitos de uma transação de cartão de pagamento, a autorização ocorre quando um comerciante recebe a aprovação de transação após o adquirente validá-la com o emissor/processador.
Backup	Cópia duplicada dos dados feita para fins de arquivamento ou para proteção contra danos ou perda.

Termo	Definição
BAU	Acrônimo de “negócios como sempre” (business as usual, no inglês). BAU são as operações de negócios normais e diárias de uma organização.
Bluetooth	Protocolo sem fio usando tecnologia de comunicação de curto alcance para facilitar a transmissão de dados por curtas distâncias.
Buffer Overflow	A vulnerabilidade que é criada com o uso de métodos de codificação não seguros, nos quais um programa pode exceder o limite do buffer e gravar dados no espaço de memória adjacente. Os Buffer Overflows são usados por hackers para obter acesso não autorizado a sistemas ou dados.
Clonagem de cartão	Um dispositivo físico, geralmente integrado a um dispositivo de leitura de cartão, projetado para capturar ilegalmente as transações e/ou armazenar informações de um cartão de crédito.

Termo	Definição
<p>Código ou valor de verificação do cartão</p>	<p>Também conhecido como código ou valor de validação do cartão ou código de segurança do cartão. Refere-se a um dos seguintes: (1) dados da tarja magnética ou (2) recursos de segurança impressos.</p> <p>(1) Elemento de dados na tarja magnética do cartão que usa um processo criptográfico seguro para proteger a integridade dos dados da tarja e revela qualquer alteração ou adulteração. Referido como CAV, CVC, CVV ou CSC, dependendo da marca do cartão de pagamento. A lista a seguir apresenta os termos de cada bandeira:</p> <ul style="list-style-type: none"> ▪ CAV – Valor de autenticação do cartão (cartões de pagamento JCB) ▪ PAN CVC – Código de validação do cartão (cartões de pagamento MasterCard) ▪ CVV – Valor de verificação de cartão (cartões de pagamento Visa e Discover) ▪ CSC – Código de segurança do cartão (American Express) <p>(2) Para cartões de pagamento Discover, JCB, MasterCard e Visa, o segundo tipo de valor de verificação ou código é o valor de três dígitos à direita impresso na área do painel de assinatura, na parte de trás do cartão. Para os cartões de pagamento American Express, o código é um número de quatro dígitos em baixo relevo impresso acima do PAN, na parte frontal dos cartões de pagamento. O código é exclusivamente associado a cada peça de plástico individual e liga o PAN ao plástico. A lista a seguir apresenta os termos de cada bandeira:</p> <ul style="list-style-type: none"> ▪ CID – Número de identificação de cartão (cartões de pagamento American Express e Discover) ▪ CAV2 – Valor de autenticação do cartão 2 (cartões de pagamento JCB) ▪ PAN CVC2 – Código de validação do cartão 2 (cartões de pagamento MasterCard) ▪ CVV2 – Valor de verificação de cartão 2 (cartões de pagamento Visa)
<p>Titular do cartão</p>	<p>Consumidor ou não para o qual é emitido um cartão de pagamento ou qualquer indivíduo autorizado a usar o cartão de pagamento.</p>
<p>Dados do titular do cartão</p>	<p>No mínimo, os dados do titular do cartão consistem no PAN completo. Os dados do titular do cartão também podem aparecer na forma do PAN completo mais qualquer um dos seguintes: nome do titular do cartão, data de expiração e/ou código de serviço</p> <p>Consulte <i>Dados de autenticação confidencial</i> para elementos de dados adicionais que podem ser transmitidos ou processados (mas não armazenados) como parte da transação de pagamento.</p>

Termo	Definição
CDE	Acrônimo de “ambiente de dados do titular do cartão” (cardholder data environment, no inglês). As pessoas, processos e tecnologias que armazenam, processam ou transmitem dados do titular do cartão ou dados de autenticação confidencial.
Tecnologias de celular	As comunicações móveis por meio de redes de telefone sem fio, incluindo, entre outros, Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA) e General Packet Radio Service (GPRS).
CERT	Acrônimo de “equipe de resposta à emergência de computador” da Carnegie Mellon University (Computer Emergency Response Team, no inglês). O programa CERT desenvolve e promove o uso de tecnologia apropriada e de práticas de gerenciamento de sistemas para resistir a ataques em sistemas de rede, para limitar danos e para garantir a continuidade de serviços críticos.
Controle de mudança	Os processos e procedimentos para revisão, teste e aprovação de mudanças nos sistemas e software para impacto antes da implementação.
CIS	Acrônimo de “centro de segurança para a internet” (Center for Internet Security, no inglês). Empresa sem fins lucrativos cuja missão é ajudar organizações a reduzirem o risco de interrupções nos negócios e no comércio eletrônico resultado de controles de segurança técnicos inadequados.
Criptografia de banco de dados no nível da coluna	Técnica ou tecnologia (software ou hardware) para criptografar conteúdos de uma coluna específica em um banco de dados versus todo o conteúdo de todo o banco de dados. Como alternativa, consulte <i>Criptografia de dados</i> ou <i>Criptografia no nível do arquivo</i> .
Controles de compensação	<p>Os controles de compensação podem ser considerados quando uma entidade não atende a um requisito explicitamente, conforme publicado, devido a limitações técnicas legítimas ou de negócios documentadas, mas diminui suficientemente o risco associado ao requisito por meio da implementação de outros controles. Os controles de compensação devem:</p> <ol style="list-style-type: none"> (1) Atender à intenção e ao rigor do requisito PCI DSS original; (2) Fornecer nível similar de defesa como requisito PCI DSS original; (3) Estar “acima e além” dos outros requisitos PCI DSS (não estar simplesmente em conformidade com outros requisitos PCI DSS) e (4) Ser proporcional ao risco adicional imposto pelo não cumprimento do requisito do PCI DSS. <p>Consulte os Apêndices B e C sobre “Controles de compensação” nos <i>Procedimento de avaliação de segurança e requisitos PCI DSS</i> para obter orientação no uso de controles de compensação.</p>

Termo	Definição
Comprometimento	Também chamado de “comprometimento de dados” ou “violação de dados”. Intrusão em um sistema de computadores no qual haja suspeita de roubo/divulgação, modificação ou destruição não autorizada dos dados do titular do cartão.
Console	Tela e teclado que permitem acesso e controle de um servidor, computador mainframe ou outro tipo de sistema em um ambiente de rede.
Consumidor	Indivíduo que compra mercadorias, serviços ou ambos.
Sistemas críticos/tecnologias críticas	Sistema ou tecnologia considerada com particular importância pela entidade. Por exemplo, um sistema crítico pode ser essencial para o desempenho de uma operação comercial ou para manutenção de uma função de segurança. Exemplos de sistemas críticos geralmente incluem sistemas de segurança, sistemas e dispositivos voltados ao público, bancos de dados e sistemas que armazenam, processam ou transmitem dados do titular do cartão. Considerações para determinar quais são as tecnologias e os sistemas específicos críticos dependerá da estratégia de avaliação de risco e do ambiente da organização.
Falsificação de solicitação entre sites (CSRF)	A vulnerabilidade que é criada a partir de métodos de codificação não seguros, que permite a execução de ações indesejáveis por meio de uma sessão autenticada. Geralmente usado em conjunto com o XSS e/ou injeção SQL.
Script entre sites (XSS)	A vulnerabilidade que é criada a partir de técnicas de codificação não seguras, resultando em validação de saída inadequada. Geralmente usado em conjunto com CSRF e/ou injeção SQL.
Chave de criptografia	Um valor que determina a saída de um algoritmo de criptografia ao transformar texto simples em texto cifrado. O comprimento da chave geralmente determina o quanto será difícil descriptografar o texto cifrado em uma determinada mensagem. Consulte <i>Criptografia robusta</i> .

Termo	Definição
Geração de chave criptográfica	<p>Geração de chave é uma das funções pertencentes ao gerenciamento de chaves. Os seguintes documentos fornecem orientação reconhecida para a geração de chave adequada:</p> <ul style="list-style-type: none"> • Publicação Especial NIST 800-133: Recomendação para geração de chave criptográfica • Serviços financeiros ISO 11568-2 — gerenciamento de chaves (varejo) — Parte 2: Cifras simétricas, gerenciamento de chaves e ciclo de vida <ul style="list-style-type: none"> ○ 4.3 Geração de chave • Serviços financeiros ISO 11568-4 — gerenciamento de chaves (varejo) — Parte 4: Sistemas criptográficos assimétricos — gerenciamento de chaves e ciclo de vida <ul style="list-style-type: none"> ○ 6.2 Principais estágios do ciclo de vida — geração • Diretrizes do Conselho Europeu de Pagamentos EPC 342-08 sobre o uso de algoritmos e o gerenciamento de chaves <ul style="list-style-type: none"> ○ 6.1.1 Geração de chave [para algoritmos simétricos] ○ 6.2.1 Geração de chave [para algoritmos assimétricos]
Gerenciamento de chave de criptografia	<p>O conjunto de processos e mecanismos que suporta o estabelecimento e a manutenção da chave de criptografia, incluindo a substituição de chaves mais antigas pelas novas chaves, conforme necessário.</p>
Criptografia	<p>Disciplina de matemática e ciência da computação a respeito de segurança de informações, criptografia e autenticação, em especial. Em aplicativos e segurança de rede, é uma ferramenta para controle de acesso, confidencialidade de informações e integridade.</p>
Cryptoperiod	<p>O intervalo de tempo durante uma chave criptográfica específica que pode ser usado para um propósito definido baseado, por exemplo, no período de tempo estabelecido e/ou na quantidade de texto cifrado produzida, de acordo com as práticas e diretrizes recomendadas pelo setor (por exemplo, <i>Publicação Especial NIST 800-57</i>).</p>
CVSS	<p>Acrônimo de “sistema de pontuação de vulnerabilidade comum” (Common Vulnerability Scoring System, no inglês). Um padrão de setor aberto e agnóstico do fornecedor, projetado para comunicar a severidade das vulnerabilidades de segurança do sistema do computador e ajudar a determinar a urgência e a prioridade de resposta. Consulte o <i>Guia do programa ASV</i> para obter mais informações.</p>
Diagrama de fluxo de dados	<p>Um diagrama que mostra como os dados fluem por meio de um aplicativo, sistema ou rede.</p>
Banco de dados	<p>Formato estruturado de organização e manutenção de informação facilmente recuperáveis. Exemplos simples de bancos de dados são tabelas e planilhas.</p>
Administrador de banco de dados	<p>Também chamado de “DBA”. Pessoa responsável por gerenciar e administrar banco de dados.</p>

Termo	Definição
Contas padrão	Conta de logon predefinida no sistema, aplicativo ou dispositivo para permitir acesso inicial quando o sistema é iniciado. Contas padrão adicionais também podem ser geradas pelo sistema, como parte do processo de instalação.
Senha padrão	Senha do administrador do sistema, do usuário e contas de serviço predefinida no sistema, aplicativo ou dispositivo; normalmente associada à conta padrão. As contas e senhas-padrão são publicadas e conhecidas, por isso mesmo facilmente descobertas.
Desmagnetização	Também chamada de “desmagnetização de disco”. Processo ou técnica que desmagnetiza o disco, de forma que todos os dados armazenados nele sejam permanentemente destruídos.
Dependência	No contexto de PA-DSS, uma dependência é um software específico ou componente de hardware (como um terminal de hardware, banco de dados, sistema operacional, API, biblioteca de códigos, etc.) que é necessário para o aplicativo de pagamento atender aos requisitos de PA-DSS.
Criptografia de disco	Técnica ou tecnologia (software ou hardware) para criptografar todos os dados armazenados em um dispositivo (por exemplo, um disco rígido ou pen drive). Como alternativa, a <i>criptografia no nível do arquivo</i> ou <i>criptografia do banco de dados no nível da coluna</i> é usada para criptografar conteúdos de arquivos ou colunas específicos.
DMZ	Abreviação de “zona desmilitarizada” (demilitarized zone, no inglês). Sub-rede física ou lógica que fornece uma camada adicional de segurança à rede privada interna de uma organização. A DMZ adiciona uma camada adicional de segurança de rede entre a Internet e a rede interna da empresa, para que as partes externas tenham apenas conexão direta com dispositivos do DMZ, em vez de toda a rede interna.
DNS	Acrônimo de “sistema de nome de domínio” ou “servidor de nome de domínio” (domain name system ou domain name server, no inglês). Um sistema que armazena informações associadas aos nomes de domínio em um banco de dados distribuído para fornecer serviços de resolução de nomes aos usuários em redes como a internet.
DSS	Acrônimo de “padrão de segurança de dados” (Data Security Standard, no inglês). Consulte <i>PA-DSS</i> e <i>PCI DSS</i> .
Controle duplo	Processo do uso de duas ou mais entidades separadas (geralmente pessoas) operando juntas para proteger funções sensíveis ou informações. As duas entidades têm responsabilidade igual pela proteção física dos materiais envolvidos em transações vulneráveis. Nenhuma pessoa sozinha tem autorização para acessar ou usar os materiais (por exemplo, a chave criptográfica). Para geração de chaves manual, transferência, carregamento, armazenamento e recuperação, o controle duplo requer a divisão de conhecimento da chave entre as entidades. (Consulte também <i>Divisão de conhecimento</i> .)

Termo	Definição
Filtragem do pacote dinâmico	Consulte <i>Inspeção classificada</i> .
ECC	Acrônimo de “criptografia de curva elíptica” (Elliptic Curve Cryptography, no inglês). Abordagem da criptografia de chave pública baseada nas curvas elípticas sobre campos finitos. Consulte <i>Criptografia robusta</i> .
Filtragem egressa	Método de filtragem de tráfego de rede de longo curso, para que apenas tráfego explicitamente permitido tenha permissão para deixar a rede.
Criptografia	Processo de conversão de informações em uma forma inteligível, com exceção de titulares de uma chave criptográfica. O uso de criptografia protege informações entre o processo de criptografia e o de descryptografia (o inverso de criptografia) com relação a divulgação não autorizada. Consulte <i>Criptografia robusta</i> .
Algoritmo de criptografia	Também chamado de “algoritmo de criptografia”. Uma sequência de instruções matemáticas usadas para transformar texto ou dados não criptografados em texto ou dados criptografados, e vice-versa. Consulte <i>Criptografia robusta</i> .
Entidade	Termo usado para representar a empresa, organização ou negócios que realizam a revisão PCI DSS.
Monitoramento de integridade do arquivo	Técnica ou tecnologia na qual determinados arquivos ou logs são monitorados para detectar se foram modificados. Quando arquivos ou logs críticos são modificados, devem ser enviados alertas para os funcionários de segurança adequados.
Criptografia no nível do arquivo	Técnica ou tecnologia (software ou hardware) para criptografar conteúdos de arquivos específicos. Como alternativa, consulte a <i>Criptografia de disco</i> ou a <i>Criptografia de banco de dados no nível da coluna</i> .
FIPS	Acrônimo de “padrão federal de processamento da informação” (Federal Information Processing Standards, no inglês). Padrões que não são publicamente reconhecidos pelo Governo Federal norte-americano; também para uso de agências e contratantes não-governamentais.
Firewall	Tecnologia de hardware e/ou software que protege recursos de rede de acesso não autorizado. O firewall permite ou nega tráfego de computador entre redes com diferentes níveis de segurança com base em um conjunto de regras e outros critérios.
Investigação	Também chamado de “análise forense computacional”. Relacionado à segurança de informações. Aplicação de ferramentas e técnicas de análise investigativas para coletar evidências de recursos computacionais e determinar a causa do comprometimento dos dados.

