CC® – Certified in Cybersecurity

ISC2

- **Nível:** Entrada
- **Duração:** 8h

Sobre o curso

Take the first step to a rewarding career with Certified in Cybersecurity (CC) from ISC2, the world's leading cybersecurity professional organization.

To help close the workforce gap, ISC2 recently launched the Certified in Cybersecurity (CC) entry-level certification. With no experience required, it opens opportunities in the field to a much broader range of candidates, including recent graduates, career changers and IT professionals. CC starts newcomers on their path to advanced cybersecurity certifications like the CISSP and future leadership roles.

Official ISC2 Certified in Cybersecurity (CC) Entry-Level Certification Training will review the content covered in the exam. It prepares candidates by building a solid foundation of knowledge they need to pass the exam and ultimately land an entry- or junior-level cybersecurity role.

Destinatários

CC training is for IT professionals, career changers, college students, recent college graduates, advanced high school students and recent high school graduates looking to start their path toward cybersecurity leadership by taking the Certified in Cybersecurity entry-level exam.

Objetivos

After completing this course, learners will be able to:

- Discuss the foundational concepts of cybersecurity
- Recognize foundational security concepts of information
- Define risk management terminology and summarize the
- Relate risk management to personal or professional
- Classify types of security
- Distinguish between policies, procedures, standards, regulations and
- Demonstrate the relationship among governance

- Analyze appropriate outcomes according to the canons of the ISC2 Code of Ethics when given
- Practice the terminology of and review security
- Explain how organizations respond to, recover from and continue to operate during unplanned disruptions.
- Recall the terms and components of incident
- Summarize the components of a business continuity
- Identify the components of disaster
- Practice the terminology and review concepts of business continuity, disaster recovery and incident response.
- Select access controls that are appropriate in a given
- Relate access control concepts and processes to given
- Compare various physical access
- Describe logical access
- Practice the terminology and review concepts of access
- Explain the concepts of network
- Recognize common networking terms and
- Identify common protocols and port and their secure
- Identify types of network (cyber) threats and
- Discuss common tools used to identify and prevent
- Identify common data center
- Recognize common cloud service
- Identify secure network design
- Practice the terminology and review concepts of network
- Explain concepts of security
- Discuss data handling best
- Identify key concepts of logging and
- Summarize the different types of encryption and their common
- Describe the concepts of configuration
- Explain the application of common security
- Discuss the importance of security awareness
- Practice the terminology and review concepts of network

Programa

- Security Principles
- Incident Response, Business Continuity and Disaster Recovery
- Access Controls Concepts
- Network Security
- Security Operations

Security Principles

- Understand the Security Concepts of Information Assurance
- Understand the Risk Management Processes
- Understand Security Controls

- Understand Governance Elements
- Understand ISC2 Code of Ethics

Incident Response, Business Continuity and Disaster Recovery

- Understand Incident Response
- Understand Business Continuity
- Understand Disaster Recovery

Access Controls Concepts

- Understand Access Control Concepts
- Understand Physical Access Controls
- Understand Logical Access controls

Network Security

- Understand Computer Networking
- Understand Network (Cyber) Threats and Attacks
- Understand Network Security Infrastructure

Security Operations

- Understand Data Security
- Understand System Hardening
- Understand Best Practice Security Policies
- Understand Security Awareness Training

Course Summary and Test Preparation

- Certification Requirements
- Scheduling the Exam
- Before the Exam
- Day of Exam
- Tips for Reading the Questions
- After the Exam

Note: Course materials are organized by chapter, not domain, which may result in domains or individual domain topics being covered in a different order than what appears in the exam outline. The chapter structure allows us to properly cover the exam domains while supporting a more cohesive learning experience.