

CompTIA Security+ : Curso de Preparação

A certificação Security+ da CompTIA (Associação das Indústrias de Tecnologia da Computação) é uma certificação “vendor-neutral” (não é direcionada a nenhum fabricante) que avalia o conhecimento e competência de profissionais técnicos que trabalham com Segurança da Informação. Profissionais que possuem a certificação CompTIA Security+ estão melhor preparados para prevenir incidentes de segurança e responder de forma efetiva, minimizando perdas quando violações ocorrem.

A certificação Security+ pode ser utilizada como uma prova eletiva para certificações especiais como MCSA Security e MCSE Security da Microsoft, bem como substitui um ano na comprovação de experiência de certificações como CISSP, SSCP e CSSLP do ISC².

Ao final do curso, uma prova simulada será aplicada e o aluno que obtiver a melhor nota da turma ganhará um voucher para fazer a prova oficial CompTIA Security+.

Quem irá se beneficiar com este curso?

Gerentes, técnicos, administradores e profissionais de Segurança da Informação, bem como profissionais de T.I. que possam se beneficiar do conhecimento em Segurança da Informação em suas atividades do dia-a-dia.

Metodologia de Ensino:

Através de uma abordagem teórica e prática, visando a cobertura de todos os assuntos cobrados na prova bem como exemplos e exercícios práticos de como este conhecimento pode ser aplicado ao dia-a-dia das organizações.

Pré-requisitos do Curso:

- Conhecimentos de TCP/IP
- Inglês técnico (slides e material do aluno em inglês)

Carga horária: 40 horas aula

Material do Curso:

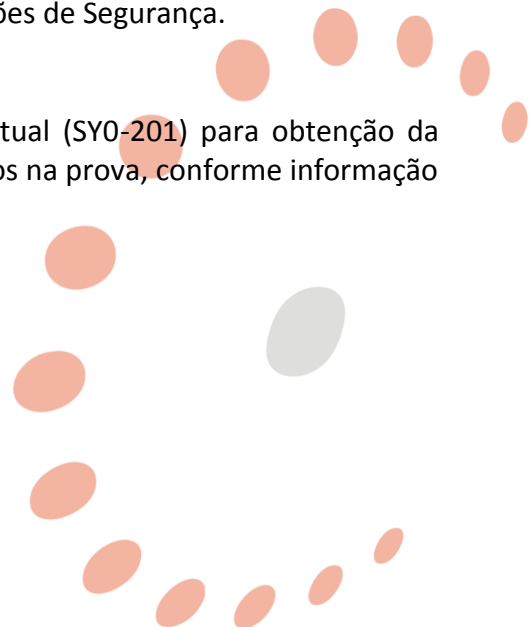
- Material utilizado é aprovado pela CompTIA como fonte de estudo pra a versão mais atual da prova.

Instrutores:

- Instrutores com certificação CISSP, com mais de 05 anos de experiência na área de Segurança da Informação, prestando consultoria, planejando e instalando soluções de Segurança.

Conteúdo Programático:

O curso espelha os requisitos e conteúdos cobrados no exame mais atual (SY0-201) para obtenção da certificação CompTIA Security+. A seguir são listados os objetivos cobrados na prova, conforme informação disponibilizada pela CompTIA.



Tópico	Assunto
Segurança de Sistemas	Diferenciar entre vários tipos de ameaça a sistemas
	Explicar os riscos de segurança relacionados a hardware e periféricos
	Implementar práticas de "hardening" de sistemas operacionais e procedimentos visando a segurança de servidores e estações de trabalho
	Aplicar procedimentos adequados relacionados a segurança de aplicações
	Implementação de aplicações de segurança
	Explicar o propósito e objetivos da tecnologia de virtualização de aplicações
Infra-Estrutura de Rede	Diferenciar entre os diferentes protocolos e suas portas, suas respectivas ameaças e medidas de segurança
	Distinguir entre elementos e componentes da arquitetura de rede
	Reconhecer o uso apropriado de ferramentas de segurança de redes para proteger o ambiente de rede
	Aplicar as medidas de segurança adequadas para proteger o ambiente de rede
	Explicar as vulnerabilidades e medidas de segurança relacionadas a equipamentos de rede
	Explicar vulnerabilidades e medidas de segurança relacionadas a alguns meios de transmissão
	Explicar vulnerabilidades e medidas de segurança associadas a redes Wireless
Controle de Acesso	Conhecer e aplicar as melhores práticas dos mecanismos de controle de acesso
	Conhecer os diferentes modelos de controle de acesso e suas diferenças
	Agrupar usuários e computadores em grupos de segurança e perfis de acesso, diferenciando o acesso e privilégio necessários
	Aplicar as medidas de segurança adequadas a compartilhamento de arquivos e impressoras
	Comparar e implementar os diversos mecanismos de controle de acesso
	Entender os diferentes modelos de autenticação e identificar os componentes de cada modelo
	Implementar vários mecanismos de autenticação e identificar seus componentes
	Explicar as diferenças entre identificar e autenticação
	Explicar e aplicar mecanismos de controle de acesso físico
Avaliação e Auditorias	Conduzir avaliação de riscos e mitigar riscos identificados
	Realizar análise de vulnerabilidade utilizando ferramentas
	Em relação a análises de vulnerabilidades, explicar o uso apropriado de testes de invasão versus análise de vulnerabilidade
	Utilização de ferramentas de monitoramento de sistemas e redes, detectando anomalias relacionadas a segurança
	Comparar e diferenciar os vários tipos de metodologias de monitoramento
	Executar procedimentos apropriados de armazenamento de logs e avaliar seus resultados
	Conduzir auditorias periódicas da segurança de sistemas
Criptografia	Explicar conceitos gerais de criptografia
	Explicar conceitos básicos de técnicas de hashing e uso apropriado dos algoritmos de hash
	Explicar conceitos básicos de técnicas de criptografia e uso apropriado dos algoritmos de criptografia
	Explicar e implementar protocolos
	Explicar os conceitos chave de uma Infra-Estrutura de Criptografia de Chave Pública
	Implementar PKI e gerência de certificados
Segurança da Organização	Explicar o planejamento de redundância e seus componentes
	Implementar procedimentos de recuperação de desastres
	Diferenciar e executar de forma apropriada procedimentos de resposta a incidentes
	Identificar e explicar legislações aplicáveis e política de segurança da organização
	Explicar a importância de medidas de segurança relacionadas ao ambiente de DataCenter
	Explicar conceitos e medidas de segurança contra engenharia social

Turmas disponíveis

Período	Dias	Horário
07/06/2010 à 18/06/2010	Segunda à Sexta	18:30 às 22:30
03/07/2010 à 11/09/2010	Sábado	08:00 às 12:00
19/07/2010 à 30/07/2010	Segunda à Sexta	18:30 às 22:30

Condições de pagamento:

- Facilitamos o pagamento, com desconto para pagamento à vista ou parcelamento em até 10 vezes sem juros no cartão ou boleto.

Certificado:

Serão emitidos certificados de participação para alunos que tiverem, no mínimo, 80% de presença.

Informações sobre a Prova da Certificação CompTIA Security+

Código do Exame (Versão 2008)	SY0-201
Quantidade de provas	Uma
Número de Questões	100
Formato da prova	Através do computador, com a possibilidade de retornar a questões anteriores não respondidas e revisar questões já respondidas.
Onde fazer a prova	Pode ser feita em um centro de testes Prometric ou VUE.
Duração da prova	90 minutos
Experiência Recomendada antes de fazer a prova (Não é necessário, porém recomendado)	<ul style="list-style-type: none">• Dois anos de experiência técnica em redes com ênfase em segurança• Treinamento e auto estudo adequado
Nota mínima para passar no teste	750 em uma escala de 100 a 900
Idioma da prova	Inglês ou espanhol

* O investimento necessário para fazer a prova SY0-201 é de USD 250,00, não incluso no valor do treinamento em questão.

INFORMAÇÕES:

E-mail: treinamento@coresec.com.br

Telefone: (85) 3458.3650

www.coresec.com.br