Instituto Europeo de Posgrado

RED SUMMA Education

Máster Online
Inteligencia Artificial Aplicada a la Ciberseguridad

HUB DE APRENDIZAJE:

DIGITech

RANKING Forbes LAS MEJORES ESCUELAS DE NEGOCIOS TOP 5 JUNIO 2022

FSO RANKING

IEP: Nº 1 DEL MUNDO EN **EMPLEABILIDAD** Y **CALIDAD DEL PROFESORADO**

ÍNDICE

PRESENTACIÓN DE LA ESCUELA

El Instituto Europeo de Posgrado es una **innovadora Escuela de Negocios 100% online,** que imparte programas de MBA, Máster 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

CARTA DEL DIRECTOR

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 se pueden 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 de 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.

Desde el año 2009, más de 130.000 alumnos de 80 nacionalidades diferentes han cursado alguno de nuestros programas. A través de este folleto, queremos abrirte las puertas de nuestra escuela, para que nos conozcas, no sólo a través de nuestras palabras, sino de sus testimonios.

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

Bienvenido a la formación a medida de tus necesidades.

Carlos Pérez Castro
Director del Instituto Europeo de Posgrado

JUSTIFICACIÓN

En un entorno digital cada vez más interconectado y vulnerable a ciberataques sofisticados, la **capacidad para analizar y gestionar grandes volúmenes de datos** se ha convertido en un pilar fundamental de la ciberseguridad.

La Inteligencia Artificial ha emergido como una herramienta muy poderosa para detectar, prevenir y mitigar amenazas en tiempo real, permitiendo a las organizaciones fortalecer su defensa frente a ataques cibernéticos y proteger sus activos digitales.

El **Máster en Inteligencia Artificial Aplicada a la Ciberseguridad** está diseñado para formar a profesionales altamente capacitados en el uso de técnicas avanzadas de IA enfocadas en la seguridad informática. A lo largo del programa, los estudiantes desarrollarán una comprensión profunda de los **algoritmos de aprendizaje automático, detección de anomalías, análisis de malware, identificación de vulnerabilidades, respuesta automatizada a incidentes y protección de infraestructuras críticas.**

Con un enfoque eminentemente práctico, el máster combina teoría y aplicación para garantizar que los alumnos puedan diseñar e implementar soluciones innovadoras en múltiples entornos, desde empresas hasta instituciones gubernamentales. Además, se abordan aspectos esenciales como la ética, la privacidad y la regulación, elementos clave en el desarrollo de soluciones de Inteligencia Artificial para la ciberseguridad. También se estudia **criptografía post-cuántica,** una pieza clave en la protección de la información ante la inminente llegada de los ordenadores cuánticos, cuya capacidad de cálculo podría comprometer los sistemas criptográficos actuales.

Este programa prepara a sus graduados para **liderar la transformación digital en el ámbito de la seguridad informática,** utilizando la IA para anticipar amenazas, reducir riesgos y tomar decisiones basadas en análisis avanzados. Con una visión estratégica y tecnológica, los estudiantes estarán equipados para afrontar los desafíos de un mundo digital en constante evolución.

Modelo Educativo Innovador: EDUex

En el corazón de nuestro máster se encuentra el **modelo educativo EDUex,** una metodología revolucionaria que integra tecnologías avanzadas y pedagogías de vanguardia para garantizar que cada estudiante no solo adquiera conocimientos fundamentales, sino que también desarrolle habilidades críticas aplicables al ámbito empresarial digital.

Este **Máster en Inteligencia Artificial Aplicada a la Ciberseguridad,** es un programa innovador para el desarrollo de tecnologías digitales 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.

OBJETIVOS

- 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

El máster está dirigido 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:
Experto en Inteligencia Artificial Aplicada a la ciberseguridad

Función principal:
Diseñar, desarrollar y aplicar soluciones de inteligencia artificial para prevenir, detectar, responder y mitigar amenazas de seguridad informática.

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.

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.

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.

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.

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.

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.

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.

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.

MODELO DE APRENDIZAJE

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.**

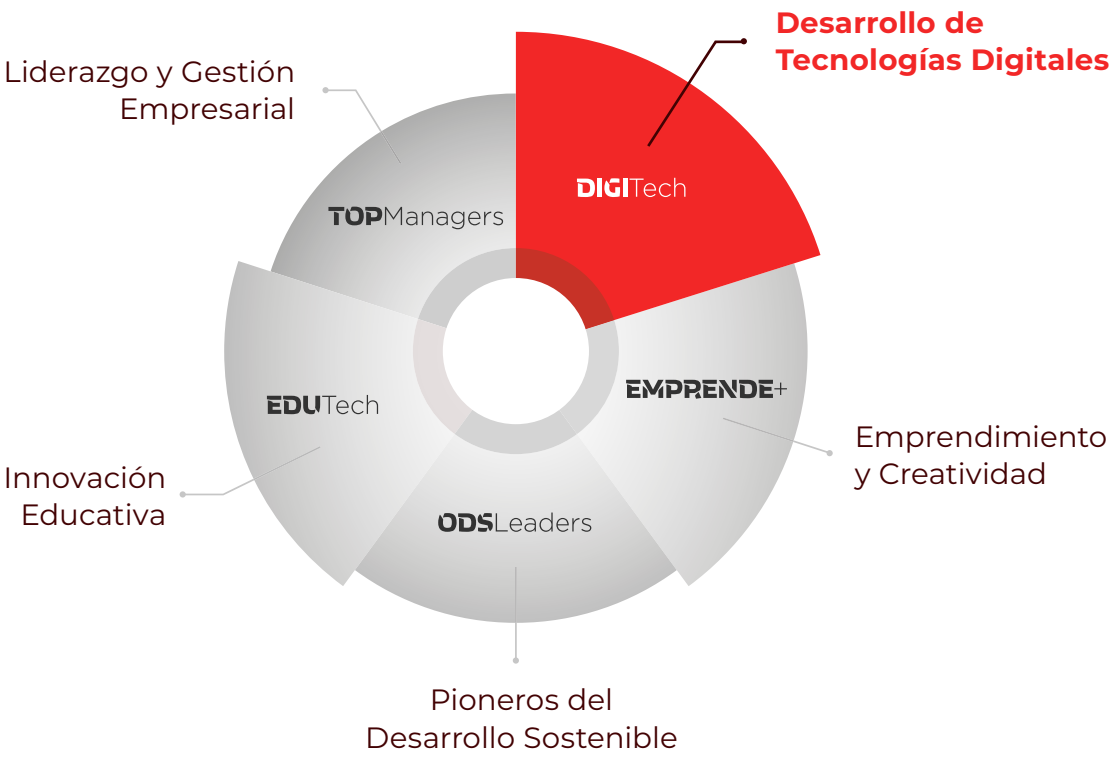
Nuestros profesores son **profesionales en activo** con experiencia en su área.

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)

Te ofrecemos una formación flexible y adaptada a tus necesitades individuales. Nuestro modelo de flexibilidad curricular estructura los programas en 3 núcleos formativos certificables:

NÚCLEO BÁSICO COMÚN

Asignaturas transversales a todos los programas.

- **Certificado en Análisis y Gestión de Riesgos con IA**

NÚCLEO DISCIPLINAR

Desarrolla competenicas específicas a tu campo de estudio.

- **Certificado en Inteligencia Artificial y Análisis Avanzado para Ciberseguridad**

NÚCLEO DE DIVERSIFICACIÓN

Elige tu área de especialización:

- **Certificado en PROexpertify Manager**

PLAN DE ESTUDIOS[1]

Modalidad: *Online*
Créditos: *86 ECTS*

[1] La Institución se reserva el derecho a realizar modificaciones en el Programa para su mejora y actualización.

