Official ISC2 Systems Security Certified Practitioner (SSCP) Training - Including Exam

Duración: 5 Días **Código del Curso: SSCP** **Método de Impartición: Curso Remoto (Virtual)**

Temario:

Official ISC2® Training for the Systems Security Certified Practitioner (SSCP®) provides a comprehensive review of the knowledge required to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability. This training course will help students review and refresh their knowledge and identify areas they need to study for the SSCP exam. Content aligns with and comprehensively covers the seven domains of the ISC2 SSCP Common Body of Knowledge (CBK®).

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

Training features:
Instruction from an ISC2 Authorized Instructor
Official ISC2 Student Training Guide
Interactive flash cards to reinforce learning
20 content-specific learning activities and 12 applied scenarios
61 content specific activities, including 6 case studies
8 end of chapter quizzes with answer explanation to assess comprehension
180 question post course assessment with answer explanation highlighting areas for further study

Updated 8/2026

Curso Remoto (Abierto)

Nuestra solución de formación remota o virtual, combina tecnologías de alta calidad y la experiencia de nuestros formadores, contenidos, ejercicios e interacción entre compañeros que estén atendiendo la formación, para garantizar una sesión formativa superior, independiente de la ubicación de los alumnos.

Dirigido a:

This training course is intended for practitioners who have at least one year of cumulative, paid workexperience in one or more of the seven domains of the ISC2 SSCP CBK and are pursuing SSCP training and certification to acquire the credibility and mobility to advance within their current information security careers. The training seminar is ideal for those with technical skills and practical, hand-on security knowledge working in operational IT positions such as, but not limited to: Network Security Engineer: Systems/Network Administrator; Security Analyst; Systems Engineer; Security Consultant/Specialist; Security Administrator; Systems/Network Analyst; Database Administrator.

Objetivos:

- **After completing this course, the student will be able to:**
- Describe security and the alignment of asset management to risk management.
- Appraise risk management options and the use of access controls to protect assets.
- Examine the field of cryptography to secure information and communication.
- Build a security posture by securing software, data, and endpoints.
- Apply network and communications security to establish a secure networked environment.
- Evaluate cloud and wireless security.
- Prepare for incident detection and response.
- Implement appropriate measures that contribute to the maturation of risk management.

Prerequisitos:

Attendees should meet the following pre-requisites:

Exámenes y certificación

Recommended as preparation for the following exam:

- Candidates must have a minimum of 1-year cumulative work experience in 1 or more of the 7 domains of the SSCP CBK. A 1-year prerequisite pathway will be granted for candidates who received a degree (bachelors or masters) in a cybersecurity program.

- (ISC)2 Certified Systems Security Certified Practitioner Candidates must have a minimum of one year cumulative work experience in one or more of the domains of the SSCP CBK. A one year prerequisite pathway will be granted for candidates who received a degree (bachelors or masters) in a cybersecurity program.

A candidate that doesn't have the required experience to become an SSCP may become an Associate of ISC2 by successfully passing the SSCP examination. The Associate of ISC2 will then have two years to earn the one year required experience. You can learn more about SSCP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/SSCP/SSCP-Experience-Requirements .

Notice: Beginning October 1, 2025, the SSCP exam will be administered as a variable-length Computer Adaptive Test (CAT) exam only. Candidates will answer 100-125 multiple-choice items with an adjusted exam length of 2 hours. For more information on CAT, please refer to www.isc2.org/certifications/computerized-adaptive-testing .

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

Contenido:

Module 1: Access Controls

- Implement authentication mechanisms
- Operate internetwork trust architectures
- Participate in the identity-management lifecycle
- Implement access controls

Module 2: Security Operations and Administration

- Understand and comply with the code of ethics
- Understand security concepts
- Document and operate security controls
- Participate in asset management
- Implement and assess compliance with controls
- Participate in change management
- Participate in security awareness and training
- Participate in physical security operations

Module 3: Risk Identification, Monitoring, and Analysis

- Understand the risk management process
- Perform security assessment activities
- Operate and maintain monitoring systems
- Analyse monitoring results

Module 4: Incident Response and Recovery

- Participate in incident handling
- Understand and support forensic investigations
- Understand and support BCP and DRP

Module 5: Cryptography

- Understand and apply fundamental concepts of cryptography
- Understand the requirements for cryptography
- Understand and support secure protocols
- Operate and implement cryptographic systems

Module 6: Networks and Communications Security

- Understand security issues related to networks
- Protect telecommunications technologies
- Control network access
- Manage LAN-based security
- Operate and configure network-based security devices
- Implement and operate wireless technologies

Module 7: Systems and Application Security

- Identify and analyse malicious code and activity
- Implement and operate endpoint device security
- Operate and configure cloud security
- Secure big data systems

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