Università	Politecnico di TORINO
Classe	LM-32 - Ingegneria informatica & LM-66 - Sicurezza informatica
Nome del corso in italiano	Sicurezza informatica *adeguamento di: Sicurezza informatica (1421443)*
Nome del corso in inglese	Cybersecurity
Lingua in cui si tiene il corso	inglese
Codice interno all'ateneo del corso	32138-139
Data di approvazione della struttura didattica	07/02/2023
Data di approvazione del senato accademico/consiglio di amministrazione	09/02/2023
Data della consultazione con le organizzazioni rappresentative a livello locale della produzione, servizi, professioni	12/12/2022 -
Data del parere favorevole del Comitato regionale di Coordinamento	09/01/2023
Modalità di svolgimento	a. Corso di studio convenzionale
Eventuale indirizzo internet del corso di laurea	https://www.polito.it/corsi/32-139
Dipartimento di riferimento ai fini amministrativi	AUTOMATICA E INFORMATICA
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.

Obiettivi formativi qualificanti della classe: LM-66 Sicurezza informatica

I laureati magistrali nei corsi di laurea della classe devono:
- conoscere gli aspetti scientifici relativi alle fondamenta della progettazione, realizzazione, verifica e manutenzione di infrastrutture e sistemi informatici sicuri e protetti
- conoscere le metodologie e gli strumenti tecnologici attraverso i quali si progettano, realizzano, verificano e mantengono infrastrutture e sistemi informatici sicuri e protetti, con attenzione sia alle tecniche formali che sperimentali
- conoscere gli aspetti relativi alla organizzazione del lavoro ed alle problematiche di carattere psicologico e sociale come elementi critici rispetto alla sicurezza delle infrastrutture e dei sistemi informatici ed alla protezione dei dati informatici, nonché gli aspetti giuridici relativi al trattamento sicuro e riservato dei dati informatici e quelli bio-sanitari e bio-etici relativi alle tecniche biometriche ed al trattamento, conservazione e trasmissione dei dati sensibili riguardanti la salute
- essere capaci di comunicare efficacemente, in forma scritta e orale, in almeno una lingua dell'Unione Europea, oltre l'italiano, anche con riferimento ai lessici disciplinari
- possedere gli strumenti cognitivi di base per l'aggiornamento continuo delle proprie conoscenze
- essere in grado di lavorare con ampia autonomia, anche assumendo responsabilità di progetti e strutture, ed evidenziando capacità relazionali e decisionali.

I principali sbocchi occupazionali e professionali dei laureati magistrali di questa classe sono negli ambiti della sicurezza di infrastrutture e sistemi informatici e del trattamento di dati sensibili per imprese, aziende di servizi, enti della pubblica amministrazione e, più in generale, per qualunque organizzazione utilizzi sistemi informatici complessi.

Ai fini indicati, i curricula dei corsi di laurea magistrale della classe:
- prevedono lezioni ed esercitazioni di laboratorio oltre ad attività progettuali autonome e attività individuali in laboratorio per non meno di 10 crediti;

- prevedono, in relazione a obiettivi specifici, attività esterne come tirocini formativi presso aziende, strutture della pubblica amministrazione e laboratori, oltre a soggiorni di studio presso altre università italiane ed europee, anche nel quadro di accordi internazionali.

In considerazione della valenza sia scientifica che professionalizzante di questo percorso formativo, 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 propedeutici a quelli di almeno uno degli ambiti disciplinari caratterizzanti l'ordinamento della presente classe di laurea magistrale.

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

La progettazione del nuovo corso di Laurea in Cybersecurity è stata realizzata consultando le organizzazioni rappresentative del mondo della produzione, dei servizi e delle professioni, nonché rappresentanti del mondo socio-economico.
Inizialmente, per la redazione del progetto formativo sono stati consultati il personale docente e ricercatore e i rappresentanti degli studenti (nei Consigli di Collegio di Ingegneria Informatica, del Cinema e Meccatronica e di Dipartimento di Automatica e Informatica). Una prima bozza di progetto formativa è stata sottoposta e approvata dagli Organi di Governo dell'Ateneo.
In una seconda fase vi sono stati numerosi colloqui con aziende ed enti, dove sono stati illustrati gli obiettivi formativi specifici del corso di studio, le modalità di accesso, la struttura e i contenuti del percorso formativo e le figure professionali che verranno create. Tra le aziende ed enti nazionali e internazionali consultati vi sono: AizoOn, Aruba, Banca Generali, Blue Reply, CERT-GARR, Compagnia San Paolo, CSI Piemonte, Hewlett Packard Enterprise, Intesa San Paolo, Law Firm, Punch Italia, Spike Reply, Telsy, Tiesse Informatica e 7 Layers.
Durante gli scambi avuti con le parti interessate, sono emersi ampi consensi sull'offerta formativa e sulle tipologie di figure professionali che il corso di laurea magistrale mira a formare. Inoltre, in base a queste analisi, sono emerse le potenzialità di diverse opportunità occupazionali in ambito industriale, nel settore pubblico e nel settore dei servizi (sicurezza industriale e consulenze professionali). Tutte le riflessioni emerse in questi incontri sono state attentamente valutate ed alcune di queste sono state integrate fin da subito nella progettazione del corso di laurea magistrale, altre saranno integrate nei prossimi anni in base all'evoluzione del CdS, come riportato nel documento di consultazione delle parti interessate. Ad esempio, in base alle riflessioni emerse, verranno attivati seminari tenuti da esperti di settore che si integreranno agli insegnamenti specialistici. In questi seminari verranno presentate le problematiche e l'attuazione della cybersecurity in contesti specifici come ad esempio in scenari di tipo bancario, automotive e industriale. Verrà, inoltre, valutato se potenziare le competenze relative alla sicurezza delle tecniche di intelligenza artificiale.

