| | |
|---|---|
| **Università** | Università degli Studi di CAGLIARI |
| **Classe** | LM-32 - Ingegneria informatica |
| **Nome del corso in italiano** | Computer Engineering, Cybersecurity and Artificial Intelligence<br>*riformulazione di: Computer Engineering, Cybersecurity and Artificial Intelligence (1379320)* |
| **Nome del corso in inglese** | Computer Engineering, Cybersecurity and Artificial Intelligence |
| **Lingua in cui si tiene il corso** | inglese |
| **Codice interno all'ateneo del corso** | 70/90^2018 |
| **Data di approvazione della struttura didattica** | 16/11/2017 |
| **Data di approvazione del senato accademico/consiglio di amministrazione** | 16/02/2018 |
| **Data della consultazione con le organizzazioni rappresentative a livello locale della produzione, servizi, professioni** | 28/09/2017 |
| **Data del parere favorevole del Comitato regionale di Coordinamento** | 17/01/2018 |
| **Modalità di svolgimento** | a. Corso di studio convenzionale |
| **Eventuale indirizzo internet del corso di laurea** | |
| **Dipartimento di riferimento ai fini amministrativi** | Ingegneria Elettrica ed Elettronica |
| **EX facoltà di riferimento ai fini amministrativi** | |
| **Massimo numero di crediti riconoscibili** | *12 DM 16/3/2007 Art 4* **Nota 1063 del 29/04/2011** |

**Obiettivi formativi qualificanti della classe: LM-32 Ingegneria informatica**

I laureati nei corsi di laurea magistrale della classe devono:

- conoscere approfonditamente gli aspetti teorico-scientifici della matematica e delle altre scienze di base ed essere capaci di utilizzare tale conoscenza per interpretare e descrivere i problemi dell'ingegneria complessi o che richiedono un approccio interdisciplinare;

- conoscere approfonditamente gli aspetti teorico-scientifici dell'ingegneria, sia in generale sia in modo approfondito relativamente a quelli dell'ingegneria informatica, nella quale sono capaci di identificare, formulare e risolvere anche in modo innovativo problemi complessi o che richiedono un approccio interdisciplinare;

- essere capaci di ideare, pianificare, progettare e gestire sistemi, processi e servizi complessi e/o innovativi;

- essere capaci di progettare e gestire esperimenti di elevata complessità;

- essere dotati di conoscenze di contesto e di capacità trasversali;

- avere conoscenze nel campo dell'organizzazione aziendale (cultura d'impresa) e dell'etica professionale;

- 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.

L'ammissione ai corsi di laurea magistrale della classe richiede il possesso di requisiti curriculari che prevedano, comunque, un'adeguata padronanza di metodi e contenuti scientifici generali nelle discipline scientifiche di base e nelle discipline dell'ingegneria, propedeutiche a quelle caratterizzanti previste nell'ordinamento della presente classe di laurea magistrale.

I corsi di laurea magistrale della classe devono inoltre culminare in una importante attività di progettazione, che si concluda con un elaborato che dimostri la padronanza degli argomenti, la capacità di operare in modo autonomo e un buon livello di capacità di comunicazione.

I principali sbocchi occupazionali previsti dai corsi di laurea magistrale della classe sono quelli dell'innovazione e dello sviluppo della produzione, della progettazione avanzata, della pianificazione e della programmazione, della gestione di sistemi complessi, sia nella libera professione sia nelle imprese manifatturiere o di servizi che nelle amministrazioni pubbliche. I laureati magistrali
potranno trovare occupazione presso industrie informatiche operanti negli ambiti della produzione hardware e software; industrie per l'automazione e la robotica; imprese operanti nell'area dei sistemi informativi e delle reti di calcolatori; imprese di servizi; servizi informatici della pubblica amministrazione.

Gli atenei organizzano, in accordo con enti pubblici e privati, stages e tirocini.

