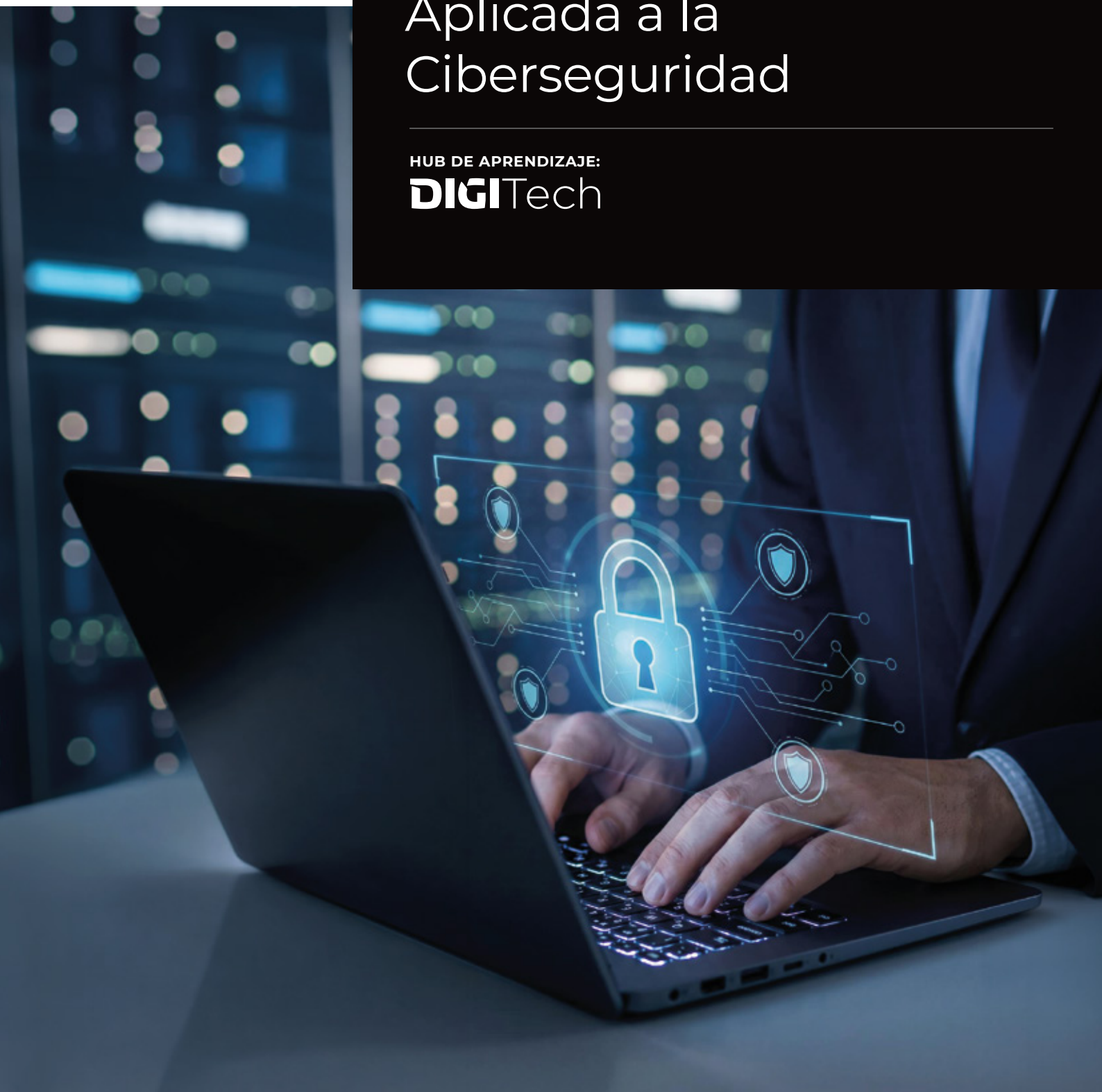
Instituto Europeo de Posgrado

RED SUMMA Education

Maestría en Inteligencia Artificial Aplicada a la Ciberseguridad

HUB DE APRENDIZAJE:
DIGITech



ÍNDICE

CARTA DE BIENVENIDA

Adaptar nuestras agendas a rígidos horarios, o desplazarnos hasta unas instalaciones que con frecuencia se encuentran alejadas de nuestro lugar de trabajo, es cada vez más difícil para muchos profesionales, que sin embargo no quieren dejar de aprender, ni renunciar a una formación de la máxima calidad; ésta es la razón de ser del Instituto Europeo de Posgrado; la Escuela de Negocios en Internet.

Los avances en los medios de comunicación han permitido que la distancia entre ir a clase, o asistir a la misma a través del ordenador, haya desaparecido casi en su totalidad. La posibilidad del uso de vídeos explicativos que puedes ver las veces que sea necesario; el uso de foros y chats para discutir casos prácticos, o la utilización de las redes sociales como forma de crear una comunidad de estudiantes, permite que los alumnos de los programas online puedan acceder a los mejores materiales, sin necesidad de desplazarse a sus lugares de trabajo o residencia.

Pero no todo es tecnología. Lo más importante del Instituto Europeo de Posgrado son las personas. Tutores Académicos que te acompañarán durante todo tu proceso formativo, para que no estés solo en ningún momento. Profesores expertos en sus materias, que resolverán todas tus dudas, y te proporcionarán los mejores materiales para tu aprendizaje. Y compañeros, con los que podrás interactuar y trabajar en grupo, para que tu experiencia sea lo más enriquecedora posible.

