TGK
DIGITAL BUSINESS

EC-Council

E|CDE
EC-Council Certified DevSecOps Engineer

Certificado por el EC-Council

Ingeniero DevSecOps

ACELERAR
DESARROLLO & DESPLIEGUE DE APLICACIONES

Domine las aplicaciones de seguridad con

Más de 80 laboratorios basados en habilidades DevSecOps nativos en la nube.

INDUSTRIA ESTADÍSTICAS

El crecimiento del mercado DevSecOps es impulsado por un aumento creciente de los ataques cibernéticos,
aumentando la necesidad para la entrega rápida de aplicaciones seguras.

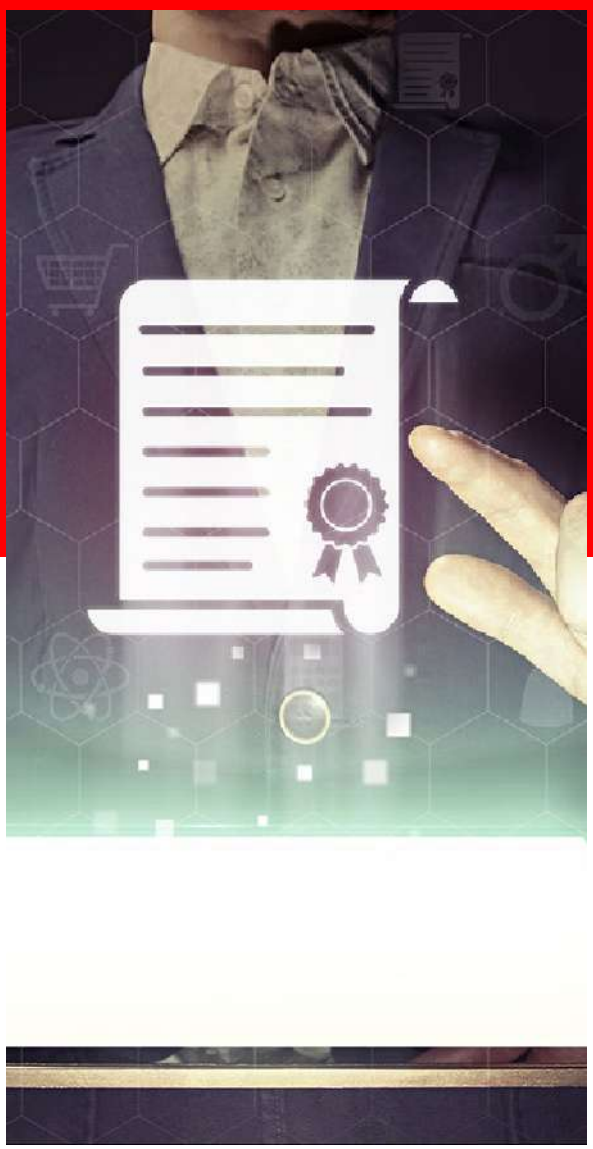
Según el Cost of a Data Breach Report 2021de IBM, el costo promedio de las filtraciones entre 50 millones y 65 millones de registros fue de USD 401 millones.

Según el análisis de filtración de datos del primer trimestre de 2022 del Identity TheftResource Center (ITRC), ha habido 398 incidentes de filtración de datos con 13 676 543 víctimas.

Según Verified Market Research, el tamaño del mercadode DevSecOps fue de 3730 millones de dólares estadounidenses en 2021 y se estima que alcance los 41660 millones de dólares estadounidenses para 2030, creciendo a una CAGR del 30,76 % de 2022 a 2030.

Certificación de ingeniero DevSecOps certificado por el Consejo de la CE (E|CDE)

Acelere la transformación digital de entornos locales y nativos de la nube con la certificación E|CDE, unprograma de laboratorio intensivo con el 70 % del plan de estudios dedicado a laboratorios y el 30 % a teoría.



Certificado del EC-Council DevSecOps Engineer (E|CDE) es un programa de certificación integral deDevSecOps práctico y dirigido por un instructor que ayuda a los profesionales a desarrollar las habilidades esenciales necesarias para diseñar, desarrollar y mantener aplicaciones e infraestructura seguras.

