Seminarios sobre Inteligencia Artificial y Ciberseguridad

IA confiable, generativa y aplicada a la ciberseguridad: formación avanzada para profesionales en activo

Organiza:

DASCI
Instituto Andaluz Interuniversitario en Ciencia de Datos e Inteligencia Computacional

Cámara Granada

Proyecto Estratégico IAFER CiB

Inteligencia Artificial Ética, Responsable y de Propósito General para Ciberseguridad

Financia:

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales

Plan de Recuperación, Transformación y Resiliencia

incibe_ Instituto Nacional de Ciberseguridad

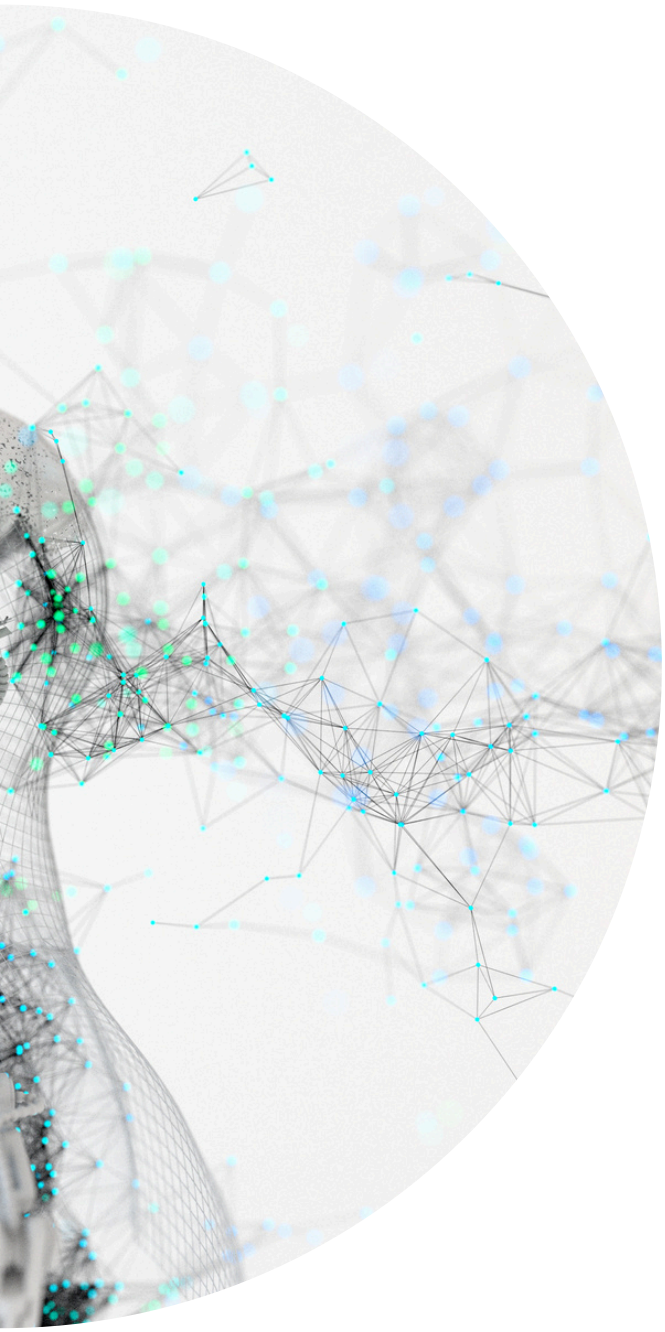
Universidad de Granada

Contacto de coordinación:
Alberto Fernández (DASCI – UGR)
alberto@decsai.ugr.es
Edificio UGR IA Av. del Conocimiento, 37, 18016 Granada, 1ª planta, despacho 1
https://dasci.es

Esta actividad es parte del **Proyecto Estratégico "Inteligencia artificial ética, responsable y de propósito general para ciberseguridad" IAFER-Cib (C074/23)**, fruto del convenio de colaboración suscrito entre el Instituto Nacional de Ciberseguridad (INCIBE) y la Universidad de Granada. Esta iniciativa se lleva a cabo en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea-Next Generation EU.