Oltre alle attività di consultazione descritte in precedenza, dal 28 novembre al 12 dicembre 2022 si è svolta la Consulta di Ateneo, a cui sono stati invitati circa 60 rappresentanti di organizzazioni della produzione, dei servizi, delle professioni e della cultura; aziende di respiro locale, nazionale ma anche internazionale. Sono stati illustrati gli obiettivi formativi specifici e le modalità di accesso al corso di studio, la struttura e i contenuti del percorso formativo proposto, i profili professionali formati e i relativi sbocchi occupazionali. Sono emersi ampi consensi rispetto al progetto culturale e formativo del CdS e alle figure professionali che esso intende formare.

Per rendere strutturato e costante il dialogo e lo scambio di opinioni e esigenze formative con le parti interessate alla formazione delle figure professionali operanti nell'ambito della sicurezza informatica, verrà costituito un Comitato di Consultazione a livello di Collegio seguendo le Linee Guida fornite dal Presidio Qualità dell'Ateneo. Il Comitato di Consultazione fornirà indicazioni sull'allineamento tra domanda e offerta formativa. Tali indicazioni permetteranno di adeguare il percorso didattico alle esigenze culturali e produttive del mondo del lavoro nazionale e internazionale. Il Comitato di Consultazione costituirà gruppi di lavoro tematici specifici per ogni corso di studi. Si prevede di convocare una riunione annuale del Comitato di Consultazione e una o due riunioni annuali per ogni gruppo di lavoro tematico.

Per quanto concerne il CdS, saranno invitati a partecipare al Comitato di Consultazione un rappresentante di AizoOn, Aruba, Blue Reply, CERT-GARR, CSI Piemonte, Hewlett Packard Enterprise, Intesa San Paolo, Spike Reply, Telsy e Tiesse Informatica.
Si prevede di convocare la prima riunione del Comitato di Consultazione entro la fine dell'anno 2022.

Vedi allegato

Sintesi del parere del comitato regionale di coordinamento

Premesso che i sistemi cyber-fisici sono diventati onnipresenti e pervasivi nella società moderna e i dispositivi e ambienti utilizzati, sono sempre più intelligenti, interconnessi, dinamici, e flessibili, gli esperti di cybersecurity devono avere una preparazione cha sia al contempo dettagliata e specialistica, ma anche olistica e trasversale. Pertanto, è emersa l'esigenza di erogare un nuovo corso di Laurea Magistrale al fine di integrare competenze interdisciplinari in campo giuridico-economico a solide basi di tipo tecnologico nel campo dell'Ingegneria Informatica in ambiti software, hardware e delle reti di calcolatori per costruire figure professionali esperte nella sicurezza informatica.

Il Co.Re.Co. preso atto delle motivazioni, ovvero di decongestionare il corso di laurea magistrale in ingegneria informatica si è optato per uno spin-off e di separare il corso di laurea istituendo un corso di laurea magistrale in cybersecurity, delle opportunità formative previste dal corso di studio, nonché delle diverse opportunità occupazionali in ambito industriale, nel settore pubblico e nel settore dei servizi (sicurezza industriale e consulenze professionali) espresse dalle parti sociali consultate e dalle organizzazioni rappresentative a livello locale della produzione dei servizi e delle professioni, esprime, all'unanimità, parere favorevole all'attivazione del Corso di Laurea Magistrale "Cybersecurity" interclasse LM-32 e LM-66, a partire dall'a.a. 2023/2024.

Vedi allegato

Obiettivi formativi specifici del corso e descrizione del percorso formativo

Oggigiorno i sistemi cyber-fisici sono diventati onnipresenti e pervasivi nella società moderna e i dispositivi e ambienti utilizzati, sono sempre più intelligenti, interconnessi, dinamici, e flessibili. Allo stesso tempo crescono sempre più le minacce informatiche e gli obblighi ed omologazioni che ogni azienda, ente o Stato devono rispettare ed implementare per non essere soggette ad attacchi e minacce di tipo informatico.
In questo scenario, gli esperti di cybersecurity devono avere una preparazione cha sia al contempo dettagliata e specialistica, ma anche olistica e trasversale. Gli esperti di cybersecurity, infatti oltre ad avere solide basi scientifiche e tecnologiche, devono avere nel loro curriculum anche competenze legali in ambito civile (ad es. per la gestione della normativa europea sulla privacy, GDPR), penale (ad es. per svolgere correttamente analisi forensi) e di economia aziendale (ad es. per gestire in maniera appropriata ed economicamente consapevole il rischio informatico). La scelta di erogare un nuovo corso di Laurea Magistrale è dunque motivata dall'esigenza di integrare competenze interdisciplinari in campo giuridico-economico a solide basi di tipo tecnologico nel campo dell'Ingegneria Informatica in ambiti software, hardware e delle reti di calcolatori per costruire figure professionali esperte nella sicurezza informatica. Per formare figure professionali che possano operare nel contesto della Cybersecurity, il CdLM in Cybersecurity sarà un corso di laurea magistrale di tipo interclasse e coprirà gli obiettivi formativi sia della classe di laurea magistrale in ingegneria informatica (LM-32) sia di quella in sicurezza informatica (LM-66).

