



DIPLOMADO

Ciberseguridad

Cantidad de horas: 36
Duración: 3 meses.
Modalidad: virtual y presencial.



**Universidad
Nacional
Tecnológica**

Descripción

La revolución 4.0 ha transformado la forma en que vivimos y trabajamos, pero también ha dado lugar a una serie de desafíos y amenazas en el ámbito de la ciberseguridad. El Diplomado en Ciberseguridad está diseñado para dotar a profesionales y entusiastas de la tecnología con los conocimientos y habilidades necesarios para comprender, prevenir y gestionar las amenazas cibernéticas en un entorno empresarial y tecnológico en constante evolución.

Este programa proporciona una base sólida y abordará tanto los aspectos técnicos como los aspectos de gestión en el campo de la ciberseguridad, preparando a los participantes para enfrentar los desafíos actuales y futuros en este campo dinámico.

A lo largo de este programa, los estudiantes desarrollarán competencias técnicas para abordar los desafíos actuales y futuros en la seguridad cibernética, tanto a nivel técnico como estratégico

Objetivo General:

Proporcionar a los participantes una base sólida para la comprensión integral de los principios, estrategias y tecnologías clave en ciberseguridad, considerando los requerimientos de calidad, higiene, así como los estándares establecidos.

Módulo 1: Fundamentos de Ciberseguridad

Al finalizar este módulo, los participantes serán capaces de:

- Comprender los principios y conceptos fundamentales de ciberseguridad.
- Reconocer la terminología y lenguaje común utilizado en el campo.
- Desarrollar conciencia sobre las amenazas cibernéticas y los riesgos asociados.

Contenido:

- Introducción a la Ciberseguridad
- Principios de Networking y Comunicaciones
- Fundamentos de Sistemas Operativos Seguros
- Criptografía Básica
- Gestión del riesgo
- Concientización sobre Amenazas Cibernéticas

Módulo 2: Protección y defensa

Al finalizar este módulo, los participantes serán capaces de:

- Describir las estrategias y técnicas para proteger activos digitales.
- Identificar incidentes de seguridad en una empresa y dar respuestas.
- Explorar conceptos de seguridad en el desarrollo de software.

Contenido:

- Firewalls y sistemas de detección/prevención de Intrusiones
- Seguridad en desarrollo de software
- Identificación y respuesta a Incidentes
- Seguridad en Aplicaciones Web
- Seguridad en dispositivos móviles

Módulo 3: Gestión de riesgos y cumplimiento

Al finalizar este módulo, los participantes serán capaces de:

- Proponer soluciones en la gestión de riesgos y el cumplimiento normativo en ciberseguridad.
- Evaluar y mitigar riesgos en entornos empresariales.
- Reconocer las leyes y regulaciones relacionadas con la ciberseguridad.

Contenido:

- Evaluación y gestión de riesgos en ciberseguridad
- Marco legal y regulatorio
- Continuidad del negocio y recuperación de desastres
- Auditoría y conformidad
- Ética y responsabilidad profesional

Módulo 4: Tecnologías emergentes en ciberseguridad

Al finalizar este módulo, los participantes serán capaces de:

- Analizar las tendencias y tecnologías más recientes en el campo de la ciberseguridad.
- Desarrollar habilidades en la implementación de soluciones avanzadas.
- Reconocer los desafíos futuros en ciberseguridad y el impacto de la ética

Contenido:

- Inteligencia Artificial y Machine Learning en Ciberseguridad
- Internet de las Cosas (IoT) y Ciberseguridad
- Ciberseguridad en la Nube
- Blockchain y Criptomonedas
- Desafíos Éticos y Futuras Tendencias

Metodología:

- Encuentros sincrónicos en espacios de formación virtual e híbrido
- Clases teóricas practica con expertos en el campo.
- Uso de aula virtual como repositorio de contenido
- Estudios de caso y simulaciones prácticas.
- Proyectos prácticos para aplicar los conocimientos adquiridos.
- Reflexión sobre casos de estudios sobre el impacto de la ciberseguridad en la empresa