Seminarios sobre Inteligencia Artificial y Ciberseguridad

Proyecto Estratégico IAFER - CiB



Inicio: 8 de julio de 2025
Fin: 28 de noviembre de 2025
Duración: 51h. - 17 sesiones (julio a noviembre, repartidas por módulos temáticos)
Horario: 10:00 - 13:00
Lugar: Sala Pioneras Informáticas - Edificio UGR AI

Seminario IA Fiable.
Responsabilidad y Gobernanza

Seminario IA Generativa.
Uso Seguro

Seminario Privacidad y Seguridad
de Datos e IA

Seminario IA aplicada
a Ciberseguridad

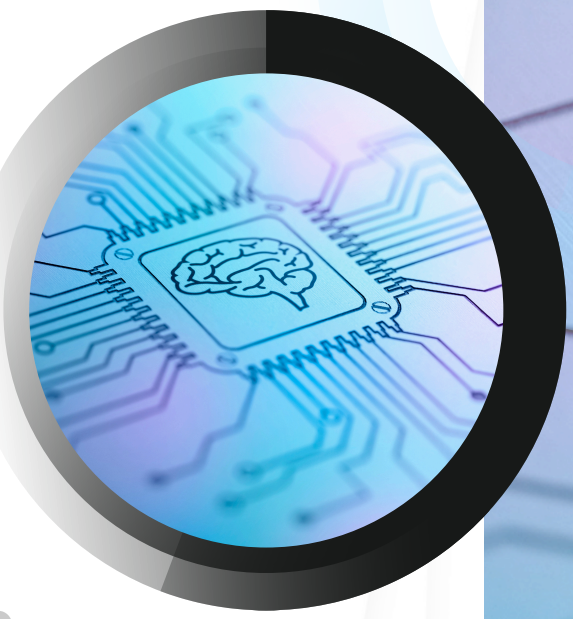
Seminario IA Fiable.
Responsabilidad y Gobernanza

01 Resumen del seminario:

Este seminario está diseñado para proporcionar a los profesionales del sector tecnológico el conocimiento esencial sobre la Inteligencia Artificial confiable y responsable, una de las áreas más críticas en la evolución tecnológica actual. A lo largo de cuatro módulos, se explorarán los requisitos de una IA fiable, su explicabilidad y los marcos regulatorios que guían su uso responsable.

Los participantes aprenderán a manejar iniciativas internacionales de regulación, entenderán la importancia de la auditabilidad y la responsabilidad en los sistemas de IA, y se adentrarán en la IA explicable (XAI), para garantizar transparencia y confianza en modelos predictivos.

Además, se abordarán los aspectos éticos de la IA, como el alineamiento de modelos y la imparcialidad en los datos y algoritmos, garantizando que los profesionales estén preparados para identificar y mitigar sesgos. Todo ello, complementado con laboratorios prácticos que permitirán aplicar los conocimientos adquiridos en casos reales de la industria.



02 Contenido tentativo:

Módulo 1: ¿Qué es y por qué es necesaria la IA fiable?: Impacto en la toma de decisiones empresariales.

Módulo 2: Regulación y Gobernanza de la IA: Cumplimiento normativo en la práctica.

Módulo 3: Ética y Tecnología: Principios en Inteligencia Artificial.

Módulo 4: Inteligencia Artificial Explicable (XAI): Uso de herramientas accesibles.

4 semanas, 12 horas.
08-11-15-18 de julio de 10:00 a 13:00 en Sala Pioneras Informáticas - Edificio UGR AI

03 Profesorado implicado:

- Francisco Herrera (Módulo 1)
- Alfonso Peralta (Módulo 2)
- Alberto Fernández (Módulo 3)
- Iván Sevillano (Módulo 4)

Seminario IA Generativa.
Uso Seguro

01 Resumen del seminario:

Este seminario está diseñado para proporcionar a los profesionales un conocimiento profundo sobre la Inteligencia Artificial Generativa (IAG) y su uso seguro en aplicaciones prácticas. A lo largo de seis módulos, los participantes explorarán desde los fundamentos de la IAG hasta su aplicación en el diseño de imágenes y la optimización de modelos generativos, abriendo nuevas posibilidades para innovar en sus proyectos y productos.

El seminario abordará cómo herramientas avanzadas de IA generativa, en particular los grandes modelos de lenguaje (Large Language Models o LLMs en inglés) están transformando la creación de contenido y otros procesos empresariales. Además, se profundizará en la adaptación y personalización de los modelos generativos, enseñando cómo ajustarlos y optimizarlos para satisfacer necesidades específicas del negocio. Se tratarán también los desafíos de la IA generativa, como la mejora en la automatización de tareas, la personalización de productos y la generación de contenido, con un enfoque aplicable a la mejora de procesos empresariales. Finalmente, se explorarán prácticas de seguridad para garantizar la robustez de los LLMs y su correcta implementación en entornos de trabajo.

Durante el seminario, los participantes podrán realizar ejercicios prácticos sobre la generación de contenido, optimización de modelos generativos y aplicación de la IA generativa en diferentes áreas de negocio, desde la automatización de informes hasta la creación de productos personalizados.

02 Contenido tentativo:

Módulo 1: Introducción a la IA Generativa y sus fundamentos: ejemplos de uso práctico.

Módulo 2: IA Generativa en el diseño de imagen: personalización de contenido.

Módulo 3: Adaptación y aplicación de Modelos de Lenguaje: creación, personalización y optimización.

Módulo 4: Desafíos de la IA Generativa.

Módulo 5: Seguridad y robustez en LLMs: buenas prácticas.

03 Profesorado implicado:

- Pedro Manuel Martínez (Módulo 1)
- Guillermo Gómez (Módulo 2)
- Carlos Peláez (Módulo 3)
- Francisco Herrera (Módulo 4)
- Cristina Zuheros (Módulo 5)

4 semanas, 15 horas.
12-19-26 de septiembre; 02-03 de octubre de 10:00 a 13:00 en Sala Pioneras Informáticas - Edificio UGR AI

Seminario Privacidad y Seguridad de Datos e IA

01 Resumen del seminario:

Este seminario ofrece un enfoque integral sobre los aspectos fundamentales de la privacidad y la seguridad de los datos en el contexto de la Inteligencia Artificial. A lo largo de cuatro módulos, los participantes aprenderán a proteger los datos personales y asegurar los modelos de IA, explorando desde los fundamentos legales y estrategias de privacidad hasta el uso de enfoques avanzados como el aprendizaje federado y el denominado como Data Centric AI (asegurar la calidad de los datos).

Los profesionales adquirirán habilidades clave para implementar tecnologías seguras, entender los desafíos legales y éticas en la IA, y aplicar prácticas innovadoras para proteger la privacidad y la seguridad en un mundo interconectado. Con ejemplos prácticos, casos de estudio y un enfoque holístico, el seminario prepara a los participantes para enfrentar los desafíos actuales y futuros de la IA responsable.

02 Contenido tentativo:

Módulo 1: Privacidad en la era de la IA: Cómo garantizar la protección de datos.

Módulo 2: Cumplimiento Normativo y Responsabilidad en la Protección de Datos.

Módulo 3: Data Centric AI: Ejemplos prácticos.

Módulo 4: Aprendizaje Federado: Privacidad, eficiencia y aplicaciones.

03 Profesorado implicado:

- Ricard Martínez (Módulo 1)
- Guillermo Hidalgo (Módulo 2)
- Julián Luengo (Módulo 3)
- Nuria Rodríguez (Módulo 4)

4 semanas, 12 horas.
10-17-24-31 de octubre de 10:00 a 13:00 en Sala Pioneras Informáticas - Edificio UGR AI

Seminario IA aplicada a Ciberseguridad

01 Resumen del seminario:

En un contexto donde las amenazas cibernéticas evolucionan constantemente, la inteligencia artificial (IA) se ha convertido en una herramienta esencial para fortalecer las capacidades de detección, respuesta y mitigación de incidentes. Este seminario proporciona una visión integral sobre la aplicación de IA en el ámbito de la ciberseguridad, explorando técnicas avanzadas utilizadas en la monitorización de redes, detección de malware, desarrollo seguro de software y automatización de respuestas ante incidentes.

