REGOLAMENTO DIDATTICO CORSO DI LAUREA MAGISTRALE

COMPUTER ENGINEERING, CYBERSECURITY AND ARTIFICIAL INTELLIGENCE (CLASSE LM-32)

A.A. 2024/25

SOMMARIO

DATI GENERALI

Denominazione del Corso di Studio	Computer Engineering, Cybersecurity and Artificial Intelligence
Classe di appartenenza	Classe LM-32: Classe delle Lauree Magistrali in Ingegneria Informatica
Durata	La durata normale del Corso di Laurea Magistrale è di 2 anni accademici e il numero dei crediti necessari per il conseguimento del titolo è pari a 120.
Struttura di riferimento	Facoltà di Ingegneria e Architettura
Dipartimento di riferimento	Ingegneria Elettrica ed Elettronica (DIEE)
Sede didattica	Via Marengo n° 2 – Cagliari
Coordinatore	Prof. Giorgio Giacinto
Sito web	https://web.unica.it/cyberai
Lingua di erogazione della didattica	Inglese
Modalità di erogazione della didattica	convenzionale (in presenza)
Accesso	libero
Posti riservati studenti non comunitari	40

Ulteriori informazioni generali sul Corso di Studio sono riportate nel sito web.

Art. 1 - Premesse e finalità

Il presente Regolamento del Corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence (classe LM-32) è deliberato dal Consiglio di Corso di Studio in conformità all'ordinamento didattico, nel rispetto della libertà di insegnamento e nel rispetto dei diritti e doveri dei docenti e degli studenti, in base al D.M. 270/2004 e successive modifiche e integrazioni, allo Statuto, al Regolamento didattico di Ateneo e al Regolamento Carriere amministrative degli studenti e alla L. 264/1999 relativa alla programmazione degli accessi.

Art. 2 - Organi del Corso di Studio

Gli organi del Corso di Studio, con una descrizione dettagliata di funzioni, compiti e responsabilità, sono definiti nel documento Il Sistema di Assicurazione della Qualità del Corso di Studio, disponibile nel sito web del corso.
Il Consiglio potrà individuare ulteriori Commissioni con l'incarico di analizzare e istruire le attività relative a specifiche funzioni del Consiglio.

Art. 3 - Obiettivi formativi specifici del Corso di Studio e descrizione del percorso formativo

Il calcolatore nelle sue diverse forme è diventato un componente essenziale nei diversi ambiti della vita sociale, economica e produttiva del paese, consentendo una accelerazione dello sviluppo unita a una maggiore efficienza e efficacia grazie alla connessione Internet e alla possibilità di elaborare grandi quantità di dati attraverso tecniche di intelligenza artificiale. A queste opportunità di sviluppo si accompagna una crescente vulnerabilità dei sistemi ad attacchi informatici mirati a compromettere la riservatezza dei dati, la loro integrità e la continuità del servizio. È quindi sempre più sentita l'esigenza di figure professionali in grado di progettare e gestire sistemi informatici avanzati in ambienti complessi civili e industriali, mitigando i rischi derivanti da potenziali attacchi informatici.

L'impostazione del corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence ha l'obiettivo di formare ingegneri altamente specializzati nell'ambito della progettazione, gestione e manutenzione di sistemi informatici complessi e sicuri in ambito industriale, con competenze avanzate nel campo della cybersecurity e dell'intelligenza artificiale, e capaci di analizzare e proporre soluzioni progettuali innovative ed efficaci in tali ambiti.

Per questo scopo, gli obiettivi formativi specifici possono essere declinati secondo quattro assi formativi, identificati nelle aree dell'ingegneria informatica, dell'ingegneria dei sistemi, della scienza della sicurezza e dell'intelligenza artificiale, con l'obiettivo complessivo di coniugare una solida formazione nei domini fondamentali dell'ingegneria informatica e dell'ingegneria dei sistemi, e la formazione specialistica sui temi della cybersecurity e dell'intelligenza artificiale.

Il laureato magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence nell'ambito dell'Ingegneria Informatica:
- conosce approfonditamente le metodologie di sviluppo software ed è capace di ideare, pianificare, progettare e gestire sistemi software complessi e/o innovativi in vari contesti applicativi;
- conosce ed è in grado di sfruttare in modo efficace le architetture di calcolo e le metodologie di comunicazione caratteristiche degli ambiti industriali, dei sistemi embedded, degli ambienti distribuiti (cloud e mobile computing) e della Internet of Things.

Questi obiettivi vengono raggiunti attraverso insegnamenti nel settore caratterizzante dell'ingegneria informatica e nei settori affini dell'elettronica e delle telecomunicazioni.

Nell'ambito della Ingegneria dei sistemi:
- conosce le metodologie e le tecnologie per la modellazione, analisi e progettazione dei sistemi di supervisione e controllo, in particolare quelli sviluppati in ambito industriale e per infrastrutture critiche, tenendo conto degli aspetti legati alla sicurezza di tipo "cyber".
Questi obiettivi vengono raggiunti attraverso insegnamenti nel settore caratterizzante dell'automatica e in settori affini dell'ingegneria industriale e dell'informazione volti a fornire la conoscenza di almeno un ambito applicativo specifico.

Nell'ambito della Scienza della sicurezza:
- conosce le metodologie per l'analisi delle vulnerabilità e di rischi cui è soggetto un sistema informatico nonché le tecnologie e metodologie per la loro mitigazione;
- è capace di ideare e progettare sistemi informatici con ridotto rischio "cyber" in relazione al contesto applicativo, di rilevare e gestire gli incidenti informatici in sistemi in esercizio, valutando le loro implicazioni giuridiche ed economiche.
Questi obiettivi vengono raggiunti attraverso insegnamenti nel settore caratterizzante dell'ingegneria informatica e nel settore affine dell'informatica giuridica.

