



SÉ

INTERNACIONAL

Programa Internacional en
DESARROLLO DE SOFTWARE Y PROGRAMACIÓN SEGURA

INFORMACIÓN ACADÉMICA

Descripción del programa

La Certificación en Desarrollo de Software y Programación está diseñada para potenciar los conocimientos y formación de desarrolladores en programación segura y mejorar las habilidades de los auditores de seguridad en el análisis y evaluación del código fuente de las aplicaciones.

Justificación del programa

Hoy en día casi todas las empresas/negocios/personas realizan operaciones en línea, es por ello que los desarrolladores de las aplicaciones, deben garantizar la protección de datos sensibles. Con el fin de proteger los datos y proporcionar directrices de desarrollo de aplicaciones seguras, Deloitte CyberSOC Academy ha desarrollado este programa. El mismo expone al alumno a diferentes lenguajes de programación y entornos de desarrollo. El temario engloba un análisis en profundidad de los riesgos presentes en cada uno de los diferentes entornos, así como las mejores prácticas seguidas por los desarrolladores más expertos para el desarrollo de aplicaciones seguras y estables. Adicionalmente, el programa abarca técnicas específicas para la identificación de vulnerabilidades en código fuente y para la ejecución de acciones que mitiguen el impacto de una aplicación inicialmente comprometida.

Deloitte se ha posicionado como consumidor de software seguro a través del uso de estas herramientas en el CyberSOC-Academy y como fabricante de este tipo de aplicaciones. Los formadores de este programa son profesionales de la seguridad y del desarrollo de software seguro.

Objetivo General

El objetivo principal del Programa Internacional en Desarrollo de Software y Programación es, desde un punto de vista neutral con respecto a fabricantes y tecnologías, el de enseñar a identificar vulnerabilidades en el código fuente de las aplicaciones, establecer los riesgos asociados a cada vulnerabilidad y definir las acciones correctivas que sean necesarias durante el ciclo de desarrollo del software.

Perfil del aspirante

Con un enfoque pedagógico y profesional, este programa está dirigido a personas, referentemente graduados y graduadas de la rama de Ingeniería Informática y a profesionales del área, que quieran adquirir las competencias y capacidades necesarias para desempeñar labores en el ámbito del Desarrollo Seguro de aplicaciones y de las auditorías del código fuente de aplicaciones.

El aspirante debe contar con conocimiento básico sobre lenguajes y entornos de programación. Deberá conocer los esquemas básicos de la programación estructurada, así como de la programación orientada a objetos.

Los estudiantes matriculados en el programa Desarrollo de Software y Programación deberán tener capacidad de estudio, voluntad de trabajo y sobre todo vocación por la seguridad de sistemas informáticos en general y de las aplicaciones y el software en particular.

Perfil profesional del egresado

Una vez cursados los estudios completos de este título el egresado podrá desarrollar labores profesionales como:

- Analista/Programador/Auditor/Consultor de seguridad de sistemas de información
- Analista/Programador/Auditor/Consultor de seguridad de aplicaciones informáticas
- Analista/Programador/Auditor/Consultor de seguridad de aplicaciones web.

ESTRUCTURA DEL CURSO

Duración

La Certificación Internacional en Desarrollo de Software y Programación segura está conformada por 4 cursos, cada uno de 40 horas.

Título que otorga

Certificado Internacional en Desarrollo de Software y Programación (certificado por Deloitte).

Registro Oficial

No requiere registro oficial ya que se trata de estudios de 4to nivel o educación no formal.

Entrega de Diploma

Una vez finalizado el curso y el certificado en aproximadamente tres meses se estaría recibiendo el Diploma de cada curso y del certificado completo.

Área de conocimiento

Seguridad informática – Ingeniería de Sistemas

Nivel y Modalidad (Sincrónica / Asincrónica)

Online: 100% virtual.

Offline: Descarga los contenidos de los cursos en tu computador para que puedas estudiar sin conexión a internet.

Educación a distancia

- Los alumnos trabajan de forma independiente y a su vez en continuo intercambio con los Profesores Tutores a través del formato de educación a distancia de Red Ilumno.
 - Estimulación del aprendizaje activo permitiéndole a los estudiantes lograr aprendizajes significativos, contribuyendo a ser partícipes en todo el proceso de enseñanza y de aprendizaje.
 - Contenidos especializados en línea Comunidades de aprendizaje Interacción y comunicación constante entre los estudiantes, los Profesores de primer nivel junto al Director del Programa, brindando una oportunidad significativa de intercambio con los profesionales más destacados.
-

- Tecnología interactiva 2.0 en constante desarrollo e investigación

Idiomas del curso

Contenidos disponibles en español y portugués.

