CLOUDFLARE

ARTIGO TÉCNICO

# Uma abordagem estratégica para manter a conformidade com o PCI DSS 4.0

# Conteúdo

# Visão geral

**Todas as organizações que processam cartões de crédito, débito ou pré-pagos devem cumprir o Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS). Isso inclui pequenos comerciantes, varejistas, sites de comércio eletrônico, bancos e grandes empresas. No entanto, a mudança para a nuvem e para o trabalho híbrido, combinada com a evolução dos padrões à medida que o PCI DSS 4.0 é implementado, dificultam a conformidade de forma eficiente.**

**É necessária uma nova abordagem para este mundo digitalmente modernizado para agilizar o processo de conformidade de uma forma escalável, permitindo que as organizações acompanhem o cenário regulatório dinâmico à medida que este acompanha a modernização digital empresarial.**

# Desafios da conformidade com o PCI DSS para as organizações atuais

A conformidade com o PCI é essencial, com os infratores sujeitos a multas, ações judiciais e investigações governamentais. No entanto, a conformidade apresenta vários desafios para instituições financeiras, comerciantes de comércio eletrônico e outros que estão sujeitos aos seus regulamentos.

E à medida que as equipas de TI perdem o controle dos seus ambientes digitais devido a uma maior dependência da computação em nuvem e do trabalho remoto, o processo de resolução desses desafios torna-se mais complexo.

**Alocação de tempo e recursos:** 53% das organizações afirmam que falta pessoal para as funções técnicas de privacidade, o que torna a conformidade um desafio.[1]

**Segurança de dados em diversos ambientes:** com o aumento da computação em nuvem e dos pagamentos em dispositivos móveis, é cada vez mais difícil garantir a conformidade em ambientes diversos e muitas vezes menos controlados.

**Complexidade na integração da pilha de tecnologia:** integrar e manter as tecnologias necessárias para atender aos padrões de conformidade, como configurações de criptografia e firewall, costuma ser complexo. Este desafio é agravado em organizações com sistemas legados ou em transformação digital.

**Auditoria:** as equipes de TI devem manter uma trilha de auditoria atualizada em todas as infraestruturas e sistemas para garantir a conformidade.

**Conformidade do fornecedor:** garantir que prestadores de serviços e fornecedores terceirizados cumpram os padrões do PCI adiciona outra camada de complexidade.

# Acompanhar as ameaças cibernéticas sofisticadas com o PCI DSS 4.0

O PCI DSS 4.0 foi lançado em 31 de março de 2022, entrando em vigor em 31 de março de 2024, e requisitos adicionais vão entrar em vigor em 31 de março de 2025. Os objetivos do PCI DSS 4.0 são:[2]

### 1. Continuar a atender às necessidades de segurança do setor de pagamentos

- **Requisitos de autenticação aprimorados:** há uma ênfase maior na autenticação, especialmente na autenticação multifator para todos os acessos ao ambiente de dados do titular do cartão (CDE). Os requisitos de senha também são mais rigorosos, aumentando de oito para doze caracteres no mínimo.
- **Requisitos de criptografia mais fortes:** o PCI DSS 4.0 exige o uso de criptografia "forte" para armazenar e transmitir dados do titular do cartão, como o TLS, que não é vulnerável a explorações conhecidas.
- **Novos requisitos de comércio eletrônico e contra phishing para enfrentar ameaças contínuas:** o PCI 4.0 tem requisitos adicionais para segurança do lado do cliente e para defesa contra phishing e engenharia social.

### 2. Promover a segurança como um processo contínuo

- **Foco adicional na análise e gestão de riscos:** as organizações são incentivadas a implementar processos contínuos de análise e gestão de riscos para identificar e resolver vulnerabilidades prontamente.
- **Maior ênfase na responsabilidade e governança:** a nova versão coloca um foco mais forte na governança dos dados do titular do cartão e na responsabilidade pela manutenção dos controles de segurança.
- **Mais orientações para implementar e atender aos requisitos de segurança:** o PCI 4.0 esclarece a intenção do padrão e os prazos utilizados.

### 3. Adicionar flexibilidade para diferentes metodologias

- **Integração de novas tecnologias:** o PCI DSS 4.0 aborda a segurança de tecnologias emergentes, como sistemas de pagamento em nuvem e em dispositivos móveis.
- **Mais flexibilidade na forma como as organizações podem atingir os objetivos de segurança:** as organizações podem usar uma “abordagem personalizada”, uma gama mais ampla de métodos para atender aos requisitos. E o PCI 4.0 oferece mais flexibilidade para estabelecer a frequência com que executam ações com base em análises de risco direcionadas.

