

Curso PCI-DSS

Formação do Profissional em Segurança da Informação

Security Officer Essentials 16 horas	Security Officer Foundation 40 horas	Security Officer Advanced 40 horas	ISO 27000	40 horas	Carreira com foco em processos e auditoria de Segurança da Informação
			Forense Computacional	32 horas	Carreira com foco investigativo em Segurança da Informação
	Engenharia Social	32 horas			
	Ethical Hacking	32 horas	Carreira com foco em tecnologias em Segurança da Informação		
Certificação Data Security					Reconhecimento Internacional em Segurança

Todos nossos cursos são preparados por mestres e profissionais reconhecidos no mercado de Segurança da Informação no Brasil e exterior.

Os cursos são ministrados em português, espanhol ou inglês, atendendo suas necessidades locais de formação.

Os cursos são oferecidos em turmas abertas compostas no máximo por 9 alunos, podendo também ser oferecido na modalidade In Company.

A formação em segurança da informação destina-se ao seguinte público:

- Gestores, consultores e técnicos nas áreas de Segurança e Tecnologia da Informação, Auditoria, Sistemas e Compliance.
- Profissionais em geral com interesse em conhecer e aprimorar as boas práticas em segurança da informação.

A nossa formação apresenta um diferencial no mercado, onde você pode se especializar na área de seu interesse, possibilitando forte reconhecimento no mercado de trabalho.



O PCI-DSS (Payment Card Industry - Data Security Standard) é um padrão de segurança criado pelo PCI-Council, composto de diversas bandeiras de cartão de crédito, como Visa, Mastercard e American Express, entre outras, que visa criar e recomendar as melhores práticas de segurança de dados a serem seguidas pelos estabelecimentos comerciais que aceitam cartões de crédito como forma de pagamento, para proteger a privacidade dos consumidores portadores de cartão de crédito.

O PCI-DSS contempla 12 requerimentos básicos que tem o objetivo de:

- 1. Manter a rede de dados segura;***
- 2. Proteger as informações de portadores de cartão de crédito;***
- 3. Manter um programa de Gerenciamento de vulnerabilidades;***
- 4. Implementar um forte controle de acessos;***
- 5. Manter uma política de segurança de informações***

Também tratamos de fraudes bancárias e dos requisitos para uma auditoria PCI-DSS, fornecendo um completo aprofundamento sobre o assunto.

Em linhas gerais o PCN analisa cada área da empresa e aponta, inclusive, os locais mais vulneráveis. É importante indicar onde é possível contar com um armazenamento seguro para instalar, se for o caso, o sistema de garantia da recuperação das informações, facilitando o backup periódico, por exemplo.

Para estar em conformidade com a PCI, a empresa deve alterar os processos e procedimentos internos, promover alterações em sistemas, melhorar a segurança de acesso à redes de dados e a ambientes e escritórios que possam conter dados confidenciais dos portadores e empresas de cartões de crédito.

Objetivo

Nosso curso sobre o tema tem como objetivo explicar sobre as tecnologias e os processos elencados nos 12 requisitos de segurança que devem ser atendidos para uma empresa se certificar com o padrão PCI, exigência cada vez maior para as empresas que trafegam, armazenam ou processam dados bancários.



Público alvo

Gestores, consultores e profissionais nas áreas de Segurança e Tecnologia da Informação, como Auditoria, Sistemas e Compliance; e profissionais da área bancária e empresas que cuidem de transações bancárias.

Benefícios

Fornecer subsídios para os alunos entenderem como funcionam as transações realizadas com cartões de crédito e realizarem uma análise de conformidade com o padrão PCI, permitindo que o mesmo possa ser implantado nas empresas.

Ao final deste treinamento o aluno estará apto para:

- Realizar uma análise de conformidade com o padrão PCI
- Conhecer medidas de segurança da informação para aumentar a segurança dos dados de cartões de crédito.
- Adaptar a infra-estrutura física e lógica da empresa para a submissão de uma auditoria oficial do PCI

Metodologia de ensino

Exposição interativa com apresentação de estudo de casos e exercícios práticos. O curso tem como proposta preparar o participante para estar apto a estruturar e modificar processos e procedimentos da empresa ao padrão PCI. Através de abordagem teórica e prática, com a aplicação de exemplos e debates, propicia um suporte para elucidação de dúvidas durante e após o término imediato do curso.

Pré requisitos

Não há pré-requisito específico, mas, recomenda-se que o participante tenha conhecimentos básicos sobre Processos de Negócios, Segurança da Informação e Gestão de Riscos, Tecnologia da Informação e Gestão Empresarial.



Material Didático

Apostila fornecida com os slides do curso e espaço para anotações.

Conteúdo Programático

1. Introdução a Compliance e ao PCI

Estabelece os conceitos básicos sobre o PCI e o PCI-DSS. Introduce conceitos de Compliance e de fraudes bancárias, como ocorrem e quais as principais formas atuais de fraudes.

- Compliance;
- Histórico da conformidade;
- Visão geral do PCI;
- Benefícios do PCI;
- Riscos da não-conformidade;
- PCI e PCI DSS;
- Fraudes Bancárias.

2. Requisitos PCI

Aborda os 12 requisitos do PCI-DSS para um ambiente que armazena, trafega ou processa dados de cartões de crédito. Tais requisitos são cobrados em auditorias de conformidade para o padrão PCI-DS.

- **Requisito 1:** Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão.
- **Requisito 2:** Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança.
- **Requisito 3:** Proteger os dados armazenados do portador do cartão.
- **Requisito 4:** Criptografar a transmissão dos dados do portador do cartão em redes abertas e públicas.
- **Requisito 5:** Usar e atualizar regularmente o software ou programas antivírus.
- **Requisito 6:** Desenvolver e manter sistemas e aplicativos seguros.
- **Requisito 7:** Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios.
- **Requisito 8:** Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador.
- **Requisito 9:** Restringir o acesso físico aos dados do portador do cartão.



- **Requisito 10:** Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão.
- **Requisito 11:** Testar regularmente os sistemas e processos de segurança
- **Requisito 12:** Manter uma política que aborde a segurança das informações para funcionários e prestadores de serviços.

Referência e Bibliografia Recomendada

Tony Bradley. **PCI Compliance**. Syngress, 2007.

PCI - Padrão de segurança de dados - Requisitos e procedimentos de avaliação da segurança - Versão 1.2 - Outubro de 2008

Mark Burnett, Dave Kleiman. **Perfect Passwords**. Syngress, 2006.

Facilitador:

MARCELO LAU,

Engenheiro pela EEM, pós-graduado em administração pela FGV e mestre em ciência forense pela POLI/USP. Atuou por mais de 12 anos em instituições financeiras em áreas de segurança da informação e prevenção a fraude.

Ocupa atualmente os seguintes cargos:

Diretor Executivo na Data Security.

Country Manager na I-SEC Brasil.

Coordenador e professor no curso de Pós-Graduação no curso de Segurança da Informação no SENAC/SP.

Professor no MBA de Segurança da Informação na FATEC-SP.

Professor em Cursos de Compliance na Febraban.

Atuou por mais de 3 anos como pesquisador da POLI/USP.



*Material desenvolvido para o
treinamento ministrado por
Marcelo Lau em parceria com o
GrupoTreinar. É proibida a
cópia deste conteúdo, no todo ou
em parte, sem autorização prévia.*
