



UNIVERSITA' DEGLI STUDI DI MILANO
MANIFESTO DEGLI STUDI A.A. 2026/27
LAUREA MAGISTRALE IN
SICUREZZA INFORMATICA (Classer LM-66 R)
Immatricolati nell'a.a. 2026/2027

GENERALITA'

Classe di laurea di appartenenza:	LM-66 R Sicurezza informatica
Titolo rilasciato:	Dottore Magistrale
Durata del corso di studi:	2 anni
Crediti richiesti per l'accesso:	180
Cfu da acquisire totali:	120
Annualità attivate:	1°
Modalità accesso:	Libero con valutazione dei requisiti di accesso
Codice corso di studi:	FBB

RIFERIMENTI

Presidente Collegio Didattico

Prof.ssa Sabrina Gaito

Coordinatore Corso di Laurea

Prof.ssa Pierangela Samarati

Docenti tutor

TUTOR PER L'ORIENTAMENTO:

Stelvio Cimato

Fabio Scotti

Sito web del corso di laurea

<https://sicurezzainformatica.cdl.unimi.it/>

Commissione Ammissioni alle Lauree Magistrali

Via Celoria 18 - 20133 Milano <https://di.unimi.it/it/dipartimento/organizzazione/commissioni> Email: ammissioni.magistrali@di.unimi.it

Commissione Orientamento in Ingresso

Via Celoria 18 - 20133 Milano <https://di.unimi.it/it/dipartimento/organizzazione/commissioni> Email: orientamento@di.unimi.it

Commissione Orientamento in Uscita

Via Celoria 18 - 20133 Milano <https://di.unimi.it/it/dipartimento/organizzazione/commissioni> Email: orientamento.uscita@di.unimi.it

Commissione Piani di Studio

Via Celoria 18 - 20133 Milano <https://di.unimi.it/it/dipartimento/organizzazione/commissioni> Email: piani.studio@di.unimi.it

Commissione Studenti Erasmus ed Internazionali

Via Celoria 18 - 20133 Milano <https://di.unimi.it/it/dipartimento/organizzazione/commissioni> Email: erasmus@di.unimi.it

Commissione Tirocini e Tesi Laurea Magistrale

Via Celoria 18 - 20133 Milano <https://di.unimi.it/it/dipartimento/organizzazione/commissioni> Email: tesi.magistrali@di.unimi.it

Commissione Trasferimenti

Via Celoria 18 - 20133 Milano <https://di.unimi.it/it/dipartimento/organizzazione/commissioni> Email: trasferimenti@di.unimi.it

Rappresentanti Studenti

Email: rappresentanti.studenti@di.unimi.it

Segreterie Studenti

Via Celoria 18 - 20133 Milano Tel. 0250325032 <https://www.unimi.it/it/node/360> <https://www.unimi.it/it/node/359/>

Ufficio per la didattica

Via Celoria 18 - 20133 Milano Tel. 0250316250/252 Sportello su appuntamento (ufficio.didattica@di.unimi.it)

CARATTERISTICHE DEL CORSO DI STUDI

Obiettivi formativi generali e specifici

Il corso di laurea magistrale in Sicurezza Informatica si propone di fornire solide basi scientifiche, metodologiche e tecnologiche per lo svolgimento di attività di ricerca, progettazione, realizzazione, verifica, coordinamento e gestione di sistemi informatici riferibili ai diversi ambiti di applicazione delle scienze e delle tecnologie informatiche nell'ambito della sicurezza e protezione dei sistemi, delle reti e delle infrastrutture informatiche, ed al trattamento sicuro e riservato dei dati. Il laureato magistrale in Sicurezza Informatica svolge attività di progettazione, realizzazione, verifica, usabilità, manutenzione, controllo e gestione di infrastrutture e sistemi informatici sicuri e protetti. Obiettivo fondamentale della sua attività è il miglioramento costante di sistemi informatici sicuri e protetti, anche con riferimento alla gestione sicura dei dati sensibili, accompagnato dalla capacità di recepire e proporre negli ambiti applicativi in cui opera le innovazioni che continuamente caratterizzano la disciplina.

Il percorso formativo è finalizzato alla creazione di professionisti dotati di competenze scientifiche e tecnologiche di alto livello, capacità metodologiche e operative e visione aperta e critica delle problematiche connesse all'adozione e all'uso delle tecnologie informatiche, con particolare riferimento all'uso delle soluzioni scientifiche e tecnologiche relative alla sicurezza informatica.

Gli obiettivi formativi sopra descritti vengono acquisiti tramite la partecipazione alle lezioni frontali, lo studio personale e attività di esercitazione in aula o in laboratorio.

I laureati che avranno crediti in numero sufficiente in opportuni gruppi di settori disciplinari potranno accedere alla professione di insegnante nelle scuole secondarie superiori, secondo le disposizioni in vigore.

Risultati di apprendimento attesi

Conoscenza e capacità di comprensione (knowledge and understanding)

Acquisizione di conoscenze e competenze di livello avanzato nei diversi ambiti concorrenti alla sicurezza di sistemi informatici complessi ed alla protezione dei dati.