A lo largo de cuatro módulos, los participantes aprenderán cómo la IA se aplica en herramientas de seguridad como los sistemas de gestión de información y eventos de seguridad (SIEM), los sistemas de detección y respuesta en endpoints (EDR) y las soluciones inteligentes de detección de intrusos. Además, se abordarán estrategias para el análisis y mitigación de amenazas emergentes, así como la implementación de IA en la detección automatizada de vulnerabilidades y el desarrollo seguro de código.
Este seminario está diseñado para proporcionar una introducción práctica a la intersección entre la inteligencia artificial (IA) y la ciberseguridad, permitiendo a los participantes adquirir conocimientos aplicables a entornos reales de seguridad informática.

02 Contenido tentativo:

Módulo 1: Fundamentos de Ciberseguridad.

Módulo 2: Detección y análisis de ciberamenazas.

Módulo 3: Malware, detección y respuesta basada en IA.

Módulo 4: Inteligencia artificial aplicada al desarrollo seguro de código

03 Profesorado implicado:

- Pedro García Teodoro (Módulo 1)
- Roberto Magán Carrión (Módulo 2)
- José Antonio Gómez Hernández (Módulo 3)
- Rafa Alejandro Rodríguez Gómez (Módulo 4)

4 semanas, 12 horas.
07-14-21-28 de noviembre de 10:00 a 13:00 en Sala Pioneras Informáticas - Edificio UGR AI

Docentes

Francisco Herrera

Francisco Herrera se licenció en Matemáticas en la Universidad de Granada en 1986, donde también se doctoró cinco años más tarde en Inteligencia Artificial. Es catedrático de Ciencias de la Computación e Inteligencia Artificial de la Universidad de Granada y director del Instituto Interuniversitario Andaluz en Data Science and Computational Intelligence (DaSCI), consorcio formado por la universidad granadina y las Universidades de Jaén y Córdoba. Desde 2020 es miembro del Consejo Asesor de Inteligencia Artificial del Gobierno de España.

Ricard Martínez

Ricard Martínez Martínez es Director de la Cátedra de Privacidad y Transformación Digital. Universidad Politécnica de Valencia. Es profesor de Derecho Constitucional y director de la Cátedra de privacidad y Transformación Digital Microsoft-Universitat de Valencia. Su doctorado en Derecho en la Universitat de València dedicado al estudio del derecho fundamental a la protección de datos mereció el Premio Extraordinario de Doctorado.

Alberto Fernández

Alberto Fernández Hilario es profesor Catedrático de Universidad en la UGR desde Julio de 2023. Su labor de investigación se centra en las áreas de Data Science, Big Data, Computational Intelligence, Ética y Confiabilidad en la Inteligencia Artificial, y problemas singulares en aprendizaje supervisado, siempre desde enfoque interdisciplinar, aplicado y orientado a los problemas.

Pedro García

Pedro García Teodoro es Catedrático de Ingeniería Telemática en la Universidad de Granada. Su labor docente e investigadora se enfoca en el campo de las redes y las comunicaciones, en particular en el ámbito de la seguridad en redes y sistemas.

Docentes

Julián Luengo

Julián Luengo Martín es Profesor Catedrático de Universidad en el Departamento de Ciencias de la Computación e Inteligencia Artificial de la Universidad de Granada (UGR). Su labor investigadora se centra en la Ciencia de Datos, la Inteligencia Computacional y el Preprocesamiento de Datos, con especial énfasis en la imputación de valores perdidos, la clasificación supervisada y la detección de anomalías en entornos de Big Data.

Alfonso Peralta

Alfonso Peralta Gutiérrez es Magistrado español experto en “digital law” y distintas ramas del derecho tecnológico como proceso judicial tecnológico, justicia predictiva, ciberseguridad, cibercrimen, inteligencia artificial, redes sociales o TICs.