Termo	Definição
FTP	Acrônimo de “protocolo de transferência de arquivos” (File Transfer Protocol, no inglês). Protocolo de rede usado para transferir dados de um computador para outro por meio de uma rede pública como a Internet. O FTP é amplamente visualizado em um protocolo inseguro, pois as senhas e o conteúdo dos arquivos são enviados sem proteção e em texto claro. O FTP pode ser implementado com segurança via SSH ou outras tecnologias. Consulte <i>S-FTP</i> .
GPRS	Acrônimo de “General Packet Radio Service”. Serviço de dados móveis disponível para usuários de celulares GSM. Reconhecido para uso eficiente de largura de banda limitada. Particularmente adequado para enviar e receber pequenos pacotes de dados, como e-mail e navegação pela Web.
GSM	Acrônimo de “Global System for Mobile Communications”. Padrão popular para celulares e redes. A ubiquidade do padrão GSM torna o roaming internacional muito comum entre operadoras de celular, permitindo que os assinantes usem seus telefones em várias partes do mundo.
Codificação hash	<p>Processamento ilegível dos dados do titular do cartão por meio da conversão e compilação dos dados em uma mensagem de comprimento fixo. A função de codificação hash é uma função de mão única (matemática) na qual um algoritmo não secreto obtém uma mensagem de comprimento arbitrário como entrada e produz uma saída de comprimento fixo (normalmente chamada de “código hash” ou “compilação de mensagem”). A função de codificação hash deve ter as seguintes propriedades:</p> <ol style="list-style-type: none"> (1) É computacionalmente impossível determinar a entrada fornecendo apenas o código hash, (2) É computacionalmente impossível encontrar duas entrada que forneçam o mesmo código hash. <p>No contexto de PCI DSS, a função de codificação hash deve ser aplicada a todo o PAN para que o código hash seja considerado como ilegível. É recomendado que os dados de hash do cartão do titular incluam uma variável de entrada (por exemplo, um “salto”) para a função de codificação hash reduzir ou anular a eficácia dos ataques de rainbow table pré-calculada (consulte a <i>variável de entrada</i>).</p> <p>Para orientações adicionais, consulte as normas do setor, como, por exemplo, versões atualizadas da Publicação Especial NIST 800-107 e 800-106, Normas Federais de Processamento das Informações (FIPS) 180-4, Padrão de Hash Seguro (SHS) e Padrão FIPS 202 SHA-3: Hash baseado em permuta e funções de saída extensíveis.</p>
Host	Hardware do computador principal no qual está o software do computador.

Termo	Definição
Provedor de hospedagem	Oferece diversos serviços para os comerciantes e para outros fornecedores de serviço. Os serviços variam de simples a complexos; de espaço compartilhado em um servidor a uma ampla variedade de opções de “carrinhos de compra”; de aplicativos de pagamento a conexões a gateways e processadores de pagamento; e de hospedagem dedicada para apenas um cliente por servidor. O provedor de host pode ser compartilhado, hospedando várias entidades em um único servidor.
HSM	Acrônimo de “módulo de segurança de hardware” ou “módulo de segurança de host” (hardware security module e host security module no inglês). Um dispositivo de hardware protegido de modo lógico e físico, que fornece um conjunto seguro de serviços criptográficos, usados para as funções de gerenciamento de chaves de criptografia e/ou decodificação de dados da conta.
HTTP	Acrônimo de “Hypertext Transfer Protocol”. Protocolo de internet aberta para transferir ou conduzir informações pela World Wide Web.
HTTPS	Acrônimo de “Hypertext Transfer Protocol Over Secure Socket Layer”. HTTP seguro que fornece autenticação e comunicação criptografada na World Wide Web feita para comunicações que precisem ser seguras, como logons da Web.
Hipervisor	Software ou firmware responsável pela hospedagem e gerenciamento de máquinas virtuais. Para os propósitos do PCI DSS, o componente do sistema hipervisor também inclui o monitor virtual da máquina (VMM).
ID	Identificador de um usuário ou aplicativo em particular.
IDS	Acrônimo de “sistema de detecção de intrusão” (intrusion-detection system, no inglês). Software ou hardware usado para identificar e alertar sobre as tentativas de intrusão ou anomalias em uma rede ou sistema. Composto por sensores que geram eventos de segurança; um console para monitorar eventos e alertas e controlar os sensores e um mecanismo central que grava eventos registrados pelos sensores do banco de dados. Utiliza um sistema de regras para a geração de alertas em resposta aos eventos de segurança detectados. Consulte <i>IPS</i> .
IETF	Acrônimo de “força tarefa de engenharia da internet” (Internet Engineering Task Force, no inglês). Comunidade internacional aberta de grande porte compreendendo designers de rede, operadores, fornecedores e pesquisadores interessados na evolução da arquitetura e na operação uniforme da internet. A IETF não possui associação formal e é aberta a qualquer indivíduo interessado.
IMAP	Acrônimo de “protocolo de acesso à mensagens da internet” (Internet Message Access Protocol, no inglês). Um protocolo de internet com camada de aplicativo que permite que um cliente de e-mail acesse e-mails em um servidor de correspondência remoto.
Token do índice	Um token criptográfico que substitui o PAN, baseado em um determinado índice para um valor imprevisível.

Termo	Definição
Segurança das informações	Proteção das informações para garantir a confidencialidade, integridade e disponibilidade.
Sistema de informações	Conjunto discreto de recursos de dados estruturados organizados para coleta, processamento, manutenção, uso, compartilhamento, disseminação ou disposição de informações.
Filtragem ingressa	Método de filtragem de tráfego de rede de entrada, para que apenas tráfego explicitamente permitido tenha permissão para entrar na rede.
Defeitos de injeção	A vulnerabilidade que é criada a partir de técnicas de codificação não seguras, resultando em validação inadequada de entrada, que permite que os hackers transmitam códigos maliciosos por um aplicativo da Web para o sistema subjacente. Essa classe de vulnerabilidades inclui injeção SQL, injeção LDAP e injeção XPath.
Variável de entrada	A sequência de dados aleatórios que é encadeada com os dados de origem antes da função hash de mão única ser aplicada. As variáveis de entrada podem ajudar a reduzir a eficácia dos ataques de rainbow table. Consulte também <i>Codificação hash</i> e <i>Rainbow tables</i> .
Porta, Serviço ou Protocolo inseguro(a)	Um protocolo, serviço ou porta que apresenta assuntos relacionados à segurança devido à falta de controle sobre a confidencialidade e/ou integridade. Os assuntos relacionados à segurança incluem serviços, protocolos ou portas que transmitem dados e credenciais de autenticação (por exemplo, senha/frase de senha) em texto claro pela internet, ou que permitam, com facilidade, a exploração por padrão ou por erro na configuração. Exemplos de serviços, protocolos ou portas não seguros incluem, entre outros, FTP, Telnet, POP3, IMAP e SNMP v1 e v2.
IP	Acrônimo de “Internet Protocol”. Protocolo de camada de rede que contém informações de endereços e algumas informações de controle que permitem que os pacotes sejam direcionados e entregues do host de origem para o host de destino. O IP é o principal protocolo de camada de rede no conjunto de protocolos da internet. Consulte <i>TCP</i> .
Endereço IP	Também chamado de “endereço do protocolo da internet”. Código numérico que identifica de forma única um determinado computador (host) na internet.
Falsificação de endereço de IP	Técnicas de ataque usadas para obter acesso não autorizado a redes ou computadores. O intruso envia mensagens enganosas a um computador com um endereço de IP indicando que a mensagem tem origem em um host confiável.
IPS	Acrônimo de “sistema de prevenção de intrusão” (intrusion prevention system, no inglês). Além do IDS, o IPS assume a etapa adicional de bloquear a tentativa de intrusão.

