Máster Título Propio

Inteligencia Artificial en Ciberseguridad

tech global university

tech global university

Máster Título Propio
Inteligencia Artificial en Ciberseguridad

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Global University**
- Acreditación: **90 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: www.techtitute.com/informatica/master/master-inteligencia-artificial-ciberseguridad

Índice

01

Presentación del programa

La Inteligencia Artificial aplicada a la Ciberseguridad es un sector en plena expansión debido al aumento de las amenazas digitales y la necesidad de respuestas proactivas y eficaces. En este ámbito, los sistemas inteligentes no solo permiten automatizar procesos repetitivos, sino también analizar grandes volúmenes de datos para identificar patrones anómalos, anticipar ataques y fortalecer sistemas de protección. Por esta razón, TECH ha elaborado una exhaustiva titulación universitaria que prepara a los informáticos para enfrentar los desafíos actuales en Ciberseguridad, ofreciéndoles las herramientas necesarias para anticiparse a las amenazas futuras, liderando iniciativas tecnológicas y garantizando la protección de infraestructuras críticas a nivel global. Todo ello, a través de un itinerario académico 100% online impartido por los mejores expertos del sector.

Con este innovador programa universitario 100% online, dominarás las técnicas más avanzadas de Criptografía moderna, y diseñarás sistemas de protección robustos para garantizar la privacidad y autenticidad de los datos"

La Inteligencia Artificial y la Ciberseguridad son dos pilares fundamentales en la era digital. Mientras que la primera se centra en el desarrollo de sistemas capaces de simular procesos cognitivos humanos, la Ciberseguridad se encarga de proteger los sistemas informáticos y los datos de ataques maliciosos. La combinación de ambas disciplinas permite crear soluciones avanzadas que no solo detectan y mitigan amenazas en tiempo real, sino que también anticipan posibles vulnerabilidades, garantizando así un entorno digital más seguro. Este contexto impulsa la necesidad de profesionales altamente cualificados que dominen tanto los fundamentos de la Inteligencia Artificial como sus aplicaciones específicas en la defensa cibernética.

A partir de estas demandas surge el Máster Título Propio en Inteligencia Artificial en Ciberseguridad de TECH, un programa estructurado en 20 exhaustivos módulos que abordan desde los fundamentos de la Inteligencia Artificial y la gestión del dato hasta el aprendizaje profundo, las redes neuronales convolucionales y la aplicación de modelos generativos en Ciberseguridad. Asimismo, profundiza en la detección de amenazas, el análisis forense digital y la criptografía moderna, utilizando herramientas como TensorFlow y modelos avanzados de Inteligencia Artificial para responder a los desafíos de un entorno digital en constante evolución. Así pues, este recorrido académico permite a los informáticos anticiparse a las amenazas emergentes y liderar estrategias de seguridad en entornos complejos.

En lo que respecta a la metodología de esta titulación universitaria, TECH ofrece un entorno 100% online que permite a los profesionales planificar de forma individual sus horarios y ritmo de estudio. Además, emplea su disruptivo sistema del *Relearning*, que facilita la asimilación progresiva de conceptos clave mediante la reiteración contextualizada y el aprendizaje activo. En esta misma línea, los egresados únicamente necesitarán contar con un dispositivo electrónico con conexión a internet para adentrarse en el Campus Virtual. Allí podrán acceder a una vasta biblioteca de recursos multimedia, como resúmenes interactivos, vídeos explicativos o lecturas especializadas basadas en la última evidencia.

Este **Máster Título Propio en Inteligencia Artificial en Ciberseguridad** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Inteligencia Artificial, Ciberseguridad y tecnologías avanzadas
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que está concebido recogen una información científica y práctica sobre aquellas disciplinas indispensables para el ejercicio profesional
- Los ejercicios prácticos donde realizar el proceso de autoevaluación para mejorar el aprendizaje
- Su especial hincapié en metodologías innovadoras
- Las lecciones teóricas, preguntas al experto, foros de discusión de temas controvertidos y trabajos de reflexión individual
- La disponibilidad de acceso a los contenidos desde cualquier dispositivo fijo o portátil con conexión a internet

Profundizarás en cómo la Inteligencia Artificial transforma la Ciberseguridad con herramientas como Redes Neuronales y modelos generativos aplicados a la detección y prevención de amenazas”

Optimizarás tu toma de decisiones estratégicas mediante el análisis predictivo y el uso de modelos avanzados en la gestión de ataques cibernéticos”

Dispondrás de los recursos multimedia más vanguardistas, desde resúmenes interactivos hasta vídeos explicativos y lecturas especializadas.

Liderarás proyectos en sectores clave, como la protección de infraestructuras y la gestión de sistemas conectados del Internet de las Cosas.

El programa incluye en su cuadro docente a profesionales del sector que vierten en esta capacitación la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

Su contenido multimedia, elaborado con la última tecnología educativa, permitirá al profesional un aprendizaje situado y contextual, es decir, un entorno simulado que proporcionará una capacitación inmersiva programada para entrenarse ante situaciones reales.

El diseño de este programa se centra en el Aprendizaje Basado en Problemas, mediante el cual el profesional deberá tratar de resolver las distintas situaciones de práctica profesional que se le planteen a lo largo del curso académico. Para ello, contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos.

02

Plan de estudios

El temario de este Máster Título Propio aborda tanto los fundamentos de la Inteligencia Artificial como sus aplicaciones específicas en el campo de la Ciberseguridad. A lo largo de este recorrido académico los informáticos profundizarán en temas clave como la algoritmia, la minería de datos y el procesamiento del lenguaje natural. También ahondarán en las redes neuronales avanzadas y sistemas inteligentes aplicados al análisis forense, así como la detección de intrusiones y defensa proactiva, lo que les permitirá adquirir las herramientas necesarias para desarrollar soluciones innovadoras frente a amenazas digitales.

Con la metodología Relearning, de la cual TECH es pionera, te especializarás en el uso de Sistemas Bioinspirados y Aprendizaje Profundo para abordar problemas complejos en la protección digital"

Módulo 1. Fundamentos de la Inteligencia Artificial

1.1. Historia de la Inteligencia Artificial
- 1.1.1. ¿Cuándo se empieza a hablar de Inteligencia Artificial?
- 1.1.2. Referentes en el cine
- 1.1.3. Importancia de la Inteligencia Artificial
- 1.1.4. Tecnologías que habilitan y dan soporte a la Inteligencia Artificial

1.2. La Inteligencia Artificial en juegos
- 1.2.1. Teoría de Juegos
- 1.2.2. *Minimax* y poda Alfa-Beta
- 1.2.3. Simulación: Monte Carlo

1.3. Redes de neuronas
- 1.3.1. Fundamentos biológicos
- 1.3.2. Modelo computacional
- 1.3.3. Redes de neuronas supervisadas y no supervisadas
- 1.3.4. Perceptrón simple
- 1.3.5. Perceptrón multicapa

1.4. Algoritmos genéticos
- 1.4.1. Historia
- 1.4.2. Base biológica
- 1.4.3. Codificación de problemas
- 1.4.4. Generación de la población inicial
- 1.4.5. Algoritmo principal y operadores genéticos
- 1.4.6. Evaluación de individuos: Fitness

1.5. Tesauros, vocabularios, taxonomías
- 1.5.1. Vocabularios
- 1.5.2. Taxonomías
- 1.5.3. Tesauros
- 1.5.4. Ontologías
- 1.5.5. Representación del conocimiento: web semántica

1.6. Web semántica
- 1.6.1. Especificaciones: RDF, RDFS y OWL
- 1.6.2. Inferencia/razonamiento
- 1.6.3. *Linked Data*

1.7. Sistemas expertos y DSS
- 1.7.1. Sistemas expertos
- 1.7.2. Sistemas de soporte a la decisión

1.8. *Chatbots* y Asistentes Virtuales
- 1.8.1. Tipos de asistentes: asistentes por voz y por texto
- 1.8.2. Partes fundamentales para el desarrollo de un asistente: *Intents*, entidades y flujo de diálogo
- 1.8.3. Integraciones: web, *Slack*, Whatsapp, Facebook
- 1.8.4. Herramientas de desarrollo de asistentes: *Dialog Flow, Watson Assistant*

1.9. Estrategia de implantación de IA

1.10. Futuro de la Inteligencia Artificial
- 1.10.1. Entendemos cómo detectar emociones mediante algoritmos
- 1.10.2. Creación de una personalidad: lenguaje, expresiones y contenido
- 1.10.3. Tendencias de la Inteligencia Artificial
- 1.10.4. Reflexiones

Módulo 2. Tipos y ciclo de vida del dato

2.1. La Estadística
- 2.1.1. Estadística: estadística descriptiva, estadística inferencias
- 2.1.2. Población, muestra, individuo
- 2.1.3. Variables: definición, escalas de medida

2.2. Tipos de datos estadísticos
- 2.2.1. Según tipo
  - 2.2.1.1. Cuantitativos: datos continuos y datos discretos
  - 2.2.1.2. Cualitativos: datos binomiales, datos nominales y datos ordinales
- 2.2.2. Según su forma
  - 2.2.2.1. Numérico
  - 2.2.2.2. Texto
  - 2.2.2.3. Lógico
- 2.2.3. Según su fuente
  - 2.2.3.1. Primarios
  - 2.2.3.2. Secundarios

2.3. Ciclo de vida de los datos
- 2.3.1. Etapas del ciclo
- 2.3.2. Hitos del ciclo
- 2.3.3. Principios FAIR

2.4. Etapas iniciales del ciclo
- 2.4.1. Definición de metas
- 2.4.2. Determinación de recursos necesarios
- 2.4.3. Diagrama de Gantt
- 2.4.4. Estructura de los datos

2.5. Recolección de datos
- 2.5.1. Metodología de recolección
- 2.5.2. Herramientas de recolección
- 2.5.3. Canales de recolección

2.6. Limpieza del dato
- 2.6.1. Fases de la limpieza de datos
- 2.6.2. Calidad del dato
- 2.6.3. Manipulación de datos (con R)

2.7. Análisis de datos, interpretación y valoración de resultados
- 2.7.1. Medidas estadísticas
- 2.7.2. Índices de relación
- 2.7.3. Minería de datos

2.8. Almacén del dato (*Datawarehouse*)
- 2.8.1. Elementos que lo integran
- 2.8.2. Diseño
- 2.8.3. Aspectos a considerar

2.9. Disponibilidad del dato
- 2.9.1. Acceso
- 2.9.2. Utilidad
- 2.9.3. Seguridad

2.10. Aspectos Normativos
- 2.10.1. Ley de protección de datos
- 2.10.2. Buenas prácticas
- 2.10.3. Otros aspectos normativos

Módulo 3. El dato en la Inteligencia Artificial

3.1. Ciencia de datos
- 3.1.1. La ciencia de datos
- 3.1.2. Herramientas avanzadas para el científico de datos

3.2. Datos, información y conocimiento
- 3.2.1. Datos, información y conocimiento
- 3.2.2. Tipos de datos
- 3.2.3. Fuentes de datos

3.3. De los datos a la información
- 3.3.1. Análisis de Datos
- 3.3.2. Tipos de análisis
- 3.3.3. Extracción de Información de un *Dataset*

3.4. Extracción de información mediante visualización
- 3.4.1. La visualización como herramienta de análisis
- 3.4.2. Métodos de visualización
- 3.4.3. Visualización de un conjunto de datos

3.5. Calidad de los datos
- 3.5.1. Datos de calidad
- 3.5.2. Limpieza de datos
- 3.5.3. Preprocesamiento básico de datos

3.6. *Dataset*
- 3.6.1. Enriquecimiento del *Dataset*
- 3.6.2. La maldición de la dimensionalidad
- 3.6.3. Modificación de nuestro conjunto de datos

3.7. Desbalanceo
- 3.7.1. Desbalanceo de clases
- 3.7.2. Técnicas de mitigación del desbalanceo
- 3.7.3. Balanceo de un *Dataset*

3.8. Modelos no supervisados
- 3.8.1. Modelo no supervisado
- 3.8.2. Métodos
- 3.8.3. Clasificación con modelos no supervisados

3.9. Modelos supervisados
- 3.9.1. Modelo supervisado
- 3.9.2. Métodos
- 3.9.3. Clasificación con modelos supervisados

3.10. Herramientas y buenas prácticas
- 3.10.1. Buenas prácticas para un científico de datos
- 3.10.2. El mejor modelo
- 3.10.3. Herramientas útiles

Módulo 4. Minería de Datos. Selección, preprocesamiento y transformación

4.1. La inferencia estadística
- 4.1.1. Estadística descriptiva vs Inferencia estadística
- 4.1.2. Procedimientos paramétricos
- 4.1.3. Procedimientos no paramétricos

4.2. Análisis exploratorio
- 4.2.1. Análisis descriptivo
- 4.2.2. Visualización
- 4.2.3. Preparación de datos

4.3. Preparación de datos
- 4.3.1. Integración y limpieza de datos
- 4.3.2. Normalización de datos
- 4.3.3. Transformando atributos

4.4. Los valores perdidos
- 4.4.1. Tratamiento de valores perdidos
- 4.4.2. Métodos de imputación de máxima verosimilitud
- 4.4.3. Imputación de valores perdidos usando aprendizaje automático

4.5. El ruido en los datos
- 4.5.1. Clases de ruido y atributos
- 4.5.2. Filtrado de ruido
- 4.5.3. El efecto del ruido

4.6. La maldición de la dimensionalidad
- 4.6.1. *Oversampling*
- 4.6.2. *Undersampling*
- 4.6.3. Reducción de datos multidimensionales

4.7. De atributos continuos a discretos
- 4.7.1. Datos continuos versus discretos
- 4.7.2. Proceso de discretización

4.8. Los datos
- 4.8.1. Selección de datos
- 4.8.2. Perspectivas y criterios de selección
- 4.8.3. Métodos de selección

4.9. Selección de instancias
- 4.9.1. Métodos para la selección de instancias
- 4.9.2. Selección de prototipos
- 4.9.3. Métodos avanzados para la selección de instancias

4.10. Preprocesamiento de datos en entornos *Big Data*

Módulo 5. Algoritmia y complejidad en Inteligencia Artificial

5.1. Introducción a las estrategias de diseño de algoritmos
- 5.1.1. Recursividad
- 5.1.2. Divide y conquista
- 5.1.3. Otras estrategias

5.2. Eficiencia y análisis de los algoritmos
- 5.2.1. Medidas de eficiencia
- 5.2.2. Medir el tamaño de la entrada
- 5.2.3. Medir el tiempo de ejecución
- 5.2.4. Caso peor, mejor y medio
- 5.2.5. Notación asintónica
- 5.2.6. Criterios de Análisis matemático de algoritmos no recursivos
- 5.2.7. Análisis matemático de algoritmos recursivos
- 5.2.8. Análisis empírico de algoritmos

5.3. Algoritmos de ordenación
- 5.3.1. Concepto de ordenación
- 5.3.2. Ordenación de la burbuja
- 5.3.3. Ordenación por selección
- 5.3.4. Ordenación por inserción
- 5.3.5. Ordenación por mezcla (*Merge_Sort*)
- 5.3.6. Ordenación rápida (*Quick_Sort*)

5.4. Algoritmos con árboles
- 5.4.1. Concepto de árbol
- 5.4.2. Árboles binarios
- 5.4.3. Recorridos de árbol
- 5.4.4. Representar expresiones
- 5.4.5. Árboles binarios ordenados
- 5.4.6. Árboles binarios balanceados

5.5. Algoritmos con *Heaps*
- 5.5.1. Los *Heaps*
- 5.5.2. El algoritmo *Heapsort*
- 5.5.3. Las colas de prioridad

5.6. Algoritmos con grafos
- 5.6.1. Representación
- 5.6.2. Recorrido en anchura
- 5.6.3. Recorrido en profundidad
- 5.6.4. Ordenación topológica

5.7. Algoritmos *Greedy*
- 5.7.1. La estrategia *Greedy*
- 5.7.2. Elementos de la estrategia *Greedy*
- 5.7.3. Cambio de monedas
- 5.7.4. Problema del viajante
- 5.7.5. Problema de la mochila

5.8. Búsqueda de caminos mínimos
- 5.8.1. El problema del camino mínimo
- 5.8.2. Arcos negativos y ciclos
- 5.8.3. Algoritmo de Dijkstra

5.9. Algoritmos *Greedy* sobre grafos
- 5.9.1. El árbol de recubrimiento mínimo
- 5.9.2. El algoritmo de Prim
- 5.9.3. El algoritmo de Kruskal
- 5.9.4. Análisis de complejidad

5.10. *Backtracking*
- 5.10.1. El *Backtracking*
- 5.10.2. Técnicas alternativas

Módulo 6. Sistemas inteligentes

6.1. Teoría de agentes
- 6.1.1. Historia del concepto
- 6.1.2. Definición de agente
- 6.1.3. Agentes en Inteligencia Artificial
- 6.1.4. Agentes en ingeniería de Software

6.2. Arquitecturas de agentes
- 6.2.1. El proceso de razonamiento de un agente
- 6.2.2. Agentes reactivos
- 6.2.3. Agentes deductivos
- 6.2.4. Agentes híbridos
- 6.2.5. Comparativa

6.3. Información y conocimiento
- 6.3.1. Distinción entre datos, información y conocimiento
- 6.3.2. Evaluación de la calidad de los datos
- 6.3.3. Métodos de captura de datos
- 6.3.4. Métodos de adquisición de información
- 6.3.5. Métodos de adquisición de conocimiento

6.4. Representación del conocimiento
- 6.4.1. La importancia de la representación del conocimiento
- 6.4.2. Definición de representación del conocimiento a través de sus roles
- 6.4.3. Características de una representación del conocimiento

6.5. Ontologías
- 6.5.1. Introducción a los metadatos
- 6.5.2. Concepto filosófico de ontología
- 6.5.3. Concepto informático de ontología
- 6.5.4. Ontologías de dominio y ontologías de nivel superior
- 6.5.5. ¿Cómo construir una ontología?

6.6. Lenguajes para ontologías y Software para la creación de ontologías
- 6.6.1. Tripletas RDF, *Turtle* y N
- 6.6.2. RDF *Schema*
- 6.6.3. OWL
- 6.6.4. SPARQL
- 6.6.5. Introducción a las diferentes herramientas para la creación de ontologías
- 6.6.6. Instalación y uso de *Protégé*

6.7. La web semántica
- 6.7.1. El estado actual y futuro de la web semántica
- 6.7.2. Aplicaciones de la web semántica

6.8. Otros modelos de representación del conocimiento
- 6.8.1. Vocabularios
- 6.8.2. Visión global
- 6.8.3. Taxonomías
- 6.8.4. Tesauros
- 6.8.5. Folksonomías
- 6.8.6. Comparativa
- 6.8.7. Mapas mentales

6.9. Evaluación e integración de representaciones del conocimiento
- 6.9.1. Lógica de orden cero
- 6.9.2. Lógica de primer orden
- 6.9.3. Lógica descriptiva
- 6.9.4. Relación entre diferentes tipos de lógica
- 6.9.5. *Prolog*: programación basada en lógica de primer orden

6.10. Razonadores semánticos, sistemas basados en conocimiento y Sistemas Expertos
- 6.10.1. Concepto de razonador
- 6.10.2. Aplicaciones de un razonador
- 6.10.3. Sistemas basados en el conocimiento
- 6.10.4. MYCIN, historia de los Sistemas Expertos
- 6.10.5. Elementos y Arquitectura de Sistemas Expertos
- 6.10.6. Creación de Sistemas Expertos

Módulo 7. Aprendizaje automático y minería de datos

7.1. Introducción a los procesos de descubrimiento del conocimiento y conceptos básicos de aprendizaje automático
- 7.1.1. Conceptos clave de los procesos de descubrimiento del conocimiento
- 7.1.2. Perspectiva histórica de los procesos de descubrimiento del conocimiento
- 7.1.3. Etapas de los procesos de descubrimiento del conocimiento
- 7.1.4. Técnicas utilizadas en los procesos de descubrimiento del conocimiento
- 7.1.5. Características de los buenos modelos de aprendizaje automático
- 7.1.6. Tipos de información de aprendizaje automático
- 7.1.7. Conceptos básicos de aprendizaje
- 7.1.8. Conceptos básicos de aprendizaje no supervisado

7.2. Exploración y preprocesamiento de datos
- 7.2.1. Tratamiento de datos
- 7.2.2. Tratamiento de datos en el flujo de análisis de datos
- 7.2.3. Tipos de datos
- 7.2.4. Transformaciones de datos
- 7.2.5. Visualización y exploración de variables continuas
- 7.2.6. Visualización y exploración de variables categóricas
- 7.2.7. Medidas de correlación
- 7.2.8. Representaciones gráficas más habituales
- 7.2.9. Introducción al análisis multivariante y a la reducción de dimensiones

7.3. Árboles de decisión
- 7.3.1. Algoritmo ID
- 7.3.2. Algoritmo C
- 7.3.3. Sobreentrenamiento y poda
- 7.3.4. Análisis de resultados

7.4. Evaluación de clasificadores
- 7.4.1. Matrices de confusión
- 7.4.2. Matrices de evaluación numérica
- 7.4.3. Estadístico de Kappa
- 7.4.4. La curva ROC

7.5. Reglas de clasificación
- 7.5.1. Medidas de evaluación de reglas
- 7.5.2. Introducción a la representación gráfica
- 7.5.3. Algoritmo de recubrimiento secuencial

7.6. Redes neuronales
- 7.6.1. Conceptos básicos
- 7.6.2. Redes de neuronas simples
- 7.6.3. Algoritmo de *Backpropagation*
- 7.6.4. Introducción a las redes neuronales recurrentes

7.7. Métodos bayesianos
- 7.7.1. Conceptos básicos de probabilidad
- 7.7.2. Teorema de Bayes
- 7.7.3. Naive Bayes
- 7.7.4. Introducción a las redes bayesianas

7.8. Modelos de regresión y de respuesta continua
- 7.8.1. Regresión lineal simple
- 7.8.2. Regresión lineal múltiple
- 7.8.3. Regresión logística
- 7.8.4. Árboles de regresión
- 7.8.5. Introducción a las máquinas de soporte vectorial (SVM)
- 7.8.6. Medidas de bondad de ajuste

7.9. *Clustering*
- 7.9.1. Conceptos básicos
- 7.9.2. *Clustering* jerárquico
- 7.9.3. Métodos probabilistas
- 7.9.4. Algoritmo EM
- 7.9.5. Método *B-Cubed*
- 7.9.6. Métodos implícitos

7.10. Minería de textos y procesamiento de lenguaje natural (NLP)
- 7.10.1. Conceptos básicos
- 7.10.2. Creación del corpus
- 7.10.3. Análisis descriptivo
- 7.10.4. Introducción al análisis de sentimientos

Módulo 8. Las redes neuronales, base de *Deep Learning*

8.1. Aprendizaje Profundo
- 8.1.1. Tipos de aprendizaje profundo
- 8.1.2. Aplicaciones del aprendizaje profundo
- 8.1.3. Ventajas y desventajas del aprendizaje profundo

8.2. Operaciones
- 8.2.1. Suma
- 8.2.2. Producto
- 8.2.3. Traslado

8.3. Capas
- 8.3.1. Capa de entrada
- 8.3.2. Capa oculta
- 8.3.3. Capa de salida

8.4. Unión de Capas y Operaciones
- 8.4.1. Diseño de arquitecturas
- 8.4.2. Conexión entre capas
- 8.4.3. Propagación hacia adelante

8.5. Construcción de la primera red neuronal
- 8.5.1. Diseño de la red
- 8.5.2. Establecer los pesos
- 8.5.3. Entrenamiento de la red

8.6. Entrenador y Optimizador
- 8.6.1. Selección del optimizador
- 8.6.2. Establecimiento de una función de pérdida
- 8.6.3. Establecimiento de una métrica

8.7. Aplicación de los Principios de las Redes Neuronales
- 8.7.1. Funciones de activación
- 8.7.2. Propagación hacia atrás
- 8.7.3. Ajuste de los parámetros

8.8. De las neuronas biológicas a las artificiales
- 8.8.1. Funcionamiento de una neurona biológica
- 8.8.2. Transferencia de conocimiento a las neuronas artificiales
- 8.8.3. Establecer relaciones entre ambas

8.9. Implementación de MLP (Perceptrón multicapa) con Keras
- 8.9.1. Definición de la estructura de la red
- 8.9.2. Compilación del modelo
- 8.9.3. Entrenamiento del modelo

8.10. Hiperparámetros de *Fine tuning* de Redes Neuronales
- 8.10.1. Selección de la función de activación
- 8.10.2. Establecer el *Learning* rate
- 8.10.3. Ajuste de los pesos

Módulo 9. Entrenamiento de redes neuronales profundas

9.1. Problemas de Gradientes
- 9.1.1. Técnicas de optimización de gradiente
- 9.1.2. Gradientes Estocásticos
- 9.1.3. Técnicas de inicialización de pesos

9.2. Reutilización de capas preentrenadas
- 9.2.1. Entrenamiento de transferencia de aprendizaje
- 9.2.2. Extracción de características
- 9.2.3. Aprendizaje profundo

9.3. Optimizadores
- 9.3.1. Optimizadores de descenso de gradiente estocástico
- 9.3.2. Optimizadores Adam y *RMSprop*
- 9.3.3. Optimizadores de momento

9.4. Programación de la tasa de aprendizaje
- 9.4.1. Control de tasa de aprendizaje automático
- 9.4.2. Ciclos de aprendizaje
- 9.4.3. Términos de suavizado

9.5. Sobreajuste
- 9.5.1. Validación cruzada
- 9.5.2. Regularización
- 9.5.3. Métricas de evaluación

9.6. Directrices Prácticas
- 9.6.1. Diseño de modelos
- 9.6.2. Selección de métricas y parámetros de evaluación
- 9.6.3. Pruebas de hipótesis

9.7. *Transfer Learning*
- 9.7.1. Entrenamiento de transferencia de aprendizaje
- 9.7.2. Extracción de características
- 9.7.3. Aprendizaje profundo

9.8. *Data Augmentation*
- 9.8.1. Transformaciones de imagen
- 9.8.2. Generación de datos sintéticos
- 9.8.3. Transformación de texto

9.9. Aplicación Práctica de *Transfer Learning*
- 9.9.1. Entrenamiento de transferencia de aprendizaje
- 9.9.2. Extracción de características
- 9.9.3. Aprendizaje profundo

9.10. Regularización
- 9.10.1. L y L
- 9.10.2. Regularización por máxima entropía
- 9.10.3. *Dropout*

Módulo 10. Personalización de Modelos y entrenamiento con *TensorFlow*

10.1. *TensorFlow*
- 10.1.1. Uso de la biblioteca *TensorFlow*
- 10.1.2. Entrenamiento de modelos con *TensorFlow*
- 10.1.3. Operaciones con gráficos en *TensorFlow*

