Logo Image not found or type unknown

PROGRAMMA DEL CORSO DI SICUREZZA DELLE RETI E CYBER SECURITY

SETTORE SCIENTIFICO

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

CFU

6

SETTORE SCIENTIFICO DISCIPLINARE

IINF-03/A

ANNO DI CORSO

III Anno

TIPOLOGIA DI ATTIVITÀ FORMATIVA

/**/
Base q

Caratterizzante X

Affine q

Altre attività q

NUMERO DI CREDITI

6 CFU

DOCENTE

Roberto Caldelli

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.

OBIETTIVI FORMATIVI SPECIFICI

/**/
Il corso si propone di fornire allo studente le competenze necessarie per comprendere e valutare problematiche di sicurezza informatica nell'ambito di realtà produttive, progettare sistemi informatici e reti con un certo livello di sicurezza, gestire le attività legate alla sicurezza informatica anche in riferimento gli obblighi normativi italiani.

RISULTATI DI APPRENDIMENTO SPECIFICI

/**/
Conoscenza e capacità di comprensione

Il corso intende fornire le conoscenze utili per comprendere gli strumenti tecnologici adoperati per garantire sicurezza nelle comunicazioni di rete in relazione alle applicazioni e alle funzionalità di sistema.

Conoscere la crittografia e le tecniche fondamentali di cifratura; conoscenza e comprensione delle più diffuse tipologie di attacchi ai sistemi di comunicazione. Conoscenza delle problematiche di sicurezza in reti interconnesse.

Capacità di applicare conoscenza e comprensione

Il corso trasferisce la capacità di applicare le conoscenze acquisite in processi di accertamento della vulnerabilità delle reti, di verificare e testare l'applicazione di procedure, strumenti e standard di sicurezza.

Autonomia di giudizio

Attraverso le competenze acquisite, lo studente potrà valutare punti di forza e punti di debolezza di soluzioni, tecniche, strumenti e servizi di sicurezza per le comunicazioni in rete.

Abilità comunicative

Lo studente svilupperà la capacità di interagire e comunicare con operatori e fornitori di tecnologie e servizi di sicurezza; capacità di comunicare e discutere in team di progettazione ed implementazione della sicurezza in reti di TLC.

Capacità di apprendimento

La capacità di apprendimento sarà stimolata attraverso la somministrazione di esercitazioni operative, caricate in piattaforma nella sezione elaborati, finalizzata anche a verificare l’effettiva comprensione degli argomenti trattati.

Lo studente acquisirà, inoltre, la capacità di seguire l'evoluzione scientifica e tecnica in ambito cybersecurity, di autoaggiornarsi su standard e procedure, su tecnologie e strumenti, sulla comparsa di nuove tipologie di rischio e di attacco.

PROGRAMMA DIDATTICO

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 - Gestione delle chiavi e scambio Diffie-Hellman 14 - Autenticazione dei messaggi 15 - Codici MAC e funzioni hash 16 - L'algoritmo SHA-512 17 - Gli algoritmi HMAC e CMAC 18 - Le firme digitali 19 - IPSec 20 - IPSec e il protocollo ESP 21 - Il protocollo SSL 22 - I protocolli TLS e HTTPS 23 - SET - Secure Electronic Transaction 24 - Intrusioni e software doloso 25 - Tipi di malware e DDoS 26 - I firewall 27 - Blockchain e Proof-of-Work 28 - Blockchain e il Ledger Distribuito 29 - Comunicazioni anonime: i protocolli Crowds e Mix 30 - Comunicazioni anonime: Tor e Deep Web

TIPOLOGIE DI ATTIVITÀ DIDATTICHE PREVISTE E RELATIVE MODALITÀ DI SVOLGIMENTO

L’insegnamento è articolato in videolezioni di circa 30 minuti corredate da dispense, slide e questionario di autovalutazione.

