segurança

Conformidade com PCI DSS

CESCE SI
SIA Group

Pontos-chave

- Normas de segurança PCI
- Quem forma o PCI SSC?
- PCI DSS, PA-DSS, PCI PTS
- Requisitos e obrigações PCI DSS
- Requisitos de PCI DSS
- Serviços profissionais do Grupo SIA para PC

Payment card Industry Data Security Standards

Normas de segurança de PCI

As normas de segurança PCI foram desenvolvidas para fomentar e melhorar a segurança dos dados dos titulares de cartões e para facilitar a adopção de medidas de segurança consistentes a nível mundial. Desde o seu início em 2006, têm sido desenvolvidas pelo **PCI Security Standards Council** e abordam diferentes áreas:

Quem forma o PCI SSC?

O PCI Security Standards Council é um fórum mundial aberto, fundado em 2006, responsável pela formulação, gestão, educação e conhecimento das normas de segurança da indústria de cartões de pagamento.

Payment Card Industry Council (PCI)

VISA MasterCard DISCOVER

Os cinco membros fundadores (*American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc.*) acordaram em incorporar o PCI DSS como requisito técnico de cada um dos seus programas de cumprimento em matéria de segurança. Além disso, reconhecem que os **Qualified Security Asssessor** (QSA) e os **Approved Scanning Vendors** (ASV) certificados pelo PCI SSC são os únicos habilitados para validar o cumprimento para com o PCI DSS.

Com as normas PCI, os requisitos próprios de cada uma das marcas de cartões são unificados, simplificando assim o processo de cumprimento com cada uma delas e facilitando a sua adopção. **Caso não cumpram com as normas**, as marcas de cartões com quem as empresas estejam a trabalhar podem impor sanções ou multas, chegando, inclusivamente, a negar o serviço de utilização dos seus cartões.

PCI DSS, PA-DSS, PCI PTS

Existem várias normas sob a PCI. As **PCI DSS** oferecem uma referência dos requisitos técnicos e operacionais desenvolvidos para proteger os dados dos titulares dos cartões. As **PCI DSS aplicam-se a todas as entidades que participam nos processos dos cartões de pagamento** (comerciantes, instituições financeiras, entidades emissoras, fornecedores de serviços, entre outras) e, em geral, todas as organizações que armazenam, processam ou transmitem dados de titulares deste tipo de cartões.

Por outro lado, aplicam-se **a fornecedores de software** e outras empresas que desenvolvem aplicações de pagamento que armazenam, processam ou transmitem dados dos titulares de cartões, sempre que as ditas aplicações sejam vendidas, distribuídas ou licenciadas a terceiros. Finalmente, as **PCI PTS** são aplicadas aos **dispositivos de pagamento** e definem os requisitos para o seu fabrico.

Requisitos e obrigações PCI DSS?

Das três normas, a PCI DSS é a que tem tido mais repercussões. Todas as organizações afectadas pela PCI DSS devem cumprir, validar e reportar o cumprimento da norma.

No entanto, as formas de validar e reportar o cumprimento variam consoante a marca dos cartões envolvida, principalmente o tipo de organização ou o volume de transações.

A título de exemplo, das cinco marcas de cartões, a **VISA e a Mastercard definem quatro níveis para o comércio**:

	Resumo das condições	Obrigações
1	• Se processarem mais de seis milhões de transações por ano, independentemente do canal. • Se comprometeu a informação dos cartões. • Se foi considerado de nível 1 por qualquer dos membros do PCI.	• Auditoria anual efectuada por um QSA • Scan de rede trimestral com um ASV.
2	• Se processarem entre um e seis milhões de transações por ano, independentemente do canal.	• Questionário de auto-avaliação anual. • Scan de rede trimestral com um ASV.
3	• Se processarem entre 20 mil e um milhão de transações por ano, independentemente do canal.	
4	• O resto *	

* O caso da Visa, os requisitos indicados para o nível 4 são apenas recomendações.