Il Corso di Laurea Magistrale in Cybersecurity rispecchia pienamente gli obiettivi formativi qualificanti la classe di Laurea Magistrale in Sicurezza Informatica (LM-66) attraverso le attività formative caratterizzanti nei seguenti ambiti:
• scientifico: attraverso lo studio approfondito della crittografia moderna e delle prossime sfide che porterà l'avvento del quantum computing
• tecnologico: attraverso la conoscenza approfondita delle metodologie e degli strumenti tecnologici attraverso i quali si progettano, realizzano, verificano e mantengono infrastrutture e sistemi informatici sicuri e protetti
• giuridico, sociale ed economico: fondamentale per poter applicare e rispettare le leggi e i regolamenti di riferimento sulla privacy e sulla protezione dei dati della cybersecurity nazionale, europea e internazionale e per poter conoscere i modelli per il management della cybersecurity e stabilire piani aziendali efficaci.

Nello stesso tempo, per poter gestire la sicurezza di sistemi informatici complessi risulta fondamentale conoscere aspetti avanzati di tipo tecnologico nel campo dell'ingegneria informatica (ambito disciplinare caratterizzante la classe di laurea magistrale LM-32) e in particolare:
• la conoscenza delle reti dei calcolatori, i sistemi cloud e le infrastrutture web
• la conoscenza delle architetture dei calcolatori e dei sistemi embedded ed IoT.

• la conoscenza dei sistemi di comunicazione wireless, bluetooth, cellulari
• la conoscenza dei sistemi software e le vari tecniche di programmazione.

Ciascuno studente deve indicare al momento dell'immatricolazione la classe entro cui intende conseguire il titolo di studio. Lo studente può comunque modificare la sua scelta, purché questa diventi definitiva al momento dell'iscrizione al secondo anno.

Nello specifico, il percorso formativo del CdLM in Cybersecurity ambisce ad allinearsi ai più importanti standard internazionali e ad essere compatibile con il framework di competenze proposto dall'ENISA ("Cybersecurity Skills Development in the EU"). In particolare, uno degli obiettivi principali è rendere tale CdLM una tra le prime implementazioni del piano di formazione sviluppato dall' European Cybersecurity Organisation (European Cybersecurity Education and Professional Training: Minimum Reference Curriculum", https://www.ecs-org.eu/documents/publications/61967913d3f81.pdf). Il CdLM si propone infatti di fornire agli studenti le competenze indispensabili a coprire tutte le fasi della cybersecurity (identificazione, protezione, monitoraggio, risposta e recupero).

Sebbene il corso interclasse si configura comunque come un unico corso, il percorso formativo prevede quattro diversi orientamenti associati alle figure professionali che il CdLM intende formare: Cyber Analyst, Cyber Designer, Cryptography expert e Cyber Legal and Compliance Officer.

Il primo anno del percorso formativo sarà comune a tutti gli orientamenti, mentre nel secondo anno lo studente potrà caratterizza la propria formazione mediante la scelta di un insieme di insegnamenti affini ad uno specifico orientamento. Gli insegnamenti obbligatori del primo anno ritenuti cardine per la figura di esperti di cybersecurity sono relativi ai settori dell'architettura degli elaboratori e della programmazione di sistema, di tecnologie e servizi di rete, della programmazione web, dei fondamenti di sicurezza informatica, della crittografia, della sicurezza del hardware e le comunicazioni wireless.

Relativamente all'orientamento Cyber Analyst la formazione verrà completata con insegnamenti che curano gli aspetti relativi alla identificazione, gestione e mitigazione degli attacchi informatici. Per quanto riguarda l'orientamento Cyber Designer la formazione è orientata a insegnamenti relativi alla progettazione, coordinamento, supervisione e implementazione di misure e tecnologie di protezione. L'orientamento Cryptography expert propone gli aspetti legati alla crittografia moderna, meccanismi e algoritmi che garantiscano le proprietà di sicurezza anche anche dopo l'avvento della transizione quantistica. L'orientamento di Cyber Legal and Compliance Officer si occupa di approfondire le conoscenze degli aspetti legali e gestionali con il compito di gestire e valutare la conformità delle soluzioni di sicurezza, esistenti o in fase di realizzazione, con gli standard esistenti, quadri legali e aspetti normativi.

La formazione magistrale si conclude con la preparazione e discussione di una tesi scritta e con la possibilità di svolgere un tirocinio presso aziende o enti di ricerca o pubbliche amministrazioni.

Si prevede di instaurare accordi con università estere che consentano di ottenere doppio titolo o titolo congiunto.

Gli obiettivi formativi ed i risultati di apprendimento attesi descritti forniscono al laureato gli strumenti sia per un inserimento diretto nel mondo del lavoro nel campo Cybersecurity, sia per la prosecuzione degli studi nell'ambito di un Corso di Dottorato di Ricerca.

