The DevSecOps Company

CertPREP COURSEWARE

# (ISC)2 CISSP Certified Information Systems Security Professional

## Sobre este curso.

El curso Certified Information Systems Security Professional (CISSP) es un compañero perfecto para prepararse para el examen CISSP. Se centra específicamente en los objetivos para el examen CISSP que presenta ISC2 en mayo de 2021. El curso revisará la retención de activos, el aprovisionamiento seguro, los ataques criptográficos, las herramientas de aprendizaje automático, la búsqueda de amenazas, el control de acceso basado en el riesgo, la confianza cero, SAML, SOAR, CASB, la seguridad de microservicios, contenedores, servicios gestionados y muchos otros temas, al tiempo que le ayudará a identificar áreas de debilidad y mejorar su conocimiento conceptual y habilidades prácticas.

El objetivo de este curso es proporcionarle todas las herramientas que necesita para prepararse para el examen CISSP, incluidos consejos de preparación, consejos para tomar exámenes, estrategias para ahorrar tiempo, preguntas de autoevaluación y exámenes de práctica, para aumentar sus posibilidades de aprobar el examen en su primer intento.

## Duración.

5 Días.

## Perfil del público.

Profesionales de seguridad de TI y líderes de seguridad que están interesados en buscar la certificación o que necesitan mantener su certificación.

## Requisitos previos.

Antes de asistir a este curso, los estudiantes deben tener:

- 1-2 años de experiencia profesional en seguridad informática
- Experiencia trabajando con seguridad de TI
- Fluidez en los procedimientos de seguridad, como la planificación de la continuidad del negocio, la planificación de desastres y la evaluación de riesgos.

## Objetivos del curso.

Al completar con éxito este curso, los estudiantes deberían ser capaces de:

- Comprender la seguridad y la gestión de riesgos.
- Clasificar información y activos.
- Revisar la arquitectura de seguridad y la ingeniería en busca de vulnerabilidades y defectos de diseño.
- Mejorar las arquitecturas, los componentes y los canales de comunicación y seguridad de la red.
- Fortalecer los controles, servicios y aprovisionamiento de la gestión de identidad y acceso (IAM).
- Mejorar la evaluación de la seguridad y los diseños de pruebas para recopilar y procesar datos para apoyar las auditorías.
- Gestionar las operaciones de seguridad.

## Examen.

Este curso no tiene un examen asociado.



**KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.**

# Temario.

## Lección 1: El examen de certificación CISSP.

- Evaluación de los requisitos del examen.
- Determinar si estás listo para el examen.
- Usando preguntas de práctica.
- Usando tu tiempo sabiamente.

## Lección 2: Comprender la seguridad de los activos.

- Métodos adecuados para la destrucción de datos.
- Desarrollo de documentos que puedan ayudar a cumplir con las leyes locales, estatales y federales.
- La implementación del cifrado y su uso para la protección de datos.
- Cómo usar el control de seguridad de los datos.

## Lección 3: Seguridad y gestión de riesgos.

- Cálculos utilizados para la gestión de riesgos.
- Enfoques aprobados para una buena gestión de la seguridad.
- Cómo realizar un análisis cualitativo de riesgos.
- Cómo realizar un análisis cuantitativo de riesgos.
- Cómo realizar un análisis de riesgo híbrido.
- Buena protección de recursos.
- Las funciones de las políticas, procedimientos, directrices y líneas de base de seguridad.
- Clasificación adecuada de los datos.
- Implementación adecuada de funciones de seguridad.
- Cómo realizar el cálculo del riesgo.

## Lección 4: Arquitectura e ingeniería de seguridad.

- Cómo seleccionar controles basados en los requisitos de seguridad del sistema.
- Uso de modelos de confidencialidad como Bell-LaPadula.
- Cómo identificar modelos de integridad como Biba y Clark-Wilson.
- Defectos comunes y problemas de seguridad asociados con los diseños de arquitectura de seguridad.
- La criptografía y cómo se utiliza para proteger la información confidencial.
- La necesidad y la colocación del control de seguridad física.

## Lección 5: Comunicaciones y seguridad de la red.

- Diseño de red segura.
- La diferencia entre las topologías LAN y WAN.
- El modelo OSI y sus capas.
- Las cuatro capas de la pila TCP/IP.
- Protocolo de convergencia.

## Lección 6: Gestión de identidad y acceso.

- Gestión de identidad y acceso.
- Cómo controlar el control físico y lógico de los activos.
- Métodos para integrar la identidad como un servicio de terceros.
- Diferencia entre el control de acceso discrecional, obligatorio basado en atributos y basado en roles.
- Cómo gestionar el ciclo de vida de aprovisionamiento de identidad y acceso.
- Cómo diferenciar los tipos de autorización.

## Lección 7: Evaluación y pruebas de seguridad.

- Evaluación y pruebas de seguridad.
- Estrategias de evaluación y prueba.
- Cómo identificar las metodologías de ataque.
- Técnicas de prueba automatizadas y manuales.
- Ejemplos y metodologías de pruebas de penetración.
- Registrar reseñas.
- Recuperación ante desastres y continuidad del negocio.
- Cómo realizar la evaluación de seguridad y las pruebas de penetración.
- Métricas de seguridad.
- Técnicas de respuesta a incidentes.

## Lección 8: Operaciones de seguridad.

- Procesos y planes de recuperación ante desastres.
- Cómo entender y apoyar las investigaciones.
- Conceptos de seguridad fundamentales.
- Diferentes tipos de RAID.
- Cómo implementar estrategias de recuperación ante desastres y estrategias de recuperación.

**KeD es una empresa sustentable, Por favor no imprimas este documento si no es necesario.**

- Cómo participar en la planificación y los ejercicios de continuidad del negocio.
- Perimetral y controles físicos internos.
- Cómo implementar procesos de recuperación ante desastres.
- Auditoría y supervisión.

### Lección 9: Seguridad del desarrollo de software.

- El papel de la seguridad en el ciclo de vida del desarrollo de software.
- Diseño de la base de datos.
- El Modelo de Madurez de Capacidad.
- Los pasos del ciclo de vida del desarrollo.
- Cómo determinar la efectividad de la seguridad del software.
- El impacto de la seguridad del software adquirida.
- Diferentes tipos de técnicas de diseño de aplicaciones.
- El papel de la gestión del cambio.
- Los tipos principales de base de datos.