Payment Card Industry (PCI)

Indústria de Cartões de Pagamento (PCI)
Padrão de Segurança de Dados

Glossário, Abreviações e Acrônimos

Termo	Definição
AAA	Protocolo de autenticação, autorização e contabilidade
Accounting	**Contabilidade**. Acompanhamento dos usuários dos recursos da rede
Access Control	**Controle de Acesso.** Mecanismos que limitam o acesso às informações ou aos recursos de processamento da informação apenas às pessoas ou aplicativos autorizados
Account Harvesting	**Busca de Conta.** Processo de identificação das contas de usuários existentes com base em tentativa e erro. [Nota: Oferecer excesso de informação em mensagem de erro pode divulgar o suficiente para que um atacante penetre e 'faça a colheita' ou comprometa o sistema]
Account Number	**Número da Conta.** Número do cartão de pagamento (crédito ou débito) que identifica o emissor e a conta do portador de cartão. Também chamado de Número da Conta do Titular ou Número de Conta Primária (Primary Account Number - PAN)
Acquirer	**Adquirente.** Membro da Bankcard Association que inicia e mantém o relacionamento com os estabelecimentos que aceitam cartões de pagamento
AES	Padrão avançado de codificação. Bloco cifrado (block cipher) adotado pelo NIST em Novembro de 2001. O algoritmo é o especificado em FIPS PUB 197
ANSI	American National Standards Institute. Uma organização privada, sem fins lucrativos que administra e coordena o sistema de avaliação do processo de padronização e conformidade voluntária dos EUA
Anti-Virus Program	**Programa Antivírus.** Programa capaz de detectar, remover e proteger contra as várias formas de códigos maliciosos ou malware, incluindo vírus, worms, Trojan horses, spyware e adware
Application	**Aplicativo**. Inclui todos os programas de software adquiridos, especialmente desenvolvidos ou grupos de programas escritos para os usuários finais, incluindo os aplicativos internos e externos (web)
Approved Standards	**Padrões Aprovados.** Os padrões aprovados são algoritmos padronizados (como ISO e ANSI) e padrões comercialmente disponíveis e bem conhecidos (como Blowfish) que atendem à necessidade de forte criptografia. Os exemplos de padrões aprovados são AES (128 bits ou mais), TDES (dois ou três chaves independentes), RSA (1024 bits) e ElGamal (1024 bits)
Asset	**Ativo, Recurso.** Informação ou recursos de processamento da informação de uma organização
Audit Log	**Registro de Auditoria.** Arquivo cronológico das atividades do sistema. Oferece um caminho suficiente para permitir a reconstrução, revisão e exame da seqüência de atividades e ambientes que cercam ou conduzem a uma operação, procedimento ou evento em uma transação desde o início até o resultado final. Às vezes especificamente denominado como trilha de auditoria de segurança
Authentication	**Autenticação.** Processo de verificação da identidade de um processo ou fato relacionado

Termo	Definição
Authorization	**Autorização.** Concessão de acesso ou outros direitos a um usuário, programa ou processo
Backup	**Cópia de Reserva.** Cópia duplicada de dados feita com o objetivo de arquivo ou para a proteção contra dano ou perda
Cardholder	**Portador de Cartão** Cliente a quem é emitido um cartão ou indivíduo autorizado a usar o cartão
Cardholder Data	**Dado do Portador do Cartão.** Tarja magnética completa ou o PAN mais qualquer um dos seguintes dados: • Nome do portador de cartão • Data de vencimento • Código de serviço
Cardholder Data Environment	**Ambiente de Dado do Portador de Cartão.** Área do sistema de rede de computador que possui os dados do portador de cartão ou dado de autenticação sigiloso e aqueles sistemas e segmentos que estão conectados ou suportam o processamento do portador de cartão, armazenagem ou transmissão. Segmentação adequada, que isola os sistemas que armazenam, processam ou transmitem os dados do portador de cartão daqueles que não o fazem, e pode reduzir o escopo do ambiente de dados do portador de cartão e em conseqüência o escopo da avaliação de PCI
