SCHEDA DELL'INSEGNAMENTO (SI)

"RISK ASSESSMENT"

SSD ING-INF/05

DENOMINAZIONE DEL CORSO DI STUDIO: LAUREA MAGISTRALE IN INGEGNERIA INFORMATICA

ANNO ACCADEMICO: 2023-2024

INFORMAZIONI GENERALI - DOCENTE

DOCENTE: ALESSANDRA DE BENEDICTIS
TELEFONO:
EMAIL: ALESSANDRA.DEBENEDICTIS@UNINA.IT

INFORMAZIONI GENERALI - ATTIVITÀ

INSEGNAMENTO INTEGRATO (EVENTUALE):
MODULO (EVENTUALE):
CANALE (EVENTUALE):
ANNO DI CORSO (I, II, III): II
SEMESTRE (I, II): II
CFU: 6

INSEGNAMENTI PROPEDEUTICI (se previsti dall'Ordinamento del CdS)

Nessuno

EVENTUALI PREREQUISITI

Nessuno

OBIETTIVI FORMATIVI

Il corso ha l'obiettivo di introdurre il processo, le principali metodologie e le tecniche per la valutazione del rischio in sistemi critici.

RISULTATI DI APPRENDIMENTO ATTESI (DESCRITTORI DI DUBLINO)

Conoscenza e capacità di comprensione

Lo studente deve dimostrare di conoscere e comprendere le problematiche relative all'identificazione, valutazione e gestione del rischio in diversi contesti safety e security-critical.

Capacità di applicare conoscenza e comprensione

Lo studente deve dimostrare di essere in grado di applicare le principali tecniche di risk assessment viste al corso a casi di studio reali.

PROGRAMMA-SYLLABUS

INTRODUZIONE E TERMINOLOGIA: Definizioni di rischio; hazard scenarios; hazard e threat; hazardous events; fault e failure; probabilità e conseguenze; spettro delle conseguenze; barriere e fattori di escalation. Modello BowTie.

PROCESSO DI GESTIONE DEL RISCHIO: Requisiti e caratteristiche di un processo di gestione del rischio. Panoramica delle principali fasi del processo di gestione del rischio. Gestione del rischio e processo decisionale: processo decisionale deterministico, processo decisionale basato sul rischio; processo decisionale informato sul rischio. La gestione del rischio nella normativa in materia di safety e security.

PROCESSO DI VALUTAZIONE DEL RISCHIO: Panoramica delle principali fasi del processo di valutazione del rischio. Definizione dell'oggetto di studio: il sistema, boundaries di un sistema; system breakdown.

CRITERI DI ACCETTAZIONE DEL RISCHIO: Principi di accettazione del rischio: equità, utilità, tecnologia. L'approccio ALARP: principi ed esempi. Panoramica di altri approcci: ALARA, SFAIRP, GAMAB, MEM. Analisi costi-benefici: valutazione di costi e benefici.

MISURE DI RISCHIO: metriche e misure di rischio individuale e di gruppo: Average Individual Risk (AIR), Location-specific Individual Risk (LSIR), Lost-time injury (LTI) frequency, Lost workdays frequency (LWF); Potential Loss of Life (PLL); Fatal Accident Rate (FAR), FN curves; Risk matrices; Risk Priority Number (RPN).

METODI DI IDENTIFICAZIONE DEGLI HAZARD: Fattori causali di un hazard; Tipi di analisi di safety risk: CD-HAT, PD-HAT, DD-HAT, SD-HAT, OD-HAT, HD-HAT, RD-HAT. Tecniche CD-HAT: metodi basati su checklist e liste di rischio preliminari (PHL). Tecniche PD-HAT: preliminary hazard analysis (PHA); HAZID. Tecniche DD-HAT: subsystem hazard analysis (SSHA); HAZOP. Tecniche SD-HAT: system hazard analysis (SHA); Analisi dei rischi operativi e di supporto (O&SHA); Failure mode, effect and criticality analysis (FMECA): identificazione di modalità, tassi, cause, effetti di guasto. Analisi di criticità qualitativa e quantitativa mediante reti di Petri.

METODI DI ANALISI CAUSALE E DI FREQUENZA: Fult tree analysis: elementi dei diagrammi FT e loro utilizzo nell'ambito del risk assessment. Diagramma di causa ed effetto; Reti bayesiane e loro utilizzo nel risk assessment; Common cause failure analysis.

SVILUPPO DEGLI HAZARD SCENARIOS: Event-trees: pivotal events, passaggi metodologici; cause-consequences analysis.

SECURITY RISK ASSESSMENT: Panoramica dei concetti di rischio per la sicurezza: principali proprietà di sicurezza, minacce, vulnerabilità, debolezze, attacchi, controlli di sicurezza. Rischio per la sicurezza: probabilità e impatto.

MODELLAZIONE DELLE MINACCE: modellazione delle minacce e threat intelligence; MITRE ATT&CK framework. Modellazione di sistemi per il threat modeling: Data Flow Diagrams (DFD) e Process Flow Diagrams (PFD). Metodologie e framework di identificazione e valutazione delle minacce: la metodologia STRIDE e il processo di modellazione delle minacce Microsoft. Strumento di modellazione delle minacce Microsoft (TMT). La metodologia DREAD. La metodologia LINDDUN. La metodologia Trike. La metodologia VAST. Il framework CVSS. La metodologia di valutazione del rischio OWASP.

ATTACK GRAPH: modellazione e strumenti.

APPROCCI STANDARD AL SECURITY RISK MANAGEMENT: FISMA: categorizzazione della sicurezza (FIPS-199 e NIST SP 800-60) e requisiti minimi di sicurezza (FIPS 200 e NIST 800-53); Il quadro di gestione del rischio NIST (NIST SP 800-37); Processo di valutazione del rischio NIST (NIST SP 800-30); NIST Cybersecurity Framework: core, livelli, profili.

MATERIALE DIDATTICO

Libro di testo:

Marvin Rausand, Stein Haugen. Risk assessment – Theory, Methods and Applications. Second edition Wiley.

Dispense e presentazioni fornite dal docente relative ad argomenti teorici e applicativi trattati al corso.

MODALITÀ DI SVOLGIMENTO DELL'INSEGNAMENTO

Il corso prevede circa il 70% di lezioni frontali in cui vengono affrontati gli argomenti teorici, mentre il restante 30% è riservato ad esercitazioni e ad interventi seminariali da parte di esperti nello sviluppo e nella gestione di sistemi critici.

VERIFICA DI APPRENDIMENTO E CRITERI DI VALUTAZIONE

a) Modalità di esame:

L'esame si articola in prova	
scritta e orale	
solo scritta	
solo orale	
discussione di elaborato progettuale	x
altro	

In caso di prova scritta i quesiti sono (*)	**A risposta multipla**	
	A risposta libera	
	Esercizi numerici	

La verifica dell'apprendimento prevede una prova orale e la discussione di un elaborato.

b) Modalità di valutazione: