ITBA Escuela de INNOVACIÓN
EVOLUCIÓN CONTINUA

Negocios Digitales

Certificación Avanzada en Ciberseguridad

La ciberseguridad y la seguridad de la información son aspectos fundamentales en las tecnologías que implementan las empresas. El crecimiento exponencial de infraestructuras, aplicaciones y procesos, genera que los conocimientos básicos de ciberseguridad y las herramientas a utilizar sean responsabilidad de todos los equipos de trabajo.

En la industria actual ya no se delega la ciberseguridad a un solo grupo de especialistas, sino que todos los equipos técnicos de trabajo deben tener los conocimientos y las herramientas para mantener sus sistemas seguros.

Al ser temas transversales a todas las áreas, es importante que tanto las industrias como las personas, incrementen sus capacidades en estos temas, los cuales requieren constante capacitación y actualización.

OBJETIVOS DEL PROGRAMA

1. Obtener los conocimientos teóricos y prácticos necesarios para poder replicarlos en sus ambientes laborales con sus equipos de trabajo.
2. Conocer demostraciones prácticas de casos reales sobre sistemas usados en la industria con herramientas de acceso libre y gratuito.
3. Evaluar y comparar casos de laboratorio contra casos reales donde los sistemas contemplen algunas protecciones de seguridad.
4. Conocer diferentes casos de cómo gestionar la seguridad de la información en empresas.

OBJETIVOS DE FORMACIÓN

Que los estudiantes:

1. Obtengan las competencias necesarias para poder gestionar la seguridad de la información en empresas.
2. Logren comprender mediante prácticas de los procedimientos técnicos necesarios para implementar acciones de Ciberseguridad.
3. Conozcan y entiendan los diferentes perfiles, roles, procesos y procedimientos que involucran un área de Ciberseguridad empresarial.

PERFIL DEL PARTICIPANTE

Administradores de Sistemas, Administradores de Redes, Desarrolladores, Auditores y todas aquellas personas con conocimientos tecnológicos previos que deseen iniciarse en el mundo de la ciberseguridad con orientación práctica.

METODOLOGÍA

Durante la certificación se realizarán encuentros sincrónicos de desarrollo de contenido, presentación de materiales, demostraciones prácticas y trabajos grupales.

De forma asincrónica se compartirán materiales que los y las estudiantes deberán revisar y actividades de laboratorio que podrán realizar para reforzar lo trabajado en los encuentros sincrónicos.

CONOCIMIENTOS MÍNIMOS

Conocimientos básicos de Linux y Windows, uso línea de comandos. Conocimientos básicos de TCP/IP. Se recomienda nivel básico de inglés para lectura de materiales.

PROGRAMA

MÓDULO 1: INTRODUCCIÓN A LA CIBERSEGURIDAD

- Ciberseguridad, Seguridad de la Información y Seguridad Informática.
- Las empresas y la Ciberseguridad. Actores, roles y perfiles.
- Gestión de la Seguridad de la Información
- Seguridad Defensiva
- Seguridad Ofensiva

MÓDULO 2: VULNERABILIDADES Y PENTEST

- Análisis de riesgos enfocado a vulnerabilidades.
- Introducción al análisis de vulnerabilidades
- Introducción al Pentest.
- Metodologías y Frameworks.
- Reportes Ejecutivos y Técnicos

MÓDULO 3: CRIPTOGRAFÍA

- Introducción a la criptografía y su historia.
- Cifrado Simétrico y Asimétrico.
- Protocolos de intercambio de claves. Diffie-Hellman
- Funciones de hash y digesto.
- Infraestructura de clave pública (PKI)
- SSL y TLS
- Autenticación. Claves, tokens, MFA.

MÓDULO 4: INTRODUCCIÓN A LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- Introducción a la seguridad de la información
- Gestión de Activos
- Políticas, procesos, y estrategia de seguridad
- Frameworks y modelos de madurez
- Política de seguridad de la información
- Gestión de riesgos
- Continuidad del Negocio
- GRC: Gobierno, Riesgo, y cumplimiento
- Métricas, estructura y gobierno

MÓDULO 5: SEGURIDAD CON IA

- IA en el ciclo de vida de desarrollo (SDLC).
- IA en el análisis dinámico en servicios Web.
- Hackeando la IA. LLM y sus vulnerabilidades.

MÓDULO 6: SEGURIDAD DEFENSIVA

- Perfiles laborales en SOC, CSIRT, DFIR y CTI.
- Arquitectura de seguridad defensiva.
- Seguridad en aplicaciones y dispositivos.
- Monitoreo y alertas.
- Respuesta a incidentes.
- Análisis Forense.

MÓDULO 7: LEYES Y CIBERDELITOS

- Tipos de delitos informáticos en Argentina.
- Procesos y acciones legales
- Información solicitada por organismos judiciales.
- Análisis de causas judiciales.

REQUISITOS DE APROBACIÓN

Asistencia igual o superior al 75%. Entregas de trabajos y evaluaciones parciales para aprobar.

CUERPO DOCENTE

SANTIAGO VALLÉS
Consultor de Seguridad Informática en el ámbito público y privado. Posee una Maestría en Ciberseguridad y se ha desempeñado como docente de grado y posgrado en UTN, ITBA y Universidad de San Andrés. Participa como redactor y divulgador en notas y artículos de tecnología en diarios y revistas nacionales. Fue Director del Departamento de Informática del ITBA.

ALEXANDER CAMPOS
Consultor en Ciberseguridad con amplia experiencia en el sector privado nacional e internacional. Ingeniero en Ciberseguridad y desarrollador. Líder Técnico. Ha alcanzado primeros puestos en competencias de programación internacionales. Posee una Maestría en Ciberseguridad UBA y se ha desempeñado como docente en ITBA.

LAUTARO PINILLA
Consultor en Ciberseguridad con experiencia en sector privado. Auditor de contratos inteligentes y sistemas web3. Se ha desempeñado en planificación e implementación de mitigación de vulnerabilidades, concientización de la seguridad y soporte para incidentes. Se ha desempeñado como docente en ITBA.

MARCELA PALLERO
Especialista en Ciberseguridad con experiencia en gestión de incidentes de seguridad informática y gestión de Seguridad de la Información nivel nacional.

Actualmente se desempeña como docente y es la Responsable del Programa Seguridad en TIC en la Fundación Sadosky

↗ Acreditación: **Certificación Avanzada en Ciberseguridad**

↗ Modalidad: **Virtual**

↗ Duración: **80 hs (46 hs sincrónicas - 34 hs asincrónicas)**

↗ Cursada: **jueves de 18:30 a 20:30 hs**