Termo	Definição
IPSEC	Abreviação de “Internet Protocol Security”. É o padrão de segurança para comunicações via IP na camada de rede por meio da criptografia e/ou autenticação de todos os pacotes de IP em uma sessão de comunicação.
ISO	No contexto das normas e práticas recomendadas para o setor, ISO refere-se à “Organização Internacional para Padronização”, (International Organization for Standardization, no inglês); trata-se de uma organização não-governamental consistindo de uma rede de institutos de padrões nacionais.
Emissor	Entidade que emite cartões de pagamento ou realiza, facilita ou apoia serviços de emissão, incluindo, mas não limitando-se a bancos de emissão e processadores de emissão. Também referido como “banco de emissão” ou “instituição financeira de emissão”.
Serviços de emissão	Exemplos de serviços de emissão podem incluir, mas não limitam-se a, autorização e personalização do cartão.
LAN	Acrônimo de “rede de área local” (local area network, no inglês). Um grupo de computadores e/ou outros dispositivos que compartilham uma linha de comunicações em comum, normalmente em um prédio ou conjunto de prédios.
LDAP	Acrônimo de “Lightweight Direct Access Protocol”. Repositório de dados de autenticação e autorização usado para consultar e modificar permissões do usuário e conceder acesso a recursos protegidos.
Privilegio menor	Ter o acesso e/ou privilégios mínimos necessários para executar funções e responsabilidades da função da tarefa.
Log	Consulte <i>Log de auditoria</i> .
LPAR	Abreviação de “partição lógica” (logical partition, no inglês). Um sistema de subdivisão, ou particionamento, dos recursos totais de um computador – processadores, memória e armazenamento – em unidades menores que possam ser executadas com uma cópia própria e distinta do sistema operacional e dos aplicativos. O particionamento lógico é tipicamente usado para permitir o uso de diferentes sistemas operacionais e aplicativos em um único dispositivo. As partições podem ou não ser configuradas para se comunicarem entre si ou dividirem alguns recursos do servidor, como interfaces de rede.
MAC	Em criptografia, acrônimo de “código de autenticação de mensagem” (message authentication code, no inglês). Um pequeno conjunto de informações usado para autenticar uma mensagem. Consulte <i>Criptografia robusta</i> .
Endereço MAC	Abreviação para “endereço de controle de acesso de mídia” (media access control address, no inglês). Valor de identificação exclusivo atribuído por fabricantes a adaptadores de rede e cartões de interface de rede.
Dado da tarja magnética	Consulte <i>Dados da tarja</i> .

Termo	Definição
Mainframe	Computadores feitos para lidar com volumes muito grandes de entrada e saída de dados e para enfatizar o throughput computing. Mainframes são capazes de executar vários sistemas operacionais, fazendo parecer que estão sendo operados vários computadores. Vários sistemas legados têm design de mainframe.
Software mal-intencionado/malware	Software ou firmware projetado para infiltrar ou danificar um sistema de computador sem o conhecimento ou consentimento do proprietário, com a intenção de comprometer a confidencialidade, integridade ou disponibilidade dos aplicativos, dados ou sistema operacional do proprietário. Esse tipo de software normalmente entra na rede durante várias atividades aprovadas pela empresa, resultando na exploração das vulnerabilidades do sistema. Entre os exemplos estão vírus, worms, Trojans (ou cavalos de Troia), spyware, adware e rootkits.
Mascaramento	No contexto do PCI DSS, é um método para ocultar um segmento de dados ao ser exibido ou impresso. O mascaramento é usado quando não houver exigência pela empresa de visualizar o PAN inteiro. O mascaramento relaciona-se à proteção do PAN quando exibido ou impresso. Consulte <i>Truncamento</i> para proteção do PAN ao ser armazenado em arquivos, bancos de dados, etc.
Ataques de eliminação de memória	Atividade de malware que examina e extrai os dados da memória à medida que são processados ou os que não foram adequadamente sobrescritos ou descarregados.
Comerciante	Para os objetivos do PCI DSS, o comerciante é definido como qualquer entidade que aceite cartões de pagamento com os logotipos de qualquer um dos cinco membros do PCI SSC (American Express, Discover, JCB, MasterCard ou Visa) como pagamento por bens e/ou serviços. Observe que o comerciante que aceita cartões de pagamento como pagamento por bens e/ou serviços também pode ser prestador de serviços, caso os serviços vendidos resultem no armazenamento, processamento ou transmissão de dados do titular do cartão em nome de outros comerciantes ou prestadores de serviço. Por exemplo, o ISP é um comerciante que aceita cartões de pagamento para faturas mensais, mas também é um prestador de serviço se hospedar comerciantes como clientes.
MO/TO	Acrônimo de “pedido por telefone/correio” (Mail-Order/Telephone-Order, no inglês).
Monitoramento	Uso de sistemas ou processos que monitoram constantemente computadores ou recursos de rede, com o objetivo de alertar os funcionários em caso de falhas de operação, alarmes ou outros eventos predefinidos.
MPLS	Acrônimo de “Multi Protocol Label Switching”. Mecanismo de rede ou telecomunicações feito para conectar um grupo de redes comutadas por pacotes.

Termo	Definição
Autenticação multifatorial	Método para autenticação do usuário, segundo o qual, pelo menos, dois fatores são verificados. 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.).
NAC	Acrônimo de “controle de acesso à rede” ou “controle de admissão da rede” (network access control e network admission control, no inglês). Um método de implementação de segurança na camada da rede ao restringir a disponibilidade dos recursos de rede aos dispositivos de término de acordo com uma política de segurança definida.
NAT	Acrônimo de “Network Address Translation”. Também conhecido como mascaramento de rede ou mascaramento de IP. Mudança de um endereço IP usado em uma rede para um endereço IP conhecido em outra rede, permitindo que uma organização tenha endereços internos que sejam visíveis internamente e endereços externos que sejam visíveis apenas externamente.
Rede	Dois ou mais computadores conectados por meio de meios físicos ou sem fio.
Administrador de rede	Equipe responsável pelo gerenciamento da rede em uma entidade. As responsabilidades normalmente incluem, entre outros, segurança de rede, instalações, atualizações, manutenção e monitoramento de atividades.
Componentes de rede	Incluem, mas não limitam-se a, firewalls, chaves, roteadores, pontos de acesso sem fio, mecanismos de rede e outros mecanismos de segurança.
Diagrama de rede	Um diagrama mostrando conexões e componentes do sistema em um ambiente em rede.
Varredura de segurança da rede	Processo no qual os sistemas de uma entidade são verificados remotamente quanto às vulnerabilidades pelo uso de ferramentas manuais ou automatizadas. Varreduras de segurança que incluem a sondagem de sistemas internos e externos e a criação de relatórios sobre os serviços expostos na rede. As varreduras podem identificar vulnerabilidades nos sistemas operacionais, serviços e dispositivos que poderiam ser usadas por indivíduos mal-intencionados.
Segmentação da rede	Também conhecido como “segmentação” ou “isolamento”. A segmentação de rede isola componentes do sistema que armazenam, processam ou transmitem dados do titular do cartão de sistemas que não o fazem. A segmentação de rede adequada pode reduzir o escopo do ambiente de dados do proprietário do cartão e, portanto, reduzir o escopo da avaliação PCI DSS. Veja a seção Segmentação de rede em <i>Requisitos do PCI DSS e os Procedimentos de Avaliação de Segurança</i> para obter orientação quanto ao uso da segmentação de rede. A segmentação de rede não é uma solicitação PCI DSS.

