

## Formação do Profissional em Segurança da Informação



*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.*



## Security Officer Foundation

***As comunicações e os meios de armazenamento das informações evoluíram mais nestes últimos anos do que em outro tempo na história conhecida. A internet comercial foi consolidada como uns dos principais meios de negócio e entretenimento e os custos de hardware e software tiveram e continuam tendo, redução significativa, bem como os processos de outsourcing se apresentaram como irreversíveis para a sobrevivência das grandes empresas, que buscam com isso reduzir custos e aumentar a produtividade, pondo foco em suas atividades fim. Por outro lado, os problemas e necessidades para a adequada segurança das informações também evoluíram – já que apareceram hackers e quadrilhas especializadas, de âmbito restrito ou internacionais, em fraudes eletrônicas.***

***A globalização potencializou os problemas de Segurança da Informação. Empresas perdem milhões de dólares com danos em computadores todos os anos, grandes companhias gastam milhares de dólares em segurança de sistemas, horas de indisponibilidade tiram a confiança de consumidores.***

***Ameaças como cavalos de tróia, por exemplo, atingem não só máquinas de empresas ou corporações, mas também usuários domésticos. Fatos estes que causam prejuízos financeiros para todos. Assim passou a ser vital a grande dependência do gerenciamento adequado das informações residentes nos diversos meios eletrônicos.***

***Portanto, o perfil do profissional que é responsável pela segurança da informação deve ser cada vez mais eclético, diversificado e dinâmico, adequado ao Security Officer Foundation (escritório de Segurança da Informação da empresa) e deve englobar um conhecimento teórico e prático para elaboração e implementação da Política de Segurança da Informação. Daí a necessidade cada vez maior de formação ou aprimoramento profissional nesta área de especialização.***

### **Objetivo**

Este curso tem como objetivo prover conhecimento das melhores práticas de Segurança da Informação de forma geral. Aprofundar o conhecimento do Gerenciamento Total da Segurança da Informação, notadamente em seus tópicos principais como a sua integridade, disponibilidade e confidencialidade.

O conteúdo visa a proporcionar ao participante a conhecer mais profundamente o gerenciamento de Risco, com grande enfoque Gestão de Continuidade de Negócios, Legislação, Forense computacional, Segurança nos sistemas operacionais dos equipamentos, sejam computadores, sejam mais vinculadas às telecomunicações, estabelecimento de políticas para a classificação de informações e procedimentos para com respostas a incidentes.



## **Público alvo**

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

## **Benefícios**

Este curso sintetiza todos os conhecimentos e áreas de segurança da informação em um único curso.

Entender e reconhecer como questões de gerenciamento de segurança afetam e são afetadas pela organização e aprofundar o seu conhecimento com o aprendizado adquirido, em outros cursos e certificações na área de segurança em geral.

Conhecer em detalhes os principais componentes da segurança da informação e como eles se integram com o objetivo de manter a integridade, disponibilidade e confidencialidade de seu conteúdo.

O aluno ao fim do curso estará apto a ampliar seus conhecimentos em áreas mais específicas em segurança da informação, além de ingressar no mercado de segurança da informação no Brasil e exterior e aplicar os conceitos gerais, do ponto de vista teórico/prático, com a realidade do dia-a-dia nas empresas.

## **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 estruturar e gerenciar o “security office” da organização. 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, 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 de TI, melhoria de processos ou Serviços de TI é recomendada, bem como conhecimentos básicos da língua inglesa, na parte de leitura especificamente, dado que muitos materiais e referências ainda se encontram neste idioma.



## Conteúdo Programático

### 1. Conceitos Gerais de Segurança da Informação:

- Conceitos e Princípios Básicos e Práticos;
- Princípios adotados em segurança;
- Histórico da Segurança da Informação;
- Tecnologias Emergentes em Segurança;
- Abrangência e Influências da Segurança;
- Controles em Segurança.

Empresas perdem milhões de dólares com danos em computadores todos os anos. Grandes companhias gastam milhares de dólares em segurança de sistemas. Horas de indisponibilidade tiram a confiança de consumidores. Ameaças como cavalos de tróia atingem não só máquinas, mas usuários domésticos que também apresentam prejuízos financeiros.

### 2. Gestão de Risco:

- Introdução aos Riscos;
- COSO;
- Prática em Gestão de Risco;
- Risco Operacional e Residual;
- Matriz de Risco;
- Risco Reputacional.

É o risco relativo às ameaças internas ou externas que podem resultar em acessos não autorizados à alguma informação. Incluem-se aqui os riscos relativos ao vazamento de dados, privacidade de dados e fraudes. Inclui-se aqui também uma ampla gama de ameaças externas como ataque por vírus, bem como ataques bem objetivos à aplicações, usuários e informações específicas - ataque a sistemas que as pessoas confiam e utilizam diariamente.

### 3. Gestão de Segurança da Informação:

- Modelo PDCA;
- O que é o SGSI;
- O que está incluso no processo de Gestão;
- Responsabilidades da Gestão;
- Requisitos de Gestão;
- Detalhamento dos Requisitos.

A Gestão da Segurança da Informação tem como foco principal as características humanas, organizacionais e estratégicas da Segurança da Informação. Ela é a base fundamental que direciona, viabiliza e dá eficácia a todas as demais atividades no escopo desta área tão desafiadora. Os serviços contemplados incluem:

- Desenvolvimento Políticas e Normas de Segurança Baseado na BS 7799 / ISO 17799;



- Análise e Gestão de Risco Baseado na ISO 13335;
- Planejamento de Disaster Recovery e Continuidade de Negócios Baseado na BS 7799 / ISO 17799;
- Treinamento e Conscientização.

#### **4. Legislação, Regulamentação, Normas, Investigação e Ética:**

- Rainbow Books;
- Legislação;
- Regulamentação;
- Controles ISO 27000;
- Ética.

A criminalização de atos praticados em computadores e redes deverá ter como contra-partida a elaboração de norma de direito civil, que estabeleça penalidades financeiras e outras, e que defina a materialidade dos direitos e obrigações no universo digital, especialmente no comércio eletrônico.

#### **5. Política de Segurança da Informação:**

- Papel da Política;
- Exemplos de Políticas;
- Políticas Híbridas;
- Conteúdos das Políticas;
- Fatores de Sucesso;
- Elaboração, Estruturação e Redação das Políticas.

As decisões que você como administrador toma ou deixa de tomar, relacionadas à segurança, irão determinar quão segura ou insegura é a sua rede, quantas funcionalidades ela irá oferecer, e qual será a facilidade de utilizá-la. No entanto, você não consegue tomar boas decisões sobre segurança, sem antes determinar quais são as suas metas de segurança. Até que você determine quais sejam elas, você não poderá fazer uso efetivo de qualquer coleção de ferramentas de segurança pois você simplesmente não saberá o que checar e quais restrições impor.

#### **6. Classificação de Informações:**

- Modelo de Classificação das Informações;
- Controles;
- Implementação da Classificação;
- Aspectos Práticos da Classificação;
- Monitoramento da Classificação.

Em um cenário de sociedade digital, em que a grande maioria das manifestações de vontade e tomadas de decisão estão em documentos eletrônicos, é fundamental que a empresa seja capaz de guardar adequadamente sua informação.

Para isso, deve ser criado um ciclo de vida da informação, desde o momento da geração, a captação, transmissão, compartilhamento, guarda e em especial, a eliminação. Não basta guardar tudo, é preciso também aplicar princípios de taxonomia de modo a que a informação possa depois ser facilmente localizada quando for necessária.



### **7. Gestão de Continuidade de Negócios:**

- Planos de Continuidade de Negócio;
- Atividades e documentos do PCN;
- Tipos de testes em PCN;
- Manutenção do PCN;
- Causas da indisponibilidade;
- Componentes a alta disponibilidade;
- Métricas e níveis de disponibilidade;
- Requisitos de Data Centers.

O serviço de Continuidade de Negócios visa implementar um processo de gestão para reduzir, a um nível aceitável, a interrupção causada por falhas de segurança ou desastres, através de planos de ação de prevenção e recuperação.

Os planos devem ser implementados e testados periodicamente para garantir que os processos de negócio possam ser recuperados dentro do prazo estipulado, gerando o menor impacto possível para o negócio.

### **8. Segurança Física e Lógica.**

- Controle de Acesso;
- Autenticação e Usuários;
- Criptografia;
- Segurança Ambiental;
- Segurança Física e Ambiental em TI;
- Tipos de Controles Ambientais e Físicos.

A segurança física visa proteger o ativo utilizando-se de barreiras físicas como portas, cadeados, crachás para acessos a salas, etc. A maneira mais simples é definir um perímetro de segurança. Tão importante quanto a segurança física é a segurança lógica, ou seja, controle de acesso, nesse caso menos é mais, se um empregado não precisa de acesso ao arquivo X o mesmo não pode ter acesso a ele, aumentando a segurança dos dados.



## 9. Segurança em Sistemas Operacionais.

- Hardening em Software, Hardware e Network;
- Ataques sobre sistemas operacionais;
- Confiança em Sistemas Operacionais;
- Requisitos de Segurança em Sistemas;
- Riscos das aplicações em Sistemas;
- Auditoria em Sistemas.

A segurança tem se tornado um dos principais focos no desenvolvimento de aplicações em geral. O crescimento do número de incidentes de segurança, entretanto, demonstra que os esforços estão sendo insuficientes para conter o avanço dos hackers. Neste tópico, serão apresentados os paradigmas de segurança sobre os quais se baseiam os sistemas operacionais de uso mais comum, e suas falhas, alertando assim para os motivos que tem levado ao crescimento do número de ataques. São apresentados, também, métodos de segurança analisando os aspectos que impedem uma rápida descamação dos mesmos.

