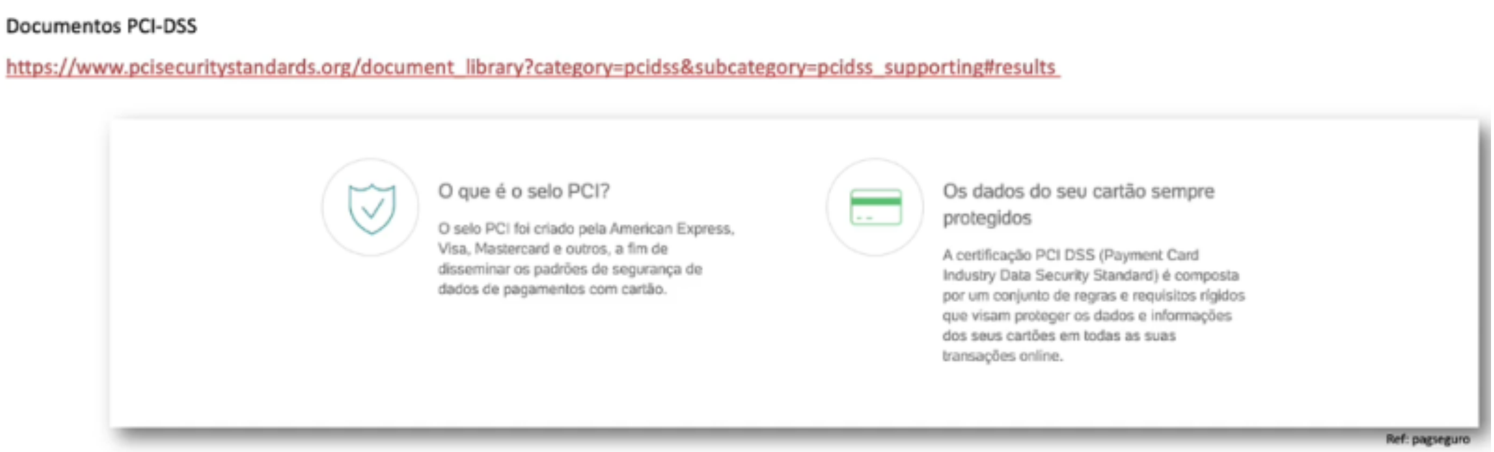
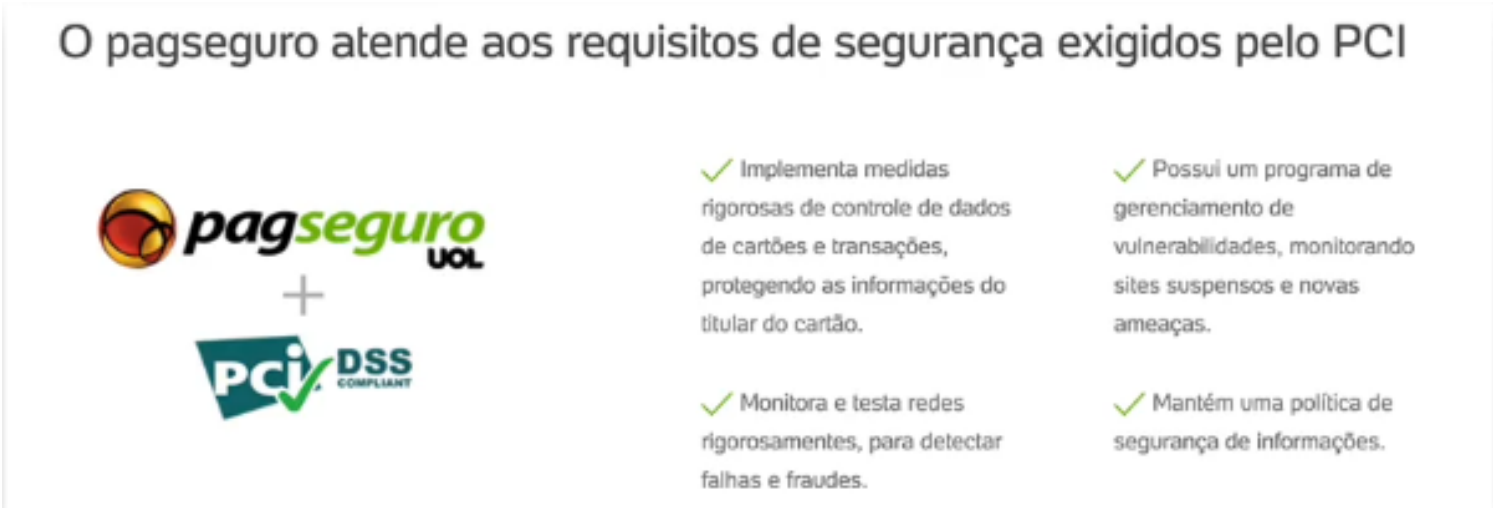
Compliance PCI-DSS

Compliance → Conformidade

O que é PCI-DSS
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
São certificações de segurança que todas as empresas que armazenam dados
de cartões de crédito devem possuir.
Elas pagam por uma auditoria anual para que, caso atinjam os níveis estabelecidos
de segurança, ganhem a certificação

Usando a DESEC como exemplo, vemos que por mais que compremos no site dela, o
gateway de pagamento não pertence à DESEC, e sim à Pagueseguro.


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~



Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security is maintained over time. Testing of security controls is especially important for any environmental changes such as deploying new software or changing system configurations.

11.1 Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Maintain an inventory of authorized wireless access points and implement incident response procedures in the event unauthorized wireless access points are detected.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. Address vulnerabilities and perform rescans as needed, until passing scans are achieved. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, complete four consecutive quarters of passing scans. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes and internal scans may be performed by internal staff.

11.3 Develop and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or modification. If segmentation is used to reduce PCI DSS scope, perform penetration tests at least annually to verify the segmentation methods are operational and effective. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after making changes to these controls. *(Note: The additional requirement for service providers is a best practice until 31 January 2018, after which it becomes a requirement.)*

11.4 Use network intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.

→ Veja, por exemplo, no requerimento 11 há uma exigência de pentests internos e externos a cada 3 meses (quaterly → trimestre) ou a cada mudança significativa na rede

Referências

Guia para Pentesters

https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

Documentos PCI-DSS

https://www.pcisecuritystandards.org/document_library?category=pcidss&subcategory=pcidss_supporting#results