PROessentials: Certificado en Análisis y Gestión de Riesgos con IA

El núcleo PROessentials 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 (6 ECTS)

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 (6 ECTS)

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 procesar de datos, analizar de grandes volúmenes de información y manipular de datos estructurados. Además, se introduce Pyspark, una herramienta crucial para el procesamiento de datos a gran escala en entornos distribuidos. El curso hace especial 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 (6 ECTS)

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 máster 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

PROadvance: Certificado en Inteligencia Artificial y Análisis Avanzado para Ciberseguridad

Las asignaturas PROadvanced 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 (6 ECTS)

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 (6 ECTS)

La asignatura 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. ntroducción 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 (6 ECTS)

Este segundo bloque de Machine Learning aplicado a la Ciberseguridad se enfoca en el uso de técnicas de aprendizaje no supervisado para detectar patrones y anomalías en entornos cibernéticos sin necesidad de etiquetas predefinidas. En particular, se profundiza en la identificación de anomalías en logs, un aspecto crucial para la detección temprana de intrusiones o actividades sospechosas. A través de algoritmos como clustering y reducción de dimensionalidad, los estudiantes aprenderán a identificar comportamientos inusuales en grandes volúmenes de datos de registros del sistema, que podrían indicar un ataque o una vulnerabilidad. La asignatura pone énfasis en cómo aplicar estos enfoques en escenarios reales de ciberseguridad, mejorando la capacidad de análisis y respuesta ante amenazas emergentes sin depender de datos previamente clasificados.

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 (6 ECTS)

La asignatura se enfoca en el estudio de arquitecturas avanzadas de Deep Learning aplicadas a la ciberseguridad. Se exploran redes neuronales profundas y otras arquitecturas, como las redes convolucionales (CNN) para tareas de visión por computador (CV), específicamente en la detección de amenazas a través del análisis de imágenes y videos de sistemas de seguridad.

Además, se aborda la evaluación de modelos de Deep Learning, proporcionando herramientas y técnicas para medir su rendimiento y efectividad en escenarios reales. La

asignatura también cubre la reutilización de modelos preentrenados, lo que permite optimizar el desarrollo y la implementación de soluciones en ciberseguridad. Un enfoque clave es el uso de RNN (Redes Neuronales Recurrentes) y LSTM (Long Short-Term Memory) para detectar patrones en secuencias temporales, como logs y tráfico de red, con el fin de identificar comportamientos anómalos o ataques que evolucionan con el tiempo. Todo esto permite mejorar la protección de sistemas y redes mediante la capacidad de modelar datos complejos y 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 (6 ECTS)

Esta asignatura se centra en la aplicación de técnicas de procesamiento de lenguaje natural (NLP) para la detección de amenazas cibernéticas relacionadas con el contenido textual. Se profundiza en el uso de algoritmos y modelos de NLP para la detección de spam, un riesgo común en la ciberseguridad que puede ser un vector de ataque para phishing u otros tipos de malware. Además, se aborda la detección de phishing mediante el análisis de correos electrónicos, mensajes y páginas web fraudulentas, identificando patrones y características lingüísticas que suelen ser indicativos de intentos de suplantación de identidad. La asignatura tiene un enfoque práctico en cómo implementar estos enfoques para automatizar la detección de amenazas y mejorar la seguridad digital, permitiendo a los estudiantes aplicar el NLP en la protección contra ataques basados en contenido textual.

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 (6 ECTS)

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, se exploran las bases de las redes generativas adversariales (GANs) y otras técnicas de IA generativa, que permiten tanto la creación de imágenes sintéticas como la detección de manipulaciones. Uno de los temas clave es la detección de deep fakes, una amenaza creciente en la ciberseguridad que involucra la creación de contenido multimedia falsificado, como videos e imágenes, con el fin de engañar o desinformar. Los estudiantes aprenderán a identificar estos contenidos fraudulentos mediante el análisis de patrones y características visuales que pueden revelar alteraciones, mejorando así las capacidades de defensa contra este tipo de ataque.

