PROFESIONAL CERTIFICADO EN SEGURIDAD DE SISTEMAS DE INFORMACION (CISSP)

Online Live

1. Certificación:

Certificado con validez internacional a nombre de New Horizons Corporation.

2. Metodología única Online Live:

La formación Online LIVE ofrece la misma educación de alta calidad que caracteriza a **New Horizons,** incluyendo conferencias en vivo, demostraciones y laboratorios virtuales, lo cual nos permite crear un espacio de aprendizaje tan efectivo como el de la modalidad presencial.

3. Presentación

Si planea construir una carrera en seguridad de la información, una de las profesiones más visibles de la actualidad, la credencial de Certified Information Systems Security Professional (CISSP®) debería ser el próximo objetivo en su carrera. 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. CISSP fue la primera credencial en el campo de la información que cumplió los estrictos requisitos de la Norma ISO/IEC 17024.

La certificación CISSP® es un estándar reconocido a nivel mundial, que confirma el conocimiento de un profesional en el campo de la seguridad de la información. Los CISSP son profesionales de la Seguridad de la Información que definen la arquitectura, el diseño, la gestión y/o los controles que garantizan la seguridad de los entornos empresariales.

4. Perfil del estudiante

Este curso está dirigido a profesionales experimentados en seguridad de TI, auditores, consultores, investigadores o instructores, incluidos analistas e ingenieros de red o de seguridad, administradores de red, especialistas en seguridad de la información y profesionales de la gestión de riesgos, que persiguen la capacitación y certificación de CISSP para adquirir la credibilidad y la movilidad para avanzar dentro de sus carreras actuales de seguridad informática o para migrar a una carrera relacionada. A través del estudio de los ocho dominios de Conocimiento Común de CISSP (CBK), los estudiantes validarán su conocimiento al cumplir con los requisitos de preparación necesarios para calificar para rendir el examen de certificación de CISSP. Los requisitos de certificación CISSP adicionales incluyen un mínimo de cinco años de experiencia profesional directa en dos o más campos relacionados con los ocho dominios de seguridad CBK.

5. Objetivos

En este curso, identificará y reforzará los principales temas de seguridad de los ocho dominios de (ISC) 2 CISSP CBK. Vas a:

- Analizar los componentes del dominio de Seguridad y Gestión de riesgos.
- Analizar componentes del dominio de seguridad de activos.
- Analizar los componentes del dominio de Ingeniería de seguridad.
- Analizar componentes del dominio de Comunicaciones y Seguridad de red.
- Analizar los componentes del dominio de Identity and Access Management.
- Analizar los componentes del dominio Evaluación y prueba de seguridad.
- Analizar componentes del dominio de operaciones de seguridad.
- Analizar componentes del dominio de Seguridad de desarrollo de software.

6. Malla curricular (53 horas)

¿Qué es CISSP?

¿Qué es el ISC2?

Requisitos para obtener la certificación

¿Cuáles son los dominios?

Módulo 1: Administración de seguridad y riesgo

- Confidencialidad, integridad y disponibilidad
- Gobierno de seguridad
  - ✓ Visión, misión y objetivos de la organización
  - ✓ Procesos organizacionales
  - ✓ Roles y responsabilidades de Seguridad
  - ✓ Estrategias de Seguridad de la Información
- El programa de seguridad completo y efectivo
  - ✓ Representación del Comité de Supervisión
  - ✓ Cuadro de control
  - ✓ Cuidado de plazos
  - ✓ Seguimiento de plazos
- Cumplimiento
- Temas legales y regulatorios
  - ✓ Cyber Crimen/Computación
  - ✓ Licencia y Propiedad intelectual
  - ✓ Importación/Exportación
  - ✓ Transbordo de flujo de datos
  - ✓ Privacidad
  - ✓ Incumplimiento de datos
  - ✓ Leyes relevantes y regulaciones
- Entendiendo la ética profesional
  - ✓ Requerimientos regulatorios para programas éticos
  - ✓ Temas en ética computacional
  - ✓ Falacias comunes en la ética computacional
  - ✓ Hackeo y activismo
  - ✓ Recursos y códigos éticos de conducta
  - ✓ Código de éticas profesionales de ISC2
  - ✓ Código de ética de soporte a la organización
- Administración de la seguridad del personal
  - ✓ Proyección de la empleabilidad del candidato
  - ✓ Acuerdos y políticas de empleo
  - ✓ Procesos de desvinculación laboral
  - ✓ Controles de Proveedores, consultores y de contratistas.
  - ✓ Privacidad
- Conceptos de administración del riesgo
  - ✓ Conceptos de administración de riesgo organizacional
  - ✓ Metodologías de aseguramiento del riesgo
  - ✓ Identificar vulnerabilidades y amenazas
  - ✓ Aseguramiento/análisis del riesgo
  - ✓ Selección de contramedidas