Termo	Definição
Network Sniffing	Também conhecida como “packet sniffing” ou “sniffing”. Uma técnica que monitora ou coleta passivamente comunicações da rede, decodifica protocolos e examina conteúdos para informações de interesse.
NIST	Acrônimo de “National Institute of Standards and Technology”. Agência federal não regulatória operando dentro da U.S. Commerce Department's Technology Administration.
NMAP	Software de varredura de segurança que mapeia redes e identifica portas abertas nos recursos de rede.
Acesso não-console	Refere-se ao acesso lógico a um componente de sistema, que ocorre em uma interface de rede em vez de ocorrer via conexão física direta ao componente do sistema. O acesso não-console inclui acesso a partir de redes internas/locais, bem como acesso a partir de redes remotas ou externas.
Usuários não consumidores	Qualquer indivíduo, excluindo titulares de cartão, que acessa os componentes do sistema, incluindo funcionários, administradores, prestadores de serviços, entre outros.
NTP	Acrônimo de “Network Time Protocol”. Protocolo de sincronização dos relógios de sistemas de computador, dispositivos de rede e outros componentes do sistema.
NVD	Acrônimo de “National Vulnerability Database.” O repositório do governo dos EUA de dados de gerenciamento de vulnerabilidade baseados em padrões. O NVD inclui bancos de dados de listas de verificação de segurança, defeitos de software relacionados à segurança, configurações erradas, nomes de produtos e métricas de impacto.
OCTAVE®	Acrônimo de “Operationally Critical Threat, Asset, and Vulnerability Evaluation.” Um conjunto de ferramentas, técnicas e métodos para planejamento e avaliação de estratégia de segurança de informações com base em riscos.
De prateleira (Off-the-Shelf)	Descrição de produtos que são itens de estoque não personalizados especificamente para um cliente ou usuário específico e que estão prontamente disponíveis para uso.
Sistema operacional/OS	Software de um sistema que é responsável pelo gerenciamento e pela coordenação de todas as atividades e pelo compartilhamento dos recursos computacionais. Exemplos de sistemas operacionais são Microsoft Windows, Mac OS, Linux e Unix.
Independência organizacional	Uma estrutura organizacional que garante que não haja conflitos de interesse entre a pessoa ou departamento que executa a atividade e a pessoa ou departamento que avalia a atividade. Por exemplo, indivíduos que executam avaliações são separados organizacionalmente do gerenciamento de ambiente que estão sendo avaliados.

Termo	Definição
OWASP	Acrônimo de “Open Web Application Security Project”. Organização sem fins lucrativos cujo objetivo é a melhoria da segurança de software de aplicativos. O OWASP mantém uma lista das vulnerabilidades mais importantes para os aplicativos Web. (Consulte http://www.owasp.org).
PA-DSS	Acrônimo de “padrão de segurança de dados de aplicativos de pagamento” (Payment Application Data Security Standard, no inglês).
PA-QSA	Acrônimo para “Assessores de segurança qualificados do aplicativo de pagamento” (Payment Application Qualified Security Assessor, no inglês). Os PA-QSAs são qualificados pela PCI SSC para avaliar os aplicativos de pagamento em relação ao PA-DSS. Consulte o <i>Guia do programa PA-DSS</i> e os <i>Requisitos de qualificação para PA-QSA</i> para obter detalhes sobre os requisitos para os funcionários e empresas PA-QSA.
Pad	Em criptografia, o “one-time pad” é um algoritmo de codificação com texto combinado com uma chave aleatória, ou “pad”, que é tão longa quanto o texto simples e usada apenas uma vez. Além disso, se a chave for realmente aleatória, nunca for reutilizada e mantida em segredo, o “one-time pad” será inviolável.
PAN	Acrônimo de “número da conta principal” e também chamado de “número da conta” (primary account number e account number, no inglês). Número exclusivo do cartão de pagamento (normalmente de crédito ou débito) que identifica o emissor e, mais particularmente, a conta do titular de cartão.
Queries parametrizadas	Meio de estruturação das queries SQL para limitar o escape e, portanto, evitar ataques de injeção.
Senha/frase de senha	Sequência de caracteres usados para a autenticação do usuário.
PAT	Acrônimo de “conversão do endereço da porta” e também chamado de “conversão do endereço da porta da rede” (port address translation e network address port translation, no inglês). Tipo de NAT que também converte os números de porta.
Patch	Atualização de um software existente para agregar funcionalidades ou para corrigir defeitos.
Aplicativo de pagamento	Para as finalidades do PA-DSS, um aplicativo de software que armazena, processa ou transmite dados do titular do cartão como parte da autorização ou acordo, em que os aplicativos de pagamento são vendidos, distribuídos ou licenciados a terceiros. Consulte o <i>Guia do programa do PA-DSS</i> para obter informações mais detalhadas.
Cartões de pagamento	Para os objetivos do PCI DSS, é qualquer cartão de pagamento/dispositivo que traga o logotipo dos membros fundadores do PCI SSC, que são American Express, Discover Financial Services, JCB International, MasterCard Worldwide ou Visa, Inc.

Termo	Definição
Processador de pagamento	Às vezes, referido como “Aplicativo de pagamento” ou “prestador de serviços de pagamento (PSP)”. Entidade engajada por um comerciante ou outra entidade para lidar com transações do cartão de pagamento em seu nome. Embora normalmente ofereçam serviços de aquisição, os processadores de pagamento não são considerados adquirentes, a menos que definidos como tal pela marca do cartão de pagamento. Ver também <i>Adquirente</i> .
PCI	Acrônimo de “indústria de cartões de pagamento” (Payment Card Industry, no inglês).
PCI DSS	Acrônimo de “padrão de segurança de dados da indústria de cartões de pagamento” (Payment Card Industry Data Security Standard, no inglês).
PDA	Acrônimo de “assistente pessoal de dados” ou “assistente digital pessoal”. Tratam-se de dispositivo móveis com recursos como celulares, e-mail ou navegadores da Web.
PED	Dispositivo de entrada PIN.
Teste de penetração	Os testes de penetração tentam identificar modos de explorar as vulnerabilidades a fim de enganar ou anular os recursos de segurança dos componentes do sistema. O teste de penetração inclui testes de rede e de aplicativos, além de controles e processos das redes e aplicativos, bem como ocorre tanto fora do ambiente (teste externo) quanto dentro dele.
Software de firewall pessoal	Um produto de software de firewall instalado em um único computador.
Informações pessoalmente identificáveis	Informações que podem ser utilizadas para identificar ou rastrear um indivíduo, incluindo, entre outros, o nome, endereço, número de seguro social, dados biométricos, data de nascimento, etc.
Equipe	Funcionários de meio período e período integral, temporários, contratantes e consultores que são “residentes” no site da entidade ou, de outra maneira, tenham acesso ao ambiente dos dados do proprietário do cartão.
PIN	Acrônimo de “número de identificação pessoal” (personal identification number, no inglês). Senha numérica secreta conhecida somente pelo usuário e pelo sistema para autenticação. O usuário só recebe acesso se o PIN fornecido for igual ao PIN do sistema. Os PINs típicos são usados em caixas eletrônicos para saques de dinheiro. Outro tipo de PIN é aquele usado em cartões com chip EMV, nos quais o PIN substitui a assinatura do titular do cartão.
Bloco de PIN	Bloco de dados usado para encapsular o PIN durante o processamento. O formato do bloco de PIN define o conteúdo do bloco e como ele será processado para recuperar o PIN. O bloco de PIN é composto pelo PIN, pela extensão PIN e pode conter um subconjunto do PAN.

Termo	Definição
POI	Acrônimo para “Ponto de interação”, o ponto inicial onde os dados são lidos a partir do cartão. Produto de transação/aceitação eletrônico, o POI consiste no hardware e software e é hospedado no equipamento de aceitação para ativar o proprietário do cartão para realizar uma transação do cartão. O POI pode ser assistido ou não assistido. As transações do POI normalmente são transações de circuito integrado (chip) e/ou baseadas na tarja magnética do cartão.
Política	Regras que valem para toda a organização e que regem o uso aceitável de recursos computacionais, práticas de segurança e desenvolvimento de orientação de procedimentos operacionais.
POP3	Acrônimo de “Post Office Protocol v3.” Um protocolo de camada de aplicativo usado por clientes de e-mail para recuperar e-mails de um servidor remoto por meio de uma conexão TCP/IP.
Porta	Pontos de conexão lógica (virtual) associados a um protocolo de comunicação particular a fim de facilitar a comunicação entre as redes.
POS	Acrônimo de “ponto de venda” (point of sale, no inglês). Hardware e/ou software usados para processar transações com cartão de pagamento nos endereços do comerciante.
Rede privada	Rede montada por uma organização que usa um espaço de endereço de IP privado. As redes privadas são comumente chamadas de redes locais ou LANs. O acesso de redes privadas a partir de redes públicas deve ser protegido corretamente com o uso de firewalls e roteadores. Ver também <i>Rede pública</i> .
Usuário privilegiado	Qualquer conta de usuário com privilégios maiores que os básicos. Normalmente, essas contas têm privilégios maiores ou elevados com mais direitos que uma conta de usuário padrão. No entanto, a extensão dos privilégios em diferentes contas privilegiadas pode variar bastante, dependendo da organização, função da tarefa e da tecnologia em uso.
Procedimento	Narrativa descritiva de uma política. O procedimento é um guia para uma política e descreve como ela deve ser implementada.
Protocolo	Método de comunicação aceito e usado dentro das redes. Especificação que descreve as regras e procedimentos que os computadores devem seguir para desempenhar as atividades em uma rede.
Servidor de proxy	Um servidor que age como um intermediário entre uma rede interna e a internet. Por exemplo, uma função de um servidor de proxy é finalizar ou negociar conexões entre conexões internas e externas, de modo que cada uma se comunique apenas com o servidor de proxy.
PTS	Acrônimo para “Segurança de transação do PIN”, o PTS é um conjunto de requisitos de avaliação modular gerenciado pelo Conselho de padrões de segurança PCI, para aceitação do PIN de terminais de POI. Consulte www.pcisecuritystandards.org .

