DIPLOMADO

SEGURIDAD DE LA INFORMACIÓN Y AUDITORÍA FORENSE

Universidad Nacional Tecnológica

Descripción

En un entorno digital dinámico y constantemente evolutivo, la seguridad de la información y la capacidad para investigar y responder a incidentes cibernéticos son cruciales. El Diplomado en Seguridad de la Información y Auditoría Forense ha sido diseñado para proporcionar a profesionales de TI y expertos en seguridad las habilidades especializadas necesarias para salvaguardar la integridad, confidencialidad y disponibilidad de la información, así como para conducir investigaciones forenses en el caso de incidentes.

Este programa se desarrolla en una modalidad virtual utilizando el Aprendizaje Basado en Proyecto (ABP) para lograr los objetivos propuesto en cada módulo a través de un conjunto de prácticas debidamente seleccionadas. Los participantes tendrán a su disposición de los recursos necesarios para asegurar el aprendizaje tanto en espacios virtuales como híbridos para asegurar la interacción de docentes y estudiantes. Tiene una duración de 16 semanas y está organizado en cuatro modulo con prácticas en cada uno. A lo largo de este programa, los estudiantes desarrollarán competencias técnicas para abordar los desafíos actuales y futuros en la seguridad de la información, tanto a nivel técnico como estratégico.

Objetivo General:

Proporcionar a los participantes de las capacidades y habilidades en las disciplinas interrelacionadas de la seguridad de la información y la auditoría forense a través de un enfoque teórico-práctico para que los participantes adquirirán competencias esenciales para diseñar, implementar y gestionar estrategias efectivas de seguridad, así como para llevar a cabo investigaciones forenses rigurosas en caso de violaciones de seguridad

Módulo 1: Fundamentos de Seguridad de la Información

Al finalizar este módulo, los participantes serán capaces de:
• Comprender los principios y conceptos fundamentales de la seguridad de la información.
• Identificar y evaluar amenazas y vulnerabilidades en sistemas de información.
• Reconocer los estándares y marcos de seguridad.

Contenido:
• Introducción a la seguridad de la información.
• Amenazas y vulnerabilidades.
• Criptografía y protección de datos.
• Normativas y estándares de seguridad.
• Gestión de riesgos y planificación estratégica.

Módulo 2: Seguridad de Redes y Sistemas

Al finalizar este módulo, los participantes serán capaces de:
• Implementar medidas de seguridad en redes y sistemas.
• Conocer técnicas de detección y prevención de intrusiones.
• Describir y explorar la seguridad en entornos de servidores.

Contenido:

• Seguridad en redes.
• Firewalls y sistemas de detección y prevención de intrusiones.
• Seguridad en sistemas operativos.
• Protección de servidores y aplicaciones.
• Gestión de identidades y accesos.

Módulo 3: Auditoría y Monitoreo de Seguridad

Al finalizar este módulo, los participantes serán capaces de:
• Reconocer los principios de auditoría y cumplimiento en la seguridad de la información
• Establecer y realizar procesos de monitoreo para la detección temprana de incidentes.
• Reconocer los aspectos legales y éticos en la auditoria forense.
• Aplicar buenas prácticas de auditoría y cumplimiento.

Contenido:

• Principios de auditoría y cumplimiento.
• Herramientas de auditoría y monitoreo.
• Auditoría de sistemas y redes.
• Gestión de incidentes y respuesta.
• Aspectos legales y éticos en auditoría forense.

Módulo 4: Auditoría Forense y Práctica Avanzada

Al finalizar este módulo, los participantes serán capaces de:
• Implementar técnicas avanzadas de auditoría forense.
• Aplicar metodologías forenses en la investigación de incidentes.
• Elaborar informes forenses claros y precisos.

Contenido:

• Introducción a la auditoría forense.
• Recopilación y preservación de evidencia.
• Análisis forense de dispositivos.
• Investigación de incidentes y malware.
• Elaboración de informes forenses.

Metodología:

• Encuentros sincrónicos en espacios de formación virtual e hibrido
• 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

Recursos:
• Aulas virtuales, espacios de interacción hibrido y plataforma para video conferencia (Ms Teams y Zoom)
• Acceso a laboratorio virtual para demostraciones prácticas.
• Materiales digitales de consulta
• Laboratorio de red con equipos virtuales y herramientas forenses especializadas
• Herramientas de análisis de tráfico.
• Software de seguridad en sistemas operativos y para el análisis forense de dispositivos
• Casos de estudio y escenarios de incidentes simulados.
• Herramientas de auditoría de seguridad.
• Plataforma de simulación de incidentes