Card Validation Value or Code	**Valor ou Código de Validação do Cartão.** Elemento de dado encontrado na tarja magnética do cartão que usa o processo de criptografia segura para proteger a integridade dos dados na tarja, e revela qualquer alteração ou falsificação. Também conhecido como CAV, CVC, CVV, ou CSC dependendo da marca do cartão de pagamento. A lista a seguir mostra os termos para cada marca de cartão: • **CAV** Card Authentication Value (cartão de pagamento JCB) • **CVC** Card Validation Code (cartão de pagamento MasterCard) • **CVV** Card Verification Value (cartão de pagamento Visa e Discover) • **CSC** Card Security Code (cartão American Express) *Nota: O segundo tipo de valor ou código de validação de cartão é o valor de três dígitos impresso à direita do número do cartão de crédito no painel de assinatura no verso do cartão. Para os cartões American Express, o código é um número não emboçado de quatro dígitos impresso acima do número do cartão na frente de todos os cartões de pagamento. O código encontra-se associado, de forma única, com cada peça de plástico individual e conecta o número da conta do cartão ao plástico. Uma visão geral é oferecida a seguir:* • **CID** Card Identification Number (cartão de pagamento American Express e Discover) • **CAV2** Card Authentication Value 2 (cartão de pagamento JCB) • **CVC2** Card Validation Code 2 (cartão de pagamento MasterCard) • **CVV2** Card Verification Value 2 (cartão de pagamento Visa)

Termo	Definição
Compensating Controls	**Controles de Compensação.** Os controles de compensação podem ser considerados quando uma entidade não pode atender a uma exigência explicitamente como definido em função de legítimas dificuldades técnicas ou do negócio, mas que teve seu risco associado com a exigência diminuído em função da implementação de outros controles. Os controles de compensação devem: 1) atender à intenção e rigor da exigência original de PCI DSS; 2) repelir uma tentativa de compromisso com força semelhante; 3) estar "acima e além" em outras exigências de PCI DSS (não simplesmente estar em conformidade com outras exigências de PCI DSS); e 4) ser proporcional com o risco adicional imposto por não atender às exigências de PCI DSS
CIS	Centro de Segurança da Internet (Center for Internet Security). Uma empresa sem fins lucrativos cuja missão é ajudar as organizações a reduzirem o risco de interrupções do negócio e e-commerce resultantes de controles de segurança técnica inadequadas
Compromise	**Comprometimento.** Intrusão no sistema de computador onde existe a suspeita de divulgação não autorizada, modificação ou destruição dos dados do portador de cartão
Console	Tela ou teclado que permite o acesso e controle do computador servidor ou mainframe em um ambiente de rede
Consumer	**Consumidor.** Indivíduo que adquire mercadorias, serviços ou ambos
Cookies	É a seqüência de dados trocados entre um servidor de web e um paginador de web para manter uma sessão. Os *cookies* podem conter as preferências do usuário e informações pessoais
Cryptography	**Criptografia.** Disciplina de matemática e computação voltada para a segurança da informação e questões relacionadas, particularmente a codificação e autenticação e aplicativos tais como o controle de acesso. Em termos de computador e segurança de rede, é uma ferramenta para o controle do acesso e confidencialidade da informação
Database	**Banco de Dados.** Formato estruturado para organizar e manter informações facilmente recuperáveis. Um exemplo de banco de dados simples são as tabelas e planilhas
Data Base Administrator - DBA	**Administrador de Banco de Dados.** Administrador de banco de dados. Indivíduo responsável pela administração e gerenciamento dos bancos de dados
DBA (DoingBusiness As)	Fazendo negócio como. A validação dos níveis de conformidade é baseada no volume de transações de um DBA ou cadeia de lojas (não de uma corporação que possui diversas cadeias)
Default Accounts	**Contas Padrão.** Conta de login no sistema, pré-definida pelo fabricante de um sistema para permitir o acesso quando o sistema é colocado em serviço pela primeira vez
Default Password	**Senha Padrão.** É a senha da administração de sistema ou contas de serviços quando o sistema é enviado pelo fabricante; usualmente associadas com as contas padrão. As contas e senhas padrão são publicadas e bem conhecidas

Termo	Definição