Formamos parte de la prestigiosa Red Summa Education, una alianza internacional de instituciones con más de 130.000 estudiantes y una sólida trayectoria de más de 15 años de experiencia en el sector. Nos especializamos en proporcionar educación totalmente en línea, reuniendo a instituciones líderes en educación superior en España, Estados Unidos y Latinoamérica.

Recibe un cordial saludo, y espero poder darte la bienvenida en alguno de nuestros programas en próximas convocatorias.

Carlos Pérez Castro
Director del Instituto Europeo de Posgrado

PRESENTACIÓN DE LA ESCUELA

El Instituto Europeo de Posgrado es una **innovadora Escuela de Negocios 100% online,** que imparte programas de Maestría y formación a empresas.

Nuestro objetivo es darte la facilidad y flexibilidad que necesitas para conciliar tus estudios con tu vida personal y laboral desde cualquier lugar, dando un impulso a tu vida tras estudiar en IEP.

Como miembros de la Red SUMMA Education, una red internacional de instituciones de educación superior virtual con presencia en Colombia, México, España, Argentina y Estados Unidos, nuestros alumnos obtienen una **Titulación Propia del Instituto Europeo de Posgrado** y una **Certificación Internacional con el aval de la Red SUMMA Education.** Ambos diplomas reafirman la calidad y el alcance global de tu formación, brindando un respaldo institucional que añade un valor significativo a tu perfil académico y profesional. Gracias al prestigio de nuestras instituciones, los estudiantes adquieren las competencias necesarias para sobresalir en el entorno empresarial y asumir con éxito responsabilidades directivas.

IEP Instituto Europeo de Posgrado | RED SUMMA Education

RED SUMMA

IEP es miembro fundador de **Red Summa Education, una alianza internacional** de instituciones con una sólida trayectoria de más de 15 años de experiencia en el sector.

Nos especializamos en proporcionar educación totalmente en línea, reuniendo a instituciones líderes en educación superior en España, Estados Unidos y Latinoamérica.

- Presencia en **5 países**
- **+130.000 alumnos**
- Alumnos de **80 nacionalidades** diferentes
- Formación **100% online**
- **+100 programas** de grado y posgrado

JUSTIFICACIÓN

La **Maestría en Inteligencia Artificial Aplicada a la Ciberseguridad** está diseñada para formar profesionales capaces de afrontar los desafíos de seguridad en un entorno digital cada vez más complejo y dinámico.

El programa integra conocimientos avanzados en inteligencia artificial, análisis de datos y ciberseguridad, permitiendo desarrollar soluciones innovadoras para la detección, prevención y respuesta ante amenazas cibernéticas.

Más allá del dominio de herramientas específicas, la maestría proporciona una visión estratégica para identificar riesgos, proteger infraestructuras críticas y fortalecer la seguridad de la información mediante el uso de tecnologías inteligentes. Los participantes adquirirán las competencias necesarias para liderar proyectos de transformación digital segura, optimizar la gestión de riesgos y contribuir a la protección de los activos digitales de las organizaciones en un contexto tecnológico en constante evolución.

MODELO EDUCATIVO INNOVADOR: EDUEX

EDUEX es un modelo educativo que combina programas académicos innovadores con docentes expertos y activos en el ámbito profesional. A través de una plataforma interactiva y pedagogías activas, el modelo está orientado a la resolución de problemas reales, el desarrollo de competencias clave y la aplicación práctica del conocimiento en contextos empresariales actuales.

La **Maestría en Inteligencia Artificial Aplicada a la Ciberseguridad,** es un programa innovador que te sumergirá en el HUB de Aprendizaje DIGITech, un ecosistema dinámico y multidisciplinario diseñado para fomentar la innovación, la colaboración y el desarrollo continuo de competencias.

OBJETIVO GENERAL

Formar profesionales capaces de diseñar, implementar y liderar estrategias de ciberseguridad basadas en inteligencia artificial, mediante la aplicación de técnicas avanzadas de análisis, detección y respuesta ante amenazas, contribuyendo a la protección de los activos digitales, la gestión de riesgos y la transformación digital segura de las organizaciones.

OBJETIVOS ESPECÍFICOS

- **Proporcionar una comprensión integral de los aspectos técnicos, analíticos y estratégicos de la Inteligencia Artificial aplicada a la ciberseguridad,** permitiendo a los estudiantes gestionar proyectos desde la conceptualización hasta la implementación.
- **Desarrollar competencias avanzadas en el uso de la Inteligencia Artificial para la detección, prevención y respuesta ante amenazas cibernéticas,** proporcionando a los alumnos un conocimiento profundo de las técnicas de aprendizaje automático aplicadas a la seguridad informática.
- **Impulsar la innovación mediante soluciones tecnológicas avanzadas y responsables,** asegurando que los estudiantes estén preparados para desarrollar tecnologías disruptivas que respeten principios de privacidad, ética y sostenibilidad en el ámbito de la ciberseguridad.
- **Preparar a los estudiantes para afrontar los desafíos regulatorios del entorno digital, brindándoles herramientas para comprender normativas de ciberseguridad** y protección de datos, así como para anticipar cambios legales relacionados con el uso de la Inteligencia Artificial en la defensa contra ciberataques.
- **Formar líderes capaces de diseñar e implementar estrategias basadas en Inteligencia Artificial que refuercen la seguridad digital** de empresas e instituciones, preparándolos para identificar vulnerabilidades, responder a incidentes y ejecutar proyectos de transformación digital con impacto.

A QUIÉN VA DIRIGIDO

La maestría está dirigida a profesionales y titulados universitarios interesados en **transformar el ámbito de la ciberseguridad mediante el uso de la Inteligencia Artificial y el análisis de datos.**

Se recomienda un perfil con conocimientos básicos en ciberseguridad, programación, redes informáticas o campos afines.

Los perfiles ideales incluyen:

- **Graduados en Ingeniería Informática, Telecomunicaciones, Ciberseguridad,** Matemáticas, Física, Estadística o similares.
- **Profesionales en seguridad informática, administración de sistemas,** auditoría y consultoría tecnológica que deseen actualizar sus competencias con el uso de la Inteligencia Artificial.
- **Emprendedores y líderes de proyectos interesados en desarrollar** soluciones tecnológicas innovadoras para la protección digital.
- **Analistas de datos y especialistas en inteligencia de amenazas** que quieran especializarse en la aplicación de la IA en la detección y prevención de ciberataques.

SALIDAS PROFESIONALES

Denominación:
Maestría en Inteligencia Artificial Aplicada a la Ciberseguridad

Función principal:

Liderar el diseño, implementación y gestión de estrategias de ciberseguridad basadas en inteligencia artificial para prevenir, detectar y responder a amenazas digitales, fortaleciendo la protección de los sistemas, datos e infraestructuras críticas, y contribuyendo a la gestión de riesgos y la seguridad de las organizaciones en entornos tecnológicos cada vez más complejos.

Las salidas profesionales para los egresados de Maestría en Inteligencia Artificial Aplicada a la Ciberseguridad son muy variadas y se encuentran en sectores clave como la banca, la industria tecnológica, el sector público y empresas de ciberseguridad. Algunas de las principales salidas profesionales incluyen:

1. Especialista en Ciberseguridad Basada en IA

- Implementación de modelos de Machine Learning para la detección de intrusiones (IDS/IPS).
- Desarrollo de herramientas de IA para la automatización de respuestas ante incidentes.
- Análisis de patrones anómalos en redes y sistemas.

2. Analista de Amenazas e Inteligencia en Seguridad (Threat Intelligence Analyst)

- Uso de algoritmos de IA para identificar y predecir ciberataques.
- Aplicación de procesamiento de lenguaje natural (NLP) para analizar amenazas en la dark web y redes sociales.
- Desarrollo de modelos de IA generativa para simular y anticipar escenarios de ataque.

3. Ingeniero en Machine Learning para Seguridad

- Creación de modelos de detección de malware utilizando Deep Learning.
- Aplicación de clústering y reducción de dimensionalidad para analizar logs y eventos de seguridad.
- Diseño de soluciones de seguridad basadas en redes neuronales avanzadas.

4. Consultor en Ciberseguridad e IA

- Asesoramiento a empresas para implementar estrategias de IA en ciberseguridad.
- Análisis de riesgos y vulnerabilidades en sistemas empresariales.
- Desarrollo de frameworks de seguridad con inteligencia artificial.

5. Red Team / Blue Team Specialist

- Uso de IA en hacking ético para detectar brechas de seguridad.
- Aplicación de Machine Learning para mejorar estrategias defensivas.
- Automatización de pruebas de penetración y simulaciones de ataque.

6. Especialista en Criptografía Post-Cuántica

- Desarrollo de soluciones criptográficas resistentes a ataques cuánticos.
- Implementación de nuevos estándares de seguridad para datos sensibles.
- Asesoramiento en la transición hacia criptografía segura en la era cuántica.

7. Arquitecto de Seguridad en MLOps y DevSecOps

- Implementación de seguridad en el ciclo de vida del Machine Learning.
- Gestión de identidades y accesos (IAM) en entornos de IA.
- Auditoría y versionado de modelos para garantizar trazabilidad y seguridad.

8. Investigador en IA y Ciberseguridad

- Desarrollo de nuevas técnicas de IA aplicadas a la seguridad digital.
- Participación en proyectos de investigación en universidades, centros tecnológicos o empresas privadas.
- Publicación de papers y contribución al avance del sector.

Este programa abre oportunidades tanto en el sector privado como en organismos gubernamentales y agencias de ciberseguridad. También es una excelente base para aquellos que deseen emprender con soluciones innovadoras en seguridad digital basada en IA.

MODELO DE APRENDIZAJE

EDUex

EDUex es un modelo de educación revolucionario enfocado en el desarrollo integral de los estudiantes. Nuestros innovadores programas están diseñados para inspirarte desde el primer día, culminando en un perfil de egreso que te impulsará hacia el éxito en tu campo de interés.