Descrizione sintetica delle attività affini e integrative

Le figure professionali formate devono avere la capacità di contestualizzare le proprie competenze nei molteplici ambiti in cui la cybersecurity trova applicazione. Risultano quindi fondamentali competenze eterogenee, parte delle quali da acquisirsi tramite attività affini e integrative. Gli studenti/studentesse, oltre ad avere solide basi scientifiche e tecnologiche, tramite le attività affini e integrative, acquisiscono nel loro curriculum competenze in ambito elettronico e delle telecomunicazioni, fondamentali per la progettazione, la realizzazione, la verifica e la manutenzione di infrastrutture e sistemi informatici sicuri e protetti.
Gli studenti e le studentesse completeranno la loro formazione in attività affini e integrative attraverso lo studio di specifici ambiti tecnologici propri dell'informatica (ad es. nel campo dell'intelligenza artificiale o dell'ingegneria del software o dell'analisi dei dati) che costituiranno il campo applicativo su cui sperimentare le problematiche di sicurezza informatica.

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)

Le conoscenze e competenze attese riguarderanno i diversi aspetti che caratterizzano la cybersecurity. Esse includono la conoscenza della sicurezza dei sistemi informativi ed in particolare la sicurezza delle reti e dei sistemi cloud, la sicurezza dei sistemi hardware ed embedded, la sicurezza delle comunicazioni wireless e device-to-device, dei protocolli e delle metodologie della crittografia moderna, della conoscenza delle metodologie usate per la security verification e per il vulnerability assessment, della conoscenza dei regolamenti nazionali e internazionali relativi alla cybersecurity e GDPR (General Data Protection Regulation), Computer Forensics e analisi del Cyber Crime.
Ogni studente/studentessa avrà l'opportunità di scegliere un orientamento del percorso di studi che gli permetterà di ampliare le proprie conoscenze in settori specifici della cybersecurity. Nello specifico, nell'orientamento Cyber Analyst verranno arricchite le conoscenze relative all'analisi ed il monitoring della sicurezza dei sistemi informativi; nell'orientamento Cyber Designer le conoscenze relative alla progettazione di sistemi sicuri; nell'orientamento Cryptography expert le conoscenze relative alla crittografia moderna e post-quantum; nell'orientamento Cyber Legal and Compliance Officer le conoscenze relative alla compliance con le regolamentazioni nazionali e internazionali generali e di settore nel contesto della cybersecurity.

Modalità didattiche
Queste conoscenze sono acquisite dagli studenti attraverso lezioni frontali, esercitazioni in aula e in laboratori informatici e di tipo sperimentale. Nella maggior parte degli insegnamenti sono anche presenti altre attività, condotte in modo autonomo da ciascuno studente o da gruppi di lavoro assistiti dai docenti e organizzati con specifici obiettivi che prevedano di approfondire ambiti relativi alla cybersecurity o effettuare analisi dello stato dell'arte. Ogni insegnamento indica quanti crediti sono riservati a ciascuna modalità didattica.

Modalità di accertamento
L'accertamento delle conoscenze e competenze di comprensione avviene tramite esami scritti e orali, che comprendono quesiti relativi agli aspetti teorici ed applicativi e tramite la discussione dei risultati delle attività autonome singole o di gruppo. Si richiede la capacità di integrare le conoscenze acquisite in insegnamenti e contesti diversi e la capacità di valutare criticamente e scegliere modelli e metodi di soluzione.

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

Al termine del percorso di studi, lo studente sarà in grado di applicare le conoscenze e competenze acquisite nei vari ambiti della cybersecurity a diversi contesti, fondendole grazie ad un'intensa attività sperimentale e di laboratorio. Ad esempio, saprà progettare e valutare la sicurezza di un sistema informatico, evidenziarne potenziali vulnerabilità e fattori di rischio. Saprà gestire le fasi di risposta ad un attacco informatico. Sarà in grado progettare ed implementare la sicurezza di una rete distribuita attraverso i principali dispostivi di protezione, determinare quando le primitive crittografiche vengono utilizzate in modo improprio in librerie software. Saprà inoltre valutare la conformità delle soluzioni e strategie di sicurezza rispetto ai riferimenti giuridici e tecnici.
Con riferimento specifico agli orientamenti: lo studente iscritto all'orientamento Cyber Analyst saprà analizzare e monitorare il traffico di una rete attraverso tecniche di Intelligenza Artificiale; lo studente iscritto all'orientamento Cyber Designer saprà progettare sistemi informativi complessi e di grandi dimensioni, sfruttando tecniche avanzate di data protection e metodi per salvaguardare la privacy e anonymity di utenti e/o aziende; lo studente iscritto all'orientamento Cryptography expert saprà analizzare e sviluppare protocolli e meccanismi crittografici e di comunicazione avanzati; lo studente iscritto all'orientamento Cyber Legal and Compliance Officer saprà valutare soluzioni e strategie di sicurezza adottate rispetto a requisiti legali, standard di riferimento o contratti aziendali.

Modalità didattiche
La capacità di applicare conoscenze e comprensione sono acquisite dallo studente tramite la progettazione guidata di progetti di sistemi di protezione, dispositivi di sicurezza integrati hardware e software, analisi di vulnerabilità e esecuzione di attacchi contro specifici sistemi. Le lezioni in aula sono dedicate all'approfondimento di aspetti teorici, mentre le esercitazioni in aula sono propedeutiche alle attività progettuali. Le attività in laboratorio sono

finalizzate alla sperimentazione pratica delle metodologie di progettazione introdotte in aula. È stimolata l'applicazione integrata di conoscenze acquisite in differenti insegnamenti o in modo autonomo.