DES	Padrão de Codificação de Dados (Data Encryption Standard - DES). Bloco cifrado (block cipher) eleito oficialmente como o Padrão Federal de Processamento da Informação (Federal Information Processing Standard - FIPS) para os Estados Unidos em 1976. O sucessor é o Padrão de Codificação Avançada (Advanced Encryption Standard - AES)
DMZ	Zona desmilitarizada. Rede adicionada entre uma rede pública e privada para prover uma camada adicional de segurança
DNS	Sistema de nome de domínio (domain name system) ou servidor de nome de domínio (domain name server). Sistema que armazena a informação associada com os nomes de domínio em um banco de dados distribuídos nas redes, tal como a Internet
DSS	Padrão de Segurança de Dados (Data Security Standard)
Dual Control	**Controle Duplo.** Processo de usar duas ou mais entidades separadas (geralmente pessoas) operando em conjunto para proteger funções sigilosas ou informações. Ambas as entidades são igualmente responsáveis pela proteção física de materiais envolvidos em transações vulneráveis. Não é permitido a nenhuma pessoa individualmente ter acesso ou usar os materiais (por exemplo, a chave criptográfica). Para a geração da chave manual, transporte, carregamento, armazenagem e recuperação, o controle duplo requer dividir o conhecimento da chave entre as entidades. Ver também conhecimento compartilhado (split knowledge)
ECC	Criptografia de curva elíptica (Elliptic curve cryptography). Abordagem da criptografia de chave pública baseada nas curvas elípticas sobre campos finitos.
Egress	Tráfego deixando uma rede através de um link de comunicação e ingressando na rede do cliente
Encryption	**Encriptação, Codificação.** Processo de converter a informação em uma forma ininteligível exceto para os possuidores de uma chave criptográfica específica. O uso de codificação protege a informação entre o processo de codificação e decodificação (o inverso de codificação) contra a divulgação não autorizada
FIPS	Padrão Federal de Processamento da Informação (Federal Information Processing Standard)
Firewall	Hardware, software ou ambos que protege os recursos de uma rede contra invasores de outras redes. Geralmente as empresas com uma intranet que permite que os funcionários tenham acesso à Internet aberta devem ter um firewall para evitar que estranhos tenham acesso aos seus recursos internos de dados privativos
FTP	Protocolo de transferência de arquivo (File transfer protocol)
GPRS	General Packet Radio Service. Serviço de dados móvel disponível aos usuários de telefones celulares GSM. Reconhecido pelo eficiente uso de banda (bandwidth) limitada. Particularmente útil para o envio de curtas seqüências de dados, tais como e-mail e web browsing

Termo	Definição
GSM	Sistema Global para Comunicações Celulares (Global System for Mobile Communications). Padrão popular para telefones celulares. A alta disseminação do padrão GSM faz com que o roteamento (roaming) internacional seja muito comum entre os operadores de telefones celulares, permitindo que os usuários usem os seus telefones em várias partes do mundo
Host	**Hoste – Hospedeiro.** Computador principal no qual o software encontra-se instalado
Hosting Provider	**Provedor de Hoste.** Oferece vários serviços aos estabelecimentos e outros provedores de serviços. Os serviços prestados podem ser simples ou complexos; desde o compartilhamento de espaço em um servidor até todas as opções encontradas em um carrinho de compras (shopping cart); desde aplicativos de pagamento até a conexão com portais de pagamentos e processadores; e como hospedeiro dedicado com um cliente por servidor
http	Protocolo de transferência de hipertexto (Hypertext transfer protocol). Protocolo de internet aberta para transferir ou conduzir a informação pela World Wide Web
ID	Identidade
IDS/IPS	Sistema de Detecção de Intrusão (Intrusion Detection System) / Sistema de Prevenção de Intrusão (Intrusion Prevention System). Usado para identificar e alertar sobre as tentativas de intrusão em uma rede ou sistema. Composto por sensores que geram eventos de segurança; um console para acompanhar os eventos e alertas e controlar os sensores; e um mecanismo central que grava os eventos registrados pelos censores em um banco de dados. Utiliza um sistema de regras para a geração de alertas em resposta aos eventos de segurança detectados. Um IPS executa a tarefa adicional de bloquear uma tentativa de intrusão.
