INFORMAÇÃO COMPLEMENTAR

PCI DSS v4.x: Diretrizes para os Controles de Compensação e Abordagem Personalizada

Versão: 1.0
Data: Junho de 2026
Autor: PCI Security Standards Council

Alterações no Documento

Data	Versão	Descrição
Junho de 2026	1.0	Publicação inicial

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

Índice

Visão Geral

O Payment Card Industry Data Security Standard (PCI DSS) oferece flexibilidade na forma como os objetivos de segurança são atendidos. O PCI DSS v4.x inclui duas abordagens para implementar e validar os controles do PCI DSS: a abordagem definida e a abordagem personalizada. Essas duas abordagens diferem em propósito, elementos, documentação e validação.

Este documento destaca cada abordagem e:

- Aborda o papel das entidades avaliadas
- Aborda o papel dos assessores associados; e
- Fornece documentação para essas abordagens e respostas às perguntas mais frequentes.

Para as entidades avaliadas, este documento inclui exemplos preenchidos de:

- Uma Planilha de Controles de Compensação;
- Uma Matriz de Controles para uma Abordagem Personalizada; e
- Uma Análise de Risco Direcionada para a Abordagem Personalizada.

Para os assessores, este documento inclui um exemplo preenchido de um Relatório de Conformidade — Modelo da Abordagem Personalizada do Apêndice E.

Público-Alvo e Objetivo

Este documento destina-se ao uso por todas as entidades que desenvolvem, operam, gerenciam ou avaliam controles de compensação ou uma abordagem personalizada. Isso inclui assessores que conduzem avaliações do PCI DSS e entidades submetidas a avaliações do PCI DSS.

O objetivo deste documento é fornecer diretrizes práticas para apoiar o uso consistente de controles de compensação e da abordagem personalizada.

O PCI Security Standards Council (PCI SSC) não é responsável por fiscalizar a conformidade nem por determinar se uma implementação específica está em conformidade. As entidades devem trabalhar com a(s) organização(ões) que gerenciam seu programa de conformidade, como um adquirente (banco adquirente), uma bandeira de pagamento ou outra entidade, para compreender as responsabilidades da entidade quanto à validação e ao relatório de conformidade.

As diretrizes deste documento não adicionam, ampliam, substituem nem prevalecem sobre os requisitos do PCI DSS ou de qualquer outro padrão do PCI SSC. No momento da publicação, a versão atual do PCI DSS é a v4.0.1; no entanto, os princípios e práticas gerais apresentados aqui também podem se aplicar a versões futuras.

Opções para Implementar e Validar os Controles do PCI DSS v4.x

O PCI DSS v4.x oferece duas formas para que uma entidade implemente e valide os requisitos do PCI DSS: a abordagem definida e a abordagem personalizada.

A abordagem definida é o método tradicional para implementação e validação dos controles do PCI DSS, em vigor desde a primeira versão do PCI DSS. **Os controles de compensação são uma opção dentro da abordagem definida** para entidades que possuem uma restrição técnica ou comercial legítima e documentada que as impede de atender ao requisito da abordagem definida conforme estabelecido. Os controles de compensação são frequentemente utilizados em situações nas quais existe um sistema ou processo legado que não pode ser atualizado para atender ao requisito.

A abordagem personalizada concentra-se no objetivo de segurança de cada requisito do PCI DSS (quando aplicável), permitindo que as entidades implementem controles para atender ao Objetivo da Abordagem Personalizada especificado pelo requisito, de uma forma que não siga rigorosamente o requisito definido. Como cada implementação personalizada é diferente, não existem procedimentos de teste definidos. Em vez disso, o assessor deve elaborar procedimentos de teste apropriados para a implementação específica, de modo que possa validar que os controles implementados atendem ao objetivo declarado.

A abordagem personalizada é uma opção para todos os requisitos do PCI DSS?

A maioria dos requisitos do PCI DSS pode ser atendida utilizando a abordagem definida ou a abordagem personalizada. No entanto, diversos requisitos não possuem um Objetivo da Abordagem Personalizada definido, o que significa que não há opção de abordagem personalizada para esses requisitos.

Para quais tipos de entidades a abordagem personalizada se destina?

A abordagem personalizada foi concebida para apoiar a inovação nas práticas de segurança, permitindo que as entidades tenham maior flexibilidade para demonstrar como seus controles de segurança atendem aos objetivos do PCI DSS. Essa abordagem é recomendada para entidades com maturidade em gestão de riscos, que demonstrem uma abordagem robusta para o gerenciamento de riscos de segurança, incluindo, entre outros, um departamento dedicado à gestão de riscos ou uma abordagem corporativa de gerenciamento de riscos.

Espera-se que os controles implementados e validados por meio da abordagem personalizada atendam ou superem o nível de segurança proporcionado pelos requisitos da abordagem definida. Consequentemente, o nível de documentação e o esforço necessários para validar implementações personalizadas também serão maiores do que os exigidos para a abordagem definida.

Uma abordagem personalizada pode ser utilizada por entidades que preenchem um SAQ?

O uso da abordagem personalizada não é suportado nos Questionários de Autoavaliação (SAQs). As entidades que desejam validar controles utilizando a abordagem personalizada podem utilizar o modelo de Relatório de Conformidade (ROC) do PCI DSS para documentar os resultados da avaliação. Questões relacionadas ao uso da abordagem personalizada, incluindo se entidades elegíveis para um SAQ podem, alternativamente, preencher um ROC para utilizar uma abordagem personalizada, devem sempre ser encaminhadas às organizações que administram os programas de conformidade, como as bandeiras de pagamento e os adquirentes.

Qual é a diferença entre um controle de compensação e a abordagem personalizada?

É importante observar que os controles de compensação têm uma finalidade diferente da abordagem personalizada. Ao contrário dos controles de compensação, que são utilizados quando a organização possui uma restrição e **não consegue** atender ao requisito conforme estabelecido, a abordagem personalizada destina-se às entidades que **optam por atender** ao requisito de forma diferente da descrita. Nesse caso, a entidade deve atender ao Objetivo da Abordagem Personalizada estabelecido, em vez de cumprir o requisito conforme redigido. A abordagem personalizada obtém melhores resultados quando a entidade possui processos de segurança robustos, práticas sólidas de gerenciamento de riscos e a capacidade de projetar, documentar, testar e manter de forma eficaz controles de segurança que atendam ao objetivo definido.

Observe que o Objetivo da Abordagem Personalizada de um requisito pode ser analisado para compreender a intenção do requisito, mesmo quando a entidade não estiver implementando uma abordagem personalizada para esse requisito.

Um controle de compensação e uma abordagem personalizada podem ser utilizados para o mesmo requisito?

Sim. Uma entidade pode utilizar controles de compensação para determinados componentes do sistema e a abordagem personalizada para atender ao mesmo requisito em outros componentes do sistema. Tomando o Requisito 5.3.1 como exemplo, uma entidade poderia utilizar um controle de compensação para atender a esse requisito em um determinado tipo de servidor, quando houver uma restrição comercial legítima e documentada que impeça esse servidor de atender ao requisito conforme estabelecido. A entidade também pode optar por utilizar a abordagem personalizada para atender ao mesmo requisito em outros componentes do sistema, quando tiver implementado uma abordagem exclusiva para detectar e tratar as ameaças mais recentes de malware. A entidade também poderia utilizar a abordagem definida, conforme estabelecida, para atender ao mesmo requisito em outro grupo de componentes do sistema.

Se uma entidade desenvolver uma abordagem personalizada que não atenda ao objetivo da abordagem personalizada, ela poderá utilizar um controle de compensação para atender a esse objetivo?

Não. Os controles de compensação não são uma opção dentro da abordagem personalizada. A abordagem personalizada destina-se a organizações que optam por desenvolver seus próprios controles para atender ao Objetivo da Abordagem Personalizada do requisito. Se uma organização desenvolver uma abordagem personalizada e posteriormente identificar restrições técnicas ou comerciais que a impeçam de atender ao Objetivo da Abordagem Personalizada, isso significa que a organização projetou uma abordagem personalizada que não consegue cumprir. É por esse motivo que os controles de compensação não são uma opção dentro da abordagem personalizada.

