CISSP® – Certified Information Systems Security Professional (e-Learning)

ISC2

- **Nível:** Avançado
- **Duração:** 35h

Sobre o curso

O curso Certified Information Systems Security Professional (CISSP®) proporciona uma visão geral e abrangente dos conhecimentos necessários às fases de conceção, projeção e gestão de toda a posição de segurança de uma organização.

Este curso de formação irá ajudar os participantes na revisão e na atualização dos seus conhecimentos, bem como na identificação da matéria e das áreas que devem estudar para o exame CISSP.

O conteúdo programático do curso encontra-se em total sintonia com os oito domínios do CISSP Common Body of Knowledge (CBK®) da ISC2, uma vez que os abrange na sua totalidade de forma a garantir a igual importância de todas as áreas pertencentes ao campo da cibersegurança.

Todo o material didático empregue no curso é oficial e desenvolvido pela ISC2, a entidade criadora do CISSP CBK, assegurando, assim, que os conteúdos formativos se encontram atualizados e relevantes. Os nossos formadores são especialistas em segurança oficiais e acreditados como CISSP, que terão sido alvo de um período de treino e de formação intensivos a fim de estarem autorizados a lecionar os conteúdos da autoria da ISC2.

Destinatários

Este curso de formação destina-se a profissionais com pelo menos cinco anos de experiência remunerada em dois, ou mais, dos oito domínios do CISSP CBK da ISC2, que pretendam ter formação como CISSP e obter a certificação correspondente. A obtenção da mesma facultar-lhes-á credibilidade e mobilidade para avançarem nas suas atuais carreiras no ramo da segurança da informação. Ainda que não se limite unicamente aos cargos listados abaixo, esta formação é ideal para quem desempenha os seguintes cargos:

- Consultor de Segurança
- Gestor de Segurança
- Diretor/Gestor de TI
- Auditor de Segurança
- Arquiteto de Segurança
- Analista de Segurança

- Engenheiro de Sistemas de Segurança
- Chief Information Security Officer
- Diretor de Segurança
- Arquiteto de Redes

Objetivos

- Saber aplicar conceitos e métodos fundamentais relativos às áreas da tecnologia e da segurança informática.
- Conseguir alinhar os objetivos operacionais da organização com as funções e as implementações de segurança.
- Determinar as melhores maneiras de proteger os ativos de uma organização à medida que estes atravessam o seu ciclo de vida.
- Saber identificar e aplicar os conceitos, princípios, estruturas e normas utilizados para desenhar, implementar, monitorizar e implementar segurança em sistemas operativos, equipamentos, redes, aplicações e nos controlos utilizados no garante dos vários níveis de confidencialidade, integridade e disponibilidade.
- Saber aplicar os princípios de design de segurança que permitem selecionar as mitigações mais adequadas às vulnerabilidades presentes nos tipos e arquiteturas de sistemas de informação mais comuns.
- Saber explicar a importância da criptografia e dos serviços de segurança que a mesma proporciona na corrente era digital.
- Conseguir avaliar os elementos de segurança física necessários face às necessidades de segurança da informação existentes.
- Conseguir avaliar os elementos que constituem a segurança da comunicação e de redes face às necessidades de segurança da informação existentes.
- Saber identificar e aplicar os conceitos e a arquitetura que definem a tecnologia e os sistemas e protocolos de implementação nas camadas 1-7 do modelo Open Systems Interconnection (OSI) adequados às necessidades de segurança da informação existentes.
- Determinar os modelos de controlo de acesso adequados aos requisitos de segurança existentes numa empresa.
- Saber aplicar controlos de acesso físico e lógico adequados às necessidades de segurança da informação existentes.
- Conseguir distinguir os principais métodos de conceção e de validação de estratégias de teste e de auditoria que melhor apoiem os requisitos de segurança da informação existentes.
- Saber aplicar controlos e contramedidas de segurança adequados de modo a otimizar tanto a função como a capacidade operacional de uma organização.
- Conseguir avaliar os riscos dos sistemas de informação que poderão afetar as atividades operacionais de uma organização.
- Determinar os métodos de controlo mais adequados para mitigar ameaças e vulnerabilidades específicas.
- Saber aplicar conceitos de segurança de sistemas de informação para mitigar o risco de vulnerabilidades de software e de sistemas ao longo do ciclo de vida dos sistemas.

Condições

Notas

O exame incluído no curso é presencial e realiza-se num centro Pearson VUE Select, como o da Rumos em Lisboa.

