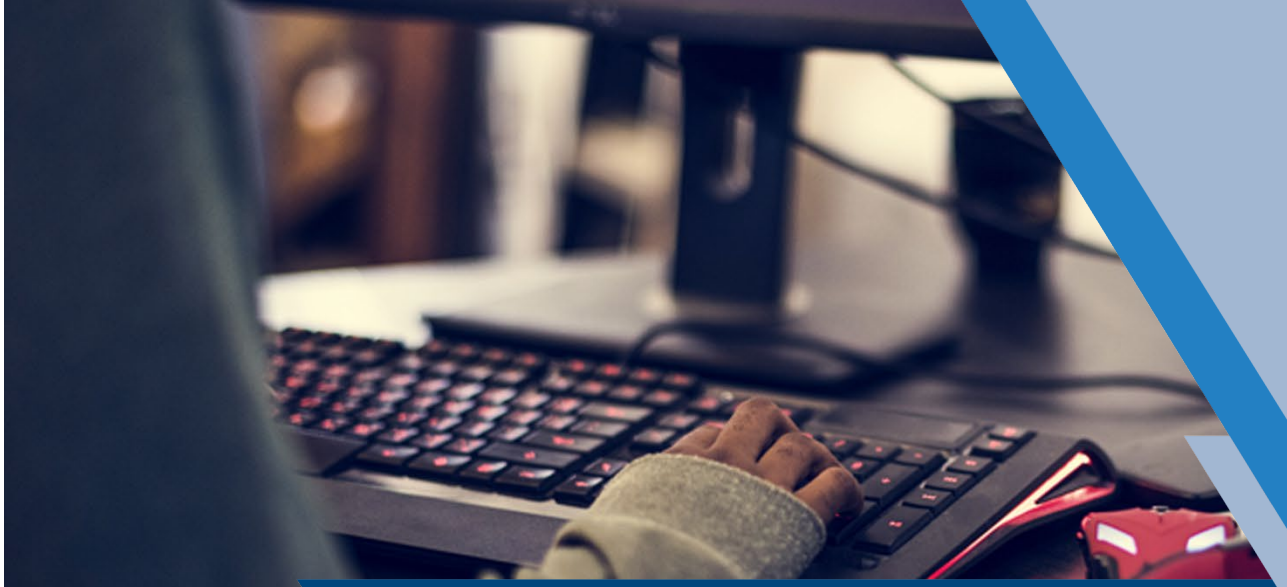

CURSOS Y Diplomados ITESO

DIPLOMADO

CIBERSEGURIDAD

Protege tu empresa desde adentro, domina la ciberseguridad y asegura tu información crítica.

Descripción

Adquiere conocimientos y habilidades necesarias para gestionar la seguridad de la información en tu empresa. Aprenderás a diseñar esquemas de seguridad, identificar vulnerabilidades, implementar técnicas de hacking ético y aplicar estándares internacionales como ISO27000. Todo esto con acceso a laboratorios de última generación y herramientas prácticas.

Inicio

21 de junio 2025

Duración

120 horas en 24 semanas

Modalidad

Presencial

Horario

Sábado
9:00 a 14:00 horas

Inversión

Contado:
$41,000 MXN o

6 pagos de:
$7,000 MXN c/u

Si desea pagar en otra moneda, se utilizará el tipo de cambio del día en que se realice el pago

CURSOS Y Diplomados ITESO

Objetivo

Aprender a diseñar esquemas de ciberseguridad en espacios laborales a través de la gestión y diseño de esquemas de seguridad y protección de datos e información, así como identificación de riesgos y aplicación de herramientas de hackeo ético en pro de la seguridad empresarial.

Dirigido a:

Profesionales dedicadas y dedicados con áreas relacionadas con las redes de computadoras, administración de la infraestructura tecnológica y/o seguridad de la información, que desee aumentar, perfeccionar y especializar sus conocimientos en el campo de la seguridad informática.