No caso dos **fornecedores de serviços,** as condições são semelhantes, se bem que diferentes em termos dos níveis:

	Resumo das condições	Obrigações
1	• Se armazenam, processam ou transmitem mais de 300 mil transacções anuais, inde-pendentemente do canal. • Se comprometeu a informação dos cartões.	• Auditoria anual efectuada por um QSA • Scan de rede trimestral com um ASV.
2	• Se armazenam, processam ou transmitem menos de 300 mil transacções anuais, independentemente do canal.	• Questionário de auto-avaliação anual. • Scan de rede trimestral (com um ASV no caso da Visa).

Como se pode verificar, nos níveis menos exigentes aceita-se a revisão através de **questionários de autoavaliação** (SAQ), que podem ser respondidos pelos próprios intervenientes. No entanto, é altamente recomendado que conte com a assessoria e experiência de auditores QSA certificados.

Requisitos de PCI DSS

Pode ver de seguida uma descrição geral dos 12 requisitos das PCS DSS (Figura 1):

Desenvolver e manter uma rede segura	1.	Instale e mantenha uma configuração de firewalls para proteger os dados dos titulares dos cartões.
	2.	Não use passwords de sistema ou outros parâmetros de segurança dados pelos fornecedores.
Proteger os dados do titular do cartão	3.	Proteja os dados do titular do cartão que forem armazenados.
	4.	Codifique a transmissão dos dados do titular do cartão nas redes públicas e abertas.
Manter um programa de administração de vulnerabilidades	5.	Utilize e actualize regularmente o software ou os programas de antivírus.
	6.	Desenvolva e mantenha sistemas e aplicações seguras.
Implementar medidas sólidas de controlo de acessos	7.	Restrinja o acesso aos dados do titular do cartão de acordo com a necessidade de saber do negócio.
	8.	Atribua um ID exclusivo a cada pessoa que tenha acesso por computador.
	9.	Restrinja o acesso físico aos dados do titular do cartão.
Supervisionar e avaliar as redes com regularidade	10.	Rastreei e supervisione todos os acessos aos recursos de rede e aos dados dos titulares dos cartões.
	11.	Teste os sistemas e os processos de segurança com regularidade.
Manter uma política de segurança da informação	12.	Mantenha uma política que aborde a segurança da informação para todo o pessoal.

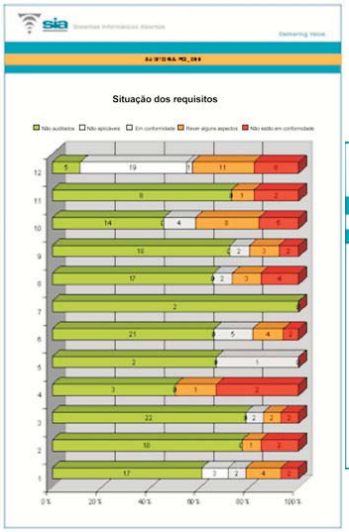
(Figura 1)

(Figura 2)

Serviços profissionais do Grupo SIA para PCI

Com mais de 20 anos de experiência como fornecedor de serviços de segurança, o Grupo SIA **conta com a certificação QSA** emitida pelo PCI SSC. Esta certificação permite-nos "acreditar" o cumprimento da norma conforme os requisitos estabelecidos pelas marcas de cartões, assim como dar assistência no momento de completar os questionários de autoavaliação. Adicionalmente, através de acordos de colaboração com companhias com certificação **ASV**, complementamos os nossos serviços com a realização de scans trimestrais de rede de acordo com a norma.
A SIA conta com uma vasta experiência em termos de segurança da informação e possui uma grande equipa de profissionais com um vasto know-how e experiência em termos de certificações como CISA, CISM, CGEIT, CRISC, LA 27001, CISSP ou CEH, entre outras.

O valor da SIA enquanto aliado no cumprimento de PCI não se resume à auditoria. A nossa condição de fornecedores de soluções integrais permite-nos oferecer **excelentes soluções para o cumprimento de PCI** em cada um dos doze requisitos (figura 1), unificando-os com o cumprimento de outros marcos semelhantes, como os derivados do SGSI, do ITIL e do COBIT,... ou das próprias políticas internas de cada companhia.