- ✓ Implementación de contramedidas contra el riesgo
- ✓ Categoría de controles
- ✓ Tipos de control de acceso
- ✓ Evaluación, monitoreo y medida de controles
- ✓ Metodología de pruebas de penetración
- ✓ Evaluación de activos tangibles e intangibles
- ✓ Mejoramiento continúo
- ✓ Marco (Framework) de la administración del riesgo

- Modelamiento de amenazas
  - ✓ Determinación y análisis de reducción de ataques potenciales
  - ✓ Tecnologías y procesos para remediar amenazas
- Práctica y estrategia de adquisiciones
  - ✓ Hardware, software y servicios
  - ✓ Gobierno de la Administración de terceros
  - ✓ Seguridad mínima y requerimientos de nivel de servicio
- Preguntas de revisión

Módulo 2: Seguridad de activos

- Seguridad de activos
- Gestión de datos
  - ✓ Determinar y mantener la propiedad de los datos
  - ✓ Política de datos
  - ✓ Algunas consideraciones
  - ✓ Roles y responsabilidades
  - ✓ Propiedad de datos
  - ✓ Custodio de datos
  - ✓ Calidad de datos
  - ✓ Documentación y organización de datos
- Estándares de datos
  - ✓ Control de ciclo de vida de los datos.
  - ✓ Especificación y modelamiento de datos.
  - ✓ Mantenimiento de base de datos
  - ✓ Auditoría de datos
  - ✓ Archivo y almacenamiento de datos
- Uso y longevidad
  - ✓ Seguridad de datos
  - ✓ Acceso, compartir y diseminación de datos
  - ✓ Publicación de datos.
  - ✓ Establecer requerimientos de manejo.

- ✓ Marca, manejo, almacenamiento y destrucción de información sensible
- Gestión de activos
  - ✓ Licenciamiento de software
  - ✓ Ciclo de vida de los equipos
- Protección de privacidad
  - ✓ La información debe ser
- Asegurar retención apropiada
  - ✓ Medios, hardware y personal.
  - ✓ Política de retención de datos de la compañía "X"
- Determinar controles de seguridad de datos
  - ✓ Datos en reposo
  - ✓ Herramientas de encriptación
  - ✓ Data en tránsito
  - ✓ Algoritmos de recolección de encriptación
  - ✓ Conexión inalámbrica
  - ✓ Líneas base
  - ✓ Determinación del alcance y medición
- Selección de estándares
  - ✓ Recursos de Estados Unidos
  - ✓ Recursos internacionales
  - ✓ Manual de marco nacional de ciber seguridad
  - ✓ Marco para mejorar la infraestructura critica de ciberseguridad
- Preguntas de revisión

Módulo 3: Ingeniería de la seguridad

- Ciclo de vida
  - ✓ Fundamentos de seguridad
  - ✓ Basado en riesgo
  - ✓ Facilidad de uso
  - ✓ Incremento de Resistencia
  - ✓ Reducir vulnerabilidades
  - ✓ Diseño pensado en red
- Conceptos fundamentales de modelos de seguridad
  - ✓ Procesadores.
  - ✓ Memoria y almacenamiento.
  - ✓ Dispositivos periféricos y otros dispositivos de entrada y salida.
  - ✓ Sistemas operativos.
  - ✓ Arquitectura de seguridad empresarial
  - ✓ Cuadros comunes de Arquitecturas
  - ✓ Tipos de modelos de seguridad