Beneficios del programa:

- Dominarás el diseño de esquemas de seguridad perimetral y técnicas de protección de datos.
- Aprenderás a evaluar vulnerabilidades con técnicas de hacking ético y herramientas de código abierto.
- Conocerás los estándares internacionales en gestión de ciberseguridad como ISO27000 y NIST.
- Desarrollarás habilidades prácticas en un laboratorio de redes de última generación.

TEMARIO

CURSOS Y Diplomados ITESO

01 Introducción a la seguridad y redes de computadoras

Conocer los principios de la ciberseguridad, tales como el análisis de riesgos, la política de seguridad, así como las referencias documentales y de estandarización más utilizadas. También aborda los conceptos básicos necesarios para entender la manera en que se crean las redes de telecomunicaciones, así como los dispositivos que son utilizados para llevar a cabo las tareas en un ambiente redes de datos, tales como enrutadores, switches y firewalls.

- Definición de ciberseguridad
- Análisis de riesgos - Activos, Vulnerabilidades, Amenazas y Contramedidas
- Política de seguridad
- Estándares relevantes - ISO27000
- Principios básicos – Confidencialidad, Integridad, Disponibilidad, No repudio y Autentificación
- Elementos para la construcción de redes
    - IPv4
    - IPv6
    - Enrutadores
    - Switches

02 Criptografía

Conocer de manera práctica los principales métodos criptográficos utilizados a lo largo de historia y los métodos más actuales para proteger la información. De igual manera, se explicará la forma de operar de los sistemas criptográficos de llave publica utilizados por protocolos como https o en firmas digitales.

- Métodos clásicos de criptografía
- Sustitución Monoalfabéticos
- Julio Cesar
- Veniegere
- Sustitución Polialfabéticos
- Hill Cipher
- Métodos modernos de criptografía
- Redes de Feistel
- DES y AES
- Sistemas de Llave Publica
- Diffie y Hellman
- PGP
- OpenSSL
- Algoritmos de Integridad

- RC4
- Aplicaciones de Criptografía
- Confidencialidad
- Autenticación
- Integridad
- No repudio

03

Herramientas de Seguridad

Conocer de manera práctica las principales herramientas y técnicas para generar seguridad en la frontera de nuestra red, generar conexiones seguras entres redes, y técnicas para monitorear nuestras en redes para prevenir ataques. Conocer de manera práctica las principales herramientas y técnicas para generar seguridad en la frontera de nuestra red, generar conexiones seguras entres redes, y técnicas para monitorear nuestras en redes para prevenir ataques.

- Firewalls
  - Basados en ACL de CISCO
  - Basados en IP TABLES de Linux
- IDS/IPS
- VPNs
- SSL
- Seguridad física

04

Gestión de la Seguridad

Dar a conocer una visión global de los elementos a considerar para la planificación de la seguridad y la metodología aplicable para la implantación de un sistema de gestión de la ciberseguridad.

- Seguridad de la información
- Modelos de seguridad
- Incidentes e impactos
- Principios y normativas de seguridad
- Medidas de protección
- Tipos de controles
- Normativas técnicas y legales
- Ciclo de vida de la seguridad
- Metodologías de análisis de riesgos – NIST, OCTAVE y MAGERIT
- Sistemas de gestión de la seguridad de la información
- Política de seguridad - Ámbitos de seguridad (personal, física, comunicaciones, acceso, desarrollo, incidentes, continuidad)
- Planes de continuidad de negocio

05

Hacking ético (*ethical hacking*)

Conocer las principales técnicas y herramientas para evaluar la seguridad de los sistemas de información y dispositivos conectados a una red. Una de las mejores formas de conocer el nivel de seguridad de un sistema de información es evaluando si es posible detectar y atacar alguna vulnerabilidad de seguridad en él o no.

