REGOLAMENTO DEL CORSO DI STUDIO TRIENNALE

Ingegneria e Scienze Informatiche per la Cybersecurity

(Interclasse L-8 L-31) A.A. 2023/24

(approvato nella seduta del CdS del 12/5/23)

Art.1 Presentazione generale del corso: Oggetto e Finalità

Scuola	SCUOLA INTERDIPARTIMENTALE DELLE SCIENZE, DELL'INGEGNERIA E DELLA SALUTE
Dipartimento	Dipartimento di Scienze Economiche Giuridiche Informatiche e Motorie
Codice Corso di Studio	ID SUA=1589813 - ID RAD=1415604 – CODICIONE=0630206200800005
Ordinamento	D.M. 270
Classe di Laurea	Interclasse L08 (CLASSE DELLE LAUREE IN INGEGNERIA DELL'INFORMAZIONE) L31 (CLASSE DELLE LAUREE IN SCIENZE E TECNOLOGIE INFORMATICHE)
Livello	I LIVELLO
Durata nominale del Corso	3 ANNI
Primo A.A. di attivazione	2022-2023
Sede del corso	Via Guglielmo Pepe - rione Gescal 80035 – Nola (NA)
Coordinatore CdS	Luigi Coppolino
Sito web della Scuola	https://sisis.uniparthenope.it/
Sito web del Dipartimento	https://disegim.uniparthenope.it/
Sito web del Corso di Studio	https://disegim.uniparthenope.it/disegim/cybersecurity-disegim

Il Corso di Laurea Triennale si prefigge l'obiettivo di far acquisire ai futuri laureati conoscenze e competenze nell'ambito della cybersecurity. In particolare, il percorso di studio è orientato alla formazione di laureati, che siano in grado di affrontare e gestire problematiche di sicurezza informatica, adottando un approccio multidisciplinare che preveda il possesso di competenze di natura teorica, metodologica e tecnologica. Il Corso di Laurea fornirà sia solide conoscenze di base nei settori delle scienze matematiche e fisiche, sia un'ampia formazione metodologica e sperimentale nelle discipline dell'ingegneria e delle scienze informatiche, declinate nel contesto della sicurezza dei dati e dei sistemi. Grazie alle competenze acquisite, il futuro laureato sarà in grado di analizzare, comprendere ed utilizzare i risultati dei continui e costanti avanzamenti scientifici e tecnologici caratterizzanti il settore della sicurezza informatica.

Art. 2 Obiettivi formativi e sbocchi occupazionali e professionali

2.1 Obiettivi formativi.

Il corso di laurea si prefigge l'obiettivo di fornire al futuro laureato un'ampia, solida e approfondita preparazione, in termini di concetti, metodologie e tecnologie, su temi relativi alla sicurezza di dati e sistemi.

Il corso fornisce sia un'essenziale conoscenza di base nei settori delle scienze matematiche e fisiche, sia una verticale preparazione su insegnamenti dell'ingegneria e delle scienze informatiche, declinati nel dominio della cybersecurity.

Il corso ha, inoltre, l'obiettivo di fornire approfondite conoscenze e competenze operative che possano mettere i laureati nelle condizioni di accedere con successo a tutti i contesti professionali, industriali e della Pubblica Amministrazione interessati all'utilizzo di soluzioni e strumenti per garantire la sicurezza dei dati trattati, dei servizi forniti e dei sistemi gestiti.

Le conoscenze informatiche sono integrate da conoscenze interdisciplinari riguardanti altri ambiti caratterizzanti

previsti per l'Ingegneria dell'Informazione, quali campi elettromagnetici, e le telecomunicazioni, e da ambiti interdisciplinare fortemente connessi alle problematiche della sicurezza informatica (aspetti legali e gestionali legati all'Informatica e problematiche di sicurezza nei sistemi di controllo industriale).
Il percorso formativo è progettato per essere altamente professionalizzante e quindi formare un laureato immediatamente pronto per essere immesso nel mondo del lavoro, tuttavia la laurea in Ingegneria e Scienze Informatiche per la cybersecurity è costruita per rendere possibile una prosecuzione, con opportuna selezione degli insegnamenti a scelta libera, sui corsi di laurea magistrale in Informatica Classe LM-18, in Ingegneria delle Telecomunicazioni Classe LM-27, disponibili anche nell'offerta formativa dell'Università Parthenope, in Sicurezza Informatica Classe LM-66 ed in Ingegneria Informatica LM-32.

2.2 Sbocchi occupazionali e professionali.
La solida e consistente preparazione ottenuta in ambito sperimentale ed applicativo consentirà al laureato in Ingegneria e Scienze Informatiche per la cybersecurity un agevole inserimento sia nel mondo aziendale che nella pubblica amministrazione principalmente con il ruolo di tecnico specializzato nella gestione sicura di sistemi, reti ed infrastrutture critiche, e nell'analisi e sviluppo di applicazioni attraverso l'uso di metodologie e tecnologie in grado di garantirne la sicurezza informatica.
Il laureato in Ingegneria e Scienze Informatiche per la cybersecurity potrà inoltre inserirsi nel mondo delle professioni in qualità di consulente per la sicurezza dei sistemi, dei dati e delle reti informatiche.
Infine, in virtù della recente entrata in vigore della normativa sulla protezione dei dati, un ulteriore sbocco professionale per il laureato in Ingegneria e Scienze Informatiche per la cybersecurity sarà rappresentato da aziende di prodotti e servizi ed enti della pubblica amministrazione chiamati a garantire il trattamento sicuro di dati sensibili.
In particolare il corso prepara alle professioni di (codifiche ISTAT):

1. Tecnici programmatori - (3.1.2.1.0)
2. Tecnici esperti in applicazioni - (3.1.2.2.0)
3. Tecnici web - (3.1.2.3.0)
4. Tecnici gestori di basi di dati - (3.1.2.4.0)
5. Tecnici gestori di reti e di sistemi telematici - (3.1.2.5.0)

Per ulteriori dettagli si consulti la scheda SUA 2022/23 del Corso di Studio con particolare riferimento alla sezione A2.a.

Art. 3 Ammissione e preparazione iniziale
Il Corso di Studio è ad accesso libero, senza prova selettiva di accesso.

3.1 Requisiti di ammissione
Per essere ammessi al Corso di Laurea occorre essere in possesso di un diploma di scuola secondaria superiore o di altro titolo di studio conseguito all'estero, riconosciuto idoneo. Il riconoscimento dell'idoneità dei titoli di studio conseguiti all'estero, ai soli fini dell'ammissione a corsi di studio, è deliberata dall'Università degli Studi di Napoli Parthenope, nel rispetto degli accordi internazionali vigenti.

