

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

Questionário de auto-avaliação B e Atestado de conformidade

**Somente máquinas de carbono ou terminais de
discagem independentes, sem armazenamento
eletrônico dos dados do portador do cartão**

Versão 1.2

Outubro de 2008

Alterações no documento

Data	Versão	Descrição
1 de outubro de 2008	1.2	Alinhar o conteúdo com o novo PCI DSS v1.2 e implementar pequenas alterações observadas desde o original v1.1.

Índice

Alterações no documento	i
Padrão de segurança de dados do PCI: documentos relacionados.....	iii
Antes de você começar	iv
Preenchendo o questionário de auto-avaliação.....	iv
Conformidade do PCI DSS – Etapas de preenchimento	iv
Orientação para não aplicabilidade de determinados requisitos específicos.....	iv
Atestado de conformidade, SAQ B.....	1
Questionário de auto-avaliação B.....	5
Proteger os dados do portador do cartão.....	5
<i>Requisito 3: Proteger os dados armazenados do portador do cartão</i>	<i>5</i>
<i>Requisito 4: Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas</i>	<i>6</i>
Implementar medidas de controle de acesso rigorosas.....	7
<i>Requisito 7: Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios</i>	<i>7</i>
<i>Requisito 9: Restringir o acesso físico aos dados do portador do cartão.....</i>	<i>7</i>
Manter uma Política de Segurança de Informações.....	8
<i>Requisito 12: Manter uma política que aborde a segurança das informações para funcionários e prestadores de serviços.....</i>	<i>8</i>
Anexo A: (não utilizado)	9
Anexo B: Controles de compensação.....	10
Anexo C: Planilha dos controles de compensação	11
Planilha dos controles de compensação – Exemplo preenchido	12
Anexo D: Explicação de não aplicabilidade.....	13

Padrão de segurança de dados do PCI: documentos relacionados

Os documentos a seguir foram criados para auxiliar comerciantes e prestadores de serviço a entenderem o Padrão de segurança de dados do PCI e o SAQ do PCI DSS.

Documento	Público
<i>Requisitos dos Padrões de Segurança de Dados do PCI e Procedimentos de Avaliação da Segurança</i>	Todos os comerciantes e prestadores de serviço
<i>Navegando pelo PCI DSS: Entendendo o porquê dos requisitos</i>	Todos os comerciantes e prestadores de serviço
<i>Padrão de segurança de dados do PCI: Diretrizes e instruções de auto-avaliação</i>	Todos os comerciantes e prestadores de serviço
<i>Padrão de segurança de dados do PCI: Questionário A de auto-avaliação e atestado</i>	Comerciantes ¹
<i>Padrão de segurança de dados do PCI: Questionário B de auto-avaliação e atestado</i>	Comerciantes ¹
<i>Padrão de segurança de dados do PCI: Questionário C de auto-avaliação e atestado</i>	Comerciantes ¹
<i>Padrão de segurança de dados do PCI: Questionário D de auto-avaliação e atestado</i>	Comerciantes ¹ e todos os prestadores de serviço
<i>Glossário de termos, abreviações e acrônimos do Padrão de segurança de dados do PCI e do Padrão de segurança de dados de aplicativos de pagamento</i>	Todos os comerciantes e prestadores de serviço

¹ Para determinar o Questionário de auto-avaliação adequado, veja *Padrão de segurança de dados do PCI: Diretrizes e instruções de auto-avaliação*, "Selecionando o SAQ e certificado que melhor se aplica à sua organização".

Antes de você começar

Preenchendo o questionário de auto-avaliação

O SAQ B foi desenvolvido para abordar requisitos aplicáveis aos comerciantes que processam os dados do portador do cartão somente em máquinas de carbono ou terminais de discagem independentes.

Esses comerciantes são definidos como Tipo de validação 2 e 3 do SAQ, aqui e no documento *Diretrizes e instruções do Questionário de auto-avaliação do PCI DSS*. Os comerciantes do Tipo de validação 2 do SAQ só processam os dados do portador do cartão por máquinas de carbono. Os comerciantes do Tipo de validação 3 do SAQ só processam os dados do portador do cartão por terminais de discagem independentes. Esses dois tipos de comerciantes podem ser do tipo real (cartão presente) ou comércio eletrônico ou pedidos por correio/telefone (cartão não presente). Esses comerciantes devem validar a conformidade ao preencherem o SAQ B e o Atestado de conformidade associado, confirmando que:

Para o Tipo de validação 2:

- Sua empresa usa somente máquinas de carbono;
- Sua empresa não transmite os dados do portador do cartão por linha telefônica nem por Internet;
- Sua empresa retenha somente relatórios ou cópias em papel dos recibos; e
- Sua empresa não armazene dados do portador do cartão em formato eletrônico.

Para o Tipo de validação 3:

- Sua empresa use somente terminais de discagem independentes (conectados por uma linha telefônica ao processador);
- Seus terminais de discagem independentes não estão conectados a outros sistemas nem à Internet;
- Sua empresa retenha somente relatórios ou cópias em papel dos recibos; e
- Sua empresa não armazene dados do portador do cartão em formato eletrônico.

Cada seção deste questionário se concentra em uma área específica de segurança, com base nas exigências do Padrão de segurança de dados do PCI.

Conformidade do PCI DSS – Etapas de preenchimento

1. Preencha o Questionário de auto-avaliação (SAQ B) segundo as instruções do arquivo *Diretrizes e instruções do Questionário de auto-avaliação do PCI DSS*.
2. Preencha integralmente o Atestado de conformidade.
3. Envie o SAQ e o Atestado de conformidade, junto com as outras documentações solicitadas, para seu adquirente.

Orientação para não aplicabilidade de determinados requisitos específicos

Não aplicabilidade: Requisitos considerados não aplicáveis ao seu ambiente deverão ser indicados com “N/A” na coluna “Especial” do SAQ. Da mesma forma, preencha a planilha “Explicação de não aplicabilidade”, no Anexo, para cada entrada “N/A”.

Atestado de conformidade, SAQ B

Instruções para envio

O comerciante deve preencher este Atestado de conformidade como uma declaração do status de conformidade dele com os *Requisitos dos Padrões de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) e Procedimentos de Avaliação da Segurança*. Preencha todas as seções aplicáveis e consulte as instruções de envio em Conformidade do PCI DSS – Etapas de preenchimento, neste documento.

Parte 1. Informações sobre a empresa do responsável pela avaliação da segurança qualificado (se aplicável)

Nome da empresa:					
Nome do PA-QSA líder:		Forma de tratamento:			
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:		Forma de tratamento:			
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
 Telecomunicações
 Gêneros alimentícios e Supermercados
 Petróleo
 E-Commerce
 Pedidos por correspondência/telefone
 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

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 2d. Qualificação para preencher o SAQ B

O comerciante certifica a qualificação de preenchimento desta versão abreviada do Questionário de auto-avaliação porque:

<input type="checkbox"/>	A. ou	O comerciante só usa máquinas de carbono para ficar com as informações do cartão de pagamento do cliente e não transmite os dados por linha telefônica ou pela Internet;
<input type="checkbox"/>	B.	O comerciante só usa terminais de discagem independentes, que não estão conectados à Internet nem a outros sistemas dentro do ambiente do comerciante;
<input type="checkbox"/>	O comerciante não armazena dados do portador do cartão em formato eletrônico; e	
<input type="checkbox"/>	Se o Comerciante não armazenar os dados do portador do cartão, esses dados só estarão em registros de papel ou cópias de recibos em papel, e não será recebido em formato eletrônico.	

Parte 3. Validação do PCI DSS

Com base nos resultados observados no SAQ B datado de (*data do preenchimento*), o estabelecimento (*nome da empresa do comerciante*) confirma o seguinte estado de conformidade (marque uma opção):

- Em conformidade:** Todas as seções do PCI SAQ estão preenchidas, e todas as perguntas foram respondidas afirmativamente, resultando em uma classificação geral de **CONFORME**, e por isso o estabelecimento (*nome da empresa do comerciante*) demonstrou conformidade integral para com o PCI DSS.
- Não conforme:** Nem todas as seções do PCI SAQ estão preenchidas, ou algumas as perguntas foram respondidas negativamente, resultando em uma classificação geral de **NÃO CONFORME**, e por isso o estabelecimento (*nome da empresa do comerciante*) não demonstrou conformidade integral para com o PCI DSS.

