Setor de cartões de pagamento (PCI)
Padrão de segurança de dados

Requisitos e procedimentos de avaliação da segurança

Versão 1.2

Outubro de 2008

Índice

Introdução e visão geral do padrão de segurança de dados do PCI

O Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI) foi desenvolvido para incentivar e aprimorar a segurança dos dados do portador do cartão e facilitar a ampla adoção de medidas de segurança de dados consistentes no mundo todo. Este documento, *Requisitos dos Padrões de Segurança de Dados do PCI e Procedimentos de Análise da Segurança,* usa como base os 12 requisitos do PCI DSS e combina-os com procedimentos de testes correspondentes em uma ferramenta de avaliação de segurança. Ele foi elaborado para ser utilizado pelos avaliadores que realizam análises in loco para comerciantes e prestadores de serviços que devem comprovar a conformidade com o PCI DSS. Abaixo, há uma visão geral de alto nível dos 12 requisitos do PCI DSS. As próximas páginas oferecem uma base a partir da qual uma avaliação de PCI DSS deve ser elaborada, realizada e registrada, enquanto os requisitos detalhados do PCI DSS começam na página 13.

Padrão de Segurança de Dados do PCI – Visão Geral Alto Nível

Construir e Manter uma Rede Segura	
Requisito 1:	Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão
Requisito 2:	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança
Proteger os Dados do Portador do Cartão	
Requisito 3:	Proteger os dados armazenados do portador do cartão
Requisito 4:	Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas
Manter um Programa de Gerenciamento de Vulnerabilidades	
Requisito 5:	Usar e atualizar regularmente o software antivírus
Requisito 6:	Desenvolver e manter sistemas e aplicativos seguros
Implementar Medidas de Controle de Acesso Rigorosas	
Requisito 7:	Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios
Requisito 8:	Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador
Requisito 9:	Restringir o acesso físico aos dados do portador do cartão
Monitorar e Testar as Redes Regularmente	
Requisito 10:	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão
Requisito 11:	Testar regularmente os sistemas e processos de segurança
Manter uma Política de Segurança de Informações	
Requisito 12:	Manter uma política que aborde a segurança das informações

Informações de aplicabilidade do PCI DSS

A tabela a seguir ilustra os elementos comumente usados do portador do cartão e dados de autenticação confidenciais; se o armazenamento de cada elemento de dados é permitido ou proibido; e se cada elemento de dados deve ser protegido. Essa tabela não é completa, mas é exibida para ilustrar os diferentes tipos de requisitos que se aplicam a cada elemento de dados.

	Elemento de dados	Armazenamento permitido	Proteção necessária	PCI DSS nec. 3.4
Dados do portador do cartão	O número da conta principal (PAN)	Sim	Sim	Sim
	O nome do portador do cartão [1]	Sim	Sim [1]	Não
	Código de serviço [1]	Sim	Sim [1]	Não
	Data de vencimento [1]	Sim	Sim [1]	Não
Dados de autenticação confidenciais [2]	Dados da tarja magnética completa [3]	Não	N/D	N/D
	CAV2/CVC2/CVV2/CID	Não	N/D	N/D
	PIN/Bloqueio de PIN	Não	N/D	N/D

[1] *Esses elementos de dados devem ser protegidos se forem armazenados em conjunto com o PAN. Essa proteção deve ser feita com base nos requisitos do PCI DSS para proteção geral do ambiente de dados do portador do cartão. Além disso, outras legislações (por exemplo, relacionadas à proteção de dados do consumidor, privacidade, roubo de identidade ou segurança de dados) podem exigir uma proteção específica desses dados ou a divulgação adequada das práticas de empresas se os dados pessoais do cliente estiverem sendo coletados durante o curso dos negócios. O PCI DSS, no entanto, não se aplica se o PAN não for armazenado, processado ou transmitido.*

[2] *Dados de autenticação confidenciais não devem ser armazenados após a autorização (mesmo se forem criptografados).*

[3] *Dados de acompanhamento completo da tarja magnética, imagem da tarja magnética no chip ou outro local.*

Escopo da avaliação quanto à conformidade com os requisitos do PCI DSS

Os requisitos de segurança do PCI DSS se aplicam a todos os componentes do sistema. Os "componentes do sistema" são definidos como qualquer componente de rede, servidor ou aplicativo que esteja incluído ou vinculado ao ambiente de dados do portador do cartão. O ambiente de dados do portador do cartão integra a rede que processa os dados do portador do cartão ou dados de autenticação sensíveis. Os componentes de rede incluem, mas não se limitam a, firewalls, chaves, roteadores, pontos de acesso sem fio, mecanismos de rede e outros mecanismos de segurança. Os tipos de servidor incluem, mas não se limitam a, o seguinte: Web, aplicativo, banco de dados, autenticação, e-mail, proxy, NTP (network time protocol) e DNS (domain name server). Os aplicativos incluem todos os aplicativos adquiridos e personalizados, incluindo os aplicativos internos e externos (Internet).

Segmentação da rede

A segmentação da rede ou o isolamento (separação) do ambiente de dados do portador do cartão do restante da rede corporativa não é um requisito do PCI DSS. Entretanto, ela é recomendada como um método que pode reduzir:

- O escopo da avaliação do PCI DSS
- O custo da avaliação do PCI DSS
- O custo e a dificuldade de implementar e manter controles do PCI DSS
- O risco de uma empresa (reduzido pela consolidação dos dados do portador do cartão em locais mais controlados e que totalizam um número menor)

Sem a segmentação adequada da rede (às vezes chamada de "rede plana"), toda a rede está no escopo da avaliação do PCI DSS. A segmentação da rede pode ser realizada por meio de firewalls internos da rede, roteadores com listas de controle de acesso rigorosas ou outras tecnologias que restringem o acesso a um determinado segmento de uma rede.

Um pré-requisito importante para reduzir o escopo do ambiente de dados do portador do cartão é uma compreensão clara das necessidades do negócio e dos processos relacionados ao armazenamento, processamento ou transmissão dos dados do portador do cartão. Restringir os dados do portador do cartão à menor quantidade de locais possível ao eliminar dados desnecessários e consolidar os dados necessários talvez exija a reformulação de práticas de negócios de longa data.

Documentar os fluxos dos dados do portador do cartão por meio de um diagrama de fluxo de dados ajuda a compreender totalmente todos os fluxos de dados do portador do cartão e assegura que qualquer segmentação de rede seja eficiente no isolamento do ambiente de dados do portador do cartão.

Se a segmentação da rede tiver sido implementada e será usada para reduzir o escopo da avaliação do PCI DSS, o avaliador deverá verificar se a segmentação é adequada para diminuir o escopo da avaliação. Em um nível elevado, a segmentação adequada da rede isola os sistemas que armazenam, processam ou transmitem dados do portador do cartão dos outros sistemas. Entretanto, a adequação de uma implementação específica da segmentação da rede varia muito e depende de aspectos como uma determina configuração de rede, das tecnologias implementadas e de outros controles que podem ser empregados.

Apêndice F: A seção Análises do PCI DSS – Abordando e Selecionando Exemplos fornece mais informações sobre a atuação do escopo durante uma avaliação do PCI DSS.

Sem fio

Se uma tecnologia sem fio for usada para armazenar, processar ou transmitir dados do portador do cartão (por exemplo, transações do ponto de venda, "quebra de linha") ou se uma LAN (local area network) sem fio estiver conectada ao ambiente de dados do portador do cartão ou a parte dele (por exemplo, não separado claramente por um firewall), os requisitos do PCI DSS e os procedimentos de teste para ambientes sem fio se aplicarão e também deverão ser realizados (por exemplo, Requisitos 1.2.3, 2.1.1 e 4.1.1). Antes da tecnologia sem fio ser implementada, uma empresa deve avaliar cuidadosamente a necessidade da tecnologia com relação ao risco. Considere a implementação da tecnologia sem fio somente para a transmissão de dados não confidenciais.

Terceiros/Terceirização

Para prestadores de serviços que devem realizar uma avaliação in loco anual, a validação da conformidade deve ser desempenhada em todos os componentes do sistema nos quais os dados do portador do cartão estão armazenados, processados ou transmitidos.

Um prestador de serviços ou comerciante pode usar um provedor terceirizado para armazenar, processar ou transmitir dados do portador do cartão em seu nome ou gerenciar componentes como roteadores, firewalls, bancos de dados, segurança física e/ou servidores. Se for o caso, talvez haja um impacto na segurança do ambiente de dados do portador do cartão.

Para aquelas entidades que terceirizam o armazenamento, o processamento ou a transmissão dos dados do portador do cartão para prestadores de serviços terceirizados, o Relatório sobre a conformidade (ROC) deve registrar a função de cada prestador de serviços, identificando claramente quais requisitos se aplicam à entidade analisada e quais se aplicam ao prestador de serviços. Há duas opções para que os prestadores de serviços terceirizados comprovem a conformidade: 1) Eles podem realizar uma avaliação do PCI DSS por conta própria e fornecer exemplos para seus clientes ára demonstrar sua conformidade ou 2) Se eles não fizerem sua própria avaliação do PCI DSS, seus serviços terão de ser analisados ao longo de cada uma das avaliações do PCI DSS de seus clientes. Para obter mais informações, consulte o indicador que começa com "Para análises do prestador de serviços gerenciado (MSP)" na Parte 3 na seção "Instruções e conteúdo para o relatório sobre conformidade" abaixo.

Além disso, os comerciantes e prestadores de serviços devem gerenciar e monitorar a conformidade do PCI DSS de todos os terceiros associados quanto ao acesso aos dados do portador do cartão. *Para obter detalhes, consulte o Requisito 12.8 nesse documento.*

Exemplos de áreas de negócios e componentes do sistema

O avaliador pode selecionar exemplos que representem áreas de negócios e componentes do sistema para avaliar os requisitos do PCI DSS. Esses exemplos devem incluir áreas de negócios e componentes do sistema, devem constituir uma seleção representativa de todos os tipos e locais das áreas de negócios, assim como os tipos dos componentes do sistema e devem ser grandes o suficiente para fornecer ao avaliador uma garantia de que os controles estão implementados conforme esperado.

Exemplos de áreas de negócios incluem escritórios corporativos, lojas, franquias e áreas de negócios em locais diferentes. Os exemplos devem incluir componentes de sistema para cada área de negócio. Por exemplo, para cada área de negócio, inclua uma série de sistemas operacionais, funções e aplicativos que são aplicáveis à área sob análise. Em cada área de negócios, o avaliador poderia selecionar servidores Sun executando Apache WWW, servidores Windows executando Oracle, sistemas do mainframe executando aplicativos de processamento de cartões legados, servidores de

transferência de dados executando HP-UX e servidores Linux executando MYSQL. Se todos os aplicativos forem executados a partir de um único SO (por exemplo, Windows ou Sun), então o exemplo também deverá incluir vários aplicativos (por exemplo, servidores do banco de dados, servidores da Web, servidores de transferência de dados). (*Consulte o Apêndice F: Análises do PCI DSS – Abordando e Selecionando.*)

Ao selecionar exemplos de áreas de negócios e componentes de sistema, os avaliadores devem considerar o seguinte:

- Se houver processos implementados de PCI DSS padrão exigidos que cada área deve seguir, o exemplo pode ser menor do que o necessário caso não haja processos padrão para fornecer uma garantia razoável de que cada área esteja configurada de acordo com o processo padrão.
- Se houver mais de um tipo de processos padrão implementados (por exemplo, para diferentes tipos de componentes de sistema ou áreas), então o exemplo deve ser grande o suficiente para incluir componentes de sistema ou áreas protegidas com cada tipo de processo.
- Se não houver processos de PCI DSS padrão implementados e cada área for responsável pelos seus próprios processos, então o tamanho dos exemplos deverá ser maior para assegurar que cada área compreenda e implemente os requisitos de PCI DSS adequadamente.

Consulte também o Apêndice F: Análises do PCI DSS – Abordando e Selecionando Exemplos.

Controles de compensação

Anualmente, quaisquer controles de compensação devem ser registrados, analisados e validados pelo avaliador e incluídos no envio do Relatório sobre conformidade, de acordo com o *Apêndice B: Controles de compensação* e *Apêndice C: Planilha dos controles de compensação.*

Para cada um dos controles de compensação, a Planilha dos controles de compensação (Apêndice C) **deve** ser preenchida. Além disso, os resultados dos controles de compensação devem ser registrados no ROC na seção de requisitos do PCI DSS correspondente.

Para obter mais detalhes sobre "controles de compensação", consulte os Apêndices B e C mencionados acima.

Instruções e conteúdo para o relatório sobre conformidade

Este documento deve ser usado como o modelo para a criação do *Relatório sobre conformidade*. A entidade avaliada deve seguir os requisitos de informe respectivos de cada bandeira de pagamento para assegurar que cada bandeira de pagamento reconheca o status de conformidade da entidade. Entre em contato com cada bandeira de pagamento para definir os requisitos e instruções de informe.

Conteúdo e formato do relatório

Siga estas instruções referentes ao conteúdo e ao formato do relatório ao preencher um Relatório sobre conformidade:

1. Resumo Executivo

Inclui o seguinte:

- Descreve o ramo do cartão de pagamento da entidade, incluindo:
  - Sua função comercial nos cartões de pagamento, que é como e por que eles armazenam, processam e/ou transmitem dados do portador do cartão

    Observação: Esse documento não visa ser uma cópia do site da entidade, mas deve ser uma descrição personalizada que demonstra que o avaliador compreende o pagamento e a função da entidade.
  - Como eles processam o pagamento (diretamente, indiretamente, etc.)
  - A quais tipos de canais de pagamento eles atendem, como cartão não presente, (por exemplo, pedido por e-mail-pedido por telefone (MOTO), e-commerce) ou cartão presente
  - Quaisquer entidades às quais eles estajm vinculados para a transmissão ou o processamento do pagamento, incluindo relacionamentos com o responsável pelo processamento
- Um diagrama de rede de alto nível (obtido junto à entidade ou criado pelo avaliador) da topografia da rede da entidade que inclui:
  - Conexões dentro e fora da rede
  - Componentes críticos no ambiente de dados do portador do cartão, incluindo dispositivos POS, sistemas, bancos de dados e servidores da Web, conforme aplicável.
  - Outros componentes de pagamento necessários, conforme aplicável.

2. Descrição do escopo de trabalho e abordagem adotada

Descreva o escopo, de acordo com a seção Escopo da avaliação desse documento, incluindo o seguinte:

- Ambiente no qual a avaliação se concentrou (por exemplo, pontos de acesso de Internet do cliente, rede corporativa interna, conexões de processamento)
- Se a segmentação da rede estiver implementada e tiver sido usada para reduzir o escopo da análise do PCI DSS, explique resumidamente essa segmentação e como o avaliador validou a eficiência da segmentação
- Registre e justifique os exemplos usados para ambas as entidades (lojas, áreas, etc.) e os componentes de sistema selecionados, incluindo:
  - Total da população
  - Número exemplificado
  - Argumento para o exemplo selecionado
  - Por que o tamanho do exemplo é suficiente para permitir que o avaliador apresente um argumento confiável de que os controles avaliados representam os controles que estão implementados em toda a entidade
  - Descreva quaisquer locais ou ambientes que armazenam, processam ou transmitem dados do portador do cartão que foram EXCLUÍDOS do escopo da análise e por que esses locais/ambientes foram excluídos
- Relacione quaisquer entidades de propriedade integral que exijam a conformidade com o PCI DSS e se elas foram analisadas separadamente ou como parte dessa avaliação
- Relacione quaisquer entidades internacionais que exijam a conformidade com o PCI DSS e se elas foram analisadas separadamente ou como parte dessa avaliação
- Relacione quaisquer LANs sem fio e/ou aplicativos de pagamento sem fio (por exemplo, terminais POS) que estejam vinculados ou que poderiam causar um impacto na segurança do ambiente de dados do portador do cartão e descreva a segurança implementada nesses ambientes sem fio
- A versão do documento Requisitos do PCI DSS e procedimentos da avaliação de segurança usada para realizar a avaliação
- Período da avaliação

3. Detalhes sobre o Ambiente Analisado

Inclua os detalhes a seguir nesta seção:

- Um diagrama de cada link de comunicação, incluindo LAN, WAN ou Internet
- A descrição do ambiente de dados do portador do cartão, por exemplo:
  - A transmissão e o processamento do documento dos dados do portador do cartão, incluindo autorização, captura, pagamento, cobrança retroativa e outros fluxos, conforme aplicável

  - A lista dos arquivos e tabelas que armazenam os dados do portador do cartão, compatível com um inventário criado (ou obtido junto ao cliente) e mantido pelo avaliador no documento. Esse inventário deve incluir, para cada armazenamento de dados do portador do cartão (arquivo, tabela, etc.):
    - A lista de todos os elementos dos dados de portador do cartão armazenados
    - Como o armazenamento de dados é protegido
    - Como o acesso aos armazenamentos de dados é registrado
- A lista de hardwares e softwares críticos utilizados no ambiente de dados do portador do cartão, junto com a descrição da função/uso de cada um deles
- A lista dos prestadores de serviços e outras entidades com as quais a empresa compartilha os dados do portador do cartão (Observação: essas entidades estão sujeitas ao Requisito 12.8 do PCI DSS)
- A lista dos produtos dos aplicativos de pagamento de terceiros e números das versões utilizadas, incluindo se cada aplicativo de pagamento foi validado de acordo com PA-DSS. Mesmo se um aplicativo de pagamento tiver sido validado por PA-DSS, o avaliador precisará verificar se o aplicativo foi implementado em conformidade com o PCI DSS e no ambiente respectivo, e de acordo com o *Guia de implementação de PA-DSS do fornecedor do aplicativo de pagamento. Observação: A utilização de aplicativos validados por PA-DSS não é um requisito do PCI DSS. Consulte cada bandeira de pagamento individualmente para compreender seus requisitos de conformidade com PA-DSS.*
- A lista das pessoas entrevistadas e seus cargos
- A lista da documentação revisada.
- Para análises do prestador de serviços gerenciado (MSP), o avaliador deve identificar com clareza quais requisitos nesse documento se aplicam ao MSP (e estão incluídos na análise) e quais não estão incluídos na análise e cuja inclusão em suas análises é de responsabilidade dos clientes do MSP. Inclua informações sobre quais endereços IP do MSP são digitalizados como parte integrante das digitalizações de vulnerabilidades trimestrais do MSP e quais endereços IP são de responsabilidade dos clientes do MSP incluir em suas próprias digitalizações trimestrais.

