CC® – Certified in Cybersecurity

ISC2

Promoção: **Curso com 10% de desconto**Aproveite já!

Live Training (também disponível em presencial)

- **Localidade:**
- **Data:** 28 Sep 2026
- **Preço:** 1900 € (Isento de IVA para Particulares)
- **Horário:** Laboral das 09h00 - 18h00
- **Nível:** Entrada
- **Duração:** 24h

Sobre o curso

O curso CC – Certified in Cybersecurity prepara-te para desenvolver os conhecimentos fundamentais de cibersegurança necessários para iniciar um percurso profissional nesta área e para realizar o exame de certificação Certified in Cybersecurity (CC).

Ao longo da formação são abordados princípios fundamentais de segurança e gestão de risco, governance, Identity and Access Management (IAM), segurança de redes e cloud, proteção de dados, operações de segurança, resposta a incidentes e testes de segurança. O programa encontra-se alinhado com o exame Certified in Cybersecurity (CC), permitindo desenvolver uma base transversal de conhecimentos relevante para funções de cibersegurança de nível inicial ou junior.

A certificação CC valida conhecimentos, competências e capacidades fundamentais para o desempenho de funções de entrada na área de cibersegurança e constitui também um ponto de partida para continuares a evoluir para certificações ISC2 mais avançadas.

Por não exigir experiência profissional prévia em cibersegurança nem formação académica específica, o CC é particularmente indicado para quem pretende dar os primeiros passos nesta área, bem como para profissionais que pretendam adquirir uma base estruturada de conhecimentos de cibersegurança.

Destinatários

Este curso destina-se a pessoas que pretendem iniciar ou desenvolver conhecimentos fundamentais na área de cibersegurança e preparar-se para a certificação **ISC2 Certified in Cybersecurity (CC)**.

É particularmente indicado para:

- Estudantes e recém-graduados que pretendam iniciar uma carreira em cibersegurança;
- Jovens profissionais em início de carreira;
- Profissionais de Tecnologias de Informação que pretendam desenvolver competências em cibersegurança;
- Profissionais em processo de reconversão para a área de cibersegurança;
- Profissionais que desempenhem ou pretendam desempenhar funções de cibersegurança de nível inicial ou junior;
- Outros profissionais que pretendam adquirir conhecimentos fundamentais de segurança para aplicar no seu contexto profissional.

Objetivos

- Compreender os princípios fundamentais de cibersegurança, gestão de risco e governance;
- Identificar os principais tipos de controlos de segurança e compreender a importância da ética e da conduta profissional;
- Compreender conceitos fundamentais de Governance, Risk and Compliance (GRC), Business Continuity e Disaster Recovery;
- Reconhecer os princípios de Identity and Access Management (IAM) e dos principais modelos de controlo de acesso;
- Compreender conceitos fundamentais de redes, segmentação, Defense in Depth, Zero Trust e segurança cloud;
- Identificar princípios e práticas de proteção de dados, encryption e gestão de ativos;
- Compreender atividades fundamentais de Security Operations, monitorização e Cyber Threat Intelligence;
- Reconhecer os princípios e processos fundamentais de Incident Response;
- Identificar diferentes abordagens de security testing e avaliação da segurança;
- Preparar-te para o exame de certificação **ISC2 Certified in Cybersecurity (CC)**.

Pré-requisitos

Não são exigidos conhecimentos profissionais prévios em cibersegurança nem uma formação académica específica para frequentar o curso ou realizar o exame **Certified in Cybersecurity (CC)**.

São, no entanto, recomendados conhecimentos básicos de Tecnologias de Informação.

A certificação CC foi desenvolvida como uma credencial de entrada na área, não sendo necessária experiência profissional prévia em cibersegurança nem diploma ou grau académico para realizar o exame.