**Sintesi della consultazione con le organizzazioni rappresentative a livello locale della produzione, servizi, professioni**

I componenti del comitato promotore hanno preliminarmente effettuato uno studio approfondito degli scenari nazionali e internazionali di riferimento contenuti in un documento distribuito il 1 Marzo 2017 ai componenti la Giunta di Dipartimento e successivamente ai membri del consiglio di dipartimento. In tale documento, oltre ad evidenziare le crescenti esigenze del mercato del lavoro a livello internazionale negli ambiti della cybersecurity e dell'intelligenza artificiale, si sottolineavano due fatti importanti a livello istituzionale nazionale:
- il protocollo d'intesa sottoscritto da CRUI (Conferenza dei Rettori delle Università Italiane) e il DIS (Dipartimento delle Informazioni per la Sicurezza), organo del Sistema di Informazione per la Sicurezza della Repubblica finalizzato a realizzare la "protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia", "favorendo la creazione di pool interuniversitari" finalizzati a realizzare "un coordinamento nazionale, strutturato e incisivo, che moltiplica le capacità individuali e le pone a servizio del sistema Paese";
- la mozione approvata il 17 febbraio 2017 dalla Camera dei Deputati che impegna il governo a "favorire una linea comune tra i Ministeri nell'approccio allo sviluppo sostenibile della robotica, dell'intelligenza artificiale e della sicurezza informatica; a promuovere attività di formazione, ricerca e sviluppo nelle scuole, nelle università e nei centri di ricerca italiani di tali tecnologie e a sostenerne le applicazioni alla produzione industriale e ai servizi civili in imprese consolidate e in start up innovative".
Le attività svolte all'interno del Dipartimento di Ingegneria Elettrica ed Elettronica, sia attraverso la partecipazione al Laboratorio Nazionale di Cybersecurity del CINI,

quale coordinamento nazionale strutturato interuniversitario, sia attraverso le attività di ricerca di base e applicata nei settori della cybersecurity e dell'intelligenza artificiale, ben si armonizzano con le richieste provenienti dalle istituzioni di un maggiore impegno in ambito formativo in questi settori.
Diversi studi a livello nazionale e internazionale, riportati sempre più frequentemente dai diversi organi di informazione nazionali e internazionali, evidenziano la crescente necessità di esperti in ambito cybersecurity e intelligenza artificiale. A titolo di esempio si citano i rapporti pubblicati dal World Economic Forum sul futuro del mondo del lavoro del 2016 (https://www.weforum.org/reports/the-futureof-jobs), e il recente rapporto annuale 2016-2017 (https://www.weforum.org/reports/annual-report-2016-2017) pubblicato nel mese di settembre 2017, dai quali emerge l'insufficienza della forza lavoro a livello mondiale negli ambiti della cybersecurity e dell'intelligenza artificiale, settori chiave per lo sviluppo scientifico, tecnologico e economico.
A livello locale, la Sardegna sta conoscendo da diversi anni una crescita della presenza di aziende che operano in ambito informatico sia nate da iniziative di imprenditori locali (Tiscali, Abinsula, ecc.), sia come sedi operative di aziende nazionali e internazionali (Vitrociset, IBM, Accenture, Huawei, ecc.), sia come start-up innovative, grazie alla presenza di incubatori e agli incentivi offerti da Sardegna Ricerche.
Gli incontri fra le aziende e l'Università di Cagliari, sia in occasione di dibattiti pubblici, sia in occasione della partecipazione congiunta a bandi competitivi per progetti di ricerca, hanno fatto emergere una crescente esigenza di formazione specifica negli ambiti propri dell'ingegneria informatica, con un'attenzione particolare ai temi della sicurezza informatica da un lato, e ai temi della intelligenza artificiale dall'altro.
A partire da queste premesse, sono state consultate dal comitato promotore 9 organizzazioni rappresentative del mondo della produzione, dei servizi e delle professioni il 18 settembre 2017, il 28 settembre 2017 e il 4 ottobre 2017. Hanno partecipato agli incontri:
- la Regione Autonoma della Sardegna, attraverso il Direttore Generale degli affari generali e della società dell'informazione (Assessorato degli affari generali)
- centro di ricerca regionale (CRS4), attraverso il responsabile dell'area sicurezza informatica
- grandi aziende internazionali in ambito informatico (Amazon e DXC Technology), attraverso la figura di due project manager
- grande impresa nazionale (Saras, Engineering Ingegneria Informatica), attraverso i responsabili di area ricerca e di settore tecnologie digitali e cybersecurity
- associazione industriali (Confindustria Sardegna Meridionale), attraverso il responsabile del settore tecnologie per l'informazione e la comunicazione
- incubatore di impresa e società di venture capital (The Net Value e United Ventures), attraverso uno dei soci
- piccole imprese con sede in Sardegna in ambito cybersecurity (Abissi), attraverso l'amministratore unico.