IETF	Internet Engineering Task Force. Comunidade internacional aberta de grande porte compreendendo designers de rede, operadores, vendedores e pesquisadores interessados na evolução da arquitetura e operação uniforme da Internet. Aberta a qualquer indivíduo interessado
Information Security	**Segurança da Informação.** Proteção da informação para assegurar a confidencialidade, integridade e disponibilidade
Information System	**Sistema de Informação.** Conjunto discreto de recursos de dados estruturados e organizados para a coleta, processamento, manutenção, uso, compartilhamento ou disposição da informação
Ingresso	**Ingresso.** Tráfego de entrada na rede por intermédio de um link de comunicação e a rede do cliente
Intrusion Detection Systems	**Sistemas de Detecção de Intrusão.** Ver IDS
IP	Protocolo da Internet (Internet protocol). Protocolo de network-layer contendo informações de endereços e algumas informações de controle que permite o roteamento dos pacotes (packets). IP é o principal protocolo de network-layer no conjunto de protocolos na Internet

Termo	Definição
IP Address	**Endereços de IP.** Código numérico que identifica de forma única um computador em particular na Internet
IP Spoofing	**Spoofing de IP.** Técnica utilizada por um intruso para obter acesso não autorizado aos computadores. O intruso envia mensagens enganosas a um computador com um endereço de IP indicando que a mensagem tem origem em um host confiável
IPSEC	Protocolo de Segurança da Internet (Internet Protocol Security - IPSEC). É o padrão de segurança para comunicações via IP através da codificação e/ou autenticação de todos os pacotes de IP. O IPSEC oferece segurança nas várias camadas da rede
ISSO	Organização Internacional de Padronização (International Organization for Standardization). Organização não governamental composta por uma rede de institutos de padronização nacionais em mais de 150 países, com um membro por país e um secretariado geral em Genebra, Suíça, que coordena o sistema
ISO 8583	Estabelece o padrão para a comunicação entre os sistemas financeiros
Key	**Chave.** Em criptografia, uma chave é um valor algoritmo aplicado a um texto não codificado para produzir o texto codificado. O comprimento da chave geralmente determina o grau de dificuldade para decodificar o texto em uma determinada mensagem
L2TP	Layer 2 tunneling protocol. Protocolo usado para suportar as redes virtuais privadas (VPNs)
LAN	Rede de área local (Local area network). Rede de computador cobrindo uma pequena área, geralmente em um edifício ou grupo de edifícios
LPAR	Partição lógica. Seção de um disco que não é uma das partições primárias. Definido em um bloco de dado através de uma partição estendida
MAC	Código de autenticação de mensagem
Magnetic Stripe Data - Track Data	**Dado da Tarja Magnética – Dado da Trilha.** Dado codificado na tarja magnética usado para autorização durante transações quando o cartão encontra-se presente. As entidades não devem manter a totalidade dos dados da tarja magnética após a autorização da transação. Especificamente, após a autorização, os códigos de serviço, dados discricionários / Valor de Validação do Cartão / Código e valores reservados proprietários devem ser destruídos; entretanto, o número da conta, data de vencimento, nome e código de serviço podem ser extraídos e retidos, se forem necessários para o negócio
Malware	Software malicioso. Desenvolvido para infiltrar-se ou danificar um sistema de computador sem o conhecimento ou consentimento do proprietário
Monitoring	**Acompanhamento.** Uso de um sistema que constantemente monitora uma rede de computador incluindo sistemas que venham a se tornar lentos ou em vias de falhar, notificando o usuário em caso de lapso de tempo em que o mesmo esteja fora de operação (outage) ou outros alarmes
MPLS	Multi protocol label switching.

