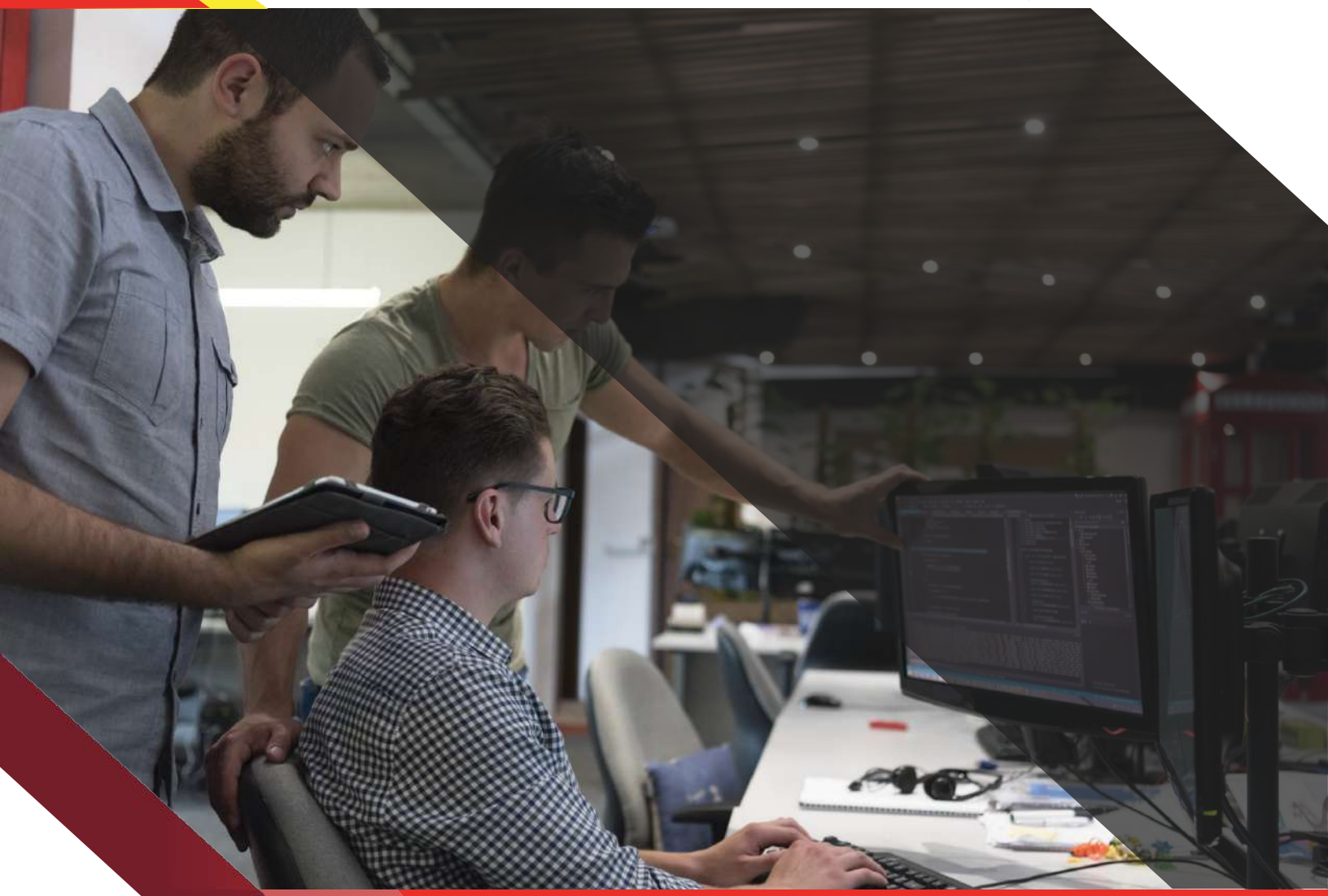
EC-Council

C|ASE .NET
Certified Application Security Engineer

C|ASE JAVA
Certified Application Security Engineer

TGK
DIGITAL BUSINESS



Ingeniero de Seguridad de Aplicaciones Certificado

www.tgk.com.mx

EC-Council

Descripción del curso

La credencial de "Certified Application Security Engineer" (CASE) fue desarrollado en colaboración con expertos en aplicación y desarrollo de software a nivel mundial.