4. Informações de contato e data do relatório

Inclui:

- As informações de contato do comerciante ou prestador de serviços e avaliador
- A data do relatório

5. Resultados das digitalizações trimestrais

- Resuma os resultados das quatro digitalizações trimestrais mais recentes no Resumo executivo, assim como nos comentários no Requisito 11.2

  Observação: Não será necessário que quatro varreduras trimestrais aprovadas sejam concluídas quanto à conformidade inicial do PCI DSS se o avaliador verificar que 1) o resultado da varredura mais recente foi uma varredura aprovada, 2) a entidade contar com políticas e procedimentos documentados que requerem a seqüência de varreduras trimestrais e 3) quaisquer vulnerabilidades observadas na varredura inicial tenham sido corrigidas conforme mostrado em uma nova varredura. Nos anos seguintes após a análise inicial do PCI DSS, quatro digitalizações trimestrais aprovadas devem ter ocorrido.

- A varredura deve abranger todos os endereços IP (na Internet) acessíveis externamente existentes na entidade, de acordo com os *Procedimentos de varredura de segurança do PCI DSS*

6. Descobertas e observações

- No Resumo executivo, sintetize quaisquer descobertas que talvez não se encaixem no formato do modelo do Relatório sobre conformidade padrão.
- Todos os avaliadores *devem* usar o modelo Requisitos detalhados do PCI DSS e procedimentos de avaliação de segurança para fornecer descrições e descobertas detalhadas no relatório sobre cada requisito, principal e secundário.
- O avaliador *deve* analisar e registrar quaisquer controles de compensação considerados para concluir que um controle esteja implementado.

  Para obter mais detalhes sobre "controles de compensação", consulte a seção Controles de compensação acima e os Apêndices B e C.

Revalidação dos itens em aberto

Um relatório sobre “controles implementados” é exigido para verificar a conformidade. O relatório será considerado como não conforme se contiver "itens em aberto" ou itens que serão concluídos em uma data futura. O comerciante/prestador de serviços deve atentar para esses itens antes de concluir a validação. Depois que esses itens receberem atenção do comerciante/prestador de serviços, o avaliador fará uma reavaliação para validar se a solução foi providenciada e todos os requisitos foram atendidos. Após a revalidação, o avaliador emitirá um novo Relatório sobre conformidade, atestando que o ambiente de dados do portador do cartão está em total conformidade e irá enviá-lo de forma consistente de acordo com as instruções (veja abaixo).

Conformidade do PCI DSS – Etapas de conclusão

1. Conclua o Relatório de conformidade (ROC) de acordo com a seção acima entitulada "Instruções e conteúdo para o Relatório sobre conformidade".
2. Certifique-se de que a(s) varredura(s) de vulnerabilidades aprovada(s) tenha(m) sido concluída(s) por um Fornecedor de varredura aprovado (ASV) do PCI SSC e obtenha uma comprovação da(s) varredura(s) aprovada(s) junto ao ASV.
3. Preencha por completo o Atestado de conformidade referente aos Prestadores de serviços ou Comerciantes, conforme aplicável. Consulte os Apêndices D e E sobre os Atestados de conformidade.
4. Envie o ROC, a comprovação de uma varredura aprovada e o Atestado de conformidade, junto com qualquer outra documentação solicitada, ao adquirente (para comerciantes) ou à bandeira de pagamento ou outro solicitante (para prestadores de serviços).

Requisitos detalhados do PCI DSS e procedimentos da avaliação de segurança

Para saber mais sobre os *Requisitos do PCI DSS e procedimentos da avaliação de segurança,* as informações a seguir definem os cabeçalhos das colunas da tabela:

- **Requisitos do PCI DSS** – Esta coluna define o Padrão de Segurança dos Dados e lista os requisitos para atingir a conformidade do PCI DSS; a conformidade será validada de acordo com esses requisitos.
- **Procedimentos de teste** – Esta coluna exibe os processos a serem seguidos pelo avaliador para validar se os requisitos do PCI DSS estão "em vigor"
- **Implementado** – Esta coluna deve ser usada pelo avaliador para fornecer uma descrição resumida dos controles que estão implementados, incluindo aqueles controles implementados como resultado dos controles de compensação. (Observação: esta coluna *não* deve ser usada para itens que ainda não estejam implementados ou para itens em aberto a serem concluídos em uma data futura.)
- **Não implementado** – Esta coluna deve ser usada pelo avaliador para fornecer uma descrição resumida dos controles que não estão implementados. Um relatório de não conformidade não deve ser enviado a uma bandeira de pagamento ou adquirente a menos que seja solicitado de forma específica. Consulte o Apêndice D e o Apêndice E: Atestados de conformidade para obter mais instruções sobre os relatórios de não conformidade.
- **Data prevista/Comentários** – Para os controles "Não implementados", o avaliador pode incluir uma data prevista na qual o comerciante ou o prestador de serviços espera que os controles estejam "Implementados". Quaisquer observações ou comentários adicionais também podem ser incluídos aqui.

Construa e mantenha uma rede segura

Requisito 1: Instalar e manter um configuração de firewall para proteger os dados do portador do cartão

Firewalls são dispositivos do computador que controlam o tráfego do computador permitido entre a rede de uma empresa (interna) e redes não confiáveis (externa), assim como o tráfego dentro e fora de muitas áreas confidenciais na rede confiável interna de uma empresa. O ambiente de dados do portador do cartão é um exemplo de uma área mais sensível dentro da rede confiável de uma empresa.

Um firewall examina todo o tráfego da rede e bloqueia aquelas transmissões que não atendem aos critérios de segurança específicos.

Todos os sistemas devem ser protegidos do acesso não autorizado de redes não confiáveis, seja acessando o sistema por meio da Internet como e-commerce, acesso à Internet através dos navegadores na área de trabalho por parte dos funcionários, acesso via e-mail dos funcionários, conexão dedicada como conexões entre negócios, por meio de redes sem fio ou de outras fontes. Com freqüência, trajetos aparentemente insignificantes que direcionam ou partem de redes não confiáveis podem fornecer caminhos não protegidos aos sistemas principais. Os firewalls são um mecanismo de proteção essencial para qualquer rede de computador.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
1.1 Definir os padrões de configuração do firewall e do roteador que incluam o seguinte:	**1.1** Obtenha e inspecione os padrões de configuração do firewall e do roteador, além de outras documentações especificadas abaixo para verificar se os padrões estão concluídos. Conclua 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	**1.1.1** Verifique se há um processo formal para testar e aprovar todas as conexões de rede e as alterações às configurações do firewall e do roteador.			
1.1.2 Diagrama da rede atual com todas as conexões com relação aos dados do portador do cartão, incluindo quaisquer redes sem fio	**1.1.2.a** Verifique há um diagrama da rede atual (por exemplo, um que mostre os fluxos de dados do portador do cartão na rede) e se ele registra todas as conexões com relação aos dados do portador do cartão, incluindo quaisquer redes sem fio.			
	1.1.2.b Verifique se o diagrama é mantido atualizado.			
1.1.3 Requisitos para um firewall em cada conexão da Internet e entre qualquer zona desmilitarizada (DMZ) e a zona da rede interna	**1.1.3** Verifique se os padrões de configuração do firewall incluem requisitos para um firewall em cada conexão da Internet entre qualquer DMZ e a zona da rede interna. Verifique se o diagrama da rede atual está de acordo com os padrões de configuração do firewall.			
1.1.4 Descrição de grupos, funções e responsabilidades quanto ao gerenciamento lógico dos componentes da rede	**1.1.4** Verifique se os padrões de configuração do firewall e do roteador incluem uma descrição dos grupos, funções e responsabilidades quanto ao gerenciamento lógico dos componentes da rede.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
1.1.5 Documentação e justificativa comercial para o uso de todos os serviços, protocolos e portas permitidas, incluindo a documentação dos recursos de segurança implementados para os protocolos considerados inseguros	**1.1.5.a** Verifique se os padrões de configuração do firewall e do roteador incluem uma lista documentada dos serviços, protocolos e portas necessárias para os negócios - por exemplo, protocolos HTTP (hypertext transfer protocol) e SSL (Secure Sockets Layer), SSH (Secure Shell) e VPN (Virtual Private Network).			
	1.1.5.b Identifique serviços, protocolos e portas permitidas inseguras; e comprove se são necessários e se os recursos de segurança estão documentados e implementados examinando os padrões de configuração do firewall e do roteador, além das configurações para cada serviço. Um exemplo de um serviço, protocolo ou porta insegura é o FTP, que transmite as credenciais do usuário em texto simples.			
1.1.6 Requisito para analisar os conjuntos de regras do firewall e do roteador pelo menos a cada seis meses	**1.1.6.a** Verifique se os padrões de configuração do firewall e do roteador exigem a análise dos conjuntos de regras pelo menos a cada seis meses.			
	1.1.6.b Obtenha e examine a documentação para verificar se os conjuntos de regras são analisados pelo menos a cada seis meses.			
1.2 Elaborar uma configuração do firewall que restrinja as conexões entre redes não confiáveis e quaisquer componentes do sistema no ambiente de dados do portador do cartão.	**1.2** Examine as configurações do firewall e do roteador para verificar se as conexões estão restritas entre as redes não confiáveis e os componentes de sistema no ambiente de dados do portador do cartão, conforme se segue:			
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 Restringir o tráfego de entrada e saída para aquele que é necessário para o ambiente de dados do portador do cartão.	**1.2.1.a** Verifique se o tráfego de entrada e saída está limitado para aquele que é necessário para o ambiente de dados do portador do cartão e se as restrições estão documentadas.			
	1.2.1.b Verifique se todos os outros tráfegos de entrada e saída são recusados de forma específica, por exemplo ao usar a opção explícita "recusar todos" ou uma recusa implícita após a declaração de permissão.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
1.2.2 Proteger e sincronizar os arquivos de configuração do roteador.	**1.2.2** Verifique se os arquivos de configuração do roteador estão protegidos e sincronizados—por exemplo, arquivos de configuração de execução (usados para a execução normal dos roteadores) e arquivos de configuração de inicialização (usados quando as máquinas são reiniciadas), e se têm as mesmas configurações seguras.			
1.2.3 Instalar firewalls de perímetro entre quaisquer redes sem fio e o ambiente de dados do portador do cartão, e configurar esses firewalls para recusar ou controlar (se esse tráfego for necessário para fins comerciais) qualquer tráfego a partir do ambiente sem fio no ambiente de dados do portador do cartão.	**1.2.3** Verifique se há firewalls de perímetro instalados entre quaisquer redes sem fio e sistemas que armazenam dados do portador do cartão e se esses firewalls recusam ou controlam (se esse tráfego for necessário para fins comerciais) qualquer tráfego a partir do ambiente sem fio no ambiente de dados do portador do cartão.			
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** Examine as configurações do firewall e do roteador, conforme detalhado abaixo, para determinar se não há acesso direto entre a Internet e os componentes do sistema, incluindo o roteador de suspensão na Internet, o roteador e firewall de DMZ, o segmento do portador do cartão de DMZ, o roteador do perímetro e o segmento interno da rede do portador do cartão.			
1.3.1 Implementar uma DMZ para limitar o tráfego de entrada e saída somente aos protocolos que são necessários para o ambiente de dados do portador do cartão.	**1.3.1** Verifique se a DMZ está implementada para limitar o tráfego de entrada e saída somente aos protocolos que são necessários para o ambiente de dados do portador do cartão.			
1.3.2 Limitar o tráfego de entrada da Internet a endereços IP na DMZ.	**1.3.2** Verifique se o tráfego de entrada da Internet está limitado a endereços IP na DMZ.			
1.3.3 Não permitir a entrada ou saída de nenhum trajeto direto com relação ao tráfego entre a Internet e o ambiente de dados do portador do cartão.	**1.3.3** Verifique se não há entradas ou saídas de trajetos diretos com relação ao tráfego entre a Internet e o ambiente de dados do portador do cartão.			
1.3.4 Não permitir que endereços internos sejam transmitidos via Internet na DMZ.	**1.3.4** Verifique que os endereços internos não podem ser transmitidos via Internet na DMZ**.**			
1.3.5 Restringir o tráfego de saída do ambiente de dados do portador do cartão à Internet de uma forma que o tráfego de saída possa acessar somente endereços IP na DMZ.	**1.3.5** Verificar que o tráfego de saída do ambiente de dados do portador do cartão à Internet pode acessar somente endereços IP na DMZ.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
1.3.6 Implementar inspeção com status, também conhecida como filtragem de pacote dinâmico. (Ou seja, somente conexões "estabelecidas" são permitidas na rede.)	**1.3.6** Verifique que o firewall desempenha a inspeção com status (filtragem de pacote dinâmico). [Somente as conexões estabelecidas devem ser permitidas e apenas se estiverem associadas a uma sessão estabelecida anteriormente (realize uma varredura da porta em todas as portas TCP com conjunto de bits "sync reset" ou syn ack"—uma resposta significa que os pacotes são permitidos mesmo se não fizerem parte de uma sessão estabelecida anteriormente).]			
1.3.7 Posicionar o banco de dados em uma zona da rede interna, separada ada DMZ.	**1.3.7** Verifique se o banco de dados está em uma zona da rede interna, separada da DMZ.			
1.3.8 Implementar o mascaramento de IP para impedir que endereços internos sejam traduzidos e revelados na Internet, usando o espaço de endereço RFC 1918. Usar as tecnologias NAT (network address translation)—por exemplo, PAT (port address translation).	**1.3.8** Para o exemplo dos componentes do firewall e do roteador, verifique se NAT ou outra tecnologia que utiliza o espaço de endereço RFC 1918 é usada para restringir a transmissão de endereços IP da rede interna para a Internet (mascaramento de IP).			
1.4 Instalar o software de firewall pessoal em quaisquer computadores móveis e/ou de propriedade do funcionário com conectividade direta à Internet (por exemplo, laptops usados pelos funcionários), que são usados para acessar a rede da empresa.	**1.4.a** Verifique se os computadores móveis e/ou de propriedade do funcionário com conectividade direta à Internet (por exemplo, laptops usados pelos funcionários), e que são usados para acessar a rede da empresa têm um software de firewall pessoal instalado e em funcionamento.			
	1.4.b Verifique se o software do firewall pessoal foi configurado pela empresa de acordo com padrões específicos e não pode ser alterado pelos usuários de computadores móveis.			

Requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança

Indivíduos mal-intencionados (dentro e fora de uma empresa) com freqüência usam senhas padrão do fornecedor e outras configurações padrão do fornecedor para comprometer os sistemas. Essas senhas e configurações são bastante conhecidas pelas comunidades de hackers e facilmente determinadas por meio de informações públicas.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
2.1 Sempre alterar os padrões disponibilizados pelo fornecedor **antes** de instalar um sistema na rede—por exemplo, incluir senhas, strings de comunidade de SNMP (simple network management protocol) e a eliminação de contas desnecessárias.	**2.1** Selecione um exemplo de componentes do sistema, servidores críticos e pontos de acesso sem fio, e tente efetuar login (com ajuda do administrador do sistema) nos dispositivos que usam contas e senhas padrão disponibilizadas pelo fornecedor para verificar se essas contas e senhas padrão foram alteradas. (Use os manuais do fornecedor e as fontes na Internet para localizar as contas/senhas disponibilizadas pelo fornecedor.)			
2.1.1 Em ambientes sem fio conectados ao ambiente de dados do portador do cartão ou que transmitam dados do portador do cartão, alterar os padrões do fornecedor sem fio, incluindo, mas não se limitando a, chaves de criptografia sem fio padrão, senhas e strings de comunidades de SNMP. Certificar-se de que as configurações de segurança do dispositivo sem fio estejam ativadas com relação a uma tecnologia de criptografia robusta para a autenticação e a transmissão.	**2.1.1** Verifique as informações a seguir referentes às configurações padrão do fornecedor para ambientes sem fio e certifique-se de que todas as redes sem fio implementam mecanismos de criptografia robustos (por exemplo, AES): ▪ As chaves de criptografia foram alteradas do padrão na instalação e são modificadas a qualquer momento que um funcionário que conheça as chaves sai da empresa ou troca de cargo ▪ As strings de comunidades de SNMP padrão nos dispositivos sem fio foram alteradas ▪ As senhas/passphrases padrão nos pontos de acesso foram alteradas ▪ O firmware nos dispositivos sem fio foi atualizado para ser compatível com a criptografia robusta para a autenticação e a transmissão em redes sem fio (por exemplo, WPA/WPA2) Outros padrões do fornecedor sem fio relacionados à segurança, se aplicável			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
2.2 Desenvolver padrões de configuração para todos os componentes do sistema. Certificar-se de que esses padrões abrangem todas as vulnerabilidades de segurança conhecidas e estão em conformidade com os padrões de endurecimento do sistema aceitos pelo setor.	**2.2.a** Analise os padrões de configuração do sistema da empresa quanto a todos os tipos de componentes do sistema e verifique se os padrões de configuração do sistema estão em conformidade com os padrões de endurecimento aceitos pelo setor—por exemplo, SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST) e Center for Internet Security (CIS).			
	2.2.b Verifique se os padrões de configuração do sistema incluem cada um dos itens abaixo (2.2.1 a 2.2.4).			
	2.2.c Verifique se os padrões de configuração do sistema serão aplicados quando novos sistemas forem configurados.			
2.2.1 Implementar somente uma função principal por servidor.	**2.2.1** Para obter um exemplo dos componentes do sistema, verifique se somente uma função principal é implementada por servidor. Por exemplo, servidores da Web, servidores do banco de dados e DNS devem ser implementados em servidores separados.			
2.2.2 Desativar todos os serviços e protocolos desnecessários e inseguros (os serviços e protocolos que não precisam desempenhar diretamente a função especificada do dispositivo).	**2.2.2** Para obter um exemplo dos componentes do sistema, inspecione os serviços do sistema ativado, daemons e protocolos. Verifique se os serviços ou protocolos desnecessários ou inseguros não estão ativados ou estão justificados e registrados quanto ao uso adequado do serviço. Por exemplo, o FTP não é usado ou é criptografado por meio de SSH ou de outra tecnologia.			
2.2.3 Configurar os parâmetros de segurança do sistema para impedir o uso incorreto.	**2.2.3.a** Entreviste os administradores do sistema e/ou os gerentes de segurança para verificar se eles conhecem as configurações comuns dos parâmetros de seguança referentes aos componentes do sistema.			
	2.2.3.b Verifique se as configurações comuns dos parâmetros de segurança estão incluídas nos padrões de configuração do sistema.			
	2.2.3.c Para obter um exemplo dos componentes do sistema, verifique se os parâmetros comuns de segurança estão definidos de forma adequada.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
2.2.4 Remover todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores da Web desnecessários.	**2.2.4** Para obter um exemplo dos componentes do sistema, verifique se todas as funcionalidades desnecessárias (por exemplo, scripts, drivers, recursos, subsistemas, sistemas de arquivo, etc.) foram removidas. Verifique se as funções ativadas estão documentadas e suporte a configuração segura, e se apenas a funcionalidade documentada está presente nas máquinas usadas como exemplo.			
2.3 Criptografar todos os acessos administrativos não-console. Usar tecnologias como SSH, VPN ou SSL/TLS para o gerenciamento baseado na Web e outros acessos administrativos não-console.	**2.3** Para obter um exemplo dos componentes do sistema, verifique se o acesso administrativo não-console é criptografado ao: ▪ Observar um administrador efetuar login em cada sistema para verificar se o método de criptografia robusto é chamado antes da senha do administrador ser solicitada; ▪ Analisar os serviços e os arquivos de parâmetro nos sistemas para determinar se o Telnet e outros comandos de login remoto não estão disponíveis para uso interno; e ▪ Verificar se o acesso do administrador às interfaces de gerenciamento baseadas na Web é criptografado com uma criptografia robusta.			
2.4 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 A: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada*.	**2.4** Realize os procedimentos de teste de **A.1.1** a **A.1.4** detalhados no *Apêndice A: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada* para avaliações do PCI DSS dos provedores de hospedagem compartilhada para verificar se os provedores de hospedagem compartilhada protegem o ambiente hospedado e os dados das suas entidades (comerciantes e prestadores de serviços).			