Modalità di accertamento
Gli accertamenti comprendono esami tradizionali (scritti e orali), con quesiti relativi agli aspetti teorici, all'analisi, alla progettazione e alla valutazione di applicazioni della cybersecurity. I quesiti di progetto richiedono la valutazione comparata di diverse scelte ("problem solving"). Viene verificata la capacità di applicare le conoscenze acquisite a problemi nuovi, anche di carattere interdisciplinare. Un accertamento complessivo delle capacità di applicare quanto appreso nei diversi insegnamenti avviene con la elaborazione della tesi di laurea, che richiede l'integrazione di conoscenze acquisite e la capacità di apportare nuovi sviluppi.

Autonomia di giudizio (making judgements)

L'autonomia di giudizio viene esercitata dagli studenti nei momenti in cui viene loro chiesto di sviluppare un progetto. La definizione delle specifiche da sviluppare non è esaustiva, come accade nella realtà, perciò lascia diversi gradi di libertà allo studente che deve essere capace di fare delle scelte personali sulla base di una valutazione delle possibili soluzioni alternative.
Questo approccio è caratteristico di alcuni insegnamenti svolti sia nel primo che nel secondo anno di corso, in particolare nei corsi di network security, di programmazione web, advanced information system security ed in tutti i laboratori sperimentali che caratterizzeranno la quasi totalità di insegnamenti nell'ambito informatico. Infine, la tesi di laurea è, di norma, un momento di sintesi nel quale lo studente è coinvolto nel gruppo di ricerca del proprio relatore di tesi o eventualmente in un contesto aziendale. Lo studente/studentessa deve elaborare ed implementare soluzioni originali su un aspetto di tematiche spesso interdisciplinari.

Abilità comunicative (communication skills)

Le abilità comunicative vengono esercitate e valutate attraverso la specifica stesura di rapporti scritti per documentare gli algoritmi ed i metodi utilizzati nelle esercitazioni di laboratorio e nello sviluppo di progetti.
Queste attività sono svolte spesso all'interno di piccoli gruppi. Ciò permette di sviluppare l'abilità di lavorare in gruppo, di sottoporre il proprio lavoro ad una valutazione esterna e di predisporre presentazioni tecniche con l'uso di slide o altre tecniche di comunicazione.
Alcuni insegnamenti prevedono la presentazione orale dei lavori individuali o di gruppo, come parte della prova di accertamento. Questa attività viene considerata come un esercizio di comunicazione in pubblico.
Il corso di studi favorisce pertanto la crescita della capacità di ricercare, valutare criticamente e comunicare informazioni, idee, problemi e soluzioni, capacità di controllare e verificare le fonti documentarie e di spiegare e documentare le proprie scelte, utilizzando opportunamente i mezzi che la moderna tecnologia informatica mette a disposizione.

Capacità di apprendimento (learning skills)

La capacità di apprendimento viene sviluppata ponendo lo studente nelle condizioni di imparare con la massima resa (o con il minimo sforzo) il materiale proposto in aula, per applicarlo nella fase di esercitazione in aula o in laboratorio e per sviluppare piccoli progetti, sottoponendogli anche del materiale aggiuntivo che deve essere elaborato autonomamente, in vista della prova d'esame e finale. Ciò permette allo studente di sviluppare le sue capacità di apprendere nello studio auto-diretto o autonomo, qualità indispensabile nell'aggiornamento continuo delle proprie conoscenze.

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

Costituiscono requisiti curriculari il titolo di laurea in Ingegneria dell'Informazione (L-8) o in Scienze e Tecnologie informatiche (L-31), o di altro titolo di studio conseguito all'estero, riconosciuto idoneo.

Alternativamente, lo studente deve aver acquisito un minimo di 40 CFU sui seguenti settori scientifico-disciplinari FIS/01, FIS/03, INF/01, ING-INF/05, MAT/02, MAT/03, MAT/05 e 60 CFU sui settori scientifico-disciplinari INF/01, ING-INF/01, ING-INF/03, ING-INF/05, SECS-S/01, MAT/03, MAT/05, MAT/06, MAT/08, MAT/09.

Inoltre, lo studente deve essere in possesso di un'adeguata preparazione personale e della conoscenza certificata della Lingua inglese almeno di livello B2, come definito dal Quadro comune europeo di riferimento per la conoscenza delle lingue (QCER).

Le modalità di verifica dell'adeguatezza della preparazione personale e i criteri per il riconoscimento della conoscenza certificata della lingua inglese sono riportati nel regolamento didattico del corso di studio.

Per gli studenti di madrelingua diversa dall'italiano sarà verificata la conoscenza della lingua italiana. Le modalità di verifica sono definite nel regolamento didattico del CdS, ove sono anche indicate - nei casi di esito negativo di detta verifica - le attività formative da inserire nel piano di studi volte all'acquisizione della conoscenza della lingua italiana richiesta agli studenti per il conseguimento del titolo.

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

Gli studenti potranno svolgere la prova finale scegliendo fra due opzioni: tesi da 22 CFU oppure tirocinio da 10 CFU e tesi da 12 CFU.