- Conoscenze di aspetti scientifici, metodologici, e tecnologici per la protezione di dati sensibili.
- Conoscenze di aspetti scientifici, metodologici, e tecnologici per lo sviluppo di reti e sistemi informatici sicuri.
- Conoscenze di aspetti scientifici, metodologici, e tecnologici per lo sviluppo di applicazioni sicure.
- Conoscenze di aspetti aziendali, economici, e giuridici relativi alla gestione della sicurezza informatica e della protezione dei dati.

Conoscenze di aspetti scientifici, metodologici, e tecnologici per l'analisi, l'usabilità e la verifica della sicurezza di sistemi e reti informatiche.

Tali conoscenze e capacità vengono acquisite attraverso lezioni teoriche ed esercitazioni pratiche e valutate al termine degli insegnamenti e dell'intero percorso di studi. La valutazione dell'apprendimento individuale risulta da una combinazione di fattori inerenti all'acquisizione di conoscenze e capacità di tipo metodologico e tecnologico nell'ambito della sicurezza informatica e delle sue applicazioni.

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

Applicazione di conoscenze e competenze nell'analisi, nel disegno, nella realizzazione e nella valutazione di sistemi informatici sicuri e protetti operanti in diversi ambiti applicativi.

- Capacità di analizzare le problematiche di protezione dati e di identificare e realizzare metodi e tecniche appropriate per la loro soluzione.
- Capacità di progettare, realizzare e gestire reti e sistemi informatici sicuri.
- Capacità di progettare, sviluppare e gestire applicazioni sicure.
- Capacità di analizzare e valutare aspetti di sicurezza informatica e protezione dei dati in diversi contesti, quali quelli aziendali/amministrativi pubblici e privati, anche in contesti di innovazione tecnologica.

Tali conoscenze e capacità vengono acquisite attraverso lezioni teoriche ed esercitazioni pratiche e valutate al termine degli insegnamenti e dell'intero percorso di studi. La valutazione dell'apprendimento individuale risulta da una combinazione di fattori inerenti all'acquisizione di conoscenze e capacità di tipo metodologico e tecnologico nell'ambito della sicurezza informatica e delle sue applicazioni.

Autonomia di giudizio (making judgements)

Acquisizione di una piena capacità di giudizio autonomo e consapevole in merito alle decisioni ed alle scelte progettuali in ambito sicurezza informatica e delle possibili implicazioni etiche delle proprie attività professionali.

- Autonomia nell'analisi di problemi (sia teorici sia pratici) al fine di identificare i punti chiave per la loro modellazione e risoluzione.
- Capacità di ragionamento critico e sistematico, sapendo elaborare in autonomia un piano di studio o di ricerca per la risoluzione di problemi complessi.
- Capacità di lettura e valutazione critica e oggettiva dei risultati ottenuti da opportune sperimentazioni, o descritti in relazioni tecnico-scientifiche e in letteratura scientifica.
- Autonomia nella progettazione, sviluppo e analisi di sistemi, reti, infrastrutture e applicazioni in ambito sicurezza informatica.
- Abilità nella valutazione delle implicazioni economiche, etiche, giuridiche, sociali e ambientali della trasformazione

digitale.

Tali conoscenze e capacità vengono acquisite attraverso lezioni teoriche ed esercitazioni pratiche e valutate al termine degli insegnamenti e dell'intero percorso di studi. La valutazione dell'apprendimento individuale risulta da una combinazione di fattori inerenti all'acquisizione di conoscenze e capacità di tipo metodologico e tecnologico nell'ambito della sicurezza informatica e delle sue applicazioni.

Abilità comunicative (communication skills)

Acquisizione di capacità relazionali e comunicative per permettere di gestire e promuovere la sicurezza informatica in diversi ambiti applicativi, anche interdisciplinari.

- Capacità di presentare e valutare criticamente per iscritto in maniera chiara, coerente e concisa, idee ed argomentazioni tecniche e metodologiche, impiegando terminologia e linguaggi tecnici appropriati.
- Capacità di formulare ed esprimere oralmente, anche in contesti pubblici, argomentazioni complesse riguardanti metodologie e tecnologie connesse alla sicurezza informatica.
- Capacità di elaborare in maniera compiuta e coerente una dissertazione originale di ricerca su un tema complesso, anche mediante l'impiego di appropriati supporti tecnologici.

Tali conoscenze e capacità vengono acquisite attraverso lezioni teoriche ed esercitazioni pratiche e valutate al termine degli insegnamenti e dell'intero percorso di studi.

Abilità di apprendimento (learning skills)

Acquisizione di capacità organizzative autonome che permettano un aggiornamento continuo delle conoscenze.

- Capacità di utilizzare biblioteche, banche dati, archivi e repertori cartacei ed elettronici per accedere ad informazioni scientifiche e fonti rilevanti.
- Capacità di identificare un problema e di individuare le attività di analisi e ricerca necessarie per giungere ad una soluzione.
- Capacità di aggiornamento delle competenze e abilità, per mantenersi costantemente aggiornati con i continui avanzamenti delle scienze informatiche e della sicurezza informatica, così da adattarsi a nuove situazioni e tipologie di problemi.

Tali conoscenze e capacità vengono acquisite attraverso lezioni teoriche ed esercitazioni pratiche e valutate al termine degli insegnamenti e dell'intero percorso di studi, in particolare attraverso lo svolgimento di approfondimenti sia metodologici sia tecnologici.