No tenemos Facultades, tenemos **HUBs de aprendizaje.**

Combinamos educación de calidad con **programas de última generación.**

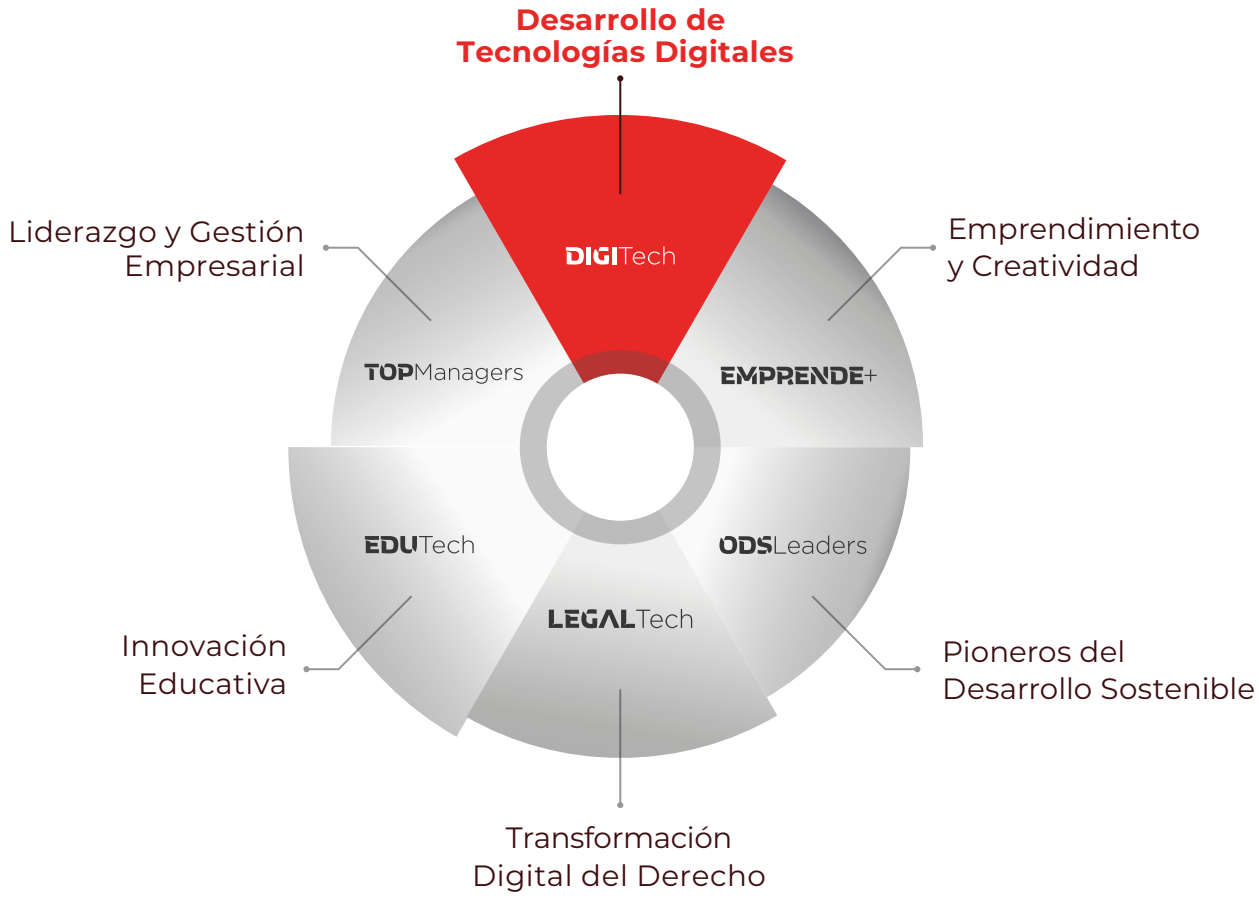
Nuestros profesores son **profesionales en activo** con experiencia en su área.

Contamos **con pedagogías activas** que mejoran tu experiencia.

Te ofrecemos **acompañamiento personalizado** acorde a tu perfil y necesidades.

HUBS de Aprendizaje

Nuestros HUBs de Aprendizaje son conjuntos de programas organizados por áreas temáticas multidisciplinarias que integran conocimientos y prácticas. Su objetivo es desarrollar profesionales completos, dotados de las habilidades y competencias demandadas por el mercado laboral.



Certificaciones Profesionales Avanzadas (CPA)

A través de tres áreas de aprendizaje: PRO-Essentials, PRO-Advanced y PRO- Expertify, los estudiantes adquieren una comprensión profunda de los principios fundamentales, se especializan en áreas específicas y expanden sus horizontes profesionales de manera interdisciplinaria.

1.Certificación Profesional Avanzada PRO-Essentials:

Núcleo básico común
Certificado en Análisis y Gestión de Riesgos con IA

2. Certificación Profesional Avanzada PRO-Advanced:

Núcleo Disciplinar
Certificado en Inteligencia Artificial y Análisis Avanzado para Ciberseguridad

3. Certificado en PRO-Expertify Manager

Núcleo de diversificación

Certificado en PRO-Expertify Manager.

Trabajo Fin de Maestría

Título de Maestría.
Se obtiene finalizando todas las asignaturas de la Maestría, incluyendo proyecto final.

PLAN DE ESTUDIOS

Certificado PRO-Essentials: Certificado en Análisis y Gestión de Riesgos con IA

l núcleo PRO-Essentials se centra en desarrollar habilidades fundamentales que son la base de los estudios de los estudiantes. Destaca el dominio de habilidades clave que pueden aplicarse en diferentes programas, fomentando la interacción entre estudiantes de diversas disciplinas y enriqueciendo sus perfiles y redes de contacto. Se establecen sólidos cimientos para que los estudiantes adquieran una comprensión profunda y experiencial, con énfasis en la calidad de los contenidos y la enseñanza para prepararlos para su crecimiento académico y profesional.

I. - Principios de Inteligencia Artificial aplicada a entornos seguros

La asignatura Principios de Inteligencia Artificial aplicada a entornos seguros proporciona una introducción a los conceptos esenciales de la inteligencia artificial y su aplicación en el ámbito de la ciberseguridad. Se abordan los fundamentos de Machine Learning, Deep Learning y técnicas de análisis de datos, destacando su papel en la detección y prevención de amenazas. Además, se exploran las oportunidades y desafíos de la IA en entornos seguros. El objetivo es ofrecer una visión integral de cómo la IA puede fortalecer la ciberseguridad, sentando las bases para su aplicación en futuros escenarios reales.