- Hackeo Ético
- Ataques conocidos
- Redes de Área Local
- Wireless
- Malware (Troyanos, Virus, Worms)
- SQL Injection
- Cross-Site Scripting
- Ingeniería Social

06

Informática Forense

Conocer la metodología de la informática forense, cómo aplicarla y las situaciones en las que resulta de utilidad. Además, conoce r la manera en que las técnicas forenses se relacionan con los sistemas informáticos a través de la gestión de incidentes en una organización, de manera que se puedan minimizar los ataques exitosos a la misma o para dar elementos para perseguir a los responsables en caso de que se logre aprovechar alguna vulnerabilidad no protegida.

- Definición de informática forense y sus principales elementos
- Gestión de incidentes de seguridad
- Prevención
- Detección y análisis
- Contención
- Resolución
- Fases y metodología
- Aseguramiento
- Identificación
- Adquisición
- Análisis
- Informe
- Peritaje
- Gestionar el desempeño

Requisitos

Trabajar en áreas de redes, infraestructura o seguridad informática.

Metodología

- En este programa las personas participantes tendrán acceso a la herramienta Hack The Box de capacitación en pruebas de seguridad basada en escenarios reales.
- Desarrollo de prácticas en un laboratorio de redes de última generación equipado con Routers, Switches, Firewalls, equipo para redes Wireless de las principales marcas.
- Durante el diplomado, darán cuenta de su aprendizaje a través de la aplicación de los conocimientos adquiridos en las sesiones teóricas en los escenarios simulados.

Acreditación

Esta experiencia educativa requiere de autogestión y autonomía, para la ejecución y seguimiento del programa.

Para acreditar el diplomado es necesario:

- Participar activamente, ya que el principal actor y sujeto de acción en torno a su propio aprendizaje es la persona participante.
- Cumplir con el 80% de los entregables (actividades, tareas o productos)
- Contar con un 80% de asistencia a las sesiones presenciales
- Al completar y acreditar el programa, se entregará un Diploma

CONOCE A LOS EXPERTOS

CURSOS Y Diplomados ITESO

Coordinación

Oscar Fernández Larios

Maestro en Informática Aplicada, ingeniero en Sistemas Computacionales, ambos en el Instituto de Estudios Superiores de Occidente (ITESO), máster en Seguridad Informática por la Universidad Oberta de Cataluña. Cuenta con varias certificaciones y especializaciones en el área de redes de datos y equipo de telecomunicaciones. Ha formado parte de la planta de profesores del ITESO desde 1995, dedicándose de lleno a la docencia a partir del año 2004, impartiendo diversas materias sobre redes de computadoras. Durante este tiempo también se ha desempeñado como coordinador de la carrera de Ingeniería en Redes y Telecomunicaciones y consultor senior del Centro de Consultoría del programa para la Gestión de la Innovación y la Tecnología (PROGINNT) del ITESO, fue director del Centro para la Gestión de la Innovación y la Tecnología (CEGINT) del ITESO.

Profesores

Álvaro I. Parres Peredo

Doctor en Ciencias de la Ingeniería por el Instituto Tecnológico y de Estudios Superiores de Occidente (ITESO) con una tesis titulada "Sistema de Detección de Intrusos basado en Anomalías a nivel de Host utilizando Rankings para la Seguridad Informática", cuenta con una maestría en Administración de Tecnologías de la Información por el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM) y es Ingeniero en Sistemas Computacionales por el ITESO. Adicionalmente cuenta con una especialidad en Mejora de Procesos de Negocio. Tiene diversas certificaciones en el campo de las redes de computadoras, la seguridad informática y la informática forense. Cuenta con diversas publicaciones en congresos internacionales y revistas arbitradas en los campos de la seguridad informática, el cómputo en la nube y las ciencias computacionales. Actualmente en el ITESO se desempeña como director del Departamento de Electrónica, Sistemas e Informática.

Alan Alfonso Lomelí Ruiz
PROMOTOR

+52 (33)3669 3482 / +52 (33)3669 3484
diplomados@iteso.mx / alan.lomelir@iteso.mx
+52 (33) 26 07 31 28

El ITESO se reserva el derecho de apertura del programa en caso de no cubrir el mínimo requerido de participantes. El contenido de esta ficha se encuentra sujeta a cambios sin previo aviso.