Para particulares
• 10% do valor total pago no ato da inscrição; restante valor até 7 dias antes do início do curso.
• Formandos não residentes em Portugal: pagamento de 50% no ato da inscrição; restante valor até 7 dias antes do início do curso.
• Possibilidade de beneficiar do Cheque Formação+Digital até 750€ (conforme elegibilidade).
• Isenção de IVA para particulares.
Para empresas
• Empresas nacionais: pagamento a 30 dias, contra fatura (acresce IVA à taxa legal em vigor).
• Empresas da UE e fora da UE: valores isentos de IVA e pagamento a pronto.

Pré-requisitos

Ter pelo menos cinco anos de experiência remunerada em dois, ou mais, dos oito domínios do CISSP CBK da ISC2.

Metodologia

A Formação Oficial ISC2 Online Self-Paced CISSP constitui uma forma inovadora de preparação para a certificação que utiliza inteligência artificial para personalizar o teu percurso de aprendizagem. Identifica as áreas que exigem foco adicional e orienta-te na preparação para o exame de forma verdadeiramente personalizada.

Estuda de forma mais inteligente com estas principais vantagens:

- **Instrução personalizada** – O conteúdo, o ritmo e a dificuldade adaptam-se ao teu nível de conhecimento, velocidade de aprendizagem e nível de confiança.
- **Maior envolvimento** – Feedback imediato e conteúdo dinâmico permitem-te aprender a um nível adequado.
- **Poupança de tempo** – O tempo de formação é otimizado ao focar-se nas áreas que exigem maior revisão.
- **Melhores resultados de aprendizagem** – A plataforma identifica as áreas que exigem revisão adicional e disponibiliza suporte direcionado para maximizar a tua compreensão do conteúdo.

A formação Certified Information Systems Security Professional (CISSP) tira partido do poder da inteligência

artificial, orientando os formandos numa experiência de aprendizagem ao seu ritmo, adaptada às suas necessidades. Abrange os conhecimentos e competências necessários para desenhar, desenvolver e gerir a postura global de segurança de uma organização.

Programa

- O Ambiente de Segurança Informática
- Segurança dos Ativos de Informação
- Gestão de Identidade e de Acesso (IAM)
- Arquitetura e Engenharia de Segurança
- Segurança da Comunicação e Redes
- Segurança do Desenvolvimento de Software
- Avaliação e Testes de Segurança
- Operações de Segurança
- Tudo em Conjunto

O Ambiente de Segurança Informática

- Justificar um código de ética organizacional.
- Relacionar os princípios de confidencialidade, integridade, disponibilidade, não-repúdio, autenticação, privacidade e segurança com os princípios de devido cuidado e diligência devida.
- Relacionar governança de segurança da informação com as estratégias de negócio, as metas, as missões e os objetivos organizacionais.
- Aplicar conceitos de cibercrime a situações de violação de dados e a outras situações que comprometam a segurança da informação.
- Relacionar os requisitos legais, contratuais e regulamentares de privacidade e proteção de dados de acordo com os objetivos de segurança da informação.
- Relacionar a circulação transfronteiriça de dados e as questões de importação-exportação de acordo com a proteção de dados, a privacidade e a proteção da propriedade intelectual.

Segurança dos Ativos de Informação

- Relacionar os modelos de gestão de ativos de TI e de ciclo de vida de segurança de dados com a segurança da informação.
- Explicar a utilização da classificação e da categorização da informação, como dois processos distintos mas relacionados.
- Descrever os diferentes estados dos dados e as suas considerações em matéria de segurança da informação.
- Descrever os diferentes cargos diretamente envolvidos no uso da informação e as considerações de segurança para os mesmos.
- Descrever os diferentes tipos e categorias de controlos de segurança da informação e a sua utilização.
- Selecionar as normas de segurança de dados adequadas aos requisitos de conformidade da organização.

Gestão de Identidade e de Acesso (IAM)

- Explicar o ciclo de vida de identidade e como se aplica a utilizadores humanos e não humanos.
- Comparar e contrastar modelos, mecanismos e conceitos de controlo de acesso.
- Explicar o papel da autenticação, autorização e contabilidade no alcance de metas e objetivos de segurança da informação.
- Explicar como as implementações de IAM devem proteger os ativos físicos e lógicos.
- Descrever o papel das credenciais e do armazenamento de identidade nos sistemas IAM.