Termo	Definição
NAT	Network address translation. Conhecido como rede oculta ou ocultando o IP. Mudança de um endereço de IP usado em uma rede para outro diferente conhecido dentro da outra rede
Network	**Rede.** Dois ou mais computadores conectados para o compartilhamento de recursos
Network Components	**Componentes de Rede.** Incluem, mas não se limitam a firewalls, switches, roteadores, pontos de acesso sem fio, dispositivos de rede e outros dispositivos de segurança
Network Security Scan	**Varredura de Segurança da Rede.** Ferramenta automatizada que verifica remotamente se existem vulnerabilidades nos sistemas do estabelecimento ou prestador de serviço. Este teste não intrusivo envolve a avaliação dos sistemas voltados externamente e baseados em endereços do IP também voltados para o exterior, emitindo relatórios sobre os serviços disponíveis para a rede externa (ou seja, os serviços disponíveis para a Internet). As varreduras identificam as vulnerabilidades nos sistemas operacionais, serviços e dispositivos que podem ser usados pelos hackers para atacar a rede privada de uma empresa
NIST	Instituto Nacional de Padrões e Tecnologia (National Institute of Standards and Technology). Agência federal não regulamentar operando dentro da U.S. Commerce Department's Technology Administration. Sua missão é a de promover a competitividade industrial e inovação nos EUA através de avanços na ciência de aferição, padrões e tecnologia, para aprimorar a segurança econômica e melhorar a qualidade de vida
Non Consumer Users	**Usuários Não Consumidores.** Qualquer indivíduo, excluindo clientes consumidores, que acessam sistemas, incluindo mas não limitado aos funcionários, administradores e prestadores de serviços
NTP	Protocolo para a sincronização dos relógios dos sistemas do computador para as redes de dados packet-switched, variable-latency
OWASP	Projeto de Aplicativo Seguro para a Web Aberta (Open Web Application Security Project - consultar http://www.owasp.org)
Payment Cardholder Environment	**Ambiente de Pagamento do Portador de Cartão.** É a parte da rede que possui os dados do portador de cartão ou dados sigilosos de autenticação
PAN	O Número de Conta Primária (Primary Account Number) é o número do cartão de pagamento (crédito ou débito) que identifica o emissor e em particular a conta do portador de cartão. Também denominado de Número da Conta (Account Number)
Password	**Senha.** É uma seqüência de caracteres usados para a autenticação do usuário

Termo	Definição
Pad	Montador/desmontador de pacotes (packet assembler/disassembler). É um dispositivo de comunicação que formata os dados de saída e extrai os dados de um pacote de entrada. Em criptografia, o "one-time PAD" é um algoritmo de codificação com texto combinado com uma chave ou *"pad"* randômica que é tão longa quanto o texto pleno e usada apenas uma vez. Adicionalmente, se a chave é realmente randômica, nunca reusada e mantida secreta, o "one-time pad" não pode ser quebrado
PAT	Tradução de endereço de port (port address translation). Característica de um dispositivo de tradução de endereço de rede (network address translation - NAT) que traduz o protocolo de controle de transmissão (transmission control protocol - TCP) ou as conexões do protocolo do datagrama do usuário (user datagram protocol - UDP) feitas a um host e port em uma rede externa para um host e port em uma rede interna
Patch	Trabalho de reparo rápido para uma parte de um programa. Durante o teste beta de produção de um software ou período de prova, e após o lançamento formal de um produto, geralmente são encontrados alguns problemas. Um patch é um reparo rápido oferecido aos usuários
PCI	Indústria de Cartão de Pagamento (Payment Card Industry)
Penetration	**Penetração.** Ato de ter sucesso em ignorar ou evitar os mecanismos de segurança e obter acesso ao sistema de um computador