El CASE evalúa las habilidades y conocimientos de seguridad críticos requeridos a lo largo de un ciclo de vida típico de desarrollo de software (SDLC), centrándose en la importancia de implementar metodologías y prácticas seguras en el entorno operativo inseguro actual.

El programa de capacitación certificado de CASE fue desarrollado para preparar a profesionales del software con las capacidades esperadas por empleadores y académicos a nivel global. Está diseñado como un curso de capacitación integral y práctico en seguridad de aplicaciones para enseñar a profesionales del software a crear aplicaciones seguras.

El programa de capacitación abarca actividades de seguridad en todas las fases del SDLC seguro: planificación, creación, pruebas e implementación de una aplicación.

A diferencia de otras capacitaciones en seguridad de aplicaciones, CASE va más allá de las pautas de prácticas de codificación segura e incluye la recopilación de requisitos seguros, el diseño robusto de aplicaciones y el manejo de problemas de seguridad en las fases posteriores al desarrollo de aplicaciones.

Esto hace que CASE sea una de las certificaciones de seguridad de aplicaciones más completas para el desarrollo de software seguro en el mercado actual. Es deseado por ingenieros, analistas y probadores de aplicaciones de software de todo el mundo y es respetado por las autoridades de contratación.

Seguridad de Aplicaciones: la Tendencia Actual y la SIGUIENTE GRAN NOVEDAD.

Para la mayoría de las organizaciones, el software y las aplicaciones determinan su éxito. Sin embargo, la rapidez, la duplicación y el ahorro de costos a menudo ocupan un lugar central, mientras que las consideraciones de seguridad quedan en segundo plano o ni siquiera se consideran. Una aplicación insegura o vulnerable pone a estas empresas en riesgo.

1.8 mil millones de sitios web activos

gestionados por 21 millones de desarrolladores en todo el mundo. Es una de las economías más grandes, con una proyección de $5.6 billones para el año 2021.

3.5 mil millones de usuarios

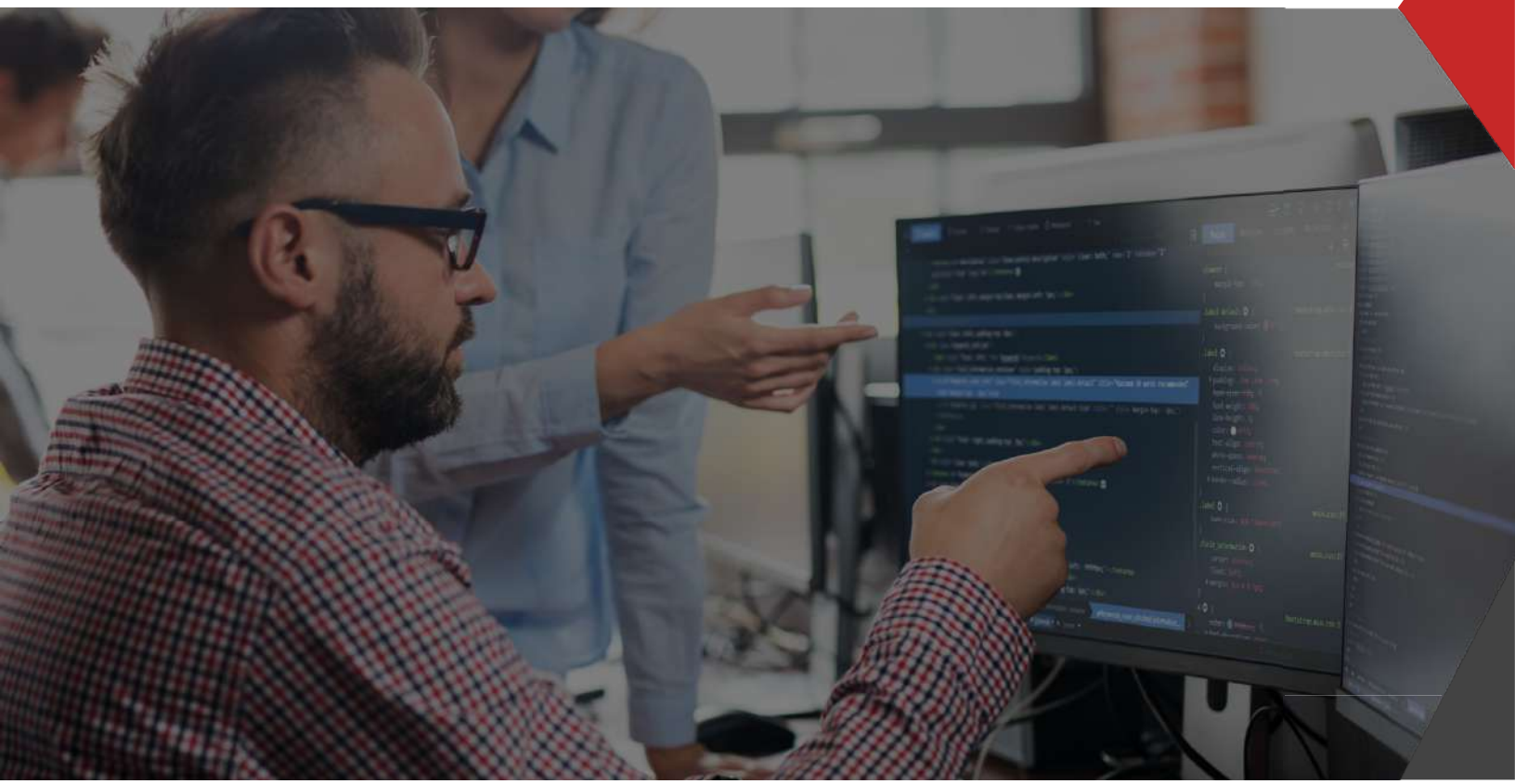
lo que convierte a Internet en la plataforma más grande para el robo de identidad y fraude financiero.