- El E|CDE cubre entornos locales y nativos de la nube (incluidos AWS Cloud y Microsoft Azure) con más de 80 laboratorios de los creadoresdel programa de piratería ética número uno del mundo, Certified Ethical Hacker (C|EH).
- Diseñado y desarrollado por pymes con contribuciones de profesionales experimentados en DevSecOps de todo el mundo.

USP clave de E|CDE

Programa de laboratorio intensivo con más de 80+ laboratorios basados en habilidades

Cubre DevSecOps tanto de aplicaciones como de infraestructura de plataformas locales y nativas de la nube

Cubre aspectos de seguridad e integración de herramientas en las ocho etapas de DevOps

Asignado con roles de trabajo en tiempo real y las responsabilidades de los ingenieros de DevSecOps

¿Por qué E|CDE?

- Agregar seguridad a un conjunto de habilidades de DevOps mejora las perspectivas de carrera.
- La información provista en el curso E|CDE se complementa con laboratorios para ayudar a los estudiantes a perfeccionar sus habilidades prácticas y prepararse para la industria.
- Este curso les enseña a los estudiantes cómo usar varias herramientas de DevSecOps y crear código seguro a lo largo del ciclo de vida del desarrollo de software.
- Los participantes se familiarizarán con las herramientas DevSecOps que permiten el desarrollo seguro de software y aplicaciones web, tanto en las instalaciones como en la nube.
- El curso E|CDE se enfoca en DevSecOps de aplicaciones y también proporciona información sobre DevSecOps de infraestructura.
- La integración de las herramientas más populares e importantes de la actualidad se ilustra en cada etapa del ciclo de vida de DevOps.
- El programa E|CDE ayuda a los ingenieros de DevSecOps a desarrollar y mejorar sus conocimientos y habilidades para proteger las aplicaciones en todas las etapas por medio de DevOps.

Cómo E|CDE puede proteger los entornos de nube

La seguridad en la nube generalmente ocurre fuera del ciclo de vida del desarrollo de software. El programa E|CDE de EC-Council permite a los equipos abordar problemas de seguridad en la nube a través de CI/CD y solucionar problemas directamente en la fuente.

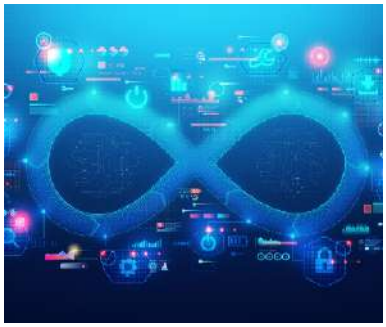
Cómo E|CDE puede proteger la nube de AWS

- AWS ofrece un conjunto de herramientas y servicios para identificar vulnerabilidades en diferentesetapas del ciclo de vida del desarrollo.
- El programa E|CDE cubre cómo integrar todas las herramientas de AWS necesarias para identificar vulnerabilidades de seguridad en varias etapas de la canalización de DevSecOps.

Cómo E|CDE puede proteger Microsoft Azure

Azure DevSecOps combina los productos y servicios de GitHub y Azure para ayudar a los equipos de DevOps y SecOps a colaborar en la creación de aplicaciones más seguras a medida que surgen nuevos tipos de ciberataques. El programa E|CDE cubre todas las últimas herramientas e integraciones en el módulo Azure DevSecOps.

¿Por qué debería obtener la certificación E|CDE?



DevSecOps es una extensión lógica de DevOps que genera seguridad en cada aplicación. Es un sistema de defensa que asegura que las aplicaciones e infraestructuras desarrolladas sean menos vulnerables a los ciberataques.

Cada aplicación en el mundo necesita un punto de control de seguridad; por lo tanto, la habilidades de DevSecOps se requieren ingenieros.

Cada empresa o trabajador independiente , que desarrolla y prueba necesidades de las aplicaciones.

Habilidades de DevSecOps.