Se uma entidade determinar que não consegue atender a um requisito do PCI DSS por meio de uma abordagem personalizada e possuir uma restrição técnica ou comercial que a impeça de atender ao requisito da Abordagem Definida conforme redigido, ela poderá optar por implementar um controle de compensação com base no requisito original da Abordagem Definida.

Comparação de Casos de Uso: Exemplos para os Controles de Compensação e Abordagem Personalizada

Esses exemplos são fornecidos apenas para diferenciar casos de uso nos quais um controle de compensação ou uma abordagem personalizada podem ser considerados. Esses casos de uso não têm a intenção de ilustrar implementações ou controles reais adequados ou recomendados para utilização em qualquer ambiente específico. A entidade deve sempre confirmar com seu assessor e com a organização à qual enviará a documentação de conformidade a aceitabilidade e o uso de quaisquer controles de compensação ou controles personalizados.

Atendido por meio de um Controle de Compensação	Atendido por meio de uma Abordagem Personalizada
Requisitos 3.3.1.2 Os SAD são armazenados após a autorização porque a entidade não dispõe da tecnologia necessária para impedir o armazenamento.	*Este requisito não é elegível para a abordagem personalizada.*
Requisitos 3.5.1 O PAN não pode ser criptografado nem tornado ilegível por outros meios devido a uma limitação técnica.	
Requisitos 5.2.1 As soluções antimalware não podem ser implantadas em determinados sistemas devido a limitações técnicas.	**Requisitos 5.2.1** Um mecanismo implementado que detecta todos os malware e evita que este seja instalado ou executado.
Requisitos 8.3.6 Uma ferramenta de um provedor de nuvem não permite alterar as configurações de senha, e as configurações fornecidas não atendem aos requisitos do PCI DSS. *Isso pode ser tratado por meio de um Controle de Compensação ou de uma Abordagem Personalizada, dependendo do controle implementado.*	
	Requisitos 11.3.1 Vulnerabilidades internas são identificadas por meio de um método diferente da varredura de vulnerabilidade interna.
Requisitos 11.3.2 Devido a uma mudança pendente na ferramenta ASV, a próxima varredura externa de vulnerabilidades não pode ser realizada dentro do prazo previsto.	*Este requisito não é elegível para a abordagem personalizada.*
	Requisitos 11.5.1 Um mecanismo diferente do IDS/IPS é usado para detectar tráfego anormal de rede.

Funções para os Controles de Compensação e Abordagem Personalizada

Função da Entidade: Controle de Compensação

Espera-se que as entidades definam os controles de compensação quando utilizados e documentem esses controles por meio do preenchimento de uma ou mais Planilhas de Controles de Compensação (CCWs). As CCWs da entidade devem incluir:

- Restrições técnicas e/ou comerciais claramente definidas que impeçam a entidade de atender ao requisito do PCI DSS conforme estabelecido.
- A definição do controle de compensação e a explicação de como esse controle atende aos objetivos do requisito original e a quaisquer riscos adicionais; por exemplo, em termos das pessoas, processos, políticas e/ou tecnologias que compõem o controle.
- O objetivo do controle original:
  - A entidade pode, mas não é obrigada a, utilizar o Objetivo da Abordagem Personalizada do requisito para esse objetivo.
- O objetivo atendido pelo controle de compensação:
  - Esse objetivo pode ser, mas não precisa ser, o Objetivo da Abordagem Personalizada declarado para o requisito do PCI DSS.
- Uma descrição de qualquer risco adicional decorrente da ausência do controle original. A documentação deve demonstrar o entendimento desse risco e a forma como ele é tratado.
- Uma explicação de como a entidade valida e testa o controle de compensação.
- Uma definição dos processos e controles implementados pela entidade para manter o controle de compensação.

Uma amostra da CCW está incluída no PCI DSS v4.x, *no Apêndice C: Planilha de Controles de Compensação.* Um modelo de *Planilha Adicional de Controles de Compensação* está disponível no site do PCI SSC, na Biblioteca de Documentos, na seção PCI DSS.

Função do Assessor: Controle de Compensação

Os assessores devem analisar minuciosamente as Planilhas de Controles de Compensação (CCWs) da entidade durante cada avaliação anual do PCI DSS para confirmar que a(s) CCW(s) documenta(m) e trata(m) de forma clara e eficaz os itens descritos no *Apêndice C*: *Planilha de Controles de Compensação*, mencionados anteriormente na seção “Função da Entidade”.

Quanto à restrição técnica ou comercial legítima documentada pela entidade, não se espera que o assessor confirme se a restrição é válida, mas apenas que ela esteja adequadamente documentada pela entidade. No entanto, espera-se que o assessor teste os elementos de controle implementados pela entidade para confirmar que o controle de compensação está implementado e operando de forma eficaz.

Espera-se que o assessor:

- Inclua as CCWs da entidade no Relatório de Conformidade (ROC) ou no Questionário de Autoavaliação (SAQ), conforme aplicável.
- Realize testes do controle de compensação, incluindo análise de configurações, revisão de documentação, observação de processos etc., conforme apropriado ao requisito e ao controle avaliados.
  - Os Procedimentos de Teste do requisito podem ser utilizados como orientação quanto ao tipo de teste esperado para aquele requisito.
- Ao preencher um ROC, para cada requisito do PCI DSS atendido por meio de um controle de compensação:
  - Marque a caixa “Controle de Compensação”.
  - Inclua uma descrição de como os testes realizados e as evidências obtidas pelo assessor demonstram que o requisito está implementado.
  - Documente os testes executados nas funções de trabalho do assessor e armazene as evidências juntamente com as demais evidências da avaliação.

Um controle de compensação pode ser utilizado para tratar um requisito que não foi atendido no passado?

Não. No PCI DSS v4.x, o Apêndice B: Controles de Compensação foi atualizado para esclarecer que controles de compensação não podem ser utilizados retroativamente para tratar um requisito que deixou de ser atendido no passado. Essa nunca foi a intenção do uso de controles de compensação. Por exemplo, uma atividade que deveria ter sido executada não foi realizada, e nenhuma ação foi tomada naquele momento para tratar a situação. No entanto, uma entidade pode implementar um controle de compensação para tratar fatores que possam afetar o cumprimento futuro de uma atividade (por exemplo, para antecipar indisponibilidades programadas de sistemas ou férias de funcionários).

Um controle de compensação pode ser utilizado para atender a vários requisitos do PCI DSS?

Sim. Um controle de compensação pode ser projetado para mitigar o risco decorrente do não atendimento de mais de um requisito. Entretanto, a forma como cada requisito é atendido por esse controle de compensação deve ser documentada separadamente em Planilhas de Controles de Compensação individuais.

Todos os objetivos e riscos associados a cada requisito devem ser tratados, e o controle de compensação deve ser validado independentemente para cada requisito.

Um controle de compensação deve ser utilizado apenas por um período limitado?

Não existe exigência de que um controle de compensação permaneça implementado apenas por um período limitado; contudo, a entidade avaliada deve revisar anualmente seus controles de compensação para confirmar que continuam eficazes e necessários. Por exemplo, uma nova tecnologia ou sistema pode exigir a revisão do controle de compensação para atender ao objetivo do requisito ou pode eliminar a necessidade do controle de controle de compensação, permitindo que o requisito original do PCI DSS passe a ser atendido conforme estabelecido.

Da mesma forma, espera-se que o assessor revise anualmente os controles de compensação da entidade para confirmar que eles continuam apropriados e necessários para tratar o risco e atender ao requisito.

Função da Entidade: Abordagem Personalizada

A entidade avaliada projeta, desenvolve, analisa, implementa e mantém seus controles personalizados, incluindo as seguintes etapas:

- Revisar as informações sobre a abordagem personalizada descritas na seção Referências e Materiais de Apoio deste documento.
- Definir e documentar cada controle personalizado, incluindo uma descrição de como o controle atende ao objetivo do requisito. Consultar o *Amostra de Modelo de Matriz de Controles*[1] para documentar informações sobre o controle personalizado.
- Realizar e documentar uma análise de risco direcionada demonstrando que o controle personalizado é suficientemente robusto para fornecer, no mínimo, proteção equivalente à do Requisito Definido. Consultar o *Amostra de Modelo de Análise de Risco Direcionada*[1] para documentar informações sobre o controle personalizado.
- Realizar e documentar testes que confirmem que cada controle personalizado atende efetivamente ao objetivo do requisito. Utilizar o *Amostra de Modelo de Matriz de Controles* para documentar os testes realizados e seus resultados.
- Descrever como a eficácia de cada uma é monitorada e mantida ao longo do tempo.
- Comunicar-se antecipadamente com o assessor sobre os planos de implementação de uma abordagem personalizada.
- Fornecer ao assessor toda a documentação referente a cada controle personalizado.

