A Abordagem Priorizada para Buscar a Conformidade do PCI DSS

O Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS) fornece uma estrutura detalhada de 12 Requisitos para proteger os dados do portador do cartão que são armazenados, processados e/ou transmitidos por comerciantes e outras organizações. Por sua natureza abrangente, o padrão fornece uma grande quantidade de informações sobre segurança - tanto que algumas pessoas que são responsáveis pela segurança dos dados do portador do cartão podem não saber por onde começar a jornada contínua de conformidade. Com esse objetivo, o PCI Security Standards Council fornece a seguinte Abordagem Priorizada para ajudar os interessados a compreender onde eles podem agir para reduzir o risco no início do processo de conformidade. Nenhuma etapa na Abordagem Priorizada fornecerá segurança abrangente ou conformidade com o PCI DSS, mas seguir suas diretrizes ajudará os interessados a agilizar o processo de proteção de dados do portador do cartão.

DESTAQUES

Pode ajudar comerciantes a identificaralvos de maior risco

Cria uma linguagem comum em todos os esforços de implementação e avaliação do PCI DSS

As etapas permitem que os comerciantes demonstrem o progresso no processo de conformidade

Qual é a Abordagem Priorizada?

A Abordagem Priorizada oferece seis etapas de segurança que ajudarão os comerciantes e outras organizações de forma gradual a se protegerem contra os fatores de maior risco e ameaças crescentes, enquanto estiverem no caminho para a conformidade com o PCI DSS. A Abordagem Priorizada e suas etapas (descritos na página 2) são destinados a oferecer os seguintes benefícios:

- Guia que uma organização pode usar para abordar seus riscos em ordem de prioridade
- Abordagem pragmática que permite "ganhos rápidos"
- Suporta planejamento financeiro e operacional
- Promove indicadores de progresso objetivos e mensuráveis
- Ajuda a promover a consistência entre avaliadores

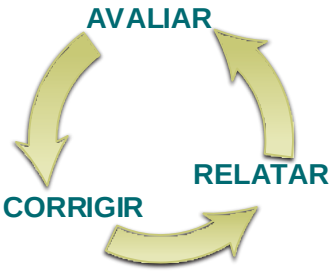
Objetivos da Abordagem Priorizada

A Abordagem Priorizada fornece um guia de atividades de conformidade com base no risco associado a armazenamento, processamento e/ou transmissão dos dados do portador do cartão. O guia ajuda a priorizar os esforços para alcançar a conformidade, estabelecer etapas, reduzir o risco de violações de dados do portador do cartão antecipadamente no processo de conformidade, e ajuda os adquirentes a medirem de forma objetiva as atividades de conformidade e a redução de riscos de comerciantes, prestadores de serviços, entre outros. A Abordagem Priorizada foi concebida depois de fatorar dados a partir de violações reais, e opiniões de Avaliadores de Segurança Qualificados, de investigadores forenses, e do Conselho do PCI Security Standards Council. Ela não é destinada a ser uma abordagem substituta, paliativa ou um atalho para a conformidade com o PCI DSS, nem é uma estrutura obrigatória única aplicável a todas as organizações. A Abordagem Priorizada é adequada para comerciantes que se submetem a uma avaliação local ou utilizam SAQ D.

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Maio de 2016

A CONFORMIDADE COM O PCI DSS É UM PROCESSO CONTÍNUO



FUNDADORES DO PCI SSC

ORGANIZAÇÕES PARTICIPANTES

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

Aviso Legal

Para atingir a conformidade com o PCI DSS, a organização deve satisfazer todos os Requisitos do PCI DSS, independentemente da ordem em que eles sejam cumpridos ou se a organização que solicita a conformidade segue a Abordagem Priorizada do PCI DSS. Este documento não modifica nem diminui o PCI DSS ou qualquer um de seus Requisitos e pode ser alterado sem aviso prévio.

O PCI SSC não é responsável por erros ou danos de qualquer natureza resultantes da utilização das informações aqui contidas. O PCI SSC não oferece nenhuma garantia, fiança ou representação de qualquer tipo relativa às informações aqui fornecidas, e não assume nenhuma responsabilidade ou obrigação em relação ao uso devido ou indevido de tais informações.

Etapas para Priorizar os Esforços de Conformidade com o PCI DSS

A Abordagem Priorizada inclui seis etapas. A matriz abaixo resume as metas e intenções de alto nível para cada etapa. O restante deste documento mapeia as etapas de cada um dos doze Requisitos do PCI DSS e seus sub-Requisitos.

Etapa	Metas
1	**Remover dados de autenticação confidenciais e limitar a retenção de dados.** Esta etapa tem como meta uma área fundamental de risco para as entidades que foram violadas. Lembre-se – se os dados de autenticação confidenciais e outros dados do portador do cartão não forem armazenados, os efeitos de uma violação serão altamente reduzidos. Se você não precisar, não os armazene
2	**Proteger sistemas e redes, e estar preparado para responder a uma violação no sistema.** Esta etapa visa a utilização de controles para pontos de acesso à maioria das violações, bem como processos de resposta.
3	**Proteger aplicativos de cartões de pagamento.** Esta etapa visa a utilização de controles para aplicativos, processos de aplicativos e servidores de aplicativos. Deficiências nessas áreas são presa fácil para violar sistemas e obter acesso aos dados do portador do cartão.
4	**Monitorar e controlar o acesso a seus sistemas.** Os controles desta etapa permitem detectar quem, o que, quando e como foi acessado seu ambiente de rede e de dados do portador do cartão.
5	**Proteger os dados armazenados do portador do cartão.** No caso das organizações que analisaram seus processos corporativos e determinaram que devem armazenar números de conta principal, a Etapa Cinco visa mecanismos fundamentais de proteção para esses dados armazenados.
6	**Finalizar os esforços de conformidade restantes e garantir que todos os controles estejam em vigor.** A intenção da Etapa Seis é concluir os requisitos do PCI DSS e finalizar todas as outras políticas, procedimentos e processos relacionados necessários para proteger o ambiente de dados do portador do cartão.

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão						
1.1 Defina e implemente os padrões de configuração do firewall e do roteador que incluam o seguinte:						
1.1.1 Um processo formal para aprovar e testar todas as conexões de rede e alterações às configurações do firewall e do roteador						6
1.1.2 Diagrama atual da rede que identifica todas as conexões entre o ambiente dos dados do titular do cartão e outras redes, incluindo qualquer rede sem fio	1					
1.1.3 Diagrama atual que mostra todos os fluxos de dados do portador do cartão em todos os sistemas e redes	1					
1.1.4 Requisitos para um firewall em cada conexão com a Internet e entre qualquer zona desmilitarizada (DMZ) e a zona de rede interna		2				
1.1.5 Descrição de grupos, funções e responsabilidades quanto ao gerenciamento dos componentes da rede						
1.1.6 Documentação de justificativa comercial e aprovação para uso de todos os serviços, protocolos e portas permitidas, inclusive documentação dos recursos de segurança implementados para os protocolos considerados não seguros.		2				
1.1.7 Requisito para analisar os conjuntos de regras do firewall e do roteador pelo menos a cada seis meses						6
1.2 Elabore configurações de firewall e roteador que restrinjam as conexões entre redes não confiáveis e qualquer componente do sistema no ambiente de dados do portador do cartão. *Observação: uma" rede não confiável" é qualquer rede que seja externa às redes que pertencem à entidade em análise e/ou que esteja além da capacidade da entidade de controlar ou gerenciar.*						
1.2.1 Restrinja o tráfego de entrada e saída ao que é necessário ao ambiente de dados do titular do cartão e rejeite especificadamente todos os outros tráfegos.		2				
1.2.2 Proteja e sincronize os arquivos de configuração do roteador.		2				
1.2.3 Instale firewalls de perímetro entre todas as redes sem fio e o ambiente de dados do portador do cartão e configure esses firewalls para recusar ou, se o tráfego for necessário para fins comerciais, permitir apenas tráfego autorizado entre o ambiente sem fio e o ambiente de dados do portador do cartão.		2				
1.3 Proibir o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do portador do cartão.						
1.3.1 Implemente uma DMZ para limitar o tráfego somente para componentes do sistema que oferece serviços, protocolos e portas acessíveis publicamente.		2				
1.3.2 Limite o tráfego de entrada da internet a endereços IP na DMZ.		2				
1.3.3 Implemente medidas contra falsificação para detectar e impedir que endereços IP de fonte falsificada entrem na rede. (Por exemplo, bloquear tráfego originado da internet com um endereço de fonte interna).		2				
1.3.4Não permita o tráfego de saída não autorizado do ambiente de dados do portador do cartão para a internet.		2				
1.3.5 Somente autorize conexões "estabelecidas" na rede.		2				

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
1.3.6 Implemente os componentes do sistema que armazenam dados do portador do cartão (como banco de dados) em uma zona da rede interna separada da DMZ e de outras redes não confiáveis.		2				
1.3.7 Não divulgue endereços IP privados e informações de roteamento a partes não autorizadas. *Observação: os métodos para ocultar o endereço IP podem incluir, entre outros:* • *Conversão de endereços de rede (NAT)* • *Implementação dos servidores contendo dados do portador do cartão atrás dos servidores de proxy/firewalls,* • *Remoção ou filtragem das propagandas de rota para redes privadas que empregam endereçamento registrado,* • *Uso interno do espaço de endereço RFC1918 em vez de endereço registrado.*		2				
1.4 Instale um software de firewall pessoal ou função equivalente em qualquer dispositivo portátil (inclusive de propriedade da empresa e/ou do funcionário) que se conecte à internet quando fora da rede (por exemplo, laptops usados pelos funcionários) e que também seja usado para acessar o CDE. As configurações do firewall (ou equivalente) incluem: • Os ajustes específicos de configuração são definidos. • O firewall pessoal (ou função equivalente) é executado ativamente. • O firewall pessoal (ou função equivalente) não pode ser alterado pelos usuários dos dispositivos de computação portáteis.		2				
1.5 Certifique-se de que as políticas de segurança e procedimentos operacionais do gerenciamento dos firewalls estejam documentados, em uso e conhecidos por todas as partes envolvidas.		2				
Requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança						
2.1 Sempre alterar os padrões disponibilizados pelo fornecedor e remover ou desabilitar contas padrão desnecessárias antes de instalar um sistema na rede. Isso se aplica a TODAS as senhas padrão, incluindo, entre outras, as utilizadas pelos sistemas operacionais, softwares que fornecem serviços de segurança, aplicativos e contas do sistema, terminais de ponto de venda (POS), aplicativos de pagamento, sequências de comunidade de Protocolo de Gerenciamento de Rede Simples (SNMP) etc.		2				
2.1.1 Em ambientes sem fio conectados ao ambiente de dados do titular do cartão ou que transmitam dados do titular do cartão, altere TODOS os padrões sem fio do fornecedor na instalação, inclusive, entre outros, chaves de criptografia padrão sem fio, senhas e strings de comunidades do SNMP.		2				
2.2 Desenvolva padrões de configuração para todos os componentes do sistema. Certifique-se de que esses padrões abrangem todas as vulnerabilidades de segurança conhecidas e estão em conformidade com os padrões de fortalecimento do sistema aceitos pelo setor. As fontes dos padrões de fortalecimento do sistema aceitos pelo setor podem incluir, entre outros: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • Instituto SysAdmin Audit Network Security (SANS) • National Institute of Standards and Technology (NIST).			3			

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
2.2.1 Implemente somente uma função principal por servidor para evitar funções que exigem diferentes níveis de segurança coexistindo no mesmo servidor. (Por exemplo, servidores Web, servidores do banco de dados e DNS devem ser implementados em servidores separados.) *Observação: Onde tecnologias de virtualização estiverem em uso, implemente somente uma função principal por componente do sistema virtual.*			3			
2.2.2 Habilite somente serviços, protocolos, daemons, etc., necessários para a função do sistema.			3			
2.2.3 Implemente recursos de segurança adicionais para todos os serviços, protocolos ou daemons exigidos considerados não seguros. *Observação: Onde SSL/antigo TLS for utilizado, os Requisitos do Apêndice A2 devem ser atendidos.*		2				
2.2.4 Configure os parâmetros de segurança do sistema para impedir o uso incorreto.			3			
2.2.5 Remova todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores Web desnecessários.			3			
2.3 Criptografe todo o acesso administrativo que não utiliza console usando criptografia forte. *Observação: Onde SSL/antigo TLS for utilizado, os Requisitos do Apêndice A2 devem ser atendidos.*		2				
2.4 Mantenha uma relação dos componentes do sistema que estão no escopo do PCI DSS.		2				
2.5 Certifique-se de que as políticas de segurança e procedimentos operacionais do gerenciamento dos padrões do fornecedor e outros parâmetros de segurança estejam documentados, em uso e conhecidos por todas as partes envolvidas.		2				
2.6 Os provedores de hospedagem compartilhada devem proteger cada ambiente hospedado da entidade e os dados do portador do cartão. Esses provedores devem atender a Requisitos específicos, conforme detalhado no Apêndice A1: Requisitos Adicionais do PCI DSS para Provedores de Hospedagem Compartilhada.			3			
Requisito 3: Proteger os dados armazenados do titular do cartão						
3.1 Mantenha a armazenagem dos dados do portador do cartão o mínimo possível, implementando políticas, processos e procedimentos de retenção e descarte de dados que incluem, pelo menos, o que segue para todo o armazenamento de dados do titular do cartão (CHD): • Limitar a quantia de dados armazenados e o tempo de retenção às restrições conforme os Requisitos legais, regulatórias e/ou comerciais • Requisitos de retenção específicos para dados do portador do cartão • Processos para exclusão segura de dados quando não mais necessários • Processos trimestrais para identificar e excluir com segurança os dados do titular do cartão que excederem a retenção definida.	1					
3.2 Não armazenar dados de autenticação confidenciais após a autorização (mesmo se estiverem criptografados). Se forem recebidos dados de autenticação confidenciais, processe todos os dados irrecuperáveis ao completar o processo de autorização. É permitido aos emissores e empresas que suportam serviços de emissão de armazenamento de dados de autenticação confidenciais se: • Houver uma justificativa comercial e • Os dados são armazenados com segurança. Os dados de autenticação confidenciais incluem os dados conforme mencionados nos seguintes Requisitos 3.2.1 até 3.2.3:	1					

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
3.2.1 Não armazene o conteúdo completo de qualquer rastreamento (da tarja magnética localizada na parte posterior do cartão, em dados equivalentes constando no chip ou outro local) após a autorização. Esses dados também são denominados como rastreamento completo, rastreamento, rastreamento 1, rastreamento 2 e dados da tarja magnética. Observação: no curso normal dos negócios, os seguintes elementos de dados da tarja magnética talvez precisem ser mantidos: • O nome do titular do cartão • O número da conta principal (PAN) • Data de vencimento • Código de serviço Para minimizar o risco, armazene somente os elementos de dados conforme necessário para os negócios.	1					
3.2.2 Não armazene o código ou valor de verificação do cartão (o número de três ou quatro dígitos impresso na frente ou no verso do cartão de pagamento usado para verificar transações sem cartão) após a autorização.	1					
3.2.3 Não armazene o número de identificação pessoal (PIN) ou o bloqueio de PIN criptografado após a autorização.	1					
3.3 Mascarar o PAN quando exibido (os primeiros seis e últimos quatro dígitos são o número máximo de dígitos a serem exibidos), de modo que somente funcionários com necessidade comercial legítima possam visualizar além dos seis primeiros/quatro últimos dígitos do PAN. *Observação: esse Requisito não substitui os Requisitos mais rigorosos em vigor quanto às exibições dos dados do portador do cartão, por exemplo, Requisitos legais ou da bandeira do cartão de pagamento para recebimentos de pontos de venda (POS).*					5	
3.4 Tornar o PAN ilegível em qualquer local onde ele esteja armazenado (inclusive dados em mídia digital portátil, mídia de backup e em registros) utilizando qualquer uma das seguintes abordagens: • Hash de direção única com base na criptografia forte (o hash deve ser do PAN inteiro) • Truncamento (a codificação hash não pode ser usada para substituir o segmento truncado do PAN) • Tokens e blocos de índice (os blocos devem ser armazenados de forma segura) • Criptografia forte com processos e procedimentos de gerenciamento-chave associados. *Observação: É um esforço relativamente simples para um indivíduo mal-intencionado reconstituir os dados do PAN original caso ele tenha acesso às versões truncadas e hash do PAN. Onde estiverem presentes versões obscurecidas e truncadas de mesmo PAN no ambiente da entidade, controles adicionais devem existir para garantir que as versões truncadas e obscurecidas não possam ser correlacionadas para reconstruir o PAN original.*					5	
3.4.1 Se a criptografia de dados for utilizada (em vez da criptografia de bancos de dados no nível de arquivo ou coluna), o acesso lógico deve ser gerenciado separadamente e independentemente de mecanismos de controle de acesso e autenticação do sistema operacional nativo (por exemplo, não utilizando bancos de dados de contas de usuário locais ou credenciais gerais de logon da rede). Chaves de decodificação não devem estar associadas a contas de usuários. *Observação: Este Requisito aplica-se também a todos os outros Requisitos de gerenciamento de chaves e criptografia do PCI DSS.*					5	
3.5 Registrar e implementar procedimentos para proteger as chaves utilizadas para armazenar os dados do portador do cartão de forma segura em relação a divulgações ou uso indevido: *Observação: Este Requisito aplica-se às chaves usadas para proteger dados armazenados do portador do cartão, e também às chaves de criptografia de chaves usadas para proteger as chaves de criptografia de dados. As chaves de criptografia de chaves devem ser, pelo menos, tão fortes quanto as chaves de criptografia dos dados.*						