Profilo professionale e sbocchi occupazionali

Specialisti nella progettazione e gestione di reti e infrastrutture informatiche sicure

Funzione in un contesto di lavoro

Esperti di problematiche avanzate di sicurezza informatica relative alla progettazione, configurazione e gestione di reti e infrastrutture informatiche per sistemi e risorse critiche. Queste figure professionali affrontano aspetti tecnologici per i quali è richiesta una conoscenza estremamente approfondita delle tecnologie e delle tendenze evolutive per la sicurezza informatica a livello globale. Sono quindi indispensabili in casi nei quali sia richiesta capacità di analisi di scenari tecnologici di elevata complessità e specificità, incluse architetture basate su IoT, cyber-physical system, cloud/fog/edge computing, architetture mobili e architetture data intensive.

Competenze associate alla funzione

Queste figure professionali sono degli specialisti di livello avanzato per aver approfondito in modo particolare tutti gli aspetti anche di maggior dettaglio degli aspetti scientifici, metodologici, tecnologici e applicativi della sicurezza informatica nelle reti e nelle infrastrutture. Competenze avanzate di questo tipo sono richieste per il rilevamento, l'analisi, la difesa e la prevenzione di intrusioni, attacchi informatici e malware.

Sbocchi occupazionali

Svolgono attività professionali specializzate nell'ambito della progettazione e nella gestione di reti e infrastrutture informatiche sicure. Questa attività potrà svolgersi, anche come libera professione, in tutti gli ambiti del settore privato e pubblico che operano nella progettazione, sviluppo, gestione, manutenzione o utilizzo di reti e infrastrutture informatiche in un'ampia gamma di settori, inclusi quello delle tecnologie delle informazioni e della comunicazione e tutti i settori applicativi che le utilizzano. Questa attività potrà inoltre svolgersi in enti di ricerca e università come supporto tecnico alle attività di ricerca e sperimentazione negli ambiti delle conoscenze e competenze di questo profilo professionale.

Specialisti nella progettazione e gestione di soluzioni per il trattamento sicuro e la protezione dei dati

Funzione in un contesto di lavoro

Esperti di problematiche avanzate relative alla protezione dei dati nel contesto della loro gestione, analisi e condivisione. Queste figure professionali affrontano problematiche per le quali è richiesta una conoscenza estremamente approfondita degli aspetti scientifici, metodologici, tecnologici e applicativi relativi alla sicurezza e privacy dei dati. Sono quindi indispensabili in casi nei quali sia richiesta capacità di analisi di scenari di elevata complessità e specificità, inclusi scenari IoT, cyber-physical, cloud/fog/edge, mobili e di architetture data intensive.

Competenze associate alla funzione

Queste figure professionali sono degli specialisti di livello avanzato per aver approfondito in modo particolare tutti gli aspetti anche di maggior dettaglio degli aspetti scientifici, metodologici, tecnologici e applicativi della sicurezza e della privacy dei dati. Competenze avanzate di questo tipo sono richieste per assicurare la gestione, analisi, utilizzo e condivisione

dei dati garantendone la protezione.

Sbocchi occupazionali

Svolgono attività professionali specializzate nell'ambito della progettazione e nella gestione di soluzioni per il trattamento sicuro dei dati che sono sempre più necessari nella moderna società digitale basata sulla raccolta, condivisione, e analisi di grandi collezioni di dati e che quindi richiede garanzie di corretta protezione e utilizzo dei dati nel rispetto di legislazioni, regolamentazioni, e dei requisiti di protezione da parte di cittadini, imprese e aziende. Questa attività potrà svolgersi, anche come libera professione, in tutti gli ambiti del settore privato e pubblico che operano nella progettazione, sviluppo, gestione, manutenzione o utilizzo di sistemi informativi, applicazioni, o scenari di trattamento dati in un'ampia gamma di settori, inclusi quello delle tecnologie delle informazioni e della comunicazione e tutti i settori applicativi che le utilizzano. Questa attività potrà inoltre svolgersi in enti di ricerca e università come supporto tecnico alle attività di ricerca e sperimentazione negli ambiti delle conoscenze e competenze di questo profilo professionale.

Specialisti nella progettazione e gestione di sistemi informatici, sistemi informativi e applicazioni con garanzie di sicurezza e privacy

Funzione in un contesto di lavoro

Esperti di problematiche avanzate di sicurezza informatica relative sia ai sistemi e alle risorse critiche di un'azienda (data center, sistemi ad alta affidabilità, proprietà intellettuale, dati sensibili) sia derivanti dalle soluzioni tecnologiche maggiormente innovative. Queste figure professionali affrontano aspetti tecnologici per i quali è richiesta una conoscenza estremamente approfondita delle tecnologie e delle tendenze evolutive a livello globale. Sono quindi indispensabili in casi nei quali sia richiesta capacità di analisi di scenari tecnologici di elevata complessità e specificità.