Nell'ambito della Intelligenza artificiale:
- conosce gli approcci alla base degli algoritmi utilizzati per l'apprendimento automatico e l'intelligenza artificiale ed è in grado di utilizzarli per ideare e progettare sistemi le cui funzionalità operative dipendono dall'elaborazione intelligente dei dati;
- è capace di utilizzare le conoscenze nel settore dell'intelligenza artificiale per progettare sistemi di protezione fisica e logica per la mitigazione del rischio "cyber" anche con l'utilizzo di tecnologie abilitanti d'avanguardia (come, per esempio, le tecnologie biometriche).
Questi obiettivi vengono raggiunti attraverso insegnamenti nel settore caratterizzante dell'ingegneria informatica.

Inoltre il laureato magistrale avrà acquisito anche le competenze necessarie per accedere a livelli di formazione superiore, quali dottorati di ricerca, master di secondo livello e scuole di specializzazione orientate alla sicurezza informatica. Tale obiettivo sarà perseguito mediante l'insieme delle attività formative ed in particolare mediante le attività connesse alla prova finale.

Per molti insegnamenti, è prevista attività progettuale svolta in laboratorio, finalizzata allo sviluppo ed alla verifica di soluzioni avanzate per problemi di complessità paragonabile a quella che si incontra nel mondo reale.

L'organizzazione delle propedeuticità e la calendarizzazione degli insegnamenti nei vari periodi sarà basata sulla suddivisione degli insegnamenti nei quattro ambiti di riferimento, caratterizzati da un significativo grado di integrazione dei contenuti formativi.

Tutti gli insegnamenti saranno erogati in lingua inglese, non solo per favorire l'internazionalizzazione e l'attrattività verso l'esterno, ma soprattutto per favorire l'approccio alla formazione continua da parte dei laureati, attraverso l'accesso a informazioni di settore disponibili prevalentemente in lingua inglese.

Art. 4 - Sbocchi occupazionali e professionali previsti per i laureati

Funzione in un contesto di lavoro:

1. Progettazione, sviluppo, gestione e collaudo di sistemi informatici in vari settori (manifatturiero, pubbliche amministrazioni, servizi) caratterizzati dall'acquisizione, la trasmissione e l'elaborazione di segnali in ambito civile, industriale e dell'informazione.
2. Progettazione, sviluppo e gestione di sistemi informatici in tutti i settori industriali dove 'sicurezza' e 'intelligenza' sono assi fondamentali (per esempio, sistemi intelligenti per la sicurezza logica e fisica).
3. Progettazione di servizi di cyber intelligence e/o cyber security.
4. Progettazione di sistemi che si avvalgono di algoritmi di Intelligenza Artificiale e Machine Learning.
5. Attività di supervisione e gestione tecnica negli ambiti di cui ai punti precedenti.
6. Ricerca fondamentale, applicata e sviluppo industriale. Supporto alla Ricerca e Sviluppo in impresa. Supporto al trasferimento tecnologico.

Competenze associate alla funzione:

Abilità di interazione con il mondo esterno orientato alla comprensione e negoziazione dei requisiti di un sistema informatico sicuro, connesso ad una specifica problematica applicativa. Capacità di analisi e definizione dei moduli di un dato sistema informatico, individuandone le criticità e problematiche implementative. Abilità di traduzione dei risultati dell'analisi di ciascun modulo in specifiche di dettaglio per quanto concerne la realizzazione (o l'integrazione) o l'ulteriore organizzazione dei sistemi software e/o dei componenti specifici del sistema complessivo, con particolare riferimento alla messa in sicurezza di ciascuno di essi con soluzioni tecnologiche allo stato dell'arte. Capacità di definizione nello specifico delle soluzioni implementative più adeguate, con riguardo alla stesura del codice, dei moduli software operativi realizzati ex novo, integrando ad essi componenti preesistenti, eventualmente modificati o aggiornati (Funzioni 1,2,5).
Capacità di individuazione di soluzioni tecniche adeguate alle caratteristiche del sistema informatico (lato hardware e software), degli aspetti organizzativi e direttivi per la realizzazione del progetto, dei vincoli tecnologici, delle prestazioni richieste, ed in particolare relative alla sua protezione da attacchi informatici di varia natura. (Funzioni 1,2,5).
Competenze avanzate nel campo della cyber-security nei sistemi informatici, e la realizzazione e messa in opera di strumenti per la mitigazione del rischio (Funzioni 2, 3).
Competenze avanzate negli ambiti dell'intelligenza artificiale e del machine learning (Funzione 4,6).
Competenze avanzate per la gestione del rischio informatico e la progettazione di sistemi informatici sicuri anche attraverso l'uso di metodologie di intelligenza artificiale (Funzioni 3,4,6).

Sbocchi professionali:

Organismi pubblici e privati operanti nella gestione e realizzazione di infrastrutture critiche, essendo cruciale in questo settore la gestione della sicurezza.
Imprese operanti nell'area dei sistemi informativi e delle reti di calcolatori, con particolare riguardo a quelle inserite nel mercato della sicurezza fisica e logica realizzata attraverso sistemi informatici.
Industrie operanti negli ambiti della produzione hardware e software.
Imprese operanti negli ambiti della produzione di servizi multimediali, del commercio elettronico e dei servizi via Internet.
Servizi informatici per la pubblica amministrazione e sanità.

Industrie per l'automazione e la robotica.
Aziende operanti nel settore dei trasporti e della logistica.
Realtà civili ed industriali in cui sono presenti apparati e sistemi per l'automazione che integrino componenti informatici, apparati di misure, trasmissione ed attuazione.
Università o centri di ricerca coinvolti negli ambiti applicativi sopra menzionati.

La formazione ad ampio spettro e non focalizzata sulle realtà industriali sarde consente al laureato di proporsi presso società o istituzioni con sede al di fuori della Sardegna e dell'Italia. L'ampia formazione di base consente, inoltre, di ricoprire, con l'avanzare della carriera, ruoli gestionali anche di rilevante responsabilità.

Come per tutte le lauree di secondo livello in ingegneria è prevista la possibilità di esercitare la libera professione come "Ingegnere" dopo aver superato un esame di Stato ed essersi iscritti all'Albo professionale.

