ILUMNO Transforming how the world learns

SÉ INTERNACIONAL

Programa Internacional en

AUDITORÍA DE SEGURIDAD DE SISTEMAS Y REDES

Deloitte.

INFORMACIÓN ACADÉMICA

Justificación del programa

Las organizaciones se enfrentan hoy en día a un amplio catálogo de amenazas de seguridad sobre sus sistemas digitales de información, gestión y negocio. La rápida evolución de estas ciber-amenazas sobre los activos internos y externos de las empresas representa actualmente el mayor porcentaje anual de pérdidas de estas empresas.

Enfocado a la identificación de vulnerabilidades en redes, sistemas y aplicaciones, este curso describirá las tecnologías y métodos utilizados actualmente por profesionales de "hacking ético" en Deloitte para la realización de tests de penetración y auditorías de seguridad. En este programa, eminentemente práctico, los alumnos serán instruidos en el desarrollo de técnicas y en el uso de herramientas que exploten al máximo sus habilidades y conocimientos para la realización de pruebas de penetración y análisis de vulnerabilidades. Adicionalmente, los contenidos de las sesiones prácticas permitirán al estudiante practicar los conocimientos adquiridos en entornos controlados de entrenamiento, no sólo a lo largo del desarrollo del curso, sino también una vez concluidas las sesiones presenciales de formación. Algunos datos de la evolución del Mercado de Ciber Seguridad son:

- El coste de la actividad del ciber crimen sigue en aumento año tras año, a un ratio del 26%
- Los ciber ataques se han posicionado como incidentes muy comunes y cotidianos. De media, 2 ataques exitosos por semana y empresa.
- Los ciber crímenes que producen las pérdidas más cuantiosas son los causados por DoS (denial of service), intrusiones a los sistemas de información y aquellos basados en web. Fuente: 2013 Cost of Cyber Crime Study: United States Ponemon Institute© Research Report

Todo lo anterior impulsa a la necesidad de llevar a cabo actividades de ciber seguridad y la necesidad de crear nuevos servicios de ciber seguridad.

Objetivo General

El objetivo del Certificación Internacional en Auditoría de Seguridad de Sistemas y Redes es, desde un punto de vista neutral con respecto a fabricantes y tecnologías, el de enseñar a identificar vulnerabilidades en redes, sistemas y aplicaciones, establecer los riesgos asociados a cada vulnerabilidad y definir las acciones correctivas que sean necesarias. El programa abarca también un módulo de análisis de código malicioso que, desde el punto de vista del auditor de seguridad, estudia la identificación de vulnerabilidades que explotan estos códigos dañinos.

Perfil del aspirante

Con un enfoque pedagógico y profesional, este curso está dirigido a graduados y graduadas (preferentemente de la rama de Ingeniería Informática) y a profesionales del área, que quieran adquirir las competencias y capacidades necesarias para desempeñar labores de auditorías de seguridad en infraestructuras de Internet o de red.

Los estudiantes matriculados deberán tener capacidad de estudio, voluntad de trabajo y sobre todo vocación para explorar sistemas informáticos en busca de vulnerabilidades.

Perfil profesional del egresado

Una vez cursados los estudios el egresado podrá trabajar, entre otras salidas, como:

- Analista/Auditor/Consultor de seguridad de sistemas de información
- Analista/Auditor/Consultor de seguridad de aplicaciones web
- Analista/Auditor/Consultor de seguridad en redes
- Analista de Malware
- White-Hat Hacker

ESTRUCTURA DEL CURSO

Duración

La Certificación Internacional en Auditoría de seguridad de Sistemas y Redes está conformada por 4 cursos.

Título que otorga

Certificación Internacional en Auditoría de seguridad de sistemas y redes con Sello 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

Ingeniería Informática

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

Curso 1: INTRODUCCIÓN AL HACKING ÉTICO

- Módulo 1: Introducción a la Seguridad
- Módulo 2: Footprinting Módulo
- Módulo 3: Fingerprinting Módulo
- Módulo 4: Seguridad en redes

Curso 2: SEGURIDAD EN REDES

- Módulo 1: Seguridad en redes: TCP/IP
- Módulo 2: Seguridad en redes: Protocolos de Aplicación.
- Módulo 3: Seguridad en redes: Otros Protocolos
- Módulo 4: Vulnerabilidades y Metasploit

Curso 3: SEGURIDAD EN APLICACIONES WEB

- Módulo 1: Ataques a credenciales
- Módulo 2: Seguridad física de los equipos
- Módulo 3: Seguridad en aplicaciones web
- Módulo 4: Seguridad en aplicaciones web

Curso 4: EL ARTE DE DESCUBRIR Y ANALIZAR MALWARE

- Módulo 1: Malware
- Módulo 2: SandBoxes
- Módulo 3: Zeus
- Módulo 4: Malware Desconocido

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, por su vasta experiencia en el campo de la ciberseguridad, en el que diariamente realizan auditorías de seguridad y tareas de hacking ético y pentesting, incluyendo nuevos test de intrusión en IPv6, metodología OWASP 2013 y un vástago conjunto de aplicaciones para la realización de prácticas en entornos controlados.

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

Prerrequisitos del programa

Conocimiento básico de los dispositivos de red, conocimientos de IPv4, conocimientos básicos de protocolos (ICMP, ARP, IP, TCP, UDP, etc.), conocimientos de Microsoft© Windows y GNU/Linux.

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.

SÉ INTERNACIONAL

ILUMNO Transforming how the world learns