En promedio ocurren 19 vulnerabilidades por día

con más del 50% de ellas consideradas críticas. Además, se ha descubierto que el 64% del 1 millón de sitios web principales, según Alexa, tienen vulnerabilidades.

¿Perteneces al grupo que sigue prácticas de codificación e implementación inseguras? ¿Eres uno de los 21 millones que ponen en riesgo la seguridad del software o de las aplicaciones web, lo que podría resultar en pérdidas catastróficas?

Ingeniero de Seguridad de Aplicaciones Certificado (CASE)



El riesgo de seguridad no se limita solo a las aplicaciones web.

Varios establecimientos minoristas reconocidos a nivel mundial han enfrentado enormes brechas de datos recientemente debido a que ignoraron la seguridad de las aplicaciones.

Empresas multimillonarias con presencia global han sufrido filtraciones masivas de datos, incluyendo la información personal y financiera de sus clientes y empleados, debido a fallas en sus aplicaciones.

Gigantes minoristas como Forever 21, GameStop, Panera Bread, Sonic, KMart y Hudson Bay (Saks Fifth Avenue) se encuentran en la lista de minoristas con miles de sucursales que utilizaron máquinas de punto de venta (POS) o pasarelas de pago que presuntamente resultaron en robos de información. También hay muchas plataformas digitales modernas como Uber, Yahoo, Dropbox, Adobe, LinkedIn y Tumblr que han enfrentado brechas similares debido a la misma razón: la falta de seguridad en las aplicaciones.

Seguridad de Aplicaciones

¿Qué tan seguro estás?

75%

de los ataques cibernéticos se dirigen a aplicaciones web.

90%

de las aplicaciones Java contienen al menos una vulnerabilidad.

69%

de los ataques a aplicaciones web aumentaron en 2017.

.NET

¡El espacio entre el parcheo de software y la seguridad es amplia!

El marco de trabajo .NET ha ganado popularidad debido a su naturaleza de código abierto, interoperabilidad, independencia del lenguaje, amplia biblioteca de códigos y facilidad de implementación. Se ha convertido en la opción preferida para los desarrolladores de aplicaciones.
Sin embargo, hay pocas clases que enseñen a los desarrolladores cómo asegurarse de que su código sea seguro y correcto. Además, cualquier brecha en el proceso de desarrollo e implementación de aplicaciones puede ser perjudicial. Los desarrolladores de .NET a menudo aprenden seguridad en el trabajo. Esto se debe principalmente a que la educación básica de programación generalmente no cubre o enfatiza las preocupaciones de seguridad.