Art. 5 - Tipologia delle attività didattiche

Il Corso di Studio è basato su attività formative relative a sei tipologie:

1) attività caratterizzanti (tipologia B);
2) attività affini o integrative (tipologia C);
3) attività a scelta dello studente (tipologia D);
4) attività relative alla preparazione della prova finale (tipologia E);
5) ulteriori attività formative (tipologia F: ulteriori conoscenze linguistiche, abilità informatiche e telematiche, attività inerenti stage e tirocini formativi presso imprese, enti pubblici o privati, ordini professionali, tirocini di orientamento e altre conoscenze utili all'inserimento nel mondo del lavoro).

Per le attività formative a scelta, agli studenti è assicurata la libertà di scelta tra tutti gli insegnamenti attivati nell'Ateneo, compresa l'acquisizione di ulteriori crediti formativi nelle discipline caratterizzanti, purché la scelta sia coerente con il progetto formativo.

La coerenza della proposta con il progetto formativo è valutata e deliberata dal Corso di Studio. Lo studente può chiedere il riconoscimento, in termini di crediti, nell'ambito delle attività formative a sua scelta, di esperienze maturate al di fuori dei percorsi curriculari universitari: rientrano fra questi i tirocini, i seminari, le ulteriori conoscenze linguistiche, le attività connesse al programma Erasmus, ecc.

Per l'acquisizione dei relativi crediti formativi universitari (CFU) è richiesto il superamento dell'esame o di altra forma di verifica del profitto.

Gli studenti che abbiano svolto il servizio civile nazionale possono chiedere al Consiglio di Corso il riconoscimento in CFU del servizio svolto. Il Consiglio, previa valutazione della documentazione presentata dallo studente e dell'attinenza tra le attività svolte durante il servizio civile e gli obiettivi formativi del Corso di Studio, può riconoscere il servizio svolto sino ad un massimo di 9 CFU, da imputare alla categoria delle attività a libera scelta dello studente. Può inoltre riconoscere ulteriori crediti, sino ad un massimo di 3, da imputare alla categoria "altre attività".

Le modalità didattiche adottate consistono in lezioni frontali ed esercitazioni pratiche. L'attività didattica è organizzata prevalentemente su base semestrale. Per gli studenti a tempo parziale o contestualmente impegnati in attività lavorative, compatibilmente con le risorse disponibili, potranno essere predisposte apposite modalità organizzative dell'attività formativa.

Art. 6 - Percorso formativo

Nell'Allegato 1 è riportato il Percorso formativo, contenente tutte le attività didattiche previste dal Corso di Laurea Magistrale, con la tabella relativa ai risultati di apprendimento attesi espressi tramite i Descrittori Europei in relazione alle singole attività formative previste, nonché i docenti di riferimento e i docenti tutor.

Art. 7 - Docenti del Corso di Studio

L'elenco dei docenti del Corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence è disponibile nel sito web del CdS e nel Manifesto annuale della Facoltà.

Art. 8 - Programmazione degli accessi

L'accesso al Corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence è libero. Esistono i vincoli imposti dai requisiti curricolari e della preparazione personale richiesti per l'ammissione.
L'utenza sostenibile indicata dal Ministero è pari a 80 studenti.

Art. 9 - Requisiti e modalità di accesso

Per essere ammessi al Corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence occorre essere in possesso della laurea o di altro titolo di studio conseguito all'estero e riconosciuto idoneo.
L'iscrizione al corso è inoltre subordinata al possesso dei requisiti curricolari ed alla verifica della adeguatezza della preparazione personale di seguito indicati.
Eventuali integrazioni curricolari necessarie per il rispetto dei requisiti di accesso potranno essere acquisite attraverso l'iscrizione a singoli insegnamenti impartiti presso i propri corsi di studio dell'Università di Cagliari.

Requisiti curricolari

(a) Possesso della laurea o del diploma universitario di durata triennale, ovvero di altro titolo di studio conseguito all'estero, ritenuto idoneo.
(b) Certificazione di livello B2 relativamente alla conoscenza della lingua inglese. Questo requisito indirizza in maniera efficace quanto richiesto dagli obiettivi formativi della classe, che stabiliscono che "I laureati nei corsi di laurea magistrale della classe devono essere in grado di utilizzare fluentemente, in forma scritta e orale, almeno una lingua dell'Unione Europea oltre l'italiano, con riferimento anche ai lessici disciplinari".
Non è richiesta la presentazione della certificazione di conoscenza della lingua inglese nel caso in cui il corso di laurea o di diploma universitario di durata triennale, ritenuto idoneo per l'accesso, sia stato erogato prevalentemente in lingua inglese.
(c) Aver acquisito almeno 12 CFU nell'insieme dei settori MAT e FIS.
(d) Aver acquisito almeno 36 crediti formativi universitari nell'insieme dei settori INF/01 e ING/INF di cui almeno 18 CFU nei settori INF/01 e ING-INF/05.
Un'apposita Commissione, designata dal Corso di Studio, ha il compito di verificare l'idoneità del candidato all'immatricolazione per quanto attiene la conformità dei requisiti curricolari e della preparazione personale nel caso questi non possano essere accertati d'ufficio, in particolare modo nel caso di laurea rilasciata all'estero.

La Commissione, analizzata la carriera dello studente, potrà individuare un percorso formativo personalizzato con una differenziazione nelle attività caratterizzanti e affini non superiore a 12 crediti formativi, nel rispetto dell'Ordinamento Didattico.

Adeguatezza della preparazione personale

Previa verifica del possesso dei requisiti curricolari effettuata con le modalità sopra indicate, la adeguatezza della preparazione individuale verrà stabilita da una Commissione del Corso di Studio mediante una prova nella quale verrà verificata la conoscenza di argomenti relativi ai settori scientifico disciplinari per i quali sono prescritti valori minimi dei crediti formativi. Per l'ambito matematico: funzioni, calcolo differenziale e integrale in più variabili, vettori e operazioni sui vettori, matrici, sistemi di equazioni lineari, autovalori e autovettori; per l'ambito fisico: cinematica, dinamica, energia, lavoro e potenza, elettricità, elettromagnetismo; per l'ambito informatico: linguaggi di programmazione e programmazione orientata agli oggetti, algoritmi e strutture dati, architettura dei calcolatori, basi di dati, reti di calcolatori, sistemi operativi. La prova di verifica si svolgerà nel rispetto delle modalità e dei tempi previsti dai Regolamenti di Ateneo e/o di Facoltà.
È considerata adeguata la preparazione personale dei laureati che abbiano conseguito una laurea di tipo tecnico-scientifico rilasciata dall'Università di Cagliari o in altre sedi o conseguita all'estero purché riconosciuta idonea con una votazione pari o superiore a 92/110 o equivalente.

Per gli studenti non comunitari residenti all'estero e che non hanno conseguito un titolo d'accesso in Italia la Commissione può effettuare una valutazione sulla base della documentazione presentata. Nello specifico, la Commissione analizzerà la carriera precedente valutando:

a) Percorso di Laurea (o titolo equivalente) di primo livello:
   - tipologia, classe e titolo di laurea
     - composizione dei crediti necessari per l'accesso anche con riferimento agli argomenti oggetto della prova di valutazione della adeguatezza della preparazione personale
     - eventuale necessità di percorso formativo personalizzato
   - media delle valutazioni conseguite nei singoli insegnamenti e posizionamento dello studente nella sua coorte (se disponibile)
   - posizionamento nazionale o internazionale dell'università che ha rilasciato il titolo
b) Conoscenza della lingua Inglese
c) Valutazione dell'attività complessiva e altri titoli rilevabile dal curriculum e da altri documenti aggiuntivi eventualmente prodotti dallo studente.

Qualora la documentazione presentata non sia sufficiente per stabilire il livello di preparazione personale potrà essere previsto un colloquio, anche per via telematica.

Gli studenti non laureati che intendano effettuare l'iscrizione condizionata ai sensi del Regolamento Carriere Amministrative Studenti dovranno possedere i requisiti curricolari e di adeguatezza della preparazione personale al momento del conseguimento del titolo, e quindi di scioglimento della riserva.
Tutti gli studenti che intendono iscriversi al corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence dovranno, entro i termini stabiliti dal Manifesto Generale

degli Studi, presentare la domanda di ammissione alla prova di verifica della adeguatezza della preparazione personale. La Commissione potrà esonerare dalla prova i candidati che soddisfino i requisiti su indicati di adeguatezza della preparazione personale.

Art. 10 - Iscrizione al Corso di Studio

Tutti coloro che intendono iscriversi al Corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence dovranno iscriversi alla prova di verifica della preparazione personale, presentando apposita domanda on-line collegandosi al sito www.unica.it >Accedi > Esse3 – Studenti e docenti., entro le scadenze indicate dal Manifesto Generale degli Studi.
I candidati dovranno allegare l'autocertificazione del titolo con gli esami superati durante la carriera e, se richiesto dal Consiglio di Corso di Studio, i relativi programmi. In caso di titolo conseguito all'estero inoltre si rimanda alle specifiche circolari ministeriali.
Poiché le attività già riconosciute ai fini dell'attribuzione dei crediti formativi nell'ambito dei corsi di laurea non possono essere nuovamente riconosciute come crediti formativi nella Laurea Magistrale, il Corso di Studio, sulla base degli esami superati nel percorso di Laurea, potrà definire il piano di studio individuale differente da quello ufficiale che dovrà essere seguito dallo studente per il conseguimento del titolo, nel rispetto dell'Ordinamento Didattico.

Le modalità operative per l'iscrizione on-line al Corso di Studio sono consultabili nel sito web dell'ateneo, alla pagina futuri studenti e studentesse>come iscriversi e immatricolarsi e nel sito web della Facoltà, alla pagina "Iscriversi>Accesso ai Corsi di Laurea Magistrale".

Art. 11 - Iscrizione ad anni successivi, trasferimenti e passaggi

Lo studente iscritto al Corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence si intende iscritto ad anni successivi al primo, per l'anno accademico di riferimento, con il pagamento della prima rata, indicata nel regolamento contribuzione studentesca, entro il termine di scadenza e nel rispetto delle altre modalità, previste annualmente nel Manifesto Generale degli Studi.

Modalità per il trasferimento da altri Corsi di Studio

Il trasferimento ed il passaggio al Corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence sono subordinati al possesso dei requisiti curricolari e alla verifica della preparazione personale previsti per l'accesso.
Gli studenti provenienti da altro Corso di Laurea Magistrale o da altro Ateneo che chiedono di essere ammessi al Corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence devono presentare la richiesta di convalida degli esami universitari già superati e di riconoscimento dei relativi crediti contestualmente alla domanda d'iscrizione, allegando l'autocertificazione delle attività formative sostenute e, se richiesto dal Corso di Studio, anche i relativi programmi.
Il Corso di Studio, previo accertamento dei requisiti richiesti per l'accesso, valuterà, anche sulla base dei programmi delle discipline, le possibili equivalenze, o le corrispondenze anche non complete nei programmi, con le materie previste nel percorso formativo e convaliderà gli esami, riconoscendo il maggior numero possibile di crediti sulla base dei programmi degli esami superati con esito positivo, anche ricorrendo a colloqui per la verifica delle conoscenze effettivamente possedute e motivando

l'eventuale mancato riconoscimento di crediti già acquisiti. In particolare, in caso di trasferimento da corsi di laurea magistrale della medesima classe e, se svolti con modalità a distanza, accreditati ai sensi della normativa vigente, saranno riconosciuti in ogni settore scientifico disciplinare almeno il 50% dei crediti acquisiti.

L'anno di corso al quale lo studente viene ammesso è deliberato dal Corso di Studio sulla base delle discipline e dei crediti convalidati.

