**Propuesta CIESPAL**

**Tema:** Privacidad y seguridad en Ciencia de Datos.

Las técnicas de aprendizaje automático y aprendizaje profundo basadas en redes neuronales están logrando resultados notables en una amplia variedad de campos.

A menudo, la entrenamiento de modelos requiere de grandes y representativos conjuntos de datos, que pueden contener información confidencial. Los modelos no deben exponer información privada de los conjuntos de datos.

En los últimos años se han desarrollado nuevas técnicas para poder precisamente mantener y asegurar la privacidad de la información utilizada en modelos de Inteligencia Artificial, Aprendizaje Automatizado y Aprendizaje Profundo.

Entre las principales podemos mencionar:

* Privacidad diferencial
* Aprendizaje Federado
* Protocolos de preservación de la privacidad

Se trata de una charla de aproximadamente 1 hora de duración y 1 hora para preguntas y respuestas.

Durante la charla se pretende explicar algunas de las principales técnicas actuales así como sus aplicaciones en diversos campos.

Se necesitará de monitor o proyector, computadora y conexión a internet.

Fecha: Jueves 29 de 18h00 a 20h00.