



CURSO INTERNACIONAL

**CERTIFIED INFORMATION SYSTEMS SECURITY
PROFESSIONAL (CISSP)**



Clases en tiempo real



40 Académicas



Acerca del Programa

Un profesional con certificación CISSP es un profesional en aseguramiento de la información que define la arquitectura, diseño, administración y/o controles que garantizan la seguridad de los entornos comerciales. El amplio campo de conocimiento y la experiencia que se necesita para aprobar el examen es lo que distingue al profesional con certificación CISSP. La credencial demuestra un nivel globalmente reconocido de competencia provisto por (ISC)2® CBK®, que cubre temas críticos en la seguridad actual, incluida la computación en la nube, seguridad móvil, seguridad en el desarrollo de aplicaciones, gestión del riesgo y más.

→ **Objetivos:**

Este curso proporciona una comprensión integral de la ciberseguridad, abordando sus conceptos y definiciones clave. Los participantes analizarán los principales dominios de seguridad, incluyendo gestión de riesgos, protección de activos, ingeniería de seguridad, seguridad en redes y comunicaciones, gestión de identidad y acceso, evaluación y pruebas de seguridad, operaciones de seguridad y desarrollo seguro de software, permitiéndoles fortalecer sus conocimientos y estrategias en la protección de sistemas y datos.

→ **Certificación:**



Certificado de participación con validez internacional, a nombre de New Horizons Corporation

→ **Beneficios**

- Material de estudios digital orientado al examen de certificación oficial
- Acceso para ingresar al curso por un año.

*Sujeto a la programación del año



01. Administración de seguridad y riesgo

- Confidencialidad, disponibilidad
- Gobierno de seguridad
- El programa de seguridad completo y efectivo
- Cumplimiento
- Temas legales y regulatorios
- Entendiendo la ética profesional
- Administración personal
- Conceptos de administración del riesgo
- Modelamiento de amenazas
- Práctica y estrategia de adquisiciones
- Preguntas de revisión

02. Seguridad de activos

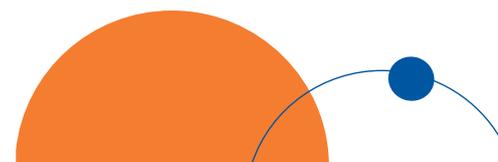
- Seguridad de activos
- Gestión de datos
- Estándares de datos
- Uso y longevidad
- Gestión de activos
- Protección de privacidad
- Asegurar retención apropiada
- Determinar controles de seguridad de datos
- Selección de estándares
- Preguntas de revisión

03. Ingeniería de la seguridad

- Ciclo de vida
- Conceptos fundamentales de modelos de seguridad
- Modelos de evaluación de seguridad de sistemas de información
- Capacidades de seguridad de Sistemas de información
- Vulnerabilidades de arquitecturas de seguridad
- Seguridad de base de datos
- Vulnerabilidades y amenazas del software y sistemas
- Vulnerabilidades en sistemas móviles
- Vulnerabilidades en sistemas incrustados y sistemas ciber-físicos
- La aplicación y el uso de la criptografía
- Sitios y consideraciones de diseño
- Planeamiento del sitio
- Diseño e implementación de seguridad
- Implementación y operación de seguridad
- Preguntas de revisión

04. Seguridad de comunicaciones y redes

- Arquitectura y diseño de redes seguras
- Implicaciones de protocolos multinivel
- Componentes de la seguridad de redes
- Canales de comunicación seguros
- Ataques de red
- Preguntas de revisión





05. Administración de identidades y accesos

- Acceso físico y lógico a bienes
- Identificación y autenticación de personas y dispositivos
- Implementación de administración de identidades
- Identidad como un servicio (IDaaS)
- Servicios de identidad integrados tercerizados
- Implementar y administrar mecanismos de autorización
- Prevenir o mitigar ataques de control de acceso
- Ciclo de vida provisional de identidad y acceso
- Preguntas de revisión

06. Evaluación y prueba de seguridad

- Importancia de la gestión de la seguridad de la información
- Acceso lógico
- Seguridad de la infraestructura de la red
- Auditoria del marco general de la gestión de la seguridad de la información
- Auditoria a la seguridad de la infraestructura de la red
- Exposiciones y controles ambientales
- Exposiciones y controles de acceso físico
- Dispositivos de computación móvil

07. Operaciones de seguridad

- Investigaciones
- Aprovisionamiento de recursos a través de administración de configuración
- Conceptos fundamentales de operaciones de seguridad
- Protección de recursos
- Respuesta ante incidentes
- Medidas preventivas contra ataques
- Parches y administración de vulnerabilidad
- Cambio y administración de configuración
- El proceso de recuperación de desastres
- Revisión del plan de pruebas
- Continuidad del negocio y otras áreas de riesgo
- Control de acceso
- Seguridad interna
- Edificación y seguridad interna
- Seguridad del personal
- Preguntas de revisión

08. Seguridad en el ciclo de vida de desarrollo de sistemas

- Entorno de la seguridad del desarrollo del software
- Entorno y controles de seguridad
- Seguridad del entorno del software
- Mecanismos de protección del software
- Evaluando la efectividad de la seguridad del software
- Preguntas de revisión



BENEFICIOS DE CLASES ONLINE EN VIVO



Online Live

Clases en tiempo real (conéctate desde el lugar que estés)



Acceso a las clases grabadas

Podrás ver las clases grabadas hasta por 90 días



Certificado Internacional

A nombre de New Horizons Corporation



Capacidad

Máximo 20 alumno



Discusiones

Con sus compañeros y el instructor en tiempo real



Informes e inscripciones:



www.newhorizons.edu.pe
940 068 987
Info@newhorizons.edu.pe

New Horizons Perú
RUC: 20306532201
Av. Santa Cruz 870, Miraflores