

Experto Universitario

Análisis y Detección de Amenazas de Ciberseguridad con Inteligencia Artificial



Experto Universitario Análisis y Detección de Amenazas de Ciberseguridad con Inteligencia Artificial

- » Modalidad: No escolarizada (100% en línea)
- » Duración: 6 meses
- » Titulación: TECH Universidad
- » Horario: a tu ritmo
- » Exámenes: online

Acceso web: www.techtute.com/inteligencia-artificial/experto-universitario/experto-analisis-deteccion-amenazas-ciberseguridad-inteligencia-artificial

Índice

01

Presentación del programa

pág. 4

02

¿Por qué estudiar en TECH?

pág. 8

03

Plan de estudios

pág. 12

04

Objetivos docentes

pág. 18

05

Salidas profesionales

pág. 22

06

Metodología de estudio

pág. 26

07

Cuadro docente

pág. 36

08

Titulación

pág. 40

01

Presentación del programa

La identificación temprana de amenazas cibernéticas es crucial para prevenir daños a las infraestructuras digitales de las organizaciones. Sin embargo, las amenazas continúan evolucionando a una velocidad sin precedentes, lo que dificulta el uso de herramientas tradicionales para mitigar riesgos. Ante esto, la Inteligencia Artificial ha revolucionado el análisis de Ciberseguridad al permitir la automatización del proceso de identificación de amenazas y la mejora de la precisión de los sistemas de detección. Por ello, los expertos necesitan manejar las técnicas de aprendizaje automático más innovadoras para identificar patrones de comportamientos anómalos y anticipar ciberataques. Con el objetivo de facilitarles esta labor, TECH lanza una revolucionaria titulación universitaria enfocada en el Análisis y Detección de Amenazas de Ciberseguridad con Inteligencia Artificial.



“

Con este Experto Universitario 100% online, utilizarás técnicas innovadoras de Inteligencia Artificial para identificar y mitigar ataques digitales en tiempo real”

Según un nuevo informe elaborado por la Organización de las Naciones Unidas, se estima que los costos globales de los ciberataques alcanzarán los 10.5 billones de dólares anuales de cara al próximo año. Este crecimiento se debe en parte a la sofisticación de los métodos de ataque, lo que hace que las técnicas tradicionales de detección sean insuficientes. En este contexto, la Inteligencia Artificial se ha convertido en una herramienta clave en la prevención de amenazas, permitiendo a los sistemas identificar patrones anómalos y responder a incidentes en tiempo real. De ahí la importancia de que los profesionales desarrollen competencias avanzadas para implementar sistemas inteligentes que mejoren la eficiencia y precisión de la detección de amenazas cibernéticas.

En este escenario, TECH presenta un pionero Experto Universitario en Análisis y Detección de Amenazas de Ciberseguridad con Inteligencia Artificial. Confeccionado por referentes en este sector, el itinerario académico profundizará en factores que comprenden desde la evaluación de amenazas asistidas por sistemas inteligentes o la aplicación de modelos generativos en la simulación de ataques hasta la creación de un sistema de defensa predictivo con soporte de ChatGPT. De este modo, los egresados obtendrán habilidades avanzadas para diseñar e implementar soluciones de ciberseguridad basadas en Inteligencia Artificial, permitiéndoles anticipar y neutralizar amenazas de manera proactiva.

Por otro lado, este programa universitario se basa en un formato 100% online, de fácil acceso desde cualquier dispositivo con conexión a internet y sin horarios predeterminados. A su vez, TECH emplea su disruptivo método de enseñanza del *Relearning*, para que los expertos profundicen en los contenidos sin recurrir a técnicas que impliquen un esfuerzo extra, como la memorización. En este sentido, lo único que necesitarán los profesionales es contar con un dispositivo electrónico con acceso a internet (como un móvil, tablet u ordenador) para acceder a los materiales didácticos más completos del mercado y disfrutar de una experiencia de primera categoría.

Este **Experto Universitario en Análisis y Detección de Amenazas de Ciberseguridad con Inteligencia Artificial** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- ♦ El desarrollo de casos prácticos presentados por expertos con un profundo conocimiento en Ciberseguridad e Inteligencia Artificial, quienes aplican estas herramientas para la detección, prevención y mitigación de ciberamenazas en entornos tecnológicos avanzados
- ♦ 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



Diseñarás sistemas de detección de intrusos basados en Inteligencia Artificial, optimizando la protección de infraestructuras críticas”

“

Dominarás algoritmos de Aprendizaje Automático para anticipar y neutralizar delitos informáticos”

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.