10.2. *TensorFlow* y NumPy
- 10.2.1. Entorno computacional NumPy para *TensorFlow*
- 10.2.2. Utilización de los arrays NumPy con *TensorFlow*
- 10.2.3. Operaciones NumPy para los gráficos de *TensorFlow*

10.3. Personalización de modelos y algoritmos de entrenamiento
- 10.3.1. Construcción de modelos personalizados con *TensorFlow*
- 10.3.2. Gestión de parámetros de entrenamiento
- 10.3.3. Utilización de técnicas de optimización para el entrenamiento

10.4. Funciones y gráficos de *TensorFlow*
- 10.4.1. Funciones con *TensorFlow*
- 10.4.2. Utilización de gráficos para el entrenamiento de modelos
- 10.4.3. Optimización de gráficos con operaciones de *TensorFlow*

10.5. Carga y preprocesamiento de datos con *TensorFlow*
- 10.5.1. Carga de conjuntos de datos con *TensorFlow*
- 10.5.2. Preprocesamiento de datos con *TensorFlow*
- 10.5.3. Utilización de herramientas de *TensorFlow* para la manipulación de datos

10.6. La API *tfdata*
- 10.6.1. Utilización de la API *tfdata* para el procesamiento de datos
- 10.6.2. Construcción de flujos de datos con *tfdata*
- 10.6.3. Uso de la API *tfdata* para el entrenamiento de modelos

10.7. El formato *TFRecord*
- 10.7.1. Utilización de la API *TFRecord* para la serialización de datos
- 10.7.2. Carga de archivos *TFRecord* con *TensorFlow*
- 10.7.3. Utilización de archivos *TFRecord* para el entrenamiento de modelos

10.8. Capas de preprocesamiento de Keras
- 10.8.1. Utilización de la API de preprocesamiento de Keras
- 10.8.2. Construcción de *pipelined* de preprocesamiento con Keras
- 10.8.3. Uso de la API de preprocesamiento de Keras para el entrenamiento de modelos

10.9. El proyecto *TensorFlow Datasets*
- 10.9.1. Utilización de *TensorFlow Datasets* para la carga de datos
- 10.9.2. Preprocesamiento de datos con *TensorFlow Datasets*
- 10.9.3. Uso de *TensorFlow Datasets* para el entrenamiento de modelos

10.10. Construcción de una Aplicación de Deep *Learning* con *TensorFlow*
- 10.10.1. Aplicación Práctica
- 10.10.2. Construcción de una aplicación de Deep *Learning* con *TensorFlow*
- 10.10.3. Entrenamiento de un modelo con *TensorFlow*
- 10.10.4. Utilización de la aplicación para la predicción de resultados

Módulo 11. *Deep Computer Vision* con redes neuronales convolucionales

11.1. La Arquitectura *Visual Cortex*
- 11.1.1. Funciones de la corteza visual
- 11.1.2. Teorías de la visión computacional
- 11.1.3. Modelos de procesamiento de imágenes

11.2. Capas convolucionales
- 11.2.1. Reutilización de pesos en la convolución
- 11.2.2. Convolución D
- 11.2.3. Funciones de activación

11.3. Capas de agrupación e implementación de capas de agrupación con Keras
- 11.3.1. *Pooling* y *Striding*
- 11.3.2. *Flattening*
- 11.3.3. Tipos de *Pooling*

11.4. Arquitecturas CNN
- 11.4.1. Arquitectura VGG
- 11.4.2. Arquitectura *AlexNet*
- 11.4.3. Arquitectura *ResNet*

11.5. Implementación de una CNN *ResNet*- usando Keras
- 11.5.1. Inicialización de pesos
- 11.5.2. Definición de la capa de entrada
- 11.5.3. Definición de la salida

11.6. Uso de modelos preentrenados de Keras
- 11.6.1. Características de los modelos preentrenados
- 11.6.2. Usos de los modelos preentrenados
- 11.6.3. Ventajas de los modelos preentrenados

11.7. Modelos preentrenados para el aprendizaje por transferencia
- 11.7.1. El Aprendizaje por transferencia
- 11.7.2. Proceso de aprendizaje por transferencia
- 11.7.3. Ventajas del aprendizaje por transferencia

11.8. Clasificación y Localización en *Deep Computer Vision*
- 11.8.1. Clasificación de imágenes
- 11.8.2. Localización de objetos en imágenes
- 11.8.3. Detección de objetos

11.9. Detección de objetos y seguimiento de objetos
- 11.9.1. Métodos de detección de objetos
- 11.9.2. Algoritmos de seguimiento de objetos
- 11.9.3. Técnicas de rastreo y localización

11.10. Segmentación semántica
- 11.10.1. Aprendizaje profundo para segmentación semántica
- 11.10.1. Detección de bordes
- 11.10.1. Métodos de segmentación basados en reglas

Módulo 12. Procesamiento del lenguaje natural (NLP) con Redes Naturales Recurrentes (RNN) y Atención

12.1. Generación de texto utilizando RNN
- 12.1.1. Entrenamiento de una RNN para generación de texto
- 12.1.2. Generación de lenguaje natural con RNN
- 12.1.3. Aplicaciones de generación de texto con RNN

12.2. Creación del conjunto de datos de entrenamiento
- 12.2.1. Preparación de los datos para el entrenamiento de una RNN
- 12.2.2. Almacenamiento del conjunto de datos de entrenamiento
- 12.2.3. Limpieza y transformación de los datos
- 12.2.4. Análisis de Sentimiento

12.3. Clasificación de opiniones con RNN
- 12.3.1. Detección de temas en los comentarios
- 12.3.2. Análisis de sentimiento con algoritmos de aprendizaje profundo

12.4. Red de codificador-decodificador para la traducción automática neuronal
- 12.4.1. Entrenamiento de una RNN para la traducción automática
- 12.4.2. Uso de una red *encoder-decoder* para la traducción automática
- 12.4.3. Mejora de la precisión de la traducción automática con RNN

12.5. Mecanismos de atención
- 12.5.1. Aplicación de mecanismos de atención en RNN
- 12.5.2. Uso de mecanismos de atención para mejorar la precisión de los modelos
- 12.5.3. Ventajas de los mecanismos de atención en las redes neuronales

12.6. Modelos *Transformers*
- 12.6.1. Uso de los modelos *Transformers* para procesamiento de lenguaje natural
- 12.6.2. Aplicación de los modelos *Transformers* para visión
- 12.6.3. Ventajas de los modelos *Transformers*

12.7. *Transformers* para visión
- 12.7.1. Uso de los modelos *Transformers* para visión
- 12.7.2. Preprocesamiento de los datos de imagen
- 12.7.3. Entrenamiento de un modelo *Transformers* para visión

12.8. Librería de *Transformers* de *Hugging Face*
- 12.8.1. Uso de la librería de *Transformers* de *Hugging Face*
- 12.8.2. Aplicación de la librería de *Transformers* de *Hugging Face*
- 12.8.3. Ventajas de la librería de *Transformers* de *Hugging Face*

12.9. Otras Librerías de *Transformers*. Comparativa
- 12.9.1. Comparación entre las distintas librerías de *Transformers*
- 12.9.2. Uso de las demás librerías de *Transformers*
- 12.9.3. Ventajas de las demás librerías de *Transformers*

12.10. Desarrollo de una Aplicación de NLP con RNN y Atención. Aplicación Práctica
- 12.10.1. Desarrollo de una aplicación de procesamiento de lenguaje natural con RNN y atención
- 12.10.2. Uso de RNN, mecanismos de atención y modelos *Transformers* en la aplicación
- 12.10.3. Evaluación de la aplicación práctica

Módulo 13. *Autoencoders, GANs,* y modelos de difusión

13.1. Representaciones de datos eficientes
- 13.1.1. Reducción de dimensionalidad
- 13.1.2. Aprendizaje profundo
- 13.1.3. Representaciones compactas

13.2. Realización de PCA con un codificador automático lineal incompleto
- 13.2.1. Proceso de entrenamiento
- 13.2.2. Implementación en Python
- 13.2.3. Utilización de datos de prueba

13.3. Codificadores automáticos apilados
- 13.3.1. Redes neuronales profundas
- 13.3.2. Construcción de arquitecturas de codificación
- 13.3.3. Uso de la regularización

13.4. Autocodificadores convolucionales
- 13.4.1. Diseño de modelos convolucionales
- 13.4.2. Entrenamiento de modelos convolucionales
- 13.4.3. Evaluación de los resultados

13.5. Eliminación de ruido de codificadores automáticos
- 13.5.1. Aplicación de filtros
- 13.5.2. Diseño de modelos de codificación
- 13.5.3. Uso de técnicas de regularización

13.6. Codificadores automáticos dispersos
- 13.6.1. Incrementar la eficiencia de la codificación
- 13.6.2. Minimizando el número de parámetros
- 13.6.3. Utilización de técnicas de regularización

13.7. Codificadores automáticos variacionales
- 13.7.1. Utilización de optimización variacional
- 13.7.2. Aprendizaje profundo no supervisado
- 13.7.3. Representaciones latentes profundas

13.8. Generación de imágenes MNIST de moda
- 13.8.1. Reconocimiento de patrones
- 13.8.2. Generación de imágenes
- 13.8.3. Entrenamiento de redes neuronales profundas

13.9. Redes adversarias generativas y modelos de difusión
- 13.9.1. Generación de contenido a partir de imágenes
- 13.9.2. Modelado de distribuciones de datos
- 13.9.3. Uso de redes adversarias

13.10. Implementación de los Modelos
- 13.10.1. Aplicación Práctica
- 13.10.2. Implementación de los modelos
- 13.10.3. Uso de datos reales
- 13.10.4. Evaluación de los resultados

Módulo 14. Computación bioinspirada

14.1. Introducción a la computación bioinspirada
- 14.1.1. Introducción a la computación bioinspirada

14.2. Algoritmos de adaptación social
- 14.2.1. Computación bioinspirada basada en colonia de hormigas
- 14.2.2. Variantes de los algoritmos de colonias de hormigas
- 14.2.3. Computación basada en nubes de partículas

14.3. Algoritmos genéticos
- 14.3.1. Estructura general
- 14.3.2. Implementaciones de los principales operadores

14.4. Estrategias de exploración-explotación del espacio para algoritmos genéticos
- 14.4.1. Algoritmo CHC
- 14.4.2. Problemas multimodales

14.5. Modelos de computación evolutiva (I)
- 14.5.1. Estrategias evolutivas
- 14.5.2. Programación evolutiva
- 14.5.3. Algoritmos basados en evolución diferencial

14.6. Modelos de computación evolutiva (II)
- 14.6.1. Modelos de evolución basados en estimación de distribuciones (EDA)
- 14.6.2. Programación genética

14.7. Programación evolutiva aplicada a problemas de aprendizaje
- 14.7.1. Aprendizaje basado en reglas
- 14.7.2. Métodos evolutivos en problemas de selección de instancias

14.8. Problemas multiobjetivo
- 14.8.1. Concepto de dominancia
- 14.8.2. Aplicación de algoritmos evolutivos a problemas multiobjetivo

14.9. Redes neuronales (I)
- 14.9.1. Introducción a las redes neuronales
- 14.9.2. Ejemplo práctico con redes neuronales

14.10. Redes neuronales (II)
- 14.10.1. Casos de uso de las redes neuronales en la investigación médica
- 14.10.2. Casos de uso de las redes neuronales en la economía
- 14.10.3. Casos de uso de las redes neuronales en la visión artificial

Módulo 15. Inteligencia Artificial: estrategias y aplicaciones

15.1. Servicios financieros
- 15.1.1. Las implicaciones de la Inteligencia Artificial en los servicios financieros. Oportunidades y desafíos
- 15.1.2. Casos de uso
- 15.1.3. Riesgos potenciales relacionados con el uso de Inteligencia Artificial
- 15.1.4. Potenciales desarrollos / usos futuros de la Inteligencia Artificial

15.2. Implicaciones de la Inteligencia Artificial en el servicio sanitario
- 15.2.1. Implicaciones de la Inteligencia Artificial en el sector sanitario. Oportunidades y desafíos
- 15.2.2. Casos de uso

15.3. Riesgos Relacionados con el uso de la Inteligencia Artificial en el servicio sanitario
- 15.3.1. Riesgos potenciales relacionados con el uso de Inteligencia Artificial
- 15.3.2. Potenciales desarrollos / usos futuros de la Inteligencia Artificial

15.4. *Retail*
- 15.4.1. Implicaciones de la Inteligencia Artificial en *Retail*. Oportunidades y desafíos
- 15.4.2. Casos de uso
- 15.4.3. Riesgos potenciales relacionados con el uso de Inteligencia Artificial
- 15.4.4. Potenciales desarrollos / usos futuros de la Inteligencia Artificial

15.5. Industria
- 15.5.1. Implicaciones de la Inteligencia Artificial en la Industria. Oportunidades y desafíos
- 15.5.2. Casos de uso

15.6. Riesgos potenciales relacionados con el uso de Inteligencia Artificial en la Industria
- 15.6.1. Casos de uso
- 15.6.2. Riesgos potenciales relacionados con el uso de Inteligencia Artificial
- 15.6.3. Potenciales desarrollos / usos futuros de la Inteligencia Artificial

15.7. Administración Pública
- 15.7.1. Implicaciones de la Inteligencia Artificial en la Administración Pública. Oportunidades y desafíos
- 15.7.2. Casos de uso
- 15.7.3. Riesgos potenciales relacionados con el uso de Inteligencia Artificial
- 15.7.4. Potenciales desarrollos / usos futuros de la Inteligencia Artificial

