TEC | Tecnológico de Costa Rica

Programa de Actualización Profesional

Principios de Ciberseguridad y Privacidad

Centro de Especializaciones TI de la Escuela de Computación TEC

Requisitos de Ingreso

- Personas con algún grado mínimo bachiller en Ingeniería en Computación, Ingeniería en Sistemas de Información, Ingeniería en Telemática, Ingeniería en Computadores.
- Es importante que las personas cuenten con experiencia previa en programación de algoritmos y administración de sistemas. Debe tener flexibilidad cognitiva para trabajar en diferentes ambientes de desarrollo de programas.

Público meta

Este es un programa para personas que laboran en el ámbito de computación y cuya intención es ampliar sus conocimientos sobre la ciberseguridad

Perfil de Ingreso

- Programa dirigido a personas egresadas o que se desarrollen en alguna de las siguientes áreas:
  - Ingeniería en Computación
  - Ingeniería en Sistemas
  - Ingeniería en Telemática
  - Ingeniería en Computadores
  - Administración de Tecnología de la Información

Perfil de Salida

- Una persona con conocimientos en principios de ciberseguridad y privacidad, es aquella capaz de crear, utilizar algoritmos y herramientas para proteger información, diseñar modelos, determinar el dominio aplicable de cada uno de ellos; de forma tal que pueda realizar, analizar posibles ataques, encontrar vulnerabilidades, proteger información sensible, garantizar la privacidad de los datos y proteger sistemas.

Sobre el programa	Programa de Capacitación compuesto por 3 módulos de 32 horas cada uno. Cada módulo se impartirá de forma bimestral. En el Desarrollo de cada uno de los módulos, se utilizará de manera transversal, lenguajes y herramientas de alto uso en la industria, los cuales se verán complementados con casos prácticos de escenarios de prueba. Todos los módulos del programa, estarán desarrollados bajo una metodología basada en proyectos.
Cantidad mínima y máxima por atender	20 Estudiantes mínimo y 30 máximo, cuando las instalaciones lo permitan
Inversión por estudiante	- Cada módulo tendrá un valor de $600, para un total de $1800+ iva = $1836 en modalidad presencial - En caso de que se imparta de manera virtual, el precio es de $500 por modulo para un total de $1500+iva = $1530. - Derechos de graduación $100 aproximadamente - Examen de suficiencia $100
Secuencia de Módulos	1. Aseguramiento de la Información 2. Protección de Sistemas 3. Ataque de Sistemas

Aprobación del Programa	Para obtener el certificado de Actualización Profesional en Principios de Ciberseguridad y Privacidad, es necesario cumplir con la aprobación de los 3 módulos.
Bibliografía	Todo el material a utilizar en el Desarrollo de las lecciones, será preparado por profesores de la Escuela de Computación, y le será entregado a los estudiantes de manera digital

TEC | Tecnológico de Costa Rica

Módulos del Programa

Nombre del Curso	**Aseguramiento de la Información**
Descripción	El curso introducirá conceptos matemáticos fundamentales para comprender el funcionamiento de los sistemas de cifrado y firmado actuales, incluyendo llave pública-privada, firma digital costarricense, sellados de tiempo, entre otros. Además se propondrán técnicas para mejorar el aseguramiento, privacidad y transparencia de los datos, como las técnicas de de-identificación y re-identificación de datos.
Tipo de Curso	Aprovechamiento Tipo teórico/práctico Para obtener el certificado correspondiente, es necesario tener una asistencia efectiva de más del 80% a las lecciones, y sus evaluaciones con un promedio mayor o igual a 70.
Cantidad de Horas Lectivas	32 Horas lectivas presenciales, 4 hrs semanales presenciales y un mínimo requerido de 6 hrs extra clase

Objetivos

Objetivo General:

Al finalizar el curso el estudiante será capaz de:

Valorar las mejores prácticas para garantizar la confidencialidad, integridad y disponibilidad de la información a través del cifrado, firmado, transparencia y privacidad de los datos.

Objetivos Específicos:

Al finalizar el curso el estudiante será capaz de:

- Identificar la importancia de la Seguridad de la Información.
- Comprender los mecanismos de cifrado actuales utilizando las bases matemáticas y conceptos básicos necesarios.
- Diseñar sistemas que protejan los datos de los usuarios mediante la infraestructura de cifrado actualmente conocida.
- Especificar procesos que garanticen la transparencia y privacidad de los datos a través de la implementación de estándares, normativas y legislación nacional e internacional.

Metodología de la enseñanza

Se abordarán clases magistrales por parte del profesor, como introducción a las actividades y conceptos que se desarrollan en cada sesión.
El curso utilizará una metodología de Aprender Haciendo, basado en el desarrollo de proyectos de forma tal que mediante el desarrollo de casos de estudio y proyectos en el laboratorio, se pueda afianzar los conocimientos adquiridos durante el transcurso de las diferentes lecciones.

Contenidos del programa

- ¿Qué es Seguridad de la Información?
  - (CIA Triad) Confidencialidad, Integridad, Disponibilidad
- ¿Qué es cifrado?
  - La matemática detrás de los Mecanismos de cifrado
  - Cifrado simétrico
  - Cifrado asimétrico: Llave pública privada
  - Sellados de Tiempo
  - PKI, DPKI
  - Firma Digital Costarricense
  - Protocolos de comunicación segura: SSL/TLS
  - Protocolos para la preservación de la privacidad
- ¿Cómo realizar un análisis forense?
  - Herramientas para el análisis forense
  - Adquisición de la evidencia: logs, memoria, discos.
  - Análisis de evidencia
  - Proceso de Investigación
  - Presentación de resultados
- ¿Cómo mantener seguros mis datos?
  - Transparencia y Privacidad
  - Disponibilidad de la información
  - Legislación Internacional: GDPR
  - Legislación Costarricense
  - Técnicas para el mejoramiento de la privacidad de los Datos
    - Técnicas de Re-identificación de Datos
    - Técnicas de Des-identificación de datos
  - Estándares Internacionales:
    - ISO 29100 - Privacy framework
    - ISO 20889 - Privacy enhancing data de-identification terminology and classification of techniques

TEC | Tecnológico de Costa Rica

Nombre del Curso	**Protección de Sistemas**
Descripción	El curso tiene como objetivo desarrollar las habilidades necesarias para la adecuada defensa de un sistema computacional, utilizando las mejores prácticas donde se garantice la Confidencialidad, Integridad y Disponibilidad del mismo. Además el curso pretende aportar las bases para diseñar políticas de seguridad, en favor de la defensa de un ambiente empresarial, tomando en cuenta un correcto análisis de riesgos, la legislación actual, estándares nacionales e internacionales.
Tipo de Curso	Aprovechamiento Tipo teórico/práctico Para obtener el certificado correspondiente, es necesario tener una asistencia efectiva de más del 80% de las lecciones, y sus evaluaciones con un promedio mayor o igual a 70.
Cantidad de Horas Lectivas	32 Horas lectivas presenciales, 4 hrs semanales presenciales y un mínimo requerido de 6 hrs extra clase
Requisitos	Haber cursado Aseguramiento de la Información, o contar con los conocimientos de ese curso.

Objetivos

Objetivo General:

Al finalizar el curso el estudiante será capaz de:

Determinar las mejores prácticas para defender un sistema computacional a través de mecanismos que potencien la protección de la Confidencialidad, Integridad y Disponibilidad de los datos.

Objetivos Específicos:

Al finalizar el curso el estudiante será capaz de:

- Valorar la integridad de la información a través del aseguramiento de la calidad y los procesos.
- Medir la disponibilidad de un sistema mediante el monitoreo.
- Diseñar mecanismos de recuperación de desastres a través de la creación de planes de contingencia y del análisis forense.
- Defender la confidencialidad de la información mediante la implementación de mecanismos de administración de la identidad
- Evaluar las mejores prácticas de programación para crear software seguro.
- Establecer políticas que garanticen la seguridad informática de una empresa a través del análisis de riesgos, estándares y normas internacionales.

Metodología de la enseñanza	Se abordarán clases magistrales por parte del profesor, como introducción a las actividades y conceptos que se desarrollan en cada sesión. El curso utilizará una metodología de Aprender Haciendo, de forma tal que mediante el desarrollo de casos de estudio y proyectos en el laboratorio, se pueda afianzar los conocimientos adquiridos durante el transcurso de las diferentes lecciones.

Contenidos del programa

- ¿Cómo garantizar la Integridad?
  - Aseguramiento de la Calidad
  - Monitoreo de Procesos
- ¿Cómo garantizar la Disponibilidad?
  - Monitoreo de Rendimiento
  - Respuesta a Incidentes de Seguridad
  - Recuperación de Desastres
  - Defensa de Red:
    - Firewalls de red y de aplicación
    - Implementación de IDS/IPS
    - Network Hardening
    - Análisis de Tráfico
- ¿Cómo garantizar la confidencialidad?
  - Control de Acceso
  - Administración de Identidad
  - Métodos de Autenticación
- ¿Cómo programar código seguro?
  - Seguridad de Software
  - Ciclo de vida de desarrollo de software Seguro
  - Usabilidad en la ciberseguridad y privacidad
  - Aspectos Sociales del desarrollo de software
  - Código malicioso y malware moderno
  - Análisis estático / Malware Analysis Lab
  - Seguridad Web
- ¿Cómo asegurar una empresa?
  - Análisis de riesgo
  - Políticas
    - Modelos de Políticas
    - Composición de Políticas
    - Monitoreo y Automatización de políticas
  - Estándares
    - Familia ISO 27000 y otros estándares como SOC 2 y PCI

TEC | Tecnológico de Costa Rica

Nombre del Curso	**Ataque de Sistemas**
Descripción	El curso introducirá a los estudiantes conceptos de ataque a sistemas computacionales, reconocimiento de puntos débiles y experimentación usando herramientas de seguridad. Los conceptos estudiados en el curso permitirán diseñar ataques dirigidos a infraestructura de prueba y comparar tipos de vulnerabilidades a través de modelos de amenazas y pruebas de penetración.
Tipo de Curso	Aprovechamiento Tipo teórico/práctico Para obtener el certificado correspondiente, es necesario tener una asistencia efectiva de más del 80% a las lecciones, y sus evaluaciones con un promedio mayor o igual a 70.
Cantidad de Horas Lectivas	32 Horas lectivas presenciales, 4 hrs semanales presenciales y un mínimo requerido de 6 hrs extra clase
Requisitos	Haber cursado Protección de Sistemas o contar con los conocimientos de ese curso.
Objetivos	**Objetivo General:** Al finalizar el curso el estudiante será capaz de: Evaluar los mejores mecanismos para atacar un sistema computacional a través

de técnicas de hacking y explotación de vulnerabilidades de sistemas.

Objetivos específicos:

Al finalizar el curso el estudiante será capaz de:

- Reconocer arquitecturas de sistemas modernos mediante la implementación de infraestructura computacional de prueba.
- Analizar los puntos débiles de un sistema a través del reconocimiento y enumeración de vulnerabilidades.
- Analizar el flujo de información en un sistema mediante la interceptación de datos.
- Diseñar ataques dirigidos a una infraestructura computacional de prueba mediante el uso de ingeniería social, exploits y vulnerabilidades de diseño.
- Comparar tipos de vulnerabilidades a través de modelos de amenazas, pruebas de penetración y análisis de requerimientos.

Metodología de la enseñanza

Se abordarán clases magistrales como introducción a las actividades que se desarrollan en cada sesión.
El curso utilizará una metodología de Aprender Haciendo, de forma tal que se pueda desarrollar el o los proyectos para ejemplificar el aprendizaje

Contenidos del programa

- El rol de los sistemas operativos en la seguridad.
- Cyber-ética
- Arquitecturas comunes de sistemas
  - Virtualización
  - Hipervisores e implementación de cloud computing
  - Industrial Control Systems
  - IoT
  - Mobile Systems
- Sistemas Distribuidos
- Reconocimiento y Escaneo
  - Footprinting
  - Puertos
  - Aplicaciones
  - Vulnerabilidades
- Protocolos de comunicación segura
  - Interceptación de datos de red
  - Ataques a TLS
- Técnicas de hacking y explotación, herramientas y puntos de entrada.
  - Vulnerabilidades y exploits de ejemplo
  - Ataques a sistemas de Control
  - Denegación de Servicio
  - Desbordamiento de Buffer
  - Ingeniería Social
  - Web Security
  - Malware
  - El uso de la automatización: Bots y Botnets
- Mantenimiento de acceso
  - Puertas traseras
- Anonimato y cubrimiento de rastros
  - Proxies
  - Redes de Anonimato
  - Protocolos de Seguridad: IPSec, TLS, SSH, OpenVPN.
- Análisis de Vulnerabilidades.
  - Modelos de Vulnerabilidades
  - Pruebas de penetración