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
3.5.1 Requisito adicional, somente para prestadores de serviços: Manter uma descrição documentada da arquitetura criptográfica que inclui: • Detalhes de todos os algoritmos, protocolos e chaves usados para a proteção dos dados do titular do cartão, inclusive a força da chave e a data de validade • Descrição do uso da chave para cada chave. • Inventário de HSMs e outras SCDs usadas para gerenciamento de chave *Observação: Este Requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se um Requisito.*					5	
3.5.2 Restrinja o acesso às chaves criptográficas ao menor número necessário de responsáveis pela proteção.					5	
3.5.3 Armazene chaves privadas e secretas usadas para criptografar/decodificar os dados do portador do cartão em uma (ou mais) das formas a seguir, em todos os momentos: • Criptografadas com uma chave de criptografia de chaves que seja ao menos tão forte quanto a chave de criptografia de dados e que esteja armazenada separadamente da chave de criptografia de dados. • Dentro de um dispositivo criptográfico seguro (por exemplo, um módulo de segurança de hardware (host) (HSM) ou dispositivo de ponto-de-interação aprovado por PTS). • Como duas partes de chave ou componentes de chave de tamanho total, de acordo com um método aceito pela empresa *Observação: não é exigido que chaves públicas sejam armazenadas em uma destas formas.*					5	
3.5.4 Armazene chaves criptográficas no menor número possível de locais.					5	
3.6 Documentar e implementar por completo todos os processos e procedimentos de gerenciamento-chave com relação às chaves criptográficas usadas para a criptografia dos dados do portador do cartão, incluindo o seguinte: *Observação: Vários padrões do setor para o gerenciamento de chaves estão disponíveis a partir de diversos recursos, incluindo NIST, que pode ser encontrado em http://csrc.nist.gov.*						
3.6.1 Geração de chaves criptográficas fortes					5	
3.6.2 Distribuição segura da chave criptográfica					5	
3.6.3 Armazenamento seguro de chaves criptográficas					5	
3.6.4 Troca de chave criptográfica para as chaves que chegaram ao final de seu cripto-período (por exemplo, após ter passado determinado período de tempo e/ou após certa quantidade de texto cifrado ter sido produzido por dada chave), conforme definido pelo fornecedor associado do aplicativo ou o dono da chave e com base nas práticas recomendadas e orientações do setor (por exemplo, a Publicação Especial NIST 800-57).					5	
3.6.5 Inutilização ou substituição (por exemplo, arquivamento, destruição e/ou revogação) de chaves consideradas necessárias quando a integridade da chave estiver enfraquecida (por exemplo, saída de um funcionário com conhecimento sobre um componente de chave de texto simples) ou quando houver suspeita de que a chave esteja comprometida. Observação: Caso chaves criptográficas inutilizadas ou recolocadas precisarem ser retidas, essas chaves deverão ser arquivadas em segurança (por exemplo, usando uma chave de criptografia de chaves). Chaves criptográficas arquivadas devem ser usadas somente para fins de decodificação/verificação.					5	

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
3.6.6 Se forem usadas operações manuais de gerenciamento de chave criptográfica de texto simples, essas operações devem ser gerenciadas com o uso de conhecimento separado e de controle duplo. Observação: Os exemplos de operações manuais de gerenciamento de chave incluem, entre outros: geração, transmissão, carregamento, armazenamento e destruição de chaves.					5	
3.6.7 Prevenção contra a substituição não autorizada de chaves criptográficas.					5	
3.6.8 Requisito para que os responsáveis pela proteção das chaves criptográficas assinem um formulário declarando que eles compreendem e aceitam suas responsabilidades pela proteção das chaves.					5	
3.7 Certificar que as políticas de segurança e procedimentos operacionais para a proteção dos dados armazenados do portador do cartão estejam documentados, em utilização, e sejam conhecidas por todas as partes afetadas.					5	
Requisito 4: Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas						
4.1 Usar protocolos de segurança e criptografia robusta para proteger dados confidenciais do portador do cartão durante a transmissão em redes abertas e públicas, incluindo os seguintes: • Somente chaves e certificados confiáveis são aceitos. • O protocolo em uso suporta apenas versões ou configurações seguras. • A força da criptografia é adequada para a metodologia de criptografia que está sendo utilizada. *Observação: Onde SSL/antigo TLS for utilizado, os Requisitos do Apêndice A2 devem ser atendidos.* *Os exemplos de redes abertas e públicas incluem, entre outros:* • *A internet* • *Tecnologias sem fio, incluindo 802.11 e Bluetooth* • *Tecnologia celular, por exemplo, Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA)* • *General Packet Radio Service (GPRS).* • *Comunicações por satélite.*		2				
4.1.1 Certifique-se de que as redes sem fio estejam transmitindo dados do titular do cartão ou estejam conectadas ao ambiente de dados do titular do cartão, siga as práticas recomendadas pelo setor para implementar a criptografia robusta na autenticação e transmissão.		2				
4.2 Jamais envie PANs desprotegidos por tecnologias de envio de mensagens ao usuário final (por exemplo, email, mensagens instantâneas, SMS, chat etc.).		2				
4.3 Certifique-se de que as políticas de segurança e procedimentos operacionais para criptografar as transmissões dos dados do portador do cartão estejam documentados, em utilização, e sejam conhecidos por todas as partes afetadas.		2				
Requisito 5: Usar e atualizar regularmente o software ou programas antivírus						
5.1 Implemente softwares de antivírus em todos os sistemas normalmente afetados por softwares mal-intencionados (especialmente em computadores pessoais e servidores).		2				
5.1.1 Certifique-se de que os programas antivírus sejam capazes de detectar, remover e proteger contra todos os tipos conhecidos de softwares mal-intencionados.		2				
5.1.2 Para sistemas que normalmente não são atacados por softwares mal-intencionados, execute avaliações periódicas para identificar e avaliar a evolução de ameaças de malware a fim de confirmar se tais sistemas continuam a não precisar de software de antivírus.		2				

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
5.2 Certifique-se de que todos os mecanismos antivírus sejam mantidos conforme segue: • São mantidos atualizados, • Executam varreduras periódicas • Geram logs de auditoria que são mantidos conforme o Requisito 10.7 do PCI DSS.		2				
5.3 Certifique-se de que os mecanismos antivírus estejam funcionando ativamente e não possam ser desativados ou alterados pelos usuários, a menos que seja especificamente autorizado pelo gerenciamento com base em cada caso por um período limitado de tempo. *Observação: as soluções de antivírus podem ser temporariamente desativadas apenas se houver necessidade técnica comprovada, conforme autorizado pelo gerenciamento com base em cada caso. Se a proteção antivírus precisar ser desativada por um motivo específico, isso deve ser formalmente autorizado. Medidas adicionais de segurança também podem precisar ser implementadas pelo período de tempo durante o qual a proteção antivírus não estiver ativa.*		2				
5.4 Certifique-se de que as políticas de segurança e procedimentos operacionais para proteger os sistemas contra malware estejam documentados, em utilização, e sejam conhecidos por todas as partes afetadas.		2				
Requisito 6: Desenvolver e manter sistemas e aplicativos seguros						
6.1 Estabeleça um processo para identificar as vulnerabilidades de segurança, usando fontes externas de boa reputação para informações de vulnerabilidades da segurança e atribua uma escala de risco (por exemplo, alto, médio ou baixo) para vulnerabilidades de segurança recentemente descobertas. *Observação: as classificações de risco devem ser baseadas nas práticas recomendadas pelo setor, bem como a consideração de impacto potencial. Por exemplo, os critérios para classificar as vulnerabilidades podem incluir a consideração da marca da base CVSS e/ou a classificação pelo fornecedor e/ou os tipos de sistemas afetados.* *Os métodos para avaliar as vulnerabilidades e classificar o nível de risco variam com base no ambiente das organizações e na estratégia de avaliação de risco. As classificações de risco devem, no mínimo, identificar todas as vulnerabilidades consideradas de alto risco ao ambiente. Além da classificação de risco, as vulnerabilidades podem ser consideradas críticas se apresentarem uma ameaça iminente ao ambiente, sistemas críticos de impacto e/ou resultariam em uma possível violação se não resolvidas. Exemplos de sistemas críticos podem incluir sistemas de segurança, dispositivos voltados ao público e sistemas, bancos de dados e outros sistemas que armazenam, processam ou transmitem dados do titular do cartão.*			3			
6.2 Certifique-se de que todos os componentes do sistema e softwares estejam protegidos de vulnerabilidades conhecidas instalando os patches de segurança aplicáveis disponibilizados pelos fornecedores. Instale patches de segurança críticos em até um mês após o lançamento. *Observação: os patches de segurança crítica devem ser identificados de acordo com o processo de classificação de risco definido no Requisito 6.1.*			3			
6.3 Desenvolva aplicativos de software internos e externos (incluindo acesso administrativo pela Web aos aplicativos) com segurança, conforme segue: • De acordo com o PCI DSS (por exemplo, autenticação e logs seguros) • Baseados nos padrões e/ou práticas recomendadas pelo setor. • Incorporar segurança da informação ao longo da vida útil do desenvolvimento do software. *Observação: isso se aplica a todos os softwares desenvolvidos internamente, bem como a softwares personalizados ou sob encomenda desenvolvidos por terceiros.*			3			
6.3.1 Remova as contas de desenvolvimento, teste e/ou personalizados, IDs de usuário e senhas antes que o aplicativo se torne ativo ou seja lançado aos clientes.			3			

