CURSO SEGURIDAD INFORMÁTICA

Certificado expedido por el Instituto Superior de Profesorado Técnico de la Universidad tecnológica Nacional.

Contenidos

Conceptos básicos de seguridad informática

En este primer módulo hacemos una introducción al mundo de la seguridad informática para conocer los conceptos básicos y la información fundamental para adoptar las diferentes temáticas a lo largo del curso.

Temáticas:

- Conceptos básicos de la seguridad informática
- Reseña e historia
- Técnicas de propagación de amenazas
- Sistemas operativos

Vulnerabilidades

En este módulo se presentan los conceptos asociados con uno de los principales vectores de propagación de amenazas utilizados hoy en día, la forma en que son utilizadas y principales controles que pueden ser implementados para prevenir ser víctimas de su explotación.

Temáticas:

- Introducción
- Conceptos básicos
- Clasificación
- Ataques basados en vulnerabilidades
- ¿Cómo protegerse?

Armado de laboratorio

Este módulo presenta las principales herramientas para montar un laboratorio que permita al estudiante tener todo un entorno preparado para el análisis de amenazas. Todas las herramientas y sistemas presentados son de un código abierto.

Temáticas:

- Estrategias
- Elementos vs. Capacidad humanas
- Herramientas Esenciales
- Virtualizando
- Distribuciones de análisis forense
- Prácticas

Análisis de malware

Los códigos maliciosos son una amenaza que más afectan a los usuarios, por lo tanto en este módulo presentamos las principales metodologías que le permitirían al estudiante analizar el comportamiento de una y poder adoptar las medidas de control necesarias.

Temáticas:

- Objetivos del análisis de malware
- Tipos de análisis de malware: estático y dinámico
- Herramientas para el análisis de malware
- Códigos maliciosos y sitios web
- Prácticas

Análisis de tráfico de red

Con este módulo se busca introducir a los estudiantes sobre la importancia de auditar el tráfico de red con diferentes tipos de herramientas. A través de ejemplos prácticos de ataques en redes de área local bastante conocidos y que actualmente siguen siendo uno de los mayores enemigos en los entornos corporativos.

Temáticas:

- Captura y análisis del tráfico de red
- Simulación de redes
- Análisis de direcciones IP y dominios DNS
- Wireshak, Tshark
- Técnicas de Anonimización

Conceptos básicos de investigación forense

Contar con conocimientos para el análisis forense permite ampliar el alcance y la profundidad de la comprensión de las amenazas que atentan contra una organización. En este módulo presentamos los conceptos básicos que ayudarán al estudiante para definir el impacto que un incidente tuvo en el negocio de la compañía.

Temáticas:

- Comenzando la investigación
- La importancia y preservación de la evidencia. Cadena de custodia
- Adquisición y duplicación de evidencias
- Arquitectura, sistemas de archivos, arranque en Windows y Linux

- Logs. Eventos y análisis de línea de tiempo
- Equipos de respuestas ante incidentes
- Técnicas anti-forenses
- Prácticas

Conceptos básicos de Ethical Hacking

Con este módulo el estudiante puede conocer cuál es la filosofía y el funcionamiento del Ethical Hacking, obteniendo las competencias sobre las herramientas y metodologías utilizadas para llevar a cabo tareas de análisis de vulnerabilidades, test de penetración y evaluaciones de redes y servidores de datos.

Temáticas:

- Introducción
- Enumeración
- Escaneo
- Ganas acceso
- Terminologías
- Prácticas

Respuesta a incidentes

El contenido de este módulo está orientado para que los estudiantes puedan conocer e incorporar conceptos importantes a la hora de enfrentarse a un incidente y, de esta manera, elaborar eficientemente la correspondiente recuperación, acortando el tiempo de respuesta frente a un eventual incidente.

Temáticas:

- Gestión y respuesta a incidentes
- Continuidad del negocio
- Herramientas de protección corporativas y hogareñas

Requisitos

- Estudios secundarios completos y ser mayor de 18 años.
- Conocimientos básicos en el uso de PC.
- Manejo de internet.
- Conocimientos deseables: redes, programación y Linux.

Modalidad

Clases teórico prácticas.

Duración

12 encuentros de 2hs c/u.

Días y horarios de cursada

Lunes de 10 a 12hs iniciando el 9 de abril y finalizando el 2 de julio.

Asistencia

Se exige un 75% de asistencias para la entrega del certificado.

Lugar de cursada

Las clases se dictan en el Centro Universitario Vicente López ubicado en Carlos Villate 4480, Munro, Vicente López.

Inscripción

Para inscribirse todos los interesados deberán acercarse al Centro Universitario Vicente López, desde el 19 de febrero hasta el 23 de marzo de 9 a 22 hs presentando la siguiente documentación:

- DNI original y fotocopia
- Fotocopia del Título Secundario
- Foto 4 x 4.

Por dudas o consultas escribir a cursos.cuv@mvl.edu.ar