Para que a entidade avaliada implemente e mantenha seus controles personalizados de forma eficaz, é importante que ela assuma a responsabilidade e a propriedade ativa desses controles.

Função do Assessor: Abordagem Personalizada

Quando a abordagem personalizada é utilizada, os assessores devem esperar receber previamente a documentação da entidade para apoiar a execução das seguintes etapas:

- Confirmar que o requisito do PCI DSS em questão é elegível para a abordagem personalizada.
- Revisar a documentação da entidade para compreender plenamente o controle personalizado.
  - Confirmar que tanto a Matriz de Controles quanto a Análise de Risco Direcionada foram concluídas e fornecidas.
- Confirmar que cada controle personalizado está suficientemente documentado, incluindo:
  - Todas as informações exigidas nos modelos de Matriz de Controles da Abordagem Personalizada e de Análise de Risco Direcionada.

[1] Dois modelos estão incluídos no documento Modelos de Amostras: Abordagem Personalizada - 1) uma Abordagem Personalizada - Amostra de Modelo de Matriz de Controles, e 2) uma Abordagem Personalizada - Amostra de Modelo de Análise de Risco Direcionada. Esse documento está disponível no site do PCI SSC, na Biblioteca de Documentos, na seção PCI DSS. Embora não seja obrigatório seguir exatamente os formatos desses modelos, a Matriz de Controles da Abordagem Personalizada e a Análise de Risco Direcionada da entidade devem conter todas as informações previstas nesses modelos, conforme definido no requisito 12.3.2 do PCI DSS.

  - Uma descrição de como o controle personalizado fornece proteção equivalente ou superior à do Requisito Definido.

- Revisar os testes realizados pela entidade sobre o controle personalizado e seus resultados para determinar se foram suficientes para avaliar adequadamente os controles.
- Desenvolver procedimentos de teste robustos que resultem em uma avaliação abrangente de cada controle personalizado.
  - A documentação fornecida pela entidade deve ser suficientemente detalhada para que o assessor compreenda o funcionamento do controle e possa desenvolver procedimentos de teste apropriados.
  - Caso o assessor conclua que os testes realizados pela entidade proporcionaram uma avaliação abrangente do controle, ele poderá, opcionalmente, aproveitá-los para realizar seus próprios testes de eficácia. Nesse caso, o assessor deverá utilizar uma amostra diferente daquela utilizada pela entidade.
- Realizar testes independentes de cada implementação de controle personalizado. Não se basear exclusivamente nos resultados dos testes realizados pela entidade. O objetivo dos testes realizados pelo assessor é determinar se o controle:
  - Atende ao Objetivo da Abordagem Personalizada do requisito;
  - É mantido de forma a assegurar sua eficácia contínua; e
  - É suficiente para resultar em uma conclusão “Implementado”.
- Documentar cada controle personalizado no Relatório de Conformidade (ROC), tanto no-requisito correspondente quanto no *Apêndice E* do ROC: *Modelo de Abordagem Personalizada*.
  - Durante uma avaliação, o assessor preenche esse apêndice para cada ocorrência em que um controle personalizado seja utilizado para atender a um requisito do PCI DSS.
  - Além de incluir informações sobre o controle personalizado provenientes da documentação da entidade, espera-se que o assessor inclua detalhes sobre os procedimentos de teste por ele desenvolvidos, as evidências revisadas para confirmar que o controle está implementado e operando de forma eficaz, bem como os resultados dos testes realizados.

Na abordagem personalizada, os testes realizados pela entidade podem substituir os testes do assessor?

Não. Os testes realizados pela entidade são obrigatórios como parte da implementação e manutenção da abordagem personalizada para demonstrar a eficácia dos controles, mas não substituem os testes desenvolvidos e executados pelo assessor. O assessor deve realizar testes independentes e basear suas conclusões de validação nos resultados desses testes. Se o assessor determinar que os testes realizados pela entidade proporcionaram uma avaliação abrangente do controle, poderá utilizar o mesmo método de teste, porém com uma amostra diferente da utilizada pela entidade.

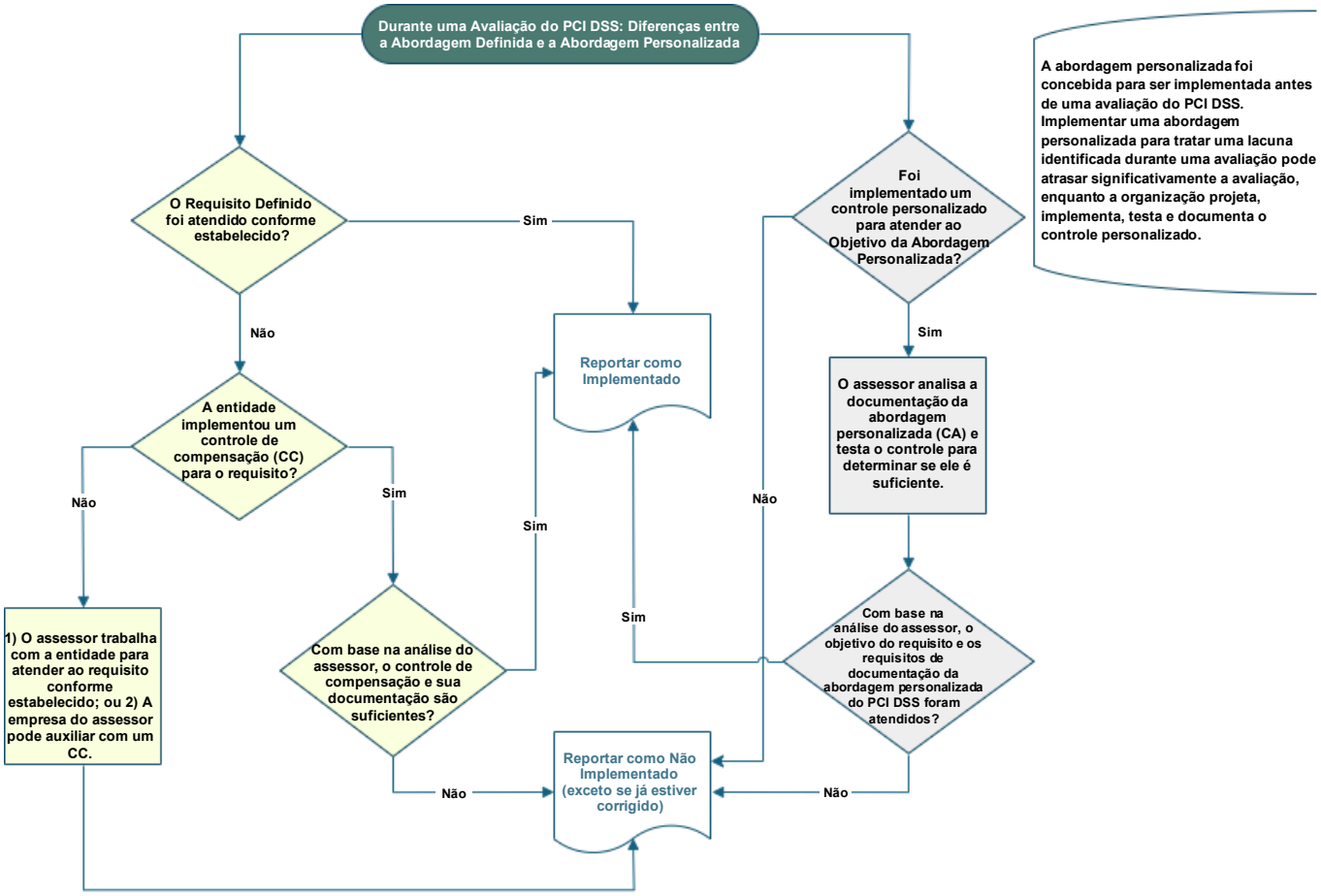
Por que a abordagem personalizada exige mais documentação do que um controle de compensação?