3.2 Procedura di ammissione
Per l'accesso al Corso di Studio in Ingegneria e Scienze Informatica per la Cybersecurity gli studenti possono sostenere una prova d'ingresso e di autovalutazione (Test CISIA TOLC-S di livello nazionale) **non selettiva**, che ha lo scopo di fornire indicazioni generali sulla preparazione dello studente nelle discipline di base e sulle sue

attitudini a intraprendere gli studi specifici. Il test di ingresso CISIA può essere sostenuto dagli studenti esclusivamente nella modalità on-line CISIA, o, più sinteticamente, TOLC-S: è un test nazionale erogato in più sedute nel periodo Febbraio-Settembre e si svolge in modalità telematica presso tutte le sedi d'Italia consorziate CISIA ed aderenti al 'Progetto TOLC'.
L'iscrizione al test TOLC va effettuata on-line sul portale gestito dal CISIA (www.cisiaonline.it). Il test sarà considerato valido anche se sostenuto in altri Atenei che adottino il medesimo test di accesso.
Ulteriori informazioni sulla struttura dei test sono reperibili al seguente link:
https://www.cisiaonline.it/area-tematica-tolc-scienze/home-tolc-s/
Il test di ingresso contiene anche la sezione di lingua inglese. Quest'ultima, sebbene non concorra al superamento del TOLC, offre allo studente una opportunità aggiuntiva: il raggiungimento di un punteggio uguale o superiore ad una fissata soglia (pubblicata sul sito del Dipartimento) consente di ottenere il riconoscimento dei 3 Crediti Formativi Universitari di lingua inglese previsti dall'ordinamento didattico del Corso di Laurea.

3.3 Attività di accoglienza per gli immatricolati
Il Corso di Studio organizza, appena prima dell'inizio dei corsi, un evento di benvenuto per le nuove matricole per introdurre al nuovo ciclo di studi universitario coloro che si sono iscritti al primo anno e presentare loro sia gli insegnamenti del primo anno sia l'insieme degli strumenti di supporto alla didattica (piattaforma di e-learning, sistema di streaming, siti web istituzionali: di Ateneo, di Scuola, di CdS, portale degli studenti).

3.4 Valutazione delle competenze in ingresso
La valutazione in ingresso è effettuata mediante test CISIA TOLC-S di livello nazionale. La prova consiste in questionari a risposta multipla su argomenti di Matematica di Base, Ragionamento e Problemi, Comprensione del Testo, Scienze di Base (pesato 0,1). Il test di ingresso contiene anche la sezione di lingua inglese. Quest'ultima, sebbene non concorra al superamento del TOLC, offre allo studente una opportunità aggiuntiva: il raggiungimento di un punteggio uguale o superiore a 20/30 consente di ottenere il riconoscimento dei 3 Crediti Formativi Universitari di lingua inglese previsti dall'ordinamento didattico del Corso di Laurea.
I risultati del TOLC vengono sostanzialmente utilizzati per accertare l'esistenza di eventuali carenze formative. Il mancato superamento della prova d'ingresso o il non aver proprio sostenuto il test, non impedisce però l'immatricolazione al Corso di Studio.

3.4.1 Modalità di Svolgimento
L'iscrizione al test va effettuata on line, sul portale www.cisiaonline.it
Allo stesso indirizzo sono disponibili tutte le informazioni necessarie agli studenti su come effettuare la registrazione all'Area TOLC e l'iscrizione al test, ed è inoltre possibile effettuare esercitazioni e prove di posizionamento (https://www.cisiaonline.it/area-tematica-tolc-cisia/tolc-esercitazioni-e-simulazioni/) e accedere al MOOC (Massive Open Online Courses) di Matematica di base (https://www.cisiaonline.it/archivio-mooc/home/).

3.4.2 Obblighi formativi aggiuntivi
In caso di mancato superamento del test, alle matricole saranno attribuiti Obblighi Formativi Aggiuntivi (OFA) consistenti nell'impossibilità a sostenere esami del secondo anno senza aver prima superato gli esami di Matematica I e Programmazione. Gli OFA si riterranno comunque soddisfatti in caso di superamento del test finale erogato in occasione dei precorsi di Matematica e Programmazione tenuti nel mese di settembre dal Dipartimento di Scienze Economiche, Giuridiche, Informatiche e Motorie.

Art. 4 Organizzazione didattica

Il Corso di Studio prevede il superamento di 20 esami, per un totale di 162 CFU, di cui 2 esami, 12 CFU, in attività scelte liberamente dallo studente fra gli insegnamenti attivati presso l'Ateneo. A questi si sommano una prova di lingua inglese, 3 CFU, un tirocinio finale da 9 CFU ed una prova finale per 6 CFU, per un totale di 180 CFU. I corsi sono organizzati su due semestri ciascun dei quali si compone di un periodo trimestrale di frequenza ai corsi e studio autonomo e di un ulteriore trimestre dedicato esclusivamente a sostenere gli esami di profitto e, in quello finale, la preparazione e la discussione della tesi.

4.1 Manifesto degli studi

Il Manifesto degli Studi è reperibile al seguente link ed è riportato in Appendice A:
https://disegim.uniparthenope.it/disegim/cybersecurity-disegim

4.2 Calendario

Il Calendario Accademico è aggiornato annualmente ed è consultabile al seguente link:
https://disegim.uniparthenope.it/disegim/cybersecurity-disegim

Il Calendario delle Lezioni è aggiornato semestralmente, nei mesi di settembre e di febbraio, ed è consultabile al link:
https://disegim.uniparthenope.it/disegim/cybersecurity-disegim

4.3 Docenti

L'elenco dei Docenti è aggiornato annualmente, nel mese di settembre, ed è consultabile al seguente link:
https://uniparthenope.coursecatalogue.cineca.it/

4.4 Piano di studi individuale

Ciascuno studente può predisporre un piano di studi individuale diverso da quello previsto dal manifesto degli studi, purché coerente con l'ordinamento didattico del Corso di Studio. Il piano di studi individuale sarà sottoposto al vaglio e all'approvazione del Consiglio del Corso di Studio.

4.5 *Obblighi di frequenza e modalità di svolgimento delle attività didattiche*

Il corso è a tempo pieno e comprende la partecipazione a lezioni, esercitazioni ed attività di laboratorio. La frequenza non è obbligatoria, ma è vivamente consigliata per consentire una continua interazione con i docenti e facilitare l'apprendimento.

Il corso è erogato in modalità mista, pertanto, un terzo delle lezioni di ciascun insegnamento è erogato a distanza mediante canali telematici.
Le lezioni a distanza sono erogate in modalità sincrona, garantendo modalità di svolgimento e interazione adeguate.
Le lezioni frontali convenzionali, nella misura dei restati due terzi del corso, si svolgono in classe secondo le modalità liberamente adottate dal docente.

Per gli studenti con esigenze specifiche che comportano l'impossibilità a seguire con regolarità ed assiduità le lezioni - quali ad esempio: studenti affetti da particolari disabilità; studenti lavoratori; studenti atleti; studenti adulti o studenti genitori; studenti detenuti - il CdS favorisce l'adozione di forme di supporto didattico a distanza quali la registrazione delle lezioni per la successiva fruizione asincrona o, nel caso di lezioni in presenza, l'attivazione di collegamenti in remoto, purché l'attività didattica sia strutturata e svolta principalmente per gli studenti presenti in classe. In caso di registrazione delle lezioni i file saranno disponibili sulla piattaforma per un

massimo di 48 ore.
In tutti i casi le modalità di svolgimento degli insegnamenti devono rispettare la normativa vigente di Ateneo.

