Denominazione	Ingegneria della sicurezza dei dati e delle comunicazioni - L9
Moduli componenti	
Settore scientifico-disciplinare	ING-INF/05
Anno di corso e semestre di erogazione	2° anno, 2° semestre
Lingua di insegnamento	Italiano
Carico didattico in crediti formativi universitari	9 CFU
Numero di ore di attività didattica frontale	72
Docenti	Prof. Carmelo Antonio Ardito
Risultati di apprendimento specifici	Al termine del corso lo studente conosce i concetti di base della sicurezza informatica. È in grado di individuare le principali problematiche di sicurezza dei sistemi informatici, di valutare in modo critico la loro sicurezza, individuando le possibili vulnerabilità, incrementando la robustezza del sistema e attuando le contromisure necessarie per mitigare le problematiche individuate. È inoltre in grado di gestire la sicurezza informatica e la valutazione dei rischi di un'azienda o di una pubblica amministrazione, avendo anche conoscenza degli aspetti legali ed etici dei crimini informatici.
Programma	**Panoramica sulla sicurezza informatica.** Concetti di sicurezza informatica. Minacce, attacchi e risorse. Requisiti funzionali di sicurezza. Principi fondamentali di progettazione della sicurezza. Superfici di attacco e alberi di attacco. Strategia di sicurezza informatica. Standard. Software dannoso. Propagazione tramite contenuto infetto (Virus), Sfruttamento di vulnerabilità (Worms), Ingegneria sociale (Posta elettronica SPAM, Trojan). Sovraccarico dei sistemi (Zombie, Bot). Attacchi Denial-of-Service. Furto di informazioni (Keylogger, Phishing, Spyware). Occultamento (Backdoor, Rootkit). Contromisure. **Strumenti crittografici.** Riservatezza con la crittografia simmetrica. Autenticazione dei messaggi e funzioni hash. Crittografia a chiave pubblica. Firme digitali e gestione delle chiavi. Numeri casuali e pseudocasuali. Applicazione pratica: Crittografia dei dati memorizzati. **Autenticazione utente.** Principi di autenticazione digitale degli utenti. Autenticazione basata su password. Autenticazione basata su token. Autenticazione biometrica. Autenticazione utente remota. Problemi di sicurezza per l'autenticazione degli utenti. **Controllo degli accessi.** Principi di controllo dell'accesso. Soggetti, oggetti e diritti di accesso. Controllo dell'accesso discrezionale. Controllo dell'accesso basato sui ruoli. Controllo dell'accesso basato sugli attributi. Gestione delle identità, delle credenziali e degli accessi. **Sicurezza dei database e dei data center.** La necessità di sicurezza dei database. Sistemi di gestione dei database. Database relazionali. Attacchi di tipo SQL Injection. Controllo dell'accesso al database. Crittografia dei database. Sicurezza del data center. **Cloud Security.** Cloud Computing. Concetti di sicurezza del cloud. Approcci alla sicurezza nel cloud **Internet of Things Security.** Internet of Things (IoT). IoT Security. **Sicurezza dei sistemi operativi.** Introduzione alla sicurezza del sistema operativo. Pianificazione della sicurezza del sistema. Hardening dei sistemi operativi. Sicurezza delle applicazioni. Manutenzione della sicurezza. Sicurezza di Linux/UNIX. Sicurezza di Windows. **Gestione della sicurezza informatica e valutazione dei rischi.** Gestione della sicurezza informatica. Contesto organizzativo e politica di sicurezza. Valutazione del rischio di sicurezza. Analisi dettagliata del rischio di sicurezza. Implementazione della gestione della sicurezza informatica. Controlli di sicurezza o salvaguardie. Piano di sicurezza informatica.

	Implementazione dei controlli. Monitoraggio dei rischi. Sicurezza delle risorse umane: Sensibilizzazione, formazione e addestramento alla sicurezza, Politiche di utilizzo della posta elettronica e di Internet, Computer Security Incident Response Team. **Aspetti legali ed etici.** Crimine informatico e criminalità informatica. Proprietà intellettuale. Privacy. Questioni etiche. **Principali Servizi Digitali al Cittadino** Posta elettronica certificata. Firma digitale. SPID. CIE. **Cybersecurity nella Pubblica Amministrazione** Principio Cloud First. Misure minime di sicurezza. Framework nazionale per la Cybersecurity e Data Protection. Linee guida sicurezza nel procurement ICT. **Conformità del dato** Rischio di conformità. Data Compliance. Sistemi di Data Compliance. GDPR.
Tipologie di attività didattiche previste e relative modalità di svolgimento	L'insegnamento è strutturato in lezioni di didattica frontale, incoraggiando l'interazione e la partecipazione attiva degli studenti. È previsto l'utilizzo di tecnologie digitali per l'erogazione delle lezioni e delle esercitazioni.
Metodi e criteri di valutazione dell'apprendimento	La valutazione dell'apprendimento (sia per studenti frequentanti che non frequentanti) consiste nello svolgimento di una prova scritta contenente quesiti teorici e pratici relativi ai contenuti del corso, proposti attraverso domande a risposta multipla e una prova progettuale. Sarà prevista inoltre una prova orale facoltativa. In questo caso, la prova scritta concorrerà alla composizione del voto finale, nella misura del 70%. Il restante 30% della valutazione si baserà sul colloquio orale finale. La valutazione del colloquio orale è espressa in trentesimi e terrà conto della proprietà di linguaggio, della capacità argomentativa, di analisi critica e di ragionamento.
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	La valutazione dell'apprendimento prevede l'attribuzione di un voto finale espresso in trentesimi. Il voto finale sarà determinato attraverso l'esame scritto sopra dettagliato. In particolare, il test si compone di 20 quesiti a risposta multipla (1 punti per ciascun quesito) e da un quesito di natura progettuale (a cui sono assegnati 10 punti) La concessione della lode sarà valutata per i soli studenti che abbiano raggiunto la valutazione complessiva di 30/30 analizzando la capacità di applicazione delle conoscenze acquisite nonché la capacità di proporre soluzioni corrette ed efficienti nella risoluzione del quesito di natura progettuale.
Propedeuticità	Non sono richiesti prerequisiti specifici, ma è auspicabile una buona familiarità con l'uso di un elaboratore.
Materiale didattico utilizzato e materiale didattico consigliato	Slides, dispense e materiale supplementare forniti dal docente. Sicurezza dei computer e delle reti. William Stallings - Giuseppe Lo Re - Alessandra De Paola. Pearson - Ediz. MyLab. 2022 (ISBN: 9788891915290)