15.8. Educación
- 15.8.1. Implicaciones de la Inteligencia Artificial en la educación. Oportunidades y desafíos
- 15.8.2. Casos de uso
- 15.8.3. Riesgos potenciales relacionados con el uso de Inteligencia Artificial
- 15.8.4. Potenciales desarrollos / usos futuros de la Inteligencia Artificial

15.9. Silvicultura y agricultura
- 15.9.1. Implicaciones de la Inteligencia Artificial en la silvicultura y la agricultura. Oportunidades y desafíos
- 15.9.2. Casos de uso
- 15.9.3. Riesgos potenciales relacionados con el uso de Inteligencia Artificial
- 15.9.4. Potenciales desarrollos / usos futuros de la Inteligencia Artificial

15.10. Recursos Humanos
- 15.10.1. Implicaciones de la Inteligencia Artificial en los Recursos Humanos. Oportunidades y desafíos
- 15.10.2. Casos de uso
- 15.10.3. Riesgos potenciales relacionados con el uso de Inteligencia Artificial
- 15.10.4. Potenciales desarrollos / usos futuros de la Inteligencia Artificial

Módulo 16. Ciberseguridad y análisis de amenazas modernas con ChatGPT

16.1. Introducción a la Ciberseguridad: amenazas actuales y el rol de la Inteligencia Artificial
- 16.1.1. Definición y conceptos básicos de Ciberseguridad
- 16.1.2. Tipos de amenazas cibernéticas modernas
- 16.1.3. Papel de la Inteligencia Artificial en la evolución de la Ciberseguridad

16.2. Confidencialidad, integridad y disponibilidad (CIA) en la era de la Inteligencia Artificial
- 16.2.1. Fundamentos del modelo CIA en Ciberseguridad
- 16.2.2. Principios de seguridad aplicados en el contexto de Inteligencia Artificial
- 16.2.3. Retos y consideraciones del CIA en sistemas impulsados por Inteligencia Artificial

16.3. Uso de ChatGPT para análisis de riesgos y escenarios de amenaza
- 16.3.1. Fundamentos de análisis de riesgos en Ciberseguridad
- 16.3.2. Capacidad de ChatGPT para identificar y evaluar escenarios de amenaza
- 16.3.3. Beneficios y limitaciones del análisis de riesgos con Inteligencia Artificial

16.4. ChatGPT en la detección de vulnerabilidades críticas
- 16.4.1. Principios de detección de vulnerabilidades en sistemas de información
- 16.4.2. Funcionalidades de ChatGPT para apoyar en la detección de vulnerabilidades
- 16.4.3. Consideraciones éticas y de seguridad al usar Inteligencia Artificial en detección de fallos

16.5. Análisis de *malware* y *ransomware* asistido por Inteligencia Artificial
- 16.5.1. Principios básicos del análisis de *malware* y *ransomware*
- 16.5.2. Técnicas de Inteligencia Artificial aplicadas en la identificación de código malicioso
- 16.5.3. Desafíos técnicos y operacionales en el análisis de *malware* asistido por Inteligencia Artificial

16.6. Identificación de ataques comunes con Inteligencia Artificial: *phishing*, ingeniería social y explotación
- 16.6.1. Clasificación de ataques: phishing, ingeniería social y explotación
- 16.6.2. Técnicas de Inteligencia Artificial para la identificación y análisis de ataques comunes
- 16.6.3. Dificultades y limitaciones de los modelos de Inteligencia Artificial en detección de ataques

16.7. ChatGPT en la capacitación y simulación de amenazas cibernéticas
- 16.7.1. Fundamentos de la simulación de amenazas para formación en Ciberseguridad
- 16.7.2. Capacidades de ChatGPT para diseñar escenarios de simulación
- 16.7.3. Beneficios de la simulación de amenazas como herramienta de capacitación

16.8. Políticas de seguridad cibernética con recomendaciones de Inteligencia Artificial
- 16.8.1. Principios para la formulación de políticas de seguridad cibernética
- 16.8.2. Rol de la Inteligencia Artificial en la generación de recomendaciones de seguridad
- 16.8.3. Componentes clave en políticas de seguridad orientadas a Inteligencia Artificial

16.9. Seguridad en dispositivos IoT y el papel de la Inteligencia Artificial
- 16.9.1. Fundamentos de la seguridad en el Internet de las Cosas (IoT)
- 16.9.2. Capacidades de la Inteligencia Artificial para mitigar vulnerabilidades en dispositivos IoT
- 16.9.3. Desafíos y consideraciones específicas de Inteligencia Artificial para la seguridad de IoT

16.10. Evaluación de amenazas y respuestas asistidas por herramientas de Inteligencia Artificial
- 16.10.1. Principios de evaluación de amenazas en Ciberseguridad
- 16.10.2. Características de las respuestas automatizadas mediante Inteligencia Artificial
- 16.10.3. Factores críticos en la efectividad de respuestas cibernéticas con Inteligencia Artificial

Módulo 17. Detección y prevención de intrusiones usando modelos de Inteligencia Artificial Generativa

17.1. Fundamentos de sistemas IDS/IPS y el papel de la Inteligencia Artificial
- 17.1.1. Definición y principios básicos de los sistemas IDS e IPS
- 17.1.2. Principales tipos y configuraciones de IDS/IPS
- 17.1.3. Contribución de la Inteligencia Artificial en la evolución de los sistemas de detección y prevención

17.2. Uso de Gemini para detección de anomalías en redes
- 17.2.1. Conceptos y tipos de anomalías en el tráfico de red
- 17.2.2. Características de Gemini para el análisis de datos de red
- 17.2.3. Beneficios de la detección de anomalías en la prevención de intrusiones

17.3. Gemini y la identificación de patrones de intrusión
- 17.3.1. Principios de identificación y clasificación de patrones de intrusión
- 17.3.2. Técnicas de Inteligencia Artificial aplicadas en la detección de patrones de amenazas
- 17.3.3. Tipos de patrones y comportamiento anómalo en seguridad de redes

17.4. Aplicación de modelos generativos en la simulación de ataques
- 17.4.1. Fundamentos de los modelos generativos en Inteligencia Artificial
- 17.4.2. Uso de modelos generativos para recrear escenarios de ataque
- 17.4.3. Ventajas y limitaciones en la simulación de ataques mediante Inteligencia Artificial generativa

17.5. *Clustering* y clasificación de eventos usando Inteligencia Artificial
- 17.5.1. Fundamentos del *clustering* y clasificación en la detección de intrusiones
- 17.5.2. Algoritmos comunes de *clustering* aplicados en Ciberseguridad
- 17.5.3. Papel de la Inteligencia Artificial en la mejora de los métodos de clasificación de eventos

17.6. Gemini en la generación de perfiles de comportamiento
- 17.6.1. Conceptos de perfilamiento de usuarios y dispositivos
- 17.6.2. Aplicación de modelos generativos en la creación de perfiles
- 17.6.3. Ventajas de los perfiles de comportamiento en la detección de amenazas

17.7. Análisis de *Big Data* para la prevención de intrusiones
- 17.7.1. Importancia del *Big Data* en la detección de patrones de seguridad
- 17.7.2. Métodos de procesamiento de grandes volúmenes de datos en Ciberseguridad
- 17.7.3. Aplicaciones de Inteligencia Artificial en el análisis y prevención basados en *Big Data*

17.8. Reducción de datos y selección de características relevantes con Inteligencia Artificial
- 17.8.1. Principios de reducción de dimensionalidad en grandes volúmenes de datos
- 17.8.2. Selección de características para mejorar la eficiencia de análisis de Inteligencia Artificial
- 17.8.3. Técnicas de reducción de datos aplicadas en Ciberseguridad

17.9. Evaluación de modelos de Inteligencia Artificial en detección de intrusos
- 17.9.1. Criterios de evaluación de modelos de Inteligencia Artificial en Ciberseguridad
- 17.9.2. Indicadores de rendimiento y precisión de los modelos
- 17.9.3. Importancia de la validación y evaluación constante en la Inteligencia Artificial

17.10. Implementación de un sistema de detección de intrusos potenciado con Inteligencia Artificial generativa
- 17.10.1. Conceptos básicos de implementación de sistemas de detección de intrusos
- 17.10.2. Integración de Inteligencia Artificial generativa en los sistemas IDS/IPS
- 17.10.3. Aspectos clave para la configuración y mantenimiento de sistemas basados en Inteligencia Artificial

Módulo 18. Criptografía moderna con asistencia de ChatGPT en la protección de datos

18.1. Principios básicos de criptografía con aplicaciones de Inteligencia Artificial
- 18.1.1. Conceptos fundamentales de criptografía: confidencialidad y autenticidad
- 18.1.2. Principales algoritmos criptográficos y su relevancia actual
- 18.1.3. Papel de la Inteligencia Artificial en la modernización de la criptografía

18.2. ChatGPT en la enseñanza y práctica de criptografía simétrica y asimétrica
- 18.2.1. Introducción a la criptografía simétrica y asimétrica
- 18.2.2. Comparación entre cifrado simétrico y asimétrico
- 18.2.3. Uso de ChatGPT en el aprendizaje de métodos criptográficos

18.3. Encriptación avanzada (AES, RSA) y recomendaciones generadas por Inteligencia Artificial
- 18.3.1. Fundamentos de los algoritmos AES y RSA en la encriptación de datos
- 18.3.2. Fortalezas y debilidades de estos algoritmos en el contexto actual
- 18.3.3. Generación de recomendaciones de seguridad en criptografía avanzada con Inteligencia Artificial

18.4. Inteligencia Artificial en la gestión y autenticación de claves
- 18.4.1. Principios de gestión de claves criptográficas
- 18.4.2. Importancia de la autenticación segura de claves
- 18.4.3. Aplicación de Inteligencia Artificial para optimizar procesos de gestión y autenticación

18.5. Algoritmos de *hashing* y ChatGPT en la evaluación de integridad
- 18.5.1. Conceptos básicos y aplicaciones de los algoritmos de *hashing*
- 18.5.2. Funciones de hash en la verificación de integridad de datos
- 18.5.3. Análisis y verificación de integridad de datos con ayuda de ChatGPT

18.6. ChatGPT en la detección de patrones de cifrado anómalos
- 18.6.1. Introducción a la detección de patrones anómalos en criptografía
- 18.6.2. Capacidad de ChatGPT para identificar irregularidades en datos cifrados
- 18.6.3. Limitaciones de los modelos de lenguaje en la detección de cifrado anómalo

18.7. Introducción a la criptografía postcuántica con simulaciones de Inteligencia Artificial
- 18.7.1. Fundamentos de la criptografía postcuántica y su importancia
- 18.7.2. Principales algoritmos postcuánticos en investigación
- 18.7.3. Uso de Inteligencia Artificial en simulaciones para el estudio de criptografía postcuántica

18.8. *Blockchain* y ChatGPT en la verificación de transacciones seguras
- 18.8.1. Conceptos básicos de *blockchain* y su estructura de seguridad
- 18.8.2. Rol de la criptografía en la integridad de *blockchain*
- 18.8.3. Aplicación de ChatGPT para explicar y analizar transacciones seguras

18.9. Protección de privacidad y aprendizaje federado
- 18.9.1. Definición y principios del aprendizaje federado
- 18.9.2. Importancia de la privacidad en el aprendizaje descentralizado
- 18.9.3. Beneficios y desafíos del aprendizaje federado para la seguridad de datos

18.10. Desarrollo de un sistema de encriptación basado en Inteligencia Artificial generativa
- 18.10.1. Principios básicos en la creación de sistemas de encriptación
- 18.10.2. Ventajas de la Inteligencia Artificial generativa en el diseño de sistemas de cifrado
- 18.10.3. Componentes y requisitos de un sistema de encriptación asistido por Inteligencia Artificial

Módulo 19. Análisis forense digital y respuesta a incidentes asistida por Inteligencia Artificial

19.1. Procesos forenses con ChatGPT para la identificación de evidencias
- 19.1.1. Conceptos básicos de análisis forense en entornos digitales
- 19.1.2. Etapas de identificación y recopilación de evidencias
- 19.1.3. Rol de ChatGPT en el apoyo a la identificación forense

19.2. Gemini y ChatGPT en la identificación y extracción de datos
- 19.2.1. Fundamentos de extracción de datos para análisis forense
- 19.2.2. Técnicas de identificación de datos relevantes
- 19.2.3. Contribución de la Inteligencia Artificial en la automatización del proceso de extracción

19.3. Análisis de *logs* y correlación de eventos con Inteligencia Artificial
- 19.3.1. Importancia de los *logs* en el análisis de incidentes
- 19.3.2. Técnicas de correlación de eventos para reconstruir incidentes
- 19.3.3. Uso de Inteligencia Artificial para identificar patrones en la correlación de logs

19.4. Recuperación de datos y restauración de sistemas usando Inteligencia Artificial
- 19.4.1. Principios de recuperación de datos y su importancia en forense digital
- 19.4.2. Técnicas de restauración de sistemas comprometidos
- 19.4.3. Aplicación de Inteligencia Artificial para mejorar los procesos de recuperación y restauración

19.5. *Machine Learning* para detección y reconstrucción de incidentes
- 19.5.1. Introducción a *Machine Learning* en la detección de incidentes
- 19.5.2. Técnicas de reconstrucción de incidentes con modelos de Inteligencia Artificial
- 19.5.3. Consideraciones éticas y prácticas en la detección de eventos

