4. Planificación de las enseñanzas

Código del plan de estudios:

4.1 Estructura básica de las enseñanzas

Tipos de materia		Nº créditos ECTS
Ob	**Obligatorias**	45
Op	**Optativas**	0
PE	**Prácticas Externas**	0
TFM	**Trabajo Fin de Máster (obligatorio en Máster)**	15
	Créditos totales	60

4.2 Organización temporal de las asignaturas

PRIMER CURSO

PRIMER CUATRIMESTRE				
Código	**Asignatura**	**Tipo**	**ECTS**	**Curso**
	Análisis Predictivo de Riesgos y Resiliencia Organizacional	Obligatoria(OB)	3	Primero
	Aplicaciones de IA en Ciberseguridad	Obligatoria(OB)	6	Primero
	IA en Seguridad Urbana y Ciudades Inteligentes	Obligatoria(OB)	3	Primero
	IA para Inteligencia y Seguridad Nacional	Obligatoria(OB)	6	Primero
	IA y Protección de Datos Personales	Obligatoria(OB)	3	Primero
	Inteligencia Artificial y Machine Learning en la Seguridad	Obligatoria(OB)	3	Primero
	Seguridad Digital y Ciberamenazas	Obligatoria(OB)	3	Primero
	Seguridad Física Inteligente y Videovigilancia con IA	Obligatoria(OB)	3	Primero
Total ECTS			**30**	

SEGUNDO CUATRIMESTRE				
Código	**Asignatura**	**Tipo**	**ECTS**	**Curso**
	Evaluación de Impacto Algorítmico y Gestión del Ciclo de Vida de Modelos de IA	Obligatoria(OB)	3	Primero
	Gobernanza de la IA y Ética en Entornos de Seguridad	Obligatoria(OB)	3	Primero
	Infraestructuras Críticas y Sistemas Ciberfísicos con IA	Obligatoria(OB)	6	Primero
	Sistemas Autónomos y Detección de Amenazas Emergentes	Obligatoria(OB)	3	Primero
	Trabajo Fin de Máster	Trabajo Fin de Título (TFT)	15	Primero
Total ECTS			**30**	

ANUALES				
Código	**Asignatura**	**Tipo**	**ECTS**	**Curso**
Total ECTS			**0**	

SEGUNDO CURSO

PRIMER CUATRIMESTRE				
Código	**Asignatura**	**Tipo**	**ECTS**	**Curso**
Total ECTS			**0**	

SEGUNDO CUATRIMESTRE				
Código	**Asignatura**	**Tipo**	**ECTS**	**Curso**
Total ECTS			**0**	

ANUALES				
Código	**Asignatura**	**Tipo**	**ECTS**	**Curso**

Total ECTS	**0**	

TERCER CURSO

PRIMER CUATRIMESTRE				
Código	**Asignatura**	**Tipo**	**ECTS**	**Curso**
Total ECTS			**0**	

SEGUNDO CUATRIMESTRE				
Código	**Asignatura**	**Tipo**	**ECTS**	**Curso**
Total ECTS			**0**	

ANUALES				
Código	**Asignatura**	**Tipo**	**ECTS**	**Curso**
Total ECTS			**0**	

4.3 Estructura en base a itinerarios formativos (si los hubiese)

No procede.

4.4 Descripción detallada de las asignaturas

ASIGNATURAS PRIMER CURSO

Asignatura: Análisis Predictivo de Riesgos y Resiliencia Organizacional	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Esteban	Acuña	28641259	Externo	2
Esteban	Acuña	28641259	Externo	2
Francisco Luis	de Andres Pérez	22985661J	Externo	1
Francisco Luis	de Andres Pérez	22985661J	Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Analizar vulnerabilidades, ciberamenazas y riesgos mediante el uso de herramientas de inteligencia artificial y sistemas de respuesta automatizada.	COM-07
Habilidades o Destrezas (HD)	Aplicar modelos de análisis predictivo para la identificación temprana de riesgos y la mejora de la resiliencia organizacional.	HD-06
Competencias (COM)	Evaluar riesgos y tomar decisiones informadas mediante el análisis predictivo de datos y el uso de modelos de aprendizaje automático.	COM-03
Conocimientos o contenidos (C)	Comprender las metodologías de análisis predictivo, evaluación de riesgos y resiliencia organizacional en entornos complejos.	C-05