### 4. Aprimorar os métodos de validação

- **Monitoramento e testes contínuos:** o novo padrão incentiva uma mudança da validação anual de conformidade para o monitoramento contínuo de segurança e conformidade.
- **Maior alinhamento entre avaliações e atestados de conformidade:** as informações contidas em questionários de autoavaliação ou relatórios de conformidade estão mais alinhadas com o que está resumido nos Atestados de Conformidade.

# Solução: uma nova abordagem aos requisitos do PCI por meio da nuvem de conectividade da Cloudflare

As equipes de segurança e TI precisam atender aos requisitos do PCI de uma forma simples e programável que se integre facilmente à sua pilha atual de segurança e tecnologia, e continuar a fazê-lo à medida que sua infraestrutura e o PCI DSS evoluem.

A resposta não é uma abordagem confusa com muitas soluções de segurança legadas e pontuais. Em vez disso, as equipes precisam de uma plataforma unificada de serviços de rede e segurança nativos de nuvem, projetada para ajudar as empresas a recuperar o controle sobre seus ambientes de TI e atender a vários requisitos de conformidade, incluindo o PCI. Essa plataforma unificada é chamada de nuvem de conectividade.

**A nuvem de conectividade da Cloudflare oferece:**

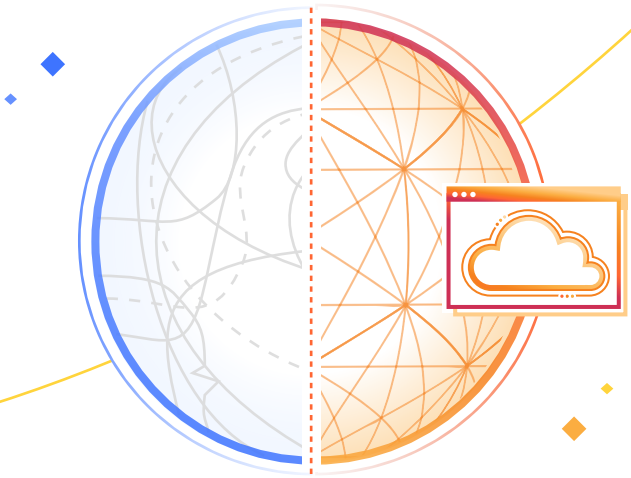
- Uma plataforma projetada para conformidade de dados
- Um mecanismo de políticas unificado
- Soberania de dados sem comprometer
- Relatórios inteligentes para satisfazer auditorias

A Cloudflare permite que as equipes de TI apliquem controles consistentes em todos os locais, usando um único plano de controle para ativá-los em todos os lugares.

As equipes podem enviar logs diretamente da borda da Cloudflare para um SIEM ou destino em nuvem preferido para auditoria. Além disso, a visibilidade em grande escala do tráfego da internet da Cloudflare significa que a Cloudflare pode identificar e defender contra novas ameaças automaticamente.

A Cloudflare é compatível com o PCI e oferece suporte nativo aos requisitos do PCI DSS 4.0. Por exemplo, a Cloudflare permite que as equipes de TI apliquem facilmente a autenticação multifator, uma das principais ênfases do PCI DSS 4.0. A Cloudflare também é compatível com os padrões de criptografia mais recentes e frequentemente contribui com eles, ajudando os clientes a atender aos requisitos do PCI DSS 4.0 para criptografia de informações confidenciais.

Um mapeamento resumido dos requisitos do PCI DSS para os recursos da nuvem de conectividade da Cloudflare pode ser encontrado na próxima página:



# Principais áreas onde a Cloudflare pode ajudar a atender aos requisitos do PCI*

| Requisito do PCI | Recurso da Cloudflare |
|---|---|
| 1. Instalar e manter controles de segurança de rede (anteriormente "instalar e manter um firewall"). | A Cloudflare protege redes, aplicativos e implantações em nuvem contra o tráfego de rede malicioso. A Cloudflare usa inteligência contra ameaças originada de centenas de bilhões de ameaças diárias para proteger sites e aplicativos web contra ameaças baseadas na web, incluindo os 10 principais ataques do OWASP e ataques zero-day. Sua plataforma de segurança nativa de nuvem, é implantada em minutos e permite que os usuários implementem mudanças nas políticas globais em segundos. |
| 2. Aplicar configurações seguras a todos os componentes do sistema. | Os usuários, dispositivos e aplicativos por trás da Cloudflare são fortemente criptografados e mascarados contra possíveis invasores na web. O API Shield da Cloudflare permite que os usuários criem proteções contra vulnerabilidades em suas APIs, identificando sequências e aplicando políticas relacionadas às transações de APIs. |
| 3. Proteger os dados armazenados por meio de criptografia ou outros métodos de proteção de dados. | A Cloudflare pode identificar informações de identificação pessoal em repouso e atende aos requisitos de tempo de retenção de log do titular do cartão. |
| 4. Criptografar os dados do titular do cartão em redes públicas abertas. | O tráfego enviado pela rede global da Cloudflare atende aos padrões de criptografia especificados neste requisito, e a Cloudflare pode bloquear a transmissão de informações de identificação pessoal que o usuário precisa identificar. |
| 5. Proteger todos os sistemas e redes contra software malicioso. | A Cloudflare atende mais de 55 milhões de solicitações HTTP por segundo, proporcionando uma visão abrangente e exclusiva dos ataques mais recentes. A Cloudflare oferece aos usuários um conjunto de proteções antimalware, incluindo antivírus, segurança de e-mail em nuvem e isolamento do navegador remoto. |
| 6. Desenvolver e manter sistemas e software seguros. | A Cloudflare pode classificar e ponderar as violações de segurança do usuário, bem como as configurações incorretas que detecta em aplicativos SaaS. Os serviços de segurança da Cloudflare podem proteger todos os aplicativos públicos voltados para a web contra ataques e explorações conhecidos. |
| 7. Restringir o acesso aos dados do titular do cartão com base na "necessidade de saber". | A Cloudflare pode impor controles de acesso granulares e com privilégios mínimos, independentemente de onde os usuários estejam localizados ou onde os dados estejam armazenados. |
| 8. Identificar usuários e autenticar o acesso aos componentes do sistema. | A Cloudflare pode impor políticas baseadas em identidade e verificações de postura de segurança (por exemplo, se a MFA foi usada) para qualquer tráfego que atravesse sua rede global. |
| 10. Registrar e monitorar todos os acessos aos componentes do sistema e aos dados do titular do cartão. | A Cloudflare fornece logs de auditoria granulares em todos os produtos de sua plataforma e integra-se à maioria dos principais SIEMs. |
| 11. Testar regularmente a segurança dos sistemas e redes. | A Cloudflare fornece testes de política de acesso limitado e funcionalidade de serviço de detecção de intrusões, além de fornecer registros detalhados para todos os seus principais produtos. |

*A Cloudflare não atende aos requisitos 9 e 12 do PCI DSS 4.0, que se referem à segurança física e à estrutura organizacional.

# Resumo: conte com a Cloudflare para ajudar a atender aos requisitos de conformidade com o PCI

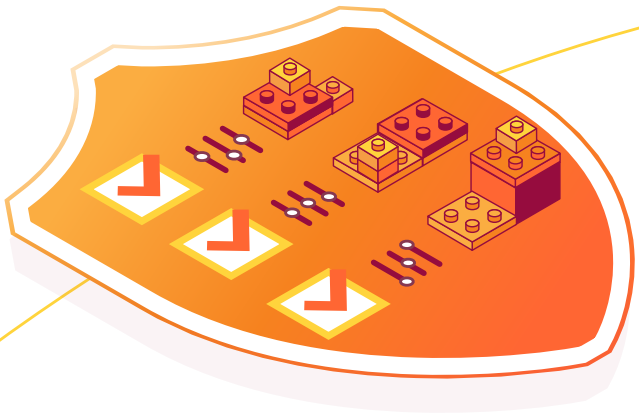
A Cloudflare é compatível com o PCI e possui recursos que ajudam os próprios clientes a atender aos requisitos de conformidade, independentemente de como é sua infraestrutura.

Na verdade, o uso da Cloudflare pode resultar em uma redução de 65%[3] na probabilidade de violação de dados, uma redução de 24%[4] nos prêmios anuais de seguro cibernético e uma redução de 59%[4] no tempo gasto no gerenciamento de sistemas e processos.

**Nossos clientes corporativos exigem contratualmente que a Stax atenda a padrões de conformidade muito específicos. Isso nos levou a aplicar controles de segurança como Zero Trust em toda a nossa infraestrutura... A Cloudflare fez exatamente o que precisávamos. Ela protegeu nossos endpoints e bloqueou nossa segurança."** [5]

**Troy Ridgewell**
Head of Security da Stax

STAX



Descubra hoje mesmo as soluções de conformidade de dados da Cloudflare. Fale com nossos especialistas para começar.

# Referências


1. https://www.isaca.org/about-us/newsroom/press-releases/2023/privacy-staff-shortages-continue-amid-increasing-demand-for-these-roles
2. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4-0-At-A-Glance.pdf
3. Relatório IBM Cost of Breach de 2022
4. Pesquisa Cloudflare TechValidate de 2023 com clientes dos serviços de aplicativos da Cloudflare
5. https://www.cloudflare.com/case-studies/stax

CLOUDFLARE



**+55 (11) 3230.4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/**

REV:BDES-5776.2024APR09