Obtenga una Ventaja Competitiva con el E|CDE

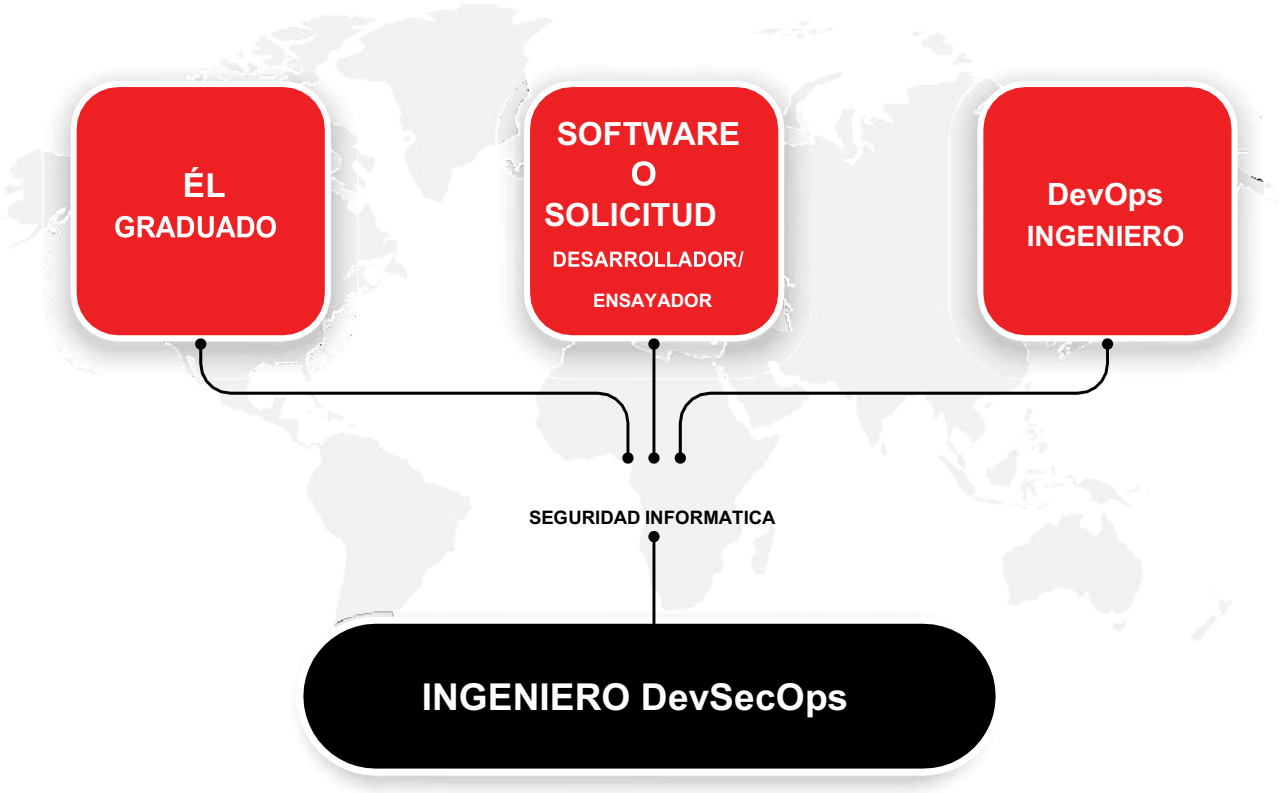
El Informe sobre el estado de la nube de 2022 de Flexera reveló que el 89 % de las organizaciones tienen una estrategia de nubes múltiples.[4]Con las empresas que migran a la nube, implementar el enfoque DevSecOps puede ayudar a garantizar la seguridad y el cumplimiento.

E|CDE es el máscompleto Programa de certificación DevSecOps que se enfoca sobre la integración de la seguridad en las etapas de planificación, codificación, creación, prueba, implementación, lanzamiento, operación y supervisión del ciclo de vida de DevOps.

E|CDE es el DevSecOps más intensivo en laboratorio programa de certificación que cubre más de 80 laboratorios prácticos guiados entregados en forma de laboratorios virtuales en línea y laboratorios de aula fuera de línea. E|CDE cubre 32 locales laboratorios enfocados, 32 laboratorios enfocados en AWS y 29 laboratorios enfocados en Azure en E|CDE.

E|CDE es el DevSecOps más buscado programa de certificación, cubriendo un mejorado y una gama más amplia de herramientas DevSecOps y prácticas ampliamente practicadas en todas las industrias.