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75
Asistencia virtual a clase y participación en foros	Continua	25

Descripción de contenidos

Análisis predictivo: conceptos, objetivos y tipos de modelos. Modelado de amenazas y vulnerabilidades a partir de datos históricos y en tiempo real. Indicadores clave de riesgo (KRIs) y métricas de resiliencia. Aplicación de algoritmos de predicción en escenarios de crisis, fallos sistémicos o ciberataques. Monte Carlo, árboles de decisión, redes bayesianas. Sistemas de alerta temprana en seguridad organizacional y continuidad del negocio. Marcos de referencia: ISO 31000 (gestión de riesgos), ISO 22301 (continuidad del negocio), NIST SP 800-30.

Asignatura: Aplicaciones de IA en Ciberseguridad	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 6 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	N° Identificación	Interno/Externo	N° ECTS Impartidos
Giselle	Cragnolino	27282062	Externo	5
Giselle	Cragnolino	27282062	Externo	5
Francisco Luis	de Andres Pérez	22985661J	Externo	1
Francisco Luis	de Andres Pérez	22985661J	Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Comunicar de forma clara y rigurosa los resultados de análisis y proyectos de IA aplicada a la seguridad, tanto a públicos especializados como no especializados.	COM-04
Competencias (COM)	Analizar vulnerabilidades, ciberamenazas y riesgos mediante el uso de herramientas de inteligencia artificial y sistemas de respuesta automatizada.	COM-07
Conocimientos o contenidos (C)	Comprender los fundamentos de la inteligencia artificial, el aprendizaje automático y sus aplicaciones en la detección y prevención de amenazas.	C-01
Habilidades o Destrezas (HD)	Analizar soluciones de detección automatizada de intrusiones y anomalías mediante herramientas de IA.	HD-03

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75
Asistencia virtual a clase y participación en foros	Continua	25

Descripción de contenidos

Detección de intrusos con aprendizaje automático (IDS/IPS). Modelos supervisados y no supervisados para detección de anomalías. Clasificación automatizada de malware y spam con redes neuronales y árboles de decisión. Aplicación de NLP en el análisis de correos y mensajes sospechosos. Detección de phishing y fraude digital mediante clustering y análisis de comportamiento. Uso de IA generativa en la simulación de amenazas y pruebas de penetración (Red/Blue

Teams). Integración de modelos de IA en entornos SOC: casos de uso reales y herramientas disponibles. Falsos positivos, adversarial ML.

Asignatura: IA en Seguridad Urbana y Ciudades Inteligentes	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	N° Identificación	Interno/Externo	N° ECTS Impartidos
Katherine	Almeida Ramos	MM0205672	Externo	1
Katherine	Almeida Ramos	MM0205672	Externo	1
Nicolás	Wild	40750840	Externo	2
Nicolás	Wild	40750840	Externo	2

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Comunicar de forma clara y rigurosa los resultados de análisis y proyectos de IA aplicada a la seguridad, tanto a públicos especializados como no especializados.	COM-04
Competencias (COM)	Diseñar estrategias de vigilancia inteligente y análisis predictivo que contribuyan a la seguridad nacional, urbana y organizacional, promoviendo la resiliencia ante incidentes.	COM-09
Habilidades o Destrezas (HD)	Desarrollar estrategias de seguridad urbana basadas en datos e inteligencia artificial para entornos de smart cities.	HD-08
Conocimientos o contenidos (C)	Comprender las metodologías de análisis predictivo, evaluación de riesgos y resiliencia organizacional en entornos complejos.	COM-07