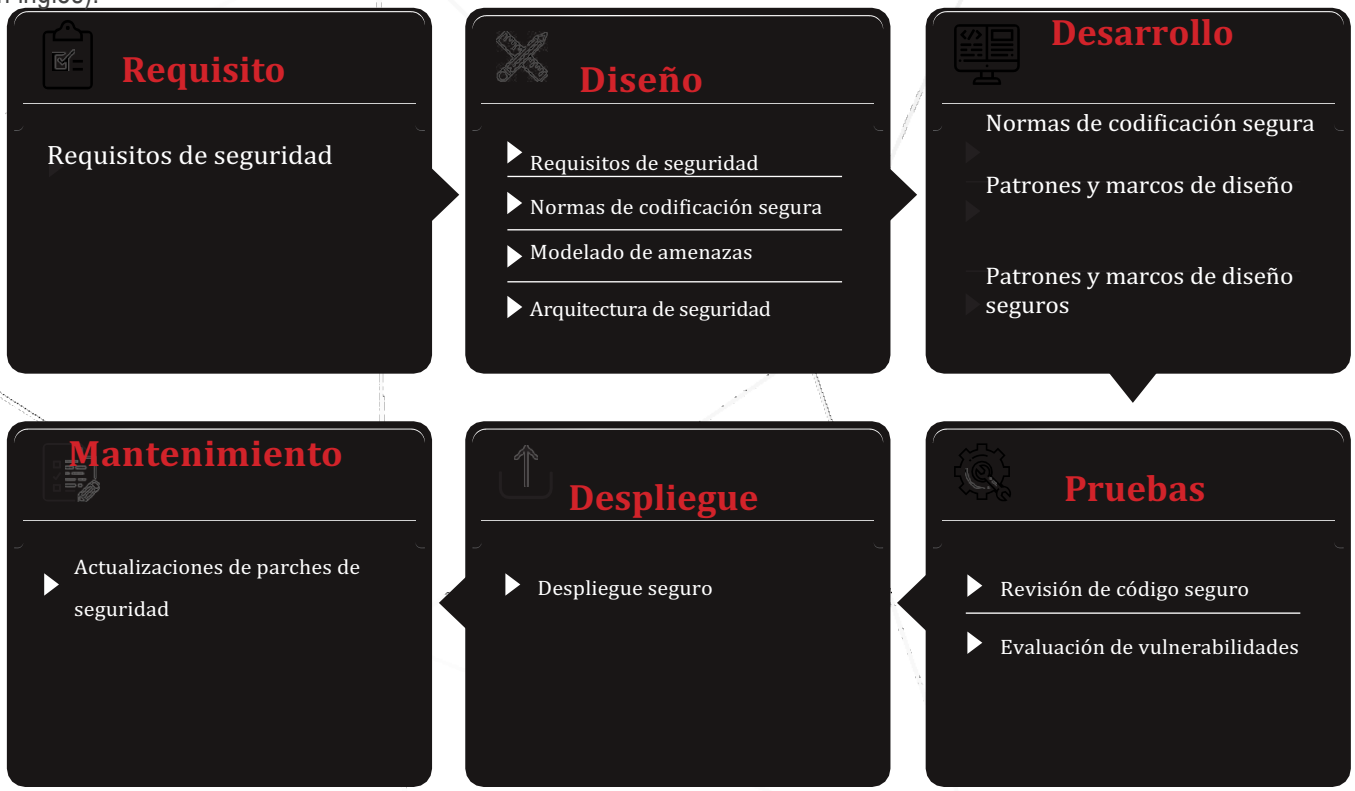
Java

¿Las aplicaciones basadas en Java: las más populares y al mismo tiempo las más vulnerables?

Según el Informe del Estado de Seguridad del Software de 2017, casi el 90% de las aplicaciones Java contienen uno o más componentes vulnerables, lo que las convierte en puntos ideales de entrada para atacantes hostiles.
Aunque Java ha avanzado mucho desde su desarrollo en 1995, el cibercrimen también se ha extendido, alcanzando niveles epidémicos, lo que aumenta la necesidad de desarrolladores de Java seguros, ya sea que estén creando un nuevo programa o actualizando uno antiguo.

Proceso de Desarrollo de Software Seguro

El programa Certified Application Security Engineer (CASE) ofrece un enfoque integral de seguridad de aplicaciones que abarca las actividades de seguridad involucradas en todas las fases del Ciclo de Vida del Desarrollo de Software (SDLC, por sus siglas en inglés).



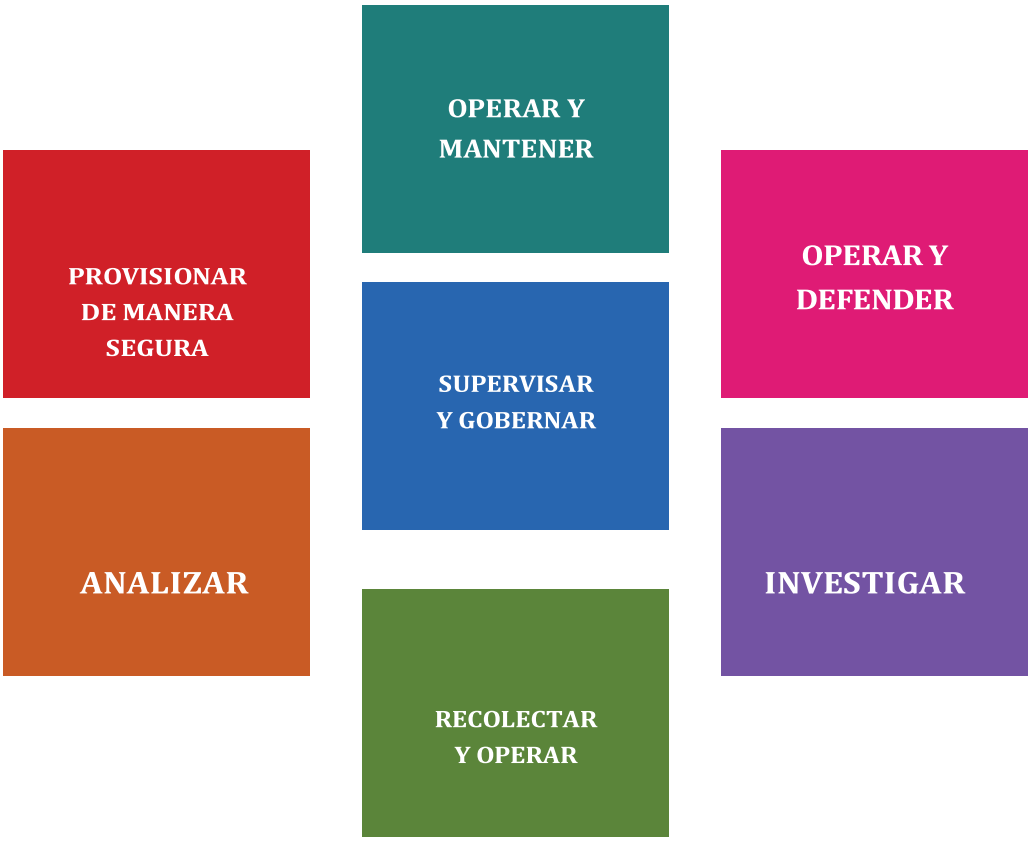
Lo que aprenderás

- Comprender en profundidad el ciclo de vida de desarrollo seguro de aplicaciones (SDLC) y los modelos de SDLC seguros.
- Conocer el OWASP Top 10, la modelación de amenazas, SAST y DAST.
- Capturar los requisitos de seguridad de una aplicación en desarrollo.
- Definir, mantener y aplicar las mejores prácticas de seguridad de aplicaciones.
- Realizar revisiones de código manuales y automáticas de aplicaciones.
- Realizar pruebas de seguridad de aplicaciones web para evaluar las vulnerabilidades.
- Desarrollar un programa integral de seguridad de aplicaciones.
- Clasificar la gravedad de los defectos y publicar informes detallados sobre los riesgos y las mitigaciones asociadas.
- Trabajar en equipo para mejorar la postura de seguridad.
- Utilizar tecnologías de escaneo de seguridad de aplicaciones como AppScan, Fortify, WebInspect, pruebas estáticas de seguridad de aplicaciones (SAST), pruebas dinámicas de seguridad de aplicaciones (DAST), inicio de sesión único y cifrado.
- Seguir estándares de codificación segura basados en las mejores prácticas aceptadas por la industria, como la
- Guía OWASP o el CERT Secure Coding, para abordar vulnerabilidades de codificación comunes.
- Crear un proceso de revisión de código fuente como parte de los ciclos de desarrollo (SDLC, Agile, CI/CD).