4.6 Propedeuticità
Non sono previste propedeuticità, anche se per ciascun insegnamento sono definiti i prerequisiti, indicati nelle schede degli insegnamenti, che costituiscono un suggerimento per gli studenti per l'ordinato procedere degli studi e il superamento degli esami.

4.7 Impegno a tempo parziale
Gli studenti che per ragioni di lavoro, familiari, di salute o per altri validi motivi reputino di non essere in grado di frequentare con continuità le attività didattiche previste dal Corso di Studio di loro interesse e ritengano di non poter sostenere i relativi esami e verifiche di profitto nei tempi previsti dai rispettivi regolamenti didattici, possono chiedere l'iscrizione a tempo parziale. L'iscrizione a tempo parziale prevede la ripartizione in due anni accademici consecutivi (per un numero di crediti sostenuti annualmente compreso fra un minimo di 26 CFU ed un massimo di 34 CFU) del totale dei crediti stabiliti dal Regolamento didattico per ogni anno a tempo pieno. L'iscrizione a tempo parziale è ammessa in favore solo degli studenti che si immatricolano o si iscrivono in corso a Corsi di studio di I livello e di II livello. Per ulteriori informazioni di dettaglio si consiglia di rivolgersi alla Segreteria Studenti e/o fare riferimento a Regolamento di Ateneo disponibile al link: https://www.uniparthenope.it/sites/default/files/statuto_regolamenti/didattica/nuovo_regolamento_part_time_1718.pdf.

4.8 Interruzione degli studi
Per informazioni sulle modalità di interruzione degli studi, si rimanda al Regolamento Didattico di Ateneo: https://www.uniparthenope.it/ateneo/statuto-e-regolamenti.

4.9 Modalità di verifica dell'apprendimento
La verifica dell'apprendimento può essere svolta dal docente dell'insegnamento prevedendo una sola prova scritta, una sola prova orale o entrambe. Le modalità di svolgimento sono a discrezione del docente del singolo insegnamento. Sul portale studenti esse3 è possibile reperire le informazioni dettagliate: https://uniparthenope.esse3.cineca.it.

4.10 Commissioni di esame
Tenendo conto di quanto previsto dall'art. 36 del Regolamento didattico sulla formazione delle Commissioni degli esami di profitto e sulle modalità di svolgimento degli esami, le Commissioni degli esami di profitto sono costituite da almeno due componenti, uno dei quali (con le funzioni di Presidente) è il titolare dell'insegnamento. Gli altri componenti possono essere docenti e ricercatori del Settore Scientifico Disciplinare dell'insegnamento o di SSD affini e, in assenza di docenti che rispettino tali caratteristiche, del Macro-settore Concorsuale o, al più, dell'Area. Possono far parte delle Commissioni degli esami di profitto anche i Cultori della materia nominati per lo specifico insegnamento dal Consiglio di Dipartimento.

4.11 Tirocinio
Il Tirocinio aziendale è una attività formativa da svolgersi presso un'azienda convenzionata, presso un ente di ricerca convenzionato. Lo scopo di tale attività è di effettuare un inserimento guidato nel mondo del lavoro. Il tirocinio deve essere svolto sotto la guida di un tutor esterno e di un docente interno del CdS. L'attribuzione della tematica oggetto del tirocinio, dell'azienda e del docente interno è stabilita dalla Commissione Tirocini dei CdS di Area Informatica, sentito lo studente. Lo svolgimento del Tirocinio può iniziare solo se lo studente ha superato gli

esami caratterizzanti specificati nel Regolamento Tirocini (consultabile sul sito web del CdS). Studente, tutor esterno e docente interno concordano preventivamente il programma delle attività da svolgere. Al termine, lo studente deve redigere una relazione dettagliata sulle attività svolte e sui risultati ottenuti. Tutor esterno e docente interno redigono una breve valutazione delle attività dello studente.
Ulteriori informazioni sullo svolgimento dei Tirocini sono rilevabili dal regolamento tirocini, reperibile, insieme alla modulistica inerente, al link: https://disegim.uniparthenope.it/disegim/cybersecurity-disegim

4.12 Conoscenze Linguistiche
L'insegnamento di Lingua Inglese (3 CFU) rientra nelle attività integrative del Corso di Studio e prevede solo un colloquio finale senza votazione. Tale accertamento viene effettuato da una Commissione costituita tra 3 componenti nominati tra i ricercatori e i professori dal Consiglio di Corso di Studio. E' prevista l'esenzione per gli studenti che presentino le seguenti certificazioni: - Trinity – Grades: da 4 a 12; - International Language Testing System (IELTS) – Livelli: 4.5 – 5.5, 5.5 – 6.5, 6.5 – 7.5, 7.5 – 9.0 - Esami ESOL di Cambridge – Livelli: PET, FCE, CAE, CPE - Michigan – Livelli: ECCE, ECPE; - London Tests of English (LTE) – Livelli: 2, 3, 4, 5 - TOLC – sezione di Inglese con punteggio uguale o superiore a 20/30.

Maggiori informazioni sono disponibili al seguente link: https://www.uniparthenope.it/disegim/cybersecurity-esonero-lingua

4.13 Riconoscimento dei crediti extrauniversitari
Per conoscenze e attività professionali pregresse, ai sensi dell'art. 14 della Legge n. 240/2010, è possibile il riconoscimento di un numero massimo di CFU pari a 12. Il riconoscimento e il numero degli eventuali crediti formativi saranno a discrezione del Consiglio di Corso di Studio.

4.14 Mobilità studentesca e studi compiuti all'estero
Gli studenti hanno la possibilità di trascorrere periodi di studio all'estero per sperimentare culture diverse e migliorare le proprie competenze linguistiche. Nell'ambito del programma di mobilità Erasmus+, il Corso di Studi attiverà diversi accordi bidirezionali con università straniere in diverse nazioni europee. Informazioni dettagliate sui programmi di scambio, le relazioni internazionali, le modalità e i regolamenti riguardanti la mobilità internazionale sono reperibili al seguente link: https://internazionalelingue.uniparthenope.it/.

4.15 Trasferimenti e Passaggi di corso di studio
Le richieste di passaggio da altro Corso di Studio o di trasferimento da altro Ateneo sono valutate dal Coordinatore del CdS e approvate dal Consiglio del CdS, con l'indicazione dei CFU riconosciuti e dell'anno di corso al quale è ammesso lo studente. Sono riconoscibili solo i CFU attribuiti ai Settori Scientifico Disciplinari previsti dal Manifesto degli Studi del CdS e che sono stati acquisiti su insegnamenti riconducibili agli insegnamenti del Manifesto degli Studi del CdS. Nel caso in cui i CFU acquisiti su un insegnamento siano inferiori a quelli del corrispondente insegnamento del CdS, i CFU mancanti devono essere acquisiti attraverso un colloquio integrativo da svolgersi secondo le stesse modalità previste per l'esame. Per il riconoscimento di CFU acquisiti presso altre Università, oltre quelle dell'Unione Europea, sarà valutata caso per caso l'equipollenza tra gli insegnamenti di cui si è superata la prova di valutazione e gli insegnamenti del manifesto egli studio del CdS. Per l'ammissione al secondo anno è necessario aver conseguito almeno 30 CFU; per l'ammissione al terzo anno è necessario aver conseguito almeno 60 CFU.