Competenze associate alla funzione

Queste figure professionali sono degli specialisti di livello avanzato per aver approfondito in modo particolare tutti gli aspetti anche di maggior dettaglio di alcune tecnologie innovative. Competenze avanzate di questo tipo possono essere richieste in tutte le aree tipiche della sicurezza informatica, dalla programmazione sicura con l'applicazione di metodologie avanzate di analisi statica e dinamica, l'analisi di codice malevolo continuamente rilasciato su Internet, tecniche avanzate di crittografia, tecniche avanzate di protezione dei dati e per garantire la loro sicurezza e confidenzialità, tecniche avanzate di intelligenza artificiale con considerazione della loro sicurezza nonché della applicazione di tali tecniche in soluzioni di sicurezza e metodologie di test e di monitoraggio di applicazioni innovative.

Sbocchi occupazionali

Il settore dell'information technology si caratterizza per la presenza, presso molte realtà aziendali, sia di grandi dimensioni sia di piccole ma molto specializzate, così come nel settore della consulenza, di eccellenze tecnologiche che prevedono la continua ricerca e applicazione delle soluzioni più innovative. In tutti questi casi la gestione dei sistemi informativi aziendali necessita di professionalità altamente specializzate in grado di affrontare scenari complessi nei quali sono impiegate tecnologie che presentano problematiche di elevata difficoltà. Questa attività potrà svolgersi, anche come libera professione, in tutti gli ambiti del settore privato e pubblico che operano nella progettazione, sviluppo, gestione, manutenzione o utilizzo di sistemi informatici e informativi, o applicazioni in un'ampia gamma di settori, inclusi quello delle tecnologie delle informazioni e della comunicazione e tutti i settori applicativi che le utilizzano. Questa attività potrà inoltre svolgersi in enti di ricerca e università come supporto tecnico alle attività di ricerca e sperimentazione negli ambiti delle conoscenze e competenze di questo profilo professionale.

Specialisti in tecnologie dell'informazione e della comunicazione

Funzione in un contesto di lavoro

Le professioni comprese in questa categoria appartengono ai profili professionali degli esperti di utilizzo nei vari contesti operativi delle tecnologie dell'informazione e della comunicazione, sulle quali il corso di studio della classe LM-66 è in buona misura basato.

Queste figure professionali integrano la capacità di sviluppo di applicazioni informatiche sofisticate con la conoscenza delle problematiche operative nei diversi contesti applicativi (inclusi IoT, cloud/fog/edge computing e architetture data intensive) occupandosi di progettare, gestire e mantenere applicazioni informatiche complesse e articolate.

Competenze associate alla funzione

Queste figure professionali possiedono un'ottima conoscenza di base ed un ampio spettro di conoscenze e competenze nei vari settori dell'informatica, sono familiari con il metodo scientifico di indagine, hanno elevate capacità di modellazione, sanno comprendere e utilizzare gli strumenti matematici di supporto alle competenze informatiche, sono in grado di gestire attività di gruppo, di operare con autonomia e di inserirsi prontamente negli ambienti di lavoro.

Sbocchi occupazionali

I laureati possono operare nei più svariati ambiti applicativi per la progettazione e la gestione di sistemi informatici complessi e per lo studio e la ricerca di nuovi sistemi ed applicazioni. Questa attività potrà svolgersi, anche come libera professione, in tutti gli ambiti del settore privato e pubblico che operano nella progettazione, sviluppo, gestione, manutenzione o utilizzo di sistemi informatici, o applicazioni in un'ampia gamma di settori, inclusi quello delle tecnologie delle informazioni e della comunicazione e tutti i settori applicativi che le utilizzano. Questa attività potrà inoltre svolgersi in enti di ricerca e università come supporto tecnico alle attività di ricerca e sperimentazione negli ambiti delle conoscenze e competenze di questo profilo professionale.

Conoscenze per l'accesso

Possono accedere al corso di laurea magistrale in Sicurezza informatica:

- i laureati della classe delle lauree in Scienze e tecnologie informatiche (L-31) e della corrispondente classe relativa al D.M. 509/99;

- i laureati in altre classi purché abbiano acquisito negli studi pregressi almeno:

48 crediti nel settore INF/01 o ING-INF/05

12 crediti nei settori MAT/01- 09

Possono altresì accedere al corso di laurea coloro che siano in possesso di altro titolo di studio conseguito all'estero e riconosciuto idoneo in base all'equipollenza che abbiano acquisito competenze e conoscenze equivalenti a quelle dei requisiti sopraindicati.

Per la verifica dei requisiti curriculari e della preparazione personale, il candidato dovrà fornire i seguenti documenti: certificazione di laurea con voto, elenco degli esami superati con voto e numero di crediti.

La verifica dell'adeguatezza della preparazione personale si baserà sull'esito riportato negli esami dei settori scientifico disciplinari indicati tra i requisiti di accesso. Quando da ciò non si evinca la piena adeguatezza della preparazione personale, al candidato verrà inoltre richiesto il superamento di un colloquio individuale

Struttura del corso

• Scansione temporale: La durata del corso di laurea magistrale in Sicurezza Informatica è di due anni. La didattica è organizzata per ciascun anno di corso in tre cicli coordinati, convenzionalmente chiamati quadrimestri.

• Crediti formativi: Per il conseguimento della laurea magistrale lo studente deve acquisire 120 crediti formativi (CFU). L'apprendimento delle competenze e delle professionalità da parte degli studenti è computato in CFU, articolati secondo quanto disposto dal Regolamento didattico d'Ateneo. I CFU sono una misura del lavoro di apprendimento richiesto allo studente e corrispondono ciascuno ad un carico standard di 25 ore di attività, articolate in uno dei seguenti modi:

- 7 ore di lezioni frontali, con annesse 18 ore di studio individuale;

- 25 ore di attività formative relative allo svolgimento della prova finale.