As implementações personalizadas variam conforme o projeto e o ambiente e são totalmente desenvolvidas pela entidade avaliada. Como o controle é projetado pela própria entidade e, portanto, não está definido no PCI DSS, também não existem procedimentos de teste predefinidos. Por esse motivo, é essencial que a documentação da entidade seja abrangente. Ela deve definir o que é o controle; como ele é implementado; qual é o risco envolvido; como esse risco é tratado; como o controle é testado pela entidade; como o controle atende ao objetivo estabelecido; como a entidade garante a eficácia contínua do controle; entre outros aspectos.

Essa documentação permite que o assessor compreenda plenamente o controle e seu funcionamento, possibilitando o desenvolvimento de procedimentos de teste apropriados e a validação independente do controle.

O diagrama abaixo ilustra como a abordagem de controles de compensação e a abordagem personalizada diferem durante uma avaliação do PCI DSS.

Figura 1: Como a Abordagem Definida e a Abordagem Personalizada Diferem Durante uma Avaliação do PCI DSS



Documentação dos Controles de Compensação e Abordagem Personalizada

As entidades são incentivadas a preparar documentação clara, completa e bem estruturada para seus controles de compensação ou personalizados. Uma documentação abrangente fornece aos assessores uma base sólida para compreender e avaliar o controle, o ambiente e a forma como o controle atende à intenção do requisito ou objetivo do PCI DSS.

A qualidade da documentação da entidade afeta diretamente a capacidade do assessor de validar os controles e chegar a uma conclusão defensável.

Tanto para controles de compensação quanto para implementações personalizadas, a documentação da entidade deve:

- Ser completa, clara e compreensível para um leitor independente.
- Ser autossuficiente, sem depender de contexto não documentado.
- Demonstrar claramente como os objetivos são atendidos e os riscos são tratados.
- Incluir evidências de como a entidade confirmou que o controle está funcionando de forma eficaz, incluindo detalhes sobre seus processos e resultados de validação, testes e garantia contínua.

Um controle de compensação ou uma abordagem personalizada podem ser validados se a documentação ou as evidências da entidade estiverem incompletas?

Não. Se a documentação não for suficiente, o assessor poderá não conseguir validar que o controle foi projetado adequadamente e está operando de forma eficaz. Se a entidade não fornecer evidências suficientes ao assessor, ou se o assessor não tiver garantia de que a documentação e os controles da entidade são suficientes, ele poderá determinar que uma conclusão “Não Implementado” é o resultado apropriado.

Independência do Assessor

A independência do assessor é um princípio fundamental das avaliações do PCI DSS e aplica-se igualmente à validação de controles de compensação e implementações personalizadas. A entidade avaliada é responsável pelo desenvolvimento, implementação e manutenção dos controles de compensação.

Os QSAs podem projetar ou implementar controles em nome de uma organização?

Embora Funcionários QSA possam auxiliar entidades no projeto ou implementação de controles, as Empresas QSA devem cumprir os requisitos de independência definidos nos *Requisitos de Qualificação para QSAs* e no *Guia do Programa QSA*. Isso inclui a implementação de controles de segregação de funções para garantir que os funcionários QSA que conduzem ou auxiliam em uma avaliação do PCI DSS sejam independentes e não estejam sujeitos a qualquer conflito de interesses.

Seria um conflito de interesses que um funcionário QSA envolvido no projeto ou implementação de um controle também realizasse testes, avaliações ou prestasse assistência na avaliação desse mesmo controle de compensação ou personalizado. Consulte a *FAQ 1562*, "Um funcionário QSA que projeta, desenvolve ou implementa controles específicos para um cliente também pode avaliar esses mesmos controles?", disponível na página de Perguntas Frequentes (FAQs) do PCI SSC, para mais informações.

Especificamente para a Abordagem Personalizada

Embora um funcionário QSA possa prestar serviços de consultoria relacionados à abordagem personalizada, uma organização que necessite que um QSA projete ou implemente seus controles personalizados pode não ser uma boa candidata para essa abordagem, pois pode ser difícil para a organização manter esse controle e garantir sua operação eficaz ao longo do tempo. Uma organização com maturidade em gestão de riscos, comprometimento e recursos necessários para desenvolver, implementar e manter seus próprios controles personalizados tem maior probabilidade de alcançar eficácia de segurança de longo prazo com controles personalizados.

Qualquer envolvimento de um assessor ou de uma empresa QSA no desenvolvimento de controles de compensação ou personalizados deve ser documentado na Seção 1.4 do Relatório de Conformidade (ROC).

Referências e Materiais de Apoio

Consulte as seguintes seções e apêndices do PCI DSS v4.x, bem como os documentos de diretrizes, modelos e formulários indicados:

Para a Abordagem Personalizada

- A Seção 8 da Introdução do PCI DSS v4.x compara os controles de compensação e a abordagem personalizada e fornece uma visão geral de ambas as abordagens.
- O Apêndice D do PCI DSS v4.x fornece mais detalhes sobre a abordagem personalizada, incluindo os elementos da análise de risco direcionada exigida e as responsabilidades da entidade e do assessor.
- No PCI DSS v4.x, a *Figura 5 – Entendendo as Partes dos Requisitos* indica a localização, dentro de cada requisito, do Requisito da Abordagem Definida e, quando aplicável, do Objetivo da Abordagem Personalizada.
- O Requisito 12.3.2, referente à Análise de Risco Direcionada (TRA) para qualquer requisito do PCI DSS atendido por meio de uma abordagem personalizada, define os elementos que devem compor essa análise.
- O Modelo de Relatório de Conformidade (ROC) do PCI DSS 4.x, Apêndice E Modelo de Abordagem Personalizada.
- *Modelos de Amostra:* A *Abordagem Personalizada* está disponível no site do PCI SSC, na Biblioteca de Documentos, na seção PCI DSS. Este documento inclui:
  - Abordagem Personalizada - Modelo de Matriz de Controle da Amostra
  - Abordagem Personalizada - Modelo de Análise de Risco Direcionada da Amostra
- *PCI DSS v4.x: Diretrizes de Análise de Risco Direcionada* - Descreve os dois tipos diferentes de análise de risco direcionada (TRAs) incluídas no PCI DSS v4.x.

Para os Controles de Compensação

- No PCI DSS v4.x:
  - A Seção Introdutória 8, que compara controles de compensação e a abordagem personalizada e fornece uma visão geral de ambas as abordagens.
  - *Apêndice B: Controles de Compensação*, que fornece a definição e os critérios básicos.
  - *Apêndice C: Planilha de Controles de Compensação*, um modelo de planilha que as entidades utilizam para definir controles de compensação quando estes são usados para atender a um requisito do PCI DSS.
- Uma *Planilha Adicional de Controles de Compensação*, para uso das entidades na documentação de controles de compensação, disponível no site do PCI SSC, na Biblioteca de Documentos, na seção PCI DSS.

Apêndice: Exemplos de Modelos Preenchidos para Controles de Compensação e Abordagem Personalizada

Exemplo Preenchido para a Entidade: Planilha de Controles de Compensação

Observe que este exemplo é fornecido apenas como uma das possíveis formas de preencher uma Planilha de Controles de Compensação e não deve ser interpretado como um exemplo de controle real adequado ou recomendado para qualquer ambiente específico.

Número e Definição do Requisito: Requisito do PCI DSS 8.4.2 – A autenticação multifator (MFA) é implementada para todo acesso ao Ambiente de Dados do Titular do Cartão (CDE).