Trayectorias profesionales en profesiones de DevSecOps



Esquema del curso e información de la clase

MÓDULO 01|Comprender la cultura DevOps

MÓDULO 02|Introducción a DevSecOps

MÓDULO 03|Canalización de DevSecOps: etapa de planificación

MÓDULO 04|Canalización de DevSecOps: etapa de código

MÓDULO 05|Canalización de DevSecOps: etapa de compilación y prueba

MÓDULO 06|Canalización de DevSecOps: etapa de lanzamiento e implementación

MÓDULO 07|Canalización de DevSecOps: etapa de operación y supervisión

¿Qué aprenderán los estudiantes?

- Comprenda los cuellos de botella de seguridad de DevOps y descubra cómo la cultura, la filosofía, las prácticas y las herramientas de DevSecOps pueden mejorar la colaboración y la comunicación entre losequipos de desarrollo y operaciones.
- Comprender la cadena de herramientas de DevSecOps y cómo incluir controles de seguridad en canalizaciones automatizadas de DevOps.
- Integre Eclipse y GitHub con Jenkins para crear aplicaciones.
- Alinear las prácticas de seguridad como la recopilación de requisitos de seguridad, el modelado de amenazas y las revisiones de código seguro con los flujos de trabajo de desarrollo.
- Integrar herramientas de modelado de amenazas como Threat Dragon, ThreatModeler y Threatspec; gestionar los requisitos de seguridad con Jira y Confluence; y use Jenkins para crear una canalización segura de CI/CD.
- Comprender e implementar pruebas de seguridad continuas con pruebas de seguridad de aplicaciones estáticas, dinámicas e interactivas y herramientas SCA (p. ej., Snyk, SonarQube, StackHawk, Checkmarx SAST, Debricked, WhiteSource Bolt).
- Integre herramientas de autoprotección de aplicaciones en tiempo de ejecución como Hdiv, Sqreen y Dynatrace que protegen las aplicaciones durante el tiempo de ejecución con menos falsos positivos y solucionan las vulnerabilidades conocidas.
- Integre SonarLint con los IDE de Eclipse y Visual Studio Code.
- Implementar herramientas como el complemento JFrog IDE y la plataforma Codacy.
- Integre pruebas de seguridad automatizadas en una canalización de CI/CD mediante Amazon CloudWatch; registro de contenedores elásticos de Amazon; y AWS CodeCommit, CodeBuild, CodePipeline, Lambda y Security Hub.
- Implementar varias herramientas y prácticas de automatización, incluidas Jenkins, Bamboo, TeamCity y Gradle.
- Realiza escaneos continuos de vulnerabilidades en compilaciones de datos y productos utilizando herramientas automatizadas como Nessus, SonarCloud, Amazon Macie y Probely.
- Implementar herramientas de prueba de penetración como gitGraber y GitMiner para proteger las canalizaciones de CI/CD.
- Utilice las herramientas de AWS y Azure para proteger las aplicaciones.
- Integrar herramientas automatizadas para identificar errores de configuración de seguridad que podrían exponer información confidencial y provocar ataques.
- Comprender el concepto de infraestructura como código , provisión y configuración de infraestructura utilizando herramientas como Ansible, Puppet y Chef.
- Audite las inserciones de código, las canalizaciones y el cumplimiento mediante herramientas de registro y supervisión como Sumo Logic, Datadog, Splunk, la pila ELK y Nagios.
- Utilice herramientas de monitoreo y alerta automatizadas (por ejemplo, Splunk, Azure Monitor, Nagios) y cree un sistema de alerta y control en tiempo real.
- Integre herramientas de cumplimiento como código como Cloud Custodian y el marco DevSec para garantizar que se cumplan los requisitos regulatorios o de cumplimiento de la organización sin obstaculizar la producción.
- Escanea y protege la infraestructura usando escáneres de contenedores e imágenes (Trivy y Qualys) y escáneres de seguridad de infraestructura (Bridgecrew y Checkov).
- Integre herramientas y prácticas para generar comentarios continuos en la canalización de DevSecOps mediante notificaciones por correo electrónico de Jenkins y Microsoft Teams.
- Integre herramientas de alerta como Opsgenie con herramientas de administración y monitoreo de registros para mejorar el rendimiento y la seguridad de las operaciones.

¿Quién puede beneficiarse de la E|CDE?

