PCI para Estabelecimentos Comerciais

Getnet

• PCI para Estabelecimentos Comerciais •

Mas o que é o **PCI DSS** ?

É o ***Padrão de Segurança de Dados da Indústria de Cartões de Pagamento***, necessária para todas empresas que processam, armazenam ou transmitem dados de cartões pela internet, e é exigida para garantir a segurança desses dados. É uma das **maiores certificações de segurança do mundo.**

Para garantir a segurança dos clientes, **as bandeiras VISA, MASTERCARD** e **AMEX** exigem que **algumas categorias de comerciantes** que **transacionam anualmente** uma quantidade especifica de **pagamentos por cartão** também **estejam em conformidade com o PCI DSS.** Veja a seguir quais são **as categorias**, os **requisitos exigidos** e o **que fazer**:

Getnet

• PCI para Estabelecimentos Comerciais •

VISA

O volume total de transações Visa em um período de 12 meses determina o nível de comerciante e os requisitos necessários para validação:

CATEGORIA	CRITÉRIO	REQUISITOS (REVISÃO ANUAL)
Nível 1	Comerciantes que processam mais de 6 milhões de transações Visa anualmente em todos os canais ou comerciantes globais identificados como Nível 1 por qualquer região Visa	Arquive um Relatório de Conformidade ("ROC") pelo Avaliador de Segurança Qualificado ("QSA") ”ou recurso interno se assinado pelo executivo da empresa. Envie um formulário de Atestado de conformidade ("AOC").
Nível 2	1 a 6 milhões de transações Visa anualmente em todos os canais	Preencha um Questionário de Autoavaliação ("SAQ"). Envie um formulário de Atestado de conformidade ("AOC").
Nível 3	20.000 a 1 milhão de transações de e-commerce Visa anualmente	Preencha um Questionário de Autoavaliação ("SAQ"). Envie um formulário de Atestado de conformidade ("AOC").
Nível 4	Comerciantes processando menos de 20.000 transações de comércio eletrônico Visa anualmente e todos os outros comerciantes processando até 1 milhão de transações Visa anualmente	Preencha um Questionário de Autoavaliação (“SAQ”) ou exercício de validação alternativo conforme definido pelo Adquirente. **Link**:https://usa.visa.com/dam/VCOM/download/merchants/bulletin-small-merchant-security.pdf

Getnet

MASTERCARD

Para definir o Nível de Classificação, é recomendado que entre em contato diretamente com a GETNET, seguindo as seguintes etapas:

- Determinar o nível do comerciante conforme o volume de transações Mastercard do período de 52 semanas mais recente;
- Confirmar os requisitos de validação PCI necessários;
- Contratar um avaliador aprovado pelo PCI, conforme apropriado, seguindo os procedimentos de validação;
- Os comerciantes classificados como Nível 1, Nível 2 ou Nível 3 devem relatar seus status de conformidade diretamente para GETNET.

Getnet

• PCI para Estabelecimentos Comerciais •

MASTERCARD

CATEGORIA	CRITÉRIO, PARA QUALQUER COMERCIANTE:	REQUISITOS (REVISÃO ANUAL)
Nível 1	• Com mais de seis milhões de transações Mastercard e Maestro combinadas anualmente. • Que sofreu uma brecha de segurança que resultou em um evento de comprometimento de dados da conta (ADC) • Que atenda aos critérios de Nível 1 da Visa • Que a Mastercard, a seu exclusivo critério, determinar deve atender aos requisitos de comerciante do Nível 1 para minimizar o risco para o sistema	Os comerciantes de nível 1 devem concluir uma avaliação anual no local conduzida por um avaliador de segurança qualificado (QSA) aprovado pelo PCI SSC ou um avaliador de segurança interno (ISA) certificado pelo PCI SSC.
Nível 2	• Com mais de um milhão, mas menor ou igual a seis milhões de transações Mastercard e Maestro combinadas anualmente • Que atenda aos critérios de Nível 2 da Visa	Os comerciantes de nível 2 devem concluir uma avaliação anual no local ou autoavaliação conduzida por um QSA aprovado pelo PCI SSC ou um ISA certificado pelo PCI SSC.
Nível 3	• Com mais de 20.000 transações combinadas de e-commerce Mastercard e Maestro anualmente, mas menor ou igual a um milhão de transações combinadas de e-commerce Mastercard e Maestro anualmente • Que atenda aos critérios de Nível 3 da Visa	Os comerciantes de nível 3 e nível 4 podem, alternativamente, a seu próprio critério, contratar um QSA aprovado pelo PCI SSC para uma avaliação no local em vez de realizar uma autoavaliação.
Nível 4	Todos os outros comerciantes.	Os comerciantes de nível 4 são obrigados a cumprir o PCI DSS. Os comerciantes de nível 4 devem consultar seu adquirente para determinar se a validação de conformidade também é necessária. **Os pequenos comerciantes podem se familiarizar com a validação de sua conformidade com o PCI DSS por meio de um Questionário de autoavaliação (SAQ).**

• PCI para Estabelecimentos Comerciais •

AMEX

A maioria dos Níveis de Comerciante é baseada no volume de transações do Cartão American Express de um Comerciante enviadas por seus Estabelecimentos que acumulam para o nível de conta American Express mais alto. Os comerciantes se enquadram em um dos três níveis especificados na tabela abaixo:

CATEGORIA	CRITÉRIO	REQUISITOS (REVISÃO ANUAL)
Nível 1	2,5 milhões de transações com cartão American Express ou mais por ano; ou qualquer comerciante que tenha incidente dados; ou caso contrário, qualquer comerciante que a American Express, considera um comerciante de nível 1	Avaliação anual no local conduzida por um avaliador de segurança qualificado (QSA) aprovado pelo PCI SSC e Varreduras de Rede Trimestrais (ASV).
Nível 2	50.000 a 2,5 milhões transações de cartões American Express por ano	Autoavaliação conduzida por um QSA aprovado pelo PCI SSC e Varreduras de Rede Trimestrais (ASV).
Nível 3	Menos de 50.000 transações de cartões American Express por ano	Autoavaliação conduzida por um QSA aprovado pelo PCI SSC e Varreduras de Rede Trimestrais (ASV).

Os comerciantes são obrigados a enviar seus documentos de validação de PCI para a GETNET, que gerenciará sua conformidade com o PCI e relatará seu status diretamente para as bandeiras.

Ficou com dúvidas?

Nos contate pelo e-mail **pcicompliance@getnet.com.br**

• PCI para Estabelecimentos Comerciais •

SAIBA MAIS

Links úteis

- ***PCI SSC:***

https://www.pcisecuritystandards.org/document_library

- ***VISA:***

https://usa.visa.com/support/small-business/security-compliance.html#2

- ***MASTERCARD:***

https://www.mastercard.us/en-us/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI/service-providers-need-to-know.html

- ***AMEX:***

https://www.americanexpress.com/content/dam/amex/uk/staticassets/merchant/pdf/support-and-services/American_Express_Data_Security_Operating_Principles.pdf

Getnet