Aplicarás técnicas de análisis de datos para identificar patrones y comportamientos anómalos en redes informáticas.

Con el sistema Relearning no tendrás que invertir una gran cantidad de horas de estudio y te focalizarás en los conceptos más relevantes.



02

¿Por qué estudiar en TECH?

TECH es la mayor Universidad digital del mundo. Con un impresionante catálogo de más de 14.000 programas universitarios, disponibles en 11 idiomas, se posiciona como líder en empleabilidad, con una tasa de inserción laboral del 99%. Además, cuenta con un enorme claustro de más de 6.000 profesores de máximo prestigio internacional.



“

Estudia en la mayor universidad digital del mundo y asegura tu éxito profesional. El futuro empieza en TECH”

La mejor universidad online del mundo según FORBES

La prestigiosa revista Forbes, especializada en negocios y finanzas, ha destacado a TECH como «la mejor universidad online del mundo». Así lo han hecho constar recientemente en un artículo de su edición digital en el que se hacen eco del caso de éxito de esta institución, «gracias a la oferta académica que ofrece, la selección de su personal docente, y un método de aprendizaje innovador orientado a formar a los profesionales del futuro».

Forbes
Mejor universidad
online del mundo

Plan
de estudios
más completo

Los planes de estudio más completos del panorama universitario

TECH ofrece los planes de estudio más completos del panorama universitario, con temarios que abarcan conceptos fundamentales y, al mismo tiempo, los principales avances científicos en sus áreas científicas específicas. Asimismo, estos programas son actualizados continuamente para garantizar al alumnado la vanguardia académica y las competencias profesionales más demandadas. De esta forma, los títulos de la universidad proporcionan a sus egresados una significativa ventaja para impulsar sus carreras hacia el éxito.

El mejor claustro docente top internacional

El claustro docente de TECH está integrado por más de 6.000 profesores de máximo prestigio internacional. Catedráticos, investigadores y altos ejecutivos de multinacionales, entre los cuales se destacan Isaiah Covington, entrenador de rendimiento de los Boston Celtics; Magda Romanska, investigadora principal de MetaLAB de Harvard; Ignacio Wistumba, presidente del departamento de patología molecular traslacional del MD Anderson Cancer Center; o D.W Pine, director creativo de la revista TIME, entre otros.

Profesorado
TOP
Internacional

La metodología
más eficaz

Un método de aprendizaje único

TECH es la primera universidad que emplea el *Relearning* en todas sus titulaciones. Se trata de la mejor metodología de aprendizaje online, acreditada con certificaciones internacionales de calidad docente, dispuestas por agencias educativas de prestigio. Además, este disruptivo modelo académico se complementa con el "Método del Caso", configurando así una estrategia de docencia online única. También en ella se implementan recursos didácticos innovadores entre los que destacan vídeos en detalle, infografías y resúmenes interactivos.

La mayor universidad digital del mundo

TECH es la mayor universidad digital del mundo. Somos la mayor institución educativa, con el mejor y más amplio catálogo educativo digital, cien por cien online y abarcando la gran mayoría de áreas de conocimiento. Ofrecemos el mayor número de titulaciones propias, titulaciones oficiales de posgrado y de grado universitario del mundo. En total, más de 14.000 títulos universitarios, en diez idiomas distintos, que nos convierten en la mayor institución educativa del mundo.

nº1
Mundial
Mayor universidad
online del mundo

La universidad online oficial de la NBA

TECH es la universidad online oficial de la NBA. Gracias a un acuerdo con la mayor liga de baloncesto, ofrece a sus alumnos programas universitarios exclusivos, así como una gran variedad de recursos educativos centrados en el negocio de la liga y otras áreas de la industria del deporte. Cada programa tiene un currículo de diseño único y cuenta con oradores invitados de excepción: profesionales con una distinguida trayectoria deportiva que ofrecerán su experiencia en los temas más relevantes.