	Informações Exigidas	Explicação
1. Restrições	Documente as restrições técnicas ou comerciais legítimas que impedem a conformidade com o requisito original.	A organização ABC opera uma plataforma legada de autorização de pagamentos (ID do Sistema: PCIPAY-AUTH-01) executada em UNIX proprietário versão 5.2. Essa plataforma não suporta integração com mecanismos modernos de MFA, incluindo RADIUS, SAML ou módulos MFA baseados em PAM. A plataforma possui suporte do fornecedor, mas não pode ser modificada sem invalidar esse suporte e comprometer a integridade do sistema. A substituição desse sistema está prevista no Projeto PCIPAY-MODERN-02, com conclusão programada para o quarto trimestre de 2027.
2. Definição dos Controles de Compensação	Defina os controles de compensação e explique como eles atendem aos objetivos do controle original e ao eventual aumento de risco.	A organização ABC implementou os seguintes controles de compensação: **Aplicação de MFA em Servidor de Acesso Intermediário** Todo acesso ao PAY-AUTH-01 é restrito a servidores administrativos de servidores de acesso intermediário dedicados, localizados no segmento de rede VLAN-SEC-ADM. O acesso aos servidores de acesso intermediário requer: ▪ Identificador único de usuário ▪ Autenticação por senha ▪ Token de autenticação baseado em hardware (dispositivo validado segundo FIPS) ▪ Integração com autenticação do Active Directory **Controles de Acesso à Rede** As regras de firewall restringem o acesso ao PAY-AUTH-01 exclusivamente a partir dos servidores de acesso intermediário. O acesso direto a partir de estações de trabalho, conexões VPN ou outros segmentos de rede é tecnicamente impedido.

	Informações Exigidas	Explicação
		Referência do conjunto de regras de firewall: FW-RULE-SET-CDE-ADM-V3. **Monitoramento e Registro de Sessões** Todas as sessões administrativas são: ▪ Registradas centralmente ▪ Encaminhadas para a plataforma corporativa SIEM (SecurityLog-SIEM-01) ▪ Retidas por no mínimo 12 meses **Gravação de Sessões** As sessões administrativas para o PAY-AUTH-01 são gravadas por meio da solução de gerenciamento de acesso privilegiado (PAM) PAM-SEC-01. As gravações são mantidas para fins de monitoramento e análise forense. **Monitoramento de Segurança e Geração de Alertas** O SIEM gera alertas para: ▪ Tentativas de acesso não autorizadas ▪ Acessos fora das janelas administrativas definidas ▪ Tentativas de elevação de privilégios Os alertas são analisados pela equipe do SOC.
3. Objetivo	Definir o objetivo do controle original.	Garantir uma autenticação forte para acesso ao CDE por meio do uso de múltiplos fatores de autenticação.
	Identificar o objetivo atendido pelo controle de compensação. **Observação:** *Esse objetivo pode, mas não precisa ser, o Objetivo da Abordagem Personalizada declarado para esse requisito no PCI DSS.*	*O controle de compensação atende ao objetivo do requisito ao impor a autenticação multifator (MFA) antes da concessão de acesso ao PCIPAY-AUTH-01 e ao impedir o acesso direto ao sistema.*
4. Risco Identificado	Identifique qualquer risco adicional decorrente da ausência do controle original.	Os riscos associados à impossibilidade de implementar MFA diretamente no PCIPAY-AUTH-01 incluem: ▪ Possível comprometimento das credenciais de autenticação ▪ Acesso não autorizado aos sistemas que armazenam dados do titular do cartão Os controles de compensação implementados mitigam esse risco ao garantir que: ▪ A autenticação MFA seja exigida antes do acesso ▪ O acesso direto seja impedido ▪ Todo acesso seja monitorado, registrado e revisado O risco residual é avaliado como Baixo.

	Informações Exigidas	Explicação
5. Validação dos Controles de Compensação	Defina como os controles de compensação foram validados e testados.	A entidade valida a eficácia dos controles de compensação por meio de: ▪ Revisões trimestrais das regras de firewall (Evidência: FW-Review-Reports) ▪ Revisões trimestrais dos acessos privilegiados (Evidência: Access-Review-Records) ▪ Verificação trimestral da aplicação de MFA nos servidores de acesso intermediário ▪ Verificação mensal da revisão de alertas do SIEM ▪ Auditoria interna anual dos controles de acesso privilegiado A entidade revisou as seguintes evidências de validação para confirmar a eficácia do controle: ▪ Configurações de firewall ▪ Configurações de controle de acesso ▪ Relatórios de alertas do SIEM ▪ Registros de gravação de sessões
6. Manutenção	Defina o(s) processo(s) e controles implementados para manter os controles de compensação.	A entidade mantém a eficácia dos controles de compensação por meio de: ▪ Procedimentos de gerenciamento de mudanças que regem mudanças de configuração em firewalls e servidores de acesso intermediário ▪ Monitoramento contínuo pelo SIEM ▪ Revisões trimestrais de acesso ▪ Revisão anual da aplicabilidade do controle de compensação Responsável pela revisão do controle de compensação: Diretor de Segurança da Informação Frequência de revisão: Anual

Exemplo Preenchido para a Entidade: Matriz de Controles para a Abordagem Personalizada

Observe que este exemplo é fornecido apenas como uma das possíveis formas de preencher uma Matriz de Controles para uma Abordagem Personalizada e não deve ser interpretado como um exemplo de controle real adequado ou recomendado para uso em qualquer ambiente específico.

Modelo de Matriz de Controles para a Abordagem Personalizada – Exemplo Preenchido **A ser preenchido pela entidade avaliada**		
Nome/Identificador do controle personalizado	Identificação e Autenticação por Voz	
Número(s) e objetivo(s) do(s) requisito(s) do PCI DSS atendidos por este(s) controle(s)	Requisito nº: 8.2.8	Objetivo: Uma seção de usuário não pode ser usada, a menos que seja por um usuário autorizado.
Detalhes do(s) controle(s):		
Qual(is) controle(s) foi(ram) implementado(s)?	A entidade opera um ambiente “Zero Touch” (Toque Zero) para fins de higiene operacional. Em vez de realizar login utilizando teclado, os usuários de um determinado ambiente interagem com seus computadores exclusivamente por meio de comandos de voz. Ao acessar um sistema pela primeira vez, o usuário emite o comando de voz “Reconhecer Usuário”, por exemplo: “Reconhecer Alice”. O sistema primeiro identifica e autentica o usuário por meio de sua impressão vocal exclusiva e, adicionalmente, realiza uma consulta ao sistema de controle de acesso físico para validar que o usuário está fisicamente presente no ambiente. Em seguida, solicita ao usuário (por exemplo, Alice) que repita três palavras aleatórias exibidas na tela, a fim de impedir o uso de gravações prévias e realizar uma segunda validação da impressão vocal. Após essa etapa, o usuário é autenticado.	

Modelo de Matriz de Controles para a Abordagem Personalizada – Exemplo Preenchido A ser preenchido pela entidade avaliada	
	O sistema permanece continuamente ouvindo comandos de voz. A sessão do usuário autenticado permanece ativa enquanto ele estiver fisicamente presente na área e é encerrada quando ele utiliza seu cartão de acesso para deixar o local. Cada vez que o usuário emite um comando, sua impressão vocal é validada. Se a impressão vocal não corresponder à do usuário autenticado, o comando é rejeitado e registrado. Os registros são enviados ao SIEM. Se outro usuário tentar utilizar o terminal no qual o usuário está autenticado, a impressão vocal não corresponderá e o sistema rejeitará o comando. Por exemplo, se Dave (que é um usuário autorizado do sistema, mas não está autenticado no terminal de Alice) ou Mary (uma invasora mal-intencionada) se aproximarem do sistema de Alice e disserem "Abra as portas da baia", o computador reconhecerá que o comando não foi emitido por Alice e responderá: "Receio não poder fazer isso." Além disso, registrará uma tentativa de acesso não autorizado. Adicionalmente, as interfaces USB e Bluetooth estão desabilitadas nos sistemas, de modo que o mecanismo de reconhecimento de voz não possa ser contornado manualmente.
Onde o(s) controle(s) está(ão) implementado(s)?	Instalação de produção 17. Nevada.
Quando o(s) controle(s) é(são) executado(s)?	Sempre que uma solicitação por voz é analisada.
Quem possui a responsabilidade geral e a prestação de contas pelo(s) controle(s)?	O Diretor de Segurança da Informação.
Quem participa do gerenciamento, manutenção e monitoramento do(s) controle(s)?	O departamento de cadastro de operações seguras é responsável pela integração de novos usuários ao sistema, incluindo o treinamento dos usuários e a obtenção de amostras de voz suficientes para a criação confiável da impressão vocal. O gerenciamento e a manutenção do sistema são terceirizados para a Acme Voiceprint Security Technologies, que é gerenciada de acordo com o requisito 12.8 e também fornece essa tecnologia a diversas instituições financeiras de destaque para detecção e validação de fraudes e para acesso a informações de clientes em centrais de atendimento.