Penetration Test	**Teste de Penetração.** Teste orientado para a segurança de um sistema de computador ou rede para buscar as vulnerabilidades que um atacante possa explorar. Além de buscar as vulnerabilidades, este teste pode envolver tentativas reais de penetração. O objetivo de um teste de penetração é detectar e identificar as vulnerabilidades e sugerir melhorias na segurança
PIN	Número de identificação pessoal (Personal identification number)
Policy	**Política.** Regras globais governando o uso dos recursos computacionais, as práticas de segurança e guiando o desenvolvimento de procedimentos operacionais para toda a organização
POS	Ponto de venda (Point of sale)
Procedure	**Procedimento.** Narrativa descritiva de uma política. Um procedimento é o "how to" para uma política e descreve como ela deve ser implementada
Protocol	**Protocolo.** Método de comunicação aceito e usado dentro das redes. Especificação que descreve as regras e procedimentos que os produtos de computador devem seguir para desempenhar as atividades em uma rede
Public Network	**Rede Pública.** Rede estabelecida e operada por um provedor de telecomunicações ou uma empresa privada reconhecida, com o propósito específico de prestar os serviços de transmissão de dados para o público. O dado deve ser codificado durante a transmissão sobre as redes públicas visto que os hackers geralmente e com facilidade, interceptam, modificam, e/ou reorientam os dados quando ainda em trânsito. Exemplos de redes públicas no âmbito do PCI DSS incluem a Internet, GPRS e GSM.
PVV	Valor de verificação do PIN (PIN verification value). Codificado na tarja magnética do cartão de pagamento

Termo	Definição
RADIUS	Serviço de autenticação e dial-in remoto do usuário (Remote authentication and dial-In user service). Autenticação e sistema de contabilidade. Verifica se as informações tais como o nome do usuário e senha que passam pelo servidor do RADIUS estão corretos e então autoriza o acesso ao serviço
RFC	Solicitação de Comentários (Request for comments)
Re-keying	Processo de mudança das chaves criptográficas para limitar a quantidade de dados a serem codificados com a mesma chave
Risk Analysis	**Análise de Risco.** Processo que identifica sistematicamente os recursos valiosos do sistema e ameaças; quantifica a exposição às perdas (ou seja, o potencial de perda) baseado nas freqüências estimadas e custos da ocorrência; e (opcionalmente) recomenda como alocar os recursos para adotar medidas visando minimizar a exposição total. Levantamento do risco
Router	**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 softwares roteadores são às vezes chamados de gateways
RSA	Algoritmo para a codificação de chaves públicas descritos 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
Sanitization	**Sanitização.** Processo de apagar dados confidenciais de um arquivo, dispositivos ou sistema; ou modificação de dados de forma a que se tornem inúteis em caso de um ataque
SANS	SysAdmin, Audit, Network, Security Institute (Ver www.sans.org)
Security Officer	**Oficial de Segurança.** Principal responsável por questões relacionadas com a segurança de uma organização
Security Policy	**Política de Segurança.** Conjunto de leis, regras e práticas que determinam como uma organização administra, protege e distribui informações confidenciais
Sensitive Authentication Data	**Dado de Autenticação Confidencial.** Informação relacionada com a segurança (Código de Validação do Cartão / Valores, dados completos de acompanhamento, PINs e PIN Blocks) usados para autenticar os portadores de cartão, aparecendo em texto pleno ou de outra forma não protegida. A divulgação, modificação ou destruição desta informação pode comprometer a segurança de um dispositivo criptográfico, sistema de informação, informação do portador de cartão ou pode ser usada em transações fraudulentas
Separation of Duties	**Separação de Tarefas.** Práticas de dividir os passos de uma função entre os diferentes indivíduos, de forma a impedir que um único indivíduo seja capaz de subverter o processo