Líderes en empleabilidad

TECH ha conseguido convertirse en la universidad líder en empleabilidad. El 99% de sus alumnos obtienen trabajo en el campo académico que ha estudiado, antes de completar un año luego de finalizar cualquiera de los programas de la universidad. Una cifra similar consigue mejorar su carrera profesional de forma inmediata. Todo ello gracias a una metodología de estudio que basa su eficacia en la adquisición de competencias prácticas, totalmente necesarias para el desarrollo profesional.



Google Partner Premier

El gigante tecnológico norteamericano ha otorgado TECH la insignia Google Partner Premier. Este galardón, solo al alcance del 3% de las empresas del mundo, pone en valor la experiencia eficaz, flexible y adaptada que esta universidad proporciona al alumno. El reconocimiento no solo acredita el máximo rigor, rendimiento e inversión en las infraestructuras digitales de TECH, sino que también sitúa a esta universidad como una de las compañías tecnológicas más punteras del mundo.



La universidad mejor valorada por sus alumnos

Los alumnos han posicionado a TECH como la universidad mejor valorada del mundo en los principales portales de opinión, destacando su calificación más alta de 4,9 sobre 5, obtenida a partir de más de 1.000 reseñas. Estos resultados consolidan a TECH como la institución universitaria de referencia a nivel internacional, reflejando la excelencia y el impacto positivo de su modelo educativo.



03

Plan de estudios

Los contenidos didácticos que conforman este Experto Universitario han sido elaborados por reconocidos expertos en el uso de Inteligencia Artificial en Ciberseguridad. Así pues, el plan de estudios ahondará en cuestiones que abarcan desde el uso de ChatGPT para el análisis de riesgo o el entrenamiento de algoritmos hasta técnicas sofisticadas de modelado predictivo. Gracias a esto, los alumnos serán capaces de aplicar soluciones avanzadas de Inteligencia Artificial para la detección y mitigación de amenazas cibernéticas en tiempo real.



“

Profundizarás en la creación de protocolos de respuesta automatizados que permitan una recuperación eficiente de los sistemas afectados por un ataque cibernético”