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Asistencia virtual a clase y participación en foros	Continua	25
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75

Descripción de contenidos

Conceptualización de ciudades inteligentes y sistemas urbanos de seguridad. Modelos predictivos para análisis del crimen y patrullaje proactivo. Videovigilancia urbana inteligente y sensores distribuidos integrados con IA. Análisis de flujos poblacionales y movilidad urbana a partir de datos en tiempo real. Sistemas de emergencia urbanos basados en IA: detección de incidentes, coordinación multiagencia, respuesta en tiempo real. Consideraciones éticas y legales del uso de IA en espacios urbanos.

Asignatura: IA para Inteligencia y Seguridad Nacional	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 6 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	N° Identificación	Interno/Externo	N° ECTS Impartidos
Natasa	Loizou	19033174	Externo	5
Natasa	Loizou	19033174	Externo	5
Katherine	Almeida Ramos	MM0205672	Externo	1
Katherine	Almeida Ramos	MM0205672	Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Diseñar estrategias de vigilancia inteligente y análisis predictivo que contribuyan a la seguridad nacional, urbana y organizacional, promoviendo la resiliencia ante incidentes.	COM-09
Competencias (COM)	Evaluar riesgos y tomar decisiones informadas mediante el análisis predictivo de datos y el uso de modelos de aprendizaje automático.	COM-03
Habilidades o Destrezas (HD)	Implementar soluciones de inteligencia artificial en contextos de seguridad nacional y defensa estratégica.	HD7
Conocimientos o contenidos (C)	Comprender los fundamentos de la gobernanza algorítmica, la transparencia y la responsabilidad en el uso de la IA aplicada a la seguridad.	C-06

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Asistencia virtual a clase y participación en foros	Continua	25
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75

Descripción de contenidos

Inteligencia estratégica y operativa en contextos nacionales y supranacionales. Recolección automatizada de información abierta (OSINT) mediante IA. Procesamiento de lenguaje natural (NLP) para el análisis de discursos ideológicos, redes sociales y señales débiles. Análisis de redes delictivas, terrorismo y crimen organizado con clustering y correlación multivariable. Modelos predictivos para generación de alertas tempranas y perfilamiento de amenazas.

Aplicaciones de IA en defensa nacional: vigilancia de fronteras, detección de actividades hostiles, apoyo a operaciones militares.

Asignatura: IA y Protección de Datos Personales	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	N° Identificación	Interno/Externo	N° ECTS Impartidos
Alicia	Rodríguez Sánchez	70903557P	Interno	1
Nicolás	Wild	40750840	Externo	2
Nicolás	Wild	40750840	Externo	2
José Luis	Domínguez Álvarez	71704654S	Interno	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Diseñar estrategias integrales de seguridad basadas en IA, incorporando criterios técnicos, éticos y normativos en su implementación.	COM-02
Conocimientos o contenidos (C)	Comprender los marcos normativos nacionales e internacionales en materia de protección de datos, ciberseguridad y ética algorítmica.	C-03
Competencias (COM)	Evaluar el cumplimiento de las normativas de protección de datos, privacidad y ética algorítmica en el uso de tecnologías de IA aplicadas a la seguridad.	COM-08
Habilidades o Destrezas (HD)	Implementar sistemas de IA que garanticen la privacidad y el cumplimiento de la normativa de protección de datos personales.	HD-04

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75
Asistencia virtual a clase y participación en foros	Continua	25

Descripción de contenidos

Principios fundamentales de protección de datos: licitud, finalidad, minimización, exactitud, conservación, integridad y confidencialidad. Aplicación del Reglamento General de Protección de Datos (RGPD/GDPR) en sistemas basados en IA. Evaluaciones de impacto en protección de datos (DPIA) y en algoritmos (AIA). Conceptos de “privacidad desde el

diseño” (Privacy by Design) y “por defecto”. Explicabilidad y transparencia en modelos automatizados (XAI). Nuevas regulaciones: propuesta de Reglamento de IA de la Unión Europea y su impacto en la seguridad.

Asignatura: Inteligencia Artificial y Machine Learning en la Seguridad	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	N° Identificación	Interno/Externo	N° ECTS Impartidos
David Santiago	Castillo	37195851	Externo	1
David Santiago	Castillo	37195851	Externo	1
Tomás William	White	41002238	Externo	2
Tomás William	White	41002238	Externo	2

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Habilidades o Destrezas (HD)	Aplicar técnicas de IA para modelar y resolver problemas complejos en entornos de seguridad.	HD-01
Competencias (COM)	Aplicar estrategias de inteligencia artificial en contextos de seguridad digital, física y estratégica.	COM-01
Competencias (COM)	Aplicar conceptos de machine learning y deep learning al desarrollo de soluciones de detección y prevención de amenazas en entornos digitales y físicos.	COM-05
Conocimientos o contenidos (C)	Comprender los fundamentos de la inteligencia artificial, el aprendizaje automático y sus aplicaciones en la detección y prevención de amenazas.	C-01

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75
Asistencia virtual a clase y participación en foros	Continua	25

Descripción de contenidos

Inteligencia artificial y sus principales aspectos. Paradigmas clave: IA simbólica, conexionista y estadística. Aprendizaje automático: supervisado, no supervisado y por refuerzo. Algoritmos fundamentales: regresión lineal/logística, árboles de decisión, máquinas de soporte vectorial, redes neuronales artificiales y clustering. Métricas de evaluación de modelos: precisión, recall, F1-score, curva ROC-AUC. Ecosistema de herramientas y librerías: Scikit-learn, TensorFlow, Keras, PyTorch.

Asignatura: Seguridad Digital y Ciberamenazas	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	N° Identificación	Interno/Externo	N° ECTS Impartidos
Gabriel Esteban	Franciosi	27551421	Externo	2
Gabriel Esteban	Franciosi	27551421	Externo	2
David Santiago	Castillo	37195851	Externo	1
David Santiago	Castillo	37195851	Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Habilidades o Destrezas (HD)	Diagnosticar vulnerabilidades en sistemas digitales mediante la identificación y clasificación de ciberamenazas.	HD-02
Conocimientos o contenidos (C)	Comprender los principios de la ciberseguridad, las arquitecturas de defensa y los mecanismos de respuesta ante incidentes digitales.	C-02
Competencias (COM)	Aplicar estrategias de inteligencia artificial en contextos de seguridad digital, física y estratégica.	COM-01
Competencias (COM)	Analizar vulnerabilidades, ciberamenazas y riesgos mediante el uso de herramientas de inteligencia artificial y sistemas de respuesta automatizada.	COM-07

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Asistencia virtual a clase y participación en foros	Continua	25
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75

Descripción de contenidos

Seguridad informática: confidencialidad, integridad, disponibilidad. Clasificación de ciberamenazas: malware, ransomware, phishing, APTs. Arquitecturas y niveles de defensa en entornos digitales: endpoints, redes, aplicaciones y nube. Principios de diseño seguro: autenticación, autorización, cifrado, monitoreo y respuesta. Marcos normativos y

estándares internacionales: ISO/IEC 27001, NIST Cybersecurity Framework, ENS (España). Ciclo de vida de un ciberataque y estrategias de defensa proactiva. Roles y funciones en un Centro de Operaciones de Seguridad (SOC).