Arquitetura e Engenharia de Segurança

- Descrever os principais componentes das normas de engenharia de segurança.
- Explicar os principais modelos de arquitetura para a segurança da informação.
- Explicar as capacidades de segurança implementadas no hardware e no firmware.
- Aplicar princípios de segurança a diferentes arquiteturas de sistemas de informação e respetivos ambientes.
- Determinar a melhor aplicação de abordagens criptográficas para resolver as necessidades de segurança da informação organizacional.
- Gerir a utilização de certificados e de assinaturas digitais adequados às necessidades organizacionais de segurança da informação.
- Descobrir as implicações da não utilização de técnicas criptográficas para proteger a cadeia de abastecimento.
- Aplicar diferentes soluções de gestão criptográfica adequadas às necessidades organizacionais de segurança das informação.
- Verificar se as soluções criptográficas estão a funcionar e a responder à evolução das ameaças do mundo real.
- Descrever as defesas contra ataques criptográficos comuns.
- Desenvolver uma lista de verificação de gestão para determinar o estado de saúde e a prontidão criptográfica de uma organização.

Segurança da Comunicação e Redes

- Descrever as características arquitetónicas, as tecnologias relevantes, os protocolos e as considerações de segurança de cada uma das camadas do modelo OSI.
- Explicar a aplicação de práticas de conceção seguras no desenvolvimento de infraestruturas de rede.
- Descrever a evolução dos métodos de segurança dos protocolos de comunicação IP.
- Explicar as implicações de segurança dos ambientes de rede ligados (cabo e fibra) e não ligados (sem fios).
- Descrever a evolução e as implicações de segurança dos principais dispositivos de rede.
- Avaliar e contrastar os problemas de segurança das comunicações de voz em infra-estruturas tradicionais e VoIP.
- Descrever e contrastar as considerações de segurança para as principais tecnologias de acesso remoto.
- Explicar as implicações de segurança das tecnologias de rede definida por software (SDN) e de virtualização de rede.

Segurança do Desenvolvimento de Software

- Reconhecer os muitos elementos de software que podem pôr em risco a segurança dos sistemas de

informação.
- Identificar e explicar as principais causas de fragilidades de segurança no código-fonte.
- Explicar as principais causas de fragilidades de segurança em sistemas de base de dados e de data warehouse.
- Esclarecer a aplicabilidade da estrutura OWASP a diversas arquiteturas web.
- Selecionar estratégias de mitigação de malware adequadas às necessidades organizacionais de segurança da informação.
- Comparar as formas como diferentes metodologias, estruturas e directrizes de desenvolvimento de software contribuem para a segurança dos sistemas.
- Explicar a implementação de controlos de segurança para ecossistemas de desenvolvimento de software.
- Escolher uma combinação adequada de testes de segurança, avaliação, controlos e métodos de gestão para diferentes sistemas e ambientes de aplicações.

Avaliação e Testes de Segurança

- Descrever a finalidade, o processo e os objetivos da avaliação e dos testes de segurança formais e informais.
- Aplicar a ética profissional e organizacional à avaliação e aos testes de segurança.
- Explicar a avaliação e os testes internos, externos e de terceiros.
- Explicar as questões de gestão e de governança relacionadas com o planeamento e a realização de avaliações de segurança.
- Explicar o papel da avaliação na tomada de decisões de segurança baseadas em dados.

Operações de Segurança

- Demostrar como se recolhe e avalia dados de segurança de forma eficiente e eficaz.
- Explicar os benefícios de segurança de uma gestão e controlo eficazes das alterações.
- Desenvolver políticas e planos de resposta a incidentes.
- Relacionar a resposta a incidentes com as necessidades de controlo de segurança e a sua utilização operacional.
- Relacionar os controlos de segurança com a melhoria e a obtenção da disponibilidade necessária dos bens e sistemas de informação.
- Compreender as ramificações de segurança e de proteção de diferentes instalações, sistemas e características de infraestruturas.

Tudo em Conjunto

- Explicar como os frameworks e os processos de governança se relacionam com a utilização operacional dos controlos de segurança da informação.
- Relacionar o processo de realização de investigações forenses com as operações de segurança da informação.
- Relacionar a continuidade do negócio e a preparação para a recuperação de desastres com as operações de segurança da informação.
- Explicar como utilizar a educação, a formação, a consciencialização e o envolvimento de todos os membros da organização como forma de reforçar e aplicar os processos de segurança da informação.
- Demostrar como se operacionaliza os sistemas de informação e a gestão de riscos da cadeia de

fornecimento de TI.