Módulo 1. Ciberseguridad y análisis de amenazas modernas con ChatGPT

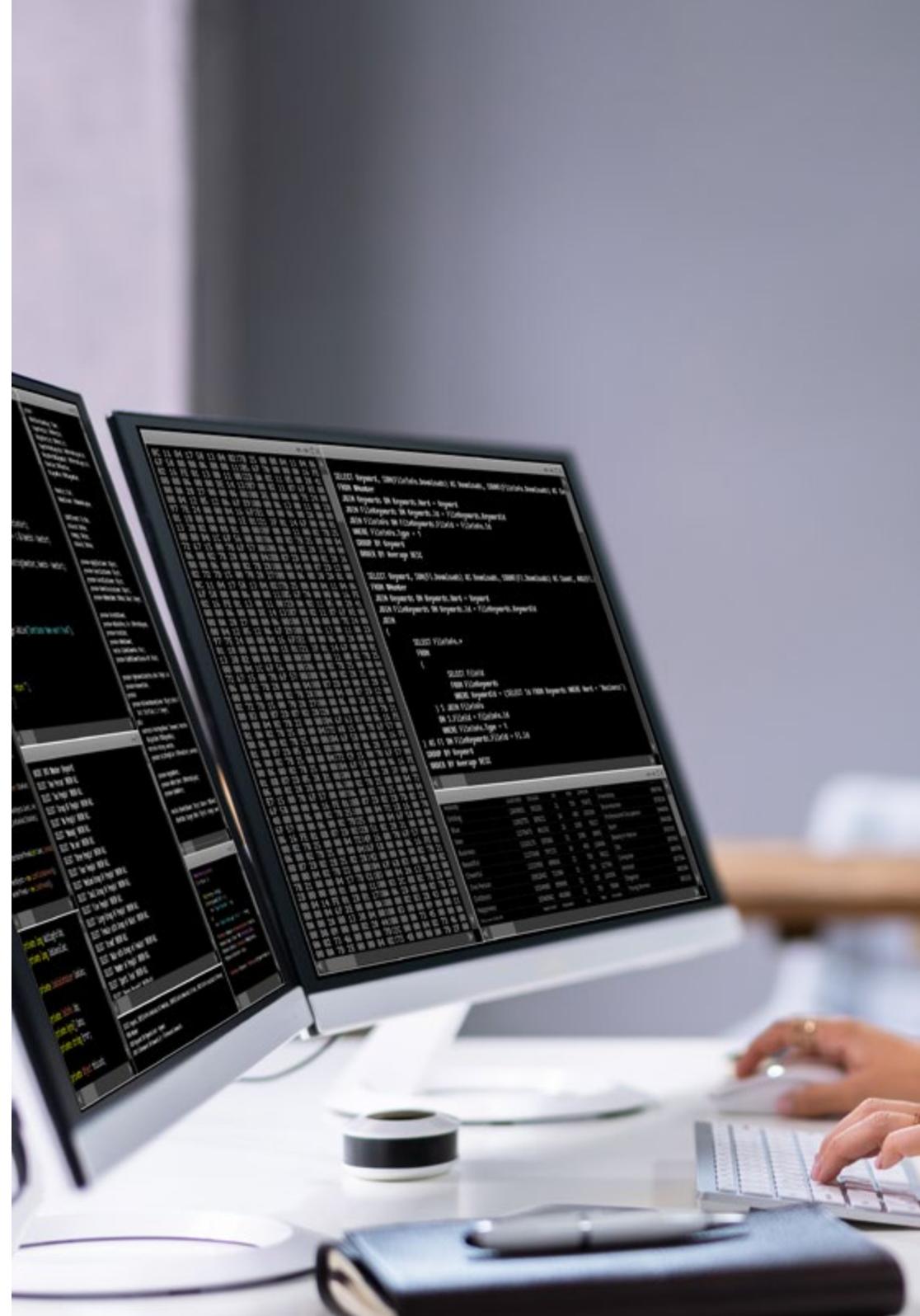
- 1.1. Introducción a la Ciberseguridad: amenazas actuales y el rol de la Inteligencia Artificial
 - 1.1.1. Definición y conceptos básicos de Ciberseguridad
 - 1.1.2. Tipos de amenazas cibernéticas modernas
 - 1.1.3. Papel de la Inteligencia Artificial en la evolución de la Ciberseguridad
- 1.2. Confidencialidad, integridad y disponibilidad (CIA) en la era de la Inteligencia Artificial
 - 1.2.1. Fundamentos del modelo CIA en Ciberseguridad
 - 1.2.2. Principios de seguridad aplicados en el contexto de Inteligencia Artificial
 - 1.2.3. Retos y consideraciones del CIA en sistemas impulsados por Inteligencia Artificial
- 1.3. Uso de ChatGPT para análisis de riesgos y escenarios de amenaza
 - 1.3.1. Fundamentos de análisis de riesgos en Ciberseguridad
 - 1.3.2. Capacidad de ChatGPT para identificar y evaluar escenarios de amenaza
 - 1.3.3. Beneficios y limitaciones del análisis de riesgos con Inteligencia Artificial
- 1.4. ChatGPT en la detección de vulnerabilidades críticas
 - 1.4.1. Principios de detección de vulnerabilidades en sistemas de información
 - 1.4.2. Funcionalidades de ChatGPT para apoyar en la detección de vulnerabilidades
 - 1.4.3. Consideraciones éticas y de seguridad al usar Inteligencia Artificial en detección de fallos
- 1.5. Análisis de *malware* y *ransomware* asistido por Inteligencia Artificial
 - 1.5.1. Principios básicos del análisis de *malware* y *ransomware*
 - 1.5.2. Técnicas de Inteligencia Artificial aplicadas en la identificación de código malicioso
 - 1.5.3. Desafíos técnicos y operacionales en el análisis de *malware* asistido por Inteligencia Artificial
- 1.6. Identificación de ataques comunes con Inteligencia Artificial: *phishing*, ingeniería social y explotación
 - 1.6.1. Clasificación de ataques: *phishing*, ingeniería social y explotación
 - 1.6.2. Técnicas de Inteligencia Artificial para la identificación y análisis de ataques comunes
 - 1.6.3. Dificultades y limitaciones de los modelos de Inteligencia Artificial en detección de ataques
- 1.7. ChatGPT en la capacitación y simulación de amenazas cibernéticas
 - 1.7.1. Fundamentos de la simulación de amenazas para formación en Ciberseguridad
 - 1.7.2. Capacidades de ChatGPT para diseñar escenarios de simulación
 - 1.7.3. Beneficios de la simulación de amenazas como herramienta de capacitación
- 1.8. Políticas de seguridad cibernética con recomendaciones de Inteligencia Artificial
 - 1.8.1. Principios para la formulación de políticas de seguridad cibernética
 - 1.8.2. Rol de la Inteligencia Artificial en la generación de recomendaciones de seguridad
 - 1.8.3. Componentes clave en políticas de seguridad orientadas a Inteligencia Artificial
- 1.9. Seguridad en dispositivos IoT y el papel de la Inteligencia Artificial
 - 1.9.1. Fundamentos de la seguridad en el Internet de las Cosas (IoT)
 - 1.9.2. Capacidades de la Inteligencia Artificial para mitigar vulnerabilidades en dispositivos IoT
 - 1.9.3. Desafíos y consideraciones específicas de Inteligencia Artificial para la seguridad de IoT
- 1.10. Evaluación de amenazas y respuestas asistidas por herramientas de Inteligencia Artificial
 - 1.10.1. Principios de evaluación de amenazas en Ciberseguridad
 - 1.10.2. Características de las respuestas automatizadas mediante Inteligencia Artificial
 - 1.10.3. Factores críticos en la efectividad de respuestas cibernéticas con Inteligencia Artificial