4.16 Esami Singoli
Chiunque sia in possesso almeno del diploma di scuola superiore può iscriversi a singole attività didattiche

formative, sostenere esami singoli e averne regolare attestazione. L'iscrizione a singole attività formative non può avvenire in contemporanea presso più Atenei, né tanto meno può essere contemporanea con l'iscrizione ad altra tipologia di corsi di studio attivati presso qualsiasi Ateneo, compresa l'Università degli Studi di Napoli Parthenope, pena la decadenza da entrambi. L'iscrizione avviene mediante presentazione di apposita domanda in bollo alla Segreteria del Corso di Studio presso cui è attivato l'insegnamento prescelto dal primo settembre al 31 marzo di ciascun anno accademico. Si possono sostenere esami di profitto per qualunque insegnamento attivato per l'anno accademico di riferimento

4.17 Prova finale

4.17.1 Obiettivi e Caratteristiche della prova Finale

Il Corso di Laurea in 'Ingegneria e Scienze Informatiche per la cybersecurity' si conclude con un elaborato, prodotto dal candidato, che ha il fine di dimostrare la padronanza degli argomenti trattati, la capacità del candidato di operare in modo autonomo e di presentare concetti con una buona chiarezza espositiva.

La prova finale consiste in un elaborato scritto, a contenuto originale o compilativo, su una delle tematiche rilevanti del Corso di Laurea, sviluppato sotto la supervisione e la responsabilità di un docente relatore. La discussione dell'elaborato avviene in sede collegiale, con il supporto di materiale multimediale preparato dal candidato.

La completezza dell'elaborazione effettuata dal candidato, l'autonomia nell'analisi e nello sviluppo dei contenuti e la capacità di comunicarli in modo rigoroso, chiaro e sintetico, insieme ad elementi derivanti dalla carriera dello studente, determineranno la valutazione finale dello studente.

4.17.2 Modalità di Svolgimento e Valutazione

La prova finale consiste nella presentazione dell'elaborato di tesi alla Commissione di Laurea e nella discussione delle tematiche affrontate.

In seduta pubblica, al candidato sarà chiesto di illustrare il lavoro svolto con l'ausilio di strumenti multimediali. La Commissione valuterà i contenuti dell'elaborato prodotto, la capacità del candidato di sintetizzare e presentare gli argomenti trattati, la proprietà di linguaggio, la consapevolezza raggiunta e lo spirito critico dimostrati dal candidato.

Lo svolgimento delle prove finali per il conseguimento del titolo è pubblico. Alla presentazione di ogni elaborato di tesi di laurea e alla successiva discussione è riservato un tempo complessivo di almeno 10 minuti. L'attribuzione del punteggio da parte della Commissione è effettuata in seduta riservata alla fine della presentazione di tutti i candidati. L'attribuzione del voto dell'esame finale per il conseguimento del titolo e la relativa proclamazione sono formalizzate da ciascuna Commissione al termine di ogni seduta. L'attribuzione del punteggio del voto di laurea è stabilita dalla Commissione giudicatrice, la quale, nel formulare la votazione, terrà conto dei criteri formulati nel seguito.

Il voto di laurea è espresso in centodecimi ed è costituito dalla somma del voto di base espresso in centodecimi e del voto dell'esame finale espresso dalla Commissione giudicatrice, come di seguito indicato. Il voto minimo di laurea per il superamento della prova finale è sessantasei centodecimi. Il voto massimo è centodieci centodecimi; a tale voto, solo all'unanimità, potrà essere aggiunta la lode. Il voto di base tiene conto della media dei voti che lo studente ha riportato negli esami di profitto, ponderata in base ai crediti dei relativi insegnamenti. Per il calcolo del voto di base, per insegnamenti si intendono esclusivamente quelli che all'interno del percorso formativo dello studente prevedono la verifica di profitto con votazione espressa in trentesimi. Il numero massimo di punti attribuibile dalla Commissione giudicatrice per l'esame finale è pari a 8. Una ulteriore eventuale premialità di 3 punti, con un massimo complessivo comunque non superiore a

11, è prevista per il riconoscimento della attività svolte nell'ambito del programma ERASMUS, come specificato al punto c). Il voto dell'esame finale deve tenere conto sia della carriera dello studente che dell'elaborato di tesi. La carriera dello studente è valutata secondo i seguenti criteri: **qualità del percorso di studi**, **durata del percorso universitario**, **partecipazione ad ulteriori attività**, come di seguito specificato.

a. Con riferimento alla qualità del percorso di studio, i punteggi attribuibili sono:
   - media superiore o uguale a 105 min 3 - max 4 punti;
   - media compresa tra 99 e 104 min 2 - max 3 punti;
   - media compresa tra 92 e 98 min 1 - max 2 punti;
   - media compresa tra 80 e 91 max 1 punto;
   - tre o più lodi 1 punto.
b. Con riferimento alla durata del percorso formativo, i punteggi attribuibili sono:
   - in corso 3 punti;
   - un anno fuori corso 1 punto.

Ai fini dell'attribuzione della relativa premialità, la durata del Corso di Studio può essere fittiziamente incrementata di 6 mesi nel caso di stage curriculare svolto presso strutture esterne all'Ateneo e che abbia un numero di CFU corrispondente non inferiore a 6. Analogamente, sempre ai fini della stessa premialità, la durata del Corso di Studio può essere fittiziamente incrementata di 6 mesi nel caso di partecipazione attiva all'80% delle adunanze degli organi collegiali, degli organismi consultivi, e degli organi di controllo e garanzia di Ateneo in qualità di rappresentante degli studenti (Senato Accademico, Consiglio di Amministrazione, Consiglio di Dipartimento, Consiglio di Corso di Studio, Commissione Paritetica di Dipartimento, Consiglio degli Studenti, Nucleo di Valutazione).
La durata del Corso di Studio per gli studenti part-time è doppia per ogni anno di iscrizione in questa modalità.

c. Con riferimento alla partecipazione ad ulteriori attività, nel caso di 12 CFU maturati all'estero con il programma ERASMUS, inclusi i CFU maturati per stage curriculari svolti all'estero, il punteggio massimo attribuibile è pari a 3 punti.
d. Il punteggio massimo attribuibile all'elaborato finale è pari a 3 punti.

Allo studente che raggiunge come valutazione complessiva 110/110 può essere attribuita la lode. La lode viene attribuita all'unanimità dalla Commissione su proposta del relatore.
Per ulteriori dettagli si veda il "Regolamento per la redazione delle tesi di laurea e di laurea magistrale".

