Orientações sobre Conformidade

PCI DSS

Introdução

A Cielo, em atendimento aos requisitos de segurança das Bandeiras, tem a obrigação de exigir que os estabelecimentos comerciais afiliados a ela estejam em conformidade com as melhores práticas de segurança estabelecidas pelo PCI Council*.

PCI Security Standards Council	* O PCI Security Standards Council é um fórum aberto global para contínuo desenvolvimento, aprimoramento, armazenamento, disseminação e implementação de padrões de segurança para a proteção de dados de contas. A missão do PCI Security Standards Council é aprimorar a segurança de dados de contas de pagamento, promovendo a educação e a conscientização sobre os Padrões de Segurança PCI. A organização foi fundada pelo American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa, Inc. [1]

Em nosso site (http://www.cielo.com.br/portal/cielo/solucoes-de-tecnologia/o-que-e-ais.html) é possível obter maiores informações sobre o PCI.

Este guia foi desenvolvido com o intuito de direcionar os estabelecimentos e-commerce que utilizam o produto BuyPageLoja e Gateways de Pagamento a se ajustarem aos requisitos estabelecidos pelo PCI.

Estes requisitos são estabelecidos com base no número de transações anuais dos Estabelecimentos e Gateways.

[1] https://pt.pcisecuritystandards.org/minisite/en/

E-commerce – BuyPageLoja que NÃO utilizam Gateway de Pagamento

Estabelecimentos que optam pelo Buy Page Loja sem a utilização de um Gateway de Pagamento são passiveis as exigências do PCI, pois irão manusear dados de cartão.

A seguir são descritos os requisitos de segurança necessários com base na quantidade de transações anuais do estabelecimento (realizadas ou planejadas):

➢ E-commerce abaixo de 20 mil transações anuais

Recomendável Scan de Vulnerabilidades trimestral e necessidade de atendimento aos requisitos abaixo:

< 20 Mil	• Não armazenar, em hipótese alguma, o código de segurança do cartão; • Armazenar o numero do cartão somente quando estritamente necessário E de forma criptografada; • Caso exista a necessidade de exibir os dados de cartão, este deve sempre estar mascarado: Exemplo: **********3456.

Comprovação de conformidade

Envie um email para a Central Cielo E-commerce (cieloecommerce@cielo.com.br) informando os dados do estabelecimento (razão social, identificação Cielo – número do estabelecimento) e a declaração de que os requisitos acima estão sendo cumpridos.

- **E-commerce acima de 20 mil e abaixo de 1 milhão de transações anuais**

> 20 Mil < 1Milhão	• Preenchimento do Questionário de Autoavaliação (SAQ – Self Assessment Questionaire) obtido em https://pt.pcisecuritystandards.org/_onelink_/pcisecurity/en2pt/doc/SAQ_D_v20_12_2_10_form_PT-BR.pdf; • Testes trimestrais de vulnerabilidade das redes através de empresa credenciada (ASV – Approved Scannning Vendor)[2].

Comprovação de conformidade

Enviar para Central Cielo E-commerce (cieloecommerce@cielo.com.br) o Questionário de Autoavaliação preenchido e o Resultado do Scan de Vulnerabilidades.
O Questionário de Autoavaliação deve ser enviado anualmente e o Scan de Vulnerabilidades trimestralmente.

[2] É responsabilidade do estabelecimento negociar o custo deste serviço com a companhia de segurança da sua preferência.

➢ **Entre 1 milhão e 6 milhões de transações anuais**

> 1 Milhão < 6 Milhões	• Para estabelecimento que possuírem esta quantidade de transações com a bandeira Mastercard, o preenchimento do Questionário de Autoavaliação deve ser realizado por um QSA. • Para estabelecimento que possuírem esta quantidade de transações com a bandeira Visa, o preenchimento do Questionário pode ser realizado por um profissional da empresa. O Questionário está disponível em https://pt.pcisecuritystandards.org/_onelink_/pcisecurity/en2pt/doc/SAQ_D_v20_12_2_10_form_PT-BR.pdf; Obs: Para estabelecimentos que possuírem esta quantidade de transações com ambas as Bandeiras (Visa e Mastercard), a regra Mastercard deve prevalecer. • Testes trimestrais de vulnerabilidade das redes através de empresa credenciada (ASV – Approved Scannning Vendor)[3].