Módulo 2. Detección y prevención de intrusiones usando modelos de Inteligencia Artificial Generativa

- 2.1. Fundamentos de sistemas IDS/IPS y el papel de la Inteligencia Artificial
 - 2.1.1. Definición y principios básicos de los sistemas IDS e IPS
 - 2.1.2. Principales tipos y configuraciones de IDS/IPS
 - 2.1.3. Contribución de la Inteligencia Artificial en la evolución de los sistemas de detección y prevención
- 2.2. Uso de Gemini para detección de anomalías en redes
 - 2.2.1. Conceptos y tipos de anomalías en el tráfico de red
 - 2.2.2. Características de Gemini para el análisis de datos de red
 - 2.2.3. Beneficios de la detección de anomalías en la prevención de intrusiones
- 2.3. Gemini y la identificación de patrones de intrusión
 - 2.3.1. Principios de identificación y clasificación de patrones de intrusión
 - 2.3.2. Técnicas de Inteligencia Artificial aplicadas en la detección de patrones de amenazas
 - 2.3.3. Tipos de patrones y comportamiento anómalo en seguridad de redes
- 2.4. Aplicación de modelos generativos en la simulación de ataques
 - 2.4.1. Fundamentos de los modelos generativos en Inteligencia Artificial
 - 2.4.2. Uso de modelos generativos para recrear escenarios de ataque
 - 2.4.3. Ventajas y limitaciones en la simulación de ataques mediante Inteligencia Artificial generativa
- 2.5. *Clustering* y clasificación de eventos usando Inteligencia Artificial
 - 2.5.1. Fundamentos del *clustering* y clasificación en la detección de intrusiones
 - 2.5.2. Algoritmos comunes de *clustering* aplicados en Ciberseguridad
 - 2.5.3. Papel de la Inteligencia Artificial en la mejora de los métodos de clasificación de eventos
- 2.6. Gemini en la generación de perfiles de comportamiento
 - 2.6.1. Conceptos de perfilamiento de usuarios y dispositivos
 - 2.6.2. Aplicación de modelos generativos en la creación de perfiles
 - 2.6.3. Ventajas de los perfiles de comportamiento en la detección de amenazas
- 2.7. Análisis de *Big Data* para la prevención de intrusiones
 - 2.7.1. Importancia del *Big Data* en la detección de patrones de seguridad
 - 2.7.2. Métodos de procesamiento de grandes volúmenes de datos en Ciberseguridad
 - 2.7.3. Aplicaciones de Inteligencia Artificial en el análisis y prevención basados en *Big Data*
- 2.8. Reducción de datos y selección de características relevantes con Inteligencia Artificial
 - 2.8.1. Principios de reducción de dimensionalidad en grandes volúmenes de datos
 - 2.8.2. Selección de características para mejorar la eficiencia de análisis de Inteligencia Artificial
 - 2.8.3. Técnicas de reducción de datos aplicadas en Ciberseguridad
- 2.9. Evaluación de modelos de Inteligencia Artificial en detección de intrusos
 - 2.9.1. Criterios de evaluación de modelos de Inteligencia Artificial en Ciberseguridad
 - 2.9.2. Indicadores de rendimiento y precisión de los modelos
 - 2.9.3. Importancia de la validación y evaluación constante en la Inteligencia Artificial
- 2.10. Implementación de un sistema de detección de intrusos potenciado con Inteligencia Artificial generativa
 - 2.10.1. Conceptos básicos de implementación de sistemas de detección de intrusos
 - 2.10.2. Integración de Inteligencia Artificial generativa en los sistemas IDS/IPS
 - 2.10.3. Aspectos clave para la configuración y mantenimiento de sistemas basados en Inteligencia Artificial

