EC-Council

TGK
DIGITAL BUSINESS

TÉCNICO CERTIFICADO EN CIBERSEGURIDAD (C/CT)

Inicie su carrera en ciberseguridad con laboratorios y exámenes basados en competencias

TE ESPERA UNA APASIONANTE CARRERA EN CIBERSEGURIDAD

Las empresas y los sectores industriales dependen cada vez más de la tecnología a medida que la transformación digital se hace omnipresente en el entorno empresarial actual. En consecuencia, la ciberseguridad es ahora relevante para cada sistema, dispositivo y byte de datos de los que dependen las organizaciones para funcionar.

La pandemia de COVID-19 ha aumentado aún más la necesidad de profesionales cualificados en ciberseguridad para hacer frente a la crisis a la que se enfrentan las organizaciones como consecuencia de la digitalización y el aumento de la ciberdelincuencia. Según PayScale (2022), los analistas de ciberseguridad en Estados Unidos ganan un salario medio anual de 77.000 USD, y la mayoría de los puestos ofrecen entre 54.000 y 116.000 USD al año. Sin embargo, a pesar de esta elevada demanda y atractiva remuneración, no hay suficientes talentos en ciberseguridad para cubrir los puestos de trabajo vacantes y proteger las posturas de seguridad de las organizaciones.

LA ESCASEZ DE TALENTO EN CIBERSEGURIDAD

Según un informe del Centro de Estudios Estratégicos e Internacionales, el 82% de los empleadores se enfrentan a una escasez de talento en ciberseguridad (Crumpler & Lewis, 2019). El sector necesita urgentemente profesionales de TI y ciberseguridad que puedan hacer frente a la amenaza global cada vez mayor de la ciberdelincuencia.

Para hacer frente a la falta de competencias en ciberseguridad, ECCouncil ha desarrollado la certificación Técnico Certificado en Ciberseguridad (C|CT). La certificación C|CT va más allá de la enseñanza de conceptos fundamentales de ciberseguridad, ya que valida los conocimientos de TI y ciberseguridad de los participantes en el curso a través de una amplia práctica y evaluación.

Establecer esta sólida base técnica en ciberseguridad sienta las bases para una futura carrera en una variedad de funciones de TI existentes. Los conocimientos y habilidades adquiridos a través del C|CT pueden crear vías para una mayor especialización en muchos dominios de ciberseguridad, incluyendo hacking ético, pruebas de penetración, análisis forense digital y seguridad de aplicaciones.

EC-Council ha desarrollado el C|CT para proporcionar a las personas que inician su carrera en TI y ciberseguridad una certificación que valide sus habilidades prácticas a nivel técnico.
Con el C|CT, EC-Council tiene como objetivo equipar a los profesionales de ciberseguridad de nivel básico con las habilidades técnicas básicas que necesitan para seguir y avanzar en sus carreras, como las de analistas de ciberseguridad, consultores, ingenieros, administradores de TI y más. El C|CT crea una base que permite a los individuos aumentar sus habilidades en dominios especializados como pruebas de penetración, consultoría de seguridad, auditoría y administración de sistemas y redes.

C|CT: UNA SOLUCIÓN INDUSTRIAL

¿QUÉ ES LA CERTIFICACIÓN C|CT?

El C|CT es un programa de ciberseguridad de nivel básico diseñado por EC Council, creador de la certificación Certified Ethical Hacker (C|EH), para responder a la necesidad y demanda mundial de técnicos en ciberseguridad.

¿QUÉ TIENE DE ÚNICO EL C|CT?

¡El único programa de ciberseguridad de referencia en todo el mundo, que ofrece **85 laboratorios prácticos reales!**

¡Una certificación práctica de inmersión impartida en un **campo de pruebas cibernéticas reales!**

50% del tiempo de formación **dedicado a los laboratorios**

¡El examen es basado en el rendimiento, combinado con actividades **cibernéticas en directo!**

Aprendizajes Multidiciplinarios, Network defense, Ethical Hacking. Análisis forense digital y operaciones seguridad

¿QUÉ OFRECE
EL PROGRAMA C|CT?