Plataforma y Materiales

Plataforma Ilumno: Una de las plataformas más modernas del mercado, los materiales estarán disponibles de forma digital en la plataforma.

Plan de Estudios

El plan de estudios consta de los siguientes cursos:

Curso 1. Introducción al Desarrollo Seguro.

El desarrollo de aplicaciones seguras, sobre todo si éstas van a dar soporte a procesos de negocio o van a estar expuestas a Internet, es el mejor mecanismo de defensa de los activos de una organización ante los ciber-ataques. La exposición masiva de estas aplicaciones vía web, desde cualquier punto del planeta, por cualquier persona, multiplica las posibilidades de que las vulnerabilidades de estos aplicativos sean explotadas interrumpiendo servicios (ataques por denegación de servicio), afectando a la integridad y confidencialidad de los datos (éstos pueden ser extraídos o manipulados), dando lugar a todo tipo de problemas y sanciones por incumplimientos normativos o legales, sin olvidar las repercusiones en la reputación o los daños a la imagen que pueden sufrir las compañías que sufren dichos ataques.

Objetivo general:

Introducir al alumno en la disciplina del Desarrollo Seguro de software. El alumno se iniciará en la definición de ciclos de vida para el de desarrollo seguro de software, en la identificación de errores comunes, vulnerabilidades y agujeros de seguridad del código fuente, identificando aquellos aspectos que pueden representar un riesgo para datos y comunicaciones en la fase de explotación del software. El curso no está centrado en ninguna tecnología concreta sino en una visión global y Universal, común a cualquier entorno de desarrollo.

Contenido.

Módulo 1. Introducción al Desarrollo Seguro

- Cómo afectan las vulnerabilidades a mi negocio.
- Seguridad de la información
- Desarrollo y Análisis de código
- OWASP TOP 10

Módulo 2. Conoce a tu enemigo

- Perfil de un atacante
 - Como ve un atacante nuestra aplicación
 - Protocolo HTTP simple y fácilmente manipulable
 - Let's Try!! Practica e interioriza
-

Módulo 3. Conceptos básicos y genéricos del desarrollo seguro

- Descripción de una arquitectura segura.
- Tipos de fallos de seguridad en software. Top 10
- Ciclo de desarrollo de software seguro.
- Metodos de detección

Módulo 4. Programación segura en e-commerce

- Terminología.
- Obtención segura de información confidencial.
- Custodia segura de información confidencial.
- Manejo seguro de información confidencial.
- Normativa PCI.

Curso 2. Certificación en OWASP 2013

La explosión masiva de aplicaciones web en todo Internet ha supuesto un reto para la seguridad de las tecnologías de la información. Actualmente los atacantes en Internet enfocan sus esfuerzos a la capa de aplicación pues es la menos protegida y la más fácil de vulnerar y se ha demostrado que la mejor protección a estas incidencias es la formación de los programadores en desarrollo seguro.

Objetivo general:

Introducir al alumno, desde un punto de vista neutral con respecto a las distintas tecnologías de desarrollo y a los distintos lenguajes de programación, a la metodología OWASP TOP TEN comúnmente utilizada. El alumno se iniciará en la descripción de las TOP 10 vulnerabilidades definidas por OWASP 2013 y de los ataques más comunes para la explotación de dichas vulnerabilidades. Este curso es fundamental y base para entender cómo suceden la mayoría de los ataques que se producen hoy en día en Internet. El curso es de interés para cualquier usuario responsable de una pequeña página web, así como para los administradores de grandes portales corporativo.

Contenido.**Módulo 1. Introducción a OWASP y OSSTM**

Introducción

Introducción a la Metodología OSSTM

Introducción a la Metodología OWASP

Estándar PCI-DSS

Módulo 2. Visión general de OWASP

Riesgos de seguridad en aplicaciones web

Visión general OWASP 2013 "Top 10"

Cambios con respecto a OWASP 2010

Resumen de los factores de riesgo

Verificación de pruebas OWASP 2013

Otros recursos OWASP

Módulo 3. Vulnerabilidades en las aplicaciones

- Introducción
- Tipos de vulnerabilidades
- Etapas en las vulnerabilidades
- Búsqueda de vulnerabilidades
- Transmisión de la información
- Mercado de vulnerabilidades

Módulo 4. Scoring de vulnerabilidades

- Enumeración de vulnerabilidades
- Mediciones y sistemas de puntuación
- Medidas de prevención contra las vulnerabilidades

Curso 3. Contramedidas Owasp para las principales vulnerabilidades En Java, Net y Php

Por primera vez se configura en un mismo curso un compendio de contramedidas atendiendo a la metodología OWASP TOP 10, para los principales entornos de desarrollo actualmente en el mercado como son JAVA, NET y PHP.