Proteger os dados do portador do cartão

Requisito 3: Proteger os dados armazenados do portador do cartão

Métodos de proteção como criptografia, truncamento, mascaramento e referenciamento são componentes essenciais da proteção de dados do portador do cartão. Se um invasor burlar outros controles de segurança da rede e obtiver acesso aos dados criptografados, sem as chaves criptográficas adequadas, os dados estarão ilegíveis e inutilizáveis para aquele indivíduo. Outros métodos eficientes de proteção dos dados armazenados devem ser considerados como oportunidades potenciais de minimização dos riscos. Por exemplo, os métodos para minimizar os riscos incluem não armazenar os dados do portador do cartão a menos que seja absolutamente necessário, truncar os dados do portador do cartão se um PAN completo não for necessário e não enviar o PAN em e-mails não criptografados.

Consulte a seção *Glossário de termos, abreviações e acrônimos do PCI DSS* para obter definições de "criptografia robusta" e outros termos do PCI DSS.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
3.1 Manter o mínimo de armazenamento de dados do portador do cartão. Desenvolver uma política de retenção e descarte de dados. Limitar a quantidade de armazenamento e o período de retenção para o que é exigido para fins comerciais, legais e/ou regulatórios, conforme documentado na política de retenção de dados.	**3.1** Obtenha e analise as políticas e procedimentos da empresa quanto à retenção e ao descarte dos dados, e desempenhe o seguinte ▪ Verifique se as políticas e os procedimentos incluem requisitos legais, regulatórios e comerciais referentes à retenção de dados, incluindo requisitos específicos quanto à retenção de dados do portador do cartão (por exemplo, os dados do portador do cartão precisam ser retidos por um período X por razões comerciais Y) ▪ Verifique se as políticas e os procedimentos incluem itens referentes ao descarte dos dados quando não forem mais necessários por razões legais, regulatórias ou comerciais, incluindo o descarte dos dados do portador do cartão ▪ Verifique se as políticas e os procedimentos incluem a abrangência de todo o armazenamento dos dados do portador do cartão ▪ Verifique se as políticas e os procedimentos incluem um processo programático (automático) para remover, pelo menos trimestralmente, os dados do portador do cartão armazenados que excedam os requisitos de retenção comercial ou, também, os requisitos quanto a uma análise, realizada pelo menos trimestralmente, para verificar se os dados do portador do cartão não excedem os requisitos de retenção comerciais			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
3.2 Não armazenar dados de autenticação confidenciais após a autorização (mesmo se estiverem criptografados). Os dados de autenticação confidenciais incluem os dados conforme mencionados nos seguintes Requisitos 3.2.1 até 3.2.3:	**3.2** Se dados de autenticação confidenciais forem recebidos e excluídos, obtenha e analise os processos de exclusão dos dados para verificar se os dados não podem ser recuperados. Para cada item dos dados de autenticação confidenciais abaixo, desempenhe as seguintes etapas:			
3.2.1 Não armazene o conteúdo completo de qualquer rastro da tarja magnética (localizada na parte posterior do cartão, em um chio ou outro local). Esses dados também são denominados como rastro completo, rastro, rastro 1, rastro 2 e dados da tarja magnética. *Observação: No curso normal dos negócios, os seguintes elementos de dados da fita magnética talvez precisem ser retidos:* ▪ *O nome do portador do cartão,* ▪ *O número da conta principal (PAN),* ▪ *A data de vencimento e* ▪ *O código de serviço* *Para minimizar o risco, armazene somente os elementos de dados conforme necessário para os negócios.* *Observação: Para obter mais informações, consulte a seção* Glossário de termos, abreviações e acrônimos do PCI DSS.	**3.2.1** Para obter um exemplo dos componentes do sistema, analise as informações a seguir e verifique se o conteúdo completo de qualquer rastro da tarja magnética na parte posterior do cartão não é armazenado em nenhuma circunstância: ▪ Dados de transação de entrada ▪ Todos os registros (por exemplo, transação, histórico, depuração, erro) ▪ Arquivos do histórico ▪ Arquivos de rastros ▪ Vários esquemas do banco de dados ▪ Conteúdo do bancos de dados			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
3.2.2 Não armazenar o código ou valor de verificação do cartão (o número de três ou quatro dígitos impresso na frente ou atrás do cartão de pagamento) usado para verificar as transações com cartão não presente. *Observação: Para obter mais informações, consulte a seção* Glossário de termos, abreviações e acrônimos do PCI DSS.	**3.2.2** Para obter um exemplo dos componentes do sistema, verifique se o código ou o valor de verificação do cartão de três ou quatro dígitos impresso na frente do cartão ou no painel de assinatura (dados CVV2, CVC2, CID, CAV2) não é armazenado sob nenhuma circunstância: ▪ Dados de transação de entrada ▪ Todos os registros (por exemplo, transação, histórico, depuração, erro) ▪ Arquivos do histórico ▪ Arquivos de rastros ▪ Vários esquemas do banco de dados ▪ Conteúdo do bancos de dados			
3.2.3 Não armazenar o PIN (personal identification number) ou o bloco de PIN criptografado.	**3.2.3** Para obter um exemplo dos componentes do sistema, analise as informações a seguir e verifique se os PINs e blocos de PIN criptografados não são armazenados sob nenhuma circunstância: ▪ Dados de transação de entrada ▪ Todos os registros (por exemplo, transação, histórico, depuração, erro) ▪ Arquivos do histórico ▪ Arquivos de rastros ▪ Vários esquemas do banco de dados ▪ Conteúdo do bancos de dados			
3.3 Mascarar o PAN quando for exibido (os seis primeiros e os quatro últimos dígitos são o número máximo de dígitos a ser exibido). *Observações:* ▪ *Esse requisito não se aplica aos funcionários e outras partes interessadas em um negócio legítimo que precisam visualizar o PAN completo.* ▪ *Esse requisito não substitui os requisitos mais rigorosos em vigor quanto às exibições dos dados do portador do cartão—por exemplo, para recebimentos do ponto de venda.*	**3.3** Obtenha e analise as políticas por escrito e examine as exibições do PAN (por exemplo, na tela, em recebimentos no formato de papel) para verificar se os PANs (primary account numbers) estão mascarados ao exibir os dados do portador do cartão, exceto para aquelas pessoas que tenham uma necessidade de negócios legítima de visualizar o PAN completo.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
3.4 Tornar o PAN, no mínimo, ilegível em qualquer local onde ele esteja armazenado em mídia digital portátil, mídia de back-up, em registros) utilizando qualquer uma das seguintes abordagens: ▪ Referências únicas com base na criptografia robusta ▪ Truncamento ▪ Tokens e blocos de índice (os blocos devem ser armazenados de forma segura) ▪ Criptografia robusta com processos e procedimentos de gerenciamento-chave associados As informações de conta MÍNIMAS que precisam ser convertidas como ilegíveis são o PAN. *Observações:* ▪ *Se, por algum motivo, uma empresa não puder tornar o PAN ilegível, consulte o* Apêndice B: Controles de compensação. ▪ *A "criptografia robusta" é definida na seção* Glossário de termos, abreviações e acrônimos do PCI DSS.	**3.4.a** Obtenha e analise a documentação sobre o sistema usado para proteger o PAN, incluindo o fornecedor, o tipo de sistema/processo e os algoritmos de criptografia (se aplicável). Verifique se o PAN for tornado ilegível usando um dos seguintes métodos: ▪ Referências únicas com base na criptografia robusta ▪ Truncamento ▪ Tokens e blocos de índice, sendo que os blocos são armazenados de forma segura ▪ Criptografia robusta, com processos e procedimentos de gerenciamento-chave associados			
	3.4.b Analise as diversas tabelas ou arquivos de um exemplo de repositórios de dados para verificar se o PAN foi tornado ilegível (ou seja, não foi armazenado em texto simples).			
	3.4.c Analise um exemplo de mídia removível (por exemplo, fitas de back-up) paa confirmar se o PAN foi tornado ilegível.			
	3.4.d Analise um exemplo de registros de auditoria para confirmar se o PAN foi transformado ou removido dos registros.			
3.4.1 Se a criptografia de disco for utilizada (em vez da criptografia de bancos de dados no nível de arquivo ou coluna), o acesso lógico deverá ser gerenciado independentemente de mecanismos de controle de acesso a sistemas operacionais nativos (por exemplo, não utilizando bancos de dados de	**3.4.1.a** Se a criptografia de disco for usada, verifique se o acesso lógico aos sistemas de arquivos criptografados foi implementado por meio de um mecanismo que seja separado do mecanismo de sistemas operacionais nativos (por exemplo, não usando os bancos de dados das contas de usuário locais).			
	3.4.1.b Verifique se as chaves criptográficas são armazenadas de forma segura (por exemplo, armazenadas nas mídias removíveis que estão protegidas adequadamente com controles de acesso robustos).			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
contas de usuário locais). As chaves de descrição não devem estar vinculadas às contas de usuário.	**3.4.1.c** Verifique se os dados do portador do cartão nas mídias removíveis estão criptografados aonde quer que estejam armazenados. *Observação: Com freqüência, a criptografia de disco não pode criptografar mídias removíveis, portanto os dados armazenados nessas mídias terão de ser criptografados separadamente.*			
3.5 Proteger as chaves criptográficas usadas para a criptografia dos dados do portador do cartão contra a divulgação e o uso incorreto:	**3.5** Verifique os processos para proteger as chaves usadas para a criptografia dos dados do portador do cartão contra a divulgação e o uso incorreto ao desempenhar o seguinte:			
3.5.1 Restringir o acesso às chaves criptográficas ao menor número necessário de responsáveis pela proteção.	**3.5.1** Analise as listas de acesso dos usuários para verificar se o acesso às chaves está restrito a poucos responsáveis pela proteção.			
3.5.2 Armazenar chaves criptográficas de forma segura no menor número possível de locais e formatos.	**3.5.2** Analise os arquivos de configuração do sistema para verificar se as chaves estão armazenadas no formato criptografado e se as chaves de criptografia principal estão armazenadas separadamente das chaves de criptografia de dados.			
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:	**3.6.a** Verifique a existência dos procedimentos de gerenciamento-chave com relação às chaves usadas para a criptografia dos dados do portador do cartão. *Observação: Vários padrões do setor para o gerenciamento-chave estão disponíveis a partir de diversos recursos, incluindo NIST, que pode ser encontrado em http://csrc.nist.gov.*			
	3.6.b Somente para os prestadores de serviços: Se o prestador de serviços compartilhar chaves com seus clientes para a transmissão de dados do portador do cartão, verifique se o prestador de serviços fornece uma documentação para os clientes que inclua uma orientação sobre como armazenar de forma segura e alterar as chaves do cliente (usadas para transmitir dados entre o cliente e o prestador de serviços).			
	3.6.c Analise os procedimentos de gerenciamento-chave e desempenhe o seguinte:			
3.6.1 Geração de chaves criptográficas robustas	**3.6.1** Verifique se os procedimentos de gerenciamento-chave foram implementados para exigir a geração de chaves robustas.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
3.6.2 Proteger a distribuição de chaves criptográficas	**3.6.2** Verifique se os procedimentos do gerenciamento-chave foram implementados para exigir a distribuição segura de chaves.			
3.6.3 Proteger o armazenamento de chaves criptográficas	**3.6.3** Verifique se os procedimentos do gerenciamento-chave foram implementados para exigir o armazenamento seguro das chaves.			
3.6.4 Alterações periódicas nas chaves criptográficas ▪ *Conforme considerado necessário e recomendado pelo aplicativo associado (por exemplo, nova atribuição de chaves); de preferência automaticamente* ▪ *Pelo menos anualmente*	**3.6.4** Verifique se os procedimentos do gerenciamento-chave foram implementados para exigir alterações periódicas das chaves pelo menos anualmente.			
3.6.5 Inutilização ou substituição de chaves criptográficas comprometidas antigas ou suspeitas	**3.6.5.a** Verifique se os procedimentos do gerenciamento-chave foram implementados para exigir a inutilização das chaves antigas (por exemplo: arquivamento, destruição e revogação, conforme aplicável).			
	3.6.5.b Verifique se os procedimentos do gerenciamento-chave foram implementados para exigir a substituição de chaves comprometidas conhecidas ou suspeitas.			
3.6.6 Separar o conhecimento e a determinação do controle duplo de chaves criptográficas	**3.6.6** Verifique se os procedimentos do gerenciamento-chave foram implementados para exigir a separação do conhecimento e do controle duplo das chaves (por exemplo, exigindo duas ou três pessoas, cada uma delas estando ciente da sua própria parte da chave, para reconstruir toda a chave).			
3.6.7 Prevenção contra a substituição não autorizada de chaves criptográficas	**3.6.7** Verifique se os procedimentos do gerenciamento-chave foram implementados para exigir a prevenção contra a substituição não autorizada das chaves.			
3.6.8 Requisito para que os responsáveis pela proteção das chaves criptográficas assinem um formulário declarando que eles compreendem e aceitam suas responsabilidades de responsáveis pela proteção das chaves	**3.6.8** Verifique se os procedimentos do gerenciamento-chave foram implementados para exigir que os responsáveis pela proteção assinem um formulário especificando que eles compreendem e aceitam suas responsabilidades de responsáveis pela proteção das chaves.			

Requisito 4: Criptografar a transmissão dos dados do portador do cartão em redes abertas e públicas

As informações confidenciais devem ser criptografadas durante a transmissão nas redes que são facilmente acessadas por indivíduos mal-intencionados. Redes sem fio configuradas de forma incorreta e vulnerabilidades na criptografia legada e protocolos de autenticação podem ser alvos contínuos de indivíduos mal-intencionados que exploram essas vulnerabilidades para obter acesso privilegiado aos ambientes de dados do portador do cartão.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
4.1 Utilizar uma criptografia robusta e protocolos de segurança como SSL/TLS ou IPSEC para proteger os dados confidenciais do portador do cartão durante a transmissão em redes abertas e públicas. *Os exemplos de redes abertas e públicas que estão no escopo do PCI DSS são:* ▪ *A Internet,* ▪ *Tecnologias sem fio,* ▪ *Global System for Mobile communications (GSM) e* ▪ *General Packet Radio Service (GPRS).*	**4.1.a** Verifique o uso da criptografia (por exemplo, SSL/TLS ou IPSEC) aonde quer que os dados do portador do cartão sejam transmitidos ou recebidos em redes abertas e públicas ▪ Verifique se a criptografia robusta é usada durante a transmissão dos dados ▪ Para implementações de SSL: – Verifique se o servidor é compatível com as versões corrigidas mais recentes. – Verifique se HTTPS é exibido como parte do Universal Record Locator (URL) do navegador. – Verifique se nenhum dado do portador do cartão é exigido quando HTTPS não for exibido no URL. ▪ Selecione um exemplo de transações à medida que recebem e observam as transações conforme elas ocorrem para verificar se os dados do portador do cartão estão criptografados durante o trânsito. ▪ Verifique se somente as chaves/certificados de SSL/TLS confiáveis são aceitas. ▪ Verifique se a força da criptografia adequada é implementada para a metodologia de criptografia sendo utilizada. (Verifique as recomentações/melhores práticas do fornecedor.)			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
4.1.1 Certificar-se de que as redes sem fio estejam transmitindo dados do portador do cartão ou estejam conectadas ao ambiente de dados do portador do cartão, usar as melhores práticas do setor (por exemplo, IEEE 802.11i) para implementar a criptografia robusta para a autenticação e a transmissão. ▪ *Para novas implementações sem fio, será proibido implementar o WEP após 31 de março de 2009.* ▪ *Para as implementações sem fio atuais, será proibido implementar o WEP após 30 de junho de 2010.*	**4.1.1** Para redes sem fio que transmitem dados do portador do cartão ou que estejam conectadas ao ambiente de dados do portador do cartão, verifique se as melhores práticas (por exemplo, IEEE 802.11i) são usads para implementar uma criptorafia robusta para a autenticação e a transmissão.			
4.2 Nunca enviar PANs não criptografadas através das tecnologias de envio de mensagens de usuário final (por exemplo, e-mail, sistemas de mensagens instantâneas, bate-papo).	**4.2.a** Verifique se a criptografia robusta é usada aonde quer que os dados do portador do cartão sejam enviados por meio das tecnologias de envio de mensagens de usuário final.			
	4.2.b Verifique a existência de uma política que afirmem que os PANs não criptografados não são enviados por meio das tecnologias de envio de mensagens de usuário final.			