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
6.3.2 Revise o código personalizado antes da liberação para produção ou clientes a fim de identificar qualquer possível vulnerabilidade no código (usando processos manuais ou automatizados) para incluir ao menos o seguinte: • As alterações dos códigos são analisadas por outras pessoas além do autor do código e por pessoas que estão cientes das técnicas de análise dos códigos e das práticas de codificação seguras. • As revisões de código garantem que o código seja desenvolvido de acordo com as diretrizes de codificação seguras. • As correções adequadas são implementadas antes da liberação. • Os resultados das análises dos códigos são revisados e aprovados pelo gerenciamento antes da liberação. *Observação: Este Requisito referente às análises dos códigos aplica-se a todos os códigos personalizados (internos e voltados ao público), como parte integrante do ciclo de vida de desenvolvimento do sistema. As análises dos códigos podem ser realizadas por equipes internas instruídas ou terceiros. Os aplicativos da Web voltados ao público também estão sujeitos a controles extras para abranger ameaças e vulnerabilidades contínuas após a implementação, conforme definido no Requisito 6.6 do PCI DSS.*			3			
6.4 Siga os procedimentos de controle de alterações para todas as alterações nos componentes do sistema. Esses processos devem incluir o seguinte:			3			
6.4.1 Separe os ambientes de teste/desenvolvimento do ambiente de produção e reforce a separação com controle de acesso.			3			
6.4.2 Separação dos deveres entre os ambientes de desenvolvimento/teste e de produção			3			
6.4.3 Os dados de produção (PANs ativos) não são usados para testes ou desenvolvimento			3			
6.4.4 Exclusão dos dados de teste e contas dos componentes do sistema antes do sistema tornar-se ativo/entrar em produção.			3			
6.4.5 Mudanças nos procedimentos de controle devem incluir o seguinte:						6
6.4.5.1 Documentação de impacto.						6
6.4.5.2 Aprovação documentada de alteração pelas partes autorizadas.						6
6.4.5.3 Teste de funcionalidade para verificar se a alteração não tem impacto adverso sobre a segurança do sistema.						6
6.4.5.4 Procedimentos de reversão.						6
6.4.6 Após concluir uma mudança significativa, todos os Requisitos relevantes do PCI DSS devem ser implementados em todos os sistemas novos ou alterados e nas redes; a documentação deve ser atualizada, conforme aplicável. *Observação: Este Requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se um Requisito.*						6
6.5 Trate as vulnerabilidades de codificação comuns nos processos de desenvolvimento do software conforme segue: • Ofereça treinamento aos desenvolvedores, pelo menos anualmente, transmitindo técnicas de codificação de segurança atualizadas, entre as quais, como evitar vulnerabilidades comuns de codificação. • Desenvolva aplicativos baseados nas diretrizes de código seguro. *Observação: as vulnerabilidades listadas nos itens 6.5.1 a 6.5.10 estavam atualizadas de acordo com as práticas recomendadas pelo setor, quando esta versão do PCI DSS foi publicada. No entanto, conforme as práticas recomendadas pelo setor para o gerenciamento de vulnerabilidades são atualizadas (por exemplo, o Guia OWASP, SANS CWE Top 25, CERT Secure Coding, etc.), as atuais práticas recomendadas devem ser usadas para estes Requisitos.*			3			
Observação: Os Requisitos 6.5.1 a 6.5.6 abaixo aplicam-se a todos os aplicativos (internos ou externos).						

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
6.5.1 Falhas na injeção, particularmente na injeção SQL. também considere as falhas de injeção OS Command Injection, LDAP e XPath, assim como outras falhas.			3			
6.5.2 Sobrecargas do buffer			3			
6.5.3 Armazenamento criptográfico não seguro			3			
6.5.4 Comunicações não seguras			3			
6.5.5 Tratamento incorreto de erros			3			
6.5.6 Todas as vulnerabilidades de "alto risco" identificadas no processo de identificação de vulnerabilidade (conforme definido no Requisito 6.1 do PCI DSS).			3			
Observação: Os Requisitos 6.5.7 a 6.5.10 abaixo aplicam-se a aplicativos da Web e a interfaces de aplicativos (internos ou externos):						
6.5.7 Script intersite (XSS)			3			
6.5.8 Controle de acesso inadequado (como referências diretas não seguras a objetos, falhas em restringir o acesso a URLs, diretórios transversais e falhas em restringir o acesso do usuário às funções).			3			
6.5.9 Solicitação intersite forjada (CSRF).			3			
6.5.10 Autenticação quebrada e gerenciamento de sessão			3			
6.6 Para aplicativos da Web voltados ao público, trate novas ameaças e vulnerabilidades continuamente e assegure que esses aplicativos estejam protegidos contra invasões conhecidos por meio de qualquer um dos métodos a seguir: • Analisar os aplicativos da Web voltados ao público por meio de ferramentas ou métodos manuais ou automáticos de avaliação de segurança das vulnerabilidades dos aplicativos, pelo menos anualmente e após quaisquer alterações *Observação: esta avaliação não é igual às varreduras de vulnerabilidades realizadas para o Requisito 11.2.* • Instalar uma solução técnica automatizada que detecte e previna invasões baseadas na Web (por exemplo, um firewall de aplicativo na Web) na frente de aplicativos da Web voltados para o público, para verificar continuamente todo o tráfego.			3			
6.7 Certifique-se de que as políticas de segurança e procedimentos operacionais para desenvolver e manter os sistemas e aplicativos estejam documentados, em utilização, e sejam conhecidos por todas as partes afetadas.			3			
Requisito 7: restringir o acesso aos dados do portador do cartão de acordo com a necessidade de conhecimento para o negócio						
7.1 Limitar o acesso aos componentes do sistema e aos dados do portador do cartão somente àquelas pessoas cuja função requer tal acesso.						
7.1.1 Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para realizar seu trabalho • O nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar os recursos.				4		
7.1.2 Restrinja o acesso a IDs de usuários privilegiados ao menor número de privilégios necessários para desempenhar as responsabilidades da função.				4		
7.1.3 Conceda acesso com base na classificação e na atribuição da função de cada indivíduo da equipe.				4		

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
7.1.4 Solicite aprovação documentada por partes autorizadas especificando os privilégios exigidos.				4		
7.2 Estabeleça sistema(s) de controle de acesso para os componentes do sistemas que limitam o acesso com base na necessidade de conhecimento do usuário e que estão configurados para "recusar todos", salvo se houver permissão específica. O(s) sistema(s) de controle de acesso deve(m) incluir o seguinte:						
7.2.1 Abrangência de todos os componentes do sistema				4		
7.2.2 A concessão dos privilégios aos indivíduos está baseada na classificação e na atribuição da função.				4		
7.2.3 Configuração padrão “recusar todos”.				4		
7.3 Certifique-se de que as políticas de segurança e os procedimentos operacionais para restringir o acesso aos dados do portador do cartão estejam documentados, em utilização, e sejam conhecidos por todas as partes afetadas.				4		
Requisito 8: Atribuir uma identidade exclusiva para cada pessoa que tenha acesso ao computador						
8.1 Defina e implemente políticas e procedimentos para garantir o gerenciamento adequado da identificação do usuário para usuários que não sejam clientes e administradores em todos os componentes do sistema, conforme segue:						
8.1.1 Atribua a todos os usuários uma identificação exclusiva antes de permitir acesso aos componentes do sistema ou aos dados do titular do cartão.		2				
8.1.2 Controle o acréscimo, a exclusão e a modificação dos IDs do usuário, credenciais e outros objetos do responsável pela identificação.		2				
8.1.3 Revogue imediatamente o acesso de quaisquer usuários desligados da empresa.		2				
8.1.4 Remover/desativar contas inativas do usuário no prazo de 90 dias.		2				
8.1.5 Controle as IDs usadas por terceiros para acessar, dar suporte ou manter os componentes do sistema via acesso remoto, conforme segue: • Ativar apenas durante o período necessário e desativar quando não estiverem em uso. • Monitorar quando estiverem em uso.		2				
8.1.6 Limite tentativas de acesso repetidas bloqueando o ID do usuário após seis tentativas, no máximo.		2				
8.1.7 Defina a duração do bloqueio para um mínimo de 30 minutos ou até que o administrador ative o ID do usuário.		2				
8.1.8 Se uma sessão estiver ociosa por mais de 15 minutos, solicite que o usuário redigite a senha para reativar o terminal.		2				
8.2 Além de atribuir uma ID exclusiva, garanta que um controle adequado da autenticação do usuário para usuários que não sejam clientes e administradores em todos os componentes do sistema, empregando pelo menos um dos métodos a seguir para autenticar todos os usuários: • 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.		2				
8.2.1 Use criptografia forte, converta todas as credenciais de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os componentes do sistema.		2				
8.2.2 Verifique a identidade do usuário antes de modificar qualquer credencial de autenticação, por exemplo, executar restauração da senha, provisionar novos tokens ou gerar novas chaves.		2				