Tutti i soggetti coinvolti hanno concordato sulla necessità di un corso in ambito ingegneria informatica in Sardegna per soddisfare le crescenti esigenze del mercato del lavoro in questo ambito, e, in particolare, hanno apprezzato la focalizzazione sui temi della cybersecurity e della intelligenza artificiale perchè temi dominanti lo sviluppo di qualunque nuova tecnologia e applicazione in ambito informatico.
Nelle consultazioni effettuate con le organizzazioni rappresentative successivamente alla predisposizione del percorso formativo, consultazioni svoltesi nei giorni 6, 8 e 17 novembre 2017, è stato espresso parere positivo sull'offerta formativa proposta, che rappresenta una risposta alle esigenze correnti del mercato del lavoro nell'ambito dell'ingegneria informatica sia a livello locale che nazionale e internazionale, soprattutto per l'approccio multidisciplinare caratteristico che non ha riscontro con altre offerte formative in ambito nazionale. Sono stati formulati suggerimenti relativi al potenziamento della formazione in ambito 'cloud computing' e 'infrastrutture critiche' anche attraverso l'organizzazione di seminari tenuti da professionisti del settore per presentare le diverse soluzioni tecnologiche disponibili sul mercato per il 'cloud computing', e casi di studio relativi alla messa in sicurezza di infrastrutture critiche.

**Sintesi del parere del comitato regionale di coordinamento**

Il Comitato Regionale di Coordinamento, nella seduta del 17/01/2018, ha deliberato di rendere parere favorevole sull'istituzione del corso

**Obiettivi formativi specifici del corso 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.

**Risultati di apprendimento attesi, espressi tramite i Descrittori europei del titolo di studio (DM 16/03/2007, art. 3, comma 7)**

**Conoscenza e capacità di comprensione (knowledge and understanding)**

Il laureato magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence avrà conseguito i seguenti obiettivi formativi, suddivisi nei quattro assi formativi dell'ingegneria informatica (1), l'ingegneria dei sistemi (2), la scienza della sicurezza (3) e l'intelligenza artificiale (4):
1.a) conosce le metodologie di sviluppo software in diversi contesti aziendali, sia nell'ambito dei sistemi informativi, sia nell'ambito dei sistemi di produzione di beni e servizi e ne comprende le ricadute applicative;
1.b) conosce le tecnologie alla base delle moderne architetture hardware e software in ambiti industriali, sistemi embedded, ambienti distribuiti e Internet of Things, comprendendone le potenzialità e limiti applicativi;
2.a) conosce e comprende gli aspetti applicativi delle metodologie di analisi e progettazione dei sistemi di supervisione e controllo e le relative tecnologie per la loro realizzazione in ambiti civili e industriali complessi;
2.b) conosce le caratteristiche di alcuni sistemi industriali che permettono la realizzazione di soluzioni informatiche avanzate basate anche su metodologie di intelligenza artificiale, analizzandone i rischi derivanti da attacchi informatici;
3.a) conosce e comprende gli aspetti relativi alla sicurezza fisica e logica dei sistemi e le metodologie per l'analisi delle vulnerabilità e del rischio "cyber";
3.b) conosce e comprende gli aspetti applicativi delle tecnologie e metodologie organizzative e gestionali per la mitigazione del rischio in fase di progettazione e di esercizio;
3.c) conosce i fondamentali aspetti economici e giuridici della sicurezza, e degli aspetti legislativi legati alla privacy e alla proprietà intellettuale e ne comprende le ricadute in ambito progettuale e gestionale;
4) conosce gli approcci all'analisi di dati basati su intelligenza artificiale e machine learning e ne comprende le applicazioni e le implicazioni in ambito cybersecurity.

