INGEGNERIA PER LA SICUREZZA DELLE INFRASTRUTTURE CRITICHE

(Lecce - Università degli Studi)

Insegnamento ENTERPRISE RISK ASSESSMENT AND MANAGEMENT MOD.A C.I.

GenCod A007238

Docente titolare Angelo CORALLO

Docenti responsabili dell'erogazione
Angelo CORALLO, MARIANNA LEZZI

Insegnamento ENTERPRISE RISK ASSESSMENT AND MANAGEMENT

Insegnamento in inglese

Settore disciplinare IEGE-01/A

Corso di studi di riferimento
INGEGNERIA PER LA SICUREZZA DELLE INFRASTRUTTURE CRITICHE

Tipo corso di studi Laurea Magistrale

Crediti 6.0

Ripartizione oraria Ore Attività frontale: 54.0

Per immatricolati nel 2026/2027

Erogato nel 2026/2027

Anno di corso 1

Lingua

Percorso INDUSTRIAL AND CIVIL INFRASTRUCTURES

Sede Lecce

Periodo Primo Semestre

Tipo esame Orale

Valutazione

Vai a **Orario dell'insegnamento**

BREVE DESCRIZIONE DEL CORSO

Il corso intende fornire le conoscenze di contesto e gli strumenti tecnici e metodologici per l'identificazione, la valutazione e la gestione dei rischi all'interno delle organizzazioni che operano in settori critici, quali energia, trasporti e infrastrutture digitali. Particolare attenzione è dedicata alle sfide di sicurezza, resilienza e continuità operativa delle infrastrutture critiche, integrando l'analisi delle tecnologie abilitanti, degli standard internazionali e dei quadri normativi vigenti.

PREREQUISITI

Nessun prerequisito

OBIETTIVI FORMATIVI	Il corso mira a fornire i modelli concettuali, le metodologie e gli strumenti operativi per l'identificazione, la valutazione e la gestione strategica dei rischi all'interno delle organizzazioni, con focus sulla resilienza e protezione delle Infrastrutture Critiche. Nello specifico: ▪ Conoscenze e comprensione: lo studente acquisirà una solida conoscenza delle tassonomie di rischio aziendale e dei principali framework metodologici per la loro identificazione e analisi, delle strategie per garantire la business continuity (continuità operativa), del funzionamento delle tecnologie a supporto delle Infrastrutture Critiche, e del quadro normativo e di standardizzazione (es. ISO) che regolamenta il settore. ▪ Capacità di applicare conoscenze e comprensione: lo studente sarà in grado di applicare gli strumenti di risk assessment ai contesti organizzativi. Saprà identificare i processi critici, valutare l'impatto di potenziali minacce e supportare i processi decisionali volti alla mitigazione del rischio e alla gestione delle crisi, in particolare all'interno di Infrastrutture Critiche. ▪ Autonomia di giudizio: lo studente svilupperà la capacità di valutare criticamente l'esposizione al rischio di un'organizzazione e di ponderare l'efficacia delle diverse strategie di mitigazione, formulando giudizi autonomi. ▪ Abilità comunicative: Il percorso formativo consentirà allo studente di padroneggiare la terminologia tecnica nel dominio di risk assessment and management. Sarà in grado di comunicare in modo chiaro ed efficace analisi di rischio e soluzioni strategiche sia a specialisti del settore sia a decisori aziendali (management). ▪ Capacità di apprendimento**:** lo studente acquisirà le conoscenze necessarie ad intraprendere con maggiore livello di autonomia l'analisi e la valutazione critica di eventi correlati alla gestione dei rischi nelle organizzazioni.
METODI DIDATTICI	Lezioni frontali ed esercitazioni
MODALITA' D'ESAME	Prova orale

PROGRAMMA ESTESO

MODULO 1: Risk Assessment and Management

- INTRODUCTION TO RISK ASSESSMENT
- RISK ANALYSIS AND TREATMENT
- RISK ANALYSIS TECHNIQUES
- RISK GOVERNANCE
- RISK ASSESSMENT METHOTOLOGIES

MODULO 2: Business Continuity and Crisis Management

- BUSINESS CONTINUITY MANAGEMENT
- BUSINESS IMPACT ANALYSIS
- CRISIS MANAGEMENT
- IDENTIFICATION AND DEVELOPMENT OF RECOVERY STRATEGIES
- IMPLEMENTATION OF EFFECTIVE CONTINGENCY PLANS
- ISO 22301

MODULO 3: Risk Assessment And Management In Critical Infrastructures (CI)

- CI PROTECTION
- SECURITY AND MONITORING TECHNOLOGIES
- TECHNOLOGIES FOR CI
- CYBERSECURITY MANAGEMENT

MODULO 4: Internet of Things (IoT) and Digital Twin (DT) for CI

- IoT FOR CI
- DT ARCHTECTURE AND ENABLING TECHNOLOGIES
- DT COMMUNICATION PROTOCOLS
- DT FOR CYBERSECURITY

MODULO 5: Artificial Intelligence (AI) for CI

- MALWARE DETECTION
- AI RISKS
- APPROACHES TO MITIGATE RISKS

MODULO 6: Bulding Information Modelling (BIM)

- INTRODUCITON TO BIM TECHNOLOGIES
- BIM TECHNOLOGIES FOR CI

MODULO 7: Cybersecurity in CI

- IT E OT CONVERGENCE
- ATTACK SURFACES
- ATTACK SURFACE MANAGEMENT

MODULO 8: Cybersecurity Procedures & Tools

- VULNERABILITY ASSESSMENT

- PENETRATION TEST
- TECHNOLOGIES FOR CYBER THREAT INTELLIGENCE

MODULO 9: European Standards for Critical Infrastructure Security

- EUROPEAN: GDPR, NIS 1&2, CER, Cyber Security Act, Cyber Resilience Act, RED, AI ACT
- NATIONAL: ACN, Strategia Cloud Italia (Cloud PA e Polo Strategico Nazionale), Perimetro Sicurezza Nazionale Cibernetico

TESTI DI RIFERIMENTO	Durante il corso verranno fornite le dispense inerenti ai moduli che compongono il corso