- Profesionales certificados por C|ASE
- Profesionales de seguridad de aplicaciones
- Ingenieros DevOps
- Ingenieros y probadores de software
- Profesionales de la seguridad informática
- Ingenieros y analistas de ciberseguridad
- Cualquier persona con conocimientos previos de seguridad de aplicaciones que desee desarrollar su carrera en DevSecOps

Roles laborales alineados con el E|CDE

- Ingeniero DevSecOps
- Ingeniero sénior de DevSecOps
- Ingeniero de Cloud DevSecOps
- Ingeniero de Azure DevSecOps
- Ingeniero de AWS DevSecOps
- Analista de DevSecOps
- Especialista en DevSecOps
- Ingeniero de operaciones DevSecOps
- Administrador de sistemas DevSecOps
- Ingeniero de sistemas DevSecOps
- Consultor DevSecOps
- Ingeniero de CI/CD de DevSecOps
- InfraestructuraDevSecOpsengineer

Requisitos previos del curso

Los estudiantes deben comprender los conceptos de seguridad de las aplicaciones.

Información de capacitación de E|CDE

Título del curso: Ingeniero de DevSecOps certificado por el EC-Council (E|CDE) **Duración del entrenamiento:**3 días

iLearn (autoaprendizaje)

Un entorno asincrónico de autoaprendizaje que ofrece el E|CDE curso en formato de video streaming

iWeek (en vivo en línea)

Aprendizaje en línea sincrónico dirigido por un instructor, lo que permite a los estudiantes asistir el curso E|CDE desde cualquier lugar

academia

Ofrece el E|CDE a través de EC-Council Academia Instituciones asociadas para estudiantes matriculados en programas universitarios o universitarios aplicables

CapacitaciónPartnerFormación dirigida por un instructor

El E|CDE está disponible en todo el mundo a través de los socios de formación autorizados de EC-Council. Este modo le ofrece el beneficio de aprender del Consejo de la CE experimentado y certificado instructores junto con sus compañeros.

Título del examen Certificado por el Consejo de la CE Ingeniero DevSecOps (E|CDE)	Código de examen 312-97	numero de preguntas 100
Duración 4 horas	Disponibilidad Portal de exámenes del EC-Council	Formato de prueba Opción multiple	Puntaje de aprobación 70.00%

Acerca deConsejo CE

El único propósito de EC-Council es construir y perfeccionar la profesión de ciberseguridad a nivel mundial. Ayudamos a individuos, organizaciones, educadores y gobiernos a abordar los problemas de la fuerza laboral global a través del desarrollo y la selección de programas educativos de seguridad cibernética de clase mundial y sus certificaciones correspondientes, y proporcionamos servicios de seguridad cibernética a algunas de las empresas más grandes del mundo.

Con la confianza de 7 de Fortune 10, 47 de Fortune 100, el Departamento de Defensa, la Comunidad de Inteligencia, la OTAN y más de 2000 de las mejores universidades, colegios y empresas de capacitación, nuestros programas han proliferado en más de 140 países y han establecido la barra en la educación en ciberseguridad.

Mejor conocido por el programa Certified Ethical Hacker, estamos dedicados a equipar a más de 230 000 soldadosde la era de la información con los conocimientos, las habilidades y las capacidades para ganar. contra los adversarios de sombrero negro. EC-Council desarrolla capacidades cibernéticas individuales y de equipo/organizaciones a través del programa Certified Ethical Hacker, seguido de una variedad de otros programas cibernéticos que incluyen Usuario certificado de computadora segura, Investigador forense de piratería informática, Analista de seguridad certificado, Defensor de red certificado, Analista SOC certificado, Analista de inteligencia de amenazas, controlador certificado de incidentes y director de seguridad de la información certificado.

Somos una organización acreditada por ANSI 17024 y hemos obtenido el reconocimiento del Departamento de Defensa bajo la Directiva 8140/8570, en el Reino Unido por parte de GCHQ, CREST y una variedad de otros organismos autorizados que influyen en toda la profesión. Fundada en 2001, EC-Council emplea a más de 400 personas en todo el mundo con 10 oficinas globales en EE. UU., Reino Unido, Malasia, Singapur, India e Indonesia. Sus oficinas en EE. UU. están en Albuquerque, NM y Tampa, FL.

DIGITAL BUSINESS

EC-Council

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