ENGINEERING FOR SAFETY OF CRITICAL INDUSTRIAL AND CIVIL

(Lecce - Università degli Studi)

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

GenCod A007238

Docente titolare Angelo CORALLO

Insegnamento ENTERPRISE RISK ASSESSMENT AND MANAGEMENT

Insegnamento in inglese

Settore disciplinare ING-IND/35

Corso di studi di riferimento ENGINEERING FOR SAFETY OF CRITICAL INDUSTRIAL AND CIVIL

Tipo corso di studi Laurea Magistrale

Crediti 6.0

Ripartizione oraria Ore Attività frontale: 54.0

Per immatricolati nel 2024/2025

Erogato nel 2024/2025

Anno di corso 1

Lingua

Percorso CIVIL INFRASTRUCTURES

Sede Lecce

Periodo Primo Semestre

Tipo esame

Valutazione

Orario dell'insegnamento https://easyroom.unisalento.it/Orario

BREVE DESCRIZIONE DEL CORSO

Il corso mira a fornire agli studenti una solida comprensione delle metodologie, delle strategie e degli strumenti necessari per identificare, valutare e gestire i rischi all'interno delle organizzazioni che lavorano in settori critici, quali energia, trasporti, comunicazioni e altro. Il corso si concentra sulle sfide legate alla sicurezza, resilienza e continuità operativa delle infrastrutture vitali, descrivendo inoltre le tecnologie utilizzate in tale ambito e gli standard e le normative vigenti.

PREREQUISITI

Nessun prerequisito.

OBIETTIVI FORMATIVI

Il corso si propone di fornire agli studenti le nozioni di base e gli strumenti necessari per la corretta valutazione e gestione dei rischi all'interno delle organizzazioni. Nello specifico:

- Conoscenze e comprensione: conoscere le tipologie di rischio, gli strumenti e le metodologie per l'identificazione e l'analisi degli stessi, comprendere le strategie da attuare per garantire la sicurezza e la continuità aziendale e, infine, conoscere le tecnologie a supporto delle Infrastrutture Critiche, nonché le normative e gli standard che regolamentano tali ambiti.
- Capacità di applicare conoscenze e comprensione: alla fine del corso lo studente sarà in grado di applicare le conoscenze acquisite e sarà quindi capace di comprendere il comportamento e le decisioni che le organizzazioni devono intraprendere nell'identificazione e gestione dei rischi all'interno delle Infrastrutture Critiche.
- Abilità comunicative: le conoscenze apprese durante il corso permetteranno agli studenti di padroneggiare il linguaggio tecnico e redigere pareri su temi di risk management.
- Capacità di apprendimento**:** Al termine del corso lo studente avrà acquisito le conoscenze necessarie che permettono di intraprendere con maggiore livello di autonomia l'analisi e la valutazione critica di eventi che riguardano la gestione dei rischi nelle organizzazioni.

METODI DIDATTICI

Lezioni frontali ed esercitazioni

MODALITA' D'ESAME	L'esame consiste in una prova orale.

PROGRAMMA ESTESO

MODULO 1: Risk Assessment

- RISK ASSESSMENT: valutazione dei rischi sia operativi che strategici utilizzando la valutazione del livello di maturità come base del modello di calcolo;
- RISK IDENTIFICATION: Definizione e importanza dell'identificazione dei rischi

Tecniche per l'identificazione dei rischi, come brainstorming, liste di controllo, interviste e analisi dei dati storici. Identificazione dei rischi in diversi tipi di infrastrutture critiche (ad esempio, trasporti, energia, telecomunicazioni). Fonti comuni di rischio nelle infrastrutture critiche, tra cui disastri naturali, guasti tecnologici, errori umani e atti dolosi.