Asignatura: Seguridad Física Inteligente y Videovigilancia con IA	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Primero

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	N° Identificación	Interno/Externo	N° ECTS Impartidos
Gabriel Esteban	Franciosi	27551421	Externo	2
Gabriel Esteban	Franciosi	27551421	Externo	2
Natasa	Loizou	19033174	Externo	1
Natasa	Loizou	19033174	Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Conocimientos o contenidos (C)	Comprender los principios de la ciberseguridad, las arquitecturas de defensa y los mecanismos de respuesta ante incidentes digitales.	C-02
Competencias (COM)	Diseñar estrategias integrales de seguridad basadas en IA, incorporando criterios técnicos, éticos y normativos en su implementación.	COM-02
Competencias (COM)	Evaluar el cumplimiento de las normativas de protección de datos, privacidad y ética algorítmica en el uso de tecnologías de IA aplicadas a la seguridad.	COM-08
Habilidades o Destrezas (HD)	Incorporar sistemas de videovigilancia inteligente basados en IA respetando principios éticos y de proporcionalidad.	HD-05

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75
Asistencia virtual a clase y participación en foros	Continua	25

Descripción de contenidos

Visión por computador aplicados a la seguridad física. Detección y reconocimiento facial: algoritmos, precisión, sesgos y regulaciones. Detección de objetos, anomalías y comportamientos en tiempo real mediante IA. Sistemas inteligentes de

CCTV: integración de analítica en cámaras y servidores. Control de accesos biométrico con IA: reconocimiento de huellas, iris, voz y rostro. Casos de uso: aeropuertos, infraestructuras críticas, eventos masivos, edificios corporativos. Desafíos éticos y legales.

Asignatura: Evaluación de Impacto Algorítmico y Gestión del Ciclo de Vida de Modelos de IA	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Francisco Luis	de Andres Pérez	22985661J	Externo	1
Francisco Luis	de Andres Pérez	22985661J	Externo	1
Tomás William	White	41002238	Externo	2
Tomás William	White	41002238	Externo	2

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Conocimientos o contenidos (C)	Comprender los fundamentos de la gobernanza algorítmica, la transparencia y la responsabilidad en el uso de la IA aplicada a la seguridad.	C-06
Habilidades o Destrezas (HD)	Evaluar el impacto ético y técnico de los modelos algorítmicos en el ciclo de vida de los sistemas de seguridad.	HD-10
Competencias (COM)	Implementar metodologías de evaluación de impacto algorítmico y gobernanza del ciclo de vida de los modelos de IA en entornos sensibles de seguridad.	COM-10
Competencias (COM)	Diseñar estrategias integrales de seguridad basadas en IA, incorporando criterios técnicos, éticos y normativos en su implementación.	COM-02

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75
Asistencia virtual a clase y participación en foros	Continua	25

Descripción de contenidos

Fases del ciclo de vida de modelos de IA: diseño, desarrollo, validación, implementación, mantenimiento y retirada. Evaluación de impacto algorítmico (AIA): marco conceptual y metodológico. Auditoría interna y externa de sistemas

inteligentes. Detección y corrección de sesgos y errores sistemáticos. Métricas para calidad, robustez y equidad de modelos. Documentación y trazabilidad de decisiones algorítmicas. Herramientas y estándares emergentes (Model Cards, Datasheets for Datasets, AI FactSheets).

Asignatura: Gobernanza de la IA y Ética en Entornos de Seguridad	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Daniel	Lascano	20531002	Externo	1
Daniel	Lascano	20531002	Externo	1
Esteban	Acuña	28641259	Externo	2
Esteban	Acuña	28641259	Externo	2

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Conocimientos o contenidos (C)	Comprender los marcos normativos nacionales e internacionales en materia de protección de datos, ciberseguridad y ética algorítmica.	C-03
Competencias (COM)	Implementar metodologías de evaluación de impacto algorítmico y gobernanza del ciclo de vida de los modelos de IA en entornos sensibles de seguridad.	COM-10
Habilidades o Destrezas (HD)	Aplicar principios de gobernanza, transparencia y ética en el diseño e implementación de estrategias de IA para entornos de seguridad.	HD-12
Competencias (COM)	Diseñar estrategias integrales de seguridad basadas en IA, incorporando criterios técnicos, éticos y normativos en su implementación.	COM-02

