PROGRAMMA DEL CORSO DI SICUREZZA DEI SISTEMI INFORMATICI

SETTORE SCIENTIFICO

ING-INF/05 (IINF-05/A)

CFU

12

ATTIVITÀ DI DIDATTICA INTERATTIVA (DI)

Attività di didattica interattiva (DI)

Le attività di Didattica interattiva consistono, per ciascun CFU, in un'ora dedicata alle seguenti tipologie di attività:
Redazione di un elaborato per ciascuna macro area in cui è suddiviso il programma del corso Partecipazione a forum tematici esplicativi Lettura area FAQ Svolgimento delle prove in itinere con feedback

TESTO CONSIGLIATO

Gli studenti che intendono approfondire le tematiche del corso, integrando le dispense e i materiali forniti dal docente, possono consultare i seguenti volumi:

- INTERNET E LE SUE INSICUREZZE: Strumenti, soggetti e contesti - Giapeto Editore

MODALITÀ DI VERIFICA DELL' APPRENDIMENTO

A prova finale consiste in un questionario a scelta multipla composto da 30 domande con 4 possibili risposte.

L'accesso alla prova scritta è consentito solamente a coloro che abbiano superato l' elaborato proposto nelle sezione di Didattica Interattiva e dopo aver visualizzato almeno 80% delle videolezioni presenti in piattaforma.

OBBLIGO DI FREQUENZA

Obbligatoria online. Ai corsisti viene richiesto di visionare almeno l'80% delle videolezioni presenti in piattaforma e superare almeno due elaborati proposti nella sezione di Didattica Interattiva

ATTIVITÀ DI DIDATTICA EROGATIVA (DE)

Le attività di didattica erogativa consistono, per ciascun CFU, nell'erogazione di 6 videolezioni corredate di testo e questionario finale.

•Il format di ciascuna videolezione prevede il video registrato del docente che illustra le slide costruite con parole chiave e schemi esemplificativi. •Il materiale testuale allegato a ciascuna lezione corrisponde a una dispensa (PDF) c con le informazioni necessarie per la corretta e proficua acquisizione dei contenuti trattati durante la lezione.

OBIETTIVI FORMATIVI PER IL RAGGIUNGIMENTO DEI RISULTATI DI APPRENDIMENTO PREVISTI NELLA SCHEDA SUA

Obiettivo principale del corso è fornire agli studenti le basi per affrontare le problematiche principali relative alla sicurezza dei sistemi informatici. Verranno date le indicazioni fondamentali necessarie per una conoscenza di base dei temi indicati nel programma.
Il corso intende fornire agli studenti la capacità di comprendere i problemi fondamentali della sicurezza per una vasta gamma di sistemi informatici, con particolare riferimento a sistemi di rete, pubbliche amministrazioni e strumenti utilizzati nel quotidiano. Il corso inoltre fornirà capacità di analizzare le vulnerabilità e le loro fonti nei sistemi informatici, di valutare i rischi a cui esse danno luogo, e di fronteggiarli adottando le tecniche di controllo delle vulnerabilità che risultino più appropriate al contesto operativo e sociale in cui si applicano. Infine il corso intende fornire spunti per la valorizzazione degli aspetti sociali, normativi ed etici delle problematiche di sicurezza.

RISULTATI DI APPRENDIMENTO ATTESI

Conoscenza e capacità di comprensione: L’obiettivo del corso è quello di fornire conoscenze in merito alle problematiche relative alla sicurezza e vulnerabilità dei sistemi informatici con particolare riferimento ai sistemi maggiormente utilizzati (web, social networks, apps, ecc.). Lo studente al termine del corso avrà acquisito i concetti per un utilizzo sicuro, consapevole delle tecnologie informatiche ed avrà sviluppato capacità di analisi critica rispetto alle problematiche, gli strumenti ed i rischi connessi.

Capacità di applicare conoscenza e comprensione: il corso ha come obiettivo quello di consentire allo studente di essere in grado di condurre l'analisi di sicurezza di un sistema, di individuarne le possibili vulnerabilità, di sviluppare misure per la prevenzione e la rilevazione di attacchi informatici e di implementare contromisure per la mitigazione degli effetti dei suddetti attacchi.

Autonomia di giudizio: lo studente deve essere in grado di analizzare in maniera autonoma i processi e le tecniche per la valutazione del livello di rischio di un sistema informatico, per il miglioramento della sensibilità e del livello di attenzione alle problematiche relative alla gestione della sicurezza informatica di un sistema o di un’infrastruttura, per la simulazione di scenari di attacco e per l’adozione di adeguate misure di protezione.

Abilità comunicative: il corso tende a rendere lo studente cosciente delle problematiche che si incontrano nell’utilizzo quotidiano delle tecnologie informatiche. Lo studente deve avere la capacità di spiegare, in maniera semplice, a persone non esperte i concetti tecnici e le tematiche scientifiche riguardanti la sicurezza informatica.

Capacità di apprendimento: lo studente sarà in grado di affrontare con autonomia qualsiasi problematica riguardante la sicurezza dei sistemi informatici. Deve essere, inoltre, in grado di aggiornarsi continuamente, tramite la consultazione di testi, pubblicazioni, report tecnici, atti di conferenze, allo scopo di acquisire la capacità di seguire corsi di approfondimento, seminari specialistici e Masters in sicurezza informatica.