19.6. Reconstrucción de incidentes y simulación con ChatGPT
- 19.6.1. Fundamentos de la reconstrucción de incidentes en análisis forense
- 19.6.2. Capacidad de ChatGPT para crear simulaciones de incidentes
- 19.6.3. Limitaciones y desafíos en la simulación de incidentes complejos

19.7. Detección de actividades maliciosas en dispositivos móviles
- 19.7.1. Características y desafíos en el análisis forense de dispositivos móviles
- 19.7.2. Principales actividades maliciosas en entornos móviles
- 19.7.3. Aplicación de Inteligencia Artificial para identificar amenazas en dispositivos móviles

19.8. Respuesta automatizada a incidentes con flujos de trabajo Inteligencia Artificial
- 19.8.1. Principios de respuesta a incidentes en Ciberseguridad
- 19.8.2. Importancia de la automatización en la respuesta rápida a incidentes
- 19.8.3. Beneficios de los flujos de trabajo asistidos por Inteligencia Artificial en la mitigación

19.9. Ética y transparencia en el análisis forense con Inteligencia Artificial generativa
- 19.9.1. Principios éticos en el uso de Inteligencia Artificial en análisis forense
- 19.9.2. Transparencia y explicabilidad de modelos generativos en forense
- 19.9.3. Consideraciones sobre privacidad y responsabilidad en el análisis

19.10. Laboratorio de análisis forense y recreación de incidentes con ChatGPT y Gemini
- 19.10.1. Estructura y objetivos de un laboratorio de análisis forense
- 19.10.2. Beneficios de los entornos controlados para la práctica forense
- 19.10.3. Componentes clave para la creación de un laboratorio de simulación

Módulo 20. Modelos predictivos de defensa proactiva en Ciberseguridad usando ChatGPT

20.1. Análisis predictivo en Ciberseguridad: técnicas y aplicaciones con Inteligencia Artificial
- 20.1.1. Conceptos básicos de análisis predictivo en seguridad
- 20.1.2. Técnicas de predicción en el ámbito de Ciberseguridad
- 20.1.3. Aplicación de Inteligencia Artificial en la anticipación de ciberamenazas

20.2. Modelos de regresión y clasificación con soporte de ChatGPT
- 20.2.1. Principios de regresión y clasificación en predicción de amenazas
- 20.2.2. Tipos de modelos de clasificación en Ciberseguridad
- 20.2.3. Asistencia de ChatGPT en la interpretación de modelos predictivos

20.3. Identificación de amenazas emergentes con predicciones de ChatGPT
- 20.3.1. Conceptos de detección de amenazas emergentes
- 20.3.2. Técnicas de identificación de nuevos patrones de ataque
- 20.3.3. Limitaciones y precauciones en la predicción de nuevas amenazas

20.4. Redes neuronales para anticipación de ataques cibernéticos
- 20.4.1. Fundamentos de redes neuronales aplicadas en Ciberseguridad
- 20.4.2. Arquitecturas comunes para detección y predicción de ataques
- 20.4.3. Desafíos en la implementación de redes neuronales en defensa cibernética

20.5. Uso de ChatGPT para simulaciones de escenarios de amenaza
- 20.5.1. Conceptos básicos de simulación de amenazas en Ciberseguridad
- 20.5.2. Capacidades de ChatGPT para desarrollar simulaciones predictivas
- 20.5.3. Factores a considerar en el diseño de escenarios simulados

20.6. Algoritmos de aprendizaje por refuerzo para optimización de defensas
- 20.6.1. Introducción al aprendizaje por refuerzo en Ciberseguridad
- 20.6.2. Algoritmos de refuerzo aplicados a estrategias de defensa
- 20.6.3. Beneficios y retos del aprendizaje por refuerzo en entornos de Ciberseguridad

20.7. Simulación de amenazas y respuestas con ChatGPT
- 20.7.1. Principios de simulación de amenazas y su relevancia en ciberdefensa
- 20.7.2. Respuestas automatizadas y optimizadas ante ataques simulados
- 20.7.3. Beneficios de la simulación para mejorar la preparación cibernética

20.8. Evaluación de precisión y efectividad en modelos predictivos de Inteligencia Artificial
- 20.8.1. Indicadores clave para la evaluación de modelos predictivos
- 20.8.2. Metodologías de evaluación de precisión en modelos de Ciberseguridad
- 20.8.3. Factores críticos en la efectividad de los modelos de Inteligencia Artificial en Ciberseguridad

20.9. Inteligencia Artificial en la gestión de incidentes y respuestas automatizadas
- 20.9.1. Fundamentos de la gestión de incidentes en Ciberseguridad
- 20.9.2. Rol de la Inteligencia Artificial en la toma de decisiones en tiempo real
- 20.9.3. Desafíos y oportunidades en la automatización de respuestas

20.10. Creación de un sistema de defensa predictivo con soporte de ChatGPT
- 20.10.1. Principios de diseño de sistemas de defensa proactiva
- 20.10.2. Integración de modelos predictivos en entornos de Ciberseguridad
- 20.10.3. Componentes clave para un sistema de defensa predictivo basado en Inteligencia Artificial

Ahondarás en la integración de ChatGPT en el análisis de riesgos y la respuesta automatizada a incidentes, para gestionar entornos digitales de alta complejidad con precisión"

03

Objetivos docentes

Este programa universitario de TECH tiene como objetivo principal dotar al profesional de las competencias necesarias para liderar proyectos de Ciberseguridad apoyados en Inteligencia Artificial. Gracias a este itinerario académico, los informáticos podrán diseñar modelos predictivos, implementar algoritmos avanzados y desarrollar estrategias efectivas para la protección tanto de sistemas como datos. Además, adquirirán habilidades para la detección proactiva de amenazas, el análisis forense digital y la optimización de recursos tecnológicos en entornos de alta complejidad.

Obtendrás competencias clave para analizar grandes volúmenes de datos, detectar patrones anómalos y gestionar amenazas en tiempo real”

Objetivos generales

- Dominar los principios fundamentales de la Inteligencia Artificial y su aplicación en la Ciberseguridad
- Analizar el ciclo de vida de los datos y su impacto en la implementación de sistemas inteligentes
- Diseñar modelos avanzados de aprendizaje automático para la detección y mitigación de amenazas
- Implementar redes neuronales profundas y sistemas de aprendizaje profundo en proyectos de Ciberseguridad
- Aplicar técnicas de minería de datos y procesamiento del lenguaje natural al análisis de riesgos
- Desarrollar estrategias basadas en Inteligencia Artificial para la protección proactiva de infraestructuras críticas
- Integrar sistemas inteligentes bioinspirados para la resolución de problemas complejos en entornos digitales
- Optimizar algoritmos y herramientas como TensorFlow para personalizar soluciones de seguridad
- Implementar métodos de análisis forense digital asistidos por Inteligencia Artificial
- Diseñar soluciones innovadoras en criptografía moderna para garantizar la integridad de los datos
- Evaluar la eficacia de los modelos predictivos y generativos aplicados a la defensa cibernética
- Fomentar la innovación en el desarrollo de herramientas basadas en Inteligencia Artificial para abordar las amenazas emergentes

Objetivos específicos

Módulo 1. Fundamentos de la Inteligencia Artificial

- Analizar la evolución histórica de la Inteligencia Artificial, desde sus inicios hasta su estado actual, identificando hitos y desarrollos clave
- Comprender el funcionamiento de las redes de neuronas y su aplicación en modelos de aprendizaje en la Inteligencia Artificial
- Estudiar los principios y aplicaciones de los algoritmos genéticos, analizando su utilidad en la resolución de problemas complejos
- Analizar la importancia de los tesauros, vocabularios y taxonomías en la estructuración y procesamiento de datos para sistemas de Inteligencia Artificial

Módulo 2. Tipos y ciclo de vida del dato

- Identificar y clasificar los distintos tipos de datos estadísticos, desde los cuantitativos hasta cualitativos
- Analizar el ciclo de vida de los datos, desde su generación hasta su eliminación, identificando las etapas clave
- Explorar las etapas iniciales del ciclo de vida de los datos, destacando la importancia de la planificación y la estructura de los datos
- Estudiar los procesos de recolección de datos, incluyendo la metodología, las herramientas y los canales de recolección
- Explorar el concepto de *Datawarehouse* (Almacén de Datos), haciendo hincapié en los elementos que lo integran y en su diseño
- Analizar los aspectos normativos relacionados con la gestión de datos, cumpliendo con regulaciones de privacidad y seguridad, así como de buenas prácticas

Módulo 3. El dato en la Inteligencia Artificial

- Dominar los fundamentos de la ciencia de datos, abarcando herramientas, tipos y fuentes para el análisis de información
- Explorar el proceso de transformación de datos en información utilizando técnicas de extracción y visualización de datos
- Estudiar la estructura y características de los *datasets*, comprendiendo su importancia en la preparación y utilización de datos para modelos de Inteligencia Artificial
- Utilizar herramientas específicas y buenas prácticas en el manejo y procesamiento de datos, asegurando la eficiencia y calidad en la implementación de la Inteligencia Artificial

Módulo 4. Minería de datos. Selección, preprocesamiento y transformación

- Dominar las técnicas de inferencia estadística para comprender y aplicar métodos estadísticos en la minería de datos
- Realizar un análisis exploratorio detallado de conjuntos de datos para identificar patrones, anomalías y tendencias relevantes
- Desarrollar habilidades para la preparación de datos, incluyendo su limpieza, integración y formateo para su uso en minería de datos
- Implementar estrategias efectivas para manejar valores perdidos en conjuntos de datos, aplicando métodos de imputación o eliminación según el contexto
- Identificar y mitigar el ruido presente en los datos, utilizando técnicas de filtrado y suavización para mejorar la calidad del conjunto de datos
- Abordar el preprocesamiento de datos en entornos *Big Data*

Módulo 5. Algoritmia y complejidad en Inteligencia Artificial

- Introducir estrategias de diseño de algoritmos, proporcionando una comprensión sólida de los enfoques fundamentales para la resolución de problemas
- Estudiar y aplicar algoritmos de ordenación, comprendiendo su funcionamiento y comparando su eficiencia en diferentes contextos
- Investigar algoritmos con *Heaps*, analizando su implementación y utilidad en la manipulación eficiente de datos
- Analizar algoritmos basados en grafos, explorando su aplicación en la representación y solución de problemas que involucran relaciones complejas
- Estudiar algoritmos *Greedy*, entendiendo su lógica y aplicaciones en la resolución de problemas de optimización
- Investigar y aplicar la técnica de *backtracking* para la resolución sistemática de problemas, analizando su eficacia en diversos escenarios

Módulo 6. Sistemas inteligentes

- Explorar la teoría de agentes, comprendiendo los conceptos fundamentales de su funcionamiento y su aplicación en Inteligencia Artificial e Ingeniería de *Software*
- Analizar el concepto de la web semántica y su impacto en la organización y recuperación de información en entornos digitales
- Evaluar y comparar distintas representaciones del conocimiento, integrando estas para mejorar la eficacia y precisión de los sistemas inteligentes
- Estudiar razonadores semánticos, sistemas basados en conocimiento y sistemas expertos, comprendiendo su funcionalidad y aplicaciones en la toma de decisiones inteligentes

Módulo 7. Aprendizaje automático y minería de datos

- Introducir los procesos de descubrimiento del conocimiento y los conceptos fundamentales del aprendizaje automático
- Evaluar clasificadores utilizando técnicas específicas para medir su rendimiento y precisión en la clasificación de datos
- Estudiar redes neuronales, comprendiendo su funcionamiento y arquitectura para resolver problemas complejos de aprendizaje automático
- Explorar métodos bayesianos y su aplicación en el aprendizaje automático, incluyendo redes y clasificadores bayesianos
- Analizar modelos de regresión y de respuesta continua para la predicción de valores numéricos a partir de datos
- Explorar la minería de textos y el procesamiento del lenguaje natural (NLP), comprendiendo cómo se aplican técnicas de aprendizaje automático para analizar y comprender el texto

Módulo 8. Las redes neuronales, base de *Deep Learning*

- Dominar los fundamentos del Aprendizaje Profundo, comprendiendo su papel esencial en el *Deep Learning*
- Explorar las operaciones fundamentales en redes neuronales y comprender su aplicación en la construcción de modelos
- Analizar las diferentes capas utilizadas en redes neuronales y aprender a seleccionarlas adecuadamente
- Comprender la unión efectiva de capas y operaciones para diseñar arquitecturas de redes neuronales complejas y eficientes
- Explorar la conexión entre neuronas biológicas y artificiales para una comprensión más profunda del diseño de modelos
- Ajustar hiperparámetros para el *Fine Tuning* de redes neuronales, optimizando su rendimiento en tareas específicas

Módulo 9. Entrenamiento de redes neuronales profundas

- Resolver problemas relacionados con los gradientes en el entrenamiento de redes neuronales profundas
- Aplicar directrices prácticas para garantizar un entrenamiento eficiente y efectivo de redes neuronales profundas
- Implementar *Transfer Learning* como una técnica avanzada para mejorar el rendimiento del modelo en tareas específicas
- Explorar y aplicar técnicas de *Data Augmentation* para enriquecer conjuntos de datos y mejorar la generalización del modelo
- Desarrollar aplicaciones prácticas utilizando *Transfer Learning* para resolver problemas del mundo real
- Comprender y aplicar técnicas de regularización para mejorar la generalización y evitar el sobreajuste en redes neuronales profundas

