Politecnico di Torino

REGOLAMENTO DIDATTICO

Corso di laurea magistrale
in
CYBERSECURITY

Dipartimento di Automatica e Informatica
Collegio di Ingegneria Informatica, del Cinema e Meccatronica

Anno accademico **2023/2024**

Emanato con D.R. n. 862/2023 del 06/09/2023

INDICE

Art. 1 - Obiettivi formativi specifici e sbocchi occupazionali

1.1 Obiettivi formativi specifici

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

1.2 Sbocchi occupazionali e professionali

Di seguito sono riportati i profili professionali che il Corso di Studio intende formare e le principali competenze della figura professionale.

Il profilo professionale che il CdS intende formare	Principali funzioni e competenze della figura professionale
	FUNZIONE IN UN CONTESTO DI LAVORO:

Cyber Analyst	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 PROFESSIONALI: 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 PROFESSIONALI:

	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 PROFESSIONALI: 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 PROFESSIONALI: 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.

1.3 Profili professionali (Codifiche ISTAT)

Con riferimento agli sbocchi occupazionali classificati dall'ISTAT, un laureato di questo Corso di Studio può intraprendere la professione di:

Codice ISTAT	Descrizione
2.1.1.4.2	Analisti di sistema
2.1.1.4.3	Analisti e progettisti di applicazioni web
2.1.1.5.1	Specialisti in reti e comunicazioni informatiche
2.1.1.5.4	Specialisti in sicurezza informatica

Art. 2 - Requisiti di ammissione al Corso di Studio

Le norme nazionali relative all'immatricolazione ai corsi di Laurea magistrale prevedono che gli Atenei verifichino il possesso:

- della **Laurea triennale o del diploma universitario di durata triennale**, ovvero di **altro titolo di studio conseguito all'estero**, riconosciuto idoneo;
- dei **requisiti curriculari**;
- dell'**adeguatezza della personale preparazione**.

REQUISITI CURRICULARI

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.

Relativamente ai requisiti curriculari, questi si intendono automaticamente soddisfatti per gli studenti in possesso di una laurea triennale nella classe L-8 o L-31. In tutti gli altri casi le domande di ammissione saranno sottoposte alla valutazione del Referente del Corso di Studio, o suo delegato, che potrà individuare, motivandole, eventuali equivalenze di crediti di settori scientifico disciplinari differenti da quelli previsti dal presente regolamento.

I crediti formativi dei settori scientifico-disciplinari, presenti sia nel primo gruppo che nel secondo, vengono conteggiati prioritariamente per soddisfare il requisito del primo gruppo. I crediti residui vengono considerati per il raggiungimento del requisito del secondo gruppo. I crediti di un insegnamento possono quindi essere considerati per soddisfare il numero minimo di crediti di entrambi i gruppi. Nel limite di 10 CFU, il Referente del Corso di Studio potrà ammettere il candidato; se il numero di crediti mancanti è superiore a 10 CFU, la valutazione sarà sottoposta all'approvazione finale del Coordinatore del Collegio o del Vice Coordinatore di Collegio.

Nel caso in cui i requisiti curriculari non risultino soddisfatti, l'integrazione curriculare, in termini di crediti, dovrà essere colmata prima dell'immatricolazione al corso di laurea magistrale effettuando:

- un'**iscrizione ai singoli insegnamenti per integrazione curriculare**, nel caso in cui l'integrazione sia inferiore o uguale a 60 crediti. Si precisa che, nel caso di Iscrizione ai singoli insegnamenti per integrazione curriculare, sarà possibile inserire nel carico didattico esclusivamente gli insegnamenti assegnati dal valutatore a titolo di carenza formativa;

oppure

- un'**abbreviazione di carriera su un corso di laurea di I livello**, nel caso in cui l'integrazione curriculare da effettuare sia superiore a 60 crediti. Il candidato dovrà valutare l'iscrizione al corso di laurea di I livello con i crediti formativi nei settori di base e caratterizzanti o affini richiesti per l'accesso al corso di Laurea Magistrale di interesse considerando le scadenze stabilite.

ADEGUATEZZA DELLA PERSONALE PREPARAZIONE

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). Per gli studenti di madrelingua diversa dall'italiano sarà verificata la conoscenza della lingua italiana almeno di livello A2 (QCER) o attraverso un esame organizzato internamente all'Ateneo o attraverso il conseguimento di una certificazione internazionale di lingua italiana. Le modalità per inserire tali attività formative nel piano di studi sono riportate nella Guida dello studente.

Le modalità di verifica dell'adeguatezza della personale preparazione sono le seguenti:

1) Per i candidati del Politecnico di Torino

Sono ammessi i candidati per i quali:

- la durata del percorso formativo è inferiore o uguale a 4 anni (1) indipendentemente dalla media;
- la durata del percorso formativo è superiore a 4 anni ma inferiore o uguale a 5 anni (1) e la media ponderata (2) degli esami è superiore o uguale a 21/30
- la durata del percorso formativo è superiore a 5 anni e la media ponderata (2) degli esami è superiore o uguale a 24/30.