PROGRAMMA DIDATTICO: ELENCO VIDEOLEZIONI/MODULI

1 Concetti base di sicurezza 2 Servizi e meccanismi di sicurezza 3 Crittografia simmetrica 4 Crittografia simmetrica: tecniche di sostituzione e di trasposizione 5 Cifratura a blocchi 6 La cifratura DES: Data Encryption Standard 7 La cifratura AES - Advanced Encryption Standard 8 La crittografia multipla 9 Modalità di funzionamento della cifratura a blocchi 10 Segretezza e crittografia simmetrica 11 Crittografia asimmetrica 12 L'algoritmo RSA 13 Autenticazione dei messaggi 14 Le firme digitali 15 Autenticazione in ambienti distribuiti 16 Sicurezza della posta elettronica e PGP 17 SET - Secure Electronic Transaction 18 Intrusioni e software doloso 19 Tipi di malware e DDoS 20 I firewall

---

LA SICUREZZA DELLE RETI: CONCETTI GENERALI: La sicurezza informatica, servizi, meccanismi e attacchi e gli attacchi alla sicurezza.

IL DOCUMENTO INFORMATICO E TRANSAZIONI ONLINE: il documento informatico e la sicurezza. Rischi e pericoli: affidabilità degli strumenti ICT. Rimedi e contromisure: l'analisi del rapporto tra sicurezza reale e sicurezza percepita.

LA GARANZIA DELLA RISERVATEZZA: La firma digitale e il documento informatico, la normativa di riferimento in materia di firma digitale, la firma elettronica, la firma elettronica qualificata: il relativo quadro normativo di riferimento a livello europeo e nazionale, la legislazione in merito alla contraffazione di firme digitali e di documenti informatici, orientamenti giurisprudenziali in ordine alla firma digitale e al reato di falsificazione della stessa. Rischi e pericoli, gli svantaggi e le vulnerabilità della firma digitale, i possibili attacchi informatici ai documenti firmati digitalmente. Rimedi e contromisure. Gli aspetti forensics.

LA GARANZIA DELLA TRASMISSIONE PEC: la Posta Elettronica Certificata: caratteristiche, i principali vantaggi della PEC, sintesi normativa in tema di Posta Elettronica Certificata, gli standard internazionali e Posta Elettronica Certificata, il regolamento d'uso della PEC. Rischi e pericoli connessi alla sicurezza, rimedi e contromisure. Gli aspetti forensics.

SICUREZZA INFORMATICA E PUBBLICA AMMINISTRAZIONE: il contesto di riferimento, ambito normativo, Il codice dell'Amministrazione Digitale e i suoi corollari, La centralità della sicurezza informatica nell'art. 51 CAD: la difficile opera di coordinamento con le altre disposizioni in materia. La politica di sicurezza nelle pubbliche amministrazioni, dall'analisi del rischio agli audit di sicurezza: le fasi del ciclo di gestione della sicurezza informatica. Business Continuity Management e Disaster Recovery, cenni all'architettura del CERT-SPC e delle Unità Locali per la Sicurezza. Le figure di responsabilità del processo di gestione della sicurezza. Reati informatici e responsabilità c.d. amministrativa, i reati informatici commessi in danno dell'amministrazione: in particolare, l'accesso abusivo ad un sistema informatico o telematico da parte di un pubblico ufficiale, cenni ai casi di attacco ad un sistema informatico pubblico: l'importanza della digital evidence.

CODICI ANONIMATO ED INDAGINI DIGITALI: Accesso, sicurezza e privacy, la vita privata nella società tecnologica. La vulnerabilità negli strumenti di comunicazione. La crittografia, i metodi crittografici, la crittografia asimmetrica, la

stenografia e il watermarking. Le ragioni dell'anonimato, anonimato e spamming, l'anonimato nella legislazione, l'anonimato e la tecnologia, i server proxy, le reti anonime, la posta elettronica anonima, l'intercettazione delle conversazioni voip.

LA VALUTAZIONE DELLA PROPRIA IN-SICUREZZA INFORMATICA: La vita privata nella società tecnologica, i malware, virus, trojan horse, worm, rootikit, botnet, phishing, zeus: uno dei più noti esempi di botnet. Rimedi e contromisure. Analisi live di un sistema host infettato del malware zeus. Analisi post-mortem di un sistema unix compromesso. La sicurezza di essere insicuri.

L'INSICUREZZA DELLA PROPRIA ED ALTRUI IDENTITA': Nativi o immigrati digitali: Il fenomeno della "insicurezza globale", la definizione del contesto e i principali riferimenti normativi in tema di identità digitale, il furto di identità. Attacchi alla persona e contraffazioni, le tecniche dell'ingegneria sociale, le false sicurezze di internet: i vettori d'attacco conosciuti e non, il pharming, il phishing, il tabnapping, lo smishing: ingannati dal proprio smartphone, codici cattivi, codici attivi e cookies, i rootkit, l'instant messaging e la chat, social networks sites, p2p, voip. La sicurezza reale, le impostazioni di sicurezza del browser web, i certificati digitali dei siti web, comprendere le licenze d'uso del software, sicurezza delle reti wireless, la tecnologia bluetooth, protezione dei dispositivi portatili, protezione dei dat trasportati, le conseguenze delle proprie in-sicurezze, la responsabilità per aziende e liberi professionisti.

L'INSICUREZZA DEI SOCIAL NETWORK: i social network, facebook, la normativa in tema di social network. I pericoli per l'utente, per la sua privacy e i suoi beni. Valide contromisure.