Contenidos:

1. Introducción a la Inteligencia Artificial y aprendizaje automático
2. Principios y aplicaciones Big Data en la ciberseguridad
3. Manejo y procesamiento de datos
4. Modelos predictivos en ciberseguridad
5. Introducción a los modelos generativos en Inteligencia Artificial
6. Retos y oportunidades de la Inteligencia Artificial en el contexto de la ciberseguridad

II. - Frameworks y herramientas de IA y Hacking Ético

Esta asignatura se centra en el uso de herramientas y lenguajes clave para el desarrollo de aplicaciones de inteligencia artificial en el ámbito de la ciberseguridad. A través de un estudio profundo de Python, se profundiza en sus librerías de analítica avanzada Numpy y Pandas con el fin de aprender a procesar datos, analizar grandes volúmenes de información y manipular datos estructurados. Además, se introduce PySpark, una herramienta crucial para el procesamiento de datos a gran escala en entornos distribuidos. El curso hace hincapié en cómo estas tecnologías se integran en el hacking ético, permitiendo a los profesionales de ciberseguridad automatizar tareas, realizar análisis de vulnerabilidades y detectar patrones de comportamiento malicioso, todo mientras optimizan el rendimiento y la escalabilidad de las soluciones.

Contenidos:

1. Python para ciberseguridad e IA (i)
2. Python para ciberseguridad e IA (ii)
3. Manipulación y análisis de datos con Pandas
4. Manipulación y análisis de datos con Numpy
5. Procesamiento de grandes volúmenes de datos con Pyspark
6. Optimización y escalabilidad de soluciones

III. - Fundamentos y estrategias de Red Team y Blue Team

En esta asignatura se aborda, desde una perspectiva general, qué es la ciberseguridad y cuál es su función dentro del área de estudio de las tecnologías de la información. Se exploran las diferentes áreas de especialización dentro de la ciberseguridad, permitiendo al alumno adquirir una visión integral de cómo dichas especializaciones conforman una práctica global de protección de la información y los activos digitales que la sustentan.

Además, esta materia sienta las bases conceptuales necesarias para garantizar que todos los alumnos partan desde un conocimiento alineado en ciberseguridad. Esto facilitará la comprensión y el abordaje de los retos que plantea el programa en IA adaptada a la ciberseguridad, asegurando una progresión coherente en el aprendizaje y aplicación de estrategias avanzadas en este campo.

Contenidos:

1. Introducción a la ciberseguridad y sus principales desafíos
2. Estrategias defensivas. El enfoque del Red Team (i): auditorías de seguridad
3. Estrategias defensivas. El enfoque del Blue Team (i): respuesta ante incidentes
4. Estrategias ofensivas. el enfoque del Red Team (ii): auditorías de seguridad avanzadas
5. Estrategias defensivas. El enfoque del Blue Team (ii): análisis forense
6. Inteligencia en ciberseguridad

Certificado PRO-Advanced: Certificado en Inteligencia Artificial y Análisis Avanzado para Ciberseguridad

Las asignaturas PRO-Advanced se centran en el desarrollo de competencias específicas en el área de especialización, así como en la adquisición de habilidades instrumentales necesarias para el trabajo en el campo de estudio. Los estudiantes se sumergen en los conceptos, teorías y prácticas centrales de su disciplina, y obtienen una caja de herramientas para aplicar estos conocimientos en situaciones reales. Además, se enfatiza el trabajo en equipo y el liderazgo, habilidades fundamentales para el éxito profesional en el área.

IV. - Analítica Avanzada para la protección digital

Se abordan técnicas analíticas avanzadas utilizadas en ciberseguridad y ciencia de datos para la detección y mitigación de amenazas. Se profundiza en métodos estadísticos para la identificación de anomalías en grandes volúmenes de datos, lo cual es esencial para detectar comportamientos inusuales que puedan indicar brechas de seguridad o ataques. Además, se exploran herramientas de visualización avanzada que permiten representar y analizar de manera eficaz los datos relacionados con amenazas cibernéticas, facilitando la interpretación y toma de decisiones rápidas ante incidentes. Esta asignatura tiene un enfoque práctico que enseña cómo aplicar estas técnicas para mejorar la protección digital y anticiparse a posibles amenazas.

Contenidos:

1. Introducción a la analítica avanzada en ciberseguridad
2. Métodos estadísticos para la detección de anomalías
3. Análisis de grandes volúmenes de datos en ciberseguridad
4. Visualización avanzada de amenazas y toma de decisiones
5. Creación de dashboards para el monitoreo de amenazas
6. Aplicación práctica de técnicas analíticas en ciberseguridad

V.- Machine Learning aplicado a la Ciberseguridad (I): Aprendizaje Supervisado

Se centra en la aplicación de técnicas de aprendizaje supervisado en la detección y prevención de amenazas cibernéticas. Se profundiza en el uso de modelos de Machine Learning para ejecutar tareas como, por ejemplo, la detección de intrusiones (IDS/IPS), el análisis de eventos de sistemas, la detección y clasificación de patrones relevantes de actividad que puedan indicar una vulnerabilidad o un ataque, o la detección de irregularidades en el tráfico de red. Para ello, se exploran algoritmos de aprendizaje supervisado y abordan enfoques que permiten aplicar los conceptos aprendidos en un entorno práctico y relevante para la ciberseguridad, optimizando la capacidad de respuesta ante incidentes y mejorando la protección de redes.