La tesi (nelle sue due opzioni da 22 o 12 CFU) ha tipicamente come oggetto un'analisi, un progetto o un'applicazione a carattere innovativo, relativi ad argomenti coerenti con gli obiettivi formativi del corso di studi, nel quale sia riconoscibile il contributo individuale del candidato, e lo sviluppo di un elaborato scritto conclusivo (Tesi di Laurea). Gli insegnamenti del secondo anno sono distribuiti in modo da consentire di dedicare un adeguato periodo allo sviluppo della prova finale.
La tesi di Laurea Magistrale rappresenta una verifica complessiva della padronanza di contenuti tecnici e delle capacità di organizzazione, di comunicazione, e di lavoro individuali, relativamente allo sviluppo di analisi o di progetti complessi. Le attività previste nella prova finale richiedono normalmente l'applicazione di quanto appreso in più insegnamenti, l'integrazione con elementi aggiuntivi e la capacità di proporre spunti innovativi.

Nel caso in cui lo studente/studentessa opti per l'opzione di prova finale costituita da tesi da 12 CFU e tirocinio da 10 CFU, svolge un tirocinio curriculare che permette di arricchire la propria preparazione con un'esperienza condotta nell'ambito di una realtà aziendale o ente di ricerca o pubblica amministrazione. L'ampia gamma di contatti che i Dipartimenti coinvolti hanno con aziende, enti di ricerca nazionali ed internazionali e pubbliche amministrazioni garantisce un'ampia offerta di proposte di tirocinio.

Modalità di assegnazione e dettagli sullo svolgimento della prova finale sono precisati nel regolamento didattico di Corso di Laurea Magistrale.

Motivazioni dell'istituzione del corso interclasse (Decreti sulle Classi, Art. 3, comma 7)

Il Corso di Laurea Magistrale in Cybersecurity si propone di rispondere alla crescente esigenza di formazione di specialisti dotati di elevate competenze nell'ambito della sicurezza informatica. La carenza di esperti in tale ambito rappresenta una seria minaccia per lo sviluppo economico e per la sicurezza nazionale ed europea.
Il corso di Laurea magistrale in Cybersecurity forma professionisti in grado di operare nella progettazione, ingegnerizzazione, sviluppo e gestione della sicurezza informatica di sistemi informativi complessi. Il CdLM in Cybersecurity è una tra le prime implementazioni del piano di formazione proposto dalla European Cybersecurity Organisation. Il percorso formativo del CdLM in Cybersecurity si allinea, dunque, ai più importanti standard e framework

internazionali. Dal punto di vista tecnico, il CdLM si propone di fornire agli studenti le competenze indispensabili a coprire tutte le fasi della cybersecurity evidenziate dal Risk Management Framework del National Institute of Standards and Technology (NIST) (pianificazione, protezione, monitoraggio, risposta e recupero).

La cybersecurity è un dominio complesso che richiede competenze tecnologiche avanzate, ma anche competenze di tipo giuridico, economico e sociale. Al fine di creare figure professionali esperte nella sicurezza informatica, il CdLM fornisce competenze interdisciplinari in campo giuridico-economico e solide basi tecnologiche nel campo dell'Ingegneria Informatica negli ambiti software, hardware e delle reti di calcolatori. Il CdLM è di tipo interclasse, coprendo gli obiettivi formativi sia della classe di laurea magistrale in Ingegneria Informatica (LM-32) sia di quella in Sicurezza Informatica (LM-66).

Il Corso di Laurea Magistrale in Cybersecurity rispecchia pienamente gli obiettivi formativi qualificanti la classe di Laurea Magistrale in Sicurezza Informatica (LM-66) attraverso le attività formative caratterizzanti nei seguenti ambiti:
• scientifico: attraverso lo studio approfondito della crittografia moderna e delle prossime sfide che porterà l'avvento del quantum computing
• tecnologico: attraverso la conoscenza approfondita delle metodologie e degli strumenti tecnologici attraverso i quali si progettano, realizzano, verificano e mantengono infrastrutture e sistemi informatici sicuri e protetti
• giuridico, sociale ed economico: fondamentale per poter applicare e rispettare le leggi e i regolamenti di riferimento sulla privacy e sulla protezione dei dati della cybersecurity nazionale, europea e internazionale e per poter conoscere i modelli per il management della cybersecurity e stabilire piani aziendali efficaci.

Nello stesso tempo, per poter gestire la sicurezza di sistemi informatici complessi risulta fondamentale conoscere aspetti avanzati di tipo tecnologico nel campo dell'ingegneria informatica (ambito disciplinare caratterizzante la classe di laurea magistrale LM-32) e in particolare:
• la conoscenza delle reti dei calcolatori, i sistemi cloud e le infrastrutture web
• la conoscenza delle architetture dei calcolatori e dei sistemi embedded ed IoT.
• la conoscenza dei sistemi di comunicazione wireless, bluetooth, cellulari
• la conoscenza dei sistemi software e le vari tecniche di programmazione.

Sebbene il corso interclasse si configuri comunque come un unico corso, il percorso formativo prevede quattro diversi orientamenti associati alle figure professionali che il CdLM intende formare: Cyber Analyst, Cyber Designer, Cryptography expert e Cyber Legal and Compliance Officer. Il primo anno del percorso formativo sarà comune a tutti gli orientamenti, mentre nel secondo anno lo studente potrà specializzare la propria formazione mediante la scelta di insegnamenti che ne caratterizzeranno il profilo rispetto alle figure professionali identificate.