Módulo 10. Personalización de modelos y entrenamiento con *TensorFlow*

- Dominar los fundamentos de *TensorFlow* y su integración con NumPy para un manejo eficiente de datos y cálculos
- Personalizar modelos y algoritmos de entrenamiento utilizando las capacidades avanzadas de *TensorFlow*
- Implementar el formato TFRecord para almacenar y acceder a grandes conjuntos de datos en *TensorFlow*
- Utilizar capas de preprocesamiento de Keras para facilitar la construcción de modelos personalizados
- Explorar el proyecto *TensorFlow Datasets* para acceder a conjuntos de datos predefinidos y mejorar la eficiencia en el desarrollo
- Desarrollar una aplicación de *Deep Learning* con *TensorFlow*, integrando los conocimientos adquiridos en el módulo

Módulo 11. *Deep Computer Vision* con Redes Neuronales Convolucionales

- Comprender la arquitectura del córtex visual y su relevancia en *Deep Computer Vision*
- Explorar y aplicar capas convolucionales para extraer características clave de imágenes
- Implementar capas de agrupación y su utilización en modelos de *Deep Computer Vision* con Keras
- Analizar diversas arquitecturas de Redes Neuronales Convolucionales (CNN) y su aplicabilidad en diferentes contextos
- Desarrollar e implementar una CNN ResNet utilizando la biblioteca Keras para mejorar la eficiencia y rendimiento del modelo
- Utilizar modelos preentrenados de Keras para aprovechar el aprendizaje por transferencia en tareas específicas
- Abordar las estrategias de detección de objetos y seguimiento de objetos utilizando Redes Neuronales Convolucionales
- Implementar técnicas de segmentación semántica para comprender y clasificar objetos en imágenes de manera detallada

Módulo 12. Procesamiento del lenguaje natural (NLP) con Redes Naturales Recurrentes (RNN) y Atención

- Desarrollar habilidades en generación de texto utilizando Redes Neuronales Recurrentes (RNN)
- Aplicar RNN en la clasificación de opiniones para análisis de sentimientos en textos
- Comprender y aplicar los mecanismos de atención en modelos de procesamiento del lenguaje natural
- Analizar y utilizar modelos *Transformers* en tareas específicas de NLP
- Ahondar en la aplicación de modelos *Transformers* en el contexto de procesamiento de imágenes y visión computacional
- Familiarizarse con la librería de *Transformers* de *Hugging Face* para la implementación eficiente de modelos avanzados
- Comparar diferentes librerías de *Transformers* para evaluar su idoneidad en tareas específicas
- Desarrollar una aplicación práctica de NLP que integre RNN y mecanismos de atención para resolver problemas del mundo real

Módulo 13. *Autoencoders, GANs,* y modelos de difusión

- Desarrollar representaciones eficientes de datos mediante *Autoencoders, GANs* y Modelos de Difusión
- Realizar PCA utilizando un codificador automático lineal incompleto para optimizar la representación de datos
- Profundizar y aplicar autocodificadores convolucionales para representaciones eficientes de datos visuales
- Generar imágenes de moda del conjunto de datos MNIST utilizando Autoencoders
- Comprender el concepto de Redes Adversarias Generativas (*GANs*) y Modelos de Difusión
- Implementar y comparar el rendimiento de Modelos de Difusión y *GANs* en la generación de datos

Módulo 14. Computación bioinspirada

- Introducir los conceptos fundamentales de la computación bioinspirada
- Analizar algoritmos de adaptación social como enfoque clave en la computación bioinspirada
- Examinar modelos de computación evolutiva en el contexto de la optimización
- Abordar la complejidad de problemas multiobjetivo en el marco de la computación bioinspirada
- Explorar la aplicación de redes neuronales en el ámbito de la computación bioinspirada
- Profundizar en la implementación y utilidad de redes neuronales en la computación bioinspirada

Módulo 15. Inteligencia Artificial: Estrategias y aplicaciones

- Desarrollar estrategias de implementación de Inteligencia Artificial en servicios financieros
- Analizar las implicaciones de la Inteligencia Artificial en la prestación de servicios sanitarios
- Identificar y evaluar los riesgos asociados al uso de la Inteligencia Artificial en el ámbito de la salud
- Evaluar los riesgos potenciales vinculados al uso de Inteligencia Artificial en la industria
- Aplicar técnicas de Inteligencia Artificial en industria para mejorar la productividad
- Diseñar soluciones de Inteligencia Artificial para optimizar procesos en la administración pública
- Evaluar la implementación de tecnologías de Inteligencia Artificial en el sector educativo
- Aplicar técnicas de Inteligencia Artificial en silvicultura y agricultura para mejorar la productividad

Módulo 16. Ciberseguridad y análisis de amenazas modernas con ChatGPT

- Comprender los conceptos fundamentales de Ciberseguridad, incluyendo las amenazas modernas y el modelo CIA
- Utilizar ChatGPT para el análisis de riesgos, detección de vulnerabilidades y simulación de escenarios de amenaza
- Desarrollar habilidades para diseñar políticas de seguridad cibernética efectivas y proteger dispositivos IoT mediante Inteligencia Artificial

- Implementar estrategias avanzadas de gestión de amenazas utilizando Inteligencia Artificial generativa para anticipar posibles ataques
- Evaluar el impacto de las amenazas modernas en infraestructuras críticas mediante técnicas de simulación asistida por Inteligencia Artificial
- Diseñar soluciones personalizadas para la protección de redes corporativas, basadas en herramientas avanzadas de Inteligencia Artificial

Módulo 17. Detección y prevención de intrusiones usando modelos de Inteligencia Artificial Generativa

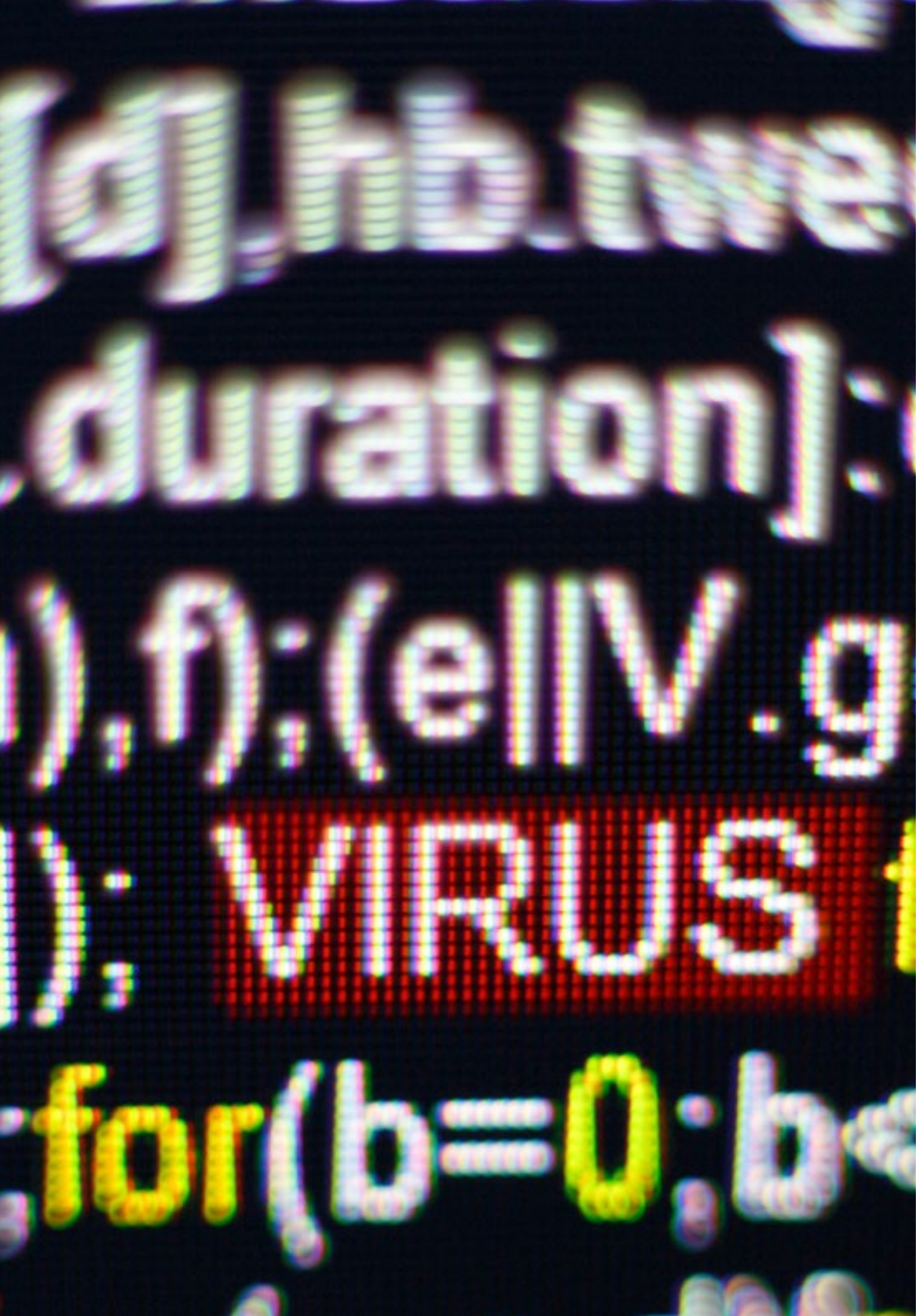
- Dominar las técnicas de detección de anomalías y patrones de intrusión con herramientas como Gemini
- Aplicar modelos generativos para simular ataques cibernéticos y mejorar la prevención de intrusiones
- Implementar sistemas IDS/IPS avanzados optimizados con Inteligencia Artificial, desarrollando perfiles de comportamiento y analizando *Big Data* en tiempo real
- Diseñar arquitecturas de seguridad integradas con Inteligencia Artificial para la protección de entornos multiusuario y sistemas distribuidos
- Utilizar modelos generativos para anticipar ataques dirigidos y elaborar contramedidas en tiempo real
- Integrar análisis predictivo en sistemas de detección para la gestión dinámica de amenazas emergentes

Módulo 18. Criptografía moderna con asistencia de ChatGPT en la protección de datos

- Dominar los fundamentos de la criptografía avanzada, incluyendo algoritmos como AES, RSA y post-cuánticos
- Utilizar ChatGPT para enseñar, practicar y optimizar métodos criptográficos
- Diseñar y gestionar sistemas de encriptación asistidos por Inteligencia Artificial, garantizando la privacidad y la autenticidad de los datos
- Evaluar la resistencia de algoritmos criptográficos frente a escenarios de ataques simulados con Inteligencia Artificial generativa
- Desarrollar estrategias de cifrado y descifrado optimizadas para proteger infraestructuras críticas y datos sensibles
- Implementar soluciones de criptografía postcuántica para mitigar riesgos futuros en sistemas basados en Inteligencia Artificial

Módulo 19. Análisis forense digital y respuesta a incidentes asistida por Inteligencia Artificial

- Aprender a identificar, extraer y analizar evidencias digitales con el apoyo de herramientas de Inteligencia Artificial
- Utilizar Inteligencia Artificial para automatizar la recuperación de datos y reconstrucción de incidentes de seguridad
- Diseñar y practicar flujos de trabajo de respuesta automatizada, asegurando rapidez y efectividad en la mitigación de incidentes



- Integrar herramientas de análisis forense avanzadas para la investigación de ciberataques complejos
- Desarrollar técnicas de reconstrucción de eventos basada en Inteligencia Artificial para auditorías postincidente
- Crear protocolos automatizados de respuesta a incidentes, priorizando la continuidad operativa y la mitigación de daños

Módulo 20. Modelos predictivos de defensa proactiva en Ciberseguridad usando ChatGPT

- Diseñar modelos predictivos avanzados basados en redes neuronales y aprendizaje por refuerzo
- Implementar simulaciones de escenarios de amenaza para entrenar equipos y mejorar la preparación ante incidentes
- Evaluar y optimizar sistemas de defensa proactiva, integrando Inteligencia Artificial generativa en la toma de decisiones y automatización de respuestas
- Desarrollar *frameworks* de defensa predictiva adaptables a infraestructuras críticas y sistemas empresariales
- Utilizar análisis predictivo para identificar vulnerabilidades emergentes antes de que sean explotadas
- Integrar Inteligencia Artificial generativa en procesos de toma de decisiones estratégicas para la mejora continua de sistemas defensivos

04

Salidas profesionales

Con las competencias y conocimientos adquiridos a través de esta titulación universitaria, los informáticos podrán acceder a un amplio abanico de oportunidades laborales en sectores clave como la Seguridad Informática, el Análisis de Riesgos y la Gestión de Infraestructuras Críticas. De esta manera, estarán habilitados para desempeñar roles estratégicos en la detección de amenazas, el diseño de modelos predictivos y la protección avanzada de datos, posicionándolos como referentes en un campo altamente demandado.

Tu perfil profesional te permitirá desempeñarte como Consultor de Ciberseguridad, asesorando a organizaciones sobre la integración de soluciones tecnológicas avanzadas"

Perfil del egresado

El egresado de este programa universitario será un profesional especializado en integrar Inteligencia Artificial y Ciberseguridad para diseñar soluciones innovadoras frente a amenazas digitales. Poseerá un profundo conocimiento de herramientas avanzadas, modelos predictivos y criptografía moderna, destacándose por su capacidad para implementar estrategias efectivas en la protección de datos y sistemas críticos. Este perfil combina excelencia técnica y visión práctica, asegurando su contribución en la transformación del entorno digital.

Ampliarás tus horizontes laborales con un enfoque especializado, manejando métodos sofisticados como la Minería de Datos, el Deep Learning y el Análisis Forense Digital.

- **Pensamiento crítico y resolución de problemas:** Capacidad para analizar situaciones complejas desde múltiples perspectivas para identificar patrones en amenazas digitales y diseñar soluciones innovadoras mediante el uso de Inteligencia Artificial que aborden desafíos tecnológicos de forma precisa y adaptativa
- **Toma de decisiones basada en datos:** Habilidad para interpretar grandes volúmenes de datos y aplicar modelos predictivos que fundamenten estrategias en tiempo real asegurando acciones orientadas a mitigar riesgos de forma eficiente
- **Adaptabilidad tecnológica:** Competencia para integrar rápidamente nuevas herramientas, tecnologías y metodologías de Inteligencia Artificial en la práctica profesional respondiendo de manera ágil a cambios en el panorama digital y a nuevas formas de ataque cibernético
- **Gestión ética y responsable:** Comprensión profunda de los aspectos legales y éticos relacionados con la protección de datos y el uso de Inteligencia Artificial actuando de forma ética y alineada con las regulaciones internacionales para garantizar el uso responsable de las tecnologías en Ciberseguridad

Después de realizar el programa título propio, podrás desempeñar tus conocimientos y habilidades en los siguientes cargos:

1. **Analista de Seguridad Cibernética con Inteligencia Artificial:** Encargado de identificar, prevenir y mitigar amenazas digitales utilizando modelos avanzados de Inteligencia Artificial para la protección de sistemas críticos.
   Responsabilidad: Implementar sistemas de detección de intrusiones basados en Inteligencia Artificial, analizar patrones de ataque y diseñar contramedidas efectivas en tiempo real.
2. **Analista Forense Digital con Inteligencia Artificial:** Responsable de identificar, extraer y analizar evidencias digitales empleando tecnologías avanzadas de Inteligencia Artificial.
   Responsabilidad: Automatizar procesos de recuperación de datos y reconstrucción de incidentes para garantizar la integridad de las investigaciones cibernéticas.
3. **Consultor en Defensa Digital Proactiva:** Asesor especializado en el desarrollo de estrategias de seguridad basadas en Inteligencia Artificial para anticiparse a amenazas emergentes en entornos empresariales.
   Responsabilidad: Realizar simulaciones de escenarios de ataque y diseñar soluciones predictivas para proteger infraestructuras críticas.
4. **Experto en Análisis Forense Digital con Inteligencia Artificial:** Encargado de investigar y reconstruir incidentes de ciberseguridad utilizando herramientas de Inteligencia Artificial para extraer y analizar evidencias digitales.
   Responsabilidad: Automatizar procesos de recuperación de datos, realizar auditorías postincidente y elaborar informes técnicos para la toma de decisiones.
5. **Diseñador de Modelos Predictivos de Ciberseguridad:** Enfocado en el desarrollo e implementación de sistemas basados en aprendizaje automático y redes neuronales para anticipar vulnerabilidades
   Responsabilidad: Crear modelos predictivos personalizados y optimizar herramientas de Inteligencia Artificial para identificar patrones de ataque antes de que se materialicen.
6. **Coordinador de Seguridad en Infraestructuras Críticas:** Responsable de supervisar la implementación de soluciones de ciberseguridad basadas en Inteligencia Artificial en sectores estratégicos como energía, transporte o finanzas.
   Responsabilidad: Monitorear amenazas en tiempo real, integrar sistemas de Inteligencia Artificial en plataformas operativas y coordinar respuestas ante incidentes.
7. **Gestor de Riesgos Cibernéticos con Inteligencia Artificial:** Se encarga de liderar la planificación y ejecución de estrategias para identificar y minimizar riesgos cibernéticos utilizando Inteligencia Artificial.
   Responsabilidad: Realizar evaluaciones de vulnerabilidades y diseñar marcos de seguridad dinámicos basados en Inteligencia Artificial Generativa.
8. **Responsable de Criptografía Postcuántica:** experto en diseñar sistemas de cifrado robustos basados en algoritmos resistentes a computadoras cuánticas, asegurando la protección de datos a largo plazo.
   Responsabilidad: Evaluar amenazas futuras y desarrollar soluciones criptográficas adaptadas a las necesidades actuales y emergentes.
9. **Administrador de Sistemas de Detección de Intrusiones con Inteligencia Artificial Generativa:** Encargado de configurar y optimizar herramientas de seguridad automatizadas que utilizan Inteligencia Artificial generativa para detectar y responder a amenazas.
   Responsabilidad: Supervisar los sistemas IDS/IPS, analizar resultados en tiempo real y actualizar algoritmos de detección según patrones emergentes.
10. **Auditor de Seguridad Digital Asistido por Inteligencia Artificial:** Responsable de evaluar y certificar sistemas de seguridad digital utilizando herramientas avanzadas de análisis asistido por Inteligencia Artificial.
    Responsabilidad: Identificar brechas de seguridad, elaborar recomendaciones prácticas y garantizar el cumplimiento de normativas internacionales de Ciberseguridad.

Salidas académicas y de investigación

Además de todos los puestos laborales para los que serás apto mediante el estudio de este Máster Título Propio de TECH, también podrás continuar con una sólida trayectoria académica e investigativa. Tras completar este programa universitario, estarás listo para continuar con tus estudios asociados a este ámbito del conocimiento y así, progresivamente, alcanzar otros méritos científicos.

05

Metodología de estudio

TECH es la primera universidad en el mundo que combina la metodología de los ***case studies*** con el ***Relearning***, un sistema de aprendizaje 100% online basado en la reiteración dirigida.

Esta disruptiva estrategia pedagógica ha sido concebida para ofrecer a los profesionales la oportunidad de actualizar conocimientos y desarrollar competencias de un modo intensivo y riguroso. Un modelo de aprendizaje que coloca al estudiante en el centro del proceso académico y le otorga todo el protagonismo, adaptándose a sus necesidades y dejando de lado las metodologías más convencionales.

TECH te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera"

El alumno: la prioridad de todos los programas de TECH

En la metodología de estudios de TECH el alumno es el protagonista absoluto. Las herramientas pedagógicas de cada programa han sido seleccionadas teniendo en cuenta las demandas de tiempo, disponibilidad y rigor académico que, a día de hoy, no solo exigen los estudiantes sino los puestos más competitivos del mercado.

Con el modelo educativo asincrónico de TECH, es el alumno quien elige el tiempo que destina al estudio, cómo decide establecer sus rutinas y todo ello desde la comodidad del dispositivo electrónico de su preferencia. El alumno no tendrá que asistir a clases en vivo, a las que muchas veces no podrá acudir. Las actividades de aprendizaje las realizará cuando le venga bien. Siempre podrá decidir cuándo y desde dónde estudiar.

"En TECH NO tendrás clases en directo (a las que luego nunca puedes asistir)"

Los planes de estudios más exhaustivos a nivel internacional

TECH se caracteriza por ofrecer los itinerarios académicos más completos del entorno universitario. Esta exhaustividad se logra a través de la creación de temarios que no solo abarcan los conocimientos esenciales, sino también las innovaciones más recientes en cada área.

Al estar en constante actualización, estos programas permiten que los estudiantes se mantengan al día con los cambios del mercado y adquieran las habilidades más valoradas por los empleadores. De esta manera, quienes finalizan sus estudios en TECH reciben una preparación integral que les proporciona una ventaja competitiva notable para avanzar en sus carreras.

Y además, podrán hacerlo desde cualquier dispositivo, pc, tableta o smartphone.

El modelo de TECH es asincrónico, de modo que te permite estudiar con tu pc, tableta o tu smartphone donde quieras, cuando quieras y durante el tiempo que quieras”

Case studies o Método del caso

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de negocios del mundo. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, su función era también presentarles situaciones complejas reales. Así, podían tomar decisiones y emitir juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Con este modelo de enseñanza es el propio alumno quien va construyendo su competencia profesional a través de estrategias como el *Learning by doing* o el *Design Thinking*, utilizadas por otras instituciones de renombre como Yale o Stanford.

Este método, orientado a la acción, será aplicado a lo largo de todo el itinerario académico que el alumno emprenda junto a TECH. De ese modo se enfrentará a múltiples situaciones reales y deberá integrar conocimientos, investigar, argumentar y defender sus ideas y decisiones. Todo ello con la premisa de responder al cuestionamiento de cómo actuaría al posicionarse frente a eventos específicos de complejidad en su labor cotidiana.

Método *Relearning*

En TECH los *case studies* son potenciados con el mejor método de enseñanza 100% online: el *Relearning*.

Este método rompe con las técnicas tradicionales de enseñanza para poner al alumno en el centro de la ecuación, proveyéndole del mejor contenido en diferentes formatos. De esta forma, consigue repasar y reiterar los conceptos clave de cada materia y aprender a aplicarlos en un entorno real.

En esta misma línea, y de acuerdo a múltiples investigaciones científicas, la reiteración es la mejor manera de aprender. Por eso, TECH ofrece entre 8 y 16 repeticiones de cada concepto clave dentro de una misma lección, presentada de una manera diferente, con el objetivo de asegurar que el conocimiento sea completamente afianzado durante el proceso de estudio.

El Relearning te permitirá aprender con menos esfuerzo y más rendimiento, implicándote más en tu especialización, desarrollando el espíritu crítico, la defensa de argumentos y el contraste de opiniones: una ecuación directa al éxito.

Un Campus Virtual 100% online con los mejores recursos didácticos

Para aplicar su metodología de forma eficaz, TECH se centra en proveer a los egresados de materiales didácticos en diferentes formatos: textos, vídeos interactivos, ilustraciones y mapas de conocimiento, entre otros. Todos ellos, diseñados por profesores cualificados que centran el trabajo en combinar casos reales con la resolución de situaciones complejas mediante simulación, el estudio de contextos aplicados a cada carrera profesional y el aprendizaje basado en la reiteración, a través de audios, presentaciones, animaciones, imágenes, etc.

Y es que las últimas evidencias científicas en el ámbito de las Neurociencias apuntan a la importancia de tener en cuenta el lugar y el contexto donde se accede a los contenidos antes de iniciar un nuevo aprendizaje. Poder ajustar esas variables de una manera personalizada favorece que las personas puedan recordar y almacenar en el hipocampo los conocimientos para retenerlos a largo plazo. Se trata de un modelo denominado *Neurocognitive context-dependent e-learning* que es aplicado de manera consciente en esta titulación universitaria.

Por otro lado, también en aras de favorecer al máximo el contacto mentor-alumno, se proporciona un amplio abanico de posibilidades de comunicación, tanto en tiempo real como en diferido (mensajería interna, foros de discusión, servicio de atención telefónica, email de contacto con secretaría técnica, chat y videoconferencia).

Asimismo, este completísimo Campus Virtual permitirá que el alumnado de TECH organice sus horarios de estudio de acuerdo con su disponibilidad personal o sus obligaciones laborales. De esa manera tendrá un control global de los contenidos académicos y sus herramientas didácticas, puestas en función de su acelerada actualización profesional.

> *La modalidad de estudios online de este programa te permitirá organizar tu tiempo y tu ritmo de aprendizaje, adaptándolo a tus horarios”*

La eficacia del método se justifica con cuatro logros fundamentales:

1. Los alumnos que siguen este método no solo consiguen la asimilación de conceptos, sino un desarrollo de su capacidad mental, mediante ejercicios de evaluación de situaciones reales y aplicación de conocimientos.
2. El aprendizaje se concreta de una manera sólida en capacidades prácticas que permiten al alumno una mejor integración en el mundo real.
3. Se consigue una asimilación más sencilla y eficiente de las ideas y conceptos, gracias al planteamiento de situaciones que han surgido de la realidad.
4. La sensación de eficiencia del esfuerzo invertido se convierte en un estímulo muy importante para el alumnado, que se traduce en un interés mayor en los aprendizajes y un incremento del tiempo dedicado a trabajar en el curso.

La metodología universitaria mejor valorada por sus alumnos

Los resultados de este innovador modelo académico son constatables en los niveles de satisfacción global de los egresados de TECH.

La valoración de los estudiantes sobre la calidad docente, calidad de los materiales, estructura del curso y sus objetivos es excelente. No en valde, la institución se convirtió en la universidad mejor valorada por sus alumnos en la plataforma de reseñas Trustpilot, obteniendo un 4,9 de 5.

Accede a los contenidos de estudio desde cualquier dispositivo con conexión a Internet (ordenador, tablet, smartphone) gracias a que TECH está al día de la vanguardia tecnológica y pedagógica.

Podrás aprender con las ventajas del acceso a entornos simulados de aprendizaje y el planteamiento de aprendizaje por observación, esto es, Learning from an expert.

Así, en este programa estarán disponibles los mejores materiales educativos, preparados a conciencia:

Material de estudio

Todos los contenidos didácticos son creados por los especialistas que van a impartir el curso, específicamente para él, de manera que el desarrollo didáctico sea realmente específico y concreto.

Estos contenidos son aplicados después al formato audiovisual que creará nuestra manera de trabajo online, con las técnicas más novedosas que nos permiten ofrecerte una gran calidad, en cada una de las piezas que pondremos a tu servicio.

Prácticas de habilidades y competencias

Realizarás actividades de desarrollo de competencias y habilidades específicas en cada área temática. Prácticas y dinámicas para adquirir y desarrollar las destrezas y habilidades que un especialista precisa desarrollar en el marco de la globalización que vivimos.