Principales Componentes de CASE

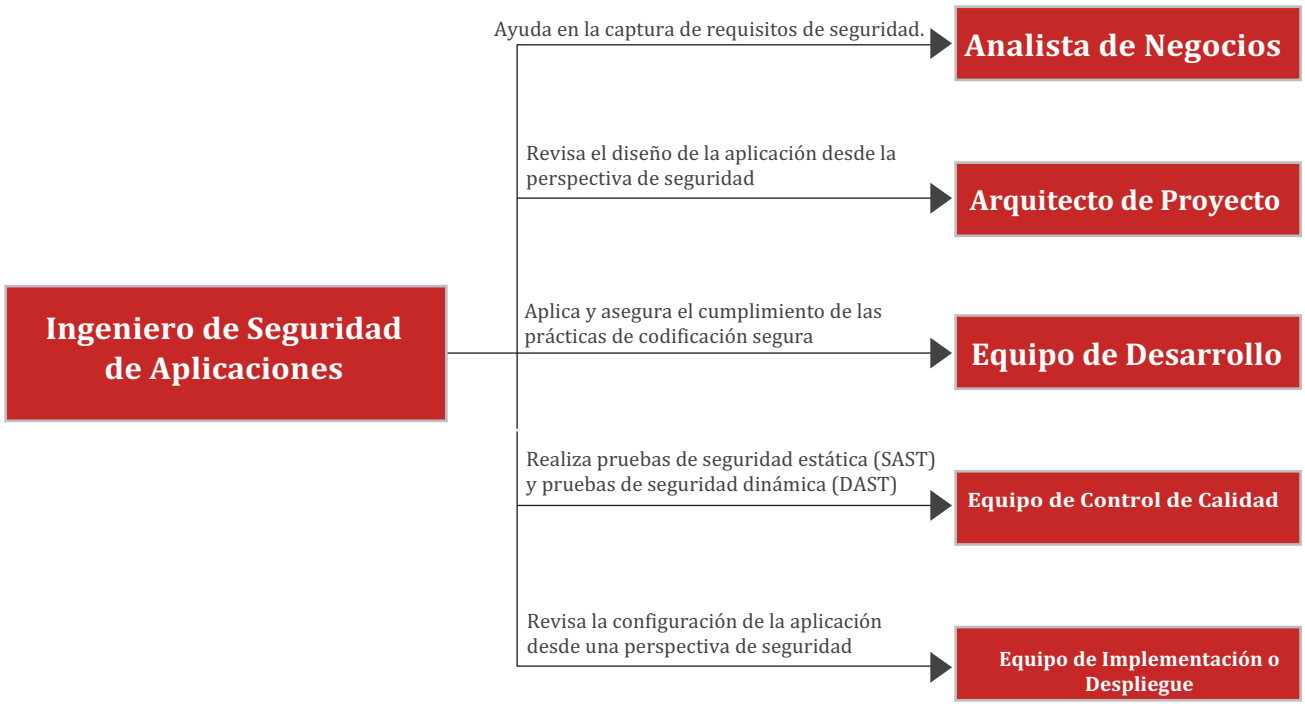
La certificación CASE es la credencial de seguridad de aplicaciones que cumple con los estándares de la industria actual, ya que es un programa completo y práctico de seguridad de aplicaciones.