Objetivo general:

Atendiendo a la metodología OWASP TOP 10 comúnmente utilizada, establecer y definir por primera vez en un mismo curso, una guía de contramedidas que ayudarán a evitar las principales TOP 10 vulnerabilidades de las aplicaciones web. El alumno se iniciará en la descripción de las contramedidas para las TOP 10 vulnerabilidades definidas por OWASP 2013 para los ataques más comunes que se suceden por la explotación de dichas vulnerabilidades. Este curso es fundamental y base para evitar y mitigar la mayoría de los ataques que se producen hoy en día en Internet. El curso es de interés para cualquier usuario responsable de una pequeña página web, así como para los administradores de grandes portales corporativos.

Contenido.**Módulo 1. A1 (Inyección SQL)**

- Introducción
- Descripción A1 - Inyección SQL
- Contramedidas

Módulo 2. A2 (Pérdida de autenticación y gestión de sesiones)

- Introducción
- Descripción A2 – Pérdida de autenticación y gestión de sesiones
- Contramedidas

Módulo 3. A3 (Secuencias de comandos en sitios cruzados - XSS)

- Introducción
 - Conceptos Básicos
 - Definición de ataques XSS
 - Tipos de ataques XSS
 - Fases de un ataque XSS
 - Metodologías de ataques XSS
-

- Detectar aplicación web vulnerable a ataques XSS
- Ejemplos de ataques XSS 3.9. Práctica local
- Contramedidas

Módulo 4. A8 (Falsificación de peticiones en sitios cruzados - CSRF)

- Introducción
- Descripción A8 – Falsificación de peticiones en sitios cruzados
- Política del mismo origen (SOP)
- Ejemplos y práctica local
- Contramedidas

Curso 4. Buenas prácticas para el Desarrollo Seguro.

Hoy en día no existen guías de desarrollo seguro para analistas y programadores que definan una checklist completa para aquellos aspectos a tener en cuenta en el ciclo de desarrollo de software, desde el punto de vista de la seguridad. En este curso se ofrece la guía de mejores prácticas diseñada por los expertos desarrolladores y auditores de Deloitte CyberSOC.

Objetivo general:

Atendiendo a la metodología OWASP TOP 10, establecer y definir por primera vez en un mismo curso, una guía de buenas prácticas que ayudarán a evitar las principales TOP 10 vulnerabilidades de las aplicaciones web. El alumno, una vez finalizado el curso, estará en disposición de definir procedimientos y políticas de desarrollo de código dentro de una misma organización, así como de establecer los controles necesarios para la fabricación de software seguro. El curso es de interés para cualquier usuario responsable de una pequeña página web, administradores de grandes portales corporativos, así como para analistas y programadores de una empresa del denominado software manufacturers.

Contenido

Módulo 1. Filtros

- Validación de entradas
- Codificación de salidas

Módulo 2. Sesiones y control de acceso

- Administración de autenticación y contraseñas
- Administración de sesiones
- Control de acceso

Módulo 3. Prácticas criptográficas

- Prácticas criptográficas
- Criptografía en JAVA
- Criptografía en .NET
- Criptografía en PHP

Módulo 4. Otras medidas

- Manejo de errores y logs
 - Protección de datos
 - Seguridad en comunicaciones
 - Configuración de los sistemas
-

- Seguridad de bases de datos
- Manejo de ficheros
- Manejo de memoria
- Prácticas generales

Nota: Es deseable para aprovechar este curso que el estudiante conozca los esquemas básicos de la programación estructurada, así como de la programación orientada a objetos. Se recomienda haber cursado “INTRODUCCIÓN AL DESARROLLO SEGURO”, “OWASP 2013” y “CONTRAMEDIDAS OWASP PARA LAS PRINCIPALES VULNERABILIDADES EN JAVA, NET Y PHP” de esta misma titulación.

Plan de Evaluación

- 4 Foros evaluables (el profesor asigna una calificación de acuerdo a la participación del alumno) por cada curso
- 1 Evaluación Autoevaluable (La plataforma califica automáticamente) por cada curso

Metodología

- Estimulación del aprendizaje activo permitiéndole a los estudiantes lograr aprendizajes significativos, contribuyendo a ser partícipes en todo el proceso de enseñanza y de aprendizaje
- Contenidos especializados en línea Comunidades de aprendizaje Interacción y comunicación constante entre los estudiantes, los Profesores de primer nivel junto al Director del Programa, brindando una oportunidad significativa de intercambio con los profesionales más destacados
- Tecnología interactiva 2.0 en constante desarrollo e investigación.

