

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	Carreira com foco em tecnologias em Segurança da Informação
			Ethical Hacking 32 horas	Reconhecimento Internacional em Segurança
Certificação Data Security				

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.



Engenharia Social

Objetivo

A engenharia social é um método utilizado em diversas partes do mundo para obtenção de informações sigilosas ou importantes em organizações.

Este curso permitirá reconhecer as ameaças da engenharia social e as formas de se proteger, dentro e fora de sua empresa.

Público alvo

Gestores, consultores e técnicos nas áreas de Segurança e Tecnologia da Informação, Auditoria, Sistemas e Compliance.

Profissionais em geral desejam conhecer as técnicas engenharia social e se proteger contra possíveis ataques.

Benefícios

Conhecer mais profundamente as vulnerabilidades advindas de ataques através de relacionamentos sociais e saber quais são os principais procedimentos e atitudes adotar.

Saber como aplicar as proteções através de técnicas específicas.

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 desenvolver análises e testes de vulnerabilidade. Através de abordagem teórica e prática, com a aplicação de exemplos e simulados, abrangendo a estrutura de controle e os processos que envolvem segurança da informação com foco em vulnerabilidade através de relacionamentos sociais, propiciando um suporte para elucidação de dúvidas durante e após o término imediato do curso.

Pré requisitos

Não existem pré requisitos mandatórios para este treinamento; no entanto, experiência de trabalho em segurança, melhoria de processos ou Serviços de TI é recomendada.

Carga Horária:

16 horas (08:30h às 17:30h) – 2 dias



Conteúdo Programático

1. Conhecendo as ameaças:

- Fatores de Risco;
- O que é Engenharia Social;
- Considerações Legais;
- Ameaças Internas e Externas;
- Características do Engenheiro Social;
- Motivação e Objetivo de um ataque;
- Tecnologia Aliada à Engenharia Social.

2. Técnicas de argumentação:

- O que é Argumentação;
- Pilares e Elementos da Argumentação;
- Técnicas Argumentativas.

3. Técnicas de convencimento:

- Psicologia Social;
- Técnicas de Persuasão e Influência.

4. Neurolinguística:

- O que é Neurolinguística;
- PNL (Programação Neurolinguística);
- Eficácia da Comunicação;
- Semelhança e Diferença entre as Pessoas;
- Métodos de Motivação;
- Regras da Comunicação com Confiança;
- Descoberta e Agrado do Seu Interlocutor.

5. Processo de coleta de informações:

- Técnicas Aplicadas em Empresas;
- Ferramentas de Coleta;
- Tratamento de Registros no Ambiente Internet;
- Redes Sociais.

6. Proteções contra a engenharia social:

- Técnicas Aplicadas em Empresas;
- Técnicas Aplicadas em Instituições Financeiras;
- Técnicas Aplicadas na Internet;
- Técnicas Aplicadas em Cadastros Pessoais;
- Conscientização;
- Métodos de Proteção;
- Estudo de Caso



Mini Currículo:

Prof. Msc. Marcelo Lau

Tem mais de 12 anos de atuação em bancos brasileiros em Segurança da Informação e Prevenção à Fraude. É professor do curso de formação em Compliance pela FEBRABAN no Brasil, professor no MBA de Segurança da Informação da FATEC/SP e coordena o curso de Gestão em Segurança da Informação e Gerenciamento de Projetos no SENAC/SP. É Engenheiro eletrônico da EEM com pós graduação em administração pela FGV e mestre em ciência forense pela POLI/USP. É reconhecido pela imprensa Brasileira e Argentina com trabalhos realizados em vários países do mundo.