El programa C|CT proporciona los conocimientos básicos esenciales para iniciar una carrera en ciberseguridad, centrándose en cuatro disciplinas: defensa de redes, hacking ético, análisis forense digital y operaciones de seguridad.

Ofertas clave:

Fundamentos sólidos

La certificación C|CT proporciona una cobertura total del dominio de ciberseguridad con conceptos clave en cada dominio combinados con laboratorios prácticos y desafíos de pensamiento crítico que producen tecnólogos de ciberseguridad de talla mundial.

Experiencia de campo en directo

Otros programas populares se basan en la simulación y la interactividad como evaluación basada en la práctica, el programa C|CT se imparte en un Cyber Range en vivo utilizando objetivos reales y sistemas de ataque reales para una práctica y plataforma de evaluación verdaderamente inmersiva y real.

Captura la bandera

La certificación C|CT ofrece retos de pensamiento crítico al estilo de captura la bandera (CTF) para acompañar cada ejercicio de laboratorio poniendo en práctica los conocimientos y proporcionando un registro probado de demostración de habilidades. Los candidatos que completen el programa C|CT obtendrán la certificación C|CT y tendrán un historial probado de realización de las tareas requeridas en un Cyber Range en vivo, demostrando a los empleadores su capacidad para realizar tareas críticas.

Certificaciones múltiples

El esquema del curso del programa C|CT va más allá de algunos de los programas de ciberseguridad de nivel de entrada más comunes, como el Security+, en un entorno de ciberescala completamente práctico en lugar de simulaciones para garantizar el desarrollo de habilidades de ciberseguridad. Creemos que los candidatos que obtengan con éxito la certificación C|CT obtendrán otras certificaciones líderes en ciberseguridad, incluida Security+, sin necesidad de más formación.

Lo más accesible

A pesar del diseño único de este curso eminentemente práctico y de sus usos de la cibercapacidad del mundo real, la certificación es una de las más accesibles del mundo.

FUNCIONES DE LOS PROFESIONALES CERTIFICADOS EN C|CT

La certificación C|CT prepara a los profesionales de TI y ciberseguridad para manejar una amplia gama de cuestiones complejas relacionadas con la seguridad del software, las redes y los sistemas de TI frente a las ciberamenazas y ataques habituales.

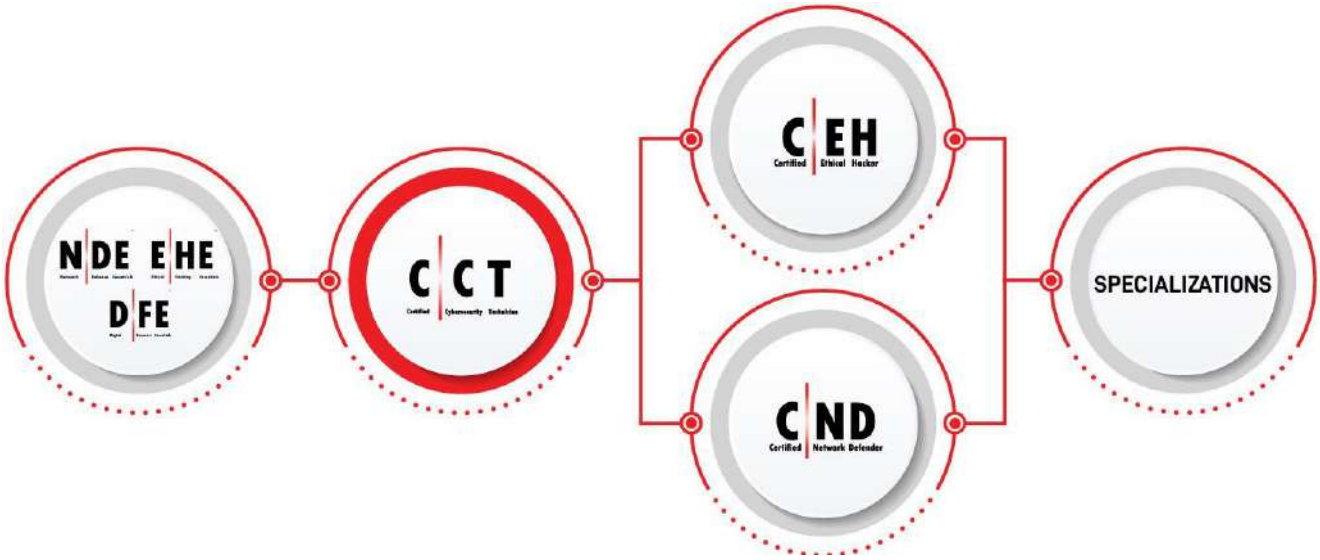
El C|CT ofrece un enfoque polifacético que incorpora defensa de redes, hacking ético y operaciones de seguridad para garantizar que los titulares de la certificación tengan una formación sólida y completa que les permita configurar, analizar e identificar problemas dentro de una organización. El curso C|CT dota a los participantes de los conocimientos necesarios para desempeñar las siguientes funciones:

- Especialista en redes de IT
- Técnico en ciberseguridad
- Director de IT
- Director en Redes
- Ingeniero en Redes
- Analista del Centro de Operaciones de Seguridad SOC

DESCRIPCIÓN DEL PUESTO DE TÉCNICO DE CIBERSEGURIDAD

Los técnicos de ciberseguridad proporcionan apoyo técnico en ciberseguridad, solucionan problemas de seguridad de la red, supervisan las alertas y siguen las políticas, procedimientos y normas pertinentes para proteger los activos de información de las organizaciones.

CARRERA DE CIBERSEGURIDAD STARTER TRACK



Nota: Esta es sólo una ruta sugerida; los cursos pueden tomarse en cualquier orden.

DESCRIPCIÓN DEL CURSO C|CT

La certificación C|CT de EC-Council sumerge a los estudiantes en una transferencia de conocimientos bien construida. La formación va acompañada de retos de pensamiento crítico y experiencias de laboratorio inmersivas que permiten a los candidatos aplicar sus conocimientos y pasar a la fase de desarrollo de habilidades en la propia clase. Al completar el programa, los profesionales certificados C|CT tendrán una base sólida en principios y técnicas de ciberseguridad, así como una exposición práctica a las tareas requeridas en los puestos de trabajo del mundo real.

C|CT ESQUEMA DEL CURSO TEMAS TRATADOS

1. AMENAZAS Y VULNERABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN
2. Ataques a la seguridad de la información
3. Fundamentos de la seguridad de las redes
4. Identificación, autenticación y autorización
5. Controles de seguridad de la red: Controles administrativos
6. Controles de seguridad de la red: Controles físicos
7. Controles de seguridad de la red: Controles técnicos
8. Evaluación de la seguridad de las redes: Técnicas y herramientas
9. Seguridad de las aplicaciones
10. Virtualización y computación en nube
11. Seguridad de redes inalámbricas
12. Seguridad de dispositivos móviles
13. Seguridad del internet de las cosas (IoT) y de la tecnología operativa (OT)
14. Criptografía
15. Seguridad de los datos
16. Resolución de problemas de red
17. Supervisión del tráfico de red
18. Monitoreo y análisis de registros de red
19. Respuesta a incidentes
20.
21. Informática forense
22. Continuidad de negocio y recuperación de desastres
    Manejo de riesgos
23. Gestión de riesgo