Termo	Definição
Rede pública	Rede estabelecida e operada por um provedor de telecomunicações terceirizado com o propósito específico de prestar serviços de transmissão de dados para o público. Os dados em redes públicas podem ser interceptados, modificados e/ou redirecionados quando ainda em trânsito. Exemplos de redes públicas incluem, entre outras, internet, tecnologias sem fio e tecnologias móveis. Ver também <i>Rede privada</i> .
PVV	Acrônimo de “valor de verificação do PIN” (PIN verification value, no inglês). Valor arbitrário codificado na tarja magnética do cartão de pagamento.
QIR	Acrônimo de “revendedor ou integrador qualificado” (Qualified Integrator or Reseller, no inglês). Consulte o <i>Guia do programa QIR</i> no site da PCI SSC para obter mais informações.
QSA	Acrônimo de “assessor de segurança qualificado” (Qualified Security Assessor, no inglês). Os QSAs são qualificados pela PCI SSC para executar o PCI DSS em avaliações no local. Consulte os <i>Requisitos de qualificação QSA</i> para obter detalhes sobre os requisitos para funcionários e empresas QSA.
RADIUS	Abreviação de “serviço de autenticação e dial-in remoto do usuário” (Remote Authentication and Dial-In User Service, no inglês). Sistema de autenticação e contabilidade. Verifica se informações como o nome do usuário e sua senha, que passam pelo servidor do RADIUS, estão corretas; em caso positivo, autoriza o acesso ao sistema. Este método de autenticação pode ser usado com token, smart card, entre outros, para oferecer autenticação multifatorial.
Ataque de rainbow table	Um método de ataque a dados usando uma tabela pré-calculada de sequências de hash (compilação de mensagens com tamanho fixo) para identificar a fonte de dados original, normalmente para descobrir senhas ou hashes de dados do titular do cartão.
Re-keying	Processo de alteração das chaves criptográficas. O re-keying periódico limita a quantidade de dados criptografados por uma única chave.
Acesso remoto	Acesso a redes de computadores a partir de um local externo à rede. As conexões de acesso remoto podem ser originadas de dentro da rede da empresa ou a partir de um local remoto fora da rede da empresa. Um exemplo de tecnologia para acesso remoto é a <i>VPN</i> .
Ambiente de laboratório remoto	Laboratório não mantido pelo PA-QSA.
Mídia eletrônica removível	Mídia que armazena dados digitalizados e que pode ser facilmente removida e/ou transportada de um computador para outro. Exemplos de mídia eletrônica removível incluem CD-ROM, DVD-ROM, flash drives em USB e discos rígidos externos/portáteis.
Revendedores/Integradores	Entidade que vende e/ou integra aplicativos de pagamento, mas não os desenvolve.

Termo	Definição
RFC 1918	Padrão identificado pela Força tarefa de engenharia da internet (IETF) que define o uso e os intervalos de endereço apropriados para redes privadas (não roteáveis pela internet).
Análise/avaliação de risco	Processo que identifica os recursos valiosos do sistema e as ameaças; quantifica a exposição às perdas (ou seja, potenciais perdas) com base nas frequências estimadas e custos da ocorrência; e, opcionalmente, recomenda como alocar os recursos para adotar medidas visando a minimizar a exposição total.
Classificação de risco	Um critério definido de medição com base na avaliação de risco e análise de risco executadas em uma dada entidade.
ROC	Acrônimo de “relatório sobre conformidade” (Report on Compliance, no inglês). Relatório que documenta resultados detalhados da avaliação de PCI DSS de uma entidade.
Rootkit	Tipo de software mal-intencionado que, quando instalado sem autorização, é capaz de esconder sua presença e ganhar controle administrativo de um sistema de computadores.
Roteador	Hardware ou software que conecta duas ou mais redes. Funciona como classificador e interpretador, verificando os endereços e passando os bits de informação para o devido destino. Os roteadores de software são às vezes chamados de gateways.
ROV	Acrônimo de “relatório sobre validação” (Report on Validation, no inglês). Relatório que documenta os resultados detalhados de uma avaliação de PA-DSS para fins do programa de PA-DSS.
RSA	Algoritmo para a codificação de chaves públicas descrito em 1977 por Ron Rivest, Adi Shamir e Len Adleman, do Massachusetts Institute of Technology (MIT); as letras RSA são as iniciais dos seus sobrenomes.
S-FTP	Acrônimo de segurança FTP (Secure-FTP, no inglês). A S-FTP tem a capacidade de criptografar informações de autenticação e arquivos de dados em trânsito. Consulte <i>FTP</i> .
Amostragem	O processo de seleção de seção cruzada de um grupo que representa todo o grupo. A amostragem pode ser usada por assessores para reduzir os esforços de teste gerias, quando é validado que a entidade tem segurança PCI DSS padrão centralizada e processos operacionais e controles corretos. A amostragem não é um requisito do PCI DSS.
SANS	Acrônimo de “SysAdmin, Audit, Networking and Security”, instituto que fornece treinamento em segurança computacional e certificação profissional. (Consulte www.sans.org .)
SAQ	Acrônimo de “questionário de autoavaliação” (Self-Assessment Questionnaire, no inglês). Ferramenta de relatório usada para documentar os resultados de autoavaliação da avaliação de PCI DSS de uma entidade.

Termo	Definição
Esquema	Descrição formal de como o banco de dados é criado, incluindo a organização dos elementos dos dados.
Escopo	Processo de identificação de todos os componentes do sistema, pessoas e processos a serem incluídos na avaliação PCI DSS. A primeira etapa de uma avaliação do PCI DSS é determinar precisamente o escopo da revisão.
SDLC	Acrônimo de “ciclo de vida de desenvolvimento do sistema” ou “ciclo de vida de desenvolvimento de software” (system development life cycle e software development lifecycle, no inglês). Fases de desenvolvimento de um software ou sistema computacional que incluem planejamento, análise, design, teste e implementação.
Codificação segura	Processo de criação e implementação de aplicativos que são resistentes à violação e ao comprometimento.
Dispositivo de criptografia segura	Um conjunto de hardware, software e firmware que implementa processos de criptografia (incluindo algoritmos de criptografia e geração de chave) e fica contido em um limite de criptografia definido. Exemplos de dispositivos de criptografia segura incluem módulos de segurança de hardware/host (HSMs) e dispositivos de ponto de interação (POIs) que foram validados para PCI PTS.
Limpeza segura	Também chamada de “exclusão segura”, um método de sobrescrever dados que residem em uma unidade de disco rígido ou outras mídias digitais, convertendo os dados não recuperáveis.
Evento de segurança	Quando uma organização considera que uma ocorrência pode ocasionar implicações potenciais de segurança a um sistema ou seu ambiente. No contexto de PCI DSS, os eventos de segurança identificam atividades diferentes ou suspeitas.
Oficial de segurança	Pessoa responsável primária pelos assuntos relacionados à segurança da entidade.
Política de segurança	Conjunto de leis, regras e práticas que determinam como uma organização deve administrar, proteger e distribuir informações confidenciais.
Protocolos de segurança	Protocolos de comunicação da rede desenvolvidos para garantir a segurança da transmissão de dados. Exemplos de protocolos de segurança incluem, entre outros, TLS, IPSEC, SSH, HTTPS etc.
Área confidencial	Qualquer central de dados, sala de servidores ou qualquer área que contenha sistemas que armazenem, processem ou transmitam dados do titular do cartão. Isso exclui as áreas nas quais há somente terminais do ponto de venda presentes, como as áreas dos caixas em uma loja de varejo.