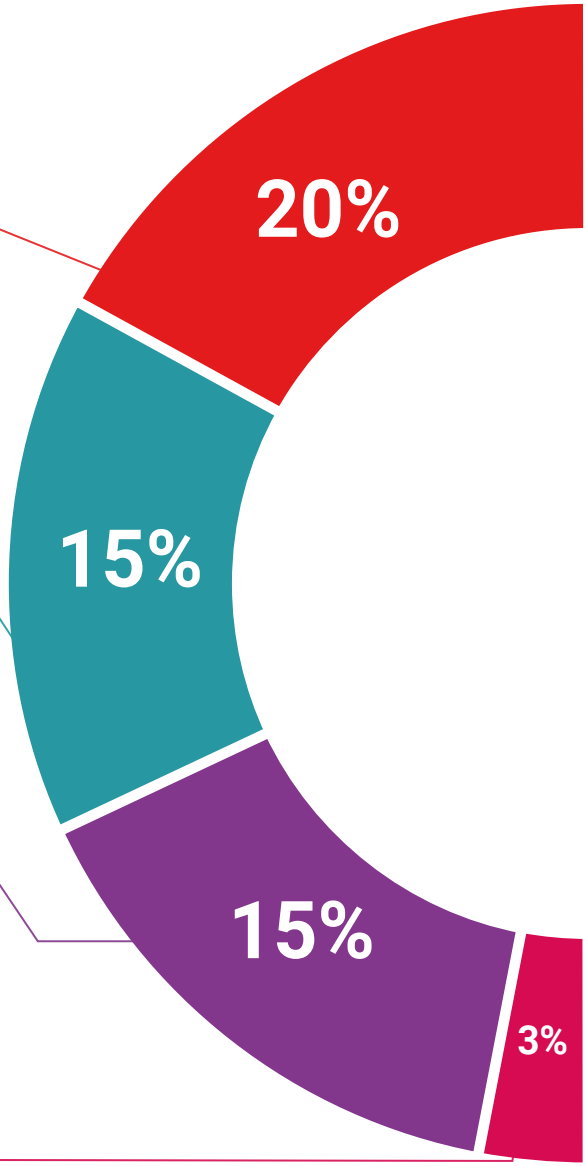
Resúmenes interactivos

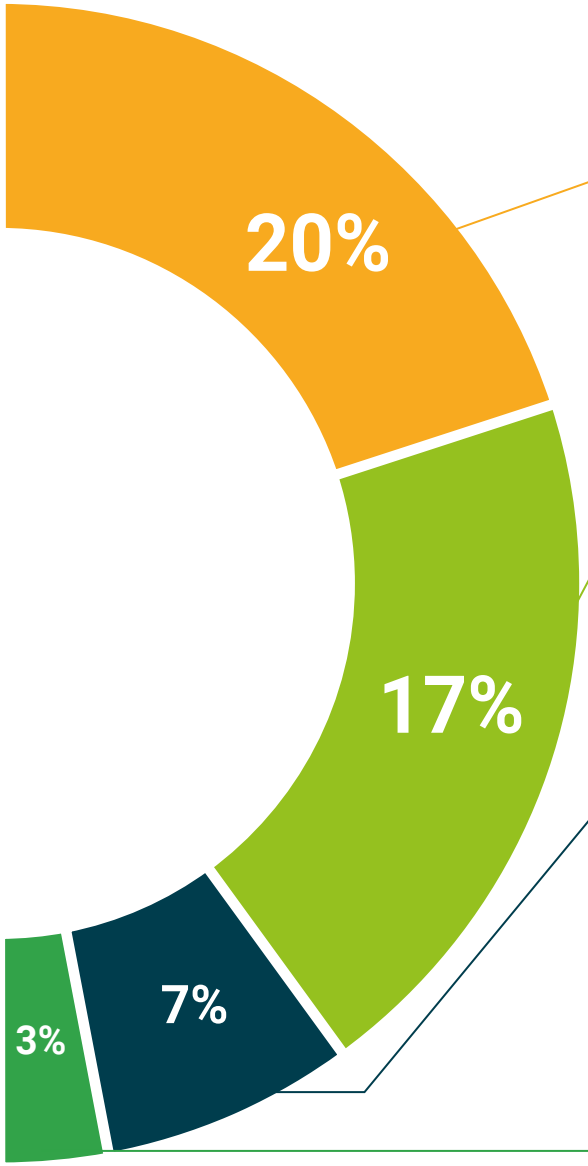
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

Este sistema exclusivo educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".

Lecturas complementarias

Artículos recientes, documentos de consenso, guías internacionales... En nuestra biblioteca virtual tendrás acceso a todo lo que necesitas para completar tu capacitación.





Case Studies

Completarás una selección de los mejores *case studies* de la materia. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.

Testing & Retesting

Evaluamos y reevaluamos periódicamente tu conocimiento a lo largo del programa. Lo hacemos sobre 3 de los 4 niveles de la Pirámide de Miller.

Clases magistrales

Existe evidencia científica sobre la utilidad de la observación de terceros expertos.

El denominado *Learning from an expert* afianza el conocimiento y el recuerdo, y genera seguridad en nuestras futuras decisiones difíciles.

Guías rápidas de actuación

TECH ofrece los contenidos más relevantes del curso en forma de fichas o guías rápidas de actuación. Una manera sintética, práctica y eficaz de ayudar al estudiante a progresar en su aprendizaje.

06

Cuadro docente

El claustro docente de este programa de TECH está integrado por expertos de renombre internacional en los campos de la Inteligencia Artificial y la ciberseguridad. Con sólidas trayectorias tanto en la investigación como en la implementación de soluciones tecnológicas avanzadas, estos profesionales aportan un enfoque práctico y estratégico al desarrollo de competencias clave en el sector. Su experiencia abarca desde la dirección de proyectos innovadores hasta la colaboración con líderes de la industria, asegurando una visión actualizada y aplicada a las demandas tecnológicas más exigentes.

Te beneficiarás tanto de la experiencia como del bagaje académico de reconocidos profesionales con una sólida reputación en Ciberseguridad y Aprendizaje Profundo"

Dirección

Dr. Peralta Martín-Palomino, Arturo

- CEO y CTO en Prometeus Global Solutions
- CTO en Korporate Technologies
- CTO en AI Shepherds GmbH
- Consultor y Asesor Estratégico Empresarial en Alliance Medical
- Director de Diseño y Desarrollo en DocPath
- Doctor en Ingeniería Informática por la Universidad de Castilla-La Mancha
- Doctor en Economía, Empresas y Finanzas por la Universidad Camilo José Cela
- Doctor en Psicología por la Universidad de Castilla-La Mancha
- Máster en Executive MBA por la Universidad Isabel I
- Máster en Dirección Comercial y Marketing por la Universidad Isabel I
- Máster Experto en Big Data por Formación Hadoop
- Máster en Tecnologías Informáticas Avanzadas por la Universidad de Castilla-La Mancha
- Miembro de: Grupo de Investigación SMILE

Profesores

D. Del Rey Sánchez, Alejandro

- Responsable de implementación de programas para mejorar la atención táctica en emergencias
- Graduado en Ingeniería de Organización Industrial
- Certificación en *Big Data* y *Business Analytics*
- Certificación en Microsoft Excel Avanzado, VBA, KPI y DAX
- Certificación en CIS Sistemas de Telecomunicación e Información

Aprovecha la oportunidad para conocer los últimos avances en esta materia para aplicarla a tu práctica diaria"

07

Titulación

El Máster Título Propio en Inteligencia Artificial en Ciberseguridad garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Máster Propio expedido por TECH Global University.

Supera con éxito este programa y recibe tu titulación universitaria sin desplazamientos ni farragosos trámites”

Este programa te permitirá obtener el título propio de **Máster en Inteligencia Artificial en Ciberseguridad** avalado por **TECH Global University**, la mayor Universidad digital del mundo.

TECH Global University, es una Universidad Oficial Europea reconocida públicamente por el Gobierno de Andorra (***boletín oficial***). Andorra forma parte del Espacio Europeo de Educación Superior (EEES) desde 2003. El EEES es una iniciativa promovida por la Unión Europea que tiene como objetivo organizar el marco formativo internacional y armonizar los sistemas de educación superior de los países miembros de este espacio. El proyecto promueve unos valores comunes, la implementación de herramientas conjuntas y fortaleciendo sus mecanismos de garantía de calidad para potenciar la colaboración y movilidad entre estudiantes, investigadores y académicos.

Este título propio de **TECH Global University**, es un programa europeo de formación continua y actualización profesional que garantiza la adquisición de las competencias en su área de conocimiento, confiriendo un alto valor curricular al estudiante que supere el programa.

Título: **Máster Título Propio en Inteligencia Artificial en Ciberseguridad**

Modalidad: **online**

Duración: **12 meses**

Acreditación: **90 ECTS**


tech global university

D/Dña _____ con documento de identificación _____ ha superado con éxito y obtenido el título de:

Máster Título Propio en Inteligencia Artificial en Ciberseguridad

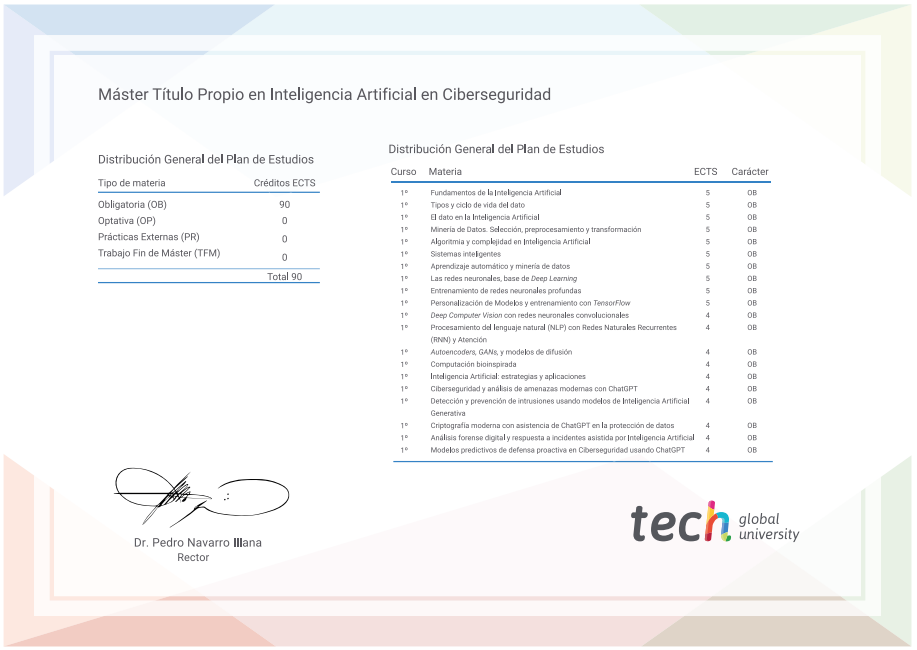
Se trata de un título propio de 2.700 horas de duración equivalente a 90 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH Global University es una universidad reconocida oficialmente por el Gobierno de Andorra el 31 de enero de 2024, que pertenece al Espacio Europeo de Educación Superior (EEES).

En Andorra la Vella, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWOR23S techtitute.com/titulos


Máster Título Propio en Inteligencia Artificial en Ciberseguridad

Distribución General del Plan de Estudios

Tipo de materia	Créditos ECTS
Obligatoria (OB)	90
Optativa (OP)	0
Prácticas Externas (PR)	0
Trabajo Fin de Máster (TFM)	0
	Total 90

Distribución General del Plan de Estudios

Curso	Materia	ECTS	Carácter
1º	Fundamentos de la Inteligencia Artificial	5	OB
1º	Tipos y ciclo de vida del dato	5	OB
1º	El dato en la Inteligencia Artificial	5	OB
1º	Minería de Datos. Selección, preprocesamiento y transformación	5	OB
1º	Algorítmia y complejidad en Inteligencia Artificial	5	OB
1º	Sistemas inteligentes	5	OB
1º	Aprendizaje automático y minería de datos	5	OB
1º	Las redes neuronales, base de *Deep Learning*	5	OB
1º	Entrenamiento de redes neuronales profundas	5	OB
1º	Personalización de Modelos y entrenamiento con *TensorFlow*	5	OB
1º	*Deep Computer Vision* con redes neuronales convolucionales	4	OB
1º	Procesamiento del lenguaje natural (NLP) con Redes Naturales Recurrentes (RNN) y Atención	4	OB
1º	Autoencoders, GANs, y modelos de difusión	4	OB
1º	Computación bioinspirada	4	OB
1º	Inteligencia Artificial: estrategias y aplicaciones	4	OB
1º	Ciberseguridad y análisis de amenazas modernas con ChatGPT	4	OB
1º	Detección y prevención de intrusiones usando modelos de Inteligencia Artificial Generativa	4	OB
1º	Criptografía moderna con asistencia de ChatGPT en la protección de datos	4	OB
1º	Análisis forense digital y respuesta a incidentes asistida por Inteligencia Artificial	4	OB
1º	Modelos predictivos de defensa proactiva en Ciberseguridad usando ChatGPT	4	OB

Dr. Pedro Navarro Illana
Rector

tech global university

*Apostilla de La Haya. En caso de que el alumno solicite que su título en papel recabe la Apostilla de La Haya, TECH Global University realizará las gestiones oportunas para su obtención, con un coste adicional.

tech global university

Máster Título Propio
Inteligencia Artificial en Ciberseguridad

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Global University**
- Acreditación: **90 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Máster Título Propio

Inteligencia Artificial en Ciberseguridad

tech global university