Contenidos:

1. Introducción a los algoritmos de clasificación en el contexto de ciberseguridad
2. Evaluación de modelos de clasificación: métricas y aplicaciones
3. Introducción a los algoritmos de regresión en el contexto de ciberseguridad
4. Evaluación de modelos de regresión: métricas y aplicaciones
5. Regularización modelos financieros: Regresión Lasso y Ridge
6. Optimización y ajuste de hiperparámetros en modelos supervisados

VI.- Machine Learning aplicado a la Ciberseguridad (II): Aprendizaje No Supervisado

Desarrollar conocimientos y habilidades en la aplicación de técnicas de aprendizaje no supervisado orientadas a la ciberseguridad, permitiendo la identificación de patrones, comportamientos anómalos y posibles amenazas en grandes volúmenes de datos. A través del uso de algoritmos de clustering y reducción de dimensionalidad, los estudiantes fortalecerán su capacidad para analizar registros y eventos de seguridad, contribuyendo a la detección temprana de vulnerabilidades e incidentes en entornos digitales complejos.

Contenidos:

1. Introducción al aprendizaje no supervisado en el contexto financiero
2. Fundamentos de los algoritmos de clustering
3. K-Means o DBSCAN para detección de anomalías
4. Árboles de decisión para la detección de fraude financiero
5. Evaluación y validación de modelos de clustering en ciberseguridad
6. Algoritmos de reducción de dimensionalidad

VII.- Deep Learning: modelos avanzados

Desarrollar competencias en el diseño, evaluación y aplicación de modelos avanzados de Deep Learning para la resolución de desafíos en ciberseguridad. A través del estudio de arquitecturas como redes convolucionales (CNN), redes neuronales recurrentes (RNN) y modelos LSTM, los estudiantes adquirirán la capacidad de analizar datos complejos, identificar amenazas, detectar patrones anómalos en secuencias temporales y aprovechar modelos preentrenados para fortalecer la protección de sistemas y redes en entornos digitales dinámicos.

Contenidos:

1. Introducción al Deep Learning en ciberseguridad
2. Redes neuronales profundas (DNN) y su aplicación en detección de amenazas
3. Redes convolucionales (CNN) para análisis de imágenes
4. Redes Neuronales Recurrentes (RNN) y LSTM para análisis de secuencias en tráfico de red
5. Evaluación y optimización de modelos de Deep Learning en ciberseguridad
6. Reutilización de modelos preentrenados y transferencia de aprendizaje

VIII.- Procesamiento de Lenguaje Natural en Defensa Digital

Desarrollar competencias en la aplicación de técnicas de procesamiento de lenguaje natural (NLP) para la identificación y prevención de amenazas cibernéticas basadas en contenido textual. A través del análisis de correos electrónicos, mensajes y sitios web, los estudiantes aprenderán a utilizar modelos y algoritmos de NLP para detectar spam, intentos de phishing y otros riesgos asociados a la ingeniería social, fortaleciendo la capacidad de automatizar procesos de defensa digital y mejorar la protección de los sistemas de información.

Contenidos:

1. Introducción al Procesamiento de Lenguaje Natural (NLP)
2. Técnicas de NLP para la detección de spam y malware en comunicaciones digitales
3. Análisis de phishing en correos electrónicos y mensajes fraudulentos mediante NLP
4. Detección de páginas web fraudulentas y análisis de contenido malicioso con NLP
5. Identificación de patrones lingüísticos en ataques de suplantación de identidad
6. Automatización de la detección de amenazas cibernéticas a través de NLP

IX.- IA Generativa para la Seguridad Digital (I): bases, creación y análisis de imágenes

La primera parte de IA Generativa para la Seguridad Digital se enfoca en el uso de modelos de inteligencia artificial generativa aplicados a la ciberseguridad, con un énfasis especial en la creación y el análisis de imágenes. A lo largo del curso, desarrollarás conocimientos y habilidades en la aplicación de técnicas de inteligencia artificial generativa para la creación, análisis y validación de contenido visual en contextos de ciberseguridad. A través del estudio de modelos generativos, como las redes generativas adversariales (GANs), los estudiantes comprenderán los fundamentos de la generación de imágenes sintéticas y adquirirán competencias para detectar manipulaciones digitales, incluyendo deep fakes, fortaleciendo su capacidad para identificar amenazas emergentes y proteger la integridad de la información en entornos digitales.

Contenidos:

1. Introducción a la IA Generativa y su aplicación en ciberseguridad
2. Redes Generativas Adversariales (GANs): Fundamentos y aplicaciones
3. Creación y análisis de imágenes sintéticas con IA generativa
4. Detección de manipulación de imágenes y videos en ciberseguridad
5. Análisis de Deep Fakes: Identificación y prevención de contenido falso
6. Técnicas avanzadas para mejorar la defensa digital contra contenido multimedia

X.- IA Generativa para la Seguridad Digital (II): generación y protección de texto

Desarrollar competencias en el uso de modelos de inteligencia artificial generativa para la creación, análisis y protección de contenido textual en entornos de ciberseguridad. A través del estudio de modelos de lenguaje de gran escala (LLM), técnicas de prompting, RAG, fine tuning y agentes inteligentes, los estudiantes adquirirán las capacidades necesarias para implementar soluciones avanzadas de automatización, detección de amenazas y análisis de información, fortaleciendo la identificación y prevención de riesgos como el spam, el phishing y otros ataques basados en contenido textual.