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
8.2.3 As senhas/frases-senha devem atender ao seguinte: • Exigir uma extensão mínima de pelo menos sete caracteres. • Conter caracteres numéricos e alfabéticos. Alternativamente, as senhas/frases secretas devem ter complexidade e força pelo menos equivalentes aos parâmetros especificados acima.		2				
8.2.4 Altere as senhas/frases-senha do usuário, pelo menos, a cada 90 dias.		2				
8.2.5 Não permita que ninguém envie uma nova senha/frase-senha que seja igual a uma das quatro últimas senhas/frases-senha usadas.		2				
8.2.6 Defina as senhas/frases-senha para o primeiro uso e ao reiniciar com um valor exclusivo para cada usuário; a alteração deve ser imediata, após a primeira utilização.		2				
8.3 Todo acesso administrativo individual que não utiliza console e todo acesso remoto ao CDE são protegidos por autenticação multifatorial. *Observação: A autenticação multifatorial exige que, no mínimo, dois dos três métodos de autenticação (consultar Requisito 8.2 para ver descrições dos métodos de autenticação) sejam usados para autenticação. Usar um fator duas vezes (por exemplo, usar duas senhas separadas) não é considerado como autenticação multifatorial.*						
8.3.1 Incorporar a autenticação multifatorial em todos os acessos que não utilizam console no CDE para funcionários com acesso administrativo. *Observação: Este Requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se um Requisito.*		2				
8.3.2 Incorpore a autenticação multifatorial para todos os acessos remotos à rede (usuário e administrador, incluindo o acesso de terceiros para suporte ou manutenção) provenientes de fora da rede da entidade.		2				
8.4 Registre e comunique os procedimentos e políticas de autenticação para todos os usuários, inclusive: • Orientação sobre selecionar credenciais fortes de autenticação • Orientação sobre como os usuários devem proteger suas credenciais de autenticação • Instruções para não reutilizar senhas anteriormente usadas • Instruções para alterar a senha se houver suspeita de que ela possa estar comprometida.				4		
8.5 Não use IDs de grupos, compartilhados ou genéricos, senhas ou outros métodos de autenticação conforme segue: • IDs genéricos de usuários são desativados ou removidos. • IDs de usuários compartilhados não existem para a administração do sistema e outras funções críticas. • IDs de usuários compartilhados e genéricos não são usados para administrar quaisquer componentes do sistema.				4		
8.5.1 Requisito adicional, somente para prestadores de serviços: Os prestadores de serviço com acesso remoto ao local do cliente (por exemplo, para suporte de servidores ou sistemas POS) devem usar uma credencial de autenticação exclusiva (como uma senha/frase) para cada cliente. *Observação: Este Requisito não é destinado a provedores de hospedagem compartilhada que acessam seu próprio ambiente de hospedagem, onde vários ambientes do cliente são hospedados.*		2				

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
8.6 Onde forem usados outros mecanismos de autenticação (por exemplo, tokens de segurança físicos ou virtuais, smart cards, certificados, etc.), o uso destes mecanismos deve ser atribuído conforme segue: • Os mecanismos de autenticação devem ser atribuídos a uma conta individual e não compartilhados entre várias contas. • Controles físicos e/ou virtuais devem ser implementados para garantir que apenas a conta pretendida possa usar o mecanismo para obter acesso.				4		
8.7 Todos os acessos a qualquer banco de dados que contenha dados do portador do cartão (inclusive acesso por meio de aplicativos, por administradores e demais usuários) são restritos, conforme segue: • Todos os acessos, consultas e ações do usuário no banco de dados ocorrem através de métodos programáticos. • Apenas os administradores do banco de dados podem acessar diretamente ou consultar o banco de dados. • Os IDs dos aplicativos para os aplicativos do banco de dados só podem ser usados pelos aplicativos (e não por usuários individuais ou outros processos sem aplicativo).				4		
8.8 Certifique-se de que as políticas de segurança e procedimentos operacionais para identificação e autenticação estejam documentados, em utilização, e sejam conhecidos por todas as partes afetadas.				4		
Requisito 9: restringir o acesso físico aos dados do portador do cartão do cartão						
9.1 Use controles de entrada facilitados e adequados para limitar e monitorar o acesso físico aos sistemas no ambiente de dados do titular do cartão.		2				
9.1.1 Use câmeras de vídeo ou outros mecanismos de controle de acesso (ou ambos) para monitorar o acesso físico individual a áreas sensíveis. Analise os dados coletados e relacione com outras entradas. Armazene, por pelo menos três meses, a menos que seja restringido de outra forma pela lei. *Observação: "Áreas confidenciais" referem-se a 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 áreas voltadas ao público nas quais há somente terminais do ponto de venda presentes, como as áreas dos caixas em uma loja de varejo.*		2				
9.1.2 Implemente controles físicos e/ou virtuais para restringir o acesso a pontos de rede acessíveis publicamente. Por exemplo, pontos de rede localizados em áreas públicas e áreas acessíveis a visitantes podem ser desativados e somente ativados quando o acesso à rede é explicitamente autorizado. Alternativamente, processos podem ser implementados para garantir que os visitantes sempre sejam acompanhados nas áreas com pontos de rede ativos.		2				
9.1.3 Restrinja o acesso físico a pontos sem fio de acesso, gateways, dispositivos portáteis, hardwares de comunicação/rede e linhas de telecomunicação.		2				
9.2 Desenvolva procedimentos para diferenciar facilmente a equipe interna dos visitantes e inclua: • Identificação de funcionários e visitantes no local (por exemplo, crachás de identificação) • Modificações nos Requisitos de acesso • Anular ou excluir identificações de funcionários que se desligaram da empresa e de visitantes que encerraram sua atividade (como crachás de identificação).					5	
9.3 Controle o acesso físico dos funcionários às áreas sensíveis, conforme segue: • O acesso deve ser autorizado e com base na função do indivíduo. • O acesso é anulado imediatamente ao término da atividade e todos os mecanismos de acesso físico, como chaves, cartões de acesso, etc., são devolvidos e desativados.		2				

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
9.4 Implemente procedimentos para identificar e autorizar visitantes. Os procedimentos devem incluir o seguinte:						
9.4.1 Os visitantes devem obter autorização antes de entrar e serem sempre acompanhados em áreas nas quais os dados do titular do cartão são processados ou mantidos.					5	
9.4.2 Os visitantes são identificados e recebem um crachá ou outra identificação com prazo de validade e que distingue visivelmente os visitantes dos funcionários internos.					5	
9.4.3 É solicitado que os visitantes apresentem o crachá ou identificação antes de sair das dependências ou na data do vencimento.					5	
9.4.4 Um registro de visitantes é usado para manter uma trilha de auditoria da atividade do visitante nas dependências, assim como aos ambientes com computador e centrais de dados onde os dados do titular do cartão são armazenados ou transmitidos. Documente no registro o nome do visitante, a empresa representada e o funcionário que autoriza o acesso físico. Armazene esse registro por pelo menos três meses, a menos que seja restringido de outra forma pela lei.					5	
9.5 Proteja toda a mídia fisicamente.					5	
9.5.1 Armazene backups de mídia em um local seguro, preferencialmente em outras instalações, como um lugar alternativo de backup ou uma instalação comercial de armazenamento. Analise a segurança do local pelo menos uma vez por ano.					5	
9.6 Mantenha controle rigoroso quanto à distribuição interna ou externa de qualquer tipo de mídia, incluindo o seguinte:						
9.6.1 Classifique a mídia para que a confidencialidade dos dados possa ser determinada.					5	
9.6.2 Envie a mídia via mensageiro seguro ou outro método de entrega que possa ser monitorado com precisão.					5	
9.6.3 Certifique-se de que o gerenciamento aprova quaisquer e todas as mídias que são movidas de uma área segura (incluindo quando as mídias forem distribuídas às pessoas).					5	
9.7 Mantenha um controle rigoroso sobre o armazenamento e a acessibilidade das mídias.						
9.7.1 Mantenha adequadamente os registros do inventário de todas as mídias e realize inventários das mídias pelo menos uma vez por ano.					5	
9.8 Destrua as mídias quando não forem mais necessárias por motivos legais ou de negócios, conforme segue:						
9.8.1 Triture, incinere ou amasse materiais impressos para que os dados do titular do cartão não possam ser recuperados. Contêineres de armazenamento usados para os materiais a serem destruídos.	1					
9.8.2 Torne os dados do titular do cartão nas mídias eletrônicas irrecuperáveis para que esses dados não possam ser reconstituídos.	1					
9.9 Proteja contra falsificação e substituição os dispositivos que capturam os dados do cartão de pagamento por meio de interação física direta com o cartão. *Observação: Estes Requisitos se aplicam aos dispositivos de leitura do cartão usados em transações com a presença do cartão (ou seja, de passar ou inserir) no ponto de venda. Este Requisito não é destinado aos componentes de entrada de chave manual, como teclados de computador e teclados de POS.*						
9.9.1 Mantenha uma lista atualizada de dispositivos. A lista deve incluir o seguinte: • Marca, modelo do dispositivo • Localização do dispositivo (por exemplo, o endereço do local ou instalação onde o dispositivo está localizado) • Número de série do dispositivo ou outro método de identificação exclusivo.		2				

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
9.9.2 Inspecione periodicamente as superfícies dos dispositivos para detectar adulteração (por exemplo, adição de espiões aos dispositivos), ou substituição (por exemplo, verificando o número de série ou outras características do dispositivo para verificar se ele não foi trocado por um dispositivo fraudulento). *Observação: exemplos de sinais de que um dispositivo possa ter sido adulterado ou substituído incluem apêndices inesperados ou cabos conectados ao dispositivo, rótulos de segurança alterados ou ausentes, revestimento quebrado ou de cor diferente, ou alterações no número de série ou outras marcas externas.*		2				
9.9.3 Treine os funcionários para que estejam cientes das tentativas de adulteração ou substituição de dispositivos. O treinamento deve incluir o seguinte: • Verifique a identidade de qualquer terceiro que alegue ser da equipe de manutenção ou reparo, antes de conceder acesso para modificar ou resolver problemas nos dispositivos. • Não instale, substitua ou devolva dispositivos sem verificação. • Esteja atento a comportamentos suspeitos ao redor dos dispositivos (por exemplo, tentativas de desconectar ou abrir os dispositivos por pessoas desconhecidas). • Reporte comportamentos suspeitos e indicações de adulteração ou substituição para a equipe apropriada (por exemplo, para um gerente ou funcionário da segurança).		2				
9.10 Certifique-se de que as políticas de segurança e procedimentos operacionais para restringir o acesso físico aos dados do portador do cartão estejam documentados, em utilização, e sejam conhecidos por todas as partes afetadas.					5	
Requisito 10: acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão						
10.1 Implemente trilhas de auditoria para ligar todos os acessos aos componentes do sistema para cada usuário individualmente.				4		
10.2 Implementar trilhas de auditoria automatizadas para todos os componentes do sistema para recuperar os seguintes eventos:						
10.2.1 Todos os acessos de usuários individuais aos dados do titular do cartão				4		
10.2.2 Todas as ações desempenhadas por qualquer pessoa com privilégios raiz ou administrativos				4		
10.2.3 Acesso a todas as trilhas de auditoria				4		
10.2.4 Tentativas inválidas de acesso lógico				4		
10.2.5 O uso e as alterações dos mecanismos de identificação e autenticação, inclusive, entre outros, a criação de novas contas, aumento de privilégios e demais alterações, adições ou exclusões de contas com privilégios raiz ou administrativos				4		
10.2.6 Inicialização, interrupção ou pausa dos registros de auditoria				4		
10.2.7 Criação e exclusão de objetos do nível do sistema				4		
10.3 Registrar pelo menos as seguintes entradas das trilhas de auditoria para todos os componentes do sistema para cada evento:						
10.3.1 Identificação do usuário				4		
10.3.2 Tipo de evento				4		
10.3.3 Data e horário				4		
10.3.4 Indicação de sucesso ou falha				4		
10.3.5 Origem do evento				4		
10.3.6 A identidade ou o nome dos dados afetados, componentes do sistema ou recurso.				4		

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
10.4 Usando tecnologia de sincronização de tempo, sincronize todos os relógios e horários críticos do sistema e assegure-se de que os seguintes itens sejam implementados para adquirir, distribuir e armazenar horários. *Observação: um exemplo de tecnologia de sincronização de horários é o Network Time Protocol (NTP).*				4		
10.4.1 Sistemas críticos têm o horário correto e consistente.				4		
10.4.2 Os dados de horário são protegidos.				4		
10.4.3 As definições de horário são recebidas de fontes de horário aceitas pelo setor.				4		
10.5 Proteger as trilhas de auditoria para que não possam ser alteradas.						
10.5.1 Limite a exibição de trilhas de auditoria às pessoas que têm uma necessidade relacionada à função.				4		
10.5.2 Proteja os arquivos de trilha de auditoria de modificações não autorizadas.				4		
10.5.3 Faça imediatamente o backup dos arquivos de trilha de auditoria em um servidor de registros centralizado ou mídias que sejam difíceis de alterar.				4		
10.5.4 Documente registros quanto às tecnologias externas em um servidor de registros centralizado, seguro ou dispositivo de mídia.				4		
10.5.5 Use softwares de monitoramento da integridade dos arquivos ou de detecção de alterações nos logs para assegurar que os dados de registro existentes não possam ser alterados sem gerar alertas (embora os novos dados que estejam sendo adicionados não gerem um alerta).				4		
10.6 Inspecione os logs e ocorrências de segurança para todos os componentes do sistema a fim de identificar irregularidades ou atividades suspeitas. *Observação: Ferramentas de coleta, análise e alerta dos logs podem ser usados para atender a este requisito.*						
10.6.1 Revise o que segue ao menos diariamente: • Todas as ocorrências de segurança • Registros de todos os componentes do sistema que armazenam, processam ou transmitem CHD e/ou SAD • Logs de todos os componentes críticos do sistema • Logs de todos os servidores e componentes do sistema que desempenham funções de segurança (por exemplo, firewalls, sistemas de detecção de invasão/sistemas de prevenção contra invasão (IDS/IPS), servidores de autenticação, servidores de redirecionamento do E-commerce, etc.).				4		
10.6.2 Revise os logs de todos os outros componentes do sistema periodicamente com base nas políticas e estratégia de gerenciamento de risco da organização, conforme determinado pela avaliação de risco anual da organização.				4		
10.6.3 Acompanhe as exceções e irregularidades identificadas durante o processo de revisão.				4		
10.7 Mantenha um histórico da trilha de auditoria por pelo menos um ano, com um mínimo de três meses imediatamente disponível para análise (por exemplo, online, arquivado ou recuperável a partir do backup).				4		

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
10.8 Requisito adicional, somente para prestadores de serviços: Implementar processo para detecção e emissão de relatórios de falhas dos sistemas de controle de segurança crítica, inclusive, entre outros, falhas relacionadas a: • Firewalls • IDS/IPS • FIM • Antivírus • Controles de acesso físico • Controles de acesso lógico • Mecanismos de registro de auditoria • Controles de segmentação (se usados) *Observação: Este Requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se um Requisito.*				4		
10.8.1 Requisito adicional, somente para prestadores de serviços: Solucionar falhas nos controles de segurança crítica em tempo hábil. Os processos para solucionar falhas nos controles de segurança devem incluir: • Restabelecimento de funções de segurança • Identificação e documentação da duração (data e hora do início ao fim) da falha de segurança • Identificar e documentar as causas de falha, incluindo a causa raiz e documentar a correção necessária para tratar da causa raiz. • Identificação e tratamento de quaisquer questões de segurança que surgiram durante a falha • Proceder à avaliação de riscos para determinar a necessidade de outras ações como resultado da falha na segurança • Implementação de controles para prevenir a causa da falha de reocorrer • Retomar o monitoramento dos controles de segurança *Observação: Este Requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se um Requisito.*				4		
10.9 Certifique-se de que as políticas de segurança e os procedimentos operacionais para monitoramento de todos os acessos aos recursos da rede e aos dados do portador do cartão estejam documentados, em utilização, e sejam conhecidos por todas as partes afetadas.				4		
Requisito 11: testar regularmente os sistemas e processos de segurança						
11.1 Implemente processos para testar a presença de pontos de acesso sem fio (802.11) e detectar e identificar todos os pontos de acesso sem fio autorizados e não autorizados trimestralmente. *Observação: Métodos que podem ser usados no processo incluem, entre outros, varreduras de rede sem fio, inspeções físicas/virtuais de componentes e infraestrutura do sistema, controle de acesso à rede (NAC) ou IDS/IPS sem fio. Qualquer método usado deve ser suficiente para detectar e identificar dispositivos autorizados e não autorizados.*				4		
11.1.1 Mantenha um inventário de pontos de acesso sem fio autorizados incluindo uma justificativa comercial documentada.				4		
11.1.2 Implemente procedimentos de resposta a incidentes para o caso de serem detectados pontos de acesso sem fio não autorizados.		2				