Módulo 3. Modelos predictivos de defensa proactiva en Ciberseguridad usando ChatGPT

- 3.1. Análisis predictivo en Ciberseguridad: técnicas y aplicaciones con Inteligencia Artificial
 - 3.1.1. Conceptos básicos de análisis predictivo en seguridad
 - 3.1.2. Técnicas de predicción en el ámbito de Ciberseguridad
 - 3.1.3. Aplicación de Inteligencia Artificial en la anticipación de ciberamenazas
- 3.2. Modelos de regresión y clasificación con soporte de ChatGPT
 - 3.2.1. Principios de regresión y clasificación en predicción de amenazas
 - 3.2.2. Tipos de modelos de clasificación en Ciberseguridad
 - 3.2.3. Asistencia de ChatGPT en la interpretación de modelos predictivos
- 3.3. Identificación de amenazas emergentes con predicciones de ChatGPT
 - 3.3.1. Conceptos de detección de amenazas emergentes
 - 3.3.2. Técnicas de identificación de nuevos patrones de ataque
 - 3.3.3. Limitaciones y precauciones en la predicción de nuevas amenazas
- 3.4. Redes neuronales para anticipación de ataques cibernéticos
 - 3.4.1. Fundamentos de redes neuronales aplicadas en Ciberseguridad
 - 3.4.2. Arquitecturas comunes para detección y predicción de ataques
 - 3.4.3. Desafíos en la implementación de redes neuronales en defensa cibernética
- 3.5. Uso de ChatGPT para simulaciones de escenarios de amenaza
 - 3.5.1. Conceptos básicos de simulación de amenazas en Ciberseguridad
 - 3.5.2. Capacidades de ChatGPT para desarrollar simulaciones predictivas
 - 3.5.3. Factores a considerar en el diseño de escenarios simulados
- 3.6. Algoritmos de aprendizaje por refuerzo para optimización de defensas
 - 3.6.1. Introducción al aprendizaje por refuerzo en Ciberseguridad
 - 3.6.2. Algoritmos de refuerzo aplicados a estrategias de defensa
 - 3.6.3. Beneficios y retos del aprendizaje por refuerzo en entornos de Ciberseguridad
- 3.7. Simulación de amenazas y respuestas con ChatGPT
 - 3.7.1. Principios de simulación de amenazas y su relevancia en ciberdefensa
 - 3.7.2. Respuestas automatizadas y optimizadas ante ataques simulados
 - 3.7.3. Beneficios de la simulación para mejorar la preparación cibernética



- 3.8. Evaluación de precisión y efectividad en modelos predictivos de Inteligencia Artificial
 - 3.8.1. Indicadores clave para la evaluación de modelos predictivos
 - 3.8.2. Metodologías de evaluación de precisión en modelos de Ciberseguridad
 - 3.8.3. Factores críticos en la efectividad de los modelos de Inteligencia Artificial en Ciberseguridad
- 3.9. Inteligencia Artificial en la gestión de incidentes y respuestas automatizadas
 - 3.9.1. Fundamentos de la gestión de incidentes en Ciberseguridad
 - 3.9.2. Rol de la Inteligencia Artificial en la toma de decisiones en tiempo real
 - 3.9.3. Desafíos y oportunidades en la automatización de respuestas
- 3.10. Creación de un sistema de defensa predictivo con soporte de ChatGPT
 - 3.10.1. Principios de diseño de sistemas de defensa proactiva
 - 3.10.2. Integración de modelos predictivos en entornos de Ciberseguridad
 - 3.10.3. Componentes clave para un sistema de defensa predictivo basado en Inteligencia Artificial

“

Manejarás software de vanguardia como TensorFlow para entrenar modelos de aprendizaje automático que fortalezcan las soluciones de Ciberseguridad en los distintos entornos organizacionales”



04

Objetivos docentes

A través de este programa universitario, los profesionales adquirirán las competencias avanzadas para dirigir estrategias de Ciberseguridad en entornos tecnológicos avanzados de forma exitosa. Mediante un enfoque práctico, desarrollarán habilidades fundamentales para implementar sistemas de detección, evaluar riesgos y crear defensas proactivas apoyadas en Inteligencia Artificial, fortaleciendo su capacidad para proteger infraestructuras digitales y responder eficientemente ante las amenazas cibernéticas emergentes.