LO QUE APRENDERÁ EN ESTE CURSO

- Conceptos clave de ciberseguridad, la seguridad de la información y de redes Amenazas, vulnerabilidades y ataques a la seguridad de la información
- Reconocer los distintos tipos de malware
- Identificación, autenticación y autorización Controles de seguridad de la red
- Controles administrativos (firmware, leyes, actos, programas de gobernanza y cumplimiento, políticas de seguridad)
    - Controles físicos (políticas de seguridad física y en el lugar de trabajo, controles medioambientales)
    - Controles técnicos (protocolos de seguridad de la red; segmentación de la red; firewall; sistemas de detección y prevención de intrusiones; honeypots; servidores proxy; redes privadas virtuales; análisis del comportamiento de los usuarios; control de acceso a la red; gestión unificada de amenazas; gestión de eventos e información de seguridad; orquestación, automatización y respuesta de seguridad; load baancers; antimalware...).
- Técnicas y herramientas de evaluación de la seguridad de las redes (caza de amenazas, inteligencia sobre amenazas, evaluación de vulnerabilidades, hacking ético, pruebas de penetración, gestión de configuraciones y activos)
- Técnicas de diseño y comprobación de la seguridad de las aplicaciones
- Fundamentos de virtualización, computación en nube y seguridad en nube
- Fundamentos de las redes inalámbricas, cifrado y medidas de seguridad
- Fundamentos de los dispositivos móviles, IoT y OT y medidas de seguridad Criptografía e infraestructura de clave pública
- Controles de seguridad de datos, métodos de copia de seguridad, conservación de datos, y técnicas de prevención de pérdida de datos.
- Solución de problemas de red, supervisión del tráfico, los registros y análisis del tráfico
- El proceso de gestión y respuesta a incidentes
- Fundamentos de informática forense y pruebas digitales; fases de una investigación forense. Conceptos de continuidad de la actividad empresarial y recuperación en caso de catástrofe
- Conceptos, fases y marcos de gestión de riesgos

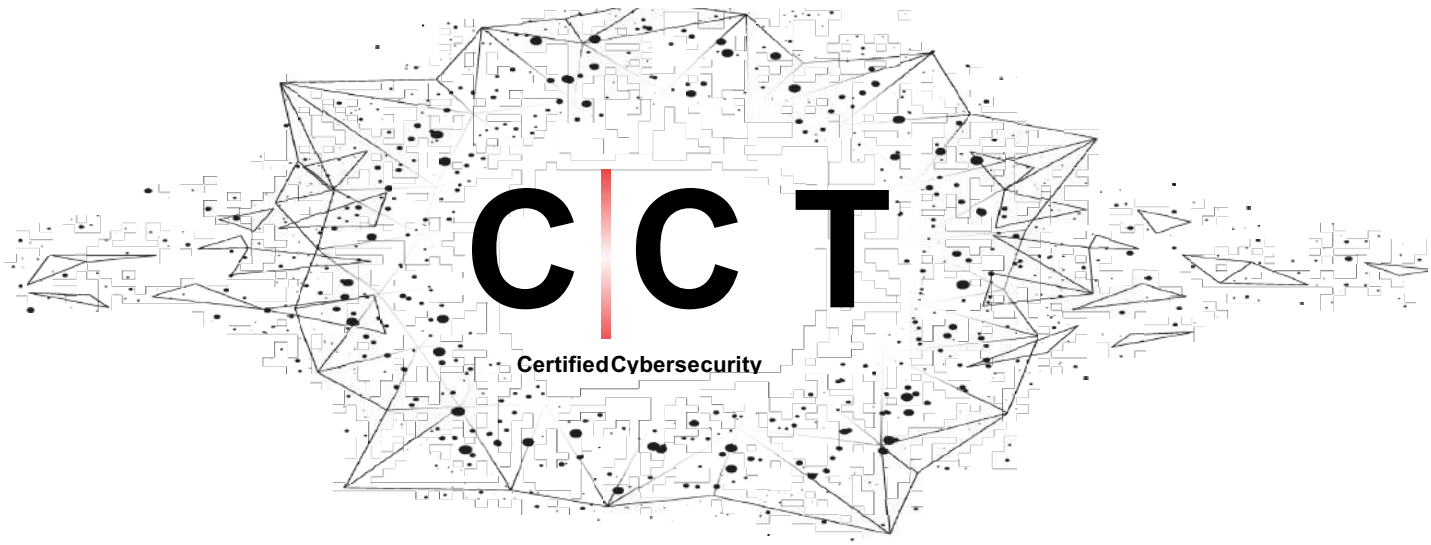
¿QUIÉN PUEDE REALIZAR ESTE CURSO?