L'acquisizione di tali conoscenze e la comprensione delle loro ricadute applicative avviene attraverso un percorso didattico composto da insegnamenti obbligatori e opzionali nei diversi ambiti di interesse dell'ingegneria dell'informazione e in alcuni ambiti specifici dell'ingegneria industriale.

La verifica delle conoscenze e delle capacità di comprensione acquisite avverrà attraverso le verifiche finali dei vari insegnamenti, le cui modalità saranno definite nelle rispettive schede descrittive.

**Capacità di applicare conoscenza e comprensione (applying knowledge and understanding)**

In riferimento ai quattro assi formativi dell'ingegneria informatica (1), l'ingegneria dei sistemi (2), la scienza della sicurezza (3) e l'intelligenza artificiale (4), il laureato magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence avrà sviluppato:
1) la capacità di progettare, sviluppare e gestire software e sistemi informatici in diversi contesti aziendali e industriali, e in ambienti distribuiti;
2) la capacità di progettare, sviluppare e gestire sistemi di controllo in sistemi industriali complessi, e in particolare negli ambiti tipici in cui un ingegnere informatico esperto in cybersecurity e intelligenza artificiale si potrà trovare ad operare, quali le smart grid, le infrastrutture critiche, e la sicurezza delle comunicazioni wireless;
3) la capacità di analizzare le vulnerabilità e il rischio cyber, di mettere in opera misure di mitigazione del rischio in contesti concreti, e di applicare le tecniche atte a massimizzare la sicurezza logica e fisica dei sistemi;
4) la capacità di applicare le tecniche basate sull'apprendimento automatico e l'intelligenza artificiale alla realizzazione di sistemi di protezione fisica e logica per la mitigazione del rischio cyber.

Tali capacità vengono sviluppate principalmente negli insegnamenti caratterizzanti ed affini obbligatori attraverso la discussione e l'esame di casi concreti, la redazione di una tesi di Laurea in lingua inglese su una delle tematiche affrontate durante il percorso formativo, o durante attività di tirocinio e formazione presso consolidate aziende nei settori orientati al mercato della sicurezza informatica.

**Autonomia di giudizio (making judgements)**

Il Laureato Magistrale sarà in grado di formulare una propria valutazione e/o giudizio sulla base della interpretazione dei dati disponibili e di modelli astratti, nonché 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. Questo si esprimerà attraverso la 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. Ciò avverrà mediante gli insegnamenti specifici volti all'apprendimento delle tecniche di sviluppo di modelli formali e di acquisizione e trattamento di dati e segnali, ma anche attraverso l'integrazione tra gli insegnamenti.
La verifica della maturità e autonomia di giudizio viene effettuata con continuità dai docenti durante il percorso formativo attraverso le verifiche periodiche e finali. In particolare, gli insegnamenti che prevedono una significativa componente progettuale, attraverso esercitazioni, tesine e/o attività di laboratorio, e la prova finale, basata su un lavoro originale, consentono di valutare la capacità di giudizio autonomo dello studente.

