INAP

INSTITUTO NACIONAL DE
ADMINISTRACIÓN PÚBLICA, A.C.

DIPLOMADO
CIBERSEGURIDAD ESTRATÉGICA

INAP.MX

SIGUENOS EN
NUESTRAS
REDES

OBJETIVO GENERAL:

Proveer de los conocimientos y herramientas en materia de Ciberseguridad Estratégica para el desarrollo de competencias y nuevas capacidades que, mediante el análisis del entorno, contribuyan a la creación de nuevos modelos de actuación en el ámbito profesional que impacte con sus resultados en la comunidad y trascienda en el ecosistema digital promoviendo la higiene y resiliencia dentro del mundo virtual que día a día manifiesta su influencia en el mundo tangible.

DRIGIDO A:

Servidores públicos de la administración pública mexicana, partidos políticos, organizaciones de la sociedad civil, sector empresarial, estudiantes.

METODOLOGÍA:

En el Diplomado se abordará la ciberseguridad, orígenes, evolución, estrategias, buenas prácticas y el estudio con respecto a su normatividad, regulación y la creciente revolución tecnológica que incluye lo principios de Machine Learning así como el Internet de las Cosas y la Inteligencia Artificial, todo esto con visión de la estrategia e inteligencia para su aplicación. Se promoverá el análisis de casos reales presentados por los cursantes y se realizará como producto final del Diplomado, una propuesta innovadora que se factible de aplicar en el área de desarrollo de las y los participantes.

El Diplomado se desarrolla a partir de sesiones a distancia en tiempo real a través de plataformas tecnológicas como Zoom, ofrecidas por el INAP.

GENERALIDADES:

01 MODALIDAD

Virtual (ZOOM)

02 REQUISITOS DE ADMISIÓN

- Llenar el formato de registro académico.
- Dos fotografías recientes tamaño infantil (blanco y negro).
- Fotocopia de identificación oficial.
- Carta compromiso de pago

03 EVALUACIÓN, ACREDITACIÓN Y RECONOCIMIENTO DEL DIPLOMADO.

- valuación, acreditación y reconocimiento del Diplomado.
- Asistencia virtual a por lo menos el 80% de cada uno de los módulos del Programa a distancia.
- Presentar en tiempo y forma los trabajos, exámenes, proyectos y/o prácticas que solicite el profesorado en cada uno de los módulos.
- Aprobar cada uno de los módulos con una calificación mínima de 7 en una escala de 10 puntos.
- Se otorgará diploma y certificado con valor curricular

PROGRAMA ACADÉMICO

MÓDULO 1 (33 horas)
Sociedad, desarrollo e informática
a. Teorías sociales del desarrollo sustentado en la tecnología.
b. La Tecnología como parte del quehacer humano.
c. Perfiles tecnológicos que impactaron en la historia.
d. Foros globales de desarrollo tecnológico: impacto y resultados.

MÓDULO 2 (21 horas)
Caracterización del Mundo Virtual
a. Orígenes del mundo virtual.
b. Etapas evolutivas en el cibermundo.
c. Precursores de la ciencia cibernética.
d. Aplicaciones, importancia y repercusiones del cibermundo en el ámbito global, aspectos normativos.

MÓDULO 3 (24 horas)
Cibergestión estratégica.
a. Construcciones y términos de mayor uso en el ciberespacio. b. Normas y estándares internacionales. c. Cibergestión estratégica. d. Guías, manuales, protocolos de actuación.

MÓDULO 4 (24 horas)
Softwares maliciosos a. Caracterización de los softwares maliciosos.
b. Tipos de softwares maliciosos.
c. Modus operandi.
d. Análisis de casos reales.

MÓDULO 5 (24 horas)
Hackers.
a. Historia y evolución de los Hackers.
b. Clasificación de los Hackers.
c. Elementos que identifican la actuación de los Hackers.
d. Estudio de casos prácticos de la actuación de los Hackers en el cibermundo.

MÓDULO 6 (36 horas)
Ingeniería Social
a. Antecedentes.
b. Mente, percepción y ciberespacio.
c. Perfiles en la ingeniería social.
d. Estudio y análisis de casos prácticos

MÓDULO 7 (21 horas)
Pentesting 101 lvl 1 a. Definición, conceptos e historia.
b. Tipos de prueba.
c. Metodología de estudio y estándares.
d. Casos prácticos.

MÓDULO 8 (24 horas)
Incidentes y delitos cibernéticos: características y metodología de estudio.
a. Tipos y características.
b. Normatividad vigente nacional e internacional.
c. Higiene y resiliencia cibernética.
d. Métodos de Estudio y análisis de casos emblemáticos.

MÓDULO 9 (21 horas)
Inteligencia Artificial, Machine learning, Internet de las cosas. a. Inteligencia Artificial y Machine Learning.
b. Internet de las cosas, su impacto en el mundo global
c. Paradigmas normativos y buenas prácticas hacía la gestión de la ciberseguridad.
d. Aplicaciones actuales y prospectiva de la inteligencia artificial, machine learning e internet de las cosas.