Art. 12 - Tirocini

Il Corso di Studio in Computer Engineering, Cybersecurity and Artificial Intelligence promuove e incoraggia le attività formative volte ad acquisire abilità utili per l'inserimento nel mondo del lavoro e ad agevolare le scelte professionali mediante la conoscenza diretta dei settori lavorativi dell'Ingegneria dell'Informazione favorendo lo svolgimento di tirocini formativi e stage presso Aziende, Enti e Pubbliche amministrazioni. La gestione di tali attività è svolta dalla Facoltà di Ingegneria e Architettura e, a livello dipartimentale all'interno del Dipartimento di Ingegneria Elettrica ed Elettronica, tramite una apposita commissione (CRML - Commissione Rapporti con il Mondo del Lavoro) che riunisce i rappresentanti di tutti i corsi di studio promossi dal dipartimento stesso.
A tale scopo, su proposta di un docente del Corso di Studio che svolge la funzione di Tutore interno, il Consiglio definisce, sulla base di convenzioni stipulate con gli Enti ospitanti, specifici progetti formativi per ogni studente interessato nei quali viene indicato un dipendente dell'Ente ospitante che svolga la funzione di Tutore esterno. Possono essere attivati anche tirocini interni sotto la responsabilità di un docente dell'Ateneo. I corrispondenti crediti sono riconosciuti con delibera del Corso di Studio, sulla base della documentazione presentata.

Art. 13 - Crediti formativi universitari

L'impegno complessivo dell'apprendimento svolto in un anno da uno studente a tempo pieno è fissato convenzionalmente in 60 crediti, a ciascuno dei quali corrispondono 25 ore di impegno. La frazione di questo impegno riservata allo studio o ad altre attività formative di tipo individuale non può essere inferiore al 50%. Ad ogni credito formativo corrispondono non più di 10 ore di lezioni frontali o attività didattiche equivalenti, comprensive di esercitazioni e attività assistite equivalenti, rimanendo le restanti da dedicare allo studio individuale.
Nel caso di attività formative di elevato contenuto sperimentale o pratico, ad un credito corrispondono da un minimo di 8 ad un massimo di 16 ore di attività assistita in aula e/o laboratorio, mentre le restanti sino al raggiungimento delle 25 ore totali previste sono da dedicare allo studio e alla rielaborazione personale, e/o alla pratica individuale in laboratorio e in campo.
Infine, per attività individuali di studio, per attività esclusivamente di laboratorio e per le attività di tirocinio ad ogni credito corrispondono 25 ore di impegno effettivo dello studente.

Art. 14 - Propedeuticità

Non sono previste propedeuticità ufficiali; tuttavia lo studente è tenuto a seguire il percorso formativo rispettando la sequenza degli insegnamenti e dei relativi esami e facendo riferimento a quanto indicato in proposito nell'allegato 1.

Art. 15 - Obblighi di frequenza

La frequenza alle attività formative è di norma obbligatoria. L'accertamento della frequenza avverrà secondo modalità e criteri stabiliti dal Corso di Studio. Potranno essere esonerati dall'obbligo della frequenza ai corsi gli studenti che ne facciano domanda con motivate e documentate ragioni.

Art. 16 - Verifiche del profitto

Il numero annuale degli appelli e la loro distribuzione nell'arco dell'anno sono stabiliti in conformità ai Regolamenti di Ateneo e della Facoltà.

Gli esami di profitto consistono in una prova finale di verifica della preparazione dello studente sul programma ufficiale del corso. Essa può avere forma sia orale, sia scritta, sia mista. La prova d'esame può comprendere la discussione di elaborati, progetti ed esperienze svolti dal candidato sotto la direzione dei docenti e tenere conto, inoltre, di eventuali prove intermedie sostenute dallo studente durante il semestre.

Le modalità di accertamento degli obiettivi formativi in esito ai singoli insegnamenti sono descritte per ciascuno di essi nelle rispettive pagine disponibili attraverso il sito web del Corso di Studio e del Docente.
La valutazione finale è espressa con una votazione in trentesimi e per il superamento dell'esame è necessaria una votazione non inferiore a 18/30. Il superamento di un esame di profitto consente allo studente l'acquisizione dei relativi crediti.
Nel caso di corsi integrati costituiti da due o più moduli didattici la valutazione complessiva del profitto non può essere frazionata in valutazioni separate sui singoli insegnamenti o moduli e verrà espressa collegialmente dai docenti titolari degli insegnamenti. I relativi crediti si acquisiranno pertanto solo a seguito della valutazione complessiva di tutti i moduli, anche qualora essi siano distribuiti su due semestri.
Le Commissioni esaminatrici sono costituite da almeno due membri nominati con le modalità previste dal Regolamento Didattico d'Ateneo.

Art. 17 - Regole per la presentazione dei Piani di Studio individuali

Lo studente può presentare un piano di studio individuale ai sensi del DM 270/2004, come integrato dal DM 96/2023 e del Regolamento Didattico d'Ateneo, che dovrà essere approvato dal Consiglio di Corso di Studio, nel rispetto dell'ordinamento didattico vigente. La presentazione dei piani di studio individuali dovrà avvenire entro il 31 ottobre, ovvero entro il 15 marzo per i soli studenti che regolarizzano l'iscrizione entro il 28 febbraio, salvo diversa delibera del Consiglio.
Gli studenti hanno comunque l'obbligo di indicare le attività formative autonomamente scelte previste dall'Art. 10 comma 5 lettera a) del D.M. 270/04. A tal fine agli studenti è assicurata la libertà di scelta tra tutti gli insegnamenti attivati nell'Ateneo, compresa l'acquisizione di ulteriori crediti formativi nelle discipline caratterizzanti, purché la scelta sia coerente con il progetto formativo.

Art. 18 - Mobilità internazionale

Il Corso di Studio in Computer Engineering, Cybersecurity and Artificial Intelligence promuove e incoraggia le attività formative all'estero. A tal fine specifiche convenzioni sono stipulate con Università estere sedi di Corsi di studio in Ingegneria dell'Informazione o ad essi affini. Il Corso di Studio riconosce i crediti maturati durante i periodi di studio all'estero, previo esame dei programmi

degli insegnamenti sostenuti e della loro coerenza con gli obiettivi formativi del Corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence.