4.18 Didattica Innovativa

Il Corso di Studio incoraggia l'uso di strumenti innovativi (piattaforme GitHub, siti per il self-assesment o soluzioni per il remote-interview come HackerRank) e la partecipazione ad iniziative di rilievo nazionale come cyberchallenge.it a cui la Parthenope partecipa dalla sua prima edizione.
Il Corso di Studi è erogato in modalità mista prevedendo pertanto che un terzo delle lezioni di ciascun insegnamento sono erogate con strumenti telematici a distanza. Anche i laboratori sono organizzati di modo da consentire esercitazioni parzialmente o totalmente in remoto, in particolare attraverso l'adozione della soluzione Azure Lab Services di Microsoft per la virtualizzazione dei laboratori e la loro accessibilità mediante cloud computing.
Il Corso di Studio organizza momenti specifici di approfondimento in sinergia con aziende, associazioni e ordini professionali, come per esempio la formazione in abilità di comunicazione e abilità sociali (soft-skills).

Appendice A: Elenco insegnamenti per la corte 2023/24

CORSO DI LAUREA IN INGEGNERIA E SCIENZE INFORMATICHE		
PER LA CYBERSECURITY		
Classe L08/L31		
Manifesto degli Studi		
per gli studenti immatricolati dall' a.a. 23/34		
I anno	**sem**	**CFU**
Aspetti legali della cybersecurity	I	6
Matematica I	I	6
Programmazione	I	12
Architettura degli Elaboratori	II	9
Aspetti Organizzativi e gestionali della Cybersecurity	II	6
Fisica Generale	II	6
Lingua inglese	II	3
Programmazione dispositivi mobili	II	6
II anno	**sem**	**CFU**
Sistemi Operativi	I	9
Algoritmi e Strutture Dati (MOD I)	I	9
Calcolo Numerico (MOD II)	II	6
Matematica II	I	6
Reti di Calcolatori (MOD I)	I	6
Crittografia (MOD II)	II	6
Basi di dati	II	6
Progettazione di software sicuro	II	6
Elementi di Telecomunicazioni	II	6
II anno	**sem**	**CFU**
Sicurezza delle reti (MOD I)	I	9
Sicurezza dei Sistemi Operativi e Cloud (MOD II)	II	6
Sicurezza dei Sistemi di Controllo Industriale	I	6
Fondamenti di Campi Elettromagnetici	I	6
Sicurezza delle Applicazioni (MOD I)	I	6
Intelligenza Artificiale per la cybersecurity (MOD II)	II	6
Esame a scelta	I	6
Esame a scelta	II	6
Tirocinio		9
Prova finale		6

Esami a scelta pre-approvati		
Sistemi di Produzione Integrati e Sostenibili	I	6
Diritto dell'Informazione e dell'Informatica	II	6

Appendice B: Matrice di Tuning

Descrittori Europei		ATTIVITA'FORMATIVE																									
Scheda Formulata con riferimento al corso di Ingegneria e scienze informatiche per la cybersecurity		Matematica I	Fisica Generale	Architettura degli Elaboratori	Programmazione	Aspetti Organizzativi e gestionali della Cybersecurity	Lingua inglese	Programmazione dispositivi mobili	Aspetti legali della Cybersecurity	Calcolo Numerico	Sistemi Operativi	Algoritmi e Strutture Dati	Reti di Calcolatori	Basi di dati	Progettazione di software sicuro	Matematica II	Elementi di Telecomunicazioni	Crittografia	Sicurezza delle reti	Sicurezza dei Sistemi Operativi e Cloud	Sicurezza delle Applicazioni	Sicurezza dei sistemi di controllo industriale	Fondamenti di Campi Elettromagnetici	Intelligenza Artificiale per la cybersecurity	Tirocinio e Prova finale
A. Conoscenza e capacità di comprensione:																											
A.01	Conoscere e comprendere gli aspetti metodologico-operativi della matematica, della fisica e delle altre scienze di base al fine di interpretare e descrivere i problemi dell'ingegneria e delle scienze	X	X							X		X				X	X									
A.02	Conoscere e comprendere principi di funzionamento dei sistemi di elaborazione fissi e mobili			X	X			X		X	X	X	X	X												
A.03	Comprensione di tipo sistemica dei dispositivi informatici			X	X			X		X	X	X	X	X			X					X	X			
A.04	Conoscenere e comprendere le tecniche per la progettazione di applicazioni software				X			X				X		X	X											
A.05	Comprendere le problematiche di sicurezza legate ad una rete di calcolatori			X							X		X					X	X	X	X					
A.06	Comprendere le problematiche di sicurezza legate al software di base di un sistema, sia esso locale o basato su virtualizzazione e cloud				X			X			X				X			X		X	X					
A.07	Comprendere le problematiche si sicurezza legate ad un processo industriale			X	X	X			X		X		X	X	X		X	X	X	X	X	X	X			
A.08	Comprendere le implicazioni in termini legali ed economico manageriali, delle problematiche di sicurezza di un sistema informatico					X			X									X				X		X		
A.09	Conoscere e comprendere l'applicazione di tecniche di data mining, machine learning e analisi dei dati per la sicurezza informatica				X				X		X	X	X	X				X	X	X	X			X		
B. Capacità applicative																											
B.01	Risolvere problemi matematici e fisici legati alle conoscenze scientifiche di base	X	X							X		X				X	X									
B.02	Applicare le conoscenze matematico/fisiche di base all'apprendimento dei corsi specialistici relativi alle aree tecnologico/progettuali	X	X							X		X				X	X	X					X			
B.03	Utilizzare tecniche e strumenti per la progettazione di componenti e sistemi informatici, applicati a processi industriali ed informativi			X	X	X		X	X		X		X	X	X		X	X	X	X	X	X	X			
B.04	Risolvere problemi concreti inerenti le reti e i sistemi di comunicazioni			X	X			X			X		X	X				X	X	X	X			X		
B.05	Pianificare soluzioni tecnologiche con riferimento ai vari contesti (sociale, ambientale, normativo, ...) in cui esse opereranno				X	X		X	X		X		X		X		X	X	X	X	X	X	X			
B.06	Analizzare, progettare e gestire una rete di calcolatori sicura												X					X	X	X	X					
B.07	Configurare, realizzare e manutenere applicazioni locali e distribuite che debbano rispondere a specifici requisiti di sicurezza				X			X			X		X	X	X					X	X			X		
B.08	Analizzare e migliorare la sicurezza di un processo industriale basato su sistemi informatici					X			X			X						X	X	X	X	X		X		
C. Autonomia di giudizio																											
C.01	Vvalutare e interpretare i dati in laboratorio									X		X					X		X	X	X	X	X	X	X	
C.02	Confrontare in maniera critica la sicurezza informatica di molteplici soluzioni tecnologiche												X	X	X			X	X	X	X	X				X
C.03	Valutare le migliori scelte per la messa in sicurezza di un sistema informatico anche con riferimento al contesto in cui					X			X				X	X	X		X	X	X	X	X	X	X			X
C.04	Valutare le implicazioni legali ed economico manageriali, delle problematiche di sicurezza di un sistema informatico e legare ad esse decisioni di tipo organizzativo gestionale					X			X										X	X	X	X		X		
D. Abilità nella comunicazione																											
D.01	Comunicazione scritta e orale in lingua italiana e in lingua inglese	X	X	X		X	X	X	X																		X
D.02	Capacità di lavorare in gruppo														X				X	X	X	X		X		
D.03	Capacità di esprimere chiaramente concetti tecnici			X		X	X		X				X	X	X				X	X	X	X	X	X	X	X
D.04	Sintesi nell'esposizione	X	X				X			X		X				X	X						X			X
D.05	Capacità di esporre oralmente o per iscritto un argomento del corso	X	X	X		X	X		X		X		X			X	X		X	X	X	X	X	X	X	X
D.06	Capacità logico deduttive nell'esposizione	X	X		X					X		X			X											X
D.07	Presentazione di un'elaborazione di dati sperimentali						X					X					X		X	X	X	X			X	X
E. Capacità di apprendere																											
E.01	Consultazione materiale bibliografico						X		X						X				X	X	X	X		X	X	
E.02	Individuazione e consultazione di banche dati, repository e altre informazioni anche in rete				X		X	X				X	X	X	X			X	X	X	X	X		X	X	
E.03	Aggiornamento continuo delle conoscenze acquisite			X	X	X	X	X	X				X	X	X			X	X	X	X	X		X	X	
E.04	Capacità di elaborare, schematizzare, riassumere i contenuti acquisiti	X	X			X	X					X			X		X		X	X	X	X	X	X	X	