Manter um programa de gerenciamento de vulnerabilidades

Requisito 5: Usar e atualizar regularmente o software ou programas antivírus

Softwares mal-intencionados, normalmente chamados de "malware"—incluindo vírus, worms e cavalos de Tróia—adentram a rede durante muitas atividades de negócios aprovadas, incluindo e-mail dos funcionários e uso da Internet, computadores móveis e dispositivos de armazenamento, resultando na exploração das vulnerabilidades do sistema. O software antivírus deve ser usado em todos os sistemas comumente afetados pelo malware para proteger os sistemas de ameaças atuais e potenciais de softwares mal-intencionados.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
5.1 Implementar softwares antivírus em todos os sistemas normalmente afetados por softwares mal-intencionados (especialmente em computadores pessoais e servidores).	**5.1** Para obter um exemplo dos componentes do sistemas incluindo todos os tipos de sistemas operacionais normalmente afetados por softwares mal-intencionados, verifique se o software antivírus foi implementado se houver uma tecnologia antivírus aplicável.			
5.1.1 Certificar-se de que todos os programas antivírus podem detectar, remover e proteger contra todos os tipos conhecidos de softwares mal-intencionados.	**5.1.1** Para obter um exemplo dos componentes do sistema, verifique se todos os programas antivírus detectam, removem e protegem contra todos os tipos conhecidos de softwares mal-intencionados (por exemplo, vírus, cavalos de Tróia, worms, spyware, adware e rootkits).			
5.2 Certificar-se de que todos os mecanismos antivírus estejam atualizados, funcionem ativamente e possam gerar registros de auditoria.	**5.2** Verifique se todos os softwares antivírus estão atualizados, funcionando ativamente e podem gerar registros ao desempenhar o seguinte:			
	5.2.a Obtenha e analise a política e verifique se ela exige a atualização dos softwares antivírus e definições.			
	5.2.b Verifique se a instalação principal do software está ativada para atualizações automáticas e digitalizações periódicas.			
	5.2.c Para obter um exemplo dos componentes do sistema incluindo todos os tipos de sistemas operacionais normalmente afetados pelos softwares mal-intencionados, verifique se as atualizações automáticas e as digitalizações periódicas estão ativadas.			
	5.2d Para obter um exemplo dos componentes do sistema, verifique se a geração de registros dos softwares antivírus está ativada e se tais registros são mantidos de acordo com o Requisito 10.7 do PCI DSS			

Requisito 6: Desenvolver e manter sistemas e aplicativos seguros

Indivíduos inescrupulosos usam as vulnerabilidades da segurança para obter acesso privilegiado aos sistemas. Muitas dessas vulnerabilidades são solucionadas pelos patches de segurança disponibilizados pelos fornecedores, que devem ser instalados pelas entidades que gerenciam os sistemas. Todos os sistemas críticos devem contar com os patches de software adequados lançados mais recentes para proteger contra a exploração e o comprometimento dos dados do portador do cartão por indivíduos e softwares mal-intencionados.

Observação: Patches de software adequados são aqueles patches que foram avaliados e testados de forma suficiente para determinar se os patches não entram em conflito com as configurações de segurança existentes. Para aplicativos desenvolvidos internamente, diversas vulnerabilidades podem ser evitadas ao utilizar processos de desenvolvimento do sistema padrão e técnicas de codificação seguras.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
6.1 Certificar-se de que todos os componentes do sistema e softwares têm os patches de segurança mais recentes disponibilizados pelos fornecedores instalados. Instalar patches de segurança críticos em até um mês após o lançamento. *Observação: Uma empresa talvez considere utilizar uma abordagem baseada nos riscos para priorizar suas instalações de patches. Por exemplo, ao priorizar mais a infra-estrutura crítica (por exemplo, dispositivos e sistemas disponibilizados ao público, bancos de dados) em vez de dispositivos internos menos críticos, para assegurar que sistemas e dispositivos de prioridade elevada sejam abordados em um mês e dispositivos e sistemas menos críticos em três meses.*	**6.1.a** Para obter um exemplo dos componentes do sistema e dos softwares relacionados, compare a lista de patches de segurança instalados em cada sistema com a lista de patches de segurança mais recentes do fornecedor para verificar se os patches atuais do fornecedor foram instalados.			
	6.1.b Analise as políticas relacionadas à instalação dos patches de segurança para verificar se elas exigem a instalação de todos os patches de segurança críticos novos em um mês.			
6.2 Definir um processo para identificar as vulnerabilidades de segurança descobertas recentemente (por exemplo, inscrever-se em serviços de alerta disponíveis gratuitamente na Internet). Atualizar os padrões de configuração conforme exigido pelo Requisito 2.2 do PCI DSS para solucionar novos problemas de vulnerabilidade.	**6.2.a** Entreviste a equipe responsável para verificar se os processos foram implementados para identificar novas vulnerabilidades de segurança.			
	6.2.b Verifique se os processos para identificar as novas vulnerabilidades de segurança que incluem a utilização de fontes externas para as informações sobre as vulnerabilidades de segurança e a atualização dos padrões de configuração do sistema analisados no Requisito 2.2 como novos problemas de vulnerabilidades são localizados.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
6.3 Desenvolver aplicativos de software de acordo com o PCI DSS (por exemplo, autenticação segura e registros) e com base nas melhores práticas do setor, além de incorporar a segurança das informações em todo o ciclo de vida do desenvolvimento dos softwares. Esses processos devem incluir o seguinte:	**6.3.a** Obtenha e analise os processos de desenvolvimento de softwares por escrito para verificar se os processos estão baseados nos padrões do setor, se a segurança está incluída em todo o ciclo de vida e se os aplicativos de software foram desenvolvidos de acordo com o PCI DSS.			
	6.3.b De uma avaliação dos processos de desenvolvimento do software por escrito, entrevistas com desenvolvedores de software e análise dos dados relevantes (documentação de configuração de rede, dados de produção e teste, etc.), verifique se:			
6.3.1 Teste de todos os patches de segurança e alterações de configuração no sistema e no software antes da implementação, incluindo, mas não se limitando a, o seguinte:	**6.3.1** Todas as alterações (incluindo os patches) são testadas antes de serem implementadas na produção.			
6.3.1.1 Validação de todas as entradas (para impedir scripting de sites cruzados, falhas na inserção, execução de arquivos mal-intencionados, etc.)	**6.3.1.1** Validação de todas as entradas (para impedir scripting de sites cruzados, falhas na inserção, execução de arquivos mal-intencionados, etc.)			
6.3.1.2 Validação adequada do tratamento de erros	**6.3.1.2** Validação adequada do tratamento de erros			
6.3.1.3 Validação de armazenamento criptográfico seguro	**6.3.1.3** Validação de armazenamento criptográfico seguro			
6.3.1.4 Validação das comunicações seguras	**6.3.1.4** Validação das comunicações seguras			
6.3.1.5 Validação de controle de acesso adequado baseado na função (RBAC)	**6.3.1.5** Validação de controle de acesso adequado baseado na função (RBAC)			
6.3.2 Ambientes de desenvolvimento/ testes e de produção separados	**6.3.2** Os ambientes de desenvolvimento/teste são separados do ambiente de produtção, com controle de acesso implementado para obrigar a separação.			
6.3.3 Separação dos deveres entre os ambientes de desenvolvimento/teste e de produção	**6.3.3** Há uma separação das tarefas entre a equipe atribuída aos ambientes de desenvolvimento/teste e a atribuída ao ambiente de produção.			
6.3.4 Os dados de produção (PANs ativos) não são usados para testes ou desenvolvimento	**6.3.4** Os dados de produção (PANs ativos) não são usados para testes ou desenvolvimento, ou são transformados antes da utilização.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
6.3.5 Remoção dos dados de teste e contas antes que os sistemas de produção tornem-se ativos	**6.3.5** Os dados e as contas de teste são removidos antes que o sistema de produção torne-se ativo.			
6.3.6 Remoção das contas dos aplicativos personalizados, IDs e senhas de usuários antes que os aplicativos tornem-se ativos ou sejam liberados para os clientes	**6.3.6** As contas dos aplicativos personalizados, IDs e/ou senhas de usuários são removidos antes que o sistema entre em produção ou seja liberado para os clientes.			
6.3.7 Analisar o código personalizado antes de liberar para produção ou para os clientes com o objetivo de identificar qualquer vulnerabilidade potencial de codificação *Observação: Esse requisito referente às análises dos códigos se aplica a todos os códigos personalizados (internos e voltados para o público), como parte integrante do ciclo de vida de desenvolvimento do sistema exigida pelo Requisito 6.3 do PCI DSS. As análises dos códigos podem ser realizadas por equipes internas instruídas ou terceiros. Os aplicativos da Web também estão sujeitos a controles extras, caso sejam voltados ao público, para abranger ameaças e vulnerabilidades contínuas após a implementação, conforme definido no Requisito 6.6 do PCI DSS.*	**6.3.7.a** Obtenha e analise as políticas para confirmar que todas as alterações nos códigos dos aplicativos personalizados referentes aos *aplicativos internos* devem ser revisadas (usando processos manuais ou automatizados), conforme se segue: ▪ As alterações dos códigos são analisadas por outras pessoas além do autor que originou o código e por pessoas que estão cientes das técnicas de análise dos códigos e das práticas de codificação seguras. ▪ As correções adequadas são implementadas antes da liberação. ▪ Os resultados das análises dos códigos são revisados e aprovados pela gerência antes da liberação.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
	6.3.7.b Obtenha e analise as políticas para confirmar que todas as alterações nos códigos dos aplicativos personalizados referentes aos *aplicativos da Web* devem ser revisados usando processos manuais ou automatizados), conforme se segue: ▪ As alterações dos códigos são analisadas por outras pessoas além do autor que originou o código e por pessoas que estão cientes das técnicas de análise dos códigos e das práticas de codificação seguras. ▪ As análises dos códigos asseguram que o código foi desenvolvido de acordo com as diretrizes de codificação seguras como o *Guia do projeto de segurança do aplicativo aberto na Web* (consulte o Requisito 6.5 do PCI DSS). ▪ As correções adequadas são implementadas antes da liberação. ▪ Os resultados das análises dos códigos são revisados e aprovados pela gerência antes da liberação.			
	6.3.7.c Selecione um exemplo de alterações recentes dos aplicativos personalizados e verifique se o código do aplicativo personalizado é analisado de acordo com os itens 6.3.7a e 6.3.7b acima.			
6.4 Seguir os procedimentos de controle de alterações para todas as alterações nos componentes do sistema. Os procedimentos devem incluir o seguinte:	**6.4.a** Obtenha e analise os procedimentos de controle de alterações da empresa relacionados à implementação dos patches de segurança e às modificações do software, e verifique se os procedimentos requerem os itens 6.4.1 a 6.4.4 abaixo.			
	6.4.b Para obter um exemplo dos componentes do sistema e dos patches de segurança/alterações recentes, monitore essas alterações com relação à documentação de controle de alterações respectiva. Para cada alteração analisada, desempenhe o seguinte:			
6.4.1 Documentação de impacto	**6.4.1** Verifique se a documentação de impacto no client está incluída na documentação de controle de alterações para cada alteração exemplificada.			
6.4.2 Endosso da gerência pelas partes apropriadas	**6.4.2** Verifique se o endosso da gerência pelas partes apropriadas está presente para cada alteração exemplificada.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
6.4.3 Teste da funcionalidade operacional	**6.4.3** Verifique se o teste da funcionalidade operacional foi realizado para alteração exemplificada.			
6.4.4 Procedimentos de reversão	**6.4.4** Verifique se os procedimentos de reversão foram preparados para cada alteração exemplificada			
6.5 Desenvolver todos os aplicativos da Web (internos e externos, e incluindo o acesso administrativo na Web ao aplicativo) com base nas diretrizes de codificação seguras, como o *Guia do projeto de segurança do aplicativo aberto da Web.* Abranger a prevenção de vulnerabilidades de codificação comuns nos processos de desenvolvimento do software, para incluir o seguinte: *Observação: As vulnerabilidades listadas nos itens 6.5.1 a 6.5.10 estavam atualizadas no guia do projeto de segurança do aplicativo aberto da Web quando a versão 1.2 do PCI DSS foi publicada. No entanto, se e quando o guia do projeto de segurança do aplicativo aberto da Web for atualizado, a versão atual deverá ser usada para esses requisitos.*	**6.5.a** Obtenha e analise os processos de desenvolvimento de software para quaisquer aplicativos baseados na Web. Verifique se os processos requerem treinamento em técnicas de codificação seguras para desenvolvedores e estão baseados em orientações, como o guia do projeto de segurança do aplicativo aberto na Web (http://www.owasp.org).			
	6.5.b Entreviste alguns desenvolvedores e obtenha uma comprovação de que eles estão instruídos sobre as técnicas de codificação seguras.			
	6.5.c Verifique se os processos foram implementados para assegurar que os aplicativos da Web não são vulneráveis ao seguinte:			
6.5.1 Scripting de sites cruzados (XSS)	**6.5.1** Scripting de sites cruzados (XSS) (Valide todos os parâmetros antes da inclusão.)			
6.5.2 Falhas na inserção, principalmente na inserção SQL. Também considere as falhas de inserção LDAP e Xpath, assim como outras falhas.	**6.5.2** Falhas na inserção, principalmente na inserção SQL (Valide a entrada para verificar se os dados do usuário não podem modificar o significado dos comandos e das consultas.)			
6.5.3 Execução de arquivos mal-intencionados	**6.5.3** Execução de arquivos mal-intencionados (Valide a entrada para verificar se o aplicativo não aceita nomes de arquivo ou arquivos de usuários.)			
6.5.4 Referências diretas a objetos inseguros	**6.5.4** Referências diretas a objetos inseguros (Não exponha referências a objetos internos aos usuários.)			
6.5.5 Falsificação de solicitações de sites cruzados (CSRF)	**6.5.5** Falsificação de solicitações de sites cruzados (CSRF) (Não responda a credenciais de autorização ou tokens enviados automaticamente pelos navegadores.)			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
6.5.6 Vazamento de informações e manuseio incorreto de erros	**6.5.6** Vazamento de informações e manuseio incorreto de erros (Não vaze informações por meio de mensagens de erro ou outros meios.)			
6.5.7 Autenticação corrompida e gerenciamento de sessão	**6.5.7** Autenticação corrompida e gerenciamento de sessão (Autentique os usuários de forma adequada e proteja as credenciais da conta e os tokens de sessão.)			
6.5.8 Armazenamento criptográfico inseguro	**6.5.8** Armazenamento criptográfico inseguro (Impeça a ocorrência de falhas criptográficas.)			
6.5.9 Comunicações inseguras	**6.5.9** Comunicações inseguras (Criptografe de forma adequada todas as comunicações autenticadas e confidenciais.)			
6.5.10 Falha em restringir o acesso a URLs	**6.5.10** Falha em restringir o acesso a URLs (Imponha consistentemente o controle de acesso na camada de apresentação e na lógica dos negócios para todos os URLs.)			
6.6 Para aplicativos da Web voltados ao público, abordar novas ameaças e vulnerabilidades continuamente e assegurar que esses aplicativos estejam protegidos contra ataques conhecidos por *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 ▪ Instalar um firewall para aplicativos da Web diante de aplicativos da Web voltados ao público	**6.6** Para aplicativos da Web *voltados ao público,* certifique-se de que *qualquer um* dos métodos a seguir esteja implementado conforme se segue: ▪ Verifique se os aplicativos da Web voltados ao público foram analisados (usando ferramentas ou métodos manuais ou automatizados de avaliação de segurança das vulnerabilidades), conforme se segue: – Pelo menos anualmente – Após quaisquer alterações – Por meio de uma empresa especializada na segurança de aplicativos – Se todas as vulnerabilidades forem corrigidas – Se o aplicativo for reavaliado após as correções ▪ Verifique se um firewall de aplicativos da Web está implementado diante dos aplicativos da Web voltados ao público para detectar e impedir ataques baseados na Web. *Observação: "Uma empresa especializada na segurança de aplicativos" pode ser uma empresa terceirizada ou uma empresa interna, desde que os analisadores sejam especializados na segurança de aplicativos e possam demonstrar que não dependem da equipe de desenvolvimento.*			

Implementar medidas de controle de acesso rigorosas

Requisito 7: Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios

Para assegurar que os dados críticos possam ser acessados somente por uma equipe autorizada, os sistemas e processos devem estar implementados para limitar o acesso com base na necessidade de divulgação e de acordo com as responsabilidades da função.

A "necessidade de divulgação" é quando os direitos de acesso são concedidos somente ao menor número possível de dados e privilégios necessários para realizar um trabalho.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
7.1 Limitar o acesso aos componentes do sistema e aos dados do portador do cartão somente àquelas pessoas cuja função requer tal acesso. As limitações de acesso devem incluir o seguinte:	**7.1** Obtenha e analise a política por escrito referente ao controle de dados, e verifique se a política incorpora o seguinte:			
7.1.1 Restrição dos direitos de acesso a IDs de usuários privilegiados ao menor número de privilégios necessários para desempenhar as responsabilidades da função	**7.1.1** Confirme se os direitos de acesso a IDs de usuários privilegiados estão restritos ao menor número de privilégios necessários para desempenhar as responsabilidades da função.			
7.1.2 A concessão dos privilégios está baseada na classificação e na atribuição da função da equipe individual	**7.1.2** Confirme se os privilégios são concedidos às pessoas com base na classificação e na atribuição da função (também chamada de "controle de acesso baseado na função" ou RBAC).			
7.1.3 O requisito de um formulário de autorização assinado pela gerência que especifica os privilégios exigidos	**7.1.3** Confirme se um formulário de autorização é exigido para todos os acesso, se ele deve especificar os privilégios exigidos e ser assinado pela gerência.			
7.1.4 Implementação de um sistema de controle de acesso automático	**7.1.4** Confirme se os controles de acesso foram implementados por meio de um sistema de controle de acesso automático.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
7.2 Estabeleça um sistema de controle de acesso para os componentes do sistema com múltiplos usuários que restringe o acesso com base na necessidade de conhecimento do usuário e está configurado para "recusar todos", a menos que seja permitido de forma específica. Esse sistema de controle de acesso deve incluir o seguinte:	**7.2** Analise as configurações do sistema e a documentação do fornecedor para verificar se um sistema de controle de acesso foi implementado, conforme se segue:			
7.2.1 Abrangência de todos os componentes do sistema	**7.2.1** Confirme se os sistemas de controle de acesso foram implementados em todos os componentes do sistema.			
7.2.2 A concessão dos privilégios às pessoas está baseada na classificação e na atribuição da função	**7.2.2** Confirme se os sistemas de controle de acesso estão configurados para impor os privilégios concedidos às pessoas com base na classificação e na atribuição da função.			
7.2.3 Configuração padrão “recusar todos”	**7.2.3** Confirme se os sistemas de controle de acesso têm uma configuração padrão “recusar todos”. *Observação: Alguns sistemas de controle de acesso são definidos, como padrão, como “permitir todos”, permitindo portanto o acesso a menos que/até que uma norma seja redigida para recusá-lo de forma específica.*			

Requisito 8: Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador.