Art. 19 - Riconoscimento CFU per abilità professionali

Secondo quanto previsto dall'articolo 5, comma 7 D.M. 270/04, possono essere riconosciuti dal Corso di Studio crediti formativi derivanti da conoscenze e abilità professionali certificate individualmente ai sensi della normativa vigente in materia, nonché altre conoscenze e abilità maturate in attività formative di secondo livello universitario alla cui progettazione e realizzazione l'Università abbia concorso. Il numero massimo di crediti formativi universitari riconoscibili è pari a 12, complessivamente tra corsi di I e II livello. Il riconoscimento sarà effettuato esclusivamente sulla base delle competenze dimostrate da ciascuno studente. Sono escluse forme di riconoscimento attribuite collettivamente.

Art. 20 - Orientamento e Tutorato

Il Corso di Studio promuove la proficua partecipazione attiva degli studenti alla vita universitaria e si attiva per prevenire la dispersione e il ritardo negli studi attraverso molteplici servizi di orientamento e tutorato. Il dettaglio dei servizi è disponibile sul sito del Corso di Studio, alla voce "Orientarsi".

Art. 21 - Prova finale

Per essere ammessi all'esame di Laurea occorre aver superato con esito positivo gli esami degli insegnamenti e completato le altre attività formative previste nel piano degli studi con le modalità stabilite dal presente regolamento, comprese quelle relative alla preparazione della prova finale, conseguendo i relativi crediti.
La prova finale consiste nella discussione di una relazione (tesi) relativa ad un lavoro individuale, svolto dal laureando sotto la supervisione di almeno un docente della Facoltà di Ingegneria e dell'Architettura dell'Università degli Studi di Cagliari, riguardo aspetti tecnici e/o scientifici pertinenti all'area dell'ingegneria dell'informazione e della sicurezza informatica o dell'intelligenza artificiale in particolare.
Il lavoro potrà consistere in un'analisi critica dello stato dell'arte o la redazione di un progetto almeno di massima o lo sviluppo di metodologie e tecniche con un certo grado di originalità o un trasferimento di metodologie e tecniche da ambiti differenti in settori dell'ingegneria dell'informazione.

L'elaborato deve essere redatto in lingua inglese.

Le attività relative alla preparazione della prova finale potranno essere svolte:
- presso uno dei gruppi di ricerca del Dipartimento di Ingegneria Elettrica ed Elettronica (DIEE) che forniscono docenza al corso di studio;
- presso un gruppo di ricerca che abbia collaborazioni con i gruppi definiti al punto precedente;
- all'estero, nell'ambito di uno dei diversi programmi internazionali offerti dall'ateneo (Erasmus Plus, Erasmus Placement, Globus Placement, etc.) o come Free Mover;
- presso un'azienda che abbia sede nel territorio regionale, nazionale o all'estero, purché la stessa attività non coincida con l'attività svolta durante un tirocinio per cui siano stati attribuiti crediti

formativi specifici, a meno che tali CFU non siano stati riconosciuti solo per una frazione lavoro svolto complessivamente.

L'elaborato viene discusso di fronte ad una commissione costituita da 5 docenti del Corso di Studio, eventualmente integrata da docenti che forniscono insegnamenti nei corsi di studio del DIEE e in genere presieduta dal coordinatore; durante la discussione lo studente potrà avvalersi di supporti grafici ed informatici.

La presentazione deve coprire la contestualizzazione del lavoro svolto, un'adeguata panoramica sulle problematiche affrontate e sullo stato dell'arte, la descrizione dei materiali e/o dei metodi utilizzati, i risultati ottenuti e le prospettive future del lavoro. La presentazione ha l'obiettivo di verificare la capacità del laureando di comunicare professionalmente e discutere con chiarezza e padronanza l'argomento scelto. Al termine della presentazione si svolge una sessione di domande da parte dei membri della commissione (difesa della tesi).

La commissione valuta la prova finale esprimendo un giudizio che, unitamente alla valutazione del percorso di studi, concorre alla determinazione del voto di laurea che sarà espresso in centodecimi.

Criteri di assegnazione del voto di laurea

Il voto di laurea è attribuito sulla base della carriera accademica, dell'elaborato di tesi e della discussione di fronte alla commissione. L'elaborato viene esaminato rispetto alla completezza dell'esame dello stato dell'arte, l'adeguatezza dei materiali e dei metodi utilizzati, la correttezza ed esaustività dei risultati ottenuti, il grado di approfondimento delle problematiche e l'innovatività delle soluzioni proposte. La presentazione viene valutata in base alla capacità del candidato di tradurre il lavoro svolto in un insieme di slide efficaci, complete e chiare e alla sua capacità di rispondere con competenza e professionalità alle domande.

Uno studente sostiene un numero n di esami con voto. Ogni esame i-esimo con i che varia da 1 a n, ha un certo numero di CFU associati ad esso. Quindi, la formula per il voto di laurea è:

$$\text{Voto di Laurea} = \text{Voto di Tesi} + \frac{\sum_{i=1}^{n} (voto\ i{-}esimo\ esame\ ) \times (CFU\ esame\ i{-}esimo)}{\sum_{i=1}^{n} (CFU\ esame\ i{-}esimo)} \times \frac{110}{30}$$

Il Voto di Tesi varia da 0 a 9 punti.

Come indicazione per l'attribuzione del voto di tesi, si utilizza la seguente classificazione della tipologia di lavoro svolto dallo studente:

Tesi compilativa: fino a 4 punti;

Tesi di progetto: fino a 6 punti;

Tesi di ricerca: fino a 9 punti.

Se il voto di laurea sulla base della media ponderata degli esami e del voto di tesi supera i 110 punti, la commissione valuta se assegnare la lode al voto massimo di 110/110.

La lode può essere assegnata all'unanimità della commissione solo se la somma del voto di tesi e della media ponderata degli esami risulta uguale o maggiore a 112.

Art. 22 - Valutazione delle attività didattiche

Il Corso di Studio promuove la valutazione di tutti gli insegnamenti da parte degli studenti e monitora e analizza periodicamente i risultati al fine di individuare azioni per il miglioramento continuo del Corso di Studio.