Programa

- Princípios de Segurança
- Governance de Segurança
- Conceitos de Identity and Access Management (IAM)
- Conceitos de Segurança de Redes e Cloud

- Operações de Segurança e Resposta a Incidentes

Princípios de Segurança

- Compreender os conceitos de cibersegurança
    - Confidencialidade
    - Integridade
    - Disponibilidade
    - Autenticação, Autorização e Accounting (AAA)
    - Não repúdio
    - Privacidade
- Compreender os conceitos de gestão de risco
    - Ciclo de vida da gestão de risco
    - Processos de gestão de risco
- Compreender os conceitos de governance
    - Regulamentos e legislação
    - Frameworks e orientações
    - Políticas, normas (por exemplo, International Organization for Standardization (ISO) e Center for Internet Security) e procedimentos
- Compreender os controlos de cibersegurança
    - Controlos técnicos
    - Controlos administrativos
    - Controlos físicos
- Manter uma conduta profissional e ética
    - Código de conduta profissional
    - Due care e due diligence
    - Código de Ética da ISC2

Governance de Segurança

- Planear Governance, Risk and Compliance (GRC)
    - Objetivo
    - Importância
    - Frameworks e ferramentas
- Compreender a redundância
    - Continuidade de Negócio (Business Continuity – BC)
    - Recuperação de Desastres (Disaster Recovery – DR)
- Compreender a sensibilização para a segurança
    - Cultura organizacional (por exemplo, importância da segurança e liderança em segurança)
    - Conceitos como engenharia social, proteção de palavras-passe e phishing
- Medir a eficácia da cibersegurança
    - Métricas-chave e Key Risk Indicators (KRI)
    - Dashboards, scorecards e relatórios

Conceitos de Identity and Access Management (IAM)

- Compreender a gestão do ciclo de vida das identidades
    - Definição de funções
    - Provisioning
    - Revisão
    - Deprovisioning
    - Frameworks e ferramentas
- Compreender os controlos de acesso lógico
    - Princípio do Menor Privilégio (Principle of Least Privilege – PoLP)
    - Segregação de Funções (Separation of Duties – SoD)
    - Modelos de controlo de acesso

Conceitos de Segurança de Redes e Cloud

- Compreender a segurança de redes
    - Conceitos como modelo Open Systems Interconnection (OSI), modelo Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6) e Virtual Private Network (VPN)
    - Firewalls (por exemplo, portas e aplicações)
    - Redes wireless (por exemplo, Wi-Fi e Bluetooth)
    - Sistemas embebidos (por exemplo, Industrial Control Systems (ICS) e Internet of Things (IoT))
- Compreender a arquitetura de segurança de redes
    - Segmentação de redes (por exemplo, zonas de firewall, Virtual Local Area Network (VLAN) e microssegmentação)
    - Defense in Depth
    - Zero Trust (ZT)
- Compreender a segurança cloud
    - Características (por exemplo, acesso amplo à rede, elasticidade rápida, serviço mensurável, self-service on-demand e partilha de recursos)
    - Modelos de serviço
    - Modelos de implementação
    - Modelo de responsabilidade partilhada (por exemplo, funções e responsabilidades)

Operações de Segurança e Resposta a Incidentes

- Compreender a segurança dos dados
    - Tratamento de dados (por exemplo, classificação, etiquetagem, masking e sanitização)
    - Criptografia (por exemplo, criptografia simétrica e assimétrica, hashing e criptografia resistente a computação quântica)
- Compreender as operações de segurança
    - Registo e monitorização de eventos de segurança
    - Triagem de eventos de segurança (por exemplo, casos de uso de incidentes, priorização e correlação)
    - Atores de ameaça (por exemplo, tipos e motivações)
    - Cyber Threat Intelligence
    - Frameworks de ameaças
- Compreender a Resposta a Incidentes (Incident Response – IR)

    - Implementação da política de tratamento de dados no Plano de Resposta a Incidentes (Incident Response Plan – IRP)
    - Exercícios de Resposta a Incidentes (por exemplo, testes e exercícios tabletop)
- Compreender a proteção de ativos
    - Gestão do ciclo de vida dos ativos (por exemplo, software e dispositivos em End of Life – EOL)
    - Gestão de configuração e de alterações
- Compreender os testes de segurança
    - Testes de preparação de segurança (por exemplo, blue teaming, purple teaming e red teaming)
    - Testes de aplicações (por exemplo, vulnerability scanning, análise estática, análise dinâmica e threat modeling)
    - Testes físicos de penetração (por exemplo, phishing, tailgating e impersonation)