La media ponderata è calcolata su tutti i crediti con voto in trentesimi acquisiti e utili per il conseguimento della laurea di primo livello con l'esclusione dei peggiori 28 crediti.
La durata del percorso formativo di ciascuno studente è valutata in base al numero di anni accademici di iscrizione a partire dalla prima immatricolazione al sistema universitario italiano: per gli studenti iscritti full-time la durata coincide con il numero di anni accademici di iscrizione, mentre per gli studenti part-time, la durata viene valutata considerando mezzo anno di iscrizione per ogni iscrizione annuale part-time. Per gli studenti iscritti full-time, afferenti al programma "Dual Career", la durata viene valutata, come per i part-time, considerando mezzo anno di iscrizione per ogni iscrizione annuale.
In caso di abbreviazione di carriera il calcolo degli anni deve essere aumentato in proporzione al numero di CFU convalidati (10-60 CFU =1 anno, ecc). I 28 CFU peggiori devono essere scorporati in proporzione al numero di CFU convalidati.

(1) l'ultima sessione utile per rispettare il requisito di media è la sessione di laurea di dicembre.
(2) la media ponderata è ottenuta dalla sommatoria (voti x crediti) / sommatoria dei crediti.

2) Per i candidati di altri Atenei italiani

Per gli studenti che hanno conseguito una Laurea triennale presso altri Atenei è richiesta la media ponderata ai crediti uguale o maggiore a 24/30 indipendentemente dal periodo occorso per conseguire il titolo. La media ponderata (sommatoria (voti x crediti) / sommatoria dei crediti) è calcolata su tutti i crediti con voto in trentesimi acquisiti e utili per il conseguimento della laurea di primo livello con l'esclusione dei peggiori 28 crediti.

3) Per i candidati in possesso di titolo di studio conseguito all'estero

Per essere ammessi ai corsi di Laurea Magistrale è necessario essere in possesso di un titolo accademico rilasciato da una Università straniera accreditata/riconosciuta, conseguito al termine di un percorso scolastico complessivo di almeno 15 anni (comprendente scuola primaria, secondaria ed università).
Coloro che hanno intrapreso un percorso universitario strutturato in cinque o sei anni accademici (diverso dal sistema 3+2) e non lo abbiano completato, per essere ammessi, devono comunque soddisfare il requisito minimo dei 15 anni di percorso complessivo (di cui minimo 3 anni a livello universitario) e aver superato 180 crediti ECTS o equivalenti(i corsi pre-universitari o gli anni preparatori non possono essere conteggiati per il raggiungimento dei crediti minimi o degli anni di scolarità sopra indicati) .
L'adeguatezza della personale preparazione e la coerenza tra i Corsi di Studio dell'Ateneo prescelti dai candidati e la loro carriera universitaria pregressa viene verificata dai docenti dello specifico CdS individuati dai Coordinatori del Collegi che valutano le domande sulla piattaforma Apply "candidati con qualifica estera".
La valutazione positiva consente l'immatricolazione unicamente nell'anno accademico per il quale la si è ottenuta. Qualora il candidato ammesso alla Laurea Magistrale non proceda - secondo le scadenze prestabilite - all'immatricolazione nell'anno accademico per il quale ha ottenuto l'ammissione - dovrà ricandidarsi e sottoporsi nuovamente a valutazione per accedere e immatricolarsi in anni accademici successivi.

***
Ulteriori informazioni possono essere reperite alla

pagina https://www.polito.it/didattica/iscriversi-studiare-laurearsi/iscrizione/corsi-di-laurea-magistrale

Art. 3 - Piano degli Studi

3.1 Descrizione del percorso formativo

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.

3.2 Attività formative programmate ed erogate

L'elenco degli insegnamenti (obbligatori e a scelta), i curricula formativi, l'eventuale articolazione in moduli, eventuali propedeuticità ed esclusioni e i docenti titolari degli insegnamenti sono consultabili alla pagina: https://didattica.polito.it/pls/portal30/sviluppo.offerta_formativa_2019.vis?p_coorte=2024&p_sdu=32&p_cds=138

L'elenco dei Settori Scientifico Disciplinari per tipo di attività formativa (caratterizzanti e affini) previsti nell'ordinamento didattico del Corso di Studio è consultabile alla pagina: https://didattica.polito.it/pls/portal30/sviluppo.vis_aiq_2022.visualizza?sducds=32138&tab=0&p_a_acc=2024

Art. 4 - Gestione della Carriera

La Guida dello studente è pubblicata annualmente sul Portale della Didattica prima dell'inizio dell'anno accademico. È organizzata per singolo Corso di Studio e reperibile dal sito del Corso di Studio.