- Modelos de evaluación de seguridad de sistemas de información
  - ✓ Modelos de seguridad comunes formales
  - ✓ Modelos de evaluación de producto
  - ✓ Directrices de implementación de seguridad industrial e internacional
- Capacidades de seguridad de Sistemas de información
  - ✓ Mecanismos de control de acceso
  - ✓ Administración segura de memoria
- Vulnerabilidades de arquitecturas de seguridad
  - ✓ Sistemas
  - ✓ Tecnología e integración de procesos
  - ✓ Único punto de fallo (SPOF)
  - ✓ Vulnerabilidades basadas en cliente
  - ✓ Vulnerabilidades basadas en servidor
- Seguridad de base de datos
  - ✓ Warehousing.
  - ✓ Inferencia.
  - ✓ Agregación.
  - ✓ Minería de datos.
  - ✓ Sistemas de datos paralelos de gran escala
  - ✓ Sistemas distribuidos
  - ✓ Sistemas criptográficos
- Vulnerabilidades y amenazas del software y sistemas
  - ✓ Basado en web
- Vulnerabilidades en sistemas móviles
  - ✓ Riesgos de la computación remota
  - ✓ Riesgos de los trabajadores móviles
  - ✓ Potenciales fuentes de ataques a dispositivos móviles
  - ✓ Ejemplos de objetivos para los atacantes
- Vulnerabilidades en sistemas incrustados y sistemas ciber-físicos
- La aplicación y el uso de la criptografía
  - ✓ La historia de la criptografía
  - ✓ Tecnología emergente
  - ✓ Principios básicos de la seguridad de la información
  - ✓ Características adicionales de los sistemas criptográficos
  - ✓ El ciclo de vida criptográfico
  - ✓ Infraestructura de llave pública (PKI)
  - ✓ Procesos de administración de claves.
  - ✓ Avances en administración de claves.
  - ✓ Estándares para instituciones financieras.
  - ✓ Segregación de obligaciones.
  - ✓ Control dual.

- ✓ Conocimientos de la división
- ✓ Creación y distribución de claves
- ✓ Firmas digitales
- ✓ Administración de derechos digitales. (DRM)
- ✓ No repudio
- ✓ Hashing
- ✓ Funciones simples de búsqueda
- ✓ Métodos de ataques criptoanalíticos

- Sitios y consideraciones de diseño
  - ✓ Encuesta de Seguridad
- Planeamiento del sitio
  - ✓ Diseño de calzada
  - ✓ Prevención del crimen a través del diseño del entorno (CPTED)
  - ✓ Ventanas
  - ✓ Amenazas de la ubicación
- Diseño e implementación de seguridad
  - ✓ Guías FEMA (Agencia de administración de emergencias federales)
- Implementación y operación de seguridad
  - ✓ Comunicaciones y cuarto de servidores
  - ✓ Seguridad de área de trabajo y restringida
  - ✓ Utilidades y consideraciones HVAC
  - ✓ Prevención, detección y supresión de fuego
- Preguntas de revisión

Módulo 4: Seguridad de comunicaciones y redes

- Arquitectura y diseño de redes seguras
  - ✓ OSI y T
  - ✓ Capa 1: Capa física
  - ✓ Capa 2: Capa de enlace a datos
  - ✓ Capa 3: Capa de red
  - ✓ Capa 4: Capa de transporte
  - ✓ Capa 5: Capa de sesión
  - ✓ Capa 6: Capa de presentación
  - ✓ Capa 7: Capa de aplicación
  - ✓ Modelo de referencia TCP/IP
  - ✓ Redes IP
  - ✓ IPv6.
  - ✓ Protocolo de control de transmisión (TCP).
  - ✓ Protocolo de usuario de datagrama (UDP).
  - ✓ Internet-Intranet.

