Certified Information Systems Auditor® (CISA®) – e-learning

ISACA

- **Nível:**
- **Duração:** 22h

Sobre o curso

A certificação CISA – Certified Information Systems Auditor, é uma credencial globalmente reconhecida que assenta na experiência de profissionais de SI, para os capacitar com elevados conhecimentos em Auditoria, Controlo e Segurança de Sistemas de Informação.

Neste curso os participantes irão abordar os 5 Domínios da Auditoria de Segurança da Informação. Estes domínios constituem as bases do CISA e é imperativo que os participantes adquiram uma compreensão completa destes aspetos para passarem com sucesso no exame CISA e utilizarem a certificação na sua organização.

Os 5 domínios do CISA:

- O Processo de Auditoria de Sistemas de Informação
- Governação e Gestão de IT
- Aquisição, Desenvolvimento e Implementação de Sistemas de Informação
- Operações, Manutenção e Suporte de Sistemas de Informação
- Proteção dos Ativos de Informação

A certificação CISA é DoD Approved 8570 Baseline Certification e cumpre os requisitos de formação DoD 8140/8570.

Destinatários

A certificação CISA é essencial para profissionais que lidam com o controlo, monitorização e avaliação da tecnologia da informação e dos sistemas de negócio de uma organização. Isto inclui:

- Auditores/consultores de SI/IT
- Gestores de compliance de IT
- Chief Compliance Officers
- Chief Risk & Privacy Officers
- Responsáveis/diretores de segurança
- Gestores/arquitetos de segurança

Objetivos

- Compreender o processo de auditoria de Sistemas de Informação e aplicar os seus princípios em diferentes contextos organizacionais.
- Identificar práticas de governação e gestão de IT que suportem o alinhamento entre tecnologia, controlo e objetivos de negócio.
- Analisar os processos de aquisição, desenvolvimento e implementação de Sistemas de Informação, assegurando o cumprimento de requisitos, controlos e boas práticas.
- Avaliar operações, manutenção e suporte de Sistemas de Informação, com foco na continuidade, desempenho e fiabilidade dos serviços.
- Reconhecer os principais mecanismos de proteção dos ativos de informação, incluindo políticas, controlos e medidas de segurança adequadas.

Condições

- Inclui respetivo exame de certificação

Pré-requisitos

Este curso não é adequado para iniciantes. É exigido que os participantes possuam, pelo menos, cinco anos de experiência na área de Auditoria de Sistemas de Informação. Espera-se que os candidatos tenham um nível elevado de experiência profissional, compromisso e conhecimento aprofundado em Auditoria de SI.

Metodologia

Este curso tem uma duração aproximada de 22 horas assíncronas e é acedido através da plataforma da ISACA. Os formandos após a conclusão do curso obterão 26.5 CPE. Os conteúdos estão disponíveis em Inglês.

Programa

- Processo de Auditoria de Sistemas de Informação
- Governação e Gestão de IT
- Aquisição, Desenvolvimento e Implementação de Sistemas de Informação
- Operações, Manutenção e Suporte de Sistemas de Informação
- Proteção dos Ativos de Informação

Domínio 1: Processo de Auditoria de Sistemas de Informação

- Desenvolvimento de uma estratégia de auditoria de IT baseada no risco
- Planeamento de auditorias específicas
- Realização de auditorias de acordo com standards de auditoria de SI

- Implementação de práticas de gestão de risco e controlo

Domínio 2: Governação e Gestão de IT

- Eficácia da estrutura de Governação de IT
- Estrutura organizacional de IT e gestão de recursos humanos (pessoal)
- Políticas, standards e procedimentos de IT da organização
- Adequação do Sistema de Gestão da Qualidade
- Controlos de gestão e monitorização de IT
- Investimento em recursos de IT
- Estratégias e políticas de contratação de IT
- Gestão dos riscos da organização relacionados com IT
- Práticas de monitorização e assurance
- Plano de continuidade de negócio da organização

Domínio 3: Aquisição, Desenvolvimento e Implementação de Sistemas de Informação

- Desenvolvimento de business cases para aquisição, desenvolvimento, manutenção e descontinuação de SI
- Práticas e controlos de gestão de projetos
- Realização de revisões às práticas de gestão de projetos
- Controlos para as fases de requisitos, aquisição, desenvolvimento e testes
- Prontidão para Sistemas de Informação
- Revisão do Plano de Projeto
- Revisões ao Sistema Pós-Implementação

Domínio 4: Operações, Manutenção e Suporte de Sistemas de Informação

- Realização de revisões periódicas aos objetivos das organizações
- Gestão de níveis de serviço
- Práticas de gestão de terceiros
- Operações e procedimentos do utilizador final
- Processo de manutenção de sistemas de informação
- As práticas de administração de dados determinam a integridade e a otimização das bases de dados
- Utilização de ferramentas e técnicas de monitorização de capacidade e desempenho
- Práticas de gestão de problemas e incidentes
- Práticas de gestão da mudança, configuração e releases
- Adequação das medidas de backup e restore
- Plano de recuperação de desastres da organização em caso de desastre

Domínio 5: Proteção dos Ativos de Informação

- Políticas, standards e procedimentos de segurança da informação
- Conceção, implementação e monitorização de controlos de segurança de sistemas e lógica
- Conceção, implementação e monitorização de processos e procedimentos de classificação de dados
- Conceção, implementação e monitorização de controlos de acesso físico e ambientais
- Processos e procedimentos para armazenar, recuperar, transportar e eliminar ativos de informação