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 falsificado

X.- IA Generativa para la Seguridad Digital (II): generación y protección de texto (6 ECTS)

La segunda parte de IA Generativa para la Seguridad Digital se centra en la aplicación de LLM para la creación y protección de contenido textual en el contexto de la ciberseguridad. Los estudiantes aprenderán sobre el consumo de modelos generativos avanzados y la técnica de prompting, que permite generar respuestas o textos específicos a partir de entradas controladas. Además, se abordarán conceptos como RAG (retrieval-augmented generation) y el fine tuning de modelos para adaptarlos a necesidades particulares, así como el uso de agentes inteligentes para automatizar tareas relacionadas con la seguridad. La asignatura también cubre el uso de plataformas en la nube y APIs para implementar estos modelos a gran escala. Un enfoque importante será la detección de amenazas cibernéticas a través de la generación y análisis de texto, especialmente en la detección de spam y phishing, donde los modelos de IA generativa pueden ser clave para identificar patrones y prevenir ataques basados en la manipulación de 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 (6 ECTS)

Esta asignatura se enfoca en la integración de prácticas de seguridad dentro del ciclo de vida del desarrollo de modelos de Machine Learning en entornos de operaciones (MLOps). Se exploran los principios de desarrollo seguro y DevSecOps, que buscan incorporar la seguridad desde las primeras etapas del desarrollo de modelos, garantizando que las soluciones sean robustas frente a posibles amenazas. La gestión de identidades y accesos (IAM) se aborda para asegurar que solo los usuarios autorizados puedan interactuar con los modelos y datos sensibles. Además, se profundiza en el cifrado de datos y modelos para proteger la información tanto en tránsito como en reposo. La asignatura también cubre el versionado y la auditoría de modelos, asegurando la trazabilidad y la transparencia de las decisiones tomadas por los sistemas de IA. Finalmente, se analiza la seguridad en los pipelines de datos, protegiendo todo el flujo de información desde la recolección hasta la implementación de los modelos, para minimizar riesgos y garantizar la integridad del proceso.

Contenidos:

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

PROexpertify: Especialízate en tu área de conocimiento

XII.- Ética, Regulación y Gobernanza en IA y Ciberseguridad (6 ECTS)

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 (6 ECTS)

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.- Trabajo Fin de Programa (8 ETCS)

El Trabajo Fin de Máster 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.

Testimonial

"En mi vida profesional, el Máster me ha permitido conocer conceptos y estrategias novedosas aplicables a mi puesto de trabajo actual. Pero, por encima de todo, destacaría el trato personalizado que recibe el alumnado. Creo que poder mantener la relación con la Escuela y los compañeros me aporta un valor añadido profesional y personal."

Vicente Verdú
Director comercial de Cosesa

CERTIFICACIONES

Respalda tu formación con **certificaciones reconocidas** que acreditan tus habilidades.

Certificación Generative AI Foundations de Critical Career Skills

- Curso de preparación opcional: Generative AI Foundations
- Gratuito
- Incluye examen de Certificación

La certificación Generative AI Foundations te especializa en diseñar y aplicar soluciones innovadoras basadas en inteligencia artificial generativa. Capacita para optimizar procesos y mejorar la personalización en áreas como marketing, desarrollo de productos y atención al cliente. Esta credencial valida tus habilidades en el uso avanzado y ético de la IA, posicionándote como líder en proyectos de transformación digital.

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.

¿QUÉ BENEFICIOS OBTENDRÁS?

- **Desarrollo Profesional:** tendrás acceso a recursos de desarrollo profesional de alta calidad que cubren una amplia gama de temas relacionados con la toma de decisiones, la comunicación, la gestión del cambio y muchos otros aspectos relevantes para los líderes y profesionales de negocios.
- **Flexibilidad:** podrás acceder al contenido online desde cualquier lugar y en cualquier momento, adaptando tu aprendizaje a tu horario y ritmo personal.
- **Contenido actualizado:** donde verás reflejadas las tendencias y mejores prácticas actuales en el mundo empresarial.
- **Evaluación y Seguimiento:** Te ayudará a medir tu progreso y comprender tus fortalezas y áreas de mejora.
- **Certificación de Harvard Business Publishing:** Obtendrás tu certificado al completar con éxito los cursos.
- **Aplicación práctica:** Los recursos y casos de estudio te ayudarán a aplicar lo que aprendes en situaciones reales en tu entorno laboral.

¿QUÉ RECURSOS TENDRÁS A TU DISPOSICIÓN?

- **Módulos de aprendizaje sobre liderazgo, gestión de proyectos, toma de decisiones estratégicas y más.**
- **Vídeos, casos de estudio de la facultad de Harvard Business School y simulaciones interactivas.**

- Evaluaciones y seguimiento de tu progreso.
- Recursos descargables para reforzar el aprendizaje.

CURSOS DISPONIBLES

- **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.**

Testimonial

“La metodología de estudio me parece la ideal para personas como yo, que estamos trabajando y no disponemos del tiempo suficiente para tener clases presenciales o llevar un ritmo de trabajo y estudio constante. Por otra parte, la involucración del personal de la Escuela y del profesorado ha sido y está siendo muy cercana al alumno, mostrando en todo momento un verdadero interés en la impartición de las clases y en el intento de mejorar y facilitar la comprensión de todos los conceptos por nuestra parte. ”

Lucía Vaquero Otero

¿POR QUÉ ELEGIR ESTE MÁSTER EN LÍNEA?

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 este máster destaca sobre otros programas incluyen:

1. Enfoque práctico y aplicado
Este máster 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. Este máster 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 máster cuenta con un claustro formado por profesionales de referencia en el sector. Nuestros docentes provienen de empresas tecnológicas líderes, 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

CLAUSTRO DOCENTE

El IEP cuenta con un claustro de profesores de **primer nivel nacional e internacional.**

MANUEL DE LUNA AMAT

Profesor de Machine Learning y Data Science en destacadas escuelas de negocio.

Graduado en Ingeniería Mecánica por la Universidad de Huelva, con un Máster en Ciencia de Datos, Big Data y Finanzas por AFI, y en Big Data y Analítica para Empresas por la Universidad Alfonso X el Sabio. Certificado como Professional Machine Learning Engineer por Google. Data Scientist en Telefónica Tech y cuenta con + 6 años de experiencia en el desarrollo de proyectos analíticos e implementación de soluciones basadas en Inteligencia Artificial.

METODOLOGÍA

Nuestra metodología online incorpora las **últimas novedades tecnológicas** que permiten hacer del e-learning un aprendizaje sencillo, cómodo y eficaz.

Con una innovadora plataforma online que permite la realización de **ejercicios interactivos** y la discusión de **casos prácticos** para desarrollar las habilidades de gestión y de análisis.

Con recursos de aprendizaje basados en avanzados **simuladores empresariales** que permiten **movilizar el conocimiento** y apoyar el emprendimiento entre nuestros alumnos.

Con **vídeos explicativos** de los profesores en cada módulo que te facilitarán el aprendizaje y te permitirán afianzar mejor los conceptos.

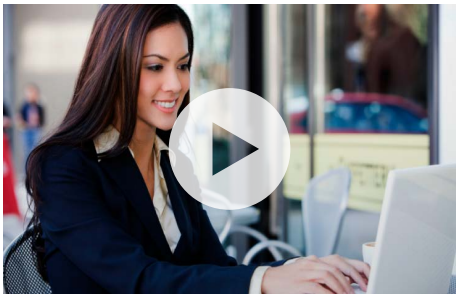
Con **Sesiones Virtuales de Repaso, Casos Prácticos Integrales** y **Masterclass Nuevas Tendencias,** que permiten ampliar conocimientos y aportar una visión práctica y aplicada a situaciones reales de las empresas.

El método de trabajo consiste en una planificación semanal de las materias, con un profesor que se encarga de acompañar a los alumnos durante todo el módulo, resolviendo sus dudas y fomentando su participación en los foros. Todo ello apoyado con la utilización del **"método del caso"** para afianzar los conocimientos adquiridos y aplicarlos a la realidad empresarial.