• Studenti impegnati a tempo parziale: Per gli studenti che effettuano l'iscrizione a tempo parziale, le attività formative e i relativi CFU da conseguire annualmente saranno distribuiti secondo le modalità previste dal Regolamento per le iscrizioni a tempo parziale di Ateneo

• Insegnamenti: Gli insegnamenti sono prevalentemente mono-disciplinari, con la possibilità di alcuni corsi integrati. Allo scopo di incentivare il processo di internazionalizzazione, si prevede che alcuni degli insegnamenti possano essere tenuti in inglese.

• Prove d'esame: Le prove di esame si svolgono individualmente per ciascun insegnamento. Nel caso di insegnamenti articolati in moduli svolti da docenti diversi, viene individuato tra loro il docente responsabile dell'insegnamento al quale compete, d'intesa con gli altri docenti interessati, il coordinamento delle modalità di verifica del profitto e delle relative verbalizzazioni. L'acquisizione da parte dello studente dei crediti stabiliti per ciascun insegnamento è subordinata al superamento delle relative prove d'esame, che danno luogo a votazione in trentesimi, salvo per eventuali attività per le quali è previsto un giudizio di idoneità.

Presentazione del piano di studi

Il piano dovrà essere obbligatoriamente presentato nel primo anno di corso: le scadenze e le modalità di presentazione sono rese note dalla Direzione Segreteria Studenti con avvisi pubblicati alla pagina <https://www.unimi.it/it/studiare/frequentare-un-corso-di-laurea/seguire-il-percorso-di-studi/piano-studi>

Dopo l'approvazione del piano degli studi, lo studente può sostenere autonomamente ulteriori esami aggiuntivi rispetto al proprio percorso formativo.

L'inserimento tra i CFU a scelta libera di insegnamenti di CdL triennali è possibile solo a fronte di motivazioni documentate. In tal caso, lo studente è tenuto a dimostrare che lo stesso o analogo insegnamento non sia stato già sostenuto nella carriera triennale, allegando opportuna documentazione al Piano Studi.

Si segnalano, inoltre, le attività inserite nel progetto di Ateneo per lo sviluppo delle competenze trasversali: <https://www.unimi.it/it/studiare/frequentare-un-corso-di-laurea/seguire-il-percorso-di-studi/competenze-e-abilita-trasversali>.

Queste attività formative sono a frequenza obbligatoria, hanno un numero definito di posti e possono essere inserite nel piano degli studi, tra le "Attività a scelta libera". I dettagli sono disponibili alla pagina <https://sicurezzainformatica.cdl.unimi.it/it/insegnamenti>

ATTENZIONE

Alcuni insegnamenti recentemente attivati dal Collegio Didattico sono incompatibili con insegnamenti precedentemente attivati (non possono essere indicati nello stesso piano di studi). Anche versioni in lingua italiana e in lingua inglese dello stesso insegnamento non possono essere entrambe inserite nel piano di studi.

Per maggiori informazioni sulle incompatibilità si rimanda al sito web del corso di studi:

<https://sicurezzainformatica.cdl.unimi.it/it/studiare/presentazione-piano-di-studio>

Calendario attività didattiche

La didattica è organizzata per ciascun anno di corso in tre cicli coordinati, convenzionalmente chiamati quadrimestri.

Primo quadrimestre: dal 14 settembre al 20 novembre 2026

Secondo quadrimestre: dall'11 gennaio al 19 marzo 2027

Terzo quadrimestre: dal 12 aprile al 18 giugno 2027

Orario lezioni

L'orario delle lezioni è disponibile al seguente indirizzo: <https://www.unimi.it/it/studiare/frequentare-un-corso-di-laurea/seguire-il-percorso-di-studi/orari-delle-lezioni>

Esami (sessioni d'esame e modalità di valutazione del profitto)

Il profitto viene valutato tramite esami scritti o orali, con valutazione in trentesimi, fatta eccezione per l'esame di Inglese, che non dà luogo a votazione ma al solo giudizio di approvazione / non approvazione.

Viene inoltre richiesto in diversi casi lo svolgimento di un progetto propedeutico all'esame orale.

L'iscrizione alle prove d'esame deve essere effettuata tramite procedura on line: <https://www.unimi.it/it/studiare/frequentare-un-corso-di-laurea/seguire-il-percorso-di-studi/esami>

Durante l'anno sono previsti almeno sei appelli d'esame, di norma nei mesi di novembre, dicembre, gennaio, marzo, aprile, giugno, luglio, settembre.

Il calendario degli appelli è consultabile alla pagina: <https://www.unimi.it/it/studiare/frequentare-un-corso-di-laurea/seguire-il-percorso-di-studi/esami/calendario-degli-appelli>

Note

Lo studente è tenuto ogni anno a verificare l'effettiva attivazione dei corsi inseriti a manifesto.

Area didattica

Sede dei corsi di area informatica: via Celoria 18 - Milano.

Altre sedi di svolgimento delle lezioni: Settore Didattico, via Celoria 20; Settore Didattico, via Golgi 19; Didattica, via Venezian 15.