**Abilità comunicative (communication skills)**

Il Laureato Magistrale deve sapere comunicare in maniera efficace agli interlocutori le proprie idee e proposte di soluzione, anche innovative e di elevata complessità, chiarendo la loro ratio nonché informazioni sia tecniche che di carattere generale. Saprà scegliere la forma ed il mezzo di comunicazione adeguati all'interlocutore, sia specialista che non specialista. Questo si esprimerà attraverso la capacità di utilizzare correttamente sia il linguaggio tecnico che quello formale e di saper esemplificare in maniera chiara i concetti e le tematiche tipiche dell'ingegneria dell'informazione. Egli sarà capace di comunicare efficacemente in forma scritta e orale.
Le abilità comunicative in ingresso, il cui livello minimo si considera certificato dal conseguimento del titolo di studi universitario di primo livello, vengono sviluppate attraverso l'attività didattica dei docenti che, utilizzando varie forme di comunicazione, costituiscono un esempio di comunicazione efficace.
Gli esami di profitto, prevedendo nel complesso sia prove scritte che orali, costituiscono sia uno stimolo a sviluppare entrambe le principali forme di espressione che un'occasione di verifica del conseguimento delle stesse.
Verrà valorizzata l'acquisizione di ulteriori conoscenze linguistiche mediante il riconoscimento di crediti per il conseguimento di attestazioni di conoscenza delle lingue straniere almeno a livello C1 per quanto riguarda la lingua inglese.

**Capacità di apprendimento (learning skills)**

Il laureato magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence avrà sviluppato le 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. Egli avrà sviluppato la capacità di attingere a diverse fonti bibliografiche al fine di acquisire nuove competenze.
Inoltre, avrà 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.
Il suo sviluppo riguardo a tematiche avanzate ed innovative dell'ingegneria dell'informazione viene ottenuto col riferimento continuo a varie fonti bibliografiche per la preparazione alle prove di esame ed alla prova finale.

Inoltre, per favorire tale obiettivo, il Corso di Studi può organizzare seminari specifici su temi di interesse per un ingegnere dell'informazione.
La verifica della capacità di apprendimento è contestuale alla verifica delle competenze durante le prove di esame, anche facendo ricorso, per alcuni insegnamenti, a modalità che prevedano la redazione di un elaborato su casi non trattati durante i corsi.
Le capacità di cui sopra verranno verificate attraverso:
- un insieme di esami prossimi a ciascuno dei punti evidenziati sopra;
- la redazione di una tesi di Laurea in lingua inglese su una delle tematiche affrontate durante il percorso formativo;
- attività di tirocinio e formazione presso consolidate aziende nei settori orientati al mercato della sicurezza informatica.

**Conoscenze richieste per l'accesso**
**(DM 270/04, art 6, comma 1 e 2)**

Per essere ammessi al Corso di Laurea Magistrale in Computer Engineering, CyberSecurity and Artificial Intelligence occorre soddisfare i seguenti requisiti:
(a) Il possesso della laurea o del diploma universitario di durata triennale, ovvero di altro titolo di studio conseguito all'estero, ritenuto idoneo.
(b) La 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".
(c) L'aver acquisito almeno 12 CFU nell'insieme dei settori MAT e FIS.
(d) L'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.

È prevista la verifica di un'adeguata preparazione personale con modalità definite nel Regolamento didattico del Corso di Studio.

**Caratteristiche della prova finale**
**(DM 270/04, art 11, comma 3-d)**

La prova finale consiste nella discussione di una relazione relativa ad un lavoro individuale, svolto dal laureando sotto la supervisione di almeno un docente della Facoltà di Ingegneria e 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.

**Sbocchi occupazionali e professionali previsti per i laureati**

**Laureato magistrale in Computer Engineering, Cybersecurity and Artificial Intelligence**

**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 occupazionali:**
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.

**Il corso prepara alla professione di (codifiche ISTAT)**

- Analisti e progettisti di software - (2.1.1.4.1)
- Analisti di sistema - (2.1.1.4.2)
- Specialisti in reti e comunicazioni informatiche - (2.1.1.5.1)
- Specialisti in sicurezza informatica - (2.1.1.5.4)

**Il corso consente di conseguire l'abilitazione alle seguenti professioni regolamentate:**

- ingegnere dell'informazione

| |
|---|
| **Il rettore dichiara che nella stesura dei regolamenti didattici dei corsi di studio il presente corso ed i suoi eventuali curricula differiranno di almeno 30 crediti dagli altri corsi e curriculum della medesima classe, ai sensi del DM 16/3/2007, art. 1 §2.** |