Appendice C: Schede sintetiche degli insegnamenti

Denominazione	**Matematica I**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Primo Ciclo Semestrale
Contenuti	Cenni sugli spazi vettoriali. Matrici e trasformazioni lineari. Sistemi lineari. Autovalori ed autovettori, diagonalizzazione. Cenni di geometria analitica nel piano e nello spazio. I numeri reali e complessi. Funzioni reali di una variabile reale. Calcolo differenziale per funzioni di una variabile, metodi iterativi numerici per equazioni non lineari. Calcolo integrale per funzioni di una variabile. Alcune basi di crittografia.
Testi di Riferimento	M.Bramanti, C.D.Pagani, S.Salsa, Analisi Matematica I con elementi di geometria e algebre lineare, Zanichelli Ed. M. Bramanti, Esercitazioni di Analisi Matematica 1, Editore: Esculapio P. Marcellini, C. Sbordone, Analisi Matematica I, Liguori Ed. P. Marcellini, C. Sbordone, Esercitazioni di Matematica, Vol I, Liguori Ed.

Denominazione	**Fisica Generale**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Secondo Ciclo Semestrale
Contenuti	Metodo scientifico e grandezze fisiche. Cinematica e dinamica del punto materiale. Leggi di conservazione: energia meccanica, quantità di moto. Gravitazione universale. Fluidi. Termodinamica. Elettromagnetismo. Cenni di Fisica Moderna: struttura atomica, semi e super conduttori, PUF.
Testi di Riferimento	"Fondamenti di Fisica", D. Halliday, R. R. Resnick, J. Walker, Casa Editrice Ambrosiana (Vol. 1 e 2). "Fisica Moderna", D. Halliday, R. R. Resnick, J. Walker, Casa Editrice Ambrosiana

	Per approfondimenti: "The Feynman Lectures on Physics", Vol. 1, R.B. Leighton, M. Sands, R.P. Feynmann, Ed. Paperback. L. Colombo: Fisica dei semiconduttori, Zanichelli

Denominazione	**Architettura degli Elaboratori**
CFU	9
Ore Attività Frontali	72
Periodo Didattico	Secondo Ciclo Semestrale
Contenuti	Reti logiche. Unità di elaborazione di base. Il livello Software, Istruzioni macchina e programmi. Set di istruzioni CISC e RISC con esempi reali. Organizzazione e gestione dell'Input/Output. Organizzazione e gestione delle memorie Pipelining. Fondamenti di Hardware Security. Hardware-assisted Security: tecnologie Intel SGX, ARM TrustZone e AMD SEV.
Testi di Riferimento	Carl Hamacher, Zvonko Vranesic, Safwat Zaky, Computer Organization and Embedded Systems,Sixth Edition, McGraw-Hill Higher Education, 2011, ISBN-10: 0073380652. Specifiche tecniche di estensioni hardware: Intel SGX (https://www.intel.com/content/www/us/en/developer/tools/ software-guard-extensions/overview.html) ARM TrustZone (https://www.arm.com/technologies/trustzone-for-cortex-a/tee-reference-documentation) AMD SEV (https://developer.amd.com/sev/)

Denominazione	**Programmazione**
CFU	12
Ore Attività Frontali	96
Periodo Didattico	Primo Ciclo Semestrale

Contenuti	Fondamenti di informatica. Programmazione procedurale. Costrutti di controllo e iterazione. Variabili, tipi, puntatori. Array. Strutture. Ricorsività. Ordinamento di array. Programmazione ad oggetti. Le classi del linguaggio C++. Ciclo di vita dei programmi. Allocazione della memoria. Polimorfismo. Ereditarietà. Gestione delle eccezioni. Meccanismi di incapsulamento. Overloading degli operatori. Template.
Testi di Riferimento	KELLEY, I. POHL; "C: didattica e programmazione", Pearson Education Italia, 2004. Programmazione in C - Kim N. King - Apogeo, 2009. Bjarne Stroustrup, "Il linguaggio C++"

Denominazione	**Aspetti Organizzativi e gestionali della Cybersecurity**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Secondo Ciclo Semestrale
Contenuti	Processi di innovazione aziendale, cambiamento tecnologico, gestionale e organizzativo dei progetti di cybersecurity. Principi di risk management, cyber resilienza e business continuity. Strumenti di analisi e valutazione per la gestione dei progetti di innovazione e dei processi di innovazione digitale. Posizione delle imprese nei processi di cybersecurity in ambito nazionale e internazionale. Pianificazione organizzativa e gestionale di un progetto di cybersecurity.
Testi di Riferimento	Melissa A. Schilling, Francesco Izzo, La gestione dell'innovazione, V edizione, McGraw-Hill Education, 2022, ISBN-10: 8838699984.