Guillermo Hidalgo

Guillermo Hidalgo es Abogado con más de 11 años de experiencia en la práctica del Ciberderecho. En la actualidad es Counsel y responsable de la práctica de Ciberderecho en MAIO LEGAL (Madrid).

José Antonio Gómez

José Antonio Gómez Hernández, es Profesor Titular de Universidad en el Departamento de Lenguajes y Sistemas Informáticos de la Universidad de Granada (UGR). Su labor investigadora se centra en la seguridad de sistemas operativos, la ciberseguridad y la informática forense, con especial énfasis en la protección de dispositivos móviles y la detección de ransomware.

Docentes

Rafael A. Rodríguez-Gómez

Rafael A. Rodríguez-Gómez es Analista de Seguridad en RTI (Real-Time Innovations), donde trabaja en el equipo Connext Security. Anteriormente, ejerció como Profesor Permanente Laboral en el Departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada, España, y fue miembro del grupo de investigación Network Security and Engineering Group (NESG) de dicha universidad.

Roberto Magán

Roberto Magán Carrión es Profesor Permanente Laboral en la UGR desde abril de 2024. Durante su carrera investigadora ha propuesto una amplia variedad de soluciones para la monitorización, detección, reacción y mitigación de ataques a la seguridad en sistemas y comunicaciones en diferentes escenarios y entornos.

Pedro Manuel Martínez

Pedro Manuel Martínez Jiménez es Profesor Titular de Universidad del departamento de Lenguajes y Sistemas Informáticos de la Universidad de Granada. Su investigación principal se desarrolla en el ámbito de la visión por computador, centrándose en el modelado de la percepción humana y la descripción semántica de las características de bajo y medio nivel de la imagen.

Cristina Zuheros

Cristina Zuheros Montes es Profesora Sustituta Interina en el Departamento de Ciencias de la Computación e Inteligencia Artificial de la Universidad de Granada (UGR). Su labor investigadora se centra en la Inteligencia Artificial, con especial énfasis en el procesamiento del lenguaje natural, la toma de decisiones multiclase y la minería de datos en redes sociales.

Docentes

Nuria Rodríguez-Barroso

Nuria Rodríguez-Barroso es doctora en Informática e Inteligencia Artificial por la Universidad de Granada, España. Actualmente trabaja en el Instituto Andaluz de Investigación en Ciencia de Datos e Inteligencia Computacional (DaSCI), donde se centra principalmente en el aprendizaje federado.

Guillermo Gómez-Trenado

Guillermo Gómez-Trenado es doctor en Informática e Inteligencia Artificial por la Universidad de Granada, España. Actualmente trabaja en Panacea Cooperative Research y colabora con la Universidad de Granada, centrándose principalmente en la IA generativa.

Iván Sevillano

Iván Sevillano García es un joven investigador predoctoral en la Universidad de Granada, vinculado al Instituto de Investigación DASCI desde 2020. Su línea de investigación abarca Ciencia de Datos, Big Data e Inteligencia Artificial explicable, con foco especialmente en métricas de calidad explicativa para modelos complejos.

Carlos Peláez

Carlos Peláez González es investigador predoctoral en el Instituto Andaluz de Ciencia de Datos e Inteligencia Computacional (DaSCI), desarrollando su labor en la Universidad de Granada. Su investigación se centra en la evaluación de la seguridad ética de los modelos generativos de lenguaje, con especial atención a los sesgos presentes en los mismos, un área de creciente relevancia en la Inteligencia Artificial actual.

Organiza:

DASCI
Instituto Andaluz Interuniversitario en Ciencia de Datos e Inteligencia Computacional

Cámara Granada

Proyecto Estratégico IAFER CiB

Inteligencia Artificial Ética, Responsable y de Propósito General para Ciberseguridad

Financia:

Financiado por la Unión Europea NextGenerationEU

Gobierno de España — Ministerio para la Transformación Digital y de la Función Pública — Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales

Plan de Recuperación, Transformación y Resiliencia

incibe_ Instituto Nacional de Ciberseguridad

Universidad de Granada