El C|CT es ideal para cualquier persona que desee iniciar su carrera en el ámbito de la ciberseguridad o adquirir una sólida comprensión de los conceptos y técnicas de ciberseguridad necesarios para ser eficaz en el trabajo. El curso es especialmente adecuado para:

- Profesionales de TI en sus primeros años de carrera, directores de TI, personas que cambian de carrera y personas que avanzan en su carrera
- Estudiantes y recién titulados

¿CUÁLES SON LOS REQUISITOS PREVIOS PARA EL C|CT?

No se exigen requisitos previos específicos para obtener la certificación C|CT, aunque los conocimientos y la experiencia previos en TI y redes con especialización en ciberseguridad pueden constituir una ventaja. Los candidatos deben tener conocimientos de informática y redes informáticas antes de acceder al programa C|CT, aunque el plan de estudios incluye las tecnologías básicas.



INFORMACIÓN SOBRE EXÁMENES Y FORMACIÓN

Título del examen: Técnico Certificado en Ciberseguridad

Código de examen: 212-82

Número de preguntas: 60

Duración: 3 horas

Lugares de disponibilidad de los exámenes: Portal de exámenes ECC

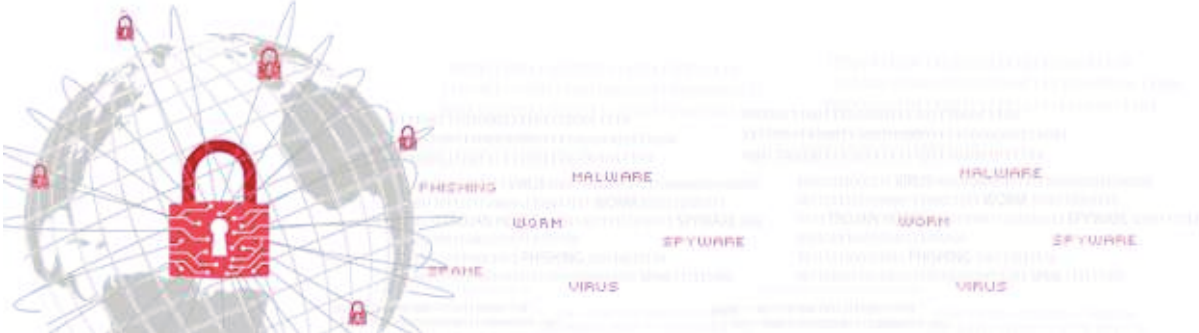
Formato del examen: Opción múltiple y examen práctico real