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 com seu adquirente ou com a(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

O comerciante confirma que:

<input type="checkbox"/>	O Questionário de auto-avaliação B do PCI DSS, Versão (<i>versão do SAQ</i>), foi preenchido segundo as instruções nele contidas.
<input type="checkbox"/>	Todas as informações contidas no SAQ mencionado anteriormente e neste atestado representam adequadamente os resultados de minha avaliação.
<input type="checkbox"/>	Eu confirmei com meu fornecedor do aplicativo de pagamento o aplicativo não armazena dados de autenticação confidenciais após a autorização.
<input type="checkbox"/>	Eu li o PCI DSS e reconheço que sempre devo manter a total conformidade total com o PCI DSS.
<input type="checkbox"/>	Não há evidências de armazenamento de dados ² da tarja magnética (ou seja, rastro), dados ³ de CAV2, CVC2, CID ou CVV2, ou dados ⁴ de PIN depois que a autorização da transação foi localizada em QUAISQUER sistemas analisados durante essa avaliação.

² Dados codificados na fita 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 rastro que podem ser retidos são o número da conta, a data de vencimento e o nome.

³ O valor de três ou quatro dígitos impressos à direita do painel de assinatura ou na frente do cartão de pagamento usado para verificar transações com cartão não presente.

⁴ 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 3b. Confirmação do comerciante

<i>Assinatura do responsável executivo pelo comerciante</i> ↑	<i>Data</i> ↑
<i>Nome do responsável executivo pelo comerciante</i> ↑	<i>Forma de tratamento</i> ↑
<i>Empresa do comerciante representada</i> ↑	

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 com seu adquirente ou com a(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 DSS	Descrição do requisito	Status de conformidade (Selecione um)		Data e ações para solucionar (se o Status de conformidade for "NÃO")
		SIM	NÃO	
3	Proteger os dados armazenados do portador do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
4	Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restringir o acesso físico aos dados do portador do cartão	<input type="checkbox"/>	<input type="checkbox"/>	
12	Manter uma política que aborde a segurança das informações	<input type="checkbox"/>	<input type="checkbox"/>	

Questionário de auto-avaliação B

Data de preenchimento:

Proteger os dados do portador do cartão

Requisito 3: Proteger os dados armazenados do portador do cartão

Pergunta	Resposta:	Sim	Não	Especial*
3.2	Todos os sistemas cumprem os seguintes requisitos em relação ao armazenamento de dados de autenticação confidenciais após a autorização (mesmo se criptografados)?	<input type="checkbox"/>	<input type="checkbox"/>	
3.2.1	<p>Não armazenar o conteúdo completo de qualquer rastro da tarja magnética (localizada na parte posterior do cartão, em um chip ou outro local). Esses dados também são denominados como rastro completo, rastro, rastro 1, rastro 2 e dados da tarja magnética.</p> <p><i>No curso normal dos negócios, os seguintes elementos de dados da tarja magnética talvez precisem ser retidos:</i></p> <ul style="list-style-type: none"> ▪ O nome do portador do cartão, ▪ O número da conta principal (PAN), ▪ A data de vencimento e ▪ O código de serviço <p><i>Para minimizar o risco, armazene somente os elementos de dados conforme necessário para os negócios. NUNCA armazene códigos ou valores de verificação do cartão ou elementos de dados de valor de verificação do PIN.</i></p> <p><i>Observação: Veja Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS para obter mais informações</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2	<p>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.</p> <p><i>Observação: Veja Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS para obter mais informações.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3	Não armazenar o PIN (<i>personal identification number</i>) ou o bloco de PIN criptografado.	<input type="checkbox"/>	<input type="checkbox"/>	
3.3	<p>O PAN é mascarado quando exibido? Os seis primeiros e os quatro últimos dígitos são o número máximo de dígitos a serem exibidos.</p> <p><i>Observações:</i></p> <ul style="list-style-type: none"> ▪ <i>Esse requisito não se aplica aos funcionários e outras partes interessadas que precisam visualizar o PAN completo.</i> ▪ <i>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.</i> 	<input type="checkbox"/>	<input type="checkbox"/>	

* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

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

Pergunta		Resposta:	<u>Sim</u>	<u>Não</u>	<u>Especial*</u>
4.2	Estão implementados procedimentos, políticas e práticas para evitar o envio de PANs não criptografados por tecnologias de mensagem do usuário final (como e-mail, mensagens instantâneas, chat)?		<input type="checkbox"/>	<input type="checkbox"/>	

* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

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

Pergunta	Resposta:	Sim	Não	Especial*
7.1 O acesso aos componentes do sistema e aos dados do portador do cartão somente àquelas pessoas cuja função requer tal acesso?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Pergunta	Resposta:	Sim	Não	Especial*
9.6 Todos os documentos impressos e as mídias eletrônicas que contêm dados do portador do cartão estão protegidos fisicamente?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7 (a) É mantido um controle rigoroso quanto à distribuição interna ou externa de qualquer tipo de mídia que contenha dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	
(b) Os controles incluem o seguinte:				
9.7.1 A mídia está classificada para que possa ser identificada como confidencial?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2 A mídia foi enviada via mensageiro seguro ou outro método de entrega que possa ser monitorado com precisão?		<input type="checkbox"/>	<input type="checkbox"/>	
9.8 Existem processos e procedimentos para garantir que a aprovação da gestão seja obtida antes de transferir toda e qualquer mídia contendo dados do portador do cartão de uma área protegida (especialmente quando a mídia for distribuída a pessoas físicas)?		<input type="checkbox"/>	<input type="checkbox"/>	
9.9 É mantido um controle rigoroso sobre o armazenamento e a acessibilidade das mídias que contêm dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10 A mídia que contém os dados do portador do cartão é destruída quando ela não é mais necessária por razões corporativas ou legais? A destruição deve ser da seguinte forma:		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.1 Os materiais impressos são fragmentados, incinerados ou reciclados, de forma que os dados do portador do cartão não possam ser reconstruídos?		<input type="checkbox"/>	<input type="checkbox"/>	

* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Manter uma Política de Segurança de Informações

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

Pergunta		Resposta:	Sim	Não	Especial*
12.1	Existe uma política de segurança estabelecida, publicada, mantida e disseminada? E ela cumpre com os itens a seguir?		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Inclui uma análise pelo menos uma vez por ano e atualizações quando o ambiente é modificado?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) Políticas de utilização para tecnologias críticas voltadas aos funcionários (por exemplo, tecnologias de acesso remoto, tecnologias wireless, mídia eletrônica removível, laptops, dados pessoais/assistentes digitais (PDAs), uso de e-mail e uso da Internet) foram desenvolvidas para definir o uso adequado dessas tecnologias para todos os funcionários e prestadores de serviços?		<input type="checkbox"/>	<input type="checkbox"/>	
12.4	A política e os procedimentos de segurança definem claramente as responsabilidades quanto à segurança das informações para todos os funcionários e prestadores de serviços?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5	As seguintes responsabilidades do gerenciamento da segurança da informação estão atribuídas a uma pessoa ou equipe?				
12.5.3	Definição, documentação e distribuição dos procedimentos de resposta e escalção de incidentes de segurança para assegurar que todas as situações sejam abordadas de modo oportuno e eficiente?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6	Foi implementado um programa formal de conscientização da segurança para conscientizar todos os funcionários sobre a importância da segurança dos dados do portador do cartão?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8	Se os dados do portador do cartão forem compartilhados com provedores de serviço, existem políticas e procedimentos mantidos e implementados para gerenciar prestadores de serviço? E essas políticas e procedimentos incluem os itens a seguir?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.1	É mantida uma lista de prestadores de serviço.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	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 possuem.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Deve haver um processo definido para a contratação dos prestadores de serviços, incluindo uma <i>due diligence</i> adequada antes da contratação.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	É mantido um programa para monitorar o status de conformidade quanto ao PCI DSS dos prestadores de serviços.		<input type="checkbox"/>	<input type="checkbox"/>	

* “Não aplicável” (N/A) ou “Controle de compensação utilizado”. As organizações que usarem essa seção deverão preencher a Planilha dos controles de compensação ou a planilha Explicação de não aplicabilidade, conforme adequado, no Anexo.

Anexo A: (não utilizado)

Esta página foi deixada em branco intencionalmente.

Anexo 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 a 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 interceptação 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 poderá 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 de um dispositivo ou uma combinação de dispositivos, aplicativos e controles que abordam todos os itens a seguir: (1) segmentação da rede interna; (2) filtragem do endereço de IP ou endereço MAC; e (3) autenticação com dois fatores dentro da rede interna.
4. Ser proporcional ao risco adicional 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.

Anexo C: Planilha dos controles de compensação

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".

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 preenchido

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.	<i>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.</i>
2. Objetivo	Definir o objetivo do controle original; identificar o objetivo atendido pelo controle de compensação.	<i>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.</i>
3. Risco identificado	Identificar qualquer risco adicional imposto pela ausência do controle original.	<i>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.</i>
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.	<i>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.</i>
7. Validação dos controles de compensação	Definir como os controles de compensação foram validados e testados.	<i>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.</i>
8. Manutenção	Definir o processo e os controles implementados para manter os controles de compensação.	<i>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 efetuem login individualmente.</i>

