Programma

"Intelligenza Artificiale: basi teoriche e applicazioni odierne; minacce ed opportunità per la cybersicurezza"

Il corso si svolgerà a distanza in modalità sincrona

Modulo 1 – Principi, scopi e metodologie di Intelligenza Artificiale - 20 ore

- Introduzione all'Intelligenza Artificiale
  - Storia e sviluppo dell'Intelligenza Artificiale;
  - Agenti Intelligenti: obiettivi, dati, modelli, algoritmi;
  - Differenza tra Intelligenza Artificiale, Machine Learning e Deep Learning;
- Tecniche di Intelligenza Artificiale:
  - Differenza tra apprendimento supervisionato e apprendimento non supervisionato;
  - Alberi Decisionali;
  - Reti neurali;
  - Deep Neural Networks;
  - Ragionamento con incertezza;
  - Apprendimento per rinforzo;
- Esercitazioni: utilizzo delle principali tecniche di intelligenza Artificiale;

Modulo 2 – Intelligenza Artificiale per la Cybersecurity e Sicurezza dell'Intelligenza Artificiale - 15 ore

- Ruolo dell'Intelligenza Artificiale nella Cybersecurity;
- Casi di studio di Intelligenza Artificiale applicata alla Cybersecurity;
- Minacce ai sistemi di Intelligenza Artificiale;
- Esercitazioni: semplici esempi di attacchi ai sistemi di intelligenza artificiale;
- Strategie di protezione;
- Aspetti etici e normativi, sicurezza e protezione dei dati;

Modulo 3 – Strumenti di Intelligenza Artificiale per la Pubblica Amministrazione - 5 ore

- Panoramica degli strumenti di IA: framework open source, soluzioni cloud;
- Strumenti di Intelligenza Artificiale Generativa.