Denominazione	**Programmazione dei Dispositivi Mobili**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Secondo Ciclo Semestrale

Contenuti	Introduzione al mobile computing. Limitazioni hardware/software e di comunicazione nei sistemi mobili. Reti di comunicazione wireless (cenni operativi): WPAN, WWAN. Architetture di applicazioni mobili. Introduzione al linguaggio Kotlin. Programmazione Kotlin avanzata. Programmazione su Google Android. componenti e risorse. Widget e layout. Gestione eventi. Meccanismi di I/O. Gestione del database embedded. Servizi in Android. Location based services. Web service.
Testi di Riferimento	Bill Phillips, Chris Stewart, and Kristin Marsicano. Android Programming: The Big Nerd Ranch Guide. Addison-Wesley Professional; RAJ KAMAL: "Mobile Computing", Oxford University Press. MARTYN MALLICK: "Mobile and Wireless Design Essentials", Ed. John Wiley & Sons. BRUCE ECKEL: "Thinking in Java"

Denominazione	**Algoritmi e Strutture Dati (MOD I)**
CFU	9
Ore Attività Frontali	72
Periodo Didattico	Primo Ciclo Semestrale
Contenuti	Analisi della Complessità Computazionale degli Algoritmi, Algoritmo Euclideo e complessità. Crittosistemi classici, Paradigma Divide et Impera, Merge-Sort e Quicksort. Struttura Dati Heap, Heapsort, Algoritmi di Visita su Alberi Binari. Attività di Laboratorio su Crittosistemi classici. Crittoanalisi, Programmazione Dinamica, Tecniche Greedy. Attività di Laboratorio su Crittoanalisi. Crittosistema RSA. Algoritmi su Grafi. Hash Table, Funzioni Hash Crittografiche, Problemi P e NP. Attività di Laboratorio su Crittosistemi RSA.
Testi di Riferimento	Thomas Cormen, Charles Leiserson, Ronald Rivest, Clifford Stein, Introduzione agli Algoritmi e Strutture Dati, Terza Edizione, McGraw-Hill Education, 2010, ISBN-10: 883866515X

	J. Katz, Y. Lindell, Yehuda, Introduction to modern cryptography, Second edition, Chapman & Hall/CRC Cryptography and Network Security, 2015.
Denominazione	**Calcolo Numerico (MOD II)**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Secondo Ciclo Semestrale
Contenuti	Calcolo scientifico e Matlab. Grafica in Matlab. Numeri interi, numeri fp, precisione, accuratezza. Numeri casuali e pseudocasuali. Generazione di semplici codici crittografici. Computazioni con numeri interi e con numeri primi. Applicazioni in ambito crittografico. Strumenti di base per l'analisi di dati. I metodi iterativi per determinare zeri, punti fissi, minimi e massimi di una funzione. Algebra lineare numerica. Applicazioni ai sistemi automatici di ranking.
Testi di Riferimento	A.QUARTERONI, C. SALERI, P. GERVASIO: "Calcolo Scientifico Esercizi e problemi risolti con MATLAB e Octave", Springer, 2017.

Denominazione	**Sistemi Operativi**
CFU	9
Ore Attività Frontali	72
Periodo Didattico	Primo Ciclo Semestrale
Contenuti	Introduzione ai SO. I sistemi a processi. Cooperazione e sincronizzazione. I threads. Algoritmi di schedulazione della CPU. La gestione della memoria. Sincronizzazione dei processi. Deadlock. Architettura di un file system. Sistemi di I/O e memoria secondaria. Sicurezza dei SO. Controllo di accesso alle risorse, Modelli formali di sistemi sicuri. Autenticazione. Il sistema Operativo UNIX. Programmazione di Sistema.
Testi di Riferimento	S. Tanenbaum, H. Bos, I moderni Sistemi Operativi, 4 Ed., Pearson, 2019

	W.R. Stevens, S.A. Rago, Advanced Programming in the Unix Environment, Addison Wesley, 3rd Ed., 2013

Denominazione	**Reti di Calcolatori (MOD I)**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Primo Ciclo Semestrale
Contenuti	Modello ISO/OSI. Tipologie ed architetture di reti. Il livello Data Link: LLC e MAC. Il livello Network. Il protocollo IP. Subnetting. Algoritmi di routing. I protocolli di controllo. IPV6. Il servizio trasporto. I protocolli TCP e UDP. Protocolli applicativi per il funzionamento della rete IP. Applicazioni e servizi Internet. Programmazione distribuita.
Testi di Riferimento	J. Kurose, K. Ross, "Computer Networking: A Top down Approach". Eigth Edition. Pearson
Denominazione	**Crittografia (MOD II)**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Secondo Ciclo Semestrale
Contenuti	Tecniche di crittografia classica. Crittografia simmetrica (es. AES, DES), principi della cifratura a blocchi. Crittografia asimmetrica (es. RSA), principi dei crittosistemi a chiave pubblica, crittografia a curva ellittica. Crittosistema di El-Gamal. Funzioni hash e autenticazione. MD4. MD5. SHA-1. Message Authentication Code. Firma digitale, PKI. Gestione e scambio di chiavi: Diffie-Hellmann.
Testi di Riferimento	William Stallings, CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE SEVENTH EDITION GLOBAL EDITION

Denominazione	**Basi di Dati**
CFU	6

Ore Attività Frontali	48
Periodo Didattico	Secondo Ciclo Semestrale
Contenuti	Introduzione alle basi di dati. Modelli dei dati. Tipologie di linguaggi per basi di dati. Modello relazionale. Algebra relazionale. Il linguaggio SQL. Progettazione di una base di dati. Modello Entità-Relazioni. Gestione delle transazioni. Proprietà ACIDE. Basi di dati distribuite. Transazioni in basi di dati distribuite. SQL per Applicazioni. Basi di dati ed applicazioni web. Web Information System (WIS). Cenni su approcci NoSQL. Sistemi informativi sicuri. Data mining. Classificazione. Clustering. Big data analytics.
Testi di Riferimento	Paolo Atzeni, Stefano Ceri, Piero Fraternali, Stefano Paraboschi, Riccardo Torlone, Basi di dati 5/ed, 2018, ISBN: 9788838694455

Denominazione	**Progettazione di software sicuro**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Secondo Ciclo Semestrale
Contenuti	Principi di ingegneria del SW. Proprietà del Software. Ciclo di vita del Software. La sicurezza nel ciclo di vita del SW nel modello Agile. Modellazione del software. Threat modelling. Security Pattern. Defensive Coding. Linee guida per la programmazione sicura. Tipici errori di programmazione. Secure programming in C/C++/Python. V&V. Analisi Statica. Analisi dinamica e testing del sw. Principi di Analisi simbolica e di tecniche di validazione formale. OWASP Secure Coding checklist.
Testi di Riferimento	Ingegneria del software, 10/Ed. Ian Sommerville, Pearson. Larman, C. (2002). Applying UML and Patterns: An Introduction to Object-oriented Analysis and Design and the Unified Process. Englewood Cliff, NJ: Prentice Hall.

Denominazione	**Matematica II**

CFU	6
Ore Attività Frontali	48
Periodo Didattico	Primo Ciclo Semestrale
Contenuti	Serie numeriche e serie di potenze. Equazioni differenziali. Funzioni vettoriali di una variabile. Funzioni di più variabili e calcolo differenziale per funzioni di più variabili. Funzioni vettoriali di più variabili. Integrali doppi. Campi vettoriali. Integrali di superficie.
Testi di Riferimento	M. Bramanti - C.D. Pagani - S. Salsa, Analisi Matematica 2, Zanichelli Editore N.Fusco - P.Marcellini - C.Sbordone, Elementi Di Analisi Matematica Due, Liguori Ed. P.Marcellini C.Sbordone, Esercitazioni Di Matematica 2, Zanichelli Ed.