- ✓ Extranet.
- ✓ Protocolo de configuración dinámico de Host (DHCP).
- ✓ Protocolo de control de mensaje de Internet (ICMP).
- ✓ Ping de muerte.
- ✓ Ataques redirigidos ICMP.
- ✓ Escaneo de ping.
- ✓ Explotación de ruta de rastreo.
- ✓ Procedimiento de llamadas remotas
- ✓ Servicios de directorio

- Implicaciones de protocolos multinivel
  - ✓ SCADA
  - ✓ Modbus
  - ✓ Protocolos convergentes
  - ✓ Implementación
  - ✓ Protocolo de voz sobre Internet (VoIP)
  - ✓ Conexiones inalámbricas
  - ✓ Seguridad de conexiones inalámbricas
  - ✓ Criptografía usada para mantener la seguridad de las comunicaciones
- Componentes de la seguridad de redes
  - ✓ Ruteo seguro/Ruteo determinístico
  - ✓ Router de Borders (Boundary Routers).
  - ✓ Non-blind spoofing.
  - ✓ Blind spoofing.
  - ✓ Ataque hombre en el medio (MitM)
  - ✓ Perímetro de seguridad.
  - ✓ Partición de red
  - ✓ Host de hogar dual (Dual-Homed Host)
  - ✓ Host de bastión
  - ✓ Zona desmilitarizada
  - ✓ Hardware
  - ✓ Medios de transmisión
  - ✓ Seguridad de punto final.
  - ✓ Redes de distribución de contenido
- Canales de comunicación seguros
  - ✓ Voz
  - ✓ Colaboración multimedia
  - ✓ Protocolos abiertos, aplicaciones y servicios
  - ✓ Acceso remoto
  - ✓ Comunicaciones de datos
  - ✓ Redes virtualizadas
- Ataques de red

- ✓ La red como un canal de ataque
- ✓ La red como un bastión de defensa.
- ✓ Objetivos de seguridad de redes y modos de ataque
- ✓ Técnicas de escaneo
- ✓ Administración de seguridad de eventos
- ✓ Ataques de fragmentación IP y paquetes hechos a mano
- ✓ Ataques de Denegación de servicio (DoS)/Denegación de servicios distribuido (DDos)
- ✓ Synflood
- ✓ Spoofing
- ✓ Sesión Highjack

- Preguntas de revisión

Módulo 5: Administración de identidades y accesos

- Acceso físico y lógico a bienes
  - ✓ Tipos de acceso
  - ✓ Sistemas de control de acceso físico (PACs)
- Identificación y autenticación de personas y dispositivos
  - ✓ Identificación, autenticación y autorización
- Implementación de administración de identidades
  - ✓ Administración de claves
  - ✓ Administración de cuentas
  - ✓ Administración de perfiles
  - ✓ Administración de directorios
  - ✓ Tecnologías de directorios
  - ✓ Factor de autenticación simple/múltiple
  - ✓ Responsabilidad
  - ✓ Administración de sesión
  - ✓ Registro y prueba de identidad
  - ✓ Sistemas de administración de credenciales
  - ✓ Riesgos y beneficios
  - ✓ Arquitectura de identificación gráfica y autenticación (GINA)
- Identidad como un servicio (IDaaS)
  - ✓ Funcionalidades IDaaS incluyen
  - ✓ Características y beneficios
- Servicios de identidad integrados tercerizados
  - ✓ Identidad de red.
  - ✓ Sincronización de directorios.
  - ✓ Identidad federada.
- Implementar y administrar mecanismos de autorización

- ✓ Control de acceso basado en roles
- ✓ Control de acceso basado en reglas.
- ✓ Control de acceso obligatorio (MACs).
- ✓ Control de acceso discrecional (DACs)

- Prevenir o mitigar ataques de control de acceso
  - ✓ Pasos preventivos proactivos
  - ✓ Centro administrativo de active directory (ADAC)
- Ciclo de vida provisional de identidad y acceso
  - ✓ Aprovisionamiento
  - ✓ Revisión
  - ✓ Revocación
- Preguntas de revisión