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
11.2 Execute varreduras quanto à presença de vulnerabilidades das redes internas e externas pelo menos trimestralmente e após qualquer mudança significativa na rede (como instalações de novos componentes do sistema, mudanças na topologia da rede, modificações das normas do firewall, aprimoramentos de produtos). *Observação: vários relatórios de varredura podem ser combinados no processo de varredura trimestral para mostrar que todos os sistemas foram mapeados e que todas as vulnerabilidades aplicáveis foram resolvidas. Pode ser exigida uma documentação adicional para verificar se as vulnerabilidades não resolvidas estão em processo de serem solucionadas.* *Para a conformidade inicial com o PCI DSS, não é necessário que as quatro varreduras trimestrais aprovadas sejam concluídas se o assessor verificar que 1) o resultado da varredura mais recente foi uma varredura aprovada, 2) a entidade possui políticas e procedimentos documentados que requerem a sequência de varreduras trimestrais e 3) as vulnerabilidades observadas nos resultados da varredura tenham sido corrigidas conforme mostrado em uma nova varredura. Nos anos seguintes após a análise inicial do PCI DSS, quatro varreduras trimestrais aprovadas devem ter ocorrido.*		**2**				
11.2.1 Realizar varreduras para verificação de vulnerabilidade interna trimestralmente. Solucionar vulnerabilidades e executar novas varreduras para verificar se todas as vulnerabilidades de "alto risco" foram resolvidas de acordo com a classificação de vulnerabilidades da entidade (conforme Requisito 6.1). As varreduras devem ser realizadas por uma equipe qualificada.		**2**				
11.2.2 Realize varreduras externas trimestrais de vulnerabilidades por meio de um Fornecedor de Varreduras Aprovado (ASV) qualificado pelo Conselho de padrões de segurança da Indústria de cartões de pagamento (PCI SSC). Realiza novas varreduras conforme necessário, até que se chegue a varreduras aprovadas. *Observação: as varreduras externas trimestrais de vulnerabilidades devem ser realizadas por um Fornecedor de Varreduras Aprovado (ASV) qualificado pelo Conselho de padrões de segurança da indústria de cartões de pagamento (PCI SSC). Consulte o Guia do programa ASV publicado no site do PCI SSC para saber sobre responsabilidades de varredura do cliente, preparação de varredura, etc.*		**2**				
11.2.3 Realize varreduras internas e externas e novas varreduras se necessário, após qualquer mudança significativa. As varreduras devem ser realizadas por uma equipe qualificada.		**2**				
11.3 Implemente uma metodologia para testes de penetração que inclua o seguinte: • É baseada nas abordagens de testes de penetração aceitas pelo setor (por exemplo, NIST SP800-115) • Abrange todo o perímetro do CDE e sistemas críticos • Inclui testes de dentro e fora da rede • Inclui testes para validar qualquer controle de redução no escopo e segmentação • Define testes de penetração na camada do aplicativo para incluir, pelo menos, as vulnerabilidades listadas no Requisito 6.5 • Define testes de penetração na camada da rede que incluam componentes compatíveis com as funções da rede e com os sistemas operacionais • Inclui revisão e consideração de ameaças e vulnerabilidades ocorridas nos últimos 12 meses • Especifica a conservação dos resultados de testes de penetração e resultados de atividades de reparo.						
11.3.1 Realize testes de penetração externos pelo menos uma vez ao ano e após qualquer melhoria ou modificação significativa na infraestrutura ou nos aplicativos (como uma melhoria no sistema operacional, uma sub-rede adicionada ao ambiente ou um servidor da Web adicionado ao ambiente).		**2**				

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
11.3.2 Realize testes de penetração internos pelo menos uma vez ao ano e após qualquer melhoria ou modificação significativa na infraestrutura ou nos aplicativos (como uma melhoria no sistema operacional, uma sub-rede adicionada ao ambiente ou um servidor da Web adicionado ao ambiente).		2				
11.3.3 As vulnerabilidades exploráveis encontradas durante o teste de penetração são corrigidas e o teste é repetido para verificar as correções.		2				
11.3.4 Se for utilizada a segmentação para isolar o CDE de outras redes, realize testes de penetração, ao menos uma vez por ano e após qualquer alteração nos métodos/controles de segmentação, para verificar se os métodos de segmentação são operacionais e eficientes, e se isolam todos os sistemas fora do escopo dos sistemas no CDE.		2				
11.3.4.1 Requisito adicional, somente para prestadores de serviços: Se a segmentação for utilizada, confirme o escopo do PCI DSS por meio do teste de penetração nos controles de segmentação, pelo menos, semestralmente e após quaisquer alterações aos controles/métodos de segmentação. *Observação: Este Requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se um Requisito.*		2				
11.4 Use técnicas de detecção de invasão e/ou prevenção contra invasões para detectar e/ou evitar invasões na rede. Monitore todo o tráfego no perímetro do ambiente de dados do titular do cartão, bem como nos pontos críticos do ambiente e alerte as equipes sobre comprometimentos suspeitos. Mantenha todos os mecanismos de detecção e prevenção contra invasões, diretrizes e assinaturas atualizados.		2				
11.5 Implemente um mecanismo de detecção de mudanças (por exemplo, ferramentas de monitoramento da integridade do arquivo) para alertar a equipe sobre modificações não autorizadas (inclusive alterações, acréscimos e exclusões) de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo; e configure o software para executar comparações de arquivos críticos, pelo menos, uma vez por semana. *Observação: Para fins de detecção de alterações, os arquivos críticos normalmente são aqueles que não são alterados com frequência, mas sua modificação poderia indicar um comprometimento do sistema ou um risco de comprometimento. Os mecanismos de detecção de alterações, como produtos de monitoramento da integridade dos arquivos, normalmente vêm pré-configurados com arquivos críticos para o sistema operacional relacionado. Outros arquivos críticos, como aqueles para os aplicativos personalizados, devem ser avaliados e definidos pela entidade (ou seja, o comerciante ou prestador de serviços).*				4		
11.5.1 Implemente um processo para responder a qualquer alerta gerado pela solução de detecção de alterações.				4		
11.6 Certifique-se de que as políticas de segurança e procedimentos operacionais para teste e monitoramento da segurança estejam documentados, em utilização, e sejam conhecidos por todas as partes afetadas.				4		
Requisito 12: Manter uma política que aborde a segurança das informações para todas as equipes						
12.1 Defina, publique, mantenha e dissemine uma política de segurança.						6
12.1.1 Revise a política de segurança ao menos uma vez por ano e atualize a política quando o ambiente for alterado.						6

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
12.2 Implemente um processo de avaliação de risco que: • Seja realizado ao menos uma vez por ano e quando houver modificações significativas no ambiente (por exemplo, aquisição, fusão, transferência, etc.), • Identifique os recursos, ameaças e vulnerabilidades críticos, e • Resulte em uma análise formal e documentada de risco. Os exemplos de metodologias de avaliação de risco incluem, entre outros, OCTAVE, ISO 27005 e NIST SP 800-30.	1					
12.3 Desenvolva o uso de políticas de tecnologias críticas e defina o uso apropriado destas tecnologias. *Observação: exemplos de tecnologias críticas incluem, entre outros, tecnologias de acesso remoto e sem fio, laptops, tablets, mídia eletrônica removível, uso de e-mails e da internet.* Garanta que essas políticas de utilização exijam o seguinte:						6
12.3.1 Aprovação explícita por partes autorizadas						6
12.3.2 Autenticação para o uso da tecnologia						6
12.3.3 Uma lista de todos esses dispositivos e equipes com acesso						6
12.3.4 Um método para determinar prontamente e precisamente o proprietário, informações de contato e propósito (por exemplo, etiqueta, codificação, e/ou inventário de dispositivos)						6
12.3.5 Usos aceitáveis da tecnologia						6
12.3.6 Locais de rede aceitáveis quanto às tecnologias						6
12.3.7 Lista dos produtos aprovados pela empresa						6
12.3.8 Desconexão automática das sessões para tecnologias de acesso remoto após um período específico de inatividade						6
12.3.9 Ativação de tecnologias de acesso remoto para fornecedores e parceiros de negócio somente quando lhes for necessário, com desativação imediata após o uso						6
12.3.10 Para funcionários que acessam os dados do titular do cartão por meio de tecnologias de acesso remoto, proíba a cópia, a transferência e o armazenamento dos dados do titular do cartão em discos rígidos locais e mídias eletrônicas removíveis, exceto se explicitamente autorizado para uma necessidade comercial definida. Onde houver uma necessidade comercial autorizada, as políticas de utilização devem exigir que os dados sejam protegidos de acordo com todos os Requisitos aplicáveis do PCI DSS.						6
12.4 Certifique-se de que a política e os procedimentos de segurança definem claramente as responsabilidades quanto à segurança da informação para todos os funcionários.						6
12.4.1 Requisito adicional, somente para prestadores de serviços: A gerência executiva deve estabelecer responsabilidades pela proteção dos dados de titulares do cartão e um programa de conformidade do PCI DSS, que contemple: • Responsabilidade geral pela manutenção da conformidade do PCI DSS • Definição de diretriz para o programa de conformidade com o PCI DSS e comunicação à gerência executiva *Observação: Este Requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se um Requisito.*						6