Modelo de Matriz de Controles para a Abordagem Personalizada – Exemplo Preenchido A ser preenchido pela entidade avaliada	
Para cada **requisito do PCI DSS ao qual o(s) controle(s) é(são) aplicado(s), a entidade fornece detalhes sobre os seguintes aspectos:**	
A entidade descreve como o(s) controle(s) implementado(s) atende(m) ao ***objetivo*** do requisito do PCI DSS.	Somente o usuário autenticado pode utilizar a sessão, pois ele é efetivamente reautenticado (por biometria de impressão vocal) cada vez que um comando é emitido. Outros usuários autorizados e usuários não autorizados não conseguem utilizar a sessão autenticada.
A entidade descreve os testes **realizados** e os respectivos resultados, demonstrando que o(s) controle(s) atende(m) ao objetivo do requisito aplicável.	Foi contratada uma avaliação de segurança da Acme Secure Testing Services para validar a operação do sistema e tentar obter acesso não autorizado a uma sessão de usuário. A empresa não conseguiu obter esse acesso. Separadamente, a mesma empresa conduziu um exercício de Red Team e também não conseguiu comprometer o sistema nem obter acesso não autorizado simulando um usuário legítimo que utiliza comandos de voz.
A entidade descreve resumidamente os resultados da análise de risco independente que **realizou**, explicando o(s) controle(s) implementado(s) e como os resultados demonstram que o(s) controle(s) fornece(m), no mínimo, um nível de proteção equivalente ao da abordagem definida para o requisito aplicável do PCI DSS. Consulte o Modelo de Análise de Risco Direcionada separado para obter detalhes sobre a documentação dessa análise de risco.	Com o controle da abordagem definida, um usuário autenticado poderia deixar sua estação de trabalho, e um agente de ameaça não autorizado teria 15 minutos para acessar a estação antes do encerramento automático da sessão. Com este controle, a sessão permanece sempre ativa enquanto o usuário estiver fisicamente presente no ambiente, e a impressão vocal de cada comando é validada para confirmar que foi emitida pelo usuário autenticado antes que o comando seja executado. Portanto, o sistema trata um nível de risco superior ao tratado pelo controle de validação da abordagem definida.
A entidade descreve as medidas implementadas para garantir que o(s) controle(s) seja(m) mantido(s) e que sua eficácia seja assegurada continuamente. *Por exemplo, como a entidade monitora a eficácia do controle, como falhas são detectadas e tratadas e quais ações são tomadas.*	Mensalmente, um membro da equipe de Governança, Risco e Conformidade (GRC) tenta assumir o controle de uma sessão de usuário emitindo comandos de voz na instalação e utilizando gravações de voz previamente capturadas. Esse exercício segue um procedimento documentado, e os resultados são gravados em áudio pelo sistema. As gravações de áudio e os registros do procedimento são revisados pelo Diretor de Governança, Risco e Conformidade depois de cada teste. Existe um procedimento para reporte de incidentes suspeitos. Se um usuário suspeitar que o sistema respondeu a uma voz diferente da do usuário autenticado, há um procedimento específico a ser seguido. Todos os usuários receberam treinamento sobre esse procedimento e já preencheram um relatório de incidente simulado. O uso desse procedimento faz parte do treinamento anual de segurança dos usuários. Até o momento, nenhum incidente foi reportado.

Exemplo Preenchido para a Entidade: Análise de Risco Direcionada para a Abordagem Personalizada

Observe que este exemplo é fornecido apenas como uma das possíveis formas de preencher uma Análise de Risco Direcionada para uma Abordagem Personalizada e não deve ser interpretado como um exemplo de controle real adequado ou recomendado para uso em qualquer ambiente específico.

Análise de Risco Direcionada para a Abordagem Personalizada - Exemplo Preenchido A ser preenchido pela entidade avaliada	
Item	**Detalhes**
1. Identifique os requisitos	
1.1 Identifique o requisito do PCI DSS conforme redigido.	8.2.8 Se uma sessão de usuário permanecer inativa por mais de 15 minutos, o usuário deverá se reautenticar para reativar o terminal ou a sessão.
1.2 Identifique o objetivo do requisito do PCI DSS conforme redigido.	Uma seção de usuário não pode ser usada, a menos que seja por um usuário autorizado.
1.3 Descreva a ameaça que o requisito foi projetado para prevenir.	Um agente de ameaça interno ou externo pode assumir o controle de uma sessão legítima deixada sem supervisão por um usuário. O agente de ameaça poderia realizar atividades, acessar dados e emitir comandos que seriam incorretamente atribuídos ao usuário autenticado. Poderia ocorrer acesso não autorizado a sistemas e dados. Os arquivos de registro seriam imprecisos, registrando a identidade do usuário autenticado para atividades que ele não realizou.
2. Descrição da solução proposta	
2.1 Nome/Identificador do controle personalizado	Identificação e Autenticação por Voz
2.2 Quais partes do requisito, conforme redigido, serão alteradas na solução proposta?	O sistema utilizado não distingue especificamente entre estados ativos e inativos e, portanto, não possui a capacidade de detectar que uma sessão permaneceu “inativa” por 15 minutos. Em vez disso, após a autenticação inicial e o login do usuário, este pode emitir comandos de voz ao sistema a qualquer momento; entretanto, cada comando emitido é verificado para garantir que foi emitido pelo usuário autenticado. Somente comandos emitidos pelo usuário autenticado são aceitos.
2.3 Como a solução proposta impedirá a ameaça?	Como cada comando de voz é verificado antes de ser executado, quaisquer comandos emitidos por alguém que não seja o usuário autenticado falharão na verificação e não serão executados pelo sistema. Dessa forma, impede-se que um agente de ameaça interno ou externo consiga assumir o controle de uma sessão legítima deixada sem supervisão.

Análise de Risco Direcionada para a Abordagem Personalizada - Exemplo Preenchido A ser preenchido pela entidade avaliada						
Item	**Detalhes**					
3. Analisar quaisquer alterações na PROBABILIDADE de ocorrência da ameaça que possam resultar em uma violação da confidencialidade dos dados do titular do cartão						
3.1 Descreva os fatores detalhados na Matriz de Controles que afetam a probabilidade de ocorrência da ameaça.	Cada comando recebido pelo sistema é validado para confirmar que foi emitido pelo usuário autenticado. Isso reduz a probabilidade de que uma sessão autenticada seja assumida por um agente de ameaça. Com o requisito da abordagem definida, um agente de ameaça dispõe de uma janela de 15 minutos para obter acesso físico a uma sessão autenticada sem supervisão e assumir seu controle. Com os controles implementados, não existe oportunidade para que um agente de ameaça emita comandos utilizando a sessão de um usuário autenticado.					
3.2 Descreva os motivos pelos quais a ameaça ainda pode ocorrer após a aplicação do controle personalizado.	O sistema foi extensivamente testado e não pode ser comprometido por soluções tecnológicas, como síntese de voz ou reprodução de gravações. Além disso, espera-se que mesmo tentativas desse tipo sejam percebidas pelo usuário autenticado, que precisa permanecer fisicamente presente no ambiente para continuar conectado. Um agente de ameaça poderia contornar o controle por meio de intimidação física do usuário autenticado; entretanto, o sistema está equipado com um monitor de condição de emergência que não fornece indicação de ativação ao usuário, mas alerta a equipe de segurança. Durante testes e exercícios de avaliação de segurança, o sistema não pôde ser contornado por atacantes simulados.					
3.3 Em que medida os controles detalhados na abordagem personalizada representam uma alteração na probabilidade de ocorrência da ameaça quando comparados ao requisito da abordagem definida?	Maior probabilidade de ocorrência da ameaça	☐	Nenhuma mudança.	☐	Menor probabilidade de ocorrência da ameaça	☒
3.4 Forneça a justificativa para sua avaliação da mudança na probabilidade de ocorrência da ameaça após a implementação dos controles personalizados.	A janela de 15 minutos permitida pelo requisito para que um agente de ameaça assuma o controle da sessão de um usuário autenticado é reduzida para zero minutos, uma vez que cada comando é validado para confirmar que foi emitido pelo usuário autenticado.					
4. Analisar quaisquer alterações no IMPACTO do acesso não autorizado aos dados da conta						
4.1 Para o escopo dos componentes de sistema cobertos por esta solução, qual volume de dados de conta estaria em risco de acesso não autorizado caso a solução falhasse?	**4.1.1** Número de PANs armazenados	Nenhuma. A entidade não armazena PANs.		**4.1.2** Número de PANs processados ou transmitidos durante um período de 12 meses	32 milhões	