Módulo 6: Evaluación y prueba de seguridad

- Evaluación y estrategia de pruebas
  - ✓ Desarrollo de software como parte del diseño de sistemas
  - ✓ Revisión de registros
  - ✓ Registro estándar de procesos de administración operacional
  - ✓ Eventos de sistema.
  - ✓ Registros de auditoria.
  - ✓ Transacciones sintéticas.
  - ✓ Revisión y prueba de código
  - ✓ Durante el planeamiento y diseño
  - ✓ Durante el desarrollo de aplicaciones
  - ✓ Ejecutable en un ambiente de prueba
  - ✓ Operación y mantenimiento del sistema
  - ✓ Prueba negativa/Mal uso de casos de prueba
  - ✓ Prueba de interfaz
- Recolectar datos del proceso de seguridad
- Auditorías internas y externas
  - ✓ Opciones de reporte SOC.
  - ✓ Tipos de reporte SOC.
  - ✓ Principios SOC2/SOC3.
  - ✓ Criterios SOC2/SOC3.
  - ✓ Punto de vista sobre el uso de reportes SOC
- Preguntas de revisión

Módulo 7: Operaciones de seguridad

- Investigaciones
  - ✓ Identificar la evidencia.

- ✓ Recolectar o adquirir la evidencia.
- ✓ Examinar o analizar la evidencia.
- ✓ Presentación de hallazgos.
- ✓ La escena del crimen
- ✓ Política, roles y responsabilidades
- ✓ Manejando y respondiendo incidentes
- ✓ Fase de recuperación
- ✓ Recolección y manejo de la evidencia
- ✓ Reporte y documentación
- ✓ Recolección y procesamiento de evidencia
- ✓ Monitoreo continuo y resultados
- ✓ Fuga de datos/prevención de pérdidas (DLP)

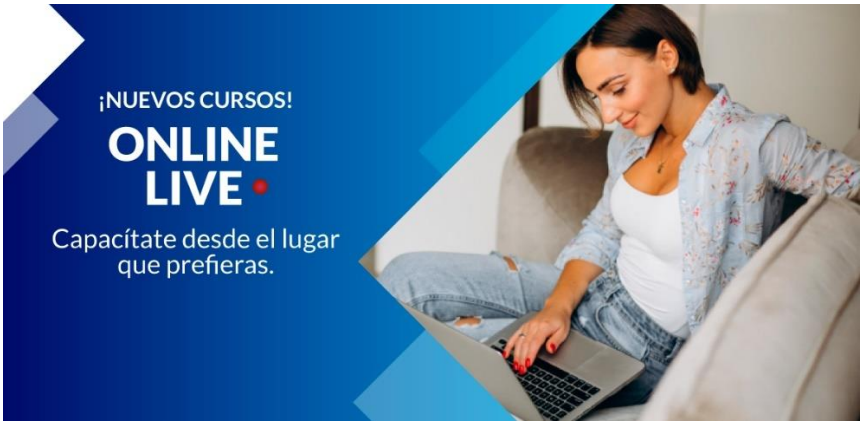
- Aprovisionamiento de recursos a través de administración de configuración
  - ✓ Los pasos CMMI para CM
- Conceptos fundamentales de operaciones de seguridad
  - ✓ Temas claves
  - ✓ Procesos operacionales y procedimientos clave
  - ✓ Controlando las cuentas privilegiadas
  - ✓ Administrando las cuentas usando grupos y roles
  - ✓ Separación de deberes y responsabilidades
  - ✓ Privilegios especiales de monitoreo
  - ✓ Rotación de trabajo.
  - ✓ Administrando el ciclo de vida de la información.
  - ✓ Acuerdos de nivel de servicio (ANS)
- Protección de recursos
  - ✓ Bienes tangibles vs intangibles
  - ✓ Hardware.
  - ✓ Administración de medios
- Respuesta ante incidentes
  - ✓ Administración de incidentes.
  - ✓ Medidas, métricas y reportes de seguridad
  - ✓ Administrando tecnologías de seguridad
  - ✓ Detección
  - ✓ Respuesta
  - ✓ Reporte
  - ✓ Recuperación
  - ✓ Solución y revisión (lecciones aprendidas)
- Medidas preventivas contra ataques
  - ✓ Revelaciones no autorizadas
  - ✓ Arquitectura del sistema de detección de intromisión de redes
- Parches y administración de vulnerabilidad

- ✓ Fuentes de de información seguridad y parches
- Cambio y administración de configuración
  - ✓ Administración de configuración
  - ✓ Estrategias de recuperación de sitios
  - ✓ Sitios de procesamiento múltiples
  - ✓ Resistencia de sistemas y requerimientos de tolerancia crítica
- El proceso de recuperación de desastres
  - ✓ Documentando el plan.
  - ✓ Respuesta
  - ✓ Personal
  - ✓ Comunicaciones y notificación a los empleados
  - ✓ Evaluación
  - ✓ Restauración
  - ✓ Brindar entrenamiento
  - ✓ Ejercitar, evaluar y mantener el plan
- Revisión del plan de pruebas
  - ✓ Mesa de ejercicio /Prueba estructurada de camino
  - ✓ Prueba de simulación
  - ✓ Prueba paralela
  - ✓ Prueba de completa interrupción/completa
  - ✓ Actualización y mantenimiento del plan
- Continuidad del negocio y otras áreas de riesgo
  - ✓ Implementación y operación del perímetro de seguridad
  - ✓ Detección de intromisión al perímetro
- Control de acceso
  - ✓ Tipos de tarjeta
  - ✓ Circuito cerrado de TV
- Seguridad interna
  - ✓ Sistemas de detección de intromisiones interiores
  - ✓ Escolta y control de visitantes
- Edificación y seguridad interna
  - ✓ Puertas
  - ✓ Bloqueo de puertas
- Seguridad del personal
  - ✓ Privacidad
  - ✓ Viaje
  - ✓ Coacción
- Preguntas de revisión

Módulo 8: Seguridad en el ciclo de vida de desarrollo de sistemas

- Entorno de la seguridad del desarrollo del software
  - ✓ Ciclo de vida del desarrollo
  - ✓ Modelos de maduración
  - ✓ Operación y mantenimiento
  - ✓ Administración del cambio
  - ✓ Equipo integrado de producto
- Entorno y controles de seguridad
  - ✓ Métodos de desarrollo de software
  - ✓ La base de datos y el entorno de data warehousing
  - ✓ Vulnerabilidades y amenazas de la base de datos
  - ✓ Controles DBMS
  - ✓ Administración del conocimiento
  - ✓ Entorno de aplicación Web
- Seguridad del entorno del software
  - ✓ Desarrollo de aplicaciones y conceptos de programación
  - ✓ El entorno del software
  - ✓ Librerías y set de herramientas
  - ✓ Cuestiones de seguridad en código origen
  - ✓ Software malicioso (Malware)
  - ✓ Protección del Malware
- Mecanismos de protección del software
  - ✓ Núcleos de seguridad, monitores de referencia y el TCB
  - ✓ Gestión de configuración
  - ✓ Seguridad de repositorios de código
  - ✓ Seguridad de interfaces de programación de aplicaciones
- Evaluando la efectividad de la seguridad del software
  - ✓ Certificación y acreditación
  - ✓ Auditoria y registro de cambios
  - ✓ Análisis y mitigación de riesgos
  - ✓ Fase de planeamiento
  - ✓ Fase de aceptación y monitoreo
  - ✓ Seguimiento
- Preguntas de revisión

MODALIDAD ONLINE LIVE NEW HORIZONS



1. Plataforma única

Utilizando la tecnología más avanzada desarrollamos nuestra propia plataforma LMS (*Learning Management System)*. A través de la plataforma de New Horizons podrás reproducir todos nuestros recursos y herramientas que poseen nuestras clases presenciales. Así mismo hemos integrado diferentes herramientas como Adobe Connect, la cual te permitirá interactuar en tiempo real con el instructor y tus compañeros de aula. Podrás realizar preguntas, resolver casos e incluso compartir tu pizarra y presentaciones como si estuvieras en un aula dentro de nuestras instalaciones.

2. Beneficios únicos

- Participarás en discusiones con tu instructor y compañeros a través de video y audio en tiempo real.
- Tendrás acceso a su aula virtual desde el primer día de clase.
- Tendrás acceso tus clases grabadas hasta por 180 días, en caso quieras volver a llevar el curso o revisar el contenido.
- Verás documentos y presentaciones en tiempo real
- Aulas virtuales con aforo no mayor a 15 participantes
- El instructor podrá ver y administrar tu computadora para una tutoría individualizada.
- Aprende desde donde te sientas cómodo y ahorra tiempo y dinero.