Contenidos:

1. Introducción a los Modelos de Lenguaje Grandes (LLM)
2. Generación y protección de contenido textual usando IA generativa
3. Técnicas de prompting: Generación de respuestas y textos específicos
4. Retrieval-Augmented Generation (RAG) y su aplicación en la protección digital
5. Fine-tuning de modelos generativos para adaptarse a necesidades de ciberseguridad
6. Detección de amenazas cibernéticas: Uso de IA generativa en la prevención de phishing y spam

XI.- Seguridad y gestión de riesgos en MLOps

Fortalecer las capacidades para integrar prácticas de seguridad y gestión de riesgos en el ciclo de vida de los modelos de Machine Learning, aplicando principios de MLOps y DevSecOps que garanticen la protección de datos, modelos e infraestructuras. Los estudiantes adquirirán conocimientos sobre gestión de identidades y accesos, cifrado, auditoría, versionado y seguridad en pipelines de datos, fortaleciendo la trazabilidad, integridad y confiabilidad de las soluciones de inteligencia artificial en entornos organizacionales.

1. Introducción a MLOps y la seguridad en el ciclo de vida del desarrollo de modelos
2. Principios de desarrollo seguro y DevSecOps en el contexto de Machine Learning
3. Gestión de identidades y accesos (IAM) para proteger modelos y datos sensibles
4. Cifrado de datos y modelos: Protección en tránsito y reposo
5. Versionado y auditoría de modelos: Garantizando trazabilidad y transparencia
6. Seguridad en los pipelines de datos: Protección en el flujo de información desde la recolección hasta la implementación

Certificado ProExpertify: Certificación profesional avanzada

El PRO Expertify es la fase de especialización avanzada del programa, donde los estudiantes cursan asignaturas que profundizan su formación y les permiten afrontar desafíos reales en el sector. Este módulo aporta una visión estratégica e interdisciplinaria, dotando a los participantes de herramientas innovadoras para analizar contextos, diseñar soluciones y liderar procesos de transformación. El Certificado PRO Expertify acredita la adquisición de estas competencias especializadas y refuerza la proyección profesional del estudiante.

I- PRO Expertify Manager

XII.- Ética, Regulación y Gobernanza en IA y Ciberseguridad

La asignatura Ética, Regulación y Gobernanza en IA y Ciberseguridad aborda los aspectos éticos y regulatorios clave en el desarrollo y uso de inteligencia artificial en el contexto de la ciberseguridad. Se profundiza en la explicabilidad de modelos, asegurando que las decisiones tomadas por los sistemas de IA sean comprensibles y transparentes. También se estudian prácticas de anonimización de datos para proteger la privacidad y cumplir con normativas como el GDPR. La asignatura cubre temas de regulación, como las leyes y estándares que afectan a la IA y la ciberseguridad, y cómo implementar marcos de gobernanza para gestionar los riesgos asociados al uso de tecnologías emergentes, garantizando un uso responsable y ético de la inteligencia artificial en la protección digital.

Contenidos:

1. Introducción a la ética, regulación y gobernanza en IA
2. Explicabilidad y transparencia en los modelos de inteligencia artificial
3. Prácticas de anonimización de datos y cumplimiento con normativas de privacidad (GDPR)
4. Regulación de la inteligencia artificial y ciberseguridad: Leyes y estándares clave
5. Marcos de gobernanza para la gestión de riesgos en tecnologías emergentes
6. Uso responsable y ético de la IA en la protección digital

XIII.- Introducción a la Criptografía: de los fundamentos a la criptografía Post-Cuántica

Esta asignatura ofrece una introducción a los principios fundamentales de la criptografía, desde los sistemas clásicos hasta los modernos, explorando su importancia en la seguridad digital. Se abordarán los conceptos esenciales de cifrado simétrico y asimétrico, firmas digitales y protocolos de seguridad utilizados en Internet. Además, se introducirá la computación cuántica y su impacto en la criptografía tradicional, explicando por qué los sistemas actuales podrían volverse inseguros ante el avance de los ordenadores cuánticos.

Contenidos:

1. Fundamentos de la Criptografía
2. Criptografía Moderna y Seguridad en Internet
3. Introducción a la computación cuántica
4. Criptografía post-cuántica
5. Métodos post-cuánticos basados en redes euclidianas (lattice-based), basados en códigos (code-based) y basados en funciones hash (hash-based).
6. Estado actual de la estandarización (NIST PQC) y desafíos futuros

XIV.- Proyecto Final

El trabajo final de la Maestría es el último paso para poder obtener el título del programa formativo. Consiste en la realización de un trabajo académico en el que se apliquen o desarrollen conocimientos adquiridos a lo largo del programa formativo. Este trabajo deberá contemplar la aplicación de competencias generales asociadas al programa.

CERTIFICACIÓN DE HARVARD MANAGEMENTOR

En el Instituto Europeo de Posgrado, nuestro **compromiso es tu éxito educativo y profesional.**

Por ello, brindamos a nuestros estudiantes un acceso exclusivo a Harvard ManageMentor, la plataforma líder a nivel mundial que ofrece una amplia gama de recursos de aprendizaje y desarrollo profesional.

Harvard ManageMentor representa la conjunción perfecta entre la renombrada excelencia académica de la Universidad de Harvard y la comodidad de la formación en línea, brindando a empresas y profesionales las herramientas necesarias para perfeccionar sus habilidades y alcanzar un nivel de desempeño excepcional.

A través de Harvard ManageMentor, tendrás accesos a cursos interactivos y recursos de alta calidad que abarcan temas esenciales en el mundo empresarial, como liderazgo, gestión, comunicación y toma de decisiones estratégicas. Esta plataforma en línea es desarrollada por Harvard Business Publishing.

OTROS BENEFICIOS QUE TE OFRECE EL PROGRAMA

Si buscas mejorar tus habilidades profesionales en áreas clave de liderazgo, gestión y desarrollo personal, con este programa, tendrás la oportunidad de realizar un curso certificado de Harvard, de manera opcional y complementario a tu formación. Elige el curso que más se adapte a tus necesidades y potencia tus habilidades profesionales obteniendo un certificado de Harvard.

¿Qué es?

Red SUMMA ha establecido un acuerdo académico con Harvard Business School Publishing, que beneficiará a todos nuestros estudiantes. Ahora, tienen la oportunidad de acceder a Harvard ManageMentor (HMM) de forma gratuita.

- **Contenido de Calidad:** Aprende de expertos en gestión y liderazgo de renombre internacional.
- **Flexibilidad:** Accede al contenido en línea desde cualquier ubicación y en el momento que mejor se adapte a tu tiempo.
- **Desarrollo Personalizado:** Utiliza herramientas de autoevaluación y seguimiento para medir tu progreso y áreas de mejora.

Oferta a la que puedes acceder

- **Liderando Personas** (Leading People)
- **Gestión de Proyectos** (Project Management)
- **Innovación y Creatividad** (Innovation and Creativity)
- **Habilidades de Presentación** (Presentation Skills)
- **Gestión de Equipos** (Team Management)
- **Diversidad, Inclusión y Pertenencia** (Diversity, Inclusion, and Belonging)
- **Persuadiendo a Otros** (Persuading Others)
- **Interacciones Difíciles** (Difficult Interactions)
- **Conceptos Básicos de Finanzas** (Finance Essentials)
- **Negociación** (Negotiating)

Elige uno de ellos y adquiere habilidades esenciales para **triunfar en el mundo empresarial.**

POR QUÉ ELEGIR ESTE PROGRAMA

Elegir este programa supone acceder a una formación innovadora, práctica y altamente especializada, diseñada para responder a las necesidades reales del sector. Algunas de las razones clave por las que esta maestría destaca sobre otros programas incluyen:

1.Enfoque práctico y aplicado

Esta maestría combina una sólida base teórica con un enfoque altamente práctico. Los estudiantes trabajan con casos reales, herramientas de última generación y metodologías utilizadas en la industria. Se prioriza el aprendizaje basado en proyectos, permitiendo a los alumnos aplicar sus conocimientos en escenarios concretos de ciberseguridad e IA.

2.Un programa pionero en un sector en auge

La convergencia entre la Inteligencia Artificial y la Ciberseguridad es un ámbito emergente y en constante evolución. Esta maestría es uno de los primeros programas especializados que aborda de manera integral el uso de IA para fortalecer la seguridad digital. La creciente demanda de expertos en este campo hace que nuestros egresados sean altamente valorados por empresas tecnológicas, consultoras y organismos gubernamentales.

3.Claustro de expertos de primer nivel

El programa cuenta con un claustro formado por profesionales de referencia en el sector. Nuestros docentes provienen de empresas tecnológicas líderes en el país, lo que garantiza una enseñanza alineada con la realidad del mercado.

4.Contenidos adaptados a las últimas tendencias tecnológicas

El programa abarca desde Machine Learning y Deep Learning hasta IA generativa aplicada a la seguridad digital. Además, se profundiza en criptografía post-cuántica, un área clave ante el avance de la computación cuántica.

5.Formación integral: técnica, estratégica y ética

Además de habilidades técnicas avanzadas, el programa pone especial énfasis en la gobernanza de IA, la regulación y la ética en ciberseguridad. Este enfoque prepara a los alumnos no solo para desarrollar soluciones innovadoras, sino también para liderar proyectos estratégicos con impacto en empresas y organismos públicos.

METODOLOGÍA

La metodología de aprendizaje se basa en el **método del caso** y en la aplicación práctica de los contenidos, permitiendo al estudiante analizar situaciones reales y tomar decisiones en contextos similares a los del entorno profesional.

El programa combina recursos digitales interactivos, casos prácticos, ejercicios aplicados y acompañamiento académico personalizado, favoreciendo un aprendizaje activo y orientado a resultados.

Además, el estudiante cuenta con sesiones virtuales de repaso, una planificación semanal de trabajo y el acompañamiento personalizado de un tutor académico, favoreciendo un aprendizaje práctico, dinámico y guiado.

CARACTERÍSTICAS DEL PROGRAMA

Duración del programa: 24 meses (lectivos)
Créditos: 75
Modalidad: Virtual.
Título Oficial: Maestría en Inteligencia Artificial Aplicada a la Ciberseguridad
Reconocimiento de Validez Oficial de Estudios por la Secretaría de Educación acuerdo número: 20252623
Certificación Internacional: Advanced Executive Program in Applied Artificial Intelligence

CERTIFICACIONES

Certificación Profesional Avanzada PRO-Essentials:
Certificado en Análisis y Gestión de Riesgos con IA

Certificación Profesional Avanzada PRO-Advanced:
Certificado en Inteligencia Artificial y Análisis Avanzado para Ciberseguridad

Certificación Profesional Avanzada PRO-Expertify:
Certificado en PRO-Expertify Manager

FORMACIÓN PREVIA

Podrán acceder al programa quienes cuenten con una titulación universitaria.

EXPERIENCIA

Para la correcta asimilación de los contenidos se recomienda contar con al menos 3 años de experiencia profesional.

ELEVA TU POTENCIAL Y TRANSFORMA TU FUTURO

MATRICÚLATE HOY

Instituto Europeo de Posgrado

+55 6274 4478 | +55 6271 6099
nuevoingreso@iep-edu.mx
iep-edu.mx