Server	**Servidor.** Computador que presta serviço a outros computadores, tais como o processamento de comunicações, armazenamento de arquivos ou acesso a um dispositivo de impressão. Os servidores incluem, mas não se limitam a web, banco de dados, autenticação, DNS, mail, proxy e NTP

Termo	Definição
Service Code	**Código de Serviço.** Número de três ou quatro dígitos em uma tarja magnética que especifica as exigências de aceitação e limitações para a leitura de uma transação de tarja magnética
Service Provider	**Prestador de Serviço**. Entidade de negócio que não é membro de uma marca de cartão de pagamento ou um estabelecimento diretamente envolvido no processamento, armazenamento, transmissão e switching ou dado de transações e informação do portador de cartão ou ambos. Isto também inclui as empresas que prestam serviços aos estabelecimentos, prestadores de serviços ou membros que controlam ou podem afetar a segurança dos dados do portador de cartão. Os exemplos incluem os prestadores de serviços de administração que oferecem firewalls gerenciados, IDS e outros serviços bem como provedores de hosting e outras entidades. As entidades tais como empresas de telecomunicações que oferecem apenas links de comunicação sem acesso à camada de aplicativo do link de comunicação estão excluídas
SHA	Secure Hash Algorithm. Uma família ou conjunto de funções criptográficas de hash. SHA-1 é geralmente a função mais usada. O uso de um valor salt único na função hashing reduz as chances de uma colisão de valores hashed
SNMP	Protocolo de Administração de uma Rede Simples (Simple Network Management Protocol). Suporta o acompanhamento de dispositivos ligados à rede em termos de quaisquer condições que demandem uma atenção administrativa
Split Knowledge	**Conhecimento Compartilhado.** Condição em que duas ou mais entidades separadamente possuem componentes importantes mas que individualmente não têm nenhum conhecimento sobre a chave criptográfica resultante
SQL	Structured (English) Query Language. Linguagem de computador usada para criar, modificar e recuperar dados de um sistema de administração de bancos de dados relacionais
SQL Injection	**Injeção SQL.** Forma de ataque a web site baseado em banco de dados. Um atacante executa comandos SQL não autorizados beneficiando-se de códigos inseguros nos sistemas conectados à Internet. Os ataques de injeção SQL são utilizados para furtar informações de um banco de dados onde a informação usualmente não estaria disponível e/ou obter acesso ao host de uma organização através do computador que está hospedando o banco de dados
SSH	Secure shell. Conjunto de protocolos que oferecem a codificação para os serviços de rede como login remoto ou transferência remota de arquivos
SSID	Service set identifier. Nome designado à rede sem fio WiFi ou IEEE 802.11
SSL	Secure sockets layer. Padrão estabelecido da indústria que codifica o canal entre um paginador e o servidor da web para assegurar a privacidade e confiabilidade do dado transmitido através deste canal

Termo	Definição
Strong Cryptography	**Criptografia Forte.** Termo geral para indicar uma criptografia que é extremamente resistente à análise criptográfica (cryptanalysis). Ou seja, com base no método criptográfico (algoritmo ou protocolo), a chave criptográfica ou dado protegido não se encontra exposto. A resistência baseia-se na chave criptográfica usada. O tamanho efetivo da chave deve atender ao tamanho mínimo de chave principal de resistência comparável recomendada. Uma referência para a resistência mínima comparável é encontrada na NIST Special Publication 800-57, de agosto de 2005 (http://csrc.nist.gov/publications/) ou outras que atendam os seguintes padrões mínimos de bits de chaves seguranças: • 80 bits para os sistemas baseados em uma chave secreta (por exemplo TDES) • 1024 bits de módulo para os algoritmos de chave pública baseados em função fatorial (por exemplo, RSA) • 1024 bits para um logaritmo discreto (por exemple, Diffie-Hellman) com um tamanho mínimo de 160 bits em um grande subgrupo (por exemplo, DSA) • 160 bits para criptografia de curva elíptica (por exemplo, ECDSA)