Además, para garantizar el ritmo de aprendizaje de los alumnos un equipo de tutores realiza un **seguimiento personalizado** de los mismos, apoyándoles y motivándoles en todo momento. De esta manera obtenemos un alto nivel de satisfacción y de finalización de los participantes.

VIDEO

Conoce mejor nuestra metodología en el siguiente video. También puedes escanear este código con tu móvil:



PROCESO DE ADMISIÓN

Para cada convocatoria se realiza el siguiente proceso de admisión, en base a una selección de alumnos para las **plazas limitadas** ofertadas:

1 • Los asesores de admisiones de IEP informarán al candidato sobre todas las cuestiones relativas al programa así como del proceso y condiciones de admisión.

2 • El candidato deberá cumplimentar el "formulario de admisión y enviarlo a IEP junto con su Currículum Vitae.

3 • El Comité de Admisiones estudiará el expediente y comunicará al estudiante, si es apto, que le concede la plaza para estudiar el programa.

4 • Una vez recibido el certificado de admisión, el estudiante deberá formalizar su matriculación.

INFORMACIÓN GENERAL

Modalidad: Virtual.
Créditos: 86
Título: Máster en Inteligencia Artificial Aplicada a la Ciberseguridad por el Instituto Europeo de Posgrado en España.
Certificación internacional: Advanced Executive Program in Applied Artificial Intelligence.

AYUDAS AL ESTUDIO / BECAS

El Instituto cuenta con un programa de becas diseñado para ayudar a los estudiantes durante su proceso de matriculación. En cada convocatoria se ofertan un número limitado de becas en base a la situación personal, profesional o económica de los candidatos. Para su adjudicación, se sigue un riguroso orden de solicitud.

FINANCIACIÓN

Existen también condiciones especiales de financiación, con el fin de ayudar a los alumnos a asumir el coste del curso a través de un sistema de pagos aplazados mediante **cuotas mensuales** cómodas y adaptadas a las necesidades de los alumnos.

RECONOCIMIENTOS

En el Instituto Europeo de Postgrado, nos enorgullece nuestra posición entre la élite en el **ámbito educativo virtual en habla hispana.** Nuestro compromiso con la excelencia es reconocido consistentemente a través de prestigiosos rankings y distinciones de instituciones de renombre internacional, destacando la calidad superior de nuestra educación y nuestra dedicación al éxito de nuestros estudiantes.

Nº1
A nivel mundial en empleabilidad y calidad del profesorado.
Ranking FSO - 2022

TOP 6
Mejor institución en formación superior online en el mundo.
Ranking FSO - 2022

TOP 5
Mejor MBA con énfasis en Dirección General.
Ranking Forbes - 2022

TOP 3
Mejor MBA Online de España 2023.
Mundo Posgrado - 2023

TOP 6
Mejores centros para cursar un MBA Online.
Ranking El Mundo - 2022

PARTNERS ACADÉMICOS

IEP colabora con una red de destacados **partners académicos** a nivel mundial, asegurando que nuestros programas se enriquezcan con diversas perspectivas y conocimientos de vanguardia. Estas alianzas nos permiten ofrecer programas **co-certificados** que aumentan el valor de nuestros títulos, brindando a nuestros estudiantes una educación globalmente reconocida y completa.

ACREDITACIONES

Nuestros programas son rigurosamente evaluados y acreditados por los **principales organismos acreditadores internacionales,** lo que confirma los altos estándares de nuestro currículo y la excepcional calidad de nuestra oferta educativa. Estas acreditaciones son un testimonio de la calidad, credibilidad y aceptación global de los programas del IEP, asegurando a nuestros estudiantes una experiencia educativa de clase mundial.

LANZA TU CARRERA Y CRECE EN LA VIDA

MATRICÚLATE HOY

Instituto Europeo de Posgrado

C/ Caléndula 93
Edificio J (Miniparc III),
Alcobendas, 28109 Madrid

+34 91 661 39 95
admisiones@iep.edu.es
www.iep.edu.es