Análise de Risco Direcionada para a Abordagem Personalizada - Exemplo Preenchido A ser preenchido pela entidade avaliada	
Item	**Detalhes**
4.2 Descrição de como os controles personalizados irão diretamente: Reduzir o número de PANs individuais comprometidos caso um agente de ameaça tenha êxito; e/ou Permitir uma notificação mais rápida às bandeiras de pagamento sobre os PANs comprometidos.	Os controles implementados não proporcionam redução do impacto do acesso não autorizado aos dados da conta.
5. Aprovação e revisão do risco	
5.1 Revisei a análise de risco acima e concordo que o uso da abordagem personalizada proposta, conforme detalhado, fornece pelo menos um nível de proteção equivalente ao da abordagem definida para o requisito aplicável do PCI DSS.	[Assinatura]
5.2 Esta análise de risco deve ser revisada e atualizada até, no máximo:	[Data]

Exemplo Preenchido para o Assessor: Relatório de Conformidade – Apêndice E: Modelo da Abordagem Personalizada

Observe que este exemplo é fornecido apenas como uma das possíveis formas de preencher o Relatório de Conformidade e não deve ser interpretado como um exemplo de controle real adequado ou recomendado para uso em qualquer ambiente específico.

Número e Definição do Requisito: Requisito 8.2.8 dos PCI DSS: Se uma sessão de usuário permanecer inativa por mais de 15 minutos, o usuário deverá se reautenticar para reativar o terminal ou a sessão.

Modelo do Relatório de Conformidade para a Abordagem Personalizada – Exemplo Preenchido A ser preenchido pelo assessor	
Identifique o nome/identificador do controle personalizado utilizado para atender ao Objetivo da Abordagem Personalizada. *(**Observação**: utilize o nome do Controle Personalizado constante na Matriz de Controles da entidade avaliada.)*	Identificação e Autenticação por Voz

Modelo do Relatório de Conformidade para a Abordagem Personalizada – Exemplo Preenchido A ser preenchido pelo assessor	
Descreva cada controle utilizado para atender ao Objetivo da Abordagem Personalizada. (***Observação**: Consulte os Requisitos e Procedimentos de Teste do Payment Card Industry Data Security Standard (PCI DSS) para o Objetivo da Abordagem Personalizada.*)	Objetivo: Uma seção de usuário não pode ser usada, a menos que seja por um usuário autorizado. 1. Os usuários acessam o sistema exclusivamente por meio de comandos verbais. O sistema primeiro identifica e autentica o usuário por meio de sua impressão vocal exclusiva e, adicionalmente, realiza uma consulta ao sistema de controle de acesso físico para validar que o usuário está fisicamente presente no ambiente. Em seguida, o sistema solicita que o usuário repita três palavras aleatórias exibidas na tela para impedir o uso de gravações prévias e realiza uma segunda validação da impressão vocal. 2. O sistema permanece continuamente ouvindo comandos de voz. A sessão do usuário autenticado permanece ativa enquanto ele estiver fisicamente presente na área e é encerrada quando ele utiliza seu cartão de acesso para deixar o local. 3. Cada vez que o usuário emite um comando, sua impressão vocal é validada. Se a impressão vocal não corresponder à do usuário autenticado, o comando é rejeitado e registrado. Os registros são enviados ao SIEM. 4. Se outro usuário tentar utilizar o terminal no qual o usuário está autenticado, a impressão vocal não corresponderá e o sistema rejeitará o comando. 5. As interfaces USB e Bluetooth estão desabilitadas nos sistemas, de modo que o mecanismo de reconhecimento de voz não possa ser contornado manualmente.
Descreva como o(s) controle(s) atende(m) ao Objetivo da Abordagem Personalizada.	Objetivo da Abordagem Personalizada: Uma seção de usuário não pode ser usada, a menos que seja por um usuário autorizado. Somente o usuário autenticado pode utilizar a sessão, pois ele é efetivamente reautenticado (por biometria de impressão vocal) cada vez que um comando é emitido. Outros usuários autorizados e usuários não autorizados não conseguem utilizar a sessão autenticada.
Identifique a documentação da Matriz de Controles analisada que dá suporte à abordagem personalizada para este requisito.	Doc-10 – Matriz de Controles da Abordagem Personalizada
Identifique a documentação da Análise de Risco Direcionada analisada que dá suporte à abordagem personalizada para este requisito.	Doc-11 – Análise de Risco Direcionada (TRA) da Abordagem Personalizada

Modelo do Relatório de Conformidade para a Abordagem Personalizada – Exemplo Preenchido A ser preenchido pelo assessor	
Identifique o(s) nome(s) do(s) assessor(es) que atesta(m) que: A entidade concluiu a Matriz de Controles, incluindo todas as informações especificadas no Modelo de Matriz de Controles do documento PCI DSS v4.x: Modelos de Exemplo para Suporte à Abordagem Personalizada, disponível no site do PCI SSC, e que os resultados da Matriz de Controles dão suporte ao uso da abordagem personalizada para este requisito. A entidade concluiu a Análise de Risco Direcionada, incluindo todas as informações especificadas no Modelo de Análise de Risco Direcionada do documento PCI DSS v4.x: Modelos de Exemplo para Suporte à Abordagem Personalizada, disponível no site do PCI SSC, e que os resultados da análise de risco dão suporte ao uso da abordagem personalizada para este requisito.	Assessor(a) Josephine

Modelo do Relatório de Conformidade para a Abordagem Personalizada – Exemplo Preenchido A ser preenchido pelo assessor		
Descreva os procedimentos de teste definidos e executados pelo assessor para **validar que os controles implementados atendem ao Objetivo da Abordagem Personalizada;** por exemplo, se o(s) controle(s) personalizado(s) é(são) suficientemente robusto(s) para fornecer pelo menos um nível de proteção equivalente ao proporcionado pela abordagem definida. ***Observação 1:*** *Sempre que possível e apropriado, devem ser realizadas análises técnicas (por exemplo, revisão de configurações, verificação da eficácia operacional etc.).* ***Observação 2:*** *Adicione linhas adicionais para cada procedimento de teste definido pelo assessor, conforme necessário. Certifique-se de que todas as colunas à direita de "Procedimento de teste definido pelo assessor" sejam copiadas para cada procedimento adicional incluído.*		
Procedimento de teste definido pelo assessor: 1.a) Após obter acesso ao ambiente, tentar efetuar login no sistema utilizando o teclado disponibilizado, se houver. 1.b) Após obter acesso ao ambiente, tentar efetuar login no sistema utilizando o comando de voz exigido.	**Identifique o que foi testado** (por exemplo, pessoas entrevistadas, componentes de sistema analisados, processos observados etc.). ***Observação****: Todos os itens testados devem ser identificados de forma única.*	Os testes foram realizados com o auxílio de Int-1, Int-2 e Int-3 no ambiente Instalação de Produção 17 – Nevada, utilizando os sistemas ConsoleA e ConsoleB, nos quais o Controle da Abordagem Personalizada está ativo. Foi realizada entrevista com Int-10 para verificar se as anomalias observadas durante os testes 1 e 2 foram registradas e analisadas.
	Identifique todas as evidências examinadas para este procedimento de teste.	Foi revisado o Doc-22 – Registro do SIEM referente ao período dos testes 1 e 2.

