



MÓDULO 1 *Fundamentos*

- Introducción a la ciberseguridad
- Legislación y buenas prácticas
- Ciclo de vida de gestión de amenazas
- Gestión de riesgos
- Gestión de identidades
- Introducción a la Inteligencia Artificial
- Intervenciones por parte de profesionales invitados

MÓDULO 2 *Ciberseguridad Defensiva*

- Gestión de incidentes
- Gestión de Centros de Operaciones de Ciberseguridad
- Gestión de redes seguras
- Gestión de microsegmentación
- Ciberseguridad en la nube
- Implementación de Zero Trust
- Inteligencia Artificial para Ciberseguridad Defensiva
- Intervenciones por parte de profesionales invitados

MÓDULO 3 *Ciberseguridad Ofensiva*

- Introducción a las pruebas de penetración
- Herramientas para pruebas de penetración
- Simulación de ataques de penetración
- Ejercicios de pruebas de penetración
- Riesgos en OT e IoT
- Ingeniería Social
- Inteligencia Artificial para Ciberseguridad Ofensiva
- Intervenciones por parte de profesionales invitados

MÓDULO 4 *Gobernanza de la Ciberseguridad*

- Desarrollo de plan rector de Ciberseguridad
- Privacidad de la información y Gobernanza de datos
- Gestión de costos de ciberseguridad
- Desarrollo seguro de Software
- Planes de Inversión en Ciberseguridad
- Inteligencia Artificial y gobernanza de la Ciberseguridad
- Intervenciones por parte de profesionales invitados

CLASES SINCRÓNICAS Y ASINCRÓNICAS

MODALIDAD A DISTANCIA

DURACIÓN: 6 MESES



ORGANIZA

DCIC
DEPARTAMENTO DE CIENCIAS
E INGENIERÍA DE LA COMPUTACIÓN

UNS
UNIVERSIDAD
NACIONAL DEL SUR