A hand is shown interacting with a digital interface. The interface features a grid of blue lines and various data points, including numbers like 1, 2, 3, 5, 6, 8, and 9. A blue button with the word "NODE" is visible in the bottom right corner. The background is a mix of white and blue geometric shapes.

NODE

“

Obtendrás competencias avanzadas en la detección de intrusiones y análisis predictivo para liderar estrategias de defensa proactiva en entornos digitales”



Objetivos generales

- ♦ Analizar las principales amenazas cibernéticas modernas y su evolución en el contexto de la Inteligencia Artificial
- ♦ Identificar patrones anómalos en sistemas digitales mediante el uso de herramientas avanzadas de Inteligencia Artificial
- ♦ Desarrollar estrategias de detección y prevención de intrusiones utilizando modelos generativos y predictivos
- ♦ Implementar sistemas de defensa proactiva basados en técnicas de análisis predictivo y aprendizaje automático
- ♦ Diseñar simulaciones de ciberataques para evaluar vulnerabilidades y optimizar las defensas
- ♦ Aplicar algoritmos de Inteligencia Artificial en la gestión de incidentes y respuestas automatizadas
- ♦ Optimizar la seguridad en dispositivos conectados mediante la mitigación de riesgos específicos del Internet de las Cosas
- ♦ Evaluar la efectividad y precisión de los modelos de Inteligencia Artificial aplicados a la Ciberseguridad
- ♦ Desarrollar políticas de seguridad cibernética fundamentadas en recomendaciones basadas en Inteligencia Artificial
- ♦ Fomentar el uso ético y responsable de la Inteligencia Artificial en la protección de sistemas y datos





Objetivos específicos

Módulo 1. 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 2. 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 3. 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

05

Salidas profesionales

Tras finalizar este Experto Universitario de TECH, los profesionales estarán altamente capacitados para asumir roles fundamentales como Analista de Ciberseguridad, Especialista en Detección de Amenazas, Consultor en Sistemas de Defensa Proactiva o Experto en Protección de Infraestructuras Digitales. Además, su enfoque en el uso de la Inteligencia Artificial aplicada les permitirá liderar proyectos innovadores en entornos corporativos, gubernamentales y tecnológicos avanzados.



“

¿Buscas ejercitarte como Chief Information Security Officer? Lógralo mediante este programa universitario en tan solo meses”

Perfil del egresado

El egresado de esta titulación universitaria será un profesional altamente cualificado para abordar los retos de la seguridad digital actual. Con conocimientos avanzados en Inteligencia Artificial, estará preparado para crear estrategias de protección, implementar sistemas para la detección de amenazas y gestionar incidentes en tiempo real. Su dominio de herramientas innovadoras y su enfoque ético lo convertirán en un experto capaz de salvaguardar infraestructuras críticas y liderar proyectos en entornos tecnológicos sofisticados.

Brindarás un asesoramiento integral a las organizaciones sobre la integración de sistemas inteligentes para fortalecer sus infraestructuras digitales.

- ♦ **Adaptabilidad tecnológica:** Habilidad para incorporar de manera eficiente nuevas herramientas, técnicas y metodologías basadas en Inteligencia Artificial, adaptándose rápidamente a los avances tecnológicos y aplicándolos en diversos entornos laborales con altos estándares de exigencia
- ♦ **Comunicación efectiva:** Competencia para expresar ideas, resultados y estrategias de manera clara y estructurada, adaptando el lenguaje técnico para que sea comprensible tanto por equipos multidisciplinares como por audiencias no especializadas en el ámbito tecnológico
- ♦ **Gestión de proyectos:** Capacidad para planificar, organizar y coordinar proyectos de ciberseguridad, supervisando la implementación de soluciones y garantizando el cumplimiento de plazos, recursos y objetivos estratégicos en contextos dinámicos y cambiantes
- ♦ **Colaboración interdisciplinaria:** Habilidad para trabajar de manera efectiva con equipos diversos, integrando conocimientos y perspectivas de áreas como Ciberseguridad, Inteligencia Artificial, tecnología y gestión empresarial, con el fin de alcanzar objetivos comunes y generar soluciones integrales





