

Seguridade da ia xenerativa en AWS: ameazas, guardrails e goberno de axentes

Descrición

Seminario centrado en ameazas específicas de aplicacións xenerativas e axentes, con especial atención ao control de acceso, protección de datos, guardrails, rastrexabilidade e goberno en contornas AWS.

Perfil do docente

.

PROGRAMA	Programación 2026/27
TIPO	SEMINARIO
PERIODO INSCRICIÓN	22/03/2027 - 07/04/2027
Nº PRAZAS	230
METODOLOXÍA	Presencial
DURACIÓN	4 horas
DATA INICIO	08/04/2027
DATA FIN	08/04/2027
HORARIO	O 08/04/2027 de 16:30 a 20:30 horas.

LUGAR DE DOCENCIA	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
PERIODO DOCENCIA	08/04/2027 - 08/04/2027

Temario

- Ameazas propias de aplicacións GenAI e axentes.
- Protección de prompts, datos e contexto.
- Guardrails e controis de contido.
- Identidade, permisos e mínimo privilexio.
- Rexistro, auditoría e goberno do ciclo de vida.