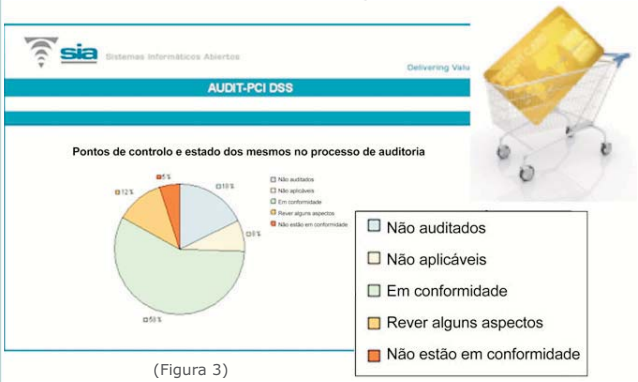
O Grupo SIA fomenta o cumprimento de PCI DSS com um enfoque orientado à melhoria contínua da segurança dos sistemas afectados, orientando os seus clientes a manter e aumentar a segurança de forma global.

Habitualmente, os nossos serviços PCI são desenvolvidos em quatro fases (figura 2), que têm como principal objectivo definir o ambiente afectado, identificar os pontos de não conformidade com a norma e orientar as ações que devem ser tomadas para os corrigir, até à emissão do relatório final.

Devido ao custo que a implementação dos requisitos PCI DSS representam, na primeira fase do projeto é especialmente importante a delimitação do alcance e a identificação dos componentes afectados. Em muitas situações, **é possível reduzir o custo e o esforço** utilizando uma segmentação de rede adequada, eliminando dados desnecessários e isolando sistemas, etc. É por este factor que o Grupo SIA recomenda dedicar todo o esforço necessário na primeira fase do projeto com o objectivo de simplificar o processo de cumprimento posterior.

Durante a fase de análise, utilizamos os **procedimentos de teste e critérios de avaliação definidos pelo PCI**. Apenas desta forma é possível garantir o cumprimento dos requisitos que são depois exigidos nos relatórios de auditoria (entidades compradoras, comerciantes ou as próprias companhias de cartões). Não só identificamos os pontos de não conformidade, como também as oportunidades de melhoria e recomendações para o cumprimento de PCI DSS.

Passado um prazo razoável para que a empresa auditada possa resolver as não conformidades, prepara-se o **Relatório de Cumprimento** e a **Declaração de Cumprimento** (figura 3). Neste ponto, é fundamental ter identificado os requisitos de reporting e os formatos com que terá de os fazer, de acordo com a entidade que os irá solicitar e o nível exigido.



(Figura 3)

O Grupo SIA, com base na experiência que possui em termos de segurança da informação pode ajudar os seus clientes no cumprimento com as normas de segurança, aumento e melhoria da segurança da informação através de outros serviços, como:
- Implementação de SGSI e análise de riscos.
- Planos de Continuidade de Negócio.
- Auditoria e adequação às normas.
- Adequação às boas práticas de ITIL.
- Marco normativo de segurança da informação.
- Planos de formação e conscienciação.
- Governance, Risk e Compliance.
- Segmentação de rede.
- Segurança do perímetro.

O Grupo SIA, fornecedor mundial de segurança, tem as seguintes certificações que demonstrama maturidade dos serviços que presta:
- Qualified Security Assessor - PCI DSS
- Gestão da Qualidade - ISO 9001:2000
- Gestão de Segurança da Informação - ISO 27001
- A Gestão de Serviços TI - ISO 20000
- Gestão do Meio Ambiente - ISO 14001:2004
- Gestão da Inovação - UNE 166002:2006
- Qualidade de Software (SPICE Nível 2) - ISO 15504

Lisboa: Edif. Ramazzotti, Av. do Forte, nº6 - piso 2 | 2790-072 Carnaxide Porto: Av. Sidónio Pais, 379 | 4100-468 Porto Tel.: +351 21 302 55 00 | Fax: +351 21 302 55 10 | www.cesce.pt