1. Seguridad más allá de la codificación segura - Desafiar la mentalidad tradicional de que la codificación segura significa una aplicación segura.
2. Pruebas y certificación del desarrollo seguro de aplicaciones en todo el ciclo de vida del desarrollo de software.
3. El programa de capacitación más completo para desarrolladores de aplicaciones que cubre técnicas como validación de entrada, prácticas de codificación defensiva, autenticación y autorización, ataques criptográficos, manejo de errores, técnicas de gestión de sesiones, entre muchas otras.
4. Una amplia gama de laboratorios para asegurar la práctica en situaciones del mundo real.
5. Disponible para .NET y Java
6. Se mapea a la “Categoría Provisión Segura" en el Marco NICE 2.0.



Análisis de Tareas Laborales

Para asegurar aún más que CASE sea relevante en los benchmarks adecuados, se diseñó para proporcionar el Análisis de Tareas Laborales (JTA, por sus siglas en inglés) de roles involucrados en la seguridad de aplicaciones, así como en muchas Áreas Especializadas dentro de la categoría "Provisión Segura" en el Marco NICE 2.0.



Esquema del Curso de CASE

- Comprensión de la seguridad de aplicaciones, amenazas y ataques
- Recopilación de requisitos de seguridad
- Diseño y arquitectura segura de aplicaciones
- Prácticas de codificación segura para la validación de entrada
- Prácticas de codificación segura para la autenticación y autorización
- Prácticas de codificación segura para la criptografía
- Prácticas de codificación segura para la gestión de sesiones
- Prácticas de codificación segura para el manejo de errores
- Pruebas estáticas y dinámicas de seguridad de aplicaciones (SAST y DAST)
- Implementación y mantenimiento seguros.

"El 100% de las aplicaciones web son vulnerables a los hackers.

- Informe de Seguridad Global 2018 de Trustwave

¿Para quién está diseñado CASE?

Desarrolladores de .NET y Java con al menos 2 años de experiencia, así como individuos que deseen convertirse en ingenieros, analistas o probadores de seguridad de aplicaciones.

Individuos involucrados en el rol de desarrollar, probar, gestionar o proteger aplicaciones.

Duración

Formación Total - 24 horas o 3 sesiones completas de día completo

Material del curso

Todos los participantes recibirán una copia personal del material del curso de CASE, un cupón para el examen de CASE de EC-Council, y acceso a iLabs (el entorno de laboratorios en la nube de EC-Council).

Certificación

El examen de CASE se puede presentar después de asistir a la capacitación oficial de CASE. Los candidatos que aprueben con éxito el examen recibirán su certificado de CASE y los privilegios de membresía. Los miembros están obligados a cumplir con las políticas de la Política de Educación Continua de EC-Council.

¡La seguridad de las aplicaciones ya no es una idea secundaria, sino una prioridad absoluta!

Obtener la certificación de Ingeniero de Seguridad de Aplicaciones

CASE permite a los desarrolladores y probadores de aplicaciones demostrar su dominio de los conocimientos y habilidades necesarios para manejar vulnerabilidades comunes de seguridad del software de aplicaciones.

- **Título del examen: Ingeniero de Seguridad de Aplicaciones Certificado**
- **Número de preguntas: 50**
- **Duración del examen: 2 horas**
- **Formato del examen: Preguntas de opción múltiple**
- **Puntuación de aprobación: 70%**
- **Disponibilidad: Portal de Exámenes de EC-Council**

Criterios de elegibilidad

Para ser elegible para presentar el Examen CASE, el candidato debe cumplir con alguno de los siguientes requisitos:

- Asistir a la capacitación oficial de EC-Council CASE a través de un Centro de Capacitación Acreditado de EC-Council (Accredited Training Centre/iWeek/iLearn) (Todos los candidatos deben pagar una tarifa de solicitud de USD 100 a menos que la tarifa de capacitación ya la incluya) o

- Ser miembro activo en buen estado de ECSP (.NET o Java) (no es necesario pagar una tarifa de solicitud duplicada, ya que esta tarifa ya ha sido pagada) o

- Tener al menos 2 años de experiencia laboral en seguridad de la información o diseño de software (se deberá pagar una tarifa de solicitud no reembolsable de USD 100) o

- Tener otras certificaciones equivalentes de la industria, como GSSP .NET/Java (se deberá pagar una tarifa de solicitud no reembolsable de USD 100).

DIGITAL BUSINESS

EC-Council

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