**Attività caratterizzanti**

| ambito disciplinare | settore | CFU min | CFU max | minimo da D.M. per l'ambito |
|---|---|---|---|---|
| Ingegneria informatica | ING-INF/04 Automatica<br>ING-INF/05 Sistemi di elaborazione delle informazioni | 50 | 75 | - |
| | **Minimo di crediti riservati dall'ateneo minimo da D.M. 45:** | - | | |

| | |
|---|---|
| **Totale Attività Caratterizzanti** | 50 - 75 |

**Attività affini**

| ambito: Attività formative affini o integrative | | CFU | |
|---|---|---|---|
| | intervallo di crediti da assegnarsi complessivamente all'attività **(minimo da D.M. 12)** | 20 | 40 |
| **A11** | ING-INF/01 - Elettronica<br>ING-INF/03 - Telecomunicazioni | 10 | 20 |
| **A12** | ING-IND/31 - Elettrotecnica<br>ING-IND/32 - Convertitori, macchine e azionamenti elettrici<br>ING-IND/33 - Sistemi elettrici per l'energia<br>ING-INF/02 - Campi elettromagnetici<br>ING-INF/06 - Bioingegneria elettronica e informatica<br>ING-INF/07 - Misure elettriche e elettroniche | 5 | 10 |
| **A13** | IUS/20 - Filosofia del diritto<br>SECS-S/01 - Statistica | 5 | 10 |

| | |
|---|---|
| **Totale Attività Affini** | 20 - 40 |

**Altre attività**

| ambito disciplinare | | CFU min | CFU max |
|---|---|---|---|
| A scelta dello studente | | 8 | 12 |
| Per la prova finale | | 15 | 18 |
| Ulteriori attività formative (art. 10, comma 5, lettera d) | Ulteriori conoscenze linguistiche | 0 | 3 |
| | Abilità informatiche e telematiche | 0 | 2 |
| | Tirocini formativi e di orientamento | 0 | 8 |
| | Altre conoscenze utili per l'inserimento nel mondo del lavoro | 0 | 2 |
| Minimo di crediti riservati dall'ateneo alle Attività art. 10, comma 5 lett. d | | 2 | |
| Per stages e tirocini presso imprese, enti pubblici o privati, ordini professionali | | - | - |

| | |
|---|---|
| **Totale Altre Attività** | 25 - 45 |

**Riepilogo CFU**

| | |
|---|---|
| **CFU totali per il conseguimento del titolo** | **120** |
| **Range CFU totali del corso** | 95 - 160 |

**Motivazioni dell'inserimento nelle attività affini di settori previsti dalla classe o Note attività affini**

I tre gruppi di insegnamento affini corrispondono rispettivamente a:
- attività obbligatorie che completano la formazione nell'ambito della ingegneria informatica nel settore delle architetture di calcolo e delle comunicazioni;
- conoscenze di contesto in ambiti industriali applicativi dell'ingegneria informatica, cybersecurity e intelligenza artificiale;
- attività complementari nei settori dell'informatica giuridica e della statistica.

**Note relative alle altre attività**

I CFU previsti per ulteriori conoscenze linguistiche potranno essere riconosciuti al conseguimento da parte dello studente di certificazione di livello C nella lingua inglese o livello B o C in altre lingue comunitarie.

I CFU previsti per abilità informatiche e telematiche potranno essere riconosciuti per la frequenza con profitto di seminari e corsi per acquisizione di competenze, anche certificate da enti esterni, su software professionale specifico coerente con il percorso di studi

I CFU previsti per tirocini formativi e di orientamento potranno essere riconosciuti alla
conclusione di tirocini svolti in azienda in ambito nazionale e internazionale finalizzati alla formazione professionale negli ambiti del corso di studi.

I CFU previsti per altre conoscenze utili per l'inserimento nel mondo del lavoro potranno essere riconosciuti per la frequenza con profitto di seminari e corsi
finalizzati ad acquisire conoscenze e competenze legate ai temi della imprenditorialità, sicurezza del lavoro, legislazione, o per certificazioni professionali coerenti con il percorso di studi.

**Note relative alle attività caratterizzanti**

RAD chiuso il 16/02/2018