Docentes Desarrolladores y tutores

El valor añadido a los contenidos y tutorización de estos cursos viene dado por la capacidad formadora de los profesionales de Deloitte CyberSOC Academy, por su vasta experiencia en el campo de la ciberseguridad, en el que diariamente realizan auditorías de seguridad sobre el código fuente de las aplicaciones de nuestros clientes y sobre las nuestras mismas, incluyendo auditorías automatizadas y con metodología OWASP 2013.

Los tutores son propios de Deloitte, por lo cual están localizados en España, es importante considerarlo por temas de las diferencias horarias para la logística de foros, respuestas e interacción con los tutores. Se recomienda desde el inicio del Programa verificar los horarios de cada actividad.

Los profesionales que han desarrollado los materiales docentes y que serán los tutores encargados de este programa son miembros del equipo de formadores de Deloitte que lo componen consultores del área de Deloitte Cyber Risk Services, analistas de seguridad, expertos en ciberinteligencia y ciberfraude, hackers profesionales, desarrolladores y analistas de código fuente, todos ellos en primera línea de defensa de los sistemas de información y comunicaciones de clientes y Firma.

El equipo de Deloitte está altamente cualificado, con formación y certificaciones de relevancia en el sector de la Seguridad con el siguiente personal acreditado:

- 12 CISSP, Certified Information Systems Security Professionals.
- 93 CISAs, Certified Information Systems Auditor. Único título internacionalmente reconocido en el mundo de la auditoría informática, otorgado, por la Information Systems Audit and Control Association (ISACA).
- 46 CISM, Certified Information Security Manager.
- 17 SAP.
- 85 BS7799 / 27001
- 9 BS25999
- 4 CIA (Certified Internal Auditor)
- 64 ITIL (IT Infrastructure Library)
- 5 CEH (Certified Ethical Hacker)
- 8 CGEIT (Certified in the Governance of Enterprise IT)
- 13 CRISC (Certified in Risk and Information Systems Control)
- 1 CSSLP (Certified Secure Software Lifecycle Professional)
- 2 CDPP (Certified Data Privacy Professional)

Las capacidades, conocimientos y experiencia de los profesionales de Deloitte CyberSOC en la gestión de incidentes de seguridad, se encuentran avalados por la adjudicación, hace ya un año, del sello por la Universidad de Carnegie Mellon: CyberSOC-CERT Computer Emergency Response

Pre requisitos del programa

Para poder ingresar a este programa el aspirante debe ser graduados y/o graduadas de la rama de Ingeniería Informática, o profesionales del área, con conocimiento básico sobre lenguajes y entornos de programación. Además, deberá conocer los esquemas básicos de la programación estructurada, así como de la programación orientada a objetos.

Sistema de evaluación

- Para finalizar satisfactoriamente este curso, los alumnos deben tener una calificación de 70.00 o más en el curso. Para finalizar de manera exitosa, el alumno deberá leer el material de lectura, interactuar en los debates en línea y realizar las tareas asignadas.
 - Toda la participación se supervisará por medios electrónicos.
 - En relación con los trabajos atrasados, se podrán aplicar penalizaciones hasta de 5 puntos por cada día de demora a partir de la fecha y el horario de presentación, salvo que se haya acordado previamente lo contrario con el cuerpo docente.
-

ADMISIONES

Requisitos mínimos de inscripción

Llenado y entrega de formulario de inscripción de acuerdo a cada universidad. Fotocopia legible de un documento de identificación. Entrega del proceso administrativo realizado o la realización del primer pago

Calendario de Admisiones

Dos o tres veces al año se realizan admisiones. Se debe solicitar el calendario actualizado por Universidad para verificar las aperturas.

Valor de la inversión, descuentos y formas de pago

Esta información depende de la Universidad o país donde se encuentre el interesado, es importante tener en cuenta que cada Universidad cuenta con descuentos y diferentes formas de pago y financiamiento que facilitaran el ingreso al certificado.

Cambios de fecha- apertura

Existe un volumen mínimo de estudiantes para confirmar la fecha de apertura original del programa, es por ello que de no alcanzar ese mínimo el programa puede sufrir cambio de fecha, dicha información se comunicará por medio de los datos suministrados en el momento de la inscripción.

b



◀ SÉ ▶

INTERNACIONAL

ILUMNO Transforming how
the world learns