Atribuir uma identificação exclusiva (ID) a cada pessoa com acesso assegura que cada indivíduo seja exclusivamente responsável pelas suas ações. Quando tal responsabilidade estiver em vigor, as ações desempenhadas nos dados e sistemas críticos serão realizadas por usuários conhecidos e autorizados, e poderão levar a eles.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
8.1 Atribuir a todos os usuários um ID exclusivo antes de permitir que eles acessem os componentes do sistema ou os dados do portador do cartão.	**8.1** Verifique se todos os usuários receberam um ID exclusivo para acessar os componentes do sistema ou os dados do portador do cartão.			
8.2 Além de atribuir um ID exclusivo, utilize pelo menos um dos métodos a seguir para autenticar todos os usuários: ▪ Senha ou passphrase ▪ Autenticação com dois fatores (por exemplo, dispositivos de token, smart card, biométrica ou chaves públicas)	**8.2** Para verificar se os usuários são autenticados usando o ID exclusivo e a autenticação adicional (por exemplo, uma senha) para acessar o ambiente de dados do portador do cartão, desempenhe o seguinte: ▪ Obtenha e analise a documentação que descreve o(s) método(s) de autenticação usado(s). ▪ Para cada tipo do método de autenticação usado e para cada tipo do componente de sistema, observe uma autenticação para verificar se autenticação está sendo executada de acordo com o(s) método(s) de autenticação documentado(s).			
8.3 Incorporar a autenticação com dois fatores para o acesso remoto (acesso no nível da rede que se origina fora dela) à rede pelos funcionários, administradores e terceiros. Usar tecnologias como a autenticação remota e o serviço dial-in (RADIUS); sistema de controle de acesso ao controlador de acesso do terminal (TACACS) com tokens; ou VPN (baseado em SSL/TLS ou IPSEC) com certificados individuais.	**8.3** Para verificar se a autenticação com dois fatores foi implementada em todo acesso remoto à rede, observe um funcionário (por exemplo, um administrador) se conectando remotamente à rede e verifique se uma senha e um item de autenticação adicional (por exemplo, smart card, token, PIN) são exigidos.			
8.4 Tornar todas as senhas ilegíveis durante a transmissão e o armazenamento em todos os componentes usando a criptografia robusta (definida em *Glossário de termos, abreviações e acrônimos do PCI DSS*).	**8.4.a** Para obter um exemplo dos componentes do sistema, analise os arquivos de senha para verificar se as senhas estão ilegíveis durante a transmissão e o armazenamento.			
	8.4.b Somente para prestadores de serviços, observe os arquivos de senha para verificar se as senhas do cliente estão criptografadas.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
8.5 Certificar-se do gerenciamento adequado da autenticação e da senha do usuário para usuários que não sejam clientes e administradores em todos os componentes do sistema, conforme se segue:	**8.5** Analise os procedimentos e entreviste as equipes para verificar se os procedimentos foram implementados visando ao gerenciamento da autenticação e da senha, desempenhando o seguinte:			
8.5.1 Controle o acréscimo, a exclusão e a modificação dos IDs do usuário, credenciais e outros objetos do responsável pela identificação.	**8.5.1.a** Selecione um exemplo de IDs do usuário, incluindo administradores e usuários gerais. Verifique se cada usuário tem autorização para usar o sistema de acordo com a política da empresa ao desempenhar o seguinte: ▪ Obtenha e analise um formulário de autorização para cada ID. ▪ Verifique se os IDs do usuário exemplificados foram implementados de acordo com o formulário de autorização (incluindo os privilégios conforme especificado e todas as assinaturas obtidas) ao rastrear as informações do formulário de autorização ao sistema.			
8.5.2 Verificar a identidade do usuário antes de realizar as redefinições de senha.	**8.5.2** Analise os procedimentos de senha e observe a equipe de segurança para verificar se, caso um usuário solicite uma redefinição de senha por telefone, e-mail, Web ou outro método remoto, a identidade do usuário será comprovada antes da redefinição da senha.			
8.5.3 Definir as senhas iniciais para um valor exclusivo para cada usuário e alterar imediatamente após a primeira utilização.	**8.5.3** Analise os procedimentos de senha e observe a equipe de segurança para verificar se as senhas iniciais para usuários novos são definidas para um valor exclusivo para cada usuário e alteradas após a primeira utilização.			
8.5.4 Revogar imediatamente o acesso de quaisquer usuários desligados da empresa.	**8.5.4** Selecione um exemplo de funcionários desligados da empresa nos últimos seis meses e analise as listas de acesso dos usuários atuais para verificar se seus IDs foram desativados ou removidos.			
8.5.5 Remover/desativar as contas dos usuários inativos pelo menos a cada 90 dias.	**8.5.5** Verifique se as contas inativas nos últimos 90 dias foram removidas ou desativadas.			
8.5.6 Ativar as contas usadas pelos fornecedores somente para a manutenção remota durante o período necessário.	**8.5.6** Verifique se quaisquer contas usadas pelos fornecedores para suportar e manter os componentes do sistema foram desativadas, ativadas pelo fornecedor somente quando necessário e monitoradas durante o uso.			
8.5.7 Transmitir os procedimentos e políticas de senha a todos os usuários que têm acesso aos dados do portador do cartão.	**8.5.7** Entreviste os usuários de um exemplo de IDs do usuário para verificar se eles estão familiarizados com os procedimentos e políticas de senha.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
8.5.8 Não usar contas e senhas em grupo, compartilhadas ou genéricas.	**8.5.8.a** Para obter um exemplo dos componentes do sistema, analise as listas de ID do usuário para verificar o seguinte ▪ IDs e contas genéricas de usuários foram desativadas ou removidas. ▪ IDs de usuários compartilhados para atividades de administração do sistema e outras funções críticas ausentes. ▪ IDs de usuários compartilhados e genéricos não são usados para administrar quaisquer componentes do sistema.			
	8.5.8.b Analise as políticas/procedimentos de senha para verificar se senhas em grupo e compartilhadas estão explicitamente proibidas.			
	8.5.8.c Entreviste os administradores do sistema para verificar se senhas em grupo ou compartilhadas não são distribuídas, mesmo se forem solicitadas.			
8.5.9 Alterar as senhas do usuário pelo menos a cada 90 dias.	**8.5.9** Para obter um exemplo dos componentes do sistema, obtenha e analise as definições de configuração do sistema para verificar se os parâmetros de senha do usuário estão definidos para exigir que os usuários alterem as senhas pelo menos a cada 90 dias. Somente para os prestadores de serviços, analise os processos internos e a documentação do cliente/usuário para verificar se as senhas do cliente devem ser alteradas periodicamente e se os clientes recebem instruções sobre quando e sob quais circunstâncias as senhas devem ser alteradas.			
8.5.10 Exigir um comprimento mínimo de senha de pelo menos sete caracteres.	**8.5.10** Para obter um exemplo dos componentes do sistema, obtenha e analise as definições da configuração do sistema para verificar se os parâmetros de senha foram definidos para exigir que as senhas tenham pelo menos sete caracteres de comprimento. Somente para prestadores de serviços, analise os processos internos e a documentação do cliente/usuário para verificar se as senhas do cliente devem atender aos requisitos de comprimento mínimo.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
8.5.11 Usar senhas que contenham caracteres alfanuméricos.	**8.5.11** Para obter um exemplo dos componentes do sistema, obtenha e analise as definições da configuração do sistema para verificar se os parâmetros de senha foram definidos para exigir que as senhas contenham caracteres alfanuméricos. Somente para prestadores de serviços, analise os processos internos e a documentação do cliente/usuário para verificar se as senhas do cliente devem conter caracteres alfanuméricos.			
8.5.12 Não permitir que ninguém envie uma nova senha que seja a mesma de uma das quatro últimas senhas que tenha sido usada.	**8.5.12** Para obter um exemplo dos componentes do sistema, obtenha e analise as definições da configuração do sistema para verificar se os parâmetros de senha foram definidos para exigir que as novas senhas não possam ser as mesas das quatro senhas usadas anteriormente. Somente para prestadores de serviços, analise os processos internos e a documentação do cliente/usuário para verificar se as novas senhas do cliente não poderão ser iguais às quatro senhas anteriores.			
8.5.13 Limitar tentativas de acesso repetidas ao bloquear o ID do usuário após seis tentativas, no máximo.	**8.5.13** Para obter um exemplo dos componentes do sistema, obtenha e analise as definições da configuração do sistema para verificar se os parâmetros de senha foram definidos para exigir que a conta de um usuário seja bloqueada após, seis tentativas inválidas de efetuar login, no máximo. Somente para prestadores de serviços, analise os processos internos e a documentação do cliente/usuário para verificar se as contas do cliente são bloqueadas temporariamente após seis tentativas inválidas de acesso, no máximo.			
8.5.14 Definir a duração do bloqueio para um mínimo de 30 minutos ou até o administrador ativar o ID do usuário.	**8.5.14** Para obter um exemplo dos componentes do sistema, obtenha e analise as definições da configuração do sistema para verificar se os parâmetros de senha são definidos para exigir que assim que a conta de um usuário for bloqueada, ela permanecerá dessa forma por pelo menos 30 minutos ou até que um administrador do sistema reconfigure a conta.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
8.5.15 Se uma sessão estiver ociosa por mais de 15 minutos, exigir que o usuário redigite a senha para reativar o terminal.	**8.5.15** Para obter um exemplo dos componentes do sistema, obtenha e analise as definições de configuração do sistema para verificar se os recursos de tempo esgotado de ociosidade do sistema/sessão foram definidos para 15 minutos ou menos.			
8.5.16 Autenticar todos os acessos para qualquer banco de dados que contenha dados do portador do cartão, incluindo acesso por meio de aplicativos, administradores e todos os outros usuários.	**8.5.16.a** Analise as definições do banco de dados e da configuração do aplicativo para verificar se a autenticação do usuário e o acesso aos bancos de dados incluem o seguinte: ▪ Todos os usuários são autenticados antes do acesso. ▪ Todos os acessos dos usuários, consultas dos usuários e ações dos usuários (por exemplo, mover, copiar, excluir) nos bancos de dados são por meio apenas de métodos programáticos (por exemplo, através dos procedimentos armazenados). ▪ O acesso direto ou as consultas aos bancos de dados estão restritos aos administradores do banco de dados.			
	8.5.16.b Analise os aplicativos do banco de dados e os IDs dos aplicativos relacionados para verificar se os IDs dos aplicativos podem ser usados somente pelos aplicativos (e não apenas por usuários individuais ou outros processos).			

Requisito 9: Restringir o acesso físico aos dados do portador do cartão.

Qualquer acesso físico aos dados ou sistemas que armazenam dados do portador do cartão fornecem a oportunidade para as pessoas acessarem dispositivos ou dados e removerem sistemas ou cópias impressas, e deve ser restrito de forma adequada.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
9.1 Usar controles de entrada facilitados e adequados para limitar e monitorar o acesso físico aos sistemas no ambiente de dados do portador do cartão.	**9.1** Verifique a existência dos controles de segurança física em cada ambiente com computador, central de dados e outras áreas físicas com sistemas no ambiente de dados do portador do cartão. ▪ Verifique se o acesso é controlado com leitores de credenciais ou outros dispositivos, incluindo credenciais autorizadas e bloqueio e chave. ▪ Observe a tentativa de um administrador do sistema de efetuar login em consoles visando aos sistemas selecionados aleatoriamente no ambiente do portador do cartão e verifique se eles estão "bloqueados" para impedir o uso não autorizado.			
9.1.1 Usar câmeras de vídeo ou outros mecanismos de controle de acesso para monitorar o acesso físico individual a áreas confidenciais. Analisar os dados coletados e relacionar com outras entradas. Armazenar, 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 portador do cartão. Isso exclui as áreas nas quais há somente terminais do ponto de venda presentes, como as áreas dos caixas em uma loja de varejo.*	**9.1.1** Verifique se câmeras de vídeo ou outros mecanismos de controle de acesso foram implantados para monitorar os pontos de entrada/saída das áreas confidenciais. Câmeras de vídeo ou outros mecanismos devem ser protegidos de violação ou desativação. Verifique se as câmeras de vídeo ou outros mecanismos são monitorados e se os dados das câmeras ou outros mecanismos são armazenados por pelo menos três meses.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
9.1.2 Restringir o acesso físico a pontos de rede acessíveis publicamente.	**9.1.2** Verifique ao entrevistar os administradores da rede e observar se os pontos de rede são ativados somente quando necessário pelos funcionários autorizados. Por exemplo, as salas de conferência usadas para receber visitantes não devem ter portas de rede ativadas com DHCP. Verifique também se os visitantes sempre são acompanhados nas áreas com pontos de rede ativos.			
9.1.3 Restringir o acesso físico a pontos de acesso sem fio, gateways e dispositivos portáteis.	**9.1.3** Verificar se o acesso físico a pontos de acesso sem fio, gateways e dispositivos portáteis é restringido de forma adequada.			
9.2 Desenvolver procedimentos para ajudar todas as equipes a diferenciar facilmente os funcionários dos visitantes, principalmente nas áreas onde os dados do portador do cartão podem ser acessados. *Para as finalidades desse requisito, "funcionário" refere-se a funcionários que trabalham em período integral e meio-período, funcionários e equipes temporárias, e prestadores de serviços e consultores que "residem" no endereço da entidade. Um "visitante" é definido como um fornecedor, convidado de um funcionário, equipes de serviço ou qualquer pessoa que precise adentrar as dependências por um breve período, normalmente um dia, no máximo.*	**9.2.a** Analise os processos e procedimentos para atribuir crachás aos funcionários e visitantes, e verifique se esses processos incluem o seguinte: ▪ Conceder novos crachás, modificar os requisitos de acesso e anular crachás de funcionários que se desligaram da empresa e de visitantes que encerraram sua atividade. ▪ Acesso limitado ao sistema de crachás			
	9.2.b Observe as pessoas dentro das dependências para verificar se é fácil fazer uma distinção entre os funcionários e os visitantes.			
9.3 Certificar-se de que todos os visitantes são identificados da seguinte forma:	**9.3** Verifique se os controles dos funcionários/visitantes foram implementados da seguinte forma:			
9.3.1 Autorizados antes de adentrar as áreas onde os dados do portador do cartão são processados ou mantidos	**9.3.1** Observe os visitantes para verificar o uso dos crachás de identificação dos visitantes. Tente obter acesso à central de dados para verificar se um crachá de identificação dos visitantes não permite o acesso sem acompanhamento a áreas físicas que armazenam dados do portador do cartão.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
9.3.2 Um token físico é fornecido (por exemplo, um crachá ou dispositivo de acesso) que expira e que identifica os visitantes como não sendo funcionários	**9.3.2** Analise os crachás dos funcionários e dos visitantes para verificar se os crachás de identificação claramente fazem uma distinção entre os funcionários e os visitantes/pessoas de fora e se os crachás dos visitantes expiram.			
9.3.3 É solicitado que os visitantes apresentem o token físico antes de sair das dependências ou na data do vencimento	**9.3.3** Observe os visitantes que saem das dependências para verificar se é solicitado que os visitantes apresentem seu crachá de identificação na saída ou quando do vencimento.			
9.4 Usar um registro de visitantes para manter um monitoramento físico da auditoria da atividade do visitante. 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.	**9.4.a** Verifique se um registro de visitantes está sendo usado para registrar o acesso físico às dependências, assim como aos ambientes com computador e centrais de dados onde os dados do portador do cartão são armazenados ou transmitidos.			
	9.4.b Verifique se o registro contém o nome do visitante, a empresa representada e o funcionário que está autorizando o acesso físico, e se é mantido por pelo menos três meses.			
9.5 Armazenar back-ups de mídia em um local seguro, de preferência em uma área externa, como um local alternativo ou de back-up, ou uma área de armazenamento comercial. Analisar a segurança do local pelo menos uma vez por ano.	**9.5** Verifique se o local de armazenamento é analisado pelo menos uma vez por ano para determinar se o armazenamento das mídias de back-up está protegido.			
9.6 Proteger fisicamente todos os documentos impressos e as mídias eletrônicas que contêm dados do portador do cartão.	**9.6** Verifique se os procedimentos para proteger os dados do portador do cartão incluem controles para proteger fisicamente os documentos impressos e as mídias eletrônicas (incluindo computadores, mídias eletrônicas removíveis, sistemas de redes e hardwares de comunicação, linhas de telecomunicação, recebimentos de documentos impressos, relatórios impressos e faxes).			
9.7 Manter o controle rigoroso quanto à distribuição interna ou externa de qualquer tipo de mídia que contenha dados do portador do cartão, incluindo o seguinte:	**9.7** Verifique se há uma política para controlar a distribuição de mídias que contêm dados do portador do cartão e se a política abrange todas as mídias distribuídas, incluindo as distribuídas às pessoas.			
9.7.1 Classifique a mídia para que ela possa ser identificada como confidencial.	**9.7.1** Verifique se todas as mídias são classificadas de uma forma que ela possa ser identificada como “confidencial.”			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
9.7.2 Enviar a mídia via mensageiro seguro ou outro método de entrega que pode ser monitorado com precisão.	**9.7.2** Verifique se a mídia enviada externamente é registrada e autorizada pela gerência e encaminhada via mensageiro seguro ou outro método de entrega que possa ser monitorado.			
9.8 Certificar-se de que a gerência aprova quaisquer e todas as mídias contendo dados do portador do cartão que são movidas de uma área segura (principalmente quando as mídias forem distribuídas às pessoas).	**9.8** Selecione um exemplo recente de vários dias de registros de monitoramento externo para todas as mídias que contêm dados do portador do cartão e verifique a presença dos detalhes de monitoramento e da autorização apropriada da gerência nos registros.			
9.9 Manter um controle rigoroso sobre o armazenamento e a acessibilidade das mídias que contêm dados do portador do cartão.	**9.9** Obtenha e analise a política para controlar o armazenamento e a manutenção dos documentos impressos e mídias eletrônicas, e verifique se a política requer inventários de mídia periódicos.			
9.9.1 Manter adequadamente os registros do inventário de todas as mídias e realizar inventários das mídias pelo menos uma vez por ano.	**9.9.1** Obter e analisar o registro do inventário das mídias para verificar se inventários periódicos das mídias são realizados pelo menos uma vez por ano.			
9.10 Destruir as mídias que contêm dados do portador do cartão quando eles não forem mais necessários por motivos de negócios ou legais, conforme se segue:	**9.10** Obtenha e analise a política de destruição periódica das mídias e verificar se ela abrange todas as mídias que contêm dados do portador do cartão e confirme o seguinte:			
9.10.1 Triturar, incinerar ou amassar materiais impressos para que os dados do portador do cartão não possam ser recuperados.	**9.10.1.a** Verifique se os materiais impressos são triturados, incinerados ou amassados de uma forma que haja uma garantia razoável de que esses materiais não possam ser recuperados.			
	9.10.1.b Analise os contêineres de armazenamento usados para as informações a serem destruídas para verificar se são seguros. Por exemplo, verifique se um contêiner “a ser triturado” tem uma trava que impede o acesso ao seu conteúdo.			
9.10.2 Tornar os dados do portador do cartão nas mídias eletrônicas indisponibilizáveis para que esses dados não possam ser recuperados.	**9.10.2** Verifique se os dados do portador do cartão nas mídias eletrônicas são indisponibilizados por meio de um programa de limpeza segura, de acordo com os padrões aceitos pelo setor quanto à exclusão segura, ou de outra forma, destruindo fisicamente as mídias (por exemplo, desmagnetizando).			