Denominazione	**Elementi di Telecomunicazioni**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Secondo Ciclo Semestrale
Contenuti	Elementi di Teoria dei Segnali. Operazioni di trasformazione sui Segnali. Serie e Trasformata di Fourier. Analisi nel dominio del tempo e della frequenza. Banda di un segnale, Conversione A/D. Teoria della Probabilità e dei Fenomeni Aleatori. Cenni di Stima e Detection. Teoria della Detection. Test di verosimiglianza, Approccio di Neyman Pearson, ROC, Informazioni a priori, Rischio Bayesiano. Sistemi di Telecomunicazioni e loro descrizione. Cenni Storici sulle Telecomunicazioni (TLC), I Sistemi di TLC analogici e digitali.
Testi di Riferimento	Claudio Prati, "Segnali e Sistemi per le Telecomunicazioni", McGraw-Hill, 2003. Sheldon Ross, "Probabilità e Statistica per l'Ingegneria e le Scienze", APOGEO Editore.

Denominazione	**Sicurezza delle Reti (MOD I)**

CFU	9
Ore Attività Frontali	72
Periodo Didattico	Primo Ciclo Semestrale
Contenuti	Introduzione alla sicurezza di rete. Richiami dello stack ISO/OSI e problemi di sicurezza dello stack TCP/IP. attacchi ARP Poisoning, ARP Spoofing, DNS Tunneling, DNS Amplification, DNS Flood Attack, DNS Spoofing, NXDOMAIN Attack. Sicurezza delle e-mail. Protocolli per la sicurezza delle comunicazioni. Protocolli di autenticazione NSPK e Kerberos. Sicurezza al livello trasporto, TLS e SSH. Sicurezza al livello IP, IPsec e VPN. In depth security: sicurezza perimetrale e riconoscimento delle intrusioni. Network Management for security. Malware. La sicurezza delle comunicazioni wireless e della IoT. Caso di studio di LoraWAN.
Testi di Riferimento	William Stallings, Cryptography And Network Security Principles And Practice Seventh Edition Global Edition
Denominazione	**Sicurezza dei Sistemi Operativi e Cloud (MOD II)**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Secondo Ciclo Semestrale
Contenuti	Autenticazione e controllo degli accessi. Sicurezza del file system. Sicurezza a livello Kernel. Sandboxing delle applicazioni. Protezione basata su trusted computing. Monitoraggio del SO mediante host-based Intrusion Detection System. Fondamenti di Piattaforme Cloud. Tecniche di difesa dei data-in-transit. Soluzioni per la sicurezza dei data-at-rest. Soluzioni per la sicurezza dei data-in-use. Monitoraggio della sicurezza sul Cloud. Il caso di studio di Google Cloud Platform.
Testi di Riferimento	Operating System Security, Trent Jaeger, Morgan & Claypool

Denominazione	**Sicurezza delle Applicazioni (MOD I)**
CFU	6
Ore Attività Frontali	48

Periodo Didattico	Primo Ciclo Semestrale
Contenuti	Framework architetturali delle applicazioni odierne con particolare attenzione alle applicazioni Web. Tecniche di Vulnerability Assesment. Penetration Testing. Common Vulnerability Scoring System. Difese contro attacchi XSS. Protezioni per Remote & Local File Inclusion. Cross Site Request Forgery. Content Security Policies (CSP).
Testi di Riferimento	Web Application Security. Andrew Hoffman. 2020. Publisher(s): O'Reilly Media, Inc.
Denominazione	**Intelligenza Artificiale per la Cybersecurity (MOD II)**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Secondo Ciclo Semestrale
Contenuti	Le basi dell'Intelligenza Artificiale (IA) e lezioni pratiche sul linguaggio di programmazione Python per l'implementazione di algoritmi di IA. Ottimizzazione con Calcolo Evolutivo; Sistemi di Apprendimento: Reti Neurali; Fuzzy Logic; relativi esempi di implementazione Python. AI e Machine Learning (ML) per la Cybersecurity. Sviluppo di sistemi intelligenti in grado di rilevare pattern e attacchi insoliti e sospetti. Testare l'efficacia di algoritmi e strumenti dell'AI per la sicurezza informatica.
Testi di Riferimento	Parisi, A., Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies, 2019. Freeman, D., Machine Learning and Security: Protecting Systems With Data and Algorithms. Editor Clarence Chio. 2018 Sebastian Raschka, Vahid Mirjaili(2017). Python Machine Learning: Machine Learning and Deep Learning with Python, scikit-learn, and TensorFlow, 2nd Edition.

Denominazione	**Sicurezza dei Sistemi di Controllo Industriale**
CFU	6
Ore Attività Frontali	48

Periodo Didattico	Primo Ciclo Semestrale
Contenuti	Introduzione all'automazione industriale. Architettura dei sistemi di controllo industriale. Analisi dei sistemi dinamici nel dominio del tempo e della frequenza. Sistemi per il controllo locale (a livello di campo). Sensori e attuatori industriali. Controllori a logica programmabile (PLC). Reti per l'automazione. Sistemi di supervisione, integrazione e sicurezza. Modello di cybersecurity.
Testi di Riferimento	P. Bolzern, R. Scattolini, N. Schiavoni, Fondamenti di Controlli Automatici, 4 ed., Mc Graw Hill Italia, 2015. P. Chiacchio, F. Basile, Tecnologie informatiche per l'automazione, Mc Graw Hill, 2004.

Denominazione	**Fondamenti di Campi Elettromagnetici**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Primo Ciclo Semestrale
Contenuti	Fondamenti matematici. Equazioni di Maxwell. Potenza ed energia associati al campo Elettromagnetico. Fondamenti di propagazione in spazio libero. Antenne elementari e parametri di antenne. Vulnerabilità della propagazione in spazio libero. Fondamenti di propagazione guidata. Vulnerabilità della propagazione in guida.
Testi di Riferimento	G. Franceschetti, Electromagnetics, Plenum Press G.Franceschetti, Campi Elettromagnetici, Boringhieri.

Denominazione	**Sistemi di produzione integrati e sostenibili**
CFU	6
Ore Attività Frontali	48
Periodo Didattico	Primo Ciclo Semestrale
Contenuti	Strategie per la produzione integrata. Tecnologie abilitanti per la smart manufacturing. Automazione nei cyber physical

	systems. Metodologie per la progettazione e per lo sviluppo di applicazioni safety-critical affidabili. Affidabilità, disponibilità, sicurezza, riservatezza, integrità, manutenibilità dei sistemi. Modelli matematici di affidabilità. Modelli matematici di disponibilità. Simulazione ed ottimizzazione di smart e sustainable systems integrati.
Testi di Riferimento	D. Falcone, F. De Felice, T.L. Saaty. Il Decision Making ed i sistemi decisionali multicriterio. Ed. HOEPLI, 2009 F. De Felice, A.Petrillo. Effetto Digitale. Ed. McGrawHill, 2021 F. De Felice, D. Falcone, A. Petrillo. World class manufacturing: origine, sviluppo e strumenti. McGraw Hill.