Certified Information Security Manager® (CISM®)

ISACA

Com certificação

- **Nível:**
- **Duração:** 16h

Sobre o curso

A certificação CISM Certified Information Security Manager, centra-se na construção, desenvolvimento e governação das operações de segurança da informação. Deter esta certificação demonstra conhecimento aprofundado, prática e uma vasta experiência no domínio da gestão da segurança da informação.

Este curso tem em conta questões práticas, como a criação de programas de segurança da informação e a gestão de incidentes, promovendo simultaneamente práticas de segurança utilizadas a nível global. O CISM ensina os participantes a adaptar a tecnologia em constante mudança às suas organizações. Isto permite que as organizações se destaquem como uma organização valiosa e possam expandir a sua base de clientes devido à implementação de profissionais certificados em CISM.

A procura de profissionais qualificados em gestão da segurança da informação está a aumentar, pelo que esta certificação da ISACA responde às necessidades das empresas. O CISM foi aceite como a norma universal a alcançar na área da segurança da informação, representando esta qualificação uma referência de destaque em termos de especialização e compromisso. Isto faz com que os detentores de CISM sejam identificados como profissionais altamente certificados na área da segurança da informação e permite que os participantes reconheçam a ligação entre os programas de segurança da informação e os objetivos mais amplos da organização.

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

Destinatários

O CISM destina-se a profissionais de segurança da informação com, pelo menos, cinco anos de experiência profissional relevante e, no mínimo, três anos na função de gestor de segurança da informação. Os cargos incluem:

- CISO

- CSO
- Segurança
- Diretor/Gestor/Consultor
- Diretor/Gestor/Consultor de IT
- Diretor e Gestor de Compliance/Risco/Privacidade

Objetivos

- Explicar a relação entre a liderança executiva, a governação empresarial e a governação da segurança da informação.
- Descrever os componentes utilizados para construir uma estratégia de segurança da informação.
- Explicar como o processo de avaliação de risco influencia a estratégia de segurança da informação.
- Articular o processo e os requisitos utilizados para desenvolver uma estratégia eficaz de resposta ao risco da informação.
- Descrever os componentes de um programa eficaz de segurança da informação.
- Explicar o processo para criar e manter um programa empresarial de segurança da informação.
- Descrever as técnicas utilizadas para avaliar a capacidade e a preparação da organização para gerir um incidente de segurança da informação.
- Descrever métodos para medir e melhorar as capacidades de resposta e recuperação.

Condições

- Inclui respetivo exame de certificação

Pré-requisitos

Para obter a certificação CISM é exigida uma experiência profissional mínima de 5 anos em auditoria, controlo ou segurança de sistemas de informação.

Metodologia

Este curso tem uma duração aproximada de 16 horas assíncronas e é acedido através da plataforma da ISACA. Os formandos obterão 20 CPE após a conclusão. Os conteúdos estão disponíveis em Inglês.

Programa

- Governação da Segurança da Informação
- Gestão do Risco da Informação e Compliance
- Desenvolvimento e Gestão do Programa de Segurança da Informação

- Gestão de Incidentes de Segurança da Informação

Domínio 1 – Governação da Segurança da Informação

- Introdução à Governação da Segurança da Informação
- Governação Eficaz da Segurança da Informação
- Governação e Relações com Terceiros
- Métricas de Segurança da Informação
- Métricas de Governação da Segurança da Informação
- Estratégia de Segurança da Informação
- Desenvolvimento da Estratégia de Segurança da Informação
- Recursos e Restrições da Estratégia
- Outros Frameworks
- Compliance
- Planos de Ação para Implementar a Estratégia
- Governação de IT Empresarial

Domínio 2 – Gestão do Risco da Informação e Compliance

- Gestão do Risco da Informação
- Visão Geral da Gestão de Risco
- Avaliação de Risco
- Classificação de Ativos de Informação
- Gestão da Avaliação
- Valorização dos Recursos de Informação
- Objetivos de Tempo de Recuperação
- Baselines de Controlo de Segurança
- Monitorização do Risco
- Formação e Sensibilização
- Documentação da Gestão do Risco da Informação

Domínio 3 – Desenvolvimento e Gestão do Programa de Segurança da Informação

- Visão Geral da Gestão do Programa de Segurança da Informação
- Objetivos do Programa de Segurança da Informação
- Conceitos do Programa de Segurança da Informação
- Recursos Tecnológicos do Programa de Segurança da Informação
- Desenvolvimento do Programa de Segurança da Informação
- Framework do Programa de Segurança da Informação
- Roadmap do Programa de Segurança da Informação
- Enterprise Information Security Architecture (EISA)
- Gestão e Administração do Programa de Segurança
- Serviços e Atividades Operacionais do Programa de Segurança
- Controlos
- Métricas e Monitorização do Programa de Segurança
- Medição do Desempenho Operacional

- Desafios Comuns dos Programas de Segurança da Informação

Domínio 4 – Gestão de Incidentes de Segurança da Informação

- Visão Geral da Gestão de Incidentes
- Procedimentos de Gestão de Incidentes
- Recursos de Gestão de Incidentes
- Objetivos da Gestão de Incidentes
- Métricas e Indicadores de Gestão de Incidentes
- Definição de Procedimentos de Gestão de Incidentes
- Procedimentos de Continuidade de Negócio e Recuperação de Desastres
- Atividades Pós-Incidente e Investigação
- Código de Ética Profissional da ISACA
- Leis e Regulamentos
- Política versus Lei numa Organização
- Ética e a Internet IAB
- Certified Information Security Manager