System Components	**Componentes de Sistema.** Qualquer componente de rede, servidor ou aplicativo incluído ou conectado ao ambiente de dados do portador de cartão
TACACS	Terminal access controller access control system. Protocolo de autenticação remota
Tamper-resistance	**Resistente à Falsificação.** Sistema que é difícil de modificar ou subverter, mesmo para um assaltante com acesso físico ao sistema
TCP	Protocolo de controle de transmissão (Transmission control protocol)
TDES	Padrão de Codificação de Dado Triplo (Triple Data Encription Standard) também conhecido como 3DES. Bloco cifrado (Block cipher) formado pelo DES cipher ao ser usado por três vezes consecutivas
TELNET	Protocolo de rede telefônica (Telephone network protocol). Geralmente usado para prover login em sessões de linha de comando orientada para o usuário entre os hosts na Internet. Programa originalmente desenvolvido para emular um único terminal conectado a outro computador
Threat	**Ameaça.** Condição que pode fazer com que a informação ou os recursos de processamento da informação sejam intencionalmente ou acidentalmente perdidos, modificados, expostos, tornados inacessíveis ou de outra forma afetados em detrimento da organização
TLS	Transport layer security. Criada com o objetivo de prover confidencialidade e integridade aos dados nas comunicações entre dois aplicativos. A TLS é a sucessora da SSL
Token	**Senha, Sinal.** Dispositivo que executa a autenticação dinâmica
Transaction Data	**Dado da Transação.** Dado relacionado com o pagamento eletrônico

Termo	Definição
Truncation	**Truncagem.** Prática de remover segmentos de dados. Geralmente, quando os números das contas estão truncados, os primeiros 12 dígitos são apagados, deixando apenas os 4 últimos dígitos
Two-factor Authentication	**Autenticação de Dois Fatores.** Autenticação que exige que os usuários utilizem duas credenciais para ter acesso ao sistema. As credenciais consistem em algo que o usuário tenha em sua posse (por exemplo, smartcards ou tokens de hardware) e algo que saibam, por exemplo, uma senha). Para ter acesso a um sistema, o usuário deve utilizar ambos os fatores
UDP	Protocolo de datagrama do usuário (User datagram protocol)
UserID	**ID do Usuário.** Uma seqüência de caracteres usada unicamente para identificar cada usuário de um sistema
Virus	**Vírus.** Programa ou seqüência de códigos que pode replicar-se e causar modificação ou destruição de software ou dado
VPN	Rede privada virtual (Virtual private network). Rede privada criada sobre uma rede pública
Vulnerability	**Vulnerabilidade,** Debilidade nos procedimentos de segurança de um sistema, no seu desenho, implementação ou controles internos, que podem ser explorados para violar as políticas de segurança do sistema
Vulnerability Scan	**Varredura de Vulnerabilidade.** Varredura usada para identificar as vulnerabilidades nos sistemas operacionais, serviços e dispositivos que podem ser usados por hackers para atacar a rede privativa de uma empresa
WEP	Wired equivalent privacy. Protocolo para prevenir a escuta acidental e objetivando a prestação de confidencialidade comparável à rede tradicional de linha terrestre. Não oferece segurança adequada contra a escuta clandestina intencional (por exemplo, análise criptográfica)
WPA	Acesso Protegido de WiFi (WiFi Protected Access (WPA and WPA2)). Protocolo de segurança para redes sem fio (WiFi). Criado em resposta às várias debilidades sérias existentes no protocolo WEP
XSS	Cross-site scripting. Tipo de vulnerabilidade de segurança geralmente encontrada nos aplicativos da web. Pode ser usado por um atacante para obter privilégios elevados no acesso a conteúdo confidencial das páginas, session cookies e uma variedade de outros objetos