Modelo do Relatório de Conformidade para a Abordagem Personalizada – Exemplo Preenchido A ser preenchido pelo assessor		
1.c) Após o usuário autorizado efetuar login no sistema, repetir as três palavras aleatórias exibidas na tela. 1.d) Após o usuário efetuar login no sistema, solicitar que outro usuário autorizado repita as três palavras aleatórias exibidas na tela. 2.a) Com o usuário autorizado presente na sala, emitir um comando de voz utilizando a voz do assessor. 2.b) Após o usuário autorizado utilizar seu cartão de acesso para deixar a área, emitir um comando de voz ao sistema utilizando uma gravação da voz do usuário emitindo um comando. 3.a) Revisar os registros do SIEM referentes aos resultados dos testes 1 e 2. 3.b) Entrevistar os responsáveis pela revisão dos registros do SIEM para determinar se foram identificadas anomalias durante os testes 1 e 2.	**Descreva os resultados** dos testes realizados pelo assessor para este procedimento e como esses resultados demonstram que os controles implementados atendem ao Objetivo da Abordagem Personalizada.	O assessor acompanhou um usuário autorizado ao entrar nos ambientes que continham os sistemas ConsoleA e ConsoleB. Teste 5.a) Inicialmente, o assessor examinou os consoles para verificar que as interfaces USB e os recursos Bluetooth não estavam disponíveis. Teste 1.a) Em seguida, o assessor constatou que não havia teclados disponíveis para efetuar login em nenhum dos consoles. Teste 1.b) O assessor então tentou efetuar login no sistema utilizando o comando de voz exigido. O sistema exibiu uma mensagem de erro informando que o assessor não era um usuário autorizado e, portanto, não podia efetuar login. Teste 1.c) O assessor observou Int-1 efetuando login em cada console, verificando que o comando de voz utilizado foi aceito pelos sistemas. Em seguida, o assessor repetiu as três palavras exibidas na tela de cada console e verificou que o sistema não autenticou o usuário e exibiu uma mensagem de erro indicando que a resposta vocal não foi reconhecida. Teste 1.d) O assessor observou Int-2 repetir as três palavras aleatórias exibidas na tela. O sistema recusou o acesso de Int-2 e exibiu uma notificação informando que a impressão vocal não correspondia à registrada. Teste 2.a) Após Int-1 efetuar login com sucesso e o sistema responder aos comandos de Int-1 para abrir o arquivo xyz, o assessor emitiu um comando para que o sistema abrisse o mesmo arquivo. O sistema recusou a solicitação e exibiu uma mensagem de alerta informando que a impressão vocal não correspondia à do usuário autorizado.

Modelo do Relatório de Conformidade para a Abordagem Personalizada – Exemplo Preenchido A ser preenchido pelo assessor		
4.a) Testado no item 2.b. 5.a) Examinar o sistema para verificar a existência de interfaces USB e recursos Bluetooth.		Teste 2.b) e Teste 4.a) O assessor observou o usuário autenticado utilizar seu cartão de acesso para sair do ambiente. Após a saída do usuário autenticado do ambiente, o assessor tentou emitir um comando ao sistema utilizando uma gravação do usuário anteriormente autenticado emitindo um comando. O sistema recusou a execução do comando e exibiu uma mensagem informando que o usuário havia sido desconectado do sistema. Teste 3.a) O assessor obteve os registros do SIEM gerados durante a execução dos testes e verificou que o sistema registrou corretamente as tentativas de acesso e de execução de comandos que falharam. Teste 3.b) O assessor entrevistou Int-10 para verificar se ela havia recebido um alerta referente à tentativa de acesso ao sistema. O assessor concluiu que o controle, conforme projetado, está funcionando como previsto e que seu desenho aparenta ser eficaz para restringir o uso da sessão exclusivamente ao usuário que obteve acesso autorizado.
Documente os procedimentos de teste definidos e executados pelo assessor para **validar que os controles são mantidos de forma a garantir sua eficácia contínua**; por exemplo, como a entidade monitora a eficácia dos controles e como falhas são detectadas, tratadas e corrigidas. ***Observação 1:*** *Sempre que possível e apropriado, devem ser realizadas análises técnicas (por exemplo, revisão de configurações, verificação da eficácia operacional etc.).* ***Observação 2:*** *Adicione linhas adicionais para cada procedimento de teste definido pelo assessor, conforme necessário. Certifique-se de que todas as colunas à direita de "Procedimento de teste definido pelo assessor" sejam copiadas para cada procedimento adicional incluído.*		
Procedimento de teste definido pelo assessor: 1) Revisar o procedimento documentado da equipe de GRC para testar os controles mensalmente. 2) Revisar as datas e horários dos resultados dos últimos 12 meses para verificar que os testes são realizados mensalmente.	**Identifique o que foi testado** (por exemplo, pessoas entrevistadas, componentes de sistema analisados, processos observados etc.) ***Observação****: Todos os itens testados devem ser identificados de forma única.*	Procedimentos de GRC (Doc-3) e resultados de testes dos últimos 12 meses (Doc-4). Entrevista com Int-1 e revisão dos resultados dos testes de março de 2025 e agosto de 2025 (Doc-16 e Doc-17) Revisão do procedimento documentado de reporte de incidentes suspeitos com Int-1. Revisão dos materiais de treinamento anual de segurança com Int-1, Int-2 e Int-3. Revisão dos relatórios de incidentes simulados preenchidos por Int-10 até Int-14. Verificação de que nenhum incidente ocorreu nos últimos 12 meses.

Modelo do Relatório de Conformidade para a Abordagem Personalizada – Exemplo Preenchido A ser preenchido pelo assessor		
3) Selecionar dois resultados de testes registrados para verificar se os controles funcionaram conforme esperado e se o Diretor de GRC revisou os resultados. 4) Revisar o procedimento documentado para reporte de incidentes suspeitos e verificar se ele descreve adequadamente as ações que o pessoal deve executar caso o sistema responda a uma voz não autenticada. 5) Revisar os materiais do treinamento anual de segurança para verificar que todos os usuários receberam treinamento sobre a utilização desse procedimento. 6) Selecionar aleatoriamente cinco relatórios de incidente simulados e revisar sua completude.	**Identifique todas as evidências** examinadas para este procedimento de teste.	Teste 1: Doc-3 Teste 2: Doc-4 Teste 3: Doc-16, Doc-17, Int-01 Teste 4: Doc-20 Teste 5: Doc-23 Teste 6: Doc-50, 51, 52, 53, 54

Modelo do Relatório de Conformidade para a Abordagem Personalizada – Exemplo Preenchido A ser preenchido pelo assessor		
7) Caso tenha ocorrido algum incidente confirmado, revisar o respectivo relatório de incidente. Revisar todos os relatórios de incidentes confirmados.	**Descreva os resultados** dos testes realizados pelo assessor para este procedimento de teste e como esses resultados demonstram que os controles implementados são mantidos para garantir eficácia contínua.	Os procedimentos de GRC para testar os controles mensalmente parecem ser claros e eficazes para determinar se os controles de comando por voz estão funcionando conforme pretendido. A equipe de GRC executou os testes mensalmente, e estes foram registrados conforme descrito nos procedimentos. Os resultados aparentam estar adequadamente documentados, incluindo a data e hora de execução, o responsável pela realização do teste e os resultados obtidos. Os procedimentos de relatório de incidentes suspeitos aparentam ser claros e adequados. Os requisitos de relatório incluem um formulário (Relatório de Incidente) de uso obrigatório pela equipe de TI da Instalação de Produção 17, Nevada. Nevada. Foi confirmado, por meio da revisão do registro de treinamentos obtido junto ao RH, que toda a equipe de TI da Instalação de Produção 17, Nevada recebeu o treinamento correspondente. Além disso, foram selecionados aleatoriamente cinco relatórios de incidentes simulados nos registros do RH, constatando-se que foram preenchidos de acordo com os procedimentos estabelecidos. Foi revisado, juntamente com Int-1, o relatório de incidentes referente aos últimos 12 meses. Embora existam incidentes registrados nesse registro, nenhum aparenta estar relacionado ao controle de comando por voz. Foi confirmado por Int-1 que não ocorreram incidentes relacionados a esse controle. Portanto, conclui-se que a manutenção do controle garante sua eficácia contínua para restringir o uso da sessão ao usuário autorizado que efetuou login no sistema.