Sbocchi occupazionali e professionali previsti per i laureati

Cyber Analyst

funzione in un contesto di lavoro:
I Cyber Analyst sono specialisti che operano nella gestione, analisi dell'esposizione ai rischi informatici e delle mitigazioni adottate. Essi monitorano e valutano l'efficacia dello stato di sicurezza dell'organizzazione, identificano le criticità dei sistemi e gli eventuali modi per sfruttarle, garantiscono il normale funzionamento o ripristino delle operazioni e servizi, approfondiscono le cause di un attacco e investigano le motivazioni di un attacco o un reato informatico.

competenze associate alla funzione:
Il Cybersecurity Analyst è una figura poliedrica in grado di fornire un approccio olistico ai problemi di verifica del livello di esposizione ai rischi informatici. Tale figura professionale è in grado: (i) di gestire attacchi e incidenti informatici, sovraintendono alle fasi e le operazioni di un Secure Operation Centre (SOC) e interagendo all'interno di un Computer Security Incident Response Team (CSIRT); (ii) di padroneggiare le principali metodologie e dirigere gli strumenti per la pianificazione, progettazione e implementazione delle attività di verifica delle vulnerabilità e di test di penetrazione oltre; (iii) di simulare attacchi software e hardware, atti a valutare l'efficacia delle misure di sicurezza in essere; (iv) di applicare e sfruttare i metodi, le pratiche e gli strumenti della digital forensics, per investigare le cause e le modalità di un reato informatico.

sbocchi occupazionali:
I Cyber Analyst sono richiesti principalmente da aziende medio-grandi ma anche da aziende di sviluppo o produzione di un prodotto, dalla pubblica amministrazione, enti per la difesa e protezione nazionale o uffici pubblici e privati preposti ad indagare sui crimini informatici.

Cyber Designer

funzione in un contesto di lavoro:
I Cyber Designer sono specialisti che possono operare nella progettazione, revisione e miglioramento degli aspetti di Cybersecurity all'interno di sistemi. Essi possono lavorare anche allo sviluppo, messa in atto e mantenimento delle soluzioni di sicurezza. Essi possono occuparsi di aspetti relativi alla progettazione vera e propria di sistemi sicuri, al coordinamento, implementazione, integrazione e mantenimento della sicurezza.

competenze associate alla funzione:
Progettare le principali soluzioni di sicurezza di un sistema informativo basandosi su requisiti di sicurezza ottenuti da un'analisi puntuale del rischio oltre che su standard e normativa di riferimento. Identificare e valutare i fattori di rischio e potenziali minacce delle proprie infrastrutture, confrontandoli con modelli di riferimento, paradigmi, architetture e tecnologie di sicurezza. Sono in grado di sviluppare, applicare, distribuire, gestire e mantenere le soluzioni di sicurezza informatica (sistemi, risorse, software, controlli e servizi) su infrastrutture e prodotti.

sbocchi occupazionali:
I Cyber Designer sono principalmente richiesti da grandi aziende, aziende di consulenza, aziende di sviluppo software o hardware, pubblica amministrazione, enti per la difesa e protezione nazionale, ma sono anche ricercati da piccole medie imprese che vogliono mitigare la loro esposizione ai rischi.

Cryptography expert

funzione in un contesto di lavoro:
I Cryptography Expert sono esperti in tecniche, meccanismi e sviluppo di dispositivi di protezione ed integrità di dati e comunicazioni. Nello specifico sono in grado di valutare, definire o sviluppare applicazioni e programmi crittografici di base ed avanzati.

competenze associate alla funzione:
Analizzare e sviluppare protocolli e meccanismi crittografici e di comunicazione, anche relativi a tecnologie e argomenti avanzati quali Crittografia Post-Quantum, Blockchain e sue applicazioni, Criptomonete e Token, Crittografia Funzionale e Omomorfica, Crittoanalisi e Zero-knowledge proof.

sbocchi occupazionali:
I Cryptography Expert sono richiesti principalmente da grandi e medie aziende, aziende di consulenza, aziende di sviluppo o produzione di prodotti di cybersecurity, ed enti per la protezione e difesa della sicurezza nazionale.

Cyber Legal and Compliance Officer

funzione in un contesto di lavoro:
I Cyber Legal and Compliance Officer gestiscono e valutano e la conformità delle soluzioni e degli ecosistemi con le leggi e i regolamenti di riferimento sulla privacy e sulla protezione dei dati della cybersecurity nazionale, europea e internazionale.
I Cyber Legal and Compliance Officer sono specialisti in grado di valutare le soluzioni e strategie di sicurezza adottate rispetto a requisiti legali, standard di riferimento o contratti aziendali.
Nello specifico queste figure provvedono a: (i) garantire la conformità e fornire consulenza legale e indicazioni su privacy e standard di protezione dei dati, leggi e regolamenti; (ii) garantire che i titolari dei dati, i responsabili, i soggetti interni o i partner e gli enti esterni siano informati dei loro diritti in materia di protezione dei dati, obblighi e responsabilità; (iii) agire come un punto di contatto chiave fra i reparti tecnici e quelli giuridico-commerciali; (iv) assistere nella progettazione, implementazione, verifica e test di conformità rispetto a standard per la sicurezza informatica e leggi di riferimento; (v) monitorare o predisporre gli audit e le attività di formazione relativi alla protezione dei dati e alla sicurezza aziendale.

