Advanced in AI Security Management™ (AAISM™)

ISACA

- **Nível:**
- **Duração:** 11h

Sobre o curso

A certificação AAISM – Advanced in AI Security Management, capacita líderes de segurança com conhecimentos e a capacidade necessária para governar, proteger e gerir sistemas de AI empresariais.

Os formandos irão adquirir uma compreensão aprofundada da governação de AI, da gestão de risco em AI e das tecnologias e controlos que sustentam operações de AI seguras e éticas.

Este curso alinha-se com os frameworks globalmente reconhecidos da ISACA, capacitando os profissionais para identificar, avaliar, monitorizar e mitigar riscos relacionados com AI, assegurando simultaneamente uma adoção responsável e compliant da AI em toda a organização.

Destinatários

- Gestores e consultores experientes em segurança da informação
- Profissionais de governação, risco e compliance que trabalham com tecnologias de AI
- Líderes de cibersegurança responsáveis por proteger ambientes empresariais de AI
- Organizações que procuram estabelecer ou maturar práticas de gestão de segurança de AI

Objetivos

- Demonstrar proficiência na gestão de frameworks de governação e estruturas de programa específicas de AI
- Avaliar estratégias de gestão de risco em AI e desenvolver planos de tratamento eficazes
- Avaliar tecnologias, arquiteturas e controlos de AI para uma utilização segura e ética
- Alinhar a governação de AI com as políticas de segurança empresariais e as normas regulamentares
- Estabelecer métricas de risco (KRIs e KPIs) para supervisão e reporting contínuos de AI
- Conceber e implementar programas de segurança de AI consistentes com as normas ISACA e ANSI
- Apoiar o planeamento de continuidade de negócio e de resposta a incidentes específico para ambientes orientados por AI

Condições

- Inclui respetivo exame de certificação

Pré-requisitos

- Possuir a certificação ISACA CISM ou ISC2 CISSP
- Experiência comprovada em funções de segurança ou consultoria
- Compreensão fundamental da avaliação, implementação e manutenção de sistemas de AI

Metodologia

Este curso tem uma duração aproximada de 11 horas assíncronas e é acedido através da plataforma da ISACA. Os formandos após a conclusão do curso obterão 11 CPE. Os conteúdos estão disponíveis em Inglês.

Programa

- Governação de AI e gestão do programa
- Gestão de risco de AI
- Tecnologias e controlos de AI

Domínio 1. Governação de AI e gestão do programa

- Considerações relativas às partes interessadas, frameworks e requisitos regulamentares
- Estrutura organizacional, papéis e modelos de governação
- Definição de charters e estabelecimento de comités diretivos de AI
- Apetência pelo risco, tolerância e alinhamento com frameworks
- Seleção e aplicação de frameworks de governação de AI adequados
- Desenvolvimento de use cases de negócio em AI e gestão das implicações de privacidade
- Estabelecimento de estratégias, políticas e procedimentos de AI
- Utilização responsável e aceitável de sistemas de AI
- Gestão de ativos de AI e ciclos de vida dos dados
- Criação de inventários de ativos de AI e protocolos de gestão de dados
- Documentação, classificação e práticas de armazenamento de modelos
- Implementação de medidas de proteção e destruição de dados de AI
- Criação de um programa de gestão de segurança de AI
- Estabelecimento de planos documentados, papéis das equipas e standards de proficiência
- Integração de ferramentas de segurança com AI e métricas de desempenho
- Desenvolvimento de KRIs e KPIs para medir a eficácia da segurança de AI
- Gestão da continuidade de negócio e da resposta a incidentes para AI

- Implementação de processos específicos de AI para deteção, notificação e escalamento
- Conceção de playbooks de resposta a AI e protocolos de red-button
- Definição de objetivos de recuperação (RTO e RPO) numa perspetiva de AI

Domínio 2. Gestão de risco de AI

- Realização de avaliações de risco de AI e definição de limiares de risco aceitável
- Realização de avaliações de impacto, conformidade e impacto na privacidade (PIAs)
- Desenvolvimento de planos de tratamento e documentação de respostas ao risco específicas de AI
- Implementação de penetration testing, testes de vulnerabilidades e red teaming focados em AI
- Gestão de ameaças adversariais e internas em ecossistemas de AI
- Identificação de ameaças com recurso a AI, deepfakes e utilização indevida de dados sintéticos
- Aplicação de threat intelligence a cadeias de ataque baseadas em AI e deteção de anomalias
- Gestão do risco de fornecedores e da cadeia de abastecimento de AI
- Realização de due diligence e definição de accountability entre fornecedor e entidade implementadora
- Gestão de dependências em pacotes e bibliotecas de software de AI
- Estabelecimento de SLAs, propriedade e considerações de IP para sistemas de AI
- Implementação de processos de controlo de acessos, responsabilidade e monitorização de fornecedores

Domínio 3. Tecnologias e controlos de AI

- Conceção de arquitetura de segurança de AI alinhada com princípios secure-by-design
- Gestão do controlo de alterações em AI e de ciclos de vida de desenvolvimento seguro (SDL)
- Proteção de infrastructure-as-code e interconectividade de modelos
- Gestão dos ciclos de vida dos modelos de AI, incluindo seleção, treino, validação e testes de regressão
- Implementação de technical evaluation, verification, and validation (TEVV) de modelos de AI
- Aplicação de controlos de gestão de dados para mitigar data poisoning, enviesamento e problemas de precisão
- Gestão de controlos de privacidade, ética, confiança e segurança em sistemas de AI
- Garantia de explicabilidade, consentimento, transparência e equidade na tomada de decisão com AI
- Manutenção de supervisão humana (human-in-the-loop) em processos automatizados
- Aplicação de medidas de confiança e segurança, como content moderation e prevenção de danos
- Monitorização do impacto ambiental e garantia de minimização e anonimização de dados
- Conceção e implementação de controlos de segurança de AI e processos de monitorização contínua
- Mapeamento de ameaças de segurança de AI para controlos e métricas
- Implementação de ciclos de vida de controlo e self-assessments (CSA)
- Disponibilização de formação de sensibilização para segurança de AI para impulsionar a preparação organizacional