Le schede di sintesi della valutazione della didattica sono reperibili nel sito dell'Ateneo e del Corso di Studio.

Art. 23 - Assicurazione della qualità

Il Corso di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence promuove una politica di programmazione e gestione delle attività volta a perseguire il miglioramento continuo, in conformità a quanto previsto dalle norme in materia di Assicurazione della Qualità dei processi formativi universitari e alle buone pratiche sia nazionali che internazionali.
I documenti relativi al Sistema di Assicurazione della Qualità del CdS sono disponibili alla pagina "Qualità e miglioramento".

Art. 24 - Trasparenza – Modalità di trasmissione delle informazioni agli studenti

Il sito web del Corso di Studio è lo strumento preferenziale per la trasmissione delle informazioni agli studenti. Attraverso il sito sono consultabili:
- i regolamenti che determinano il funzionamento del Corso di Laurea Magistrale;
- l'ordinamento didattico del Corso di Laurea Magistrale;
- il percorso formativo del Corso di Laurea Magistrale;
- i calendari e gli orari delle attività didattiche;
- i calendari e gli orari degli appelli d'esame e di laurea;
- le informazioni sui docenti e sugli insegnamenti.

Sui siti web del Corso di Studio e della Facoltà di Ingegneria e Architettura possono essere pubblicate inoltre:
- informazioni generali;
- avvisi;
- modulistica;
- altre informazioni utili.

Art. 25 - Diploma supplement

Ai sensi della normativa in vigore, l'Università rilascia, a richiesta, come supplemento al diploma di Laurea Magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence, un certificato che riporta, anche in lingua inglese e secondo modelli conformi a quelli adottati dai Paese europei, le principali indicazioni relative al curriculum specifico seguito dallo studente per conseguire il titolo.

Art. 26 - Contemporanea iscrizione a due Corsi di Studio

Secondo quanto previsto nel Decreto Ministeriale n. 930 del 29 luglio 2022, attuativo della Legge n. 33 del 12 aprile 2022, recante "Disposizioni in materia di iscrizione contemporanea a due corsi di istruzione superiore", fermo restando l'obbligo del possesso dei titoli di studio necessari per l'accesso ai diversi livelli della istruzione universitaria, è prevista la possibilità di iscriversi contemporaneamente a due corsi di istruzione superiore all'interno dello stesso Ateneo oppure appartenenti ad Atenei, scuole o istituti superiori a ordinamento speciale, anche esteri.

Nel caso di contemporanea iscrizione a due Corsi di Studio, qualora lo studente abbia già maturato CFU nel corso di prima iscrizione, il Consiglio di Corso di Studio procede al riconoscimento delle attività formative svolte; nel caso di attività formative mutuate, il riconoscimento è concesso automaticamente.
Nel caso di riconoscimento parziale delle attività formative sostenute in un Corso di Studio, il CdS facilita la fruizione da parte dello studente di attività formative integrative al fine del pieno riconoscimento dell'attività formativa svolta.
Il mancato riconoscimento di crediti deve essere adeguatamente motivato.

Art. 27 - Norme finali e transitorie

Per quanto non espressamente indicato nel presente regolamento si rimanda alla normativa vigente.

Allegato 1 - Percorso formativo

1° anno

Sem	Insegnamento	SSD	TAF	CFU	Ore
1	Industrial Software Development	ING-INF/05	B	7	70
1	Cybersecurity Technologies and Risk Management	ING-INF/05	B	8	80
1	Supervisory control and monitoring	ING-INF/04	B	9	90
	Corso integrato: Network and Application Security				
1	- Modulo: Network Security	ING-INF/03	C	4	40
2	- Modulo: Web security and malware analysis	ING-INF/05	B	6	60
	Corso integrato: Intelligent Systems				
1	- Modulo: Artificial Intelligence	ING-INF/05	B	6	60
2	- Modulo: Machine Learning	ING-INF/05	B	7	70
2	Computer Vision Technologies and Biometrics	ING-INF/05	B	6	60
2	Fault diagnosis and estimation in dynamical systems	ING-INF/04	B	5	50

2° anno

Sem	Insegnamento	SSD	TAF	CFU	Ore
	Corso integrato: Embedded Systems				
1	- Modulo: Advanced Embedded Systems	ING-INF/01	C	8	80
1	- Modulo: Internet of Things and Digital Twins	ING-INF/03	C	6	60
	Corso integrato: Computer Forensics				
1	- Modulo: Computer Forensics Techniques	ING-INF/05	B	5	50
2	- Modulo: Computer Law	IUS/20	C	5	50
	Un corso a scelta tra:				
1	Machine Learning Security	ING-INF/05	B	5	50
2	Networked control systems and security	ING-INF/04	B	5	50
2	Stochastic Models	ING-INF/04	B	5	50

Ulteriori crediti da acquisire

Sem	Attività formativa	SSD*	TAF*	CFU	h
	1 insegnamento dalla tabella 1		C	6	
	Other activities		F	2	
	Elective activities1		D	10	
	Final examination		E	15	

TOTAL CREDITS 120

(1) La scelta dei relativi crediti formativi deve essere coerente con il percorso formativo dello studente e deve avere l'approvazione vincolante del Consiglio di Corso di Studio.