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75
Asistencia virtual a clase y participación en foros	Continua	25

Descripción de contenidos

Principios éticos fundamentales: justicia, transparencia, responsabilidad, no maleficencia. Desafíos éticos del uso de IA en seguridad: sesgos algorítmicos, discriminación, autonomía y toma de decisiones. Gobernanza algorítmica: definición,

modelos y niveles de intervención. Auditoría de algoritmos y supervisión humana en procesos automatizados. Regulaciones emergentes: propuesta de Reglamento de IA de la Unión Europea, guías de la OCDE, UNESCO y Comisión Europea. Modelos de gobernanza multinivel: institucional, técnico y social. Transparencia en entornos de seguridad algorítmica: explicabilidad, trazabilidad y documentación.

Asignatura: Infraestructuras Críticas y Sistemas Ciberfísicos con IA	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 6 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Daniel	Lascano	20531002	Externo	5
Daniel	Lascano	20531002	Externo	5
Francisco Luis	de Andres Pérez	22985661J	Externo	1
Francisco Luis	de Andres Pérez	22985661J	Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Integrar estrategias de IA en infraestructuras críticas, sistemas ciberfísicos y dispositivos autónomos, garantizando su fiabilidad, seguridad y trazabilidad.	COM-06
Conocimientos o contenidos (C)	Identificar los componentes tecnológicos y operativos de las infraestructuras críticas y sistemas ciberfísicos con integración de IA.	C-04
Conocimientos o contenidos (C)	Comprender las metodologías de análisis predictivo, evaluación de riesgos y resiliencia organizacional en entornos complejos.	C-05
Competencias (COM)	Evaluar riesgos y tomar decisiones informadas mediante el análisis predictivo de datos y el uso de modelos de aprendizaje automático.	COM-03
Habilidades o Destrezas (HD)	Planificar la integración de tecnologías de IA en la protección y gestión de infraestructuras críticas y sistemas ciberfísicos.	HD-09

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75
Asistencia virtual a clase y participación en foros	Continua	25

Descripción de contenidos

Definición y clasificación de infraestructuras críticas: energía, transporte, salud, agua, telecomunicaciones, etc. Introducción a los sistemas ciberfísicos (CPS) e Internet de las Cosas (IoT) industrial. Supervisión y control de entornos industriales: SCADA, PLCs, sensores y actuadores. Aplicación de IA en mantenimiento predictivo, detección de fallos y optimización de procesos. Ciberamenazas específicas a entornos OT (Operational Technology). Modelado de riesgos y simulación de incidentes en infraestructuras críticas. Resiliencia sistémica: estrategias de recuperación ante incidentes, redundancia y diseño seguro.

Asignatura: Sistemas Autónomos y Detección de Amenazas Emergentes	**Código**:

Carácter: Obligatoria(OB) **ECTS:** 3 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Francisco Luis	de Andres Pérez	22985661J	Externo	1
Francisco Luis	de Andres Pérez	22985661J	Externo	1
Tomás William	White	41002238	Externo	1
Tomás William	White	41002238	Externo	1
Nicolás	Wild	40750840	Externo	1
Nicolás	Wild	40750840	Externo	1

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Competencias (COM)	Integrar estrategias de IA en infraestructuras críticas, sistemas ciberfísicos y dispositivos autónomos, garantizando su fiabilidad, seguridad y trazabilidad.	COM-06
Conocimientos o contenidos (C)	Identificar los componentes tecnológicos y operativos de las infraestructuras críticas y sistemas ciberfísicos con integración de IA.	C-04
Competencias (COM)	Aplicar estrategias de inteligencia artificial en contextos de seguridad digital, física y estratégica.	COM-01
Habilidades o Destrezas (HD)	Incorporar sistemas autónomos capaces de detectar y responder ante amenazas emergentes en tiempo real.	HD-11