Monitorar e Testar as Redes Regularmente

Requisito 10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão.

Mecanismos de registro e a capacidade de monitorar as atividades dos usuários são fundamentais na prevenção, detecção ou minimização do impacto do comprometimento dos dados. A presença de registros em todos os ambientes permite o monitoramento, o alerta e a análise completa quando algo dá errado. Determinar a causa de um comprometimento é muito difícil sem registros das atividades do sistema.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
10.1 Definir um processo para vincular todos os acessos aos componentes do sistema (principalmente o acesso realizado com privilégios administrativos como raiz) para cada usuário individual.	**10.1** Verifique por meio da observação e entreviste o administrador do sistema perguntando se as trilhas de auditoria estão habilitadas e ativadas para os componentes do sistema.			
10.2 Implementar trilhas de auditoria automatizadas para todos os componentes do sistema para recuperar os seguintes eventos:	**10.2** Por meio de entrevistas, análise de registros de auditoria e de suas configurações, desempenhe o seguinte:			
10.2.1 Todos os acessos individuais aos dados do portador do cartão	**10.2.1** Verifique se todos os acessos individuais aos dados do portador do cartão estão registrados.			
10.2.2 Todas as ações desempenhadas por qualquer pessoa com privilégios raiz ou administrativos	**10.2.2** Verifique se as ações desempenhadas por qualquer pessoa com privilégios raiz ou administrativos são registradas.			
10.2.3 Acesso a todas as trilhas de auditoria	**10.2.3** Verificar se o acesso a todas as trilhas de auditoria é registrado.			
10.2.4 Tentativas inválidas de acesso lógico	**10.2.4** Verifique se as tentativas inválidas de acesso lógico são registradas.			
10.2 5 Uso de mecanismos de identificação e autenticação	**10.2.5** Verifique se o uso dos mecanismos de identificação e autenticação é registrado.			
10.2.6 Inicialização dos registros de auditoria	**10.2.6** Verificar se a inicialização dos registros de auditoria é registrada.			
10.2.7 Criação e exclusão de objetos do nível do sistema	**10.2.7** Verificar se a criação e a exclusão de objetos do nível do sistema são registrados.			
10.3 Registrar pelo menos as seguintes entradas das trilhas de auditoria para todos os componentes do sistema para cada evento:	**10.3** Por meio de entrevistas e da observação, para cada evento auditável (no item 10.2), desempenhe o seguinte:			
10.3.1 Identificação do usuário	**10.3.1** Verifique se a identificação do usuário está incluída nas entradas do registro.			
10.3.2 Tipo do evento	**10.3.2** Verifique se o tipo do evento está incluído nas entradas do registro.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
10.3.3 Data e horário	**10.3.3** Verifique se a data e o horário estão incluídos nas entradas do registro.			
10.3.4 Indicação de êxito ou falha	**10.3.4** Verifique se a indicação de êxito ou falha está incluída nas entradas do registro.			
10.3.5 Origem do evento	**10.3.5** Verifique se a origem do evento está incluída nas entradas do registro.			
10.3.6 A identidade ou o nome dos dados afetados, componentes do sistema ou recurso	**10.3.6** Verifique se a identidade ou o nome dos dados afetados, componentes do sistema ou recursos está incluído nas entradas do registro.			
10.4 Sincronizar todos os relógios e horários do sistema crítico.	**10.4** Obtenha e analise o processo para a aquisição e a distribuição do horário correto na empresa, assim como as configurações dos parâmetros do sistema relacionadas ao horário com relação a alguns exemplos dos componentes do sistema. Verifique se as informações a seguir estão incluídas no processo e foram implementadas:			
	10.4.a Verifique se uma versão conhecida e estável do NTP (Network Time Protocol) ou tecnologia semelhante, mantida atualizada de acordo com os Requisitos 6.1 e 6.2 do PCI DSS, é usada para a sincronização dos horários.			
	10.4.b Verifique se os servidores internos não estão recebendo sinais de horário de fontes externas. [Dois ou três servidores de horário centrais na empresa recebem sinais de horário externos [diretamente de um rádio especial, satélites GPS ou outras fontes externas com base no International Atomic Time e UTC (GMT anteriormente)], estabelecem uma conexão entre si para manter o horário preciso e compartilham o horário com outros servidores internos.]			
	10.4.c Verifique se hosts externos especiais foram atribuídos, a partir dos quais os servidores de horário aceitarão as atualizações de horário do NTP (para impedir que indivíduos mal-intencionados alterem o relógio). Além disso, essas atualizações podem ser criptografas com uma chave simétrica e as listas de controle de acesso podem ser criadas que especificam os endereços IP das máquinas clientes que serão fornecidas com o serviço do NTP (para impedir o uso de servidores de horário internos). Acesse o site www.ntp.org para obter mais informações			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
10.5 Proteger as trilhas de auditoria para que não possam ser alteradas.	**10.5** Entreviste o administrador do sistema e analise as permissões para verificar se as trilhas de auditoria estão protegidas de uma forma que não possam ser alteradas da seguinte forma:			
10.5.1 Limitar a exibição de trilhas de auditoria às pessoas que têm uma necessidade relacionada à função.	**10.5.1** Verifique se apenas os indivíduos que têm uma necessidade relacionada à função podem visualizar arquivos de trilha de auditoria.			
10.5.2 Proteger os arquivos de trilha de auditoria de modificações não autorizadas.	**10.5.2** Verifique se os arquivos de trilha de auditoria atuais estão protegidos de modificações não autorizadas por meio de mecanismos de controle de acesso, separação física e/ou separação da rede.			
10.5.3 Fazer imediatamente o back-up dos arquivos de trilha de auditoria em um servidor de registros centralizado ou mídias que sejam difíceis de alterar.	**10.5.3** Verifique se é realizado imediatamente o back-up dos arquivos de trilha de auditoria atuais em um servidor de registros centralizado ou mídias que sejam difíceis de alterar.			
10.5.4 Documentar registros quanto às tecnologias externas em um servidor de registros na LAN interna.	**10.5.4** Verifique se os registros quanto às tecnologias externas (por exemplo, sem fio, firewalls, DNS, e-mail) são transferidos ou copiados em um servidor de registro interno centralizado ou mídia seguros.			
10.5.5 Usar softwares de monitoramento da integridade dos arquivos ou de detecção de alterações nos registros 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).	**10.5.5** Verifique o uso de softwares de monitoramento da integridade dos arquivos ou de detecção de alterações nos registros ao analisar as configurações do sistema e os arquivos e resultados monitorados das atividades de monitoramento.			
10.6 Analisar os registros de todos os componentes do sistema pelo menos diariamente. As análises dos registros incluem aqueles servidores que desempenham funções de segurança como sistema de detecção de invasões (IDS) e servidores de protocolo de autenticação, autorização e inventário (AAA) (por exemplo, RADIUS). *Observação: As ferramentas de coleta, análise e alerta dos registros podem ser usadas para estar em conformidade com o Requisito 10.6*	**10.6.a** Obtenha e analise as políticas e os procedimentos de segurança para verificar se eles incluem procedimentos para analisar os registros de segurança pelo menos diariamente e se o acompanhamento das exceções é exigido.			
	10.6.b Por meio da observação e de entrevistas, verifique se as análises de registros regulares são realizadas em todos os componentes do sistema.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
10.7 Manter um histórico da trilha de auditoria por pelo menos um ano, com um mínimo de três meses imediatamente disponível para análise (por exemplo, on-line, arquivado ou recuperável a partir do back-up).	**10.7.a** Obtenha e analise as políticas e procedimentos de segurança, e verifique se eles incluem políticas de retenção de registros de auditoria e requerem a retenção dos registros de auditoria por pelo menos um ano.			
	10.7.b Verifique se os registros de auditoria estão disponíveis pelo menos referente ao período de um ano e se há processos implementados para recuperar pelo menos os registros dos últimos três meses para a análise imediata.			

Requisito 11: Testar regularmente os sistemas e processos de segurança.

As vulnerabilidades estão sendo continuamente descobertas por indivíduos mal-intencionados e pesquisadores, e são apresentadas por novos softwares. Os componentes do sistema, processos e softwares personalizados devem ser testados com freqüência para assegurar que os controles de segurança continuem refletindo um ambiente em transformação.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
11.1 Testar a presença de pontos de acesso sem fio usando um analisador sem fio pelo menos trimestralmente ou implementando um IDS/IPS sem fio para identificar todos os dispositivos sem fio que estão sendo usados.	**11.1.a** Verifique se um analisador sem fio é usado pelo menos trimestralmente ou se um IDS/IPS sem fio é implementado e configurado para identificar todos os dispositivos sem fio.			
	11.1.b Se um IDS/IPS sem fio for implementado, verifique se a configuração gerará alertas à equipe.			
	11.1 c Verifique se o Plano de Resposta a Incidentes da empresa (Requisito 12.9) inclui uma resposta no caso de dispositivos sem fio não autorizados serem detectados.			
11.2 Executar digitalizações quanto às 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, upgrades de produtos). *Observação: As digitalizações trimestrais quanto às vulnerabilidades externas devem ser realizadas por um Fornecedor de Digitalizações Aprovado (ASV) qualificado pelo Conselho de Segurança de Dados do Setor de Cartões de Pagamento (PCI SSC) As digitalizações realizadas após as alterações na rede devem ser desempenhadas pela equipe interna da empresa.*	**11.2.a** Inspecione o resultado dos quatro últimos trimestres das digitalizações quanto às vulnerabilidades da rede interna, host e aplicativos para verificar se testes de segurança periódicos dos dispositivos no ambiente de dados do portador do cartão são realizados. Verifique se o processo de digitalização incluem novas digitalizações até que os resultados de aprovação sejam obtidos. *Observação: As digitalizações externas realizadas após as mudanças na rede e as digitalizações internas podem ser desempenhadas pela equipe interna qualificada da empresa ou por terceiros.*			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
	11.2.b Verifique se as digitalizações externas estão ocorrendo trimestralmente de acordo com os Procedimentos de Digitalização de Segurança do PCI ao inspecionar o resultado dos últimos quatro trimestres das digitalizações quanto às vulnerabilidades externas para verificar se: ▪ Quatro digitalizações trimestrais ocorreram no último período de 12 meses; ▪ Os resultados de cada digitalização satisfazem os Procedimentos de Digitalização de Segurança do PCI (por exemplo, nenhuma vulnerabilidade urgente, crítica ou elevada); ▪ As digitalizações foram concluídas por um Fornecedor de Digitalizações Aprovado (ASV) qualificado pelo PCI SSC. *Observação: Não será necessário que quatro digitalizações trimestrais aprovadas sejam concluídas quanto à conformidade inicial do PCI DSS se o avaliador verificar que 1) o resultado da digitalização mais recente foi uma digitalização aprovada, 2) a entidade contar com políticas e procedimentos documentados que requerem a seqüência de digitalizações trimestrais e 3) as vulnerabilidades observadas nos resultados da digitalização tenham sido corrigidas conforme mostrado em uma nova digitalização. Nos anos seguintes após a análise inicial do PCI DSS, quatro digitalizações trimestrais aprovadas devem ter ocorrido.*			
	11.2.c Verifique se as digitalizações internas e/ou externas são realizadas após qualquer mudança significativa na rede ao inspecionar os resultados das digitalizações do ano anterior. Verifique se o processo de digitalização incluem novas digitalizações até que os resultados de aprovação sejam obtidos.			
11.3 Realizar testes de penetração externos e internos pelo menos uma vez por ano e após qualquer upgrade ou modificação significativa na infra-estrutura ou nos aplicativos (como um upgrade no sistema operacional, uma sub-rede adicionada ao ambiente ou um servidor da Web adicionado ao ambiente). Esses testes de penetração devem incluir o seguinte:	**11.3.a** Obtenha e analise os resultados do teste de penetração mais recente para verificar se os testes de penetração são realizados pelo menos uma vez por ano e após quaisquer mudanças significativas no ambiente. Verifique se as vulnerabilidades observadas foram corrigidas e os testes repetidos.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
	11.3.b Verifique se o teste foi realizado por um recurso interno qualificado ou um terceiro externo qualificado e, caso seja aplicável, se há uma independência organizacional do responsável pelo teste (não é necessário que seja um QSA ou ASV).			
11.3.1 Testes de penetração na camada da rede	**11.3.1** Verifique se o teste de penetração inclui testes de penetração na camada da rede. Esses testes devem incluir componentes que são compatíveis com as funções da rede, assim como com os sistemas operacionais.			
11.3.2 Testes de penetração na camada dos aplicativos	**11.3.2** Verifique se o teste de penetração inclui testes de penetração na camada dos aplicativos. Para aplicativos da Web, os testes devem incluir, pelo menos, as vulnerabilidades listadas no Requisito 6.5.			
11.4 Usar sistemas de detecção de invasão e/ou sistemas de prevenção contra invasão para monitorar todo o tráfego no ambiente de dados do portador do cartão e alertar as equipes sobre comprometimentos suspeitos. Manter todos os mecanismos de detecção e prevenção contra invasões atualizados.	**11.4.a** Verifique o uso dos sistemas de detecção e/ou prevenção contra invasões, e se o tráfego no ambiente de dados do portador do cartão é monitorado.			
	11.4.b Confirme se o IDS e/ou IPS estão configurados para alertar as equipes sobre comprometimentos suspeitos.			
	11.4.c Analise as configurações de IDS/IPS e confirme se os dispositivos de IDS/IPS estão configurados, mantidos e atualizados de acordo com as instruções dos fornecedores para assegurar uma proteção ideal.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
11.5 Implementar softwares de monitoramento da integridade dos arquivos para alertar as equipes quanto à modificação não autorizada de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo; e configurar o software para realizar comparações de arquivos críticos pelo menos semanalmente. *Observação: Para fins de monitoramento da integridade dos arquivos, os arquivos críticos normalmente são aqueles que não são alterados com freqüência, mas sua modificação poderia indicar um comprometimento do sistema ou um risco de comprometimento. Normalmente, os produtos de monitoramento da integridade dos arquivos 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).*	**11.5** Verifique o uso de produtos de monitoramento de integridade de arquivos no ambiente de dados do portador do cartão ao observar as configurações do sistema e os arquivos monitorados, assim como ao analisar os resultados das atividades de monitoramento. Exemplos de arquivos que devem ser monitorados: ▪ Executáveis do sistema ▪ Executáveis dos aplicativos ▪ Arquivos de configuração e parâmetro ▪ Arquivos de registro e auditoria centralmente armazenados, históricos ou arquivados			

Manter uma Política de Segurança de Informações

Requisito 12: Manter uma política que aborde a segurança das informações para funcionários e prestadores de serviços.

Uma política de segurança sólida determina o tom da segurança para toda a empresa e informa aos funcionários o que é esperado deles. Todos os funcionários devem estar cientes da confidencialidade dos dados e de suas responsabilidades para protegê-los. Para as finalidades desse requisito, "funcionários" refere-se a funcionários que trabalham em período integral e meio-período, funcionários e equipes temporárias, e prestadores de serviços e consultores que "residem" no endereço da empresa.