## 10. Segurança em Telecomunicações:

- Fundamentos e arquitetura de rede;
- Proteção de Perímetro;
- Segurança em Telecomunicações;
- Tipos de Análise de Vulnerabilidade;
- Passos de uma análise de vulnerabilidade.

Com a crescente convergência de telecomunicações e informática, temos a necessidade de aplicar controles de segurança para garantir que estes recursos de telecomunicações não se tornem ameaças. Atualmente, com a Internet e a utilização crescente de meios sem fio temos mais uma área para aplicar controles.

## 11. Segurança em Redes sem fio:

- Computação Móvel;
- Princípios e Segurança na Comunicação Sem Fio;
- Rede de Telefonia Móvel;
- Redes de Dados Sem Fio.

Apesar das melhorias da tecnologia, as redes sem fio ainda são uma novidade, e diferentemente das redes que utilizam cabos, as quais necessitam de conhecimentos técnicos mais específicos, a montagem e a instalação de redes Wi-Fi podem ser efetuadas sem maiores problemas por um usuário iniciante. Essa facilidade, contudo, apresenta um risco associado, pois muitas instalações (caseiras ou não) estão sendo realizadas com padrões dos fabricantes, ou seja, completamente expostas a qualquer tipo de ataque.



## 12. Forense Computacional.

- Introdução e Conceitos;
- Aspectos Principais da Perícia Forense;
- Processos da Justiça;
- Princípios Forenses;
- Evasão Forense;
- Laudo Pericial.

Forense Computacional é o ramo da criminalística que compreende a aquisição, prevenção, restauração e análise de evidências computacionais, quer sejam os componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais. Na Figura 2.1 é apresentado um modelo proposto por Ubrich e Valle (2005), que procede de uma estrutura hierárquica de duas classes multiníveis (Aspectos Legais e Aspectos Técnicos).

## 13. Resposta a Incidentes:

- Questionamentos em Resposta a Incidentes;
- Processo de criação do CSIRT;
- Questões Estratégicas e Técnicas;
- Membros do CSIRT;
- Ferramentas usadas em CSIRT;
- Detecção de Intrusão em Sistemas.

A segurança da informação deixou de ser um problema exclusivo dos setores relacionados a TI, ou mesmo de uma organização, indústria ou governo em particular, para dar lugar a estratégias regionais e mundiais que permitam enfrentar, de forma organizada, as ameaças e vulnerabilidades que acompanham o uso da tecnologia.

É comprovada a eficiência dos grupos de resposta a incidente de segurança (do inglês, CSIRT) em prover uma resposta rápida e eficiente a incidentes de segurança. Ao reconhecer, analisar e responder mais rápido estes incidentes, os danos causados por eles também são reduzidos, bem como o custo para a sua recuperação.



#### 14. Segurança na Gestão de Pessoas:

- Abrangência na Gestão de Pessoas;
- Engenharia Social;
- Ameaças Internas e Externas;
- Motivação e Objetivos de um ataque;
- Boas Práticas em Gestão;
- Processo de Coleta de Dados Pessoais;
  - Análise do contratado (funcionário / terceirizado).
  - Análise prévia de perfis de usuários.
  - Conscientização das normas e procedimentos em segurança.
  - Controle de fluxo de informações por meio pessoal.
  - Análise do histórico do funcionário.
  - Aptidões profissionais e pessoais.

**Carga Horária:** 40 horas (08:30h às 17:30h) – 5 dias



Mini Currículo:



## 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. Dezenas de Entrevistas em Rádio, TV, Mídia Impressa e publicações online nos mais diversos canais de comunicação de cobertura regional e nacional no Brasil e Argentina como TV Globo, SBT, Valor Econômico, Estado de São Paulo, entre outros. Dentre as quais podemos acessar a seguinte, concedida à Record News:

<http://www.recordnewstv.com.br/linkbrasil/>

E outras notícias de destaque:

<http://www.usp.br/agen/bols/2006/rede1927.htm>

<http://revistaepoca.globo.com/Epoca/0,6993,EPT1111045-1881,00.html>

<http://www.datasecur.com.br/noticia.htm>

<http://g1.globo.com/Noticias/Tecnologia/0,,AA1295104-6174,00.html>

<http://www.nic.br/imprensa/clipping/2005/midia36.htm>

<http://www.internetsegura.org/noticias/noticias.asp?temp=5&id=201>

[http://gsisic.serpro.gov.br/noticias/Seguranca/20061002\\_01](http://gsisic.serpro.gov.br/noticias/Seguranca/20061002_01)

<http://www1.folha.uol.com.br/folha/informatica/ult124u21892.shtml>