PROGRAMMA DEL CORSO DI SICUREZZA E DISASTER RECOVERY NEI SISTEMI INFORMATICI

SETTORE SCIENTIFICO

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

CFU

6

OBIETTIVI

/**/
Il corso si propone di fornire agli studenti le competenze di base per l'analisi e il progetto di sistemi informatici sicuri

RISULTATI DI APPRENDIMENTO ATTESI

/**/
Conoscenza e capacità di comprensione

Lo studente al termine del corso sarà in grado di rappresentare la dinamica di un sistema di sicurezza informatica facendo uso di opportuni modelli e sarà in grado di analizzare il comportamento di essi attraverso specifiche metodologie. Sarà inoltre in grado di risolvere alcuni problemi decisionali, con particolare riferimento ai problemi appartenenti ai livelli tattico e operativo.

Capacità di applicare conoscenza e comprensione
Gli sono capaci di applicare le loro conoscenze e capacità di comprensione risolvendo problemi collegabili a tematiche nuove o non familiari; in tal modo sono capaci di operare in contesti più ampi ed interdisciplinari nei quali si richiede la soluzione di problematiche ambientali. Tali capacità vengono applicate mediante tecniche e strumenti per la progettazione di componenti, sistemi e processi; mediante l’analisi ed interpretazione dei dati.

Autonomia di giudizio
Una buona capacità di selezionare, elaborare e interpretare dati viene acquisita in relazione sia al trattamento delle misure, sia più in generale alla gestione dei dati di interesse.

Abilità comunicative
L’esposizione del materiale didattico e l’ascolto delle lezioni consentiranno agli studenti di argomentare con un lessico preciso ed appropriato.

Capacità di apprendimento

Gli studenti sviluppano le capacità di apprendimento necessarie per continuare in modo autonomo od auto-diretto gli approfondimenti sia in campo professionale che scientifico.

MODALITÀ DI ESAME ED EVENTUALI VERIFICHE DI PROFITTO IN ITINERE

/**/
L’esame può essere sostenuto sia in forma scritta che in forma orale. Gli appelli orali sono previsti nella sola sede centrale di Roma. Gli esami scritti, invece, possono essere sostenuti sia nella sede centrale che nelle sedi periferiche.

L’esame orale consiste in un colloquio nel corso del quale il docente formula di solito tre domande. L’esame scritto consiste nello svolgimento di un test con 31 domande. Per ogni domanda lo studente deve scegliere una di 4 possibili risposte. Solo una risposta è corretta.
Sia le domande orali che le domande scritte sono formulate per valutare sia il grado di comprensione delle nozioni teoriche sia la capacità di ragionare utilizzando tali nozioni. Le domande sulle nozioni teoriche consentiranno di valutare il livello di comprensione. Le domande che richiedono l’elaborazione di un ragionamento consentiranno di valutare il livello di competenza e l’autonomia di giudizio maturati dallo studente.
Le abilità di comunicazione e la capacità di apprendimento saranno valutate attraverso le interazioni dirette tra docente e studente che avranno luogo durante la fruizione del corso (videoconferenze ed elaborati proposti dal docente).

MODALITÀ DI ISCRIZIONE E DI GESTIONE DEI RAPPORTI CON GLI STUDENTI

/**/
L’iscrizione ed i rapporti con gli studenti sono gestiti mediante la piattaforma informatica che permette l’iscrizione ai corsi, la fruizione delle lezioni, la partecipazione a forum e tutoraggi, il download del materiale didattico e la comunicazione con il docente. Un tutor assisterà gli studenti nello svolgimento di queste attività.

ATTIVITÀ DI DIDATTICA EROGATIVA (DE)

/**/
36 Videolezioni + 36 test di autovalutazione Impegno totale stimato: 36 ore

ATTIVITÀ DI DIDATTICA INTERATTIVA (DI)

/**/
Redazione di un elaborato

Partecipazione a una web conference

Svolgimento delle prove in itinere con feedback

Svolgimento della simulazione del test finale

Totale 6 ore

ATTIVITÀ DI AUTOAPPRENDIMENTO

/**/
108 ore per lo studio individuale

LIBRO DI RIFERIMENTO

/**/
Dispense del docente. R. Anderson "Security engineering", Wiley.

PROGRAMMA DIDATTICO

Il docente si riserva il diritto di modificare i titoli delle delle lezioni

1 - INTRODUZIONE ALLA CYBERSECURITY 2 - ELEMENTI FONDAMENTALI DEL PERIMETRO DI SICUREZZA E TERMINOLOGIA 3 - SICUREZZA DELLE INFORMAZIONI 4 - MINACCE, ATTACCANTI E RISCHIO INFORMATICO 5 - ATTACCHI, CONTROLLI E CONTROMISURE 6 - AUTENTICAZIONE 7 - MECCANISMI DI AUTENTICAZIONE 8 - CONTROLLO DEGLI ACCESSI 9 - CRITTOGRAFIA: CONCETTI GENERALI 10 - CIFRATURA A CHIAVE SIMMETRICA 11 - CIFRATURA A CHIAVE ASIMMETRICA 12 - SCAMBIO DELLE CHIAVI E CERTIFICATI 13 - SUPPORTO ALL'INTEGRITA' DELL'INFORMAZIONE 14 - FIRMA DIGITALE 15 - SUPPORTO ALLA DISPONIBILITÀ 16 - TIPI DI ATTACCO ALLA DISPONIBILITA' 17 - DISTRIBUTED DENIAL OF SERVICE E BOTNET 18 - I MALWARE 19 - COMPORTAMENTO ED EFFETTI DI UN MALWARE 20 - PROPAGAZIONE, ATTIVAZIONE E AREE DI RESIDENZA DI UN MALWARE 21 - CONTROMISURE PER I MALWARE 22 - ATTACCHI INFORMATICI: ATTACCHI AI BROWSER 23 - ATTACCHI TRAMITE SITI WEB 24 - ATTACCHI TRAMITE E-MAIL 25 - DIFESA PERIMETRALE DELLA RETE 26 - I FIREWALL 27 - SISTEMI DI DIFESA DALLE INTRUSIONI 28 - INTRUSION PREVENTION SYSTEMS E SIEM 29 - ANALISI E ASSESSMENT DI VULNERABILITÀ 30 - DISASTER RECOVERY - PANORAMICA 31 - DISASTER RECOVERY COME ATTIVITÀ STRATEGICA 32 - DISASTER RECOVERY COME PIANO OPERATIVO 33 - DISASTER RECOVERY COME PROGETTO AZIENDALE 34 - VERSO UN PIANO DI RIPRISTINO 35 - SVILUPPARE IL PIANO DELLE WORKSTATION E DEI LOCALI 36 - SVILUPPARE IL PIANO DI RIPRISTINO DI INFRASTRUTTURA IT E DEI DATI