Modo de examen: Servicios de supervisión a distancia

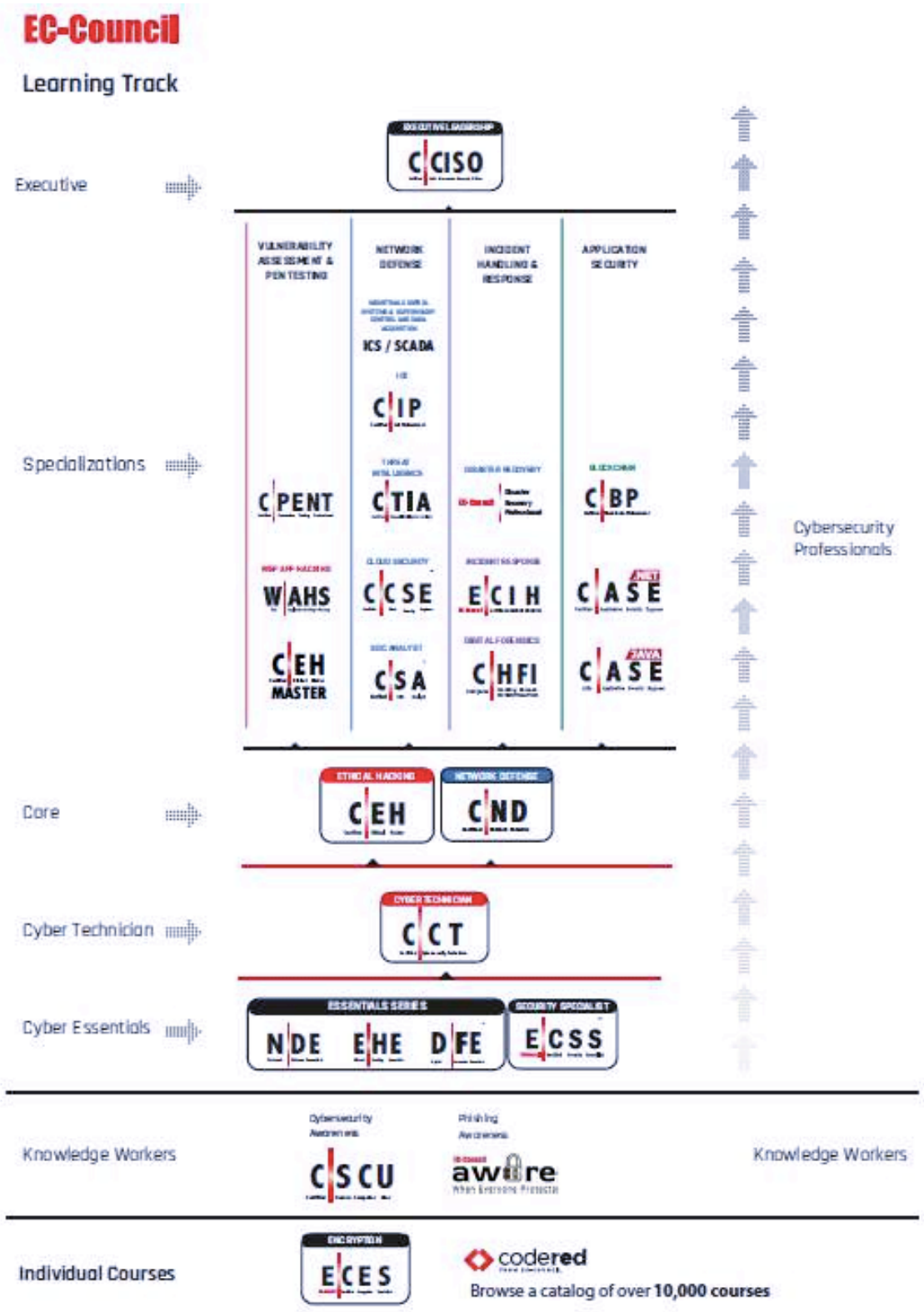
Puntuación mínima para aprobar: 70%.

Duración de la formación: 5 días

Modalidad: Formación con instructor iWeek (aprendizaje en línea synchronous) iLearn (aprendizaje en línea asynchronous) CodeRed (aprendizaje en línea asynchronous)



SU ITINERARIO DE APRENDIZAJE HACIA UNA PROMETEDORA CARRERA



SOBRE EC-COUNCIL

Establecemos las normas: C|ND, C|EH, C|HFIC|ND, C|EH, C|HFI

EC-Council cuenta con la confianza de siete de las 10 empresas de Fortune, 47 de las 100 de Fortune, el Departamento de Defensa (DoD), las comunidades mundiales de inteligencia, la OTAN y más de 2.000 de las mejores universidades, escuelas superiores y empresas de formación. Los programas de EC-Council están disponibles en más de 140 países y sientan las bases de la formación en ciberseguridad.

EC-Council es una organización acreditada por la ANSI 17024 y ha obtenido el reconocimiento del DoD en virtud de la Directiva 8140/8570, el GCHQ en el Reino Unido, CREST y otros organismos autorizados que influyen en la profesión de la ciberseguridad. Conocida sobre todo por el programa C|EH, nos dedicamos a equipar a los trabajadores de la ciberseguridad del mañana con los conocimientos, habilidades y capacidades necesarios para luchar contra los adversarios maliciosos y ganar.

Acreditaciones y reconocimientos de EC-Council

Committee on National Security Systems

American National Standards Institute

National Initiative for Cybersecurity Education

US Army credentialing Assistance

Department of Defense

American Council on Education

NCSC Certified Training

DIGITAL BUSINESS

EC-Council

Envia un Correo a:
academiaciber@tgk.com.mx
Siguenos en nuestras redes