Termo	Definição
Dados de autenticação confidenciais	Informações relacionadas à segurança (incluindo, entre outros, a validação dos códigos/valores do cartão, dados totais da tarja magnética, (da tarja magnética ou equivalente em um chip) PINs e blocos de PIN) usados para autenticar os titulares do cartão e/ou autorizar transações do cartão de pagamento.
Separação de tarefas	Ato de dividir os passos de uma função entre diferentes indivíduos, de forma a impedir que um único indivíduo seja capaz de subverter o processo.
Servidor	Computador que presta serviço a outros computadores, como processamento de comunicações, armazenamento de arquivos ou acesso a um dispositivo de impressão. Os servidores incluem, mas não de forma exclusiva, banco de dados, aplicativos, autenticação, DNS, correio, proxy e NTP.
Código de serviço	Número de três ou quatro dígitos da tarja magnética que vem em seguida à data de validade do cartão de pagamento nos dados da tarja. Ele é usado para várias coisas, como para definir atributos de serviço, diferenciar entre comércio nacional e internacional e identificar restrições de uso.
Prestador de serviço	Entidade de negócios que não é uma bandeira de pagamento, diretamente envolvida no processamento, armazenamento ou na transmissão de dados do titular do cartão em nome de outra entidade. Isso inclui também as empresas que prestam serviços que controlam ou podem afetar a segurança dos dados do titular de cartão, como por exemplo prestadores de serviços gerenciados que oferecem firewalls gerenciados, IDS e outros serviços, bem como provedores de hosting e outras entidades. Se uma entidade fornece um serviço que envolve <i>somente</i> a provisão do acesso à rede pública, como empresa de telecomunicações que fornece apenas o link de comunicação, ela não pode ser considerada como uma prestadora de serviços para tal serviço (embora possa ser considerada como uma prestadora de serviços para outros serviços).
Token de sessão	No contexto do gerenciamento da sessão web, um token de sessão (também referido como “identificador de sessão” ou “ID de sessão”) é um identificador exclusivo (como um “cookie”) usado para controlar uma sessão específica entre um navegador e um servidor da web.
SHA-1/SHA-2	Acrônimo de “algoritmo de hash seguro” (Secure Hash Algorithm, no inglês). Uma família ou conjunto de funções criptográficas de hash relacionadas, incluindo SHA-1 e SHA-2. Consulte <i>Criptografia robusta</i> .
Smart card	Também conhecido como “cartão com chip” ou “cartão IC (cartão com circuito integrado)”. Tipo de cartão de pagamento que possui circuitos integrados incorporados. Os circuitos, também chamados de “chip”, contêm dados do cartão de pagamento, incluindo, entre outros, dados equivalentes aos dados da tarja magnética.

Termo	Definição
SNMP	Acrônimo de “protocolo de administração de rede simples” (Simple Network Management Protocol, no inglês). Suporta o acompanhamento de dispositivos ligados à rede para quaisquer condições que demandem atenção administrativa.
Conhecimento compartilhado	Um método em que duas ou mais entidades possuem separadamente componentes importantes, mas que individualmente não transmitem nenhum conhecimento sobre a chave de criptografia resultante.
Spyware	Tipo de software mal-intencionado que, quando instalado, intercepta ou assume controle parcial do computador do usuário sem conhecimento dele.
SQL	Acrônimo de “Structured Query Language”. Linguagem computacional usada para criar, modificar e recuperar dados de um sistema de administração de bancos de dados relacionais.
Injeção SQL	Forma de ataque a site baseado em banco de dados. Um indivíduo mal-intencionado executa comandos SQL não autorizados beneficiando-se de códigos inseguros nos sistemas conectados à internet. Os ataques de injeção SQL são utilizados para furtrar informações de um banco de dados nos quais as informações normalmente não estariam disponíveis e/ou obter acesso ao host de uma organização por meio do computador que hospeda o banco de dados.
SSH	Abreviação de “Secure Shell”. Conjunto de protocolos que oferecem codificação para os serviços de rede, como logon remoto ou transferência remota de arquivos.
SSL	Acrônimo de “Secure Sockets Layer”. Padrão do setor que criptografa o canal entre um navegador e um servidor da web. Substituído por TLS. Consulte <i>TLS</i> .
Inspeção com status	Também chamada de “filtragem dinâmica de pacote”. Recurso de firewall que fornece segurança aprimorada ao manter os registros do estado das conexões de rede. Programado para distinguir pacotes legítimos para várias conexões. Somente pacotes correspondentes a uma conexão estabelecida serão permitidos pelo firewall, todos os outros serão rejeitados.

Termo	Definição
Criptografia robusta	<p>Criptografia baseada em algoritmos testados e aceitos pelo setor, juntamente com comprimentos da chave que fornecem, no mínimo, 112 bits de eficiência referente à robustez e às práticas adequadas no gerenciamento de chaves. Criptografia é um método para proteger dados e inclui tanto a criptografia (reversível) quanto a codificação hash (“mão única” ou não reversível). Ver <i>Codificação hash</i>.</p> <p>No momento da publicação, exemplos de padrões e algoritmos testados e aceitos pelo setor incluem AES (128 bits e superior), TDES/TDEA (chaves de comprimento triplo), RSA (2048 bits e superior), ECC (224 bits e superior) e DSA/D-H (2048/224 bits e superior). Consulte a versão atualizada da Publicação Especial de NIST 800-57, Parte 1 (http://csrc.nist.gov/publications/) para obter orientação sobre algoritmos e chave robusta em criptografia.</p> <p>Observação: <i>Os exemplos acima são adequados para armazenamento persistente de dados do titular do cartão. Os requisitos mínimos de criptografia para operações baseadas em transações, conforme definição no PCI PIN e PTS, são mais flexíveis, pois há controles adicionais estabelecidos para reduzir o nível de exposição.</i></p> <p><i>Recomenda-se que todas as novas implementações usem, pelo menos, 128-bits de eficiência referente à robustez da chave.</i></p>
SysAdmin	<p>Abreviação de “administrador do sistema” (system administrator, no inglês). Pessoa com privilégios elevados que é responsável por gerenciar um sistema computacional ou rede.</p>
Componentes do sistema	<p>Quaisquer dispositivos de rede, servidores, dispositivos de computação ou aplicativos incluídos ou conectados ao ambiente de dados do titular do cartão.</p>
Objeto no nível do sistema	<p>Qualquer coisa no componente do sistema requisitado para sua operação, incluindo, entre outros, tabelas de banco de dados, procedimentos armazenados, arquivos de configuração e executáveis de aplicativos, arquivos de configuração do sistema, bibliotecas estáticas e compartilhadas e DLLs, executáveis do sistema, drivers do dispositivo e arquivos de configuração de dispositivo e componentes de terceiros.</p>
TACACS	<p>Acrônimo de “sistema de controle de acesso ao controlador de acesso do terminal” (Terminal Access Controller Access Control System, no inglês). Protocolo de autenticação remota comumente usado em redes que se comunica, entre um servidor de acesso remoto e um servidor de autenticação para determinar os direitos de acesso do usuário à rede. Este método de autenticação pode ser usado com token, smart card, entre outros, para oferecer autenticação multifatorial.</p>
TCP	<p>Acrônimo de “Transmission Control Protocol”. Um dos principais protocolos de camada de transporte do conjunto de protocolo de internet (IP) e a linguagem de comunicação básica ou protocolo de internet. Consulte <i>IP</i>.</p>