Per ogni insegnamento è prevista1 videolezione di didattica erogativa in modalità sincrona a contenuto innovativo ed interattivo, secondo modalità definite dal docente di riferimento,vi è altresì la possibilità di redazionedi un elaborato per insegnamento, differenziato in termini di difficoltà rispetto all’ampiezza dei CFU assegnati.

Il modello didattico 2025-2026, in ottemperanza al D.M. 1835 del 6 dicembre 2024, prevede di norma, per ogni CFU, un totale di almeno 7 ore di didattica. La didattica erogativa è perciò effettuata dall’Anno Accademico 2025/2026 per l’80% in modalità asincrona, articolata in un numero di videolezioni coerente ai CFU complessivi del singolo insegnamento, corredate da materiale didattico adeguato allo studio individuale e, per almeno il 20%, in modalità sincrona

La didattica erogativa asincrona prevede per ogni ora una videolezione registrata, una dispensa corredata da riferimenti bibliografici, note, tabelle, immagini, grafici ed un questionario di dieci domande di autovalutazione con quattro possibili risposte di cui solo una corretta e tre distrattori, oltre un file di riepilogo relativo agli obiettivi ed alla struttura in paragrafi della lezione, con l’aggiunta di alcune parole chiave. Nel dettaglio la videolezione corrisponde alla singola lezione teorica del docente.La didattica sincrona si compone di una web conferenze per CFU e di un elaborato per insegnamento, differenziato in termini di difficoltà rispetto all’ampiezza dei CFU assegnati.L’obiettivo della didattica erogativa in modalità sincrona è assicurare tutte quelle attività che tipicamente richiedono apprendimenti “in situazione” o rapporto “face to face”, quali laboratori, seminari, esperienze sul campo, tirocini, ecc., tenendo conto anche delle metodologie a carattere innovativo e volte a favorire l’interazione docente-studenti e tra studenti

Sono previsti:

interventi didattici rivolti da parte del docente/tutor all’intera classe (o a un suo sottogruppo), tipicamente sotto forma di dimostrazioni o spiegazioni aggiuntive (ad esempio dimostrazione o suggerimenti operativi su come si risolve un problema, esercizio esimilari); gli interventi brevi effettuati dai corsisti (ad esempio in ambienti di discussione o di collaborazione); le e-tivity strutturate (individuali o collaborative), sotto forma tipicamente di report, esercizio, studio di

caso, problem solving, web quest,progetto,produzionediartefatto(ovariantiassimilabili),effettuati dai corsisti, con relativo feed-back; le forme tipiche di valutazione formativa, con il carattere di questionari o test initinere; le esperienze di apprendimento in situazione realizzabili attraverso ambienti di simulazione, oppure attraverso la virtualizzazione di laboratori didattici.
Nelle suddette attività convergono molteplici strumenti didattici, che agiscono in modo sinergico sul percorso di formazione ed apprendimento dello studente. La partecipazione attiva alle suddette attività ha come obiettivo quello di stimolare gli studenti lungo tutto il percorso didattico e garantisce loro la possibilità di ottenere una valutazione aggiuntiva che si sommerà alla valutazione dell'esame finale.

Nel computo delle ore della didattica erogativa sono escluse le interazioni a carattere orientativo sui programmi, sul Corso di Studio, sull'uso della piattaforma e simili, che rientrano nei servizi di tutoraggio per l'orientamento. Sono altresì escluse le ore di tutorato didattico disciplinare, cioè la mera ripetizione di contenuti già proposti nella forma erogativa attraverso colloqui di recupero o approfondimento one-to-one.

MODALITÀ E CRITERI DI VALUTAZIONE DELL'APPRENDIMENTO

/**/
La partecipazione alla didattica erogativa ha la finalità, tra le altre, di valutare lo studente durante l'apprendimento in itinere.

L'esame finale può essere sostenuto in forma scritta o in forma orale; lo studente può individuare, in autonomia, la modalità di svolgimento della prova, sempre rispettando la calendarizzazione predisposta dall'Ateneo.

L'esame orale consiste in un colloquio nel corso del quale il docente formula almeno tre domande.

