



REGOLAMENTO DIDATTICO DEL CORSO DI LAUREA MAGISTRALE IN SICUREZZA INFORMATICA

Il presente Regolamento disciplina l'organizzazione e il funzionamento del corso di laurea magistrale in Sicurezza Informatica, appartenente alla classe delle lauree LM-66 Sicurezza Informatica, attivato presso l'Università degli Studi di Milano.

In ottemperanza a quanto disposto dall'art. 11, comma 2, della legge 19 novembre 1990, n. 341, dall'art. 12 del D.M. 22 ottobre 2004, n. 270, così come modificato dal D.M. 96/2023 e dal Regolamento didattico d'Ateneo, il presente Regolamento specifica, nel rispetto della libertà di insegnamento e dei diritti e doveri dei docenti e degli studenti, gli aspetti organizzativi e funzionali del corso di laurea magistrale in Sicurezza Informatica, in analogia con il relativo Ordinamento didattico, quale definito nel Regolamento didattico d'Ateneo, nel rispetto della classe alla quale il corso afferisce.

Il Dipartimento di Informatica "Giovanni degli Antoni" è il Dipartimento referente del Corso di Studi.

Art. 1 - Obiettivi formativi specifici del corso di laurea magistrale e profili professionali di riferimento (Scheda Sua - Quadro A4.a)

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.

Profili professionali di riferimento (Scheda Sua - Quadro A2.a)

Specialisti nella progettazione e gestione di reti e infrastrutture informatiche sicure



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

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

Specialisti in tecnologie dell'informazione e della comunicazione

Art. 2 - Accesso (Scheda Sua - Quadro A3.a + Quadro A3.b)

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.

La verifica del possesso dei requisiti consisterà nella valutazione della carriera universitaria pregressa, effettuata sulla base dei seguenti titoli: 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.

Modalità di riconoscimento dei crediti

Per il riconoscimento dei CFU nei casi di trasferimento da altro Ateneo o di passaggio da altro corso di studio dell'Ateneo, si applica quanto disposto dal Regolamento didattico di Ateneo. Il Collegio didattico delibera caso per caso se debbano essere previste o meno forme di verifica di CFU acquisiti ed eventuali esami integrativi. Per il riconoscimento delle attività di studio svolte all'estero e dei relativi CFU, si applica quanto disposto dal Regolamento didattico di Ateneo.

Il numero massimo di crediti individualmente riconoscibili, ai sensi dell'art. 3, comma 2, del DM 931/2024, per conoscenze e abilità professionali certificate, nonché per altre conoscenze e abilità maturate in attività formative di livello post-secondario alla cui progettazione e realizzazione l'università abbia concorso, è quantificato in un massimo di 24 CFU.

Art. 3 - Organizzazione del corso di laurea magistrale

Il corso è organizzato come specificato nel seguito.

- **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.
- **Metodi didattici:** Le conoscenze vengono principalmente acquisite tramite la partecipazione alle lezioni frontali e lo studio personale. Le abilità sono principalmente sviluppate tramite attività di esercitazione in aula o in laboratorio, in modo autonomo o supervisionato.



- **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.
- **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.
- **Lingua inglese:** Per completare il percorso didattico è richiesta la conoscenza della lingua inglese con livello B2 (QCER, Quadro Comune Europeo di Riferimento). Tale conoscenza viene accertata dal Centro linguistico d'Ateneo SLAM secondo le modalità previste nel Manifesto degli Studi.
- **Struttura del corso:** I 120 crediti formativi (CFU) che ogni studente deve acquisire sono suddivisi in:
 - 54 CFU acquisiti in *insegnamenti fondamentali*, uguali per tutti;
 - 12 CFU acquisiti in *insegnamenti a scelta guidata*, ovvero da scegliere dalla tabella degli insegnamenti affini;
 - 12 CFU acquisiti in *insegnamenti a scelta libera*;
 - 3 CFU acquisiti per la conoscenza di almeno una *lingua straniera*;
 - 39 CFU acquisiti per la *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; le specifiche attività formative, di tutorato e di sostegno indirizzate a queste tipologie di studenti, saranno indicate nel Manifesto degli studi.

Art. 4 - Settori scientifico-disciplinari e relativi insegnamenti

Gli insegnamenti del corso di laurea magistrale in Sicurezza Informatica, definiti in relazione ai suoi obiettivi formativi, nell'ambito dei settori scientifico-disciplinari di pertinenza, sono riportati nella seguente tabella.

Insegnamento	Settore scientifico-disciplinare
--------------	----------------------------------



Affidabilità dei sistemi	INF/01
Analisi e gestione del rischio	SECS-S/01
Intelligenza artificiale per la sicurezza e la privacy	INF/01
Crittografia	INF/01
Digital forensics	INF/01
Fondamenti giuridici per la sicurezza e la privacy	IUS/20
Gestione della sicurezza nelle imprese	SECS-P/08
Gestione sicura dei dati	INF/01
Machine learning per la sicurezza dei sistemi e delle reti	INF/01
Quantum e post-quantum computing	INF/01
Privacy e protezione dei dati	INF/01
Progettazione di sistemi operativi sicuri	INF/01
Sicurezza nelle architetture data intensive	INF/01
Sicurezza nelle reti	INF/01
Specifiche e verifica di sistemi critici	INF/01
Tecniche di protezione dei sistemi	INF/01
Tecniche di protezione del software	INF/01
Tecniche e applicazioni biometriche	INF/01

Art.5 - Piano didattico

Il *piano didattico* indica tutte le attività formative previste per il conseguimento della laurea magistrale in Sicurezza Informatica. Durante il primo anno lo studente presenta il proprio piano didattico individuale, che descrive la scelta di: 12 CFU da insegnamenti affini; 12 CFU acquisiti da insegnamenti a scelta dello studente (scelti fra gli affini, quelli erogati da altri corsi di studio del CCD di Informatica, nonché 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). La verifica della coerenza del progetto formativo proposto, nel suo complesso, viene valutata da un'apposita commissione.

Attività Caratterizzanti

TAF*	Ambito disciplinare	Insegnamento	SSD	CFU	Nr. esami	Anno di corso
B	Formazione Scientifica	Analisi e gestione del rischio