Termo	Definição
TDES	Acrônimo de “padrão de codificação de dado triplo” e também conhecido como “3DES” ou “DES triplo” (Triple Data Encryption Standard, 3DES e Triple DES, no inglês). Cifrador de bloco formado a partir da cifra DES usando-a três vezes. Consulte <i>Criptografia robusta</i> .
TELNET	Abreviação de “protocolo de rede telefônica” (telephone network protocol, no inglês). Geralmente usado para fazer sessões de logon em linha de comando orientada pelo usuário entre dispositivos em uma rede. As credenciais dos usuários são transmitidas em texto simples.
Ameaça	Condição ou atividade que pode fazer com que as informações ou os recursos de processamento de informações sejam intencionalmente ou acidentalmente perdidos, modificados, expostos, inutilizados ou de outra forma afetados em detrimento da organização.
TLS	Acrônimo de “segurança da camada de transporte” (Transport Layer Security, no inglês). Criada com o objetivo de prover confidencialidade e integridade aos dados nas comunicações entre dois aplicativos. A TLS é a sucessora da SSL.
Token	No contexto do controle de acesso e autenticação, token é um valor fornecido por hardware ou software, que funciona com servidor de autenticação ou VPN para executar a autenticação dinâmica ou multifatorial. Consulte <i>RADIUS</i> , <i>TACACS</i> e <i>VPN</i> . Ver também <i>Token de sessão</i> .
Dados da tarja	Também conhecido como “dados da tarja magnética” ou “dados da faixa magnética”. Dado criptografado da tarja magnética ou no chip usado para autorização e/ou autenticação durante transações de pagamento. Pode ser a imagem da tarja magnética em um chip ou os dados na trilha 1 e/ou trilha 2 da tarja magnética.
Dados da transação	Dados relacionados à transação com cartão de pagamento eletrônico.
Trojan	Também chamado de “cavalo de Troia”. Tipo de software mal-intencionado que, quando instalado, permite que o usuário execute uma função normal enquanto o Trojan age de forma mal-intencionada no sistema computacional sem conhecimento do usuário.
Truncamento	Método para deixar o PAN integral ilegível, removendo permanentemente um segmento dos dados do PAN. Consulte Truncamento para proteção do PAN ao ser <i>armazenado</i> em arquivos, bancos de dados, etc. Consulte <i>Mascaramento</i> para proteção do PAN quando <i>exibido</i> em telas, recibos de papel, etc.
Rede confiável	Rede de uma organização que está dentro da capacidade de controle e gerenciamento da empresa.
Rede não confiável	Rede externa àquela pertencente a uma organização e que está fora da capacidade de controle ou gerenciamento dela.
URL	Acrônimo de “Uniform Resource Locator”. Uma sequência de texto formatada usada por navegadores da Web, clientes de e-mail e outros softwares para identificar um recurso de rede na internet.

Termo	Definição
Metodologia de versão	Um processo de atribuição de esquemas de versão para identificar exclusivamente um estado particular de um aplicativo ou software. Esses esquemas seguem um formato de número de versão, uso de número de versão e qualquer elemento curinga, conforme definido pelo fornecedor de software. Os números de versão são, geralmente, atribuídos em ordem crescente e correspondem a uma mudança particular no software.
Utensílio virtual (VA)	O VA aplica o conceito de um dispositivo pré-configurado para realização de um conjunto específico de funções e execução do dispositivo como carga de trabalho. Frequentemente, um dispositivo de rede existente, como roteador, comutador ou firewall, é virtualizado para executar como um utensílio virtual.
Hipervisor virtual	Consulte <i>Hipervisor</i> .
Máquina virtual	Ambiente de operação autocontido que comporta-se como um computador separado. Também é conhecido como “Convidado” e é executado no topo do hipervisor.
Monitor de máquina virtual (VMM)	O VMM está incluído no hipervisor e no software que implementa a abstração de hardware da máquina virtual. Ele gerencia o processador, a memória e outros recursos do sistema para alocar o que cada sistema de operação convidado requer.
Terminal de pagamento virtual	Um terminal de pagamento virtual é um acesso baseado no navegador da Web ao site do adquirente, processador ou prestador de serviços terceirizado para autorização de transações com cartões de pagamento, nas quais o comerciante insere manualmente os dados do cartão de pagamento por meio de navegador da Web conectado de forma segura. Diferentemente dos terminais físicos, os terminais virtuais não leem dados diretamente do cartão de pagamento. 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.
Comutador ou roteador virtual	Um comutador ou roteador virtual é uma entidade lógica que apresenta a funcionalidade de roteamento e comutação de dados de nível da infraestrutura de rede. Um comutador virtual é uma parte integral da plataforma do servidor virtualizado como driver do hipervisor, módulo ou plug-in.
Virtualização	A virtualização refere-se à abstração lógica dos recursos de computação de limitações físicas. As abstrações comuns são referidas como máquinas virtuais ou VMs, compondo o conteúdo de uma máquina física e permitindo que ela opere em um hardware físico diferente e/ou juntamente com outras máquinas virtuais no mesmo hardware físico. Em adição aos VMs, a virtualização pode ser realizada em muitos outros recursos de computação, incluindo aplicações, desktops, redes e armazenamento.

Termo	Definição
VLAN	Abreviação de “LAN virtual” ou “rede local virtual” (virtual LAN e virtual local area network, no inglês). Rede local lógica que vai além de uma única rede local física tradicional.
VPN	Acrônimo de “rede privada virtual” (virtual private network, no inglês). Uma rede de computadores na qual algumas das conexões são circuitos virtuais dentro de uma rede maior, como a internet, em vez de conexões diretas por fios físicos. Quando for o caso, diz-se que os pontos finais da rede virtual passam por um túnel pela rede maior. Enquanto um aplicativo comum é formado por comunicações seguras pela internet pública, a VPN pode ou não ter recursos de segurança, como autenticação ou criptografia de conteúdo. O VPN pode ser usado com um token, smart card, etc., para fornecer autenticação de dois fatores.
Vulnerabilidade	Falha ou fraqueza que, se explorada, pode resultar em comprometimento intencional ou não intencional do sistema.
WAN	Acrônimo de “rede remota” (wide area network, no inglês). Rede de computadores que cobre uma grande área, muitas vezes um sistema de computadores de toda uma empresa ou região.
Aplicativo Web	Aplicativo que é geralmente acessado por meio de navegador da Web ou de serviços da Web. Os aplicativos Web podem estar disponíveis por meio da internet ou de uma rede privada e interna.
Servidor da Web	Computador que contém um programa que aceita solicitações de HTTP de clientes da Web e apresenta as respostas de HTTP (normalmente páginas da Web).
WEP	Acrônimo de “privacidade equivalente com fio” (Wired Equivalent Privacy, no inglês). Algoritmo débil usado para criptografar redes wireless. Várias debilidades sérias foram identificadas por especialistas do setor, de forma que a conexão WEP pode ser quebrada com softwares prontamente disponíveis em questão de minutos. Consulte <i>WPA</i> .
Curinga	Um caractere que pode ser substituído por um subconjunto definido de possíveis caracteres em um esquema de versão de aplicativo. No contexto do PA-DSS, os curingas podem ser usados opcionalmente para representar uma mudança sem impacto na segurança. Um curinga é o único elemento variável do esquema de versão do fornecedor e é usado para indicar que há apenas alterações menores, sem impacto na segurança entre cada versão representada pelo elemento de caractere curinga.
Ponto de acesso wireless	Também chamado de “AP”. Dispositivo que permite que dispositivos de comunicação wireless se conectem a uma rede wireless. Normalmente conectado a uma rede com fio, ele pode revezar os dados entre dispositivos wireless e dispositivos com fio na rede.
Redes wireless	Rede que conecta computadores sem uma conexão física com fios.

Termo	Definição
WLAN	Acrônimo de “rede local sem fio” (wireless local area network, no inglês). Rede local que liga dois ou mais computadores ou dispositivos sem fio.
WPA/WPA2	Acrônimo de “Acesso Wi-Fi protegido” (WiFi Protected Access, no inglês). Protocolo de segurança criado para proteger redes wireless. WPA é o sucessor do WEP O WPA2 também foi lançado como a próxima geração de WPA.