L'esame scritto consiste nello svolgimento di un test a risposta multipla con 31 domande. Per ogni domanda lo studente deve scegliere una delle 4 possibili risposte. Solo una risposta è corretta.

Sia la verifica in forma orale che i quesiti in forma scritta sono formulati per valutare il grado di comprensione delle nozioni teoriche e la capacità di sviluppare il ragionamento utilizzando le nozioni acquisite per verificare la capacità di apprendimento ovvero il livello di apprendimento raggiunto dallo studente. I quesiti 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 studenti che avranno luogo durante la fruizione del corso proposte dal docente o dal tutor.

CRITERI DI MISURAZIONE DELL'APPRENDIMENTO E ATTRIBUZIONE DEL VOTO FINALE

/**/
La didattica sincrona garantisce una premialità massima di 2 punti che si somma al voto dell'esame finale, suddivisa in 1 punto per la didattica erogativa sincrona (Webconference) ed 1 punto didattica erogativa sincrona (Elaborato). La premialità massima per le Webconference è di un punto sul voto di esame. Ogni studente può partecipare a tutte le Webconference erogate. Per ciascuna di esse, il superamento del test finale di apprendimento –che richiede almeno quattro risposte corrette su cinque domande relative al tema trattato – consente di ottenere un punteggio pari a 0,5. Una volta raggiunto un punteggio totale di 1, allo studente viene riconosciuta la premialità. La redazione dell'elaborato consente una premialità pari ad 1 punto sul voto dell'esame, se considerato sufficiente. Saranno rese disponibili due tracce di elaborati.

È data facoltà allo studente di partecipare alla didattica erogativa sincrona.

La valutazione finale ha lo scopo di misurare il grado di comprensione delle nozioni teoriche e la capacità di sviluppare il ragionamento utilizzando le nozioni acquisite per verificare la capacità di apprendimento ovvero il livello di apprendimento raggiunto dallo studente. Il giudizio riguarda l'intero percorso formativo del singolo insegnamento ed è di tipo sommativo.
Il voto finale dell'esame di profitto tiene conto del punteggio ottenuto nella verifica di profitto al quale si sommano le premialità che lo studente può aver ottenuto partecipando alla didattica erogativa sincrona e deriva, quindi, dalla somma delle due valutazioni. Il voto derivante dalla didattica sincrona verrà sommato al voto dell'esame se quest'ultimo sarà pari o superiore a diciotto trentesimi.
Il voto finale è espresso in trentesimi. Il voto minimo utile al superamento della prova è di diciotto trentesimi.

Ciascun test dovrà essere composto da 31 domande, così da garantire la possibilità di conseguire la lode, in ottemperanza alle norme Europee sul Diploma Supplement. L'attribuzione della lode è concessa esclusivamente allo studente che ha risposto positivamente alle prime 30 domande ed anche all'ultima domanda.

ATTIVITÀ DI DIDATTICA EROGATIVA ASINCRONA

Di norma massimo l'80% delle lezioni è svolto in modalità asincrona.

ATTIVITÀ DI DIDATTICA EROGATIVA SINCRONA CON RELATIVO FEED-BACK AL SINGOLO STUDENTE DA PARTE DEL DOCENTE O DEL TUTOR

Almeno il 20% delle lezioni è svolto in modalità sincrona e possono prevedere:

è Partecipazione web conference

è Redazione di un elaborato

è Svolgimento delle prove in itinere con feedback

è Svolgimento della simulazione del test finale

MATERIALE DIDATTICO UTILIZZATO

è Videolezioni

è Dispense predisposte dal docente e/o slide del docente

è Questionario di autovalutazione

è Materiali predisposti per le lezioni sincrone

è Testo di riferimento suggerito dal docente (facoltativo)

"Crittografia e Sicurezza delle Reti" 2/ed., William Stallings, Ed. McGraw-Hill. "Cryptography and Network Security", 7/ed., William Stallings, Pearson.

Il materiale didattico è sempre disponibile in piattaforma e consultabile dallo studente nei tempi e nelle modalità ad egli più affini.