Laboratori didattica

Laboratorio informatico (Silab) presso il Dipartimento di Informatica, via Celoria 18, Milano.

Tutorato

Gli studenti possono rivolgersi ai docenti tutor per l'orientamento e alla Segreteria Didattica del Dipartimento di Informatica per ricevere informazioni e assistenza sui servizi messi a disposizione dal Collegio Didattico, sulla compilazione del piano studi, sui tirocini e la prova finale e, in generale, sull'organizzazione del Corso di Studi.

I nominativi dei tutor per l'orientamento, indicati nel presente Manifesto, e le loro funzioni vengono presentati agli studenti durante la Giornata di Accoglienza che si svolge il primo giorno di lezione dell'anno accademico.

Prove di lingua / Informatica

Per poter conseguire il titolo di studio è richiesta la conoscenza della lingua inglese di livello B2 del Quadro Comune Europeo di Riferimento per le lingue (QCER). Tale livello può essere attestato nei seguenti modi:

- tramite l'invio di una certificazione linguistica conseguita non oltre i 3 anni antecedenti la data di presentazione della stessa, di livello B2 o superiore (per la lista delle certificazioni linguistiche riconosciute dall'Ateneo si rimanda al sito: <https://www.unimi.it/it/node/39322>). La certificazione deve essere caricata al momento dell'immatricolazione o, successivamente, sul portale <http://studente.unimi.it/uploadCertificazioniLingue>;

- tramite Placement Test, erogato dal Centro linguistico d'Ateneo SLAM esclusivamente durante il I anno, da ottobre a gennaio (dicembre per il triennio). In caso di non superamento del test, sarà necessario seguire i corsi erogati da SLAM.

Il Placement Test è obbligatorio per tutti coloro che non sono in possesso di una certificazione valida.

Coloro che non sosterranno il Placement Test entro gennaio (dicembre per i bienni e i cicli unici) oppure non supereranno il test finale del corso entro 6 tentativi, dovranno conseguire privatamente una certificazione entro la laurea.

Obbligo di frequenza

La frequenza ai corsi e ai laboratori è fortemente consigliata.

Caratteristiche della prova finale

Il corso di laurea magistrale prevede lo svolgimento di una tesi di laurea magistrale, presso una struttura dell'Università o di altro Ente pubblico o privato da presentare e discutere in sede di prova finale per il conseguimento della laurea magistrale. La tesi di laurea magistrale è un elaborato scritto, in italiano o in inglese preparato dallo studente sotto la supervisione di un relatore e concernente un'esperienza scientifica originale, attinente ai temi della sicurezza informatica.

Il lavoro di tesi deve comprendere un'attività di progettazione o di ricerca o di analisi di caso, che dimostri la padronanza degli argomenti e degli strumenti utilizzati, nonché la capacità di operare in modo autonomo nel campo della sicurezza informatica e delle relative applicazioni.

La prova finale si conclude con una discussione orale dei risultati presentati nell'elaborato di fronte ad una commissione.

ESPERIENZA DI STUDIO ALL'ESTERO NELL'AMBITO DEL PERCORSO FORMATIVO

L'Università degli Studi di Milano sostiene la mobilità degli studenti, offrendo l'opportunità di svolgere periodi di studio e di tirocinio all'estero, arricchendo il proprio percorso formativo in un contesto internazionale e stimolante.

Gli accordi stipulati dall'Ateneo con oltre 300 università dei 27 Paesi dell'Unione nell'ambito del programma Erasmus+

permettono agli studenti regolarmente iscritti di svolgere parte del proprio percorso di studi presso una delle università partner o seguire percorsi di tirocinio/stage presso imprese, centri di formazione e di ricerca e altre organizzazioni.

Analoghe opportunità di mobilità internazionale vengono garantite inoltre anche per destinazioni extra-europee, grazie ai rapporti di collaborazione stabiliti dall'Ateneo con numerose prestigiose istituzioni.

L'Università degli Studi di Milano fa inoltre parte della 4EU+ European University Alliance, che offre opportunità di mobilità (virtuale, mista e fisica) tra gli 8 atenei multidisciplinari e fortemente orientati alla ricerca che costituiscono l'Alleanza. Fanno parte dell'Alleanza 4EU+, con il nostro ateneo, Charles University di Praga, Università di Heidelberg, Université Paris-Panthéon-Assas, Sorbonne Université di Parigi, Università di Copenaghen, Università di Ginevra e Università di Varsavia