competenze associate alla funzione:
I Cyber Legal and Compliance Officer sono specialisti in grado di valutare le soluzioni e strategie di sicurezza adottate rispetto a requisiti legali, standard di riferimento o contratti aziendali. Nello specifico queste figure provvedono a: (i) garantire la conformità e fornire consulenza legale e indicazioni su privacy e standard di protezione dei dati, leggi e regolamenti; (ii) garantire che i titolari dei dati, i responsabili, i soggetti interni o i partner e gli enti esterni siano informati dei loro diritti in materia di protezione dei dati, obblighi e responsabilità; (iii) agire come un punto di contatto chiave fra i reparti tecnici e quelli giuridico-commerciali; (iv) assistere nella progettazione, implementazione, verifica e test di conformità rispetto a standard per la sicurezza informatica e leggi di riferimento; (v) monitorare o predisporre gli audit e le attività di formazione relativi alla protezione dei dati e alla sicurezza aziendale.

sbocchi occupazionali:
I Cyber Legal and Compliance Officer sono richiesti da amministrazioni, enti o uffici privati, aziende di consulenza, aziende di sviluppo di prodotti di grandi, medie e piccole dimensioni.

Il corso prepara alla professione di (codifiche ISTAT)

- Analisti di sistema - (2.1.1.4.2)
- Analisti e progettisti di applicazioni web - (2.1.1.4.3)
- 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

Raggruppamento settori

Gruppo	**Settori**	**CFU**	**LM-32**	**LM-66**
			Attività - ambito	**Attività - ambito**
1	ING-INF/05	18-36	*Carat*Ingegneria informatica	*Carat*Ambito Scientifico
2	ING-INF/05	18-30	*Carat*Ingegneria informatica	*Carat*Ambito Tecnologico
3	IUS/01 , M-PSI/05 , SECS-P/08	12-18	Attività formative affini o integrative	*Carat*Ambito Giuridico, Sociale ed Economico
4	ING-INF/03 , ING-INF/05 , MAT/03	20-40	Attività formative affini o integrative	Attività formative affini o integrative
Totale crediti		68 - 124		

Riepilogo crediti

LM-32 Ingegneria informatica			
Attività	**Ambito**	**Crediti**	
Carat	Ingegneria informatica	36	66
Attività formative affini o integrative		32	58
Minimo CFU da D.M. per le attività caratterizzanti **45** Minimo crediti assegnati dall'ateneo per le attività caratterizzanti **48** Somma crediti minimi ambiti caratterizzanti **36**			
Minimo CFU da D.M. per le attività affini **12** Somma crediti minimi ambiti affini **32**			
Totale		68	124

LM-66 Sicurezza informatica			
Attività	**Ambito**	**Crediti**	
Carat	Ambito Giuridico, Sociale ed Economico	12	18
Carat	Ambito Scientifico	18	36
Carat	Ambito Tecnologico	18	30
Attività formative affini o integrative		20	40
Minimo CFU da D.M. per le attività caratterizzanti **48** Minimo crediti assegnati dall'ateneo per le attività caratterizzanti **48** Somma crediti minimi ambiti caratterizzanti **48**			
Minimo CFU da D.M. per le attività affini **12** Somma crediti minimi ambiti affini **20**			
Totale		68	124

Attività caratterizzanti

LM-32 Ingegneria informatica

ambito disciplinare	settore	CFU
Ingegneria informatica	ING-INF/05 Sistemi di elaborazione delle informazioni	36 - 66
Minimo di crediti riservati dall'ateneo minimo da D.M. 45:		48
Totale per la classe		36 - 66

LM-66 Sicurezza informatica

ambito disciplinare	settore	CFU
Ambito Scientifico	ING-INF/05 Sistemi di elaborazione delle informazioni	18 - 36 cfumin 18
Ambito Tecnologico	ING-INF/05 Sistemi di elaborazione delle informazioni	18 - 30 cfumin 18
Ambito Giuridico, Sociale ed Economico	IUS/01 Diritto privato M-PSI/05 Psicologia sociale SECS-P/08 Economia e gestione delle imprese	12 - 18 cfumin 12
Minimo di crediti riservati dall'ateneo minimo da D.M. 48:		48
Totale per la classe		48 - 84

Attività affini

LM-32 Ingegneria informatica

ambito disciplinare	CFU min	CFU max
Attività formative affini o integrative	32 - 58 cfumin 12	
Totale per la classe	32 - 58	

LM-66 Sicurezza informatica

ambito disciplinare	CFU min	CFU max
Attività formative affini o integrative	20 - 40 cfumin 12	
Totale per la classe	20 - 40	

Altre attività

ambito disciplinare		CFU min	CFU max
A scelta dello studente		8	16
Per la prova finale		12	22
Ulteriori attività formative (art. 10, comma 5, lettera d)	Ulteriori conoscenze linguistiche	0	6
	Abilità informatiche e telematiche	-	-
	Tirocini formativi e di orientamento	0	10
	Altre conoscenze utili per l'inserimento nel mondo del lavoro	-	-
Minimo di crediti riservati dall'ateneo alle Attività art. 10, comma 5 lett. d		4	
Per stages e tirocini presso imprese, enti pubblici o privati, ordini professionali		0	10

Totale Altre Attività	24 - 64

Riepilogo CFU

CFU totali per il conseguimento del titolo	**120**
Range CFU totali per la classe LM-32 **Range CFU totali per la classe LM-66**	92 - 188 92 - 188

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

Note relative alle altre attività

Note relative alle attività caratterizzanti

RAD chiuso il 13/02/2023