Official ISC2 Certified Cloud Security Professional (CCSP) Training - Including Exam

Duración: 5 Días **Código del Curso: CCSP** **Método de Impartición: Curso Cerrado (In-Company)**

Temario:

Official ISC2® Training Seminar for the Certified Cloud Security Professional (CCSP®) provides a comprehensive review of the knowledge required for understanding cloud computing and its information security risks and mitigation strategies. This training course will help students review and refresh their knowledge and identify areas they need to study for the CCSP exam. Content aligns with and comprehensively covers the six domains of the ISC2 CCSP Common Body of Knowledge (CBK®), ensuring relevancy across all disciplines in the field of cloud security.

Official courseware is developed by ISC2 – creator of the CCSP CBK – to ensure your training is relevant and up-to-date. Our instructors are verified security experts who hold the CCSP and have completed intensive training to teach ISC2 content.

Training features:
Instruction from an ISC2 Authorized Instructor
Official ISC2 Student Training Guide
Chapter quizzes
Interactive flash cards to reinforce learning
Real-world learning activities and scenarios
Case studies and discussions
Post-course assessment questions to gauge exam readiness

Dirigido a:

This training is intended for professionals who have at least five years of full-time IT experience, including three years in information security and at least one year in cloud security, and are pursuing CCSP certification to enhance credibility and career mobility. Example job functions include, but are not limited to: Enterprise Architect; Security Administrator; Systems Engineer; Security Architect; Security Consultant; Security Engineer; Security Manager; Systems Architect.

Objetivos:

- **After Completing this course you should be able to:**
- Understand legal frameworks and guidelines that affect cloud services.
- Recognize the fundamentals of data privacy regulatory/legislative mandates.
- Assess risks, vulnerability, threats and attacks in the cloud environment.
- Evaluate the design and plan for cloud infrastructure security controls.
- Evaluate what is necessary to manage security operations.
- Understand what operational controls and standards to implement.
- Describe the types of cloud deployment models in the types of as a service cloud models currently available today.
- Identify key terminology and associated definitions related to cloud technology. Be able to establish a common terminology for use within a team or workgroup.
- Build a business case for cloud adoption and be able to determine with business units the benefits of the cloud and cloud migration strategies.

Prerequisitos:

Candidates must have a minimum of 5 years cumulative paid work experience in information technology, of which 3 years must be in information security and 1 year in 1 or more of the 6 domains of the CCSP CBK. Earning CSA's CCSK certificate can be substituted for 1 year of experience in 1 or more of the 6 domains of the CCSP CBK. Earning (ISC)²'s CISSP credential can be substituted for the entire CCSP experience requirement.

A candidate that doesn't have the required experience to become a

Exámenes y certificación

Recommended as preparation for the following exam:

- (ISC)2 Certified Cloud Security Professional

To qualify for this cybersecurity certification, you must pass the exam and have at least **five years** of cumulative work experience in information technology, of which **three years** must be in information security, and **one year** in one or more of the six domains of the ISC2 CCSP Exam Outline.

CCSP may become an Associate of (ISC)² by successfully passing the CCSP examination. The Associate of (ISC)² will then have 6 years to earn the 5 years required experience. You can learn more about CCSP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CCSP/experience-requirements .

- CISSP - Official ISC2 Certified Information Systems Security Professional Training (CISSP) incl Exam

Learn more about CCSP Experience Requirements .

Don't have enough experience yet? You can still pass the CCSP exam and become an Associate of ISC2 while you earn the required work experience.

Please note an exam voucher is included as part of this course

Contenido:

Chapter 1: Cloud Concepts, Architecture and Design

- State the essential characteristics of cloud computing
- Describe the fundamental cloud computing services
- Describe the cloud computing reference architectures
- Explain cloud computing activities
- Compare cloud service capabilities and models
- Describe cloud deployment models

Chapter 2: Cloud Governance: Legal, Risk and Compliance

- Explain the issues with international conflict of law
- Interpret guidelines for digital forensics
- Identify the fundamentals of data privacy regulatory/legislative mandates
- Summarize audit process, methodologies and cloud-ready adaptations
- Describe risk management related to cloud services
- Identify due care/diligence activities related to service contracts

Chapter 3: Cloud Data Security

- Discuss cloud data security concepts
- Describe cryptography
- Explain data discovery and classification technologies
- Interpret cloud data storage architectures
- Analyze information rights management
- Assess cloud data security strategies
- Compare solutions for cloud data retention, deletion and archival policies
- Explain basic security concepts in the cloud

Chapter 4: Cloud Platform and Infrastructure Security

- Compare cloud infrastructure components
- Select standard practices for implementing a secure data center design
- Assess risks, vulnerability, threats and attacks in the cloud environment
- Discover components for planning and implementing security controls
- Evaluate the design and plan for cloud infrastructure security controls
- Appraise appropriate identity and access management (IAM) solutions
- Recommend business continuity and disaster recovery (BCDR) standards

Chapter 5: Cloud Application Security

- Explain training and awareness solutions for application security
- Assess challenges in the secure software development life cycle (SDLC) process
- Select a threat model for securing software development
- Demonstrate cloud software assurance and validation
- Choose verified secure software
- Explain the specifics of a cloud application architecture

Chapter 6: Cloud Security Operations

- Analyze what is used to manage and operate physical and logical infrastructure of a cloud environment
- Discuss operational controls and standards
- Identify methodologies for supporting digital forensics
- Identify critical communication needs with relevant parties
- Define auditability, traceability and accountability of security-relevant data events
- Select requirements to implement secure operations
- Summarize economic characteristics of cloud computing
- Evaluate cloud computing ROI and KPI metrics
- Summarize cloud computing security concepts
- Describe key security considerations for each service model
- Analyze key cloud service provider contractual relationship documents

Información Adicional:

Note: Throughout this course, exam domains may be covered in several chapters. Included in the course is a table indicating where the exam outline

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid