New Horizons
Learn What Earns


CURSO INTERNACIONAL

# Certified Ethical Hacker v13 con AI (CEH)

Clases en tiempo real  53 Académicas

Curso Oficial

EC-Council

## Acerca del Programa

De los creadores de Certified Ethical Hacker (CEH) llega la versión 13, completamente renovada e integrada con capacidades de inteligencia artificial. Este programa, estructurado en 20 módulos de aprendizaje, abarca más de 550 técnicas de ataque y te brinda la base esencial para destacar como profesional en ciberseguridad.

- Accede a opciones de aprendizaje flexibles adaptadas a tu ritmo.
- Obtén un certificado con reconocimiento internacional.
- Desarrolla habilidades reales con más de 221 laboratorios prácticos.

## Novedades de la versión 13

**Impulsado por IA.**
La primera certificación de piratería ética del mundo que aprovecha el poder de la IA.

**Experiencia práctica**
Perfecciona tus habilidades en escenarios reales con laboratorios especializados, donde aplicarás vectores de ataque y dominarás herramientas avanzadas de hacking ético.

**40% más de eficiencia**
Aprende técnicas impulsadas por IA que aumentan la eficiencia en la ciberdefensa hasta en un 40 %, mientras optimizas y agilizas tu flujo de trabajo.

**Plan de estudios actualizado y potente**
Domina las últimas técnicas de ataque avanzadas, las tendencias más recientes y sus contramedidas efectivas.

**Aumento de productividad 2x**
Detección avanzada de amenazas, toma de decisiones optimizada, aprendizaje adaptativo, informes precisos y automatización de tareas repetitivas.

**Habilidades del mundo real, dominio demostrado**
Participa en competiciones globales de hacking cada mes, reta a tus compañeros y asciende en la clasificación.

## Certificación:

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

Certificación Internacional CEH v13
Sujeta a la aprobación del examen oficial, con el respaldo de EC-Council.

## Beneficios:

- Material oficial digita: manuales, guías y lecturas con acceso por 2 años para reforzar lo aprendido.
- Laboratorios virtuales en la nube con más de 200 ejercicios y escenarios de ataque (acceso por 6 meses).
- C|EH Practical (vigencia: 1 año): examen práctico que valida tus habilidades en un entorno real resolviendo 20 desafíos en 6 horas.
- Voucher oficial de certificación CEH con 1 año de vigencia. Incluye 1 retoma sin costo adicional, examen teórico
- 10 videos oficiales de EC-Council para reforzar técnicas y conceptos clave (acceso por 1 año).
- Global C|EH Challenge (vigencia: 1 año): retos internacionales tipo Capture The Flag para medirte mensualmente con profesionales de todo el mundo.


## Avanza en tu carrera con CEH, ahora con capacidades de inteligencia artificial adicionales

Adquiere habilidades listas para la industria aprendiendo las estrategias tácticas multiplataforma que emplean los ciberdelincuentes más sofisticados (incluida la IA), para que puedas detectar vulnerabilidades antes que ellos.

- El 92% de los empleadores prefieren a los graduados de CEH para trabajos de piratería ética
- El 95% eligió CEH para su crecimiento profesional
- Los módulos están asignados a más de 45 puestos de trabajo en ciberseguridad
- 4 de cada 5 empresas afirman que la IA es una prioridad estratégica
- 1 de cada 2 profesionales recibió ascensos después del CEH

# Marco de aprendizaje

El exclusivo marco de 4 pasos de EC-Council ofrece un enfoque estructurado e integral para dominar la piratería ética.

## Paso 1

### Aprender

CEH ofrece una combinación equilibrada de formación teórica y laboratorios prácticos con escenarios del mundo real, todo ello potenciado por inteligencia artificial.

## Paso 2

### Certificar

Al finalizar la capacitación, podrás rendir ambos exámenes para demostrar tus habilidades y obtener la certificación CEH Master.

- Tomar el examen de conocimientos
- Completar el examen práctico

## Paso 3

### Comprender

CEH te ayuda a desarrollar experiencia real en hacking ético, mediante prácticas inmersivas en un campo cibernético simulado.

## Paso 4

### Competir

Obtén acceso por un año a 12 desafíos CTF (Capture The Flag). Cada mes enfrentarás un nuevo reto con temáticas diferentes, diseñadas para fortalecer las habilidades y capacidades esenciales de un hacker ético.

# Lo que aprenderás

La certificación Certified Ethical Hacker (CEH) de EC-Council te brinda las habilidades y conocimientos necesarios para impulsar tu carrera en la era de la IA. Con CEH aprenderás a pensar como un hacker y a identificar vulnerabilidades ocultas antes de que lo hagan los ciberdelincuentes.

Te equiparemos para:

**Encuentre y corrija debilidades:**

Descubre cómo los piratas informáticos vulneran los sistemas y aprende a proteger tu información de manera segura.

**Conviértete en un experto en seguridad:**

Domina las herramientas y técnicas clave para reforzar la seguridad de tu organización.

**Proteja su reputación:**

Prevén proactivamente las violaciones de datos y asegura la lealtad de tus clientes.

**Domine la piratería ética con IA:**

Impulsa tus competencias en hacking ético con técnicas basadas en IA y enfréntate con ventaja a los ciberataques.

# Malla curricular

**01. Introducción al hacking ético**

Aprende los fundamentos esenciales de la seguridad de la información, incluyendo conceptos de hacking ético, controles de seguridad, normativas relevantes y procedimientos estándar.

**02. Huellas y reconocimiento**

Aprende a utilizar las técnicas y herramientas más recientes para realizar footprinting y reconocimiento, una fase clave y fundamental en el proceso de hacking ético.

**03. Scanning Networks**

Aprenda diferentes técnicas de escaneo de red y contramedidas.

**04. Enumeración**

Aprende diversas técnicas de enumeración, incluyendo exploits en Border Gateway Protocol (BGP) y Network File Sharing (NFS), junto con sus contramedidas.

**05. Análisis de vulnerabilidades**

Aprende a identificar vulnerabilidades de seguridad en la red, la infraestructura de comunicación y los sistemas finales de una organización objetivo. Además, conoce los distintos tipos de evaluación de vulnerabilidades y las herramientas más utilizadas para llevarlas a cabo.

**06. Hackeo de sistemas**

Obtén conocimientos sobre diversas metodologías de hacking de sistemas empleadas para descubrir vulnerabilidades en redes y equipos, incluyendo la esteganografía, los ataques de esteganálisis y las técnicas para cubrir huellas.

**07. Amenazas de malware**

Obtén conocimientos sobre los distintos tipos de malware (troyanos, virus, gusanos, entre otros), así como sobre malware APT y fileless. Aprende procedimientos de análisis y las contramedidas más efectivas para su detección y prevención.

**08. Olfatear**

Aprende las técnicas de rastreo de paquetes y su aplicación en la detección de vulnerabilidades de red, así como las contramedidas para protegerte frente a este tipo de ataques.

**09. Ingeniería social**

Aprende conceptos y técnicas de ingeniería social, incluyendo cómo identificar intentos de fraude, auditar vulnerabilidades a nivel humano y proponer contramedidas efectivas.

# Malla curricular

**10. Denegación de servicio**

Obtén información sobre las distintas técnicas de ataque de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS), así como sobre las estrategias de protección más efectivas frente a ellos.

**11. Secuestro de sesiones**

Aprende las diferentes técnicas de secuestro de sesiones utilizadas para identificar debilidades en la gestión de sesiones a nivel de red, autenticación, autorización y criptografía, junto con sus contramedidas.

**12. Cómo evadir sistemas de detección de intrusos (IDS), firewalls y honeypots**

Aprende sobre firewalls, sistemas de detección de intrusiones (IDS) y técnicas de evasión de honeypots, así como sobre las herramientas utilizadas para auditar el perímetro de una red en busca de debilidades y sus contramedidas.

**13. Hackeando servidores web**

Obtén información sobre los ataques a servidores web, incluyendo metodologías integrales utilizadas para auditar vulnerabilidades en infraestructuras de servidores y las contramedidas correspondientes.

**14. Hackeando aplicaciones web**

Obtén información sobre los ataques a aplicaciones web, incluyendo metodologías integrales de hacking utilizadas para auditar vulnerabilidades y las contramedidas correspondientes.

**15. Inyección SQL**

Obtén información sobre las técnicas de ataque de inyección SQL, los métodos de evasión y las contramedidas para prevenirlas.

**16. Hackeando redes inalámbricas**

Aprende sobre los diferentes tipos de cifrado, las principales amenazas, metodologías y herramientas de hacking, así como las herramientas de seguridad y contramedidas aplicadas a redes inalámbricas.

**17. Hackeando plataformas móviles**

Aprende sobre los principales vectores de ataque en plataformas móviles, técnicas de hacking en Android e iOS, gestión de dispositivos móviles, pautas de seguridad y herramientas de protección.

# Malla curricular

**18. Hacking de IoT y OT**

Aprende sobre los distintos tipos de ataques dirigidos al Internet de las Cosas (IoT) y a la Tecnología Operativa (OT), incluyendo metodologías y herramientas de hacking, así como las contramedidas para enfrentarlos.

**19. Computación en la nube**

Aprende los conceptos clave de la computación en la nube, incluyendo tecnologías de contenedores y computación sin servidor, así como las principales amenazas, ataques, metodologías de hacking y las herramientas y técnicas de seguridad en la nube.

**20. Criptografía**

Obtén información sobre algoritmos de cifrado, herramientas de criptografía, infraestructura de clave pública (PKI), cifrado de correo electrónico y de disco, así como sobre ataques criptográficos y herramientas de criptoanálisis.

## Somos Partner Oficial de EC-COUNCIL

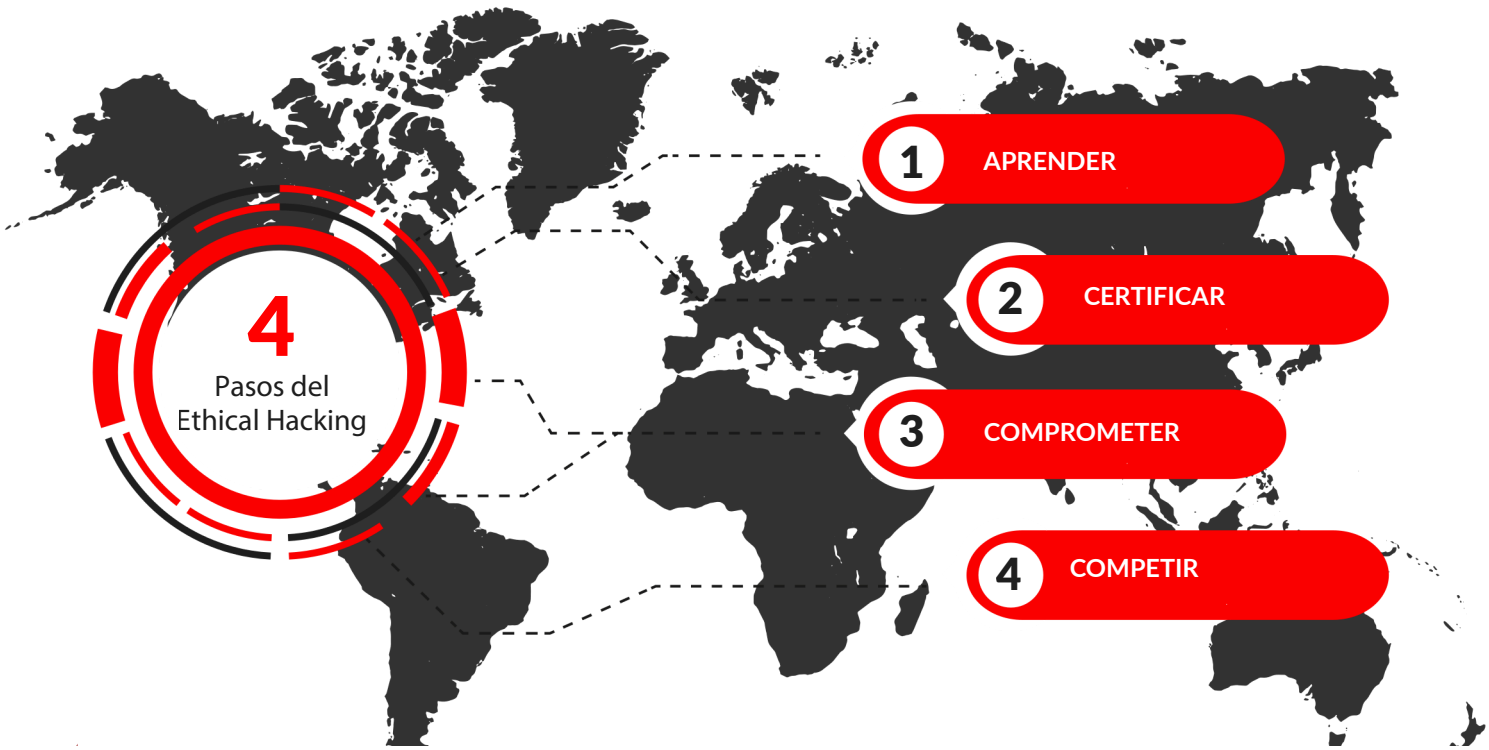
EC-Council

En New Horizons nos enorgullece ser Partner Oficial de EC-Council®, una de las organizaciones líderes a nivel mundial en certificaciones de ciberseguridad y hacking ético. Esta alianza refuerza nuestro compromiso con la excelencia en la capacitación tecnológica, ofreciendo programas certificados que permiten a profesionales y empresas fortalecer sus competencias en seguridad informática y estar preparados para enfrentar los desafíos del mundo digital.


Repetición de exámenes: este beneficio otorga a los candidatos el comprobante correspondiente en el portal ECC EXAM, excluyendo los cargos administrativos del supervisor, los cuales se aplican en cada intento de examen. Válido únicamente para el examen CEH. Para más información, comuníquese con su proveedor de capacitación.

# Un marco de aprendizaje único, impulsado por IA

## CEH sigue un marco único de 4 pasos



# ¿A quién va dirigido el CEH?

### Profesionales de la ciberseguridad

Impulsa tu carrera en ciberseguridad con CEH, ahora potenciado por el poder de la IA.

### Equipos y organizaciones

Potencia el conocimiento de tu equipo con una certificación en hacking ético impulsada por IA.

### Gobierno y ejército

CEH cuenta con la confianza y el reconocimiento a nivel mundial por parte de departamentos gubernamentales y organismos de defensa.

### Educadores

Crea y desarrolla tus propios programas y cursos de ciberseguridad, adaptados a tus necesidades.

# Detalles del examen

La certificación se obtiene al aprobar el examen de conocimientos. Para alcanzar el nivel CEH Master, es necesario rendir un examen práctico adicional, el cual es opcional.

## Examen de conocimientos

El examen de conocimientos pondrá a prueba tus habilidades en:

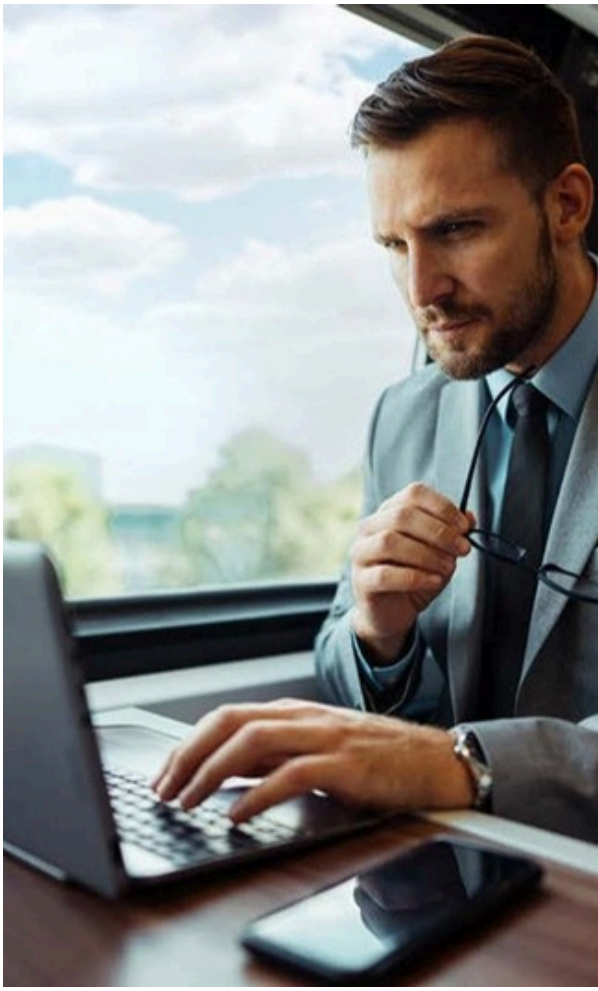
- Amenazas a la seguridad de la información y vectores de ataque
- Detección de ataques
- Prevención de ataques
- Procedimientos de respuesta
- Metodologías de seguridad

**Formato** Opción múltiples
**Duración** 4 horas
**Preguntas** 125
**Entrega** En línea a través del portal de exámenes ECC
**Puntuación** de aprobación del 60% al 85%

## Examen práctico

El examen práctico es opcional, pero te brinda la oportunidad de alcanzar un nivel superior de certificación. En él pondrás a prueba tus habilidades prácticas en:

- Uso de herramientas de escaneo de puertos (por ejemplo, Nmap, Hping).
- Detección de vulnerabilidades en sistemas y redes.
- Ataques a sistemas, incluyendo DoS, DDoS, secuestro de sesiones, ataques a servidores web y aplicaciones web, inyección SQL y amenazas inalámbricas.
- Metodologías de inyección SQL y técnicas de evasión.
- Herramientas de seguridad para aplicaciones web (por ejemplo, Acunetix WVS).
- Herramientas de detección de inyección SQL (por ejemplo, IBM Security AppScan).
- Protocolos de comunicación aplicados en entornos de seguridad.



**Duración:** 6 horas
**Preguntas:** 20
Entrega de la gama iLabs Cyber
Puntuación de aprobación del 60% al 85%

## Maestro CEH

Al completar con éxito tanto el examen teórico C|EH como el examen práctico C|EH, se otorga la designación C|EH Master. Esta certificación representa un alto nivel de competencia en conocimientos, habilidades y capacidades de hacking ético, con un total de 6 horas de evaluaciones que validan la experiencia del candidato. Además, los 10 mejores puntajes a nivel global en ambos exámenes son reconocidos en la clasificación mundial de hacking ético C|EH Master.

# BENEFICIOS DE CLASES ONLINE EN VIVO

**Online Live**

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

**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