Contiene, a titolo esemplificativo, informazioni e scadenze relative a:

- calendario accademico;
- piano carriera e carico didattico;
- crediti liberi;
- formazione linguistica;
- studiare all'estero/programmi di mobilità;
- regole per il sostenimento degli esami;
- abbreviazione carriera;
- interruzione, rinuncia e sospensione degli studi;
- trasferimenti in entrata e in uscita e passaggi interni;
- decadenza.

Art. 5 - Prova finale

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.

La prova finale ha un valore pari a 12 oppure 22 crediti, corrispondenti a un periodo di tempo che va da circa un trimestre a un semestre di lavoro a tempo pieno.

L'argomento e le attività relative alla prova finale sono concordati con un docente del Politecnico (relatore di Tesi). Le attività possono essere condotte anche presso altri enti o aziende, in Italia o all'estero, sotto la supervisione di un docente relatore del Politecnico e di un tutore dell'ente esterno.
Gli studenti che abbiano conseguito almeno 48 crediti devono fare la richiesta dell'argomento della tesi in modalità on-line attraverso un'apposita procedura disponibile nella propria pagina personale del portale della didattica nella sezione denominata 'Tesi', rispettando le scadenze per la sessione di interesse pubblicate nella Guida dello Studente – Sezione Calendario Tematico.
Le attività relative alla preparazione della Tesi di Laurea e i relativi risultati devono essere presentati e discussi pubblicamente, in presenza di una commissione di docenti che esprime una valutazione del lavoro svolto e della presentazione. La tesi di Laurea e la presentazione devono essere in lingua inglese. Le commissioni preposte alle prove finali esprimono i propri giudizi tenendo conto dell'intero percorso di studi dello studente, valutandone la maturità culturale e la capacità di elaborazione intellettuale personale, nonché la qualità del lavoro.

La determinazione del voto finale è assegnata alla commissione di laurea che prenderà in esame la media complessiva degli esami su base 110. A tale media la commissione potrà sommare, di norma, sino ad un massimo di 8 punti prendendo in considerazione:
• la valutazione del lavoro svolto per la tesi (impegno, autonomia, rigore metodologico, rilevanza dei risultati raggiunti etc.);
• la presentazione della tesi (chiarezza espositiva etc.);
• l'eccellenza del percorso di studi (ad esempio, il numero delle lodi conseguite, il tempo impiegato per terminare gli studi etc.).

La lode potrà essere assegnata al raggiungimento del punteggio complessivo 112,51 a discrezione della commissione.
Se la tesi ha le caratteristiche necessarie, può essere concessa la dignità di stampa soltanto qualora il voto finale sia centodieci e lode e il parere della commissione sia unanime.

Ulteriori informazioni e scadenze si trovano nel Regolamento studenti e nella Guida dello Studente.

Rilascio del Diploma Supplement:
Come previsto dall'art. 11, comma 8 dei D.D.M.M. 509/1999 e 270/2004, il Politecnico di Torino rilascia il Diploma Supplement, una relazione informativa che integra il titolo di studio conseguito, con lo scopo di migliorare la trasparenza internazionale dei titoli attraverso la descrizione del curriculum degli studi effettivamente seguito. Tale certificazione, conforme ad un modello europeo sviluppato per iniziativa della Commissione Europea, del Consiglio d'Europa e dell'UNESCO – CEPES, viene rilasciata in edizione bilingue (italiano-inglese) ed è costituita da circa dieci pagine.
Maggiori informazioni al link:
https://didattica.polito.it/certificati_autocertificazioni/it/diploma_supplement

Art. 6 - Rinvii

6.1 Regolamento Studenti

Il Regolamento Studenti disciplina diritti e doveri dello studente e contiene le regole amministrative e disciplinari alla cui osservanza sono tenuti tutti gli studenti iscritti ai Corsi di studio o a singole attività formative dell'Ateneo.

6.2 Altri Regolamenti

Aspetti particolari relativi alla carriera degli studenti sono disciplinati con appositi Regolamenti o Bandi pubblicati sul sito di Ateneo.

In particolare si ricordano:

- il Regolamento Tasse contiene gli importi delle tasse da versare annualmente. La procedura per chiedere la riduzione delle tasse è spiegata in un'apposita guida;
- il Regolamento di Ateneo per l'erogazione di contributi finalizzati al sostegno e all'incremento della mobilità studentesca verso l'estero contiene i principi e le regole per l'attribuzione e l'erogazione delle borse di mobilità. Le modalità di gestione di tutte le tipologie di mobilità sono quanto più possibile uniformate attraverso l'emanazione di bandi di concorso unitari, pubblicati due volte all'anno nella sezione dedicata del sito https://www.polito.it/didattica/iscriversi-studiare-laurearsi/studiare-all-estero;
- il Codice etico per quanto espressamente riferito anche agli studenti.