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Pruebas escritas (Foro de reflexión, Ejercicio práctico y Test de autoaprendizaje)	Final	75
Asistencia virtual a clase y participación en foros	Continua	25

Descripción de contenidos

Definición y clasificación de sistemas autónomos aplicados a seguridad. Robótica, drones, sensores inteligentes y plataformas móviles con capacidades de IA. Aplicaciones en vigilancia perimetral, patrullaje autónomo, búsqueda y rescate, y logística de emergencia. Integración de datos multifuente: video, audio, geolocalización, térmico. Técnicas de IA para la detección de amenazas emergentes: patrones inusuales, correlación de anomalías, aprendizaje en tiempo real. Riesgos y limitaciones operativas de los sistemas autónomos.

Asignatura: Trabajo Fin de Máster	**Código**:

Carácter: Trabajo Fin de Título (TFT) **ECTS:** 15 **Curso:** Primero **Cuatrimestre:** Segundo

Idiomas de impartición: Español

Porcentajes de moldalidad de impartición

- **Presencial:** 0 %
- **Virtual:** 100 %
- **Híbrido:** 0 %

Profesores

Nombre	Apellidos	Nº Identificación	Interno/Externo	Nº ECTS Impartidos
Alicia	Rodríguez Sánchez	70903557P	Interno	0
Alicia	Rodríguez Sánchez	70903557P	Interno	0
Daniel	Lascano	20531002	Externo	0
Daniel	Lascano	20531002	Externo	0
David Santiago	Castillo	37195851	Externo	0
David Santiago	Castillo	37195851	Externo	0
DANIEL	TERRÓN SANTOS	44431395H	Interno	0
DANIEL	TERRÓN SANTOS	44431395H	Interno	0
Katherine	Almeida Ramos	MM0205672	Externo	0
Katherine	Almeida Ramos	MM0205672	Externo	0
José Luis	Domínguez Álvarez	71704654S	Interno	0
José Luis	Domínguez Álvarez	71704654S	Interno	0
Esteban	Acuña	28641259	Externo	0
Esteban	Acuña	28641259	Externo	0
Nicolás	Wild	40750840	Externo	0
Nicolás	Wild	40750840	Externo	0
Francisco Luis	de Andres Pérez	22985661J	Externo	0
Francisco Luis	de Andres Pérez	22985661J	Externo	0
Gabriel Esteban	Franciosi	27551421	Externo	0
Gabriel Esteban	Franciosi	27551421	Externo	0

Tomás William	White	41002238	Externo	0
Tomás William	White	41002238	Externo	0
Natasa	Loizou	19033174	Externo	0
Natasa	Loizou	19033174	Externo	0

Resultados de aprendizaje previstos

Tipo de resultado	Descripción	Código
Habilidades o Destrezas (HD)	Planificar la integración de tecnologías de IA en la protección y gestión de infraestructuras críticas y sistemas ciberfísicos.	HD-09
Habilidades o Destrezas (HD)	Aplicar principios de gobernanza, transparencia y ética en el diseño e implementación de estrategias de IA para entornos de seguridad.	HD12
Conocimientos o contenidos (C)	Comprender las metodologías de análisis predictivo, evaluación de riesgos y resiliencia organizacional en entornos complejos.	C-05
Habilidades o Destrezas (HD)	Incorporar sistemas de videovigilancia inteligente basados en IA respetando principios éticos y de proporcionalidad.	HD-05
Competencias (COM)	Analizar vulnerabilidades, ciberamenazas y riesgos mediante el uso de herramientas de inteligencia artificial y sistemas de respuesta automatizada.	COM-07
Competencias (COM)	Evaluar el cumplimiento de las normativas de protección de datos, privacidad y ética algorítmica en el uso de tecnologías de IA aplicadas a la seguridad.	COM-08
Competencias (COM)	Diseñar estrategias de vigilancia inteligente y análisis predictivo que contribuyan a la seguridad nacional, urbana y organizacional, promoviendo la resiliencia ante incidentes.	COM-09
Conocimientos o contenidos (C)	Comprender los principios de la ciberseguridad, las arquitecturas de defensa y los mecanismos de respuesta ante incidentes digitales.	C-02
Conocimientos o contenidos (C)	Comprender los marcos normativos nacionales e internacionales en materia de protección de datos, ciberseguridad y ética algorítmica.	C-03
Competencias (COM)	Diseñar estrategias integrales de seguridad basadas en IA, incorporando criterios técnicos, éticos y normativos en su implementación.	COM-02
Competencias (COM)	Evaluar riesgos y tomar decisiones informadas mediante el análisis predictivo de datos y el uso de modelos de aprendizaje automático.	COM-03
Competencias (COM)	Comunicar de forma clara y rigurosa los resultados de análisis y proyectos de IA aplicada a la seguridad, tanto a públicos especializados como no especializados.	COM-04
Competencias (COM)	Aplicar conceptos de machine learning y deep learning al desarrollo de soluciones de detección y prevención de amenazas en entornos digitales y físicos.	COM-05