Comprovação de conformidade

Enviar para e-seg@cielo.com.br o Questionário de Autoavaliação preenchido e o Resultado do Scan de Vulnerabilidades.
O Questionário de Autoavaliação deve ser enviado anualmente e o Scan de Vulnerabilidades trimestralmente.

[3] É responsabilidade do estabelecimento negociar o custo deste serviço com a companhia de segurança da sua preferência.

➢ **Acima de 6 milhões de transações anuais**

> 6 Milhões	• Auditorias utilizando Assessores de Segurança Independentes (QSA[4]); • Testes trimestrais da vulnerabilidade das redes através de empresa credenciadas (ASV – Approved Scannning Vendor).

Comprovação de conformidade

Enviar para e-seg@cielo.com.br o AOC (Attestation of Compliance) emitido pelo QSA após avaliação da situação do cliente e o resultado do Scan de Vulnerabilidades.
O AOC deve ser enviado anualmente e o Scan de Vulnerabilidades trimestralmente.

[4] Acrônimo de "Assessor de Segurança Qualificado" (Qualified Security Assessor), aprovado para a empresa pelo PCI SSC para conduzir avaliações on-site para o PCI DSS.

E-commerce – BuyPageLoja que utilizam Gateway de Pagamento

Estabelecimentos que optam pelo Buy Page Loja utilizando um Gateway de Pagamento e NÃO manuseiam dados de cartão, são isentos da necessidade da conformidade com o PCI DSS, uma vez que todo o manuseio dos dados de cartão ocorre no ambiente do Gateway.

O gateway utilizado deve estar em conformidade com requisitos de segurança estabelecidos pelo PCI. No link abaixo é possível obter a lista de gateways homologados:

http://www.cielo.com.br/portal/cielo/servicos/gateways-de-pagamento.html.

Caso o estabelecimento comercial manuseie dados de cartão, mesmo por alguns momentos, é obrigatório o atendimento dos requisitos descritos no parágrafo **E-commerce – BuyPageLoja que NÃO utilizam Gateway de Pagamento**

Gateways de Pagamento

Gateway de Pagamento são passiveis as exigências do PCI, pois irão manusear em seu ambiente os dados de cartão.

Uma vez em conformidade com os requisitos do PCI, o nome do Gateway será divulgado em nosso site como Gateway em conformidade com o PCI e homologado.

Abaixo são descritos os requisitos de segurança necessários com base na quantidade de transações anuais do Gateway (realizadas ou planejadas):

➢ **Abaixo de 300 mil transações anuais**

< 300 Mil	• Preenchimento do Questionário de Autoavaliação (SAQ – Self Assessment Questionaire), que pode ser obtido no link: https://pt.pcisecuritystandards.org/_onelink_/pcisecurity/en2pt/doc/SAQ_D_v20_12_2_10_form_PT-BR.pdf • Testes trimestrais de vulnerabilidade das redes através de empresa credenciada (ASV – Approved Scannning Vendor)

Comprovação de conformidade

Enviar um email para e-seg@cielo.com.br informando ser um Gateway de Pagamento, juntamente com o Questionário de Auto-Avaliação preenchido e o Resultado do Scan de Vulnerabilidades.
O Questionário de Auto-Avaliação deve ser enviado anualmente e o Scan de Vulnerabilidades trimestralmente.

➢ **Acima de 300 mil transações anuais:**

> 300 Mil	• Auditorias no local por parte dos Assessores de Segurança Independentes (QSA) • Testes trimestrais da vulnerabilidade das redes através de empresa credenciadas (ASV – Approved Scannning Vendor)

Comprovação de conformidade

Enviar para e-seg@cielo.com.br o AOC (Attestation of Compliance) e o Resultado do Scan de Vulnerabilidades informando ser um Gateway de Pagamento.
O AOC deve ser enviado anualmente e o Scan de Vulnerabilidades trimestralmente.

Penalidades pelo Não Cumprimento do PCI

Não cumprir com os requisitos do programa PCI ou não corrigir as vulnerabilidades de segurança pode resultar em:

- Multas a critério das bandeiras;
- Restrições ao estabelecimento;
- Proibição permanente do estabelecimento ou provedor de serviço de participar de vendas com cartões

Independente do nível aplicado para validar o cumprimento de uma organização, é de responsabilidade de cada entidade cumprir com as Normas de Segurança do PCI.

Qualquer dúvida entre em contato conosco pelo email:
e-seg@cielo.com.br