

Corso in CYBER & DATA RISK MANAGEMENT E ARTIFICIAL INTELLIGENCE

Rischi Cibernetici e Sicurezza dei Dati, connessioni con l'Intelligenza Artificiale (AI) e il Quadro Normativo Europeo

On Demand

ON DEMAND - Programma Dettagliato delle Lezioni

Modulo: CYBER & DATA RISK MANAGEMENT E ARTIFICIAL INTELLIGENCE

Rischi Cibernetici e Sicurezza dei Dati, connessioni con l'Intelligenza Artificiale (AI) e il Quadro Normativo Europeo

Lezione 1

INTRODUZIONE AI CYBER RISK E ALL'INTELLIGENZA (IA)

Introduzione ai Cyber Rischi e all'Intelligenza Artificiale

- Introduzione ai cyber rischi
- Nozioni di base sull'intelligenza artificiale (IA)
- Come l'IA viene utilizzata in diversi settori
- Panoramica delle minacce cibernetiche specifiche dell'IA

Vulnerabilità dell'Intelligenza Artificiale

- Tipologie di vulnerabilità nei sistemi di IA
- Esempi di attacchi a modelli di IA (e.g., attacchi adversariali)
- Metodi per identificare le vulnerabilità

Privacy e IA

- Implicazioni sulla privacy derivanti dall'uso dell'IA
- Regolamentazioni e leggi sulla privacy
- Tecniche per proteggere la privacy nei sistemi di IA

IA e Sicurezza dei Dati

- Gestione dei dati in sistemi di IA
- Tecniche di cifratura e anonimizzazione dei dati
- Strategie di sicurezza per la protezione dei dati utilizzati da IA

Lezione 2

IMPLEMENTAZIONE SICURA DELL'IA E GESTIONE DEI RISCHI

Implementazione Sicura dell'IA

- Principi di sicurezza by design
- Strumenti e framework per la sicurezza nell'implementazione dell'IA
- Best practice per lo sviluppo sicuro di modelli di IA

Monitoraggio e Gestione dei Rischi

- Monitoraggio continuo dei sistemi di IA
- Strumenti per la gestione dei rischi
- Incident response e gestione degli incidenti cibernetici

Quadro Normativo Europeo sull'IA e Cyber Sicurezza

- Panoramica delle normative europee sull'IA
- Direttiva NIS (Network and Information Systems)
- Regolamento Generale sulla Protezione dei Dati (GDPR)
- Proposta di Regolamento sull'Intelligenza Artificiale (AI Act)

Casi di Studio e Analisi di Incidenti

- Analisi di casi reali di attacchi a sistemi di IA
- Rappresentazione di esperienze da incidenti passati
- Discussione su come prevenire futuri incidenti

lezioni rispetto al calendario inizialmente prestabilito. Inoltre, si riserva il diritto di modificare in ogni momento i contenuti, dei programmi ed il corpo docente al fine di perseguire miglioramenti didattici in linea con i cambiamenti di mercato e le subentranti esigenze organizzative.