Competencias (COM)	Integrar estrategias de IA en infraestructuras críticas, sistemas ciberfísicos y dispositivos autónomos, garantizando su fiabilidad, seguridad y trazabilidad.	COM-06
Competencias (COM)	Implementar metodologías de evaluación de impacto algorítmico y gobernanza del ciclo de vida de los modelos de IA en entornos sensibles de seguridad.	COM-10
Conocimientos o contenidos (C)	Comprender los fundamentos de la inteligencia artificial, el aprendizaje automático y sus aplicaciones en la detección y prevención de amenazas.	C-01
Conocimientos o contenidos (C)	Comprender los fundamentos de la gobernanza algorítmica, la transparencia y la responsabilidad en el uso de la IA aplicada a la seguridad.	C-06
Habilidades o Destrezas (HD)	Aplicar técnicas de IA para modelar y resolver problemas complejos en entornos de seguridad.	HD-01
Habilidades o Destrezas (HD)	Analizar soluciones de detección automatizada de intrusiones y anomalías mediante herramientas de IA.	HD-03
Habilidades o Destrezas (HD)	Implementar soluciones de inteligencia artificial en contextos de seguridad nacional y defensa estratégica.	HD-07
Habilidades o Destrezas (HD)	Desarrollar estrategias de seguridad urbana basadas en datos e inteligencia artificial para entornos de smart cities.	HD-08
Competencias (COM)	Aplicar estrategias de inteligencia artificial en contextos de seguridad digital, física y estratégica.	COM-01
Conocimientos o contenidos (C)	Identificar los componentes tecnológicos y operativos de las infraestructuras críticas y sistemas ciberfísicos con integración de IA.	C-04
Habilidades o Destrezas (HD)	Diagnosticar vulnerabilidades en sistemas digitales mediante la identificación y clasificación de ciberamenazas.	HD-02
Habilidades o Destrezas (HD)	Implementar sistemas de IA que garanticen la privacidad y el cumplimiento de la normativa de protección de datos personales.	HD-04
Habilidades o Destrezas (HD)	Aplicar modelos de análisis predictivo para la identificación temprana de riesgos y la mejora de la resiliencia organizacional.	HD-06
Habilidades o Destrezas (HD)	Evaluar el impacto ético y técnico de los modelos algorítmicos en el ciclo de vida de los sistemas de seguridad.	HD-10
Habilidades o Destrezas (HD)	Incorporar sistemas autónomos capaces de detectar y responder ante amenazas emergentes en tiempo real.	HD-11

Tabla de evaluacion

Prueba	Tipo	% Ponderado
Elaboración y defensa del TFM	Final	100

Descripción de contenidos

Desarrollo de un plan integral para el diseño y la puesta en marcha de una estrategia de seguridad, utilizando tecnologías de inteligencia artificial y aplicado a un escenario operativo real o simulado.