Tabella 1. Elenco degli insegnamenti di tipologia C (1 a scelta tra quelli proposti)

Sem	Insegnamento	SSD	TAF	CFU	Ore
	1° anno				
2	Corso integrato: Smart Grid and Critical Infrastructures - Modulo: Industrial Informatics for energy storage systems	ING-IND/32	C	2	20
2	- Modulo: Critical infrastructures for innovative power distribution	ING-IND/33	C	2	20
2	- Modulo: Measurements and Cybersecurity for Smart Grid	ING-INF/07	C	2	20
2	Data driven models for system engineering	ING-IND/31	C	6	60
	2° anno				
1	Physical-layer techniques for Wireless communication security	ING-INF/02	C	6	60

Risultati di apprendimento attesi, espressi tramite i Descrittori Europei del titolo di studio

	ATTIVITÀ FORMATIVE																				
	Industrial Software Development	Supervisory control and monitoring	Cybersecurity Technologies and Risk Management	Fault diagnosis and estimation in dynamical systems	Computer Vision Technologies and Biometrics	Network and Application Security - CI - Network Security	Network and Application Security - CI - Web security and malware analysis	Intelligent Systems -CI- Artificial Intelligence	Intelligent Systems -CI- Machine Learning	Computer Forensics -CI- Computer Forensics Techniques	Computer Forensics -CI- Computer Law	Embedded Systems -CI- Advanced Embedded Systems	Embedded Systems -CI- Internet of Things and Digital	Smart Grid and Critical Infrastructures - CI - Industrial Informatics for energy storage sytems	Smart Grid and Critical Infrastructures - CI - Critical infrastructures for innovative power distribution	Smart Grid and Critical Infrastructures - CI - Measurements and Cyber Security for Smart Grid	Data driven models for system engineering	Physical-layer techniques for Wireless communication security	Machine Learning Security	Networked control systems and security	Stochastic Models	Final examination
A – Conoscenza e capacità di comprensione																					
A1) Conoscere e comprendere le metodologie di sviluppo software in diversi ambiti aziendali, e, in particolare, in ambienti distribuiti. Conoscere e comprendere le basi delle metodologie per lo sviluppo di software sicuro.	x		x	x		x	x					x	x							x		x
B1) Conoscere e comprendere le architetture di calcolo e le metodologie di comunicazione caratteristiche dei sistemi embedded e della Internet of Things.				x								x	x					x		x		x
C1) Conoscere e comprendere le metodologie per la modellazione di sistemi complessi, e le tecnologie per il loro governo, con particolare riferimento agli aspetti legati alla sicurezza informatica.	x	x	x	x										x	x	x	x			x	x	x
D1) Conoscere e comprendere gli aspetti relativi alla sicurezza logica e fisica delle reti e di sistemi complessi, le tecnologie informatiche e le metodologie organizzative e gestionali per la progettazione di software sicuro e per la mitigazione del rischio e l'analisi dei sistemi in caso di violazione.	x	x	x	x	x	x	x			x					x	x		x		x		x
E1) Conoscere e comprendere gli aspetti economici e giuridici legati alla sicurezza informatica.	x	x	x	x						x	x				x					x		x
F1) Conoscere e comprendere gli approcci alla base degli algoritmi utilizzati per l'apprendimento automatico e l'intelligenza artificiale, e la loro applicazione alla realizzazione di meccanismi di protezione fisica e logica.			x		x			x	x								x		x			x
B – Capacità di applicare conoscenza e comprensione																					
A2) Capacità di applicare le conoscenze relative alla progettazione, sviluppo e verifica del software in ambiti complessi, anche con riferimento alle tematiche di sviluppo di software sicuro.	x		x	x		x	x					x	x							x		x
B2) Capacità di applicare le conoscenze relative alle architetture di sistemi embedded e Internet of Things finalizzate allo sviluppo software in ambito distribuito e alla analisi di sicurezza dal punto di vista del rischio derivante da attacchi informatici.	x		x	x								x	x					x		x		x

C2) Capacità di applicare le conoscenze relative alla modellazione e gestione di sistemi complessi, con particolare attenzione agli aspetti di sicurezza e di gestione del rischio.	x	x	x	x				x			x			x	x	x	x			x	x	x
D2) Capacità di formulare e applicare soluzioni all'avanguardia per la mitigazione del rischio nel campo della cybersecurity, sia in fase di progettazione, sia in fase di esercizio, in diversi contesti applicativi, e per la gestione dei sistemi in presenza di violazione.	x	x	x	x	x	x	x	x	x	x	x				x	x		x	x	x		x
F2) Capacità di implementare soluzioni algoritmiche originali adeguate ottenute o derivate dalla conoscenza delle metodologie di intelligenza artificiale, anche con applicazione alla sicurezza fisica e logica dei sistemi.			x		x	x	x	x	x		x						x		x			x
C – Autonomia di giudizio																							
1) Essere in grado di formulare una propria valutazione e/o giudizio sulla base della interpretazione dei dati disponibili e di modelli astratti.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2) Essere in grado di individuare le modalità, anche originali ed innovative, di raccolta di dati aggiuntivi eventualmente necessari per conseguire una maggiore certezza riguardo temi complessi dell'ingegneria dell'informazione, con particolare enfasi sugli aspetti di sicurezza informatica	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3) Avere capacità del saper fare, del saper prendere iniziative e decisioni nella consapevolezza dei rischi, tenendo conto oltre che dell'evoluzione e sviluppo della tecnica anche dell'impatto economico e sociale delle scelte.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
D – Abilità nella comunicazione																							
Saper comunicare in maniera efficace informazioni e idee, nonché discutere problemi e soluzioni. Sapere scegliere la forma e il mezzo di comunicazione adeguati all'interlocutore, sia specialista che non specialista.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E – Capacità di apprendere																							
1) Avere capacità di auto-formazione che sono necessarie ad un ingegnere per aggiornarsi con continuità rispetto all'evoluzione della scienza e della tecnica nel campo dell'ingegneria dell'informazione	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2) Avere la capacità di attingere a diverse fonti bibliografiche al fine di acquisire nuove competenze.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3) Avere la capacità di auto-apprendimento necessaria ad intraprendere studi successivi, come corsi di Master di secondo livello e di Dottorato nell'ambito dell'ingegneria dell'informazione, e sicurezza informatica in particolare, nonché ad intraprendere l'attività lavorativa presso centri di ricerca e progettazione avanzata.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Docenti di riferimento e Tutor docenti disponibili per gli studenti

Docenti di riferimento	**Tutor docenti**
Biggio Battista	Biggio Battista
Franceschelli Mauro	Franceschelli Mauro
Fumera Giorgio	Giacinto Giorgio
Giacinto Giorgio	Maiorca Davide
Lodi Matteo Bruno	Seatzu Carla
Maiorca Davide	