- RISK ANALYSIS: analisi del rischio a partire dal contesto del business ed inclusivo della gestione delle parti interessate, delle minacce e della SWOT analysis;
- RISK TREATMENT: trattamento dei rischi collegato agli obiettivi di business, alle azioni correttive ed emissione automatica di documenti quali RTP, BIA (business impact analysis), PIA, …
- STRUMENTI E METODOLOGIE DI ANALISI DEL RISCHIO E DEI GUASTI
- FMEA
- FMECA
- FTA
- HACCP
- HAZOP
- RISK GOVERNANCE: considerazioni sulla costruzione di un modello organizzativo aziendale a supporto della rilevazione dei dati e delle relazioni interdipartimentali;
- METODOLOGIE DI VALUTAZIONE DEL RISCHIO: ISO 31000, NIST 800-39

MODULO 2: Business Continuity and Crisis Management

- BIA (business impact analysis)
- IDENTIFICATION AND DEVELOPMENT OF RECOVERY STRATEGIES: pianificazione dell'emergenza, comunicazione della crisi, coordinamento con le parti interessate e analisi postincidente.
- IMPLEMENTATION OF EFFECTIVE CONTINGENCY PLANS
- ISO 22301

MODULO 3: Critical Infrastructures

- DEFINIZIONE
- SETTORI (trasporti, acquedotti, energia, aviazione, oil&gas, ecc.)
- "DIPENDENZE" FRA INFRASTRUTTURE CRITICHE (Approcci di modellazione delle dipendenze)
- TECNOLOGIE PER LA SICUREZZA E IL MONITORAGGIO (Videosorveglianza, Biometria, Sensori, Data Mining, ecc.)

MODULO 4: Tecnologie per le Infrastrutture Critiche

- INTRODUZIONE INDUSTRIA 4.0
- PILASTRI
- BEST PRACTICES APPLICATE ALLE IC

MODULO 5: BIM

- DEFINIZIONE
- LIVELLI
- APPLICAZIONI
- STRUMENTI
- BIM PER LE INFRASTRUTTURE CRITICHE (Dati, Sensori e altre tecnologie abilitanti, Casi d'uso rilevanti)

MODULO 6: IoT PER LE IC

- DEFINIZIONE
- TIPOLOGIE DI SENSORI
- ARCHITETTURE COMUNI
- PROTOCOLLI DI TRASMISSIONE

MODULO 7: DIGITAL TWIN PER LE IC

- DEFINIZIONE
- ARCHITETTURA
- TECNOLOGIE ABILITANTI
- PROTOCOLLI DI COMUNICAZIONE
- DT PER I CYBER-SECURITY TEST NELLE IC

MODULO 8: IA PER LE IC

- DEFINIZIONE
- MACHINE LEARNING
- MALWARE DETECTION
- RISCHI LEGATI ALL'IA
- APPROCCI PER MITIGARE I RISCHI

MODULO 9: CRITICAL INFRASTRUCTURE SECURIT

- DEFINIZIONE E DIFFERENZA TRA SAFETY E SECURITY
- ASSET CRITICI (Sistemi industriali, ICS, SCADA, ecc.)
- VULNERABILITÀ (fisiche, di configurazione, di architettura e progettazione, ecc.)
- POSSIBILI MINACCE E ATTACCHI PIÙ SIGNIFICATIVI (avversaria, accidentale, strutturale, ambientale) + esempi di attacchi reali
- IMPATTI (fisici, economici e sociali)

MODULO 10: CYBER SECURITY IN CRITICAL INFRASTRUCTURES

- CONVERGENZA IT E OT
- SUPERFICI DI ATTACCO (tipologie: digitale, fisica, ingegneria sociale, ecc.)
- GESTIONE DELLA SUPERFICIE D'ATTACCO (identificazione asset, classificazione, analisi e priorità, remediation, monitoraggio continuo)

MODULO 11: CYBER SECURITY PROCEDURES & TOOLS

- VULNERABILITY ASSESSMENT
- PENETRATION TEST
- TECNOLOGIE PER LA CYBER THREAT INTELLIGENCE
- SISTEMI PER IL RILEVAMENTO E PREVENZIONE DELLE INTRUSIONI
- SIEM
- SECURITY OPERATION CENTER
- INCIDENT RESPONSE
- DIGITAL FORENSICS

MODULO 12: NORMATIVE EUROPEE E NAZIONALI PER LA SICUREZZA DELLE INFRASTRUTTURE CRITICHE

- EUROPEE: GDPR, NIS 1&2, CER, Cyber Security Act, Cyber Resilience Act, RED, AI ACT
- NAZIONALI: ACN, Strategia Cloud Italia (Cloud PA e Polo Strategico Nazionale), Perimetro Sicurezza Nazionale Cibernetico
- RICERCA: Cyberchallenge, PNRR PE SERICS

ESERCITAZIONI

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