TEMARIO

CURSO EN IA

PARA PROFESIONALES DE

CIBERSEGURIDAD Y PRIVACIDAD

Dominio	Subdominio	Apartados
Conceptos básicos	Presentación del Curso Introducción a sistemas de IA, agentes, Machine Learning, Deep Learning e IA generativa IA e impacto en negocio	
Ciberseguridad e IA:	Taxonomías de amenazas a sistemas de IA	Ataques a sistemas de Deep Learning Ataques a a sistemas de IA generativa
	Securización en el uso de sistemas de IA	Ciberseguridad del propio sistema de IA: acceso al sistema y sus funcionalidades, permisos de acceso a información en entornos cerrados, difusión de la información.
	IA para prevención y detección	IA como elemento de defensa: incorporación de IA en el departamento de Ciberseguridad
Regulación de la IA:	Unión Europea	Introducción al Reglamento (UE) de Inteligencia Artificial: criterios subjetivos, materiales y territoriales de aplicación, clasificación de sistemas y modelos en función del nivel de riesgo, marco sancionador y principales obligaciones de los distintos operadores
	España	Iniciativas legislativas en España: (i) constitución y regulación de la AESIA, (ii) Sandbox regulatorio, (iii) iniciativas en CCAA.
	Visión internacional	Regulación de la IA en derecho comparado
La IA en la empresa y AAPP	Gobierno de la IA	Establecimiento de un modelo de gobernanza de IA: roles, funciones, responsabilidades; Ejemplos prácticos para el gobierno de la IA en el ciclo de vida de proyectos con IA, y qué papel juegan las distintas áreas de la organización.
	Riesgos de la IA	Escenarios de casos de IA y sus riesgos
	Riesgos de Uso	Implantación de modelos en la empresa y AAPP: riesgos, oportunidades, impacto, expectativas y diseño de estrategias
	Contratación de IA y responsabilidades internas y de proveedores.	Roles, modelos de relación y responsabilidades. Tipos de contrato en función de los roles y responsabilidades. Aspectos a tener en cuenta en la selección y negociación
	IA y activos intangibles	Afectación de la IA a la protección de datos personales y a la propiedad intelectual/industrial. Casos de uso permitidos y retos de cumplimiento: entrenamiento de modelos, reutilización de información protegida, extensión de protección a los resultados de la IA.
	IA Compliance	Establecimiento de un modelo de cumplimiento y sistema de gestión de Inteligencia Artificial: objetivos de control, catálogo de controles La función de auditoría en el contexto de la IA.


isms
rorum
INTERNATIONAL
INFORMATION
SECURITY
COMMUNITY