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

- 1. Analista de Ciberseguridad Especializado en Inteligencia Artificial:** Encargado de identificar vulnerabilidades y amenazas en sistemas digitales mediante el uso de herramientas avanzadas de Inteligencia Artificial para proteger redes y datos críticos.
- 2. Especialista en Detección de Intrusiones en Sistemas:** Responsable de implementar y gestionar sistemas de detección de intrusiones potenciados con Inteligencia Artificial para evitar accesos no autorizados en infraestructuras digitales.
- 3. Consultor en Seguridad de Dispositivos Conectados:** Encargado de mitigar riesgos asociados a dispositivos del Internet de las Cosas, garantizando su seguridad en entornos empresariales y domésticos.
- 4. Especialista en Análisis Predictivo de Ciberamenazas:** Se centra en anticipar posibles ataques mediante la aplicación de modelos predictivos y técnicas de aprendizaje automático.
- 5. Analista de Respuesta a Incidentes con Inteligencia Artificial:** Encargado de gestionar y automatizar la respuesta ante incidentes cibernéticos utilizando herramientas de Inteligencia Artificial.
- 6. Auditor de Vulnerabilidades Asistido por Inteligencia Artificial:** Responsable de evaluar sistemas digitales para detectar fallos de seguridad y proponer soluciones efectivas con el soporte de herramientas de Inteligencia Artificial.

“

Diseñarás soluciones avanzadas de Ciberseguridad basadas en Inteligencia Artificial para detectar y prevenir amenazas cibernéticas”

06

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 intenso 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 según el índice global score, 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.



07

Cuadro docente

La premisa fundamental de TECH consiste en proporcionar las titulaciones universitarias más completas y renovadas del panorama académico, por lo que selecciona con rigurosidad sus claustros docentes. Para el diseño e impartición de este Experto Universitario, ha reunido a los especialistas más destacados en el campo del Análisis y Detección de Amenazas de Ciberseguridad con Inteligencia Artificial. Así pues, han elaborado diversos contenidos didácticos que sobresalen por su excelsa calidad y por ajustarse a los requerimientos del mercado laboral. De esta forma, los alumnos se adentrarán en una experiencia de alta intensidad que ampliará sus horizontes profesionales considerablemente.



“

Un experimentado grupo docente, altamente especializado en el uso de Inteligencia Artificial en Ciberseguridad, te guiará durante todo el proceso de aprendizaje y resolverá las dudas que puedan surgirse”

Dirección



Dr. Peralta Martín-Palomino, Arturo

- ♦ CEO y CTO en Prometheus 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



Una experiencia de capacitación única, clave y decisiva para impulsar tu desarrollo profesional”

08

Titulación

El Experto Universitario en Análisis y Detección de Amenazas de Ciberseguridad con Inteligencia Artificial garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Experto Universitario expedido por TECH Universidad.



“

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

Este **Experto Universitario en Análisis y Detección de Amenazas de Ciberseguridad con Inteligencia Artificial** contiene el programa científico más completo y actualizado del mercado.

Tras la superación de la evaluación, el alumno recibirá por correo postal* con acuse de recibo su correspondiente título de **Experto Universitario** emitido por **TECH Universidad**.

Este título expedido por **TECH Universidad** expresará la calificación que haya obtenido en el Experto Universitario, y reunirá los requisitos comúnmente exigidos por las bolsas de trabajo, oposiciones y comités evaluadores de carreras profesionales.

Título: **Experto Universitario en Análisis y Detección de Amenazas de Ciberseguridad con Inteligencia Artificial**

Modalidad: **No escolarizada (100% en línea)**

Duración: **6 meses**



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



Experto Universitario
Análisis y Detección de
Amenazas de Ciberseguridad
con Inteligencia Artificial

- » Modalidad: No escolarizada (100% en línea)
- » Duración: 6 meses
- » Titulación: TECH Universidad
- » Horario: a tu ritmo
- » Exámenes: online

Experto Universitario

Análisis y Detección de Amenazas de Ciberseguridad con Inteligencia Artificial

```
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000
```