Cosa offre il corso di studi

La formazione del corso di studi può essere arricchita includendo esperienze educative in atenei all'estero, sia per approfondire alcune tematiche disciplinari sia come esperienza umana e di socializzazione in contesti tecnologici stimolanti, dinamici e internazionali. E' offerta la possibilità di periodi di studio per seguire insegnamenti da includere nel piano di studi individuale nell'ambito di accordi Erasmus+ con oltre 50 atenei in Belgio, Finlandia, Francia, Germania, Grecia, Lituania, Norvegia, Paesi Bassi, Polonia, Portogallo, Repubblica Ceca, Romania, Slovenia, Spagna, Svizzera, Turchia, Ungheria. Tipicamente tali periodi durano 5 mesi e prevedono attività didattiche per circa 30 CFU. Le tematiche offerte in tali periodi sono tipicamente nell'area delle tecnologie dell'informazione e comunicazione e delle relative applicazioni. Il riconoscimento delle attività svolte avviene in base all'accordo preventivo di riconoscimento (Learning Agreement) definito dallo studente con il responsabile del Dipartimento di Informatica per gli scambi Erasmus prima di iniziare le attività stesse e all'effettivo completamento delle attività con esito positivo; gli insegnamenti superati positivamente sostituiranno attività formative previste dal manifesto degli studi, ricoprendo le stesse aree tematiche o complementandone le competenze di base acquisite. Il riconoscimento dei CFU acquisiti all'estero e la definizione del piano degli studi che li includa vengono effettuati dall'apposita commissione istruttoria del Collegio Didattico di Informatica. Analogamente, è possibile effettuare periodi di tirocinio in tali atenei per lo svolgimento delle attività di studio per la tesi di laurea. Il riconoscimento è analogo a quello previsto per gli insegnamenti.

Erasmus: il coordinatore di queste iniziative per il Dipartimento di Informatica è il prof. Fabio Scotti.

Programmi internazionali: il coordinatore di queste iniziative per il Dipartimento di Informatica è il prof. Davide Rocchesso.

Ulteriori informazioni didattiche sulla mobilità internazionale per gli studenti di corsi erogati dal Dipartimento di Informatica sono disponibili a <https://di.unimi.it/it/rapporti-internazionali/mobilita-internazionale/opportunita-internazionali>

Modalità di partecipazione ai programmi di mobilità - mobilità Erasmus

Gli studenti dell'Università degli Studi di Milano partecipano ai programmi di mobilità Erasmus per studio e tirocinio tramite una procedura pubblica di selezione finalizzata a valutare, grazie a specifiche commissioni:

- la carriera accademica
- la proposta di programma di studio/tirocinio all'estero del candidato
- la conoscenza della lingua straniera di lavoro
- le motivazioni alla base della candidatura

Bando e incontri informativi

La selezione pubblica annuale per l'Erasmus studio si svolge in genere a febbraio e prevede la pubblicazione di un bando che specifica sedi, numero di posti e requisiti richiesti.

Per quanto riguarda l'Erasmus Traineeship, vengono generalmente pubblicati due bandi all'anno che prevedono rispettivamente la possibilità di reperire autonomamente una sede di tirocinio o di presentare domanda per una sede definita tramite accordo inter-istituzionale.

L'Ateneo organizza incontri informativi generali e/o declinati per area disciplinare per illustrare le opportunità di mobilità internazionale e le modalità di partecipazione.

Borsa di studio Erasmus +

Per i soggiorni all'estero che rientrano nel programma Erasmus+, l'Unione Europea assegna ai vincitori della selezione una borsa di mobilità a supporto delle spese sostenute, che può essere integrata da un contributo dell'Ateneo per gli studenti in condizioni economiche svantaggiate.

Corsi di lingua

Gli studenti che superano le selezioni per i programmi di mobilità possono avvalersi dei corsi intensivi di lingue straniere proposti ogni anno dal Centro linguistico d'Ateneo SLAM.

<https://www.unimi.it/it/node/8/>

Maggiori informazioni alla pagina: <https://www.unimi.it/it/node/274/>

Per assistenza:

Ufficio Mobilità internazionale

Via Santa Sofia 9 (secondo piano)

Tel. 02 503 13501-12589-13495-13502

MODALITA' DI ACCESSO: 1° ANNO LIBERO CON VALUTAZIONE DEI REQUISITI DI ACCESSO

Informazioni e modalità organizzative per immatricolazione

Domanda di ammissione

La domanda di ammissione è obbligatoria e dovrà essere effettuata per via telematica dal 22 gennaio al 31 ottobre 2026 (dettagli sul sito <https://www.unimi.it/it/studiare/frequentare-un-corso-di-laurea/isciversi-un-corso-di-laurea>). Possono presentare la domanda di ammissione i candidati già in possesso della laurea e coloro che la conseguiranno entro il 31 dicembre 2026.

L'ammissione richiede il possesso di requisiti curriculari minimi e di un'adeguata preparazione personale (si veda sopra: "conoscenze per l'accesso").

Immatricolazione

Potranno immatricolarsi solo i laureati che avranno superato con esito positivo la valutazione della carriera.

I candidati ammessi potranno immatricolarsi nei tempi e con le procedure riportati all'indirizzo: <https://www.unimi.it/it/studiare/frequentare-un-corso-di-laurea/isciversi/isciversi-un-corso-magistrale>.

Gli studenti dell'Ateneo che abbiano presentato domanda di ammissione e che nel corso della laurea triennale abbiano acquisito CFU in eccedenza rispetto ai 180 necessari, seguendo corsi e/o laboratori previsti nel corso di laurea magistrale, potranno richiederne il riconoscimento ai fini del conseguimento dei 120 CFU richiesti.

N° posti riservati a studenti extracomunitari non soggiornanti in Italia

5

1° ANNO DI CORSO Attività formative obbligatorie				
Erogazione	Attività formativa	Modulo/Unità didattica	Cfu	Settore
	Accertamento di lingua inglese - livello B2 (3 CFU)		3	NN
1 quadrimestre	CRITTOGRAFIA		6	INFO-01/A
1 quadrimestre	GESTIONE SICURA DEI DATI		6	INFO-01/A
1 quadrimestre	PRIVATEZZA E PROTEZIONE DEI DATI		6	INFO-01/A
2 quadrimestre	INTELLIGENZA ARTIFICIALE PER LA SICUREZZA E LA PRIVATEZZA		6	INFO-01/A
2 quadrimestre	TECNICHE DI PROTEZIONE DEL SOFTWARE		6	INFO-01/A
3 quadrimestre	SICUREZZA NELLE ARCHITETTURE DATA INTENSIVE		6	INFO-01/A
3 quadrimestre	SICUREZZA NELLE RETI		6	INFO-01/A
Totale CFU obbligatori			45	
Attività a scelta				
Per i 12 CFU a scelta guidata, lo studente deve scegliere fra gli insegnamenti della seguente tabella.				
2 quadrimestre	AFFIDABILITA' DEI SISTEMI		6	INFO-01/A
2 quadrimestre	GESTIONE DELLA SICUREZZA NELLE IMPRESE		6	ECON-07/A
2 quadrimestre	TECNICHE E APPLICAZIONI BIOMETRICHE		6	INFO-01/A
3 quadrimestre	DIGITAL FORENSICS		6	INFO-01/A
3 quadrimestre	INFORMATION MANAGEMENT		6	INFO-01/A
3 quadrimestre	MACHINE LEARNING PER LA SICUREZZA DEI SISTEMI E DELLE RETI		6	INFO-01/A
3 quadrimestre	SPECIFICA E VERIFICA DI SISTEMI CRITICI		6	INFO-01/A
2° ANNO DI CORSO (da attivare a partire dall'a.a. 2027/28) Attività formative obbligatorie				
Erogazione	Attività formativa	Modulo/Unità didattica	Cfu	Settore
1 quadrimestre	ANALISI E GESTIONE DEL RISCHIO		6	STAT-01/A
1 quadrimestre	FONDAMENTI GIURIDICI PER LA SICUREZZA E LA PRIVATEZZA		6	GIUR-17/A
Totale CFU obbligatori			12	
Attività a scelta				
Ulteriori insegnamenti per la scelta guidata attivati a partire dall'a.a. 2027/28.				
1 quadrimestre	QUANTUM E POST-QUANTUM COMPUTING		6	INFO-01/A
1 quadrimestre	SICUREZZA DEI SISTEMI IOT		6	INFO-01/A
1 quadrimestre	SISTEMI PER LA PROTEZIONE E LA DIFESA DEGLI ATTACCHI INFORMATICI		6	INFO-01/A
Altre attività a scelta				
<p>Lo studente è tenuto ad acquisire 12 cfu a libera scelta attingendo dalla tabella della scelta guidata, oppure scegliendo fra quelli erogati da altri corsi di studio del Collegio Didattico di Informatica, nonché fra tutti gli insegnamenti attivati dall'Ateneo purché coerenti con il progetto formativo e i cui contenuti non siano sovrapposti a quelli di insegnamenti erogati dal CdS in Sicurezza Informatica o da altri corsi di studio di cui è referente il Dipartimento di Informatica.</p> <p>Gli studenti possono richiedere il riconoscimento di cfu per attività formative presso enti esterni, presentando la relativa certificazione. Ogni certificazione può dare luogo ad un massimo di 3 cfu, e possono essere riconosciute fino a 2 certificazioni. Lo studente che intende chiedere il riconoscimento delle certificazioni deve compilare il modulo di "istanza" disponibile alla pagina https://www.unimi.it/it/studiare/servizi-gli-studenti/segreteria-infostudenti/modulistica-generale e consegnarlo alla segreteria del proprio corso di studio unitamente alla copia delle certificazioni conseguite.</p>				

La valutazione verrà effettuata da un'apposita commissione sulla base dei seguenti parametri:

- **Validità:** la certificazione deve essere stata ottenuta da un massimo di 5 anni.
- **Specificità:** la certificazione deve avere come oggetto competenze riferibili a quelle previste dal corso di laurea in cui lo studente è regolarmente iscritto.
- **Specializzazione:** la certificazione deve riguardare competenze specialistiche e/o professionalizzanti.
- **Livello:** la certificazione deve attestare competenze di livello medio o avanzato. Sono escluse certificazioni di base ed entry level.

Le richieste sopra indicate possono essere presentate solo dagli studenti che non abbiano già ottenuto tali riconoscimenti durante il percorso triennale.

Attività conclusive

PROVA FINALE		39	NN
	Totale CFU obbligatori	39	

RICONOSCIMENTI E VECCHI ORDINAMENTI

Riconoscimenti crediti già acquisiti

La Commissione Trasferimenti (<https://di.unimi.it/it/dipartimento/organizzazione/commissioni>) è responsabile di valutare il trasferimento dei CFU acquisiti con esami sostenuti in altri corsi di laurea, di nuovo e di vecchio ordinamento, sulla base delle tabelle di equipollenza approvate dal Collegio Didattico. Per gli insegnamenti per i quali non è prevista una equipollenza tabellare, la commissione proverà a stabilire una equipollenza in base ai contenuti degli insegnamenti. Qualora non fosse possibile stabilire una equipollenza, la commissione proverà a utilizzare i crediti come insegnamenti liberi a scelta.