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
12.5 Atribua a um indivíduo ou a uma equipe as seguintes responsabilidades de gerenciamento da segurança da informação:						6
12.5.1 Defina, documente e distribua políticas e procedimentos de segurança.						6
12.5.2 Monitore e analise os alertas e as informações de segurança e distribua para as equipes apropriadas.						6
12.5.3 Defina, documente e distribua procedimentos de resposta e escalação de incidentes de segurança para assegurar que todas as situações sejam abordadas de modo oportuno e eficiente.		2				
12.5.4 Administre as contas dos usuários, incluindo adições, exclusões e modificações.						6
12.5.5 Monitore e controle todos os acessos aos dados.						6
12.6 Implemente um programa formal sobre conscientização de segurança para conscientizar todos os funcionários em relação à política e aos procedimentos de segurança dos dados do titular do cartão.						6
12.6.1 Instrua os funcionários quando da contratação e pelo menos uma vez por ano. Observação: Os métodos podem variar dependendo da função de cada funcionário e do nível de acesso aos dados do portador do cartão.						6
12.6.2 Solicite que os funcionários reconheçam, pelo menos uma vez ao ano, que leram e compreenderam a política e os procedimentos de segurança da empresa.						6
12.7 Analise bem os potenciais funcionários antes de contratar a fim de minimizar o risco de invasões a partir de fontes internas. (Exemplos de verificações da formação incluem o histórico do emprego anterior, ficha criminal, histórico de crédito e verificações das referências.) *Observação: Para os funcionários, como caixas de loja, que têm acesso somente a um número do cartão por vez ao viabilizar uma transação, esse Requisito é apenas uma recomendação.*						6
12.8 Mantenha e implemente políticas e procedimentos para controlar os prestadores de serviços com quem os dados do portador são compartilhados, ou que possam afetar a segurança dos dados, conforme segue:		2				
12.8.1 Mantenha uma lista dos prestadores de serviços, incluindo uma descrição dos serviços prestados.		2				
12.8.2 Mantenha um acordo por escrito que inclua um reconhecimento de que os prestadores de serviços são responsáveis pela segurança dos dados do titular do cartão que eles possuírem, ou que os armazenam, processam ou transmitem em nome do cliente, ou ao ponto de que eles possam impactar a segurança do ambiente dos dados do titular do cartão do cliente. *Observação: as informações exatas contidas no reconhecimento dependerão do acordo entre as duas partes, dos detalhes do serviço a ser prestado e das responsabilidades atribuídas a cada parte. O reconhecimento não precisa ser exatamente igual ao fornecido neste Requisito.*		2				
12.8.3 Certifique-se de que haja um processo definido para a contratação dos prestadores de serviços, incluindo uma diligência devida adequada antes da contratação.		2				
12.8.4 Mantenha um programa para monitorar anualmente o status de conformidade com o PCI DSS dos prestadores de serviços.		2				
12.8.5 Mantenha informações sobre quais Requisitos do PCI DSS são administrados por cada prestador de serviços e quais são administrados pela entidade.		2				

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
12.9 Requisito adicional, somente para prestadores de serviços: Os prestadores de serviços reconhecem por escrito aos clientes que eles são responsáveis pela segurança dos dados do titular do cartão que eles possuírem, ou que os armazenam, processam ou transmitem em nome do cliente, ou ao ponto de que eles possam impactar a segurança do ambiente dos dados do titular do cartão do cliente. *Observação: as informações exatas contidas no reconhecimento dependerão do acordo entre as duas partes, dos detalhes do serviço a ser prestado e das responsabilidades atribuídas a cada parte. O reconhecimento não precisa ser exatamente igual ao fornecido neste requisito.*		2				
12.10 Implemente um plano de resposta a incidentes. Prepare-se para reagir imediatamente a uma falha no sistema.						
12.10.1 Crie o plano de resposta a incidentes para ser implementado no caso de violações do sistema. Certifique-se de que o plano aborda o seguinte, pelo menos: • Funções, responsabilidades e estratégias de comunicação e contato no caso de uma violação, incluindo a notificação às bandeiras de pagamento, pelo menos • Procedimentos de resposta específicos a incidentes • Procedimentos de recuperação e continuidade dos negócios • Processos de backup dos dados • Análise dos Requisitos legais visando o relato das violações • Abrangência e resposta de todos os componentes críticos do sistema • Referência ou inclusão de procedimentos de resposta a incidentes por parte das bandeiras.		2				
12.10.2 Revise e teste o plano, inclusive todos os elementos previstos no Requisito 12.10.1, pelo menos, anualmente.		2				
12.10.3 Designe equipes específicas para estarem disponíveis em tempo integral para responder aos alertas.		2				
12.10.4 Forneça treinamento adequado à equipe que é responsável pela resposta às falhas do sistema.		2				
12.10.5 Inclua alertas a partir dos sistemas de monitoramento de segurança, incluindo, entre outros, detecção e prevenção contra invasões, firewalls e sistemas de monitoramento da integridade dos arquivos.		2				
12.10.6 Desenvolva um processo para modificar e aprimorar o plano de resposta a incidentes, de acordo com as lições aprendidas e para incorporar os desenvolvimentos do setor.		2				
12.11 Requisito adicional, somente para prestadores de serviços: Proceda à análise, pelo menos, trimestralmente para confirmar se os funcionários estão cumprindo as políticas de segurança e os procedimentos operacionais. As análises devem abranger os seguintes processos: • Revisão diária dos registros • Comentários de conjunto de regras de firewall • Aplicação de padrões de configuração em novos sistemas • Responder a alertas de segurança • Alterar processos de gestão *Observação: Este Requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se um Requisito.*						6

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.

Requisitos do PCI DSS v3.2	Etapa					
	1	2	3	4	5	6
12.11.1 Requisito adicional, somente para prestadores de serviços: Mantenha a documentação do processo de revisão trimestral e considere: • Documentar os resultados das revisões • Revisar e assinar os resultados por funcionários com atribuição da responsabilidade do programa de conformidade com o PCI DSS *Observação: Este Requisito é uma prática recomendada até 31 de janeiro de 2018, após esta data torna-se um Requisito.*						6
Apêndice A1: Requisitos Adicionais do PCI DSS para Provedores de Hospedagem Compartilhada						
A1 Proteger os dados e o ambiente hospedado de cada entidade (ou seja, do comerciante, prestador de serviços ou outra entidade), de acordo com os itens A1.1 a A1.4: O provedor de hospedagem deve cumprir esses Requisitos e todas as outras seções relevantes do PCI DSS. *Observação: Mesmo que o provedor de hospedagem cumpra esses Requisitos, a conformidade da entidade que usa o provedor de hospedagem não está assegurada. Cada entidade deve estar em conformidade com o PCI DSS e validar a conformidade, conforme aplicável.*			3			
A.1.1 Certifique-se de que cada entidade execute somente os processos com acesso ao ambiente de dados do titular do cartão daquela entidade.			3			
A.1.2 Restrinja o acesso e os privilégios de cada entidade somente ao próprio ambiente de dados do portador do cartão.			3			
A1.3 Certifique-se de que os registros e percursos de auditoria estão ativados e são exclusivos para o ambiente de dados do titular do cartão de cada entidade, além de estarem em conformidade com o Requisito 10 do PCI DSS.			3			
A1.4 Permita que os processos providenciem investigação forense oportuna em caso de comprometimento a qualquer comerciante ou prestador de serviços hospedado.			3			
Apêndice A2: Requisitos adicionais do PCI DSS para entidades usando SSL/antigo TLS *Observação: Este Apêndice aplica-se a entidades que usam SSL/antigo TLS como controle de segurança para proteger o CDE e/ou CHD*						
A2.1 Nos locais onde terminais POS POI (e pontos de terminação SSL/TLS aos quais se conectam) usam SSL e/ou antigo TLS, a entidade deve: • Confirmar se os dispositivos não estão suscetíveis a ataques conhecidos para os protocolos citados. Ou: • Implementar um plano de migração e mitigação de risco.		2				
A2.2 Entidades com implementações vigentes (outras que não conforme previstas na seção A2.1), que usam os protocolos SSL e/ou TLS antigo devem estabelecer um plano formal de migração e redução de riscos.		2				
A2.3 Requisito adicional, somente para prestadores de serviços: Até 30 de junho de 2016, todos os prestadores de serviço deverão oferecer serviço seguro. *Observação: Antes de 30 de junho de 2016, o prestador de serviços deve ter uma opção de protocolo seguro incluída na sua oferta de serviços, ou ter um Plano de Redução de Riscos e Migração documentado (conforme A2.2) que inclui uma data-alvo para fornecer uma opção de protocolo seguro até 30 de junho de 2016. Após esta data, todos os provedores de serviço devem oferecer uma opção de protocolo seguro para o seu serviço.*		2				

© 2016 PCI Security Standards Council LLC. A intenção deste documento é fornecer informações suplementares, que não substituem nem prevalecem sobre Padrões de Segurança SSC do PCI ou seus documentos de apoio.