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
12.1 Definir, publicar, manter e disseminar uma política de segurança que realize o seguinte:	**12.1** Analise a política de segurança das informações e verifique se a política foi publicada e disseminada a todos os usuários de sistema relevantes (incluindo fornecedores, prestadores de serviços e parceiros comerciais).			
12.1.1 Atende a todos os requisitos do PCI DSS.	**12.1.1** Verifique se a política atende a todos os requisitos do PCI DSS.			
12.1.2 Inclui um processo anual que identifica ameaças e vulnerabilidades, e resulta em uma avaliação de risco formal.	**12.1.2** Verifique se a política de segurança das informações inclui um processo de avaliação de risco anual que identifica ameaças, vulnerabilidades e resulta em uma avaliação de risco formal.			
12.1.3 Inclui uma análise pelo menos uma vez por ano e atualizações quando o ambiente é modificado.	**12.1.3** Verifique se a política de segurança das informações é analisada pelo menos uma vez por ano e atualizada conforme necessário para refletir as alterações nos objetivos de negócios ou no ambiente de risco.			
12.2 Desenvolver procedimentos de segurança operacional diariamente que estejam em conformidade com os requisitos nessa especificação (por exemplo, procedimentos de manutenção da conta do usuário e procedimentos de análise de registros).	**12.2.a** Analise os procedimentos de segurança operacional diariamente. Verifique se eles estão em conformidade com essa especificação e incluem procedimentos administrativos e técnicos para cada um dos requisitos.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
12.3 Desenvolver políticas de utilização para tecnologias críticas voltadas aos funcionários (por exemplo, tecnologias de acesso remoto, tecnologias sem fio, mídia eletrônica removível, laptops, dados pessoais/assistentes digitais (PDAs), uso de e-mail e uso da Internet) para definir o uso adequado dessas tecnologias para todos os funcionários e prestadores de serviços. Assegurar que essas políticas de utilização exijam o seguinte:	**12.3** Obtenha e analise a política de tecnologias críticas voltadas aos funcionários e desempenhe o seguinte:			
12.3.1 Aprovação explícita da gerência	**12.3.1** Verifique se as políticas de utilização exigem a aprovação da gerência para usar as tecnologias.			
12.3.2 Autenticação para o uso da tecnologia	**12.3.2** Verifique se as políticas de utilização exigem que todo o uso da tecnologia seja autenticado com ID de usuário e senha ou outro item de autenticação (por exemplo, token).			
12.3.3 Uma lista de todos esses dispositivos e equipes com acesso	**12.3.3** Verifique se as políticas de utilização exigem uma lista de todos os dispositivos e equipes autorizadas a usar os dispositivos.			
12.3.4 Identificação dos dispositivos com proprietário, informações de contato e finalidade	**12.3.4** Verifique se as políticas de utilização exigem a identificação dos dispositivos com proprietário, informações de contato e finalidade.			
12.3.5 Usos aceitáveis da tecnologia	**12.3.5** Verifique se as políticas de utilização exigem usos aceitáveis quanto à tecnologia.			
12.3.6 Locais de rede aceitáveis quanto às tecnologias	**12.3.6** Verifique se as políticas de utilização exigem locais de rede aceitáveis quanto à tecnologia.			
12.3.7 Lista dos produtos aprovados pela empresa	**12.3.7** Verifique se as políticas de utilização exigem uma lista de produtos aprovados pela empresa.			
12.3.8 Desconexão automática das sessões quanto às tecnologias de acesso remoto após um período específico de inatividade	**12.3.8** Verifique se as políticas de utilização exigem a desconexão automática das sessões quanto às tecnologias de acesso remoto após um período específico de inatividade.			
12.3.9 Ativação das tecnologias de acesso remoto para fornecedores somente quando for necessário por parte dos fornecedores, com uma desativação imediata após o uso	**12.3.9** Verifique se as políticas de utilização exigem a ativação de tecnologias de acesso remoto usadas pelos fornecedores somente quando for necessário por parte dos fornecedores, com uma desativação imediata após o uso.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
12.3.10 Ao acessar os dados do portador do cartão por meio de tecnologias de acesso remoto, proibir a cópia, a transferência e o armazenamento dos dados do portador do cartão em discos rígidos locais e mídias eletrônicas removíveis.	**12.3.10** Verifique se as políticas de utilização proíbem a cópia, a transferência ou o armazenamento dos dados do portador do cartão em discos rígidos locais e mídias eletrônicas removíveis ao acessar esses dados por meio de tecnologias de acesso remotas.			
12.4 Certificar-se de que a política e os procedimentos de segurança definem claramente as responsabilidades quanto à segurança das informações para todos os funcionários e prestadores de serviços.	**12.4** Verifique se as políticas de segurança das informações definem claramente as responsabilidades quanto à segurança das informações para os funcionários e prestadores de serviços.			
12.5 Atribuir um indivíduo ou uma equipe às seguintes responsabilidades de gerenciamento da segurança das informações:	**12.5** Verifique a atribuição formal da segurança das informações com relação a um Responsável pela Segurança ou outro membro do gerenciamento que tenha conhecimento sobre segurança. Obtenha e analise as políticas e procedimentos de segurança das informações para verificar se as seguintes responsabilidades da segurança das informações foram atribuídas de modo específico e formal:			
12.5.1 Definir, documentar e distribuir políticas e procedimentos de segurança.	**12.5.1** Verifique se a responsabilidade pela criação e distribuição de políticas e procedimentos de segurança foi formalmente atribuída.			
12.5.2 Monitorar e analisar os alertas e as informações de segurança, e distribuir para as equipes apropriadas.	**12.5.2** Verifique se a responsabilidade pelo monitoramento e análise dos alertas de segurança, e pela distribuição de informações às equipes de gerenciamento adequadas da segurança das informações e das unidades de negócios foi formalmente atribuída.			
12.5.3 Definir, documentar e distribuir procedimentos de resposta e escalação de incidentes de segurança para assegurar que todas as situações sejam abordadas de modo oportuno e eficiente.	**12.5.3** Verifique se a responsabilidade pela criação e distribuição de procedimentos de resposta e escalação de incidentes segurança foi formalmente atribuída.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
12.5.4 Administrar as contas dos usuários, incluindo adições, exclusões e modificações	**12.5.4** Verifique se a responsabilidade pela administração das contas dos usuários e do gerenciamento da autenticação foi formalmente atribuída.			
12.5.5 Monitorar e controlar todos os acessos aos dados.	**12.5.5** Verifique se a responsabilidade pelo monitoramento e controle de todos os acessos aos dados foi formalmente atribuída.			
12.6 Implementar um programa formal de conscientização da segurança para conscientizar todos os funcionários sobre a importância da segurança dos dados do portador do cartão.	**12.6.a** Verifique a existência de um programa formal de conscientização da segurança para todos os funcionários.			
	12.6.b Obtenha e analise os procedimentos e a documentação do programa de conscientização de segurança, e desempenhe o seguinte:			
12.6.1 Instruir os funcionários quando da contratação e pelo menos uma vez por ano.	**12.6.1.a** Verifique se o programa de conscientização da segurança fornece vários métodos para transmitir a conscientização e instruir os funcionários (por exemplo, cartazes, cartas, memorandos, treinamento baseado na Web, reuniões e promoções).			
	12.6.1.b Verifique se os funcionários participam do treinamento de conscientização quando da contratação e pelo menos uma vez por ano.			
12.6.2 Exigir que os funcionários reconheçam, pelo menos uma vez por ano, que leram e compreenderam a política e os procedimentos de segurança da empresa.	**12.6.2** Verifique se o programa de conscientização da segurança exige que os funcionários reconheçam (por exemplo, por escrito ou eletronicamente), pelo menos uma vez por ano, que leram e compreenderam a política de segurança das informações da empresa.			
12.7 Selecionar funcionários potenciais (veja a definição de "funcionário" no item 9.2 acima) antes da contratação para minimizar o risco de ataques de fontes internas. *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.*	**12.7** Indagar a gerência do departamento dos Recursos Humanos e conferir se as verificações da formação são realizadas (dentro das restrições das leis locais) junto aos funcionários antes de contratar quem terá acesso aos dados do portador do cartão ou ao ambiente desses dados. (Exemplos de verificações da formação incluem o histórico do emprego anterior, ficha criminal, histórico de crédito e verificações das referências.)			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
12.8 Se os dados do portador do cartão forem compartilhados com prestadores de serviços, manter e implementar políticas e procedimentos para gerenciar os prestadores de serviços, incluindo o seguinte:	**12.8** Se a entidade que estiver sendo avaliada compartilhar dados do portador do cartão com prestadores de serviços (por exemplo, áreas de armazenamento de fitas de back-up, prestadores de serviços gerenciados, como empresas de hospedagem na Web ou prestadores de serviços de segurança, ou aqueles que recebem dados para fins de determinação de fraude), analise, por meio da observação, as políticas e procedimentos, além da documentação de suporte, e desempenhe o seguinte:			
12.8.1 Manter uma lista dos prestadores de serviços.	**12.8.1** Verificar se uma lista dos prestadores de serviços é mantida.			
12.8.2 Manter um acordo por escrito que inclua um reconhecimento de que os prestadores de serviços são responsáveis pela segurança dos dados do portador do cartão que eles possuírem.	**12.8.2** Verifique se o acordo por escrito inclui um reconhecimento dos prestadores de serviços quanto à sua responsabilidade pela proteção dos dados do portador do cartão.			
12.8.3 Certificar-se de que haja um processo definido para a contratação dos prestadores de serviços, incluindo uma diligência devida adequada antes da contratação.	**12.8.3** Verifique se as políticas e procedimentos estão documentados e foram seguidos, incluindo a diligência devida adequada antes da contratação de qualquer prestador de serviços.			
12.8.4 Manter um programa para monitorar o status de conformidade quanto ao PCI DSS dos prestadores de serviços.	**12.8.4** Verifique se a entidade avaliada conta com um programa para monitorar o status de conformidade quanto ao PCI DSS dos prestadores de serviços.			
12.9 Implementar um plano de resposta a incidentes. Preparar-se para responder imediatamente a uma falha no sistema.	**12.9** Obtenha e analise o Plano de Resposta a Incidentes e os procedimentos relacionados, e desempenhe o seguinte:			

(o item 12.9 continua na próxima página)

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
12.9.1 Criar o plano de resposta a incidentes a ser implementado no caso de falha no sistema. Certificar-se de que o plano aborda o seguinte, pelo menos: ▪ Funções, responsabilidades e estratégias de comunicação e contato no caso de um comprometimento, incluindo a notifcação às bandeiras de pagamento, pelo menos ▪ Procedimentos de resposta específicos a incidentes ▪ Procedimentos de recuperação e continuidade dos negócios ▪ Processos de back-up dos dados ▪ Análise dos requisitos legais visando ao relato dos comprometimentos ▪ Abrangência e resposta de todos os componentes críticos do sistema ▪ Referência ou inclusão de procedimentos de resposta a incidentes por parte das bandeiras de pagamento	**12.9.1** Verifique se o Plano de Resposta a Incidentes inclui: ▪ Funções, responsabilidades e estratégias de comunicação no caso de um comprometimento, incluindo a notifcação às bandeiras de pagamento, pelo menos ▪ Procedimentos de resposta específicos a incidentes, ▪ Procedimentos de recuperação e continuidade dos negócios, ▪ Processos de back-up dos dados ▪ Análise dos requisitos legais referentes ao relato dos comprometimentos (por exemplo, Lei 1386 da Califórnia, que exige a notificação dos clientes afetados no caso de um comprometimento real ou suspeito para qualquer negócio que seja realizado com moradores da Califórnia em seu banco de dados) ▪ Abrangência e resposta de todos os componentes críticos do sistema ▪ Referência ou inclusão de procedimentos de resposta a incidentes por parte das bandeiras de pagamento			
12.9.2 Testar o plano pelo menos uma vez por ano.	**12.9.2** Verificar se o plano é testado pelo menos uma vez por ano.			
12.9.3 Designar equipes específicas para estarem disponíveis em tempo integral para responder aos alertas.	**12.9.3** Verifique, por meio da observação e da analise das políticas se há uma resposta a incidentes em tempo integral e uma cobertura de monitoramento para qualquer evidência de atividade não autorizada, detecção de pontos de acesso sem fio não autorizados, alertas de IDS críticos e/ou relatórios de sistemas críticos não autorizados ou alterações nos arquivos de conteúdo.			
12.9.4 Fornecer o treinamento adequado à equipe que é responsável pela resposta às falhas do sistema.	**12.9.4** Verifique, por meio da observação e da análise das políticas, se a equipe responsável pelas falhas do sistema é treinada periodicamente.			

Requisitos do PCI DSS	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
12.9.5 Incluir alertas de sistemas de detecção de invasão, prevenção contra invasões e monitoramento da integridade dos arquivos.	**12.9.5** Verifique, por meio da observação e da análise dos processos, se o monitoramento e a resposta aos alertas dos sistemas de segurança, incluindo os pontos de acesso sem fio não autorizados são abordados no Plano de Resposta a Incidentes.			
12.9.6 Desenvolver 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.	**12.9.6** Verifique, por meio da observação e da análise das políticas, se há 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.			

Apêndice A: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada

Requisito A.1: Os provedores de hospedagem compartilhada devem proteger o ambiente de dados do portador do cartão

Conforme mencionado no Requisito 12.8, todos os prestadores de serviços com acesso aos dados do portador do cartão (incluindo os provedores de hospedagem compartilhada) devem seguir o PCI DSS. Além disso, o Requisito 2,4 afirma que os provedores de hospedagem compartilhada devem proteger o ambiente hospedado e os dados de cada entidade. Portanto, os provedores de hospedagem compartilhada também devem estar em conformidade com os requisitos nesse Apêndice.

Requisitos	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
A.1 Proteja o ambiente hospedado e os dados de cada entidade (seja comerciante, prestador de serviços ou outra entidade), de acordo com os itens A.1.1 a A.1.4: Um provedor de hospedagem deve atender a esses requisitos, assim como a todas as outras seções relevantes do PCI DSS. *Observação: Embora um provedor de hospedagem possa atender a esses requisitos, a conformidade da entidade de que utiliza o provedor de hospedagem não é assegurada. Cada entidade* deve *estar em conformidade com o PCI DSS e validar a conformidade, conforme aplicável.*	**A.1** Especificamente para uma avaliação do PCI DSS de um provedor de hospedagem compartilhada, para verificar se os provedores de hospedagem compartilhada protegem o ambiente hospedado e os dados das entidades (comerciantes e prestadores de serviços), selecione um exemplo de servidores (Microsoft Windows e Unix/Linux) dentre vários exemplos representativos de comerciantes e prestadores de serviços, e desempenhe o que está descrito nos itens A.1.1 a A.1.4 abaixo.			
A.1.1 Certificar-se de que cada entidade executa somente os processos que têm acesso aos dados do portador do cartão daquela entidade.	**A.1.1** Se um provedor de hospedagem compartilhada permitir que as entidades (por exemplo, comerciantes ou prestadores de serviços) executem seus próprios aplicativos, verifique se os processos desses aplicativos são executados usando o ID exclusivo da entidade. Por exemplo: ▪ Nenhuma entidade no sistema pode usar um ID de usuário do servidor da Web compartilhado. ▪ Todos os scripts CGI usados por uma entidade devem ser criados e executados como o ID do usuário exclusivo da entidade.			

Requisitos	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
A.1.2 Restringir o acesso e os privilégios de cada entidade somente ao próprio ambiente de dados do portador do cartão.	**A.1.2.a** Verifique se o ID do usuário de qualquer processo de aplicativos não é um usuário privilegiado (raiz/admin).			
	A.1.2.b Verifique se cada entidade (comerciante, prestador de serviços) lei, gravou ou executou as permissões somente referentes aos arquivos e diretórios que possui ou para os arquivos de sistema necessários (restringidos por meio das permissões do sistema de arquivo, listas de controle de acesso, chroot, jailshell, etc.). IMPORTANTE: Os arquivos de uma entidade não podem ser compartilhados em grupo.			
	A.1.2.c Verifique se os usuários da entidade não têm acesso de gravação aos binários compartilhados do sistema.			
	A.1.2.d Verifique se a visualização das entradas de registro é restrita à entidade detentora.			
	A.1.2.e Para assegurar que cada entidade não possa monopolizar os recursos do servidor para explorar as vulnerabilidades (por exemplo, condições de erro, aceleração e reinicialização, resultando, por exemplo, em excessos de buffer), verifique se as restrições foram implementadas para a utilização destes recursos do sistema: ▪ Espaço em disco ▪ Largura de banda ▪ Memória ▪ CPU			
A.1.3 Certificar-se de que os registros e as trilhas de auditoria estão ativadas e são exclusivas para o ambiente de dados do portador do cartão de cada entidade, além de estarem em conformidade com o Requisito 10 do PCI DSS.	**A.1.3.a** Verifique se o provedor de hospedagem compartilhada ativou os registros conforme se segue, para o ambiente de cada comerciante e prestador de serviços: ▪ Os registros são ativados para os aplicativos de terceiros comuns. ▪ Como padrão, os registros estão ativados. ▪ Os registros estão disponíveis para análise pela entidade detentora. ▪ As localizações dos registros são informadas com clareza à entidade detentora.			

Requisitos	Procedimentos de teste	Implementado	Não implementado	Data prevista/ Comentários
A.1.4 Permitir que os processos providenciem uma investigação forense oportuna no caso de um comprometimento em qualquer comerciante ou prestador de serviços hospedado.	**A.1.4** Verifique se o provedor de hospedagem compartilhada definiu políticas que fornecem uma investigação forense oportuna dos servidores relacionados no caso de um comprometimento.			

Apêndice B: Controles de compensação

Os controles de compensação podem ser considerados na maioria dos requisitos do PCI DSS quando uma entidade não for capaz de atender a um requisito de forma explícita, conforme informado, devido à restrições de negócios documentadas ou técnicas legítimas, mas minimizou o risco associado ao requisito de modo suficiente por meio da implementação de outros controles, incluindo os de compensação.

Os controles de compensação devem atender aos seguintes critérios:

1. Atender a intenção e o rigor do requisito original do PCI DSS.
2. Fornecer um nível semelhante de defesa ao requisito original do PCI DSS, como o controle de compensação que contrabalança o risco de modo suficiente para o qual o requisito original do PCI DSS tenha sido criado para fornecer uma defesa. (Consulte a seção *Navegando no PCI DSS* para obter informações sobre a intenção de cada requisito do PCI DSS.)
3. Estar "acima e além" dos outros requisitos do PCI DSS. (Simplesmente estar em conformidade com os requisitos do PCI DSS não é um controle de compensação.)

   Ao utilizar o critério de avaliação "acima e além" para controles de compensação, considere o seguinte:

   Observação: Os itens nas alternativas a) a c) abaixo são apenas exemplos. Todos os controles de compensação devem ser analisados e validados quanto à suficiência pelo responsável pela avaliação que realiza a análise do PCI DSS. A efetividade de um controle de compensação depende das especificidades do ambiente no qual o controle está implementado, dos controles de segurança ao redor e da configuração do controle. As empresas devem estar cientes de que um determinado controle de compensação não será efetivo em todos os ambientes.

   a) Os requisitos existentes do PCI DSS NÃO PODERÃO ser considerados como controles de compensação se já tiverem sido exigidos para o item sob análise. Por exemplo, as senhas para o acesso administrativo não console devem ser enviadas criptografadas para minimizar o risco de interceptação de senhas administrativas em texto simples. Uma entidade não pode usar outros requisitos de senha do PCI DSS (bloqueio contra invasores, senhas complexas, etc.) para compensar a falta de senhas criptografadas, já que esses outros requisitos de senha não minimizam o risco de intercepção de senhas em texto simples. Além disso, os outros controles de senha já são requisitos do PCI DSS referente ao item sob análise (contas).

   b) Os requisitos existentes do PCI DSS PODERÃO ser considerados como controles de compensação se forem exigidos para outra área, mas não para o item sob análise. Por exemplo, uma autenticação com dois fatores é um requisito do PCI DSS para o acesso remoto. A autenticação com dois fatores *a partir da rede interna* também pode ser considerada um controle de compensação para o acesso administrativo não console quando a transmissão de senhas criptografadas não for compatível. A autenticação com dois fatores poderá ser um controle de compensação aceitável se; (1) atender à intenção do requisito original ao abordar o risco de interceptação de senhas administrativas em texto simples; e (2) for configurada de modo adequado e em um ambiente seguro.

   c) Os requisitos existentes do PCI DSS podem ser combinados com novos controles para se tornarem um controle de compensação. Por exemplo, se uma empresa não for capaz de tornar os dados do portador do cartão ilegíveis de acordo com o requisito 3.4 (por exemplo, por meio da criptografia), um controle de compensação poderia consistir em um dispositivo ou uma combinação de dispositivos, aplicativos e controles que abordam todos os itens a seguir: (1) segmentação da rede interna; (2) filtragem de endereço IP ou endereço MAC; e (3) autenticação com dois fatores dentro da rede interna.
4. Ser proporcional ao risco extra imposto pelo não cumprimento do requisito do PCI DSS

O responsável pela avaliação deve analisar os controles de compensação por completo durante cada avaliação anual do PCI DSS para validar se cada controle de compensação aborda adequadamente o risco para o qual o requisito do PCI DSS original foi elaborado, de acordo com os itens 1 a 4 acima. Para manter a conformidade, os processos e controles devem estar implementados para assegurar que os controles de compensação permaneçam efetivos após a conclusão da avaliação.

Apêndice C: Planilha dos controles de compensação

Use esta planilha para definir os controles de compensação para qualquer requisito no qual os controles de compensação são usados para atender a um requisito do PCI DSS. Os controles de compensação também devem ser documentados no Relatório sobre Conformidade na seção do requisito do PCI DSS correspondente.

Observação: *Somente as empresas que realizaram uma análise dos riscos e têm restrições de negócios documentadas ou tecnológicas legítimas podem considerar o uso dos controles de compensação para atingir a conformidade.*

Número e definição do requisito:

	Informações necessárias	Explicação
1. Restrições	Listar as restrições que impossibilitam a conformidade com o requisito original.	
2. Objetivo	Definir o objetivo do controle original; identificar o objetivo atendido pelo controle de compensação.	
3. Risco identificado	Identificar qualquer risco adicional imposto pela ausência do controle original.	
4. Definição dos controles de compensação	Definir os controles de compensação e explique como eles abordam os objetivos do controle original e o aumento dos riscos, caso haja algum.	
5. Validação dos controles de compensação	Definir como os controles de compensação foram validados e testados.	
6. Manutenção	Definir o processo e os controles implementados para manter os controles de compensação.	

Planilha dos controles de compensação – Exemplo completo

Use esta planilha para definir os controles de compensação com relação a qualquer requisito no qual a opção "YES" (Sim) tenha sido assinalada e os controles de compensação tenham sido mencionados na coluna "Especial".

Número do requisito: *8.1—Todos os usuários são identificados com um nome de usuário exclusivo antes de permitir que eles acessem os componentes do sistema ou os dados do portador do cartão?*

	Informações necessárias	Explicação
1. Restrições	Listar as restrições que impossibilitam a conformidade com o requisito original.	*A empresa XYZ utiliza Servidores Unix independentes sem LDAP. Sendo assim, cada um deles requer um login "raiz". A empresa XYZ não pode gerenciar o login "raiz" nem é possível registrar todas as atividades "raiz" por usuário.*
2. Objetivo	Definir o objetivo do controle original; identificar o objetivo atendido pelo controle de compensação.	*O objetivo de exigir logins exclusivos é duplo. Primeiro, não é considerado aceitável, da perspectiva de segurança, compartilhar credenciais de login. Segundo, ter logins compartilhados impossibilita afirmar em definitivo quem é responsável por uma determinada ação.*
3. Risco identificado	Identificar qualquer risco adicional imposto pela ausência do controle original.	*O risco adicional ocorre no sistema de controle de acesso ao não assegurar que todos os usuários tenham um ID exclusivo e possam ser monitorados.*
4. Definição dos controles de compensação	Definir os controles de compensação e explique como eles abordam os objetivos do controle original e o aumento dos riscos, caso haja algum.	*A empresa XYZ solicitará que todos os usuários efetuem login nos servidores a partir dos seus desktops usando o comando SU. Esse comando permite que um usuário acesse a conta "raiz" e desempenhe ações na conta "raiz", mas possa efetuar login no diretório de registro do SU. Nesse caso, as ações de cada usuário podem ser monitoradas por meio da conta do SU.*
5. Validação dos controles de compensação	Definir como os controles de compensação foram validados e testados.	*A empresa XYZ demonstra ao responsável pela avaliação o comando SU que está sendo executado e se as pessoas que estão usando o comando efetuaram login para identificar que se o indivíduo está desempenhando ações com privilégios raiz.*
6. Manutenção	Definir o processo e os controles implementados para manter os controles de compensação.	*A empresa XYZ documenta os processos e procedimentos para assegurar que as configurações do SU não sejam modificadas, alteradas ou removidas para permitir que os usuários individuais executem comandos raiz sem serem monitorados ou efetuarem login individualmente.*

Apêndice D: Atestado de conformidade – Comerciantes

Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI)

Atestado de conformidade para avaliações in loco – Comerciantes

Versão 1.2

Outubro de 2008

Instruções para envio

Este documento deve ser preenchido por um Responsável pela Avaliação da Segurança Qualificado (QSA) ou comerciante (se a auditoria interna do comerciante realizar a validação) como uma declaração do status de conformidade do comerciante com o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS). Preencha todas as seções aplicáveis e envie ao adquirente ou à bandeira de pagamento solicitante.

Parte 1. Informações sobre a empresa do responsável pela avaliação da segurança qualificado

Nome da empresa:					
Nome do PA-QSA líder:			Cargo:		
Telefone:			E-mail:		
Endereço comercial:			Cidade:		
Estado/Província:		País:		CEP:	
URL:					

Parte 2. Informações sobre a organização do comerciante

Nome da empresa:			DBA(s):		
Contato:			Cargo:		
Telefone:			E-mail:		
Endereço comercial:			Cidade:		
Estado/Província:		País:		CEP:	
URL:					

Parte 2a. Tipo de negócio do comerciante (assinale todas as alternativas que se aplicam)

☐ Varejista ☐ Telecomunicação ☐ Gêneros alimentícios e Supermercados

☐ Petróleo ☐ E-Commerce ☐ Pedidos por correspondência/telefone

☐ Viagem e entretenimento ☐ Outros (especificar):

Listar as áreas e locais incluídos na análise do PCI DSS:

Parte 2b. Relações

Sua empresa se relaciona com um ou mais agentes de terceiros (por exemplo, gateways, empresas de hospedagem na Web, agentes de passagens aéreas, agentes de programas de fidelidade, etc)? ☐ Sim ☐ Não

Sua empresa se relaciona com mais de um adquirente? ☐ Sim ☐ Não

Parte 2c. Processamento das transações

Aplicativo de pagamento sendo usado: Versão do aplicativo de pagamento:

Parte 3. Validação do PCI DSS

Com base nos resultados observados no Relatório de Conformidade ("ROC") datado *(date of ROC)*, *(QSA Name/Merchant Name)* afirme o status de conformidade a seguir com relação à entidade identificada na Parte 2 desse documento com *(date)* (assinale uma):

☐ **Em conformidade:** Todos os requisitos no ROC são considerados "implementados[4]" e uma digitalização aprovada foi concluída pelo Fornecedor de Digitalizações Aprovado do PCI SSC, *(ASV Name)* portanto *(Merchant Company Name)* foi demonstrada a total conformidade com o PCI DSS *(insert version number)*.

☐ **Não conformidade:** Alguns requisitos no ROC são considerados "não implementados", resultando em uma avaliação geral **NÃO CONFORMIDADE ou** uma digitalização aprovada não foi concluída por um Fornecedor de Digitalizações Aprovado do PCI SCC, portanto *(Merchant Company Name)* a conformidade total com o PCI DSS não foi demonstrada.

Data prevista quanto à conformidade:

Uma entidade que estiver enviando esse formulário com um status de Não Conformidade talvez tenha de preencher o Plano de Ação na Parte 4 desse documento. *Verifique junto ao seu adquirente ou à(s) bandeira(s) de pagamento antes de preencher a Parte 4, já que nem todas as bandeiras de pagamento exigem essa seção.*

Parte 3a. Confirmação do status em conformidade

Confirmações do QSA/Comerciante:

☐	O ROC foi preenchido de acordo com os *Requisitos do PCI DSS e os Procedimentos da Avaliação de Segurança*, Versão *(insert version number)* e as instruções nesse documento.
☐	Todas as informações contidas no ROC mencionado anteriormente e neste atestado representam adequadamente os resultados desta avaliação em todos os aspectos materiais.
☐	O comerciante confirmou junto ao fornecedor do aplicativo de pagamento que seu aplicativo de pagamento não armazena dados de autenticação confidenciais após a autorização.
☐	O comerciante leu o PCI DSS e reconhece que sempre deve manter a total conformidade com o PCI DSS.
☐	Não há evidências de armazenamento de dados da tarja magnética (ou seja, rastro)[5], dados de CAV2, CVC2, CID ou CVV2[6], ou dados de PIN[7] depois que a autorização da transação foi localizada em QUAISQUER sistemas analisados durante essa avaliação.

Parte 3b. Reconhecimentos do QSA e do comerciante

Assinatura do QSA líder ↑	***Data:***
Nome do QSA líder:	***Cargo:***

Assinatura do responsável executivo pelo comerciante ↑	***Data:***
Nome do responsável executivo pelo comerciante:	***Cargo:***

[4] Os resultados "implementados" devem incluir os controles de compensação analisados pelo QSA/Auditoria interna do comerciante. Se os controles de compensação forem considerados como suficientes na minimização do risco associado ao requisito, o QSA deve assinalar o requisito como "implementado".

[5] Dados codificados na tarja magnética utilizados para autorização durante a transação com o cartão. As entidades não podem reter esses dados após a autorização da transação. Os únicos elementos dos dados de rastreamento que podem ser retidos são o número da conta, a data de vencimento e o nome.

[6] O valor de três ou quatro dígitos impresso no painel de assinatura ou na frente do cartão de pagamento usado para verificar transações virtuais com o cartão.

[7] Número de identificação pessoal inserido pelo portador do cartão durante uma transação com o cartão e/ou bloqueio de PIN criptografado dentro da mensagem da transação.

Parte 4 Plano de ação referente ao status de não conformidade

Selecione o "Status de conformidade" adequado para cada requisito. Se você responder "Não" a qualquer um dos requisitos, será solicitado que a data na qual a empresa estará em conformidade seja fornecida além do requisito e de uma descrição resumida das ações que estão sendo realizadas para atender ao requisito. *Verifique junto ao seu adquirente ou à(s) bandeira(s) de pagamento antes de preencher a Parte 4, já que nem todas as bandeiras de pagamento exigem essa seção.*

Requisito do PCI	Descrição	Status de conformidade (Selecione um)	Data e ações para solucionar (se o Status de conformidade for "Não")
1	Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão.	☐ Sim ☐ Não	
2	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança	☐ Sim ☐ Não	
3	Proteger os dados armazenados do portador do cartão.	☐ Sim ☐ Não	
4	Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas.	☐ Sim ☐ Não	
5	Usar e atualizar regularmente o software antivírus.	☐ Sim ☐ Não	
6	Desenvolver e manter sistemas e aplicativos seguros.	☐ Sim ☐ Não	
7	Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios.	☐ Sim ☐ Não	
8	Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador.	☐ Sim ☐ Não	
9	Restringir o acesso físico aos dados do portador do cartão.	☐ Sim ☐ Não	
10	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão.	☐ Sim ☐ Não	
11	Testar regularmente os sistemas e processos de segurança.	☐ Sim ☐ Não	
12	Manter uma política que aborde a segurança das informações.	☐ Sim ☐ Não	

Apêndice E: Atestado de conformidade – Prestadores de serviços

Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI)

Atestado de conformidade para avaliações in loco – Prestadores de serviços

Versão 1.2

Outubro de 2008

Instruções para envio

O Responsável pela Avaliação da Segurança Qualificado (QSA) e o Prestador de serviços devem preencher este documento como uma declaração do status de conformidade do Prestador de serviços com o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS). Preencha todas as seções aplicáveis e envie à bandeira de pagamento solicitante.

Parte 1. Informações sobre a empresa do responsável pela avaliação da segurança qualificado					
Nome da empresa:					
Nome do PA-QSA líder:			Cargo:		
Telefone:			E-mail:		
Endereço comercial:			Cidade:		
Estado/Província:		País:		CEP:	
URL:					

Parte 2. Informações sobre a organização do prestador de serviços					
Nome da empresa:			DBA(s):		
Contato:			Cargo:		
Telefone:			E-mail:		
Endereço comercial:			Cidade:		
Estado/Província:		País:		CEP:	
URL:					

Parte 2a. Serviços fornecidos (assinale todos os que se aplicam)

☐ Autorização	☐ Programas de fidelidade	☐ Servidor de Controle de Acesso Seguro 3D
☐ Comutação	☐ IPSP (E-commerce)	☐ Processar transações com tarja magnética
☐ Gateway de pagamentos	☐ Exclusão e definição	☐ Processar transações MO/TO
☐ Hospedagem	☐ Processamento de emissões	☐ Outros (especificar):

Listar as áreas e locais incluídos na análise do PCI DSS:

Parte 2b. Relações

Sua empresa se relaciona com um ou mais prestadores de serviços de terceiros (por exemplo, gateways, empresas de hospedagem na Web, agentes de passagens aéreas, agentes de programas de fidelidade, etc)?
☐ Sim ☐ Não

Parte 2c. Processamento das transações

Como e em qual capacidade seu negócio armazena, processa e/ou transmite dados do portador do cartão?

Aplicativo de pagamento sendo usado: *Versão do aplicativo de pagamento:*

Parte 3. Validação do PCI DSS

Com base nos resultados observados no Relatório de Conformidade ("ROC") datado *(date of ROC)*, *(QSA Name)* afirme o status de conformidade a seguir com relação à entidade identificada na Parte 2 desse documento com *(date)* (assinale uma):

☐ **Em conformidade:** Todos os requisitos no ROC são considerados "implementados[8]" e uma digitalização aprovada foi concluída pelo Fornecedor de Digitalizações Aprovado do PCI SSC, *(ASV Name)* portanto *(Service Provider Name)* foi demonstrada a total conformidade com o PCI DSS *(insert version number)*.

☐ **Não conformidade:** Alguns requisitos no ROC são considerados "não implementados", resultando em uma avaliação geral **NÃO CONFORMIDADE ou** uma digitalização aprovada não foi concluída por um Fornecedor de Digitalizações Aprovado do PCI SCC, portanto *(Service Provider Name)* a conformidade total com o PCI DSS não foi demonstrada.

Data prevista quanto à conformidade:

Uma entidade que estiver enviando esse formulário com um status de Não Conformidade talvez tenha de preencher o Plano de Ação na Parte 4 desse documento. *Verifique junto à(s) bandeira(s) de pagamento antes de preencher a Parte 4, já que nem todas as bandeiras de pagamento exigem essa seção.*

Parte 3a. Confirmação do status em conformidade

Confirmação do QSA e do prestador de serviços:

☐	O ROC foi preenchido de acordo com os *Requisitos do PCI DSS e os Procedimentos da Avaliação de Segurança*, Versão *(insert version number)* e as instruções nesse documento.
☐	Todas as informações contidas no ROC mencionado anteriormente e neste atestado representam adequadamente os resultados desta avaliação em todos os aspectos materiais.
☐	O prestador de serviços leu o PCI DSS e reconhece que sempre deve manter a total conformidade com o PCI DSS.
☐	Não há evidências de armazenamento de dados da tarja magnética (ou seja, rastro)[9], dados de CAV2, CVC2, CID ou CVV2[10], ou dados de PIN[11] depois que a autorização da transação foi localizada em QUAISQUER sistemas analisados durante essa avaliação.

Parte 3b. Reconhecimentos do QSA e do prestador de serviços

Assinatura do QSA líder ↑	***Data:***
Nome do QSA líder:	***Cargo:***

Assinatura do responsável executivo pelo prestador de serviços ↑	***Data:***
Nome do responsável executivo pelo prestador de serviços:	***Cargo:***

[8] Os resultados "implementados" devem incluir os controles de compensação analisados pelo QSA. Se os controles de compensação forem considerados como suficientes na minimização do risco associado ao requisito, o QSA deve assinalar o requisito como "implementado".

[9] Dados codificados na tarja magnética utilizados para autorização durante a transação com o cartão. As entidades não podem reter esses dados após a autorização da transação. Os únicos elementos dos dados de rastreamento que podem ser retidos são o número da conta, a data de vencimento e o nome.

[10] O valor de três ou quatro dígitos impresso no painel de assinatura ou na frente do cartão de pagamento usado para verificar transações virtuais com o cartão.

[11] Número de identificação pessoal inserido pelo portador do cartão durante uma transação com o cartão e/ou bloqueio de PIN criptografado dentro da mensagem da transação.

Parte 4 Plano de ação referente ao status de não conformidade

Selecione o "Status de conformidade" adequado para cada requisito. Se você responder "Não" a qualquer um dos requisitos, será solicitado que a data na qual a empresa estará em conformidade seja fornecida além do requisito e de uma descrição resumida das ações que estão sendo realizadas para atender ao requisito. *Verifique junto à(s) bandeira(s) de pagamento antes de preencher a Parte 4, já que nem todas as bandeiras de pagamento exigem essa seção.*

Requisito do PCI	Descrição	Status de conformidade (Selecione um)	Data e ações para solucionar (se o Status de conformidade for "Não")
1	Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão.	☐ Sim ☐ Não	
2	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança	☐ Sim ☐ Não	
3	Proteger os dados armazenados do portador do cartão.	☐ Sim ☐ Não	
4	Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas.	☐ Sim ☐ Não	
5	Usar e atualizar regularmente o software antivírus.	☐ Sim ☐ Não	
6	Desenvolver e manter sistemas e aplicativos seguros.	☐ Sim ☐ Não	
7	Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios.	☐ Sim ☐ Não	
8	Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador.	☐ Sim ☐ Não	
9	Restringir o acesso físico aos dados do portador do cartão.	☐ Sim ☐ Não	
10	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão.	☐ Sim ☐ Não	
11	Testar regularmente os sistemas e processos de segurança.	☐ Sim ☐ Não	
12	Manter uma política que aborde a segurança das informações.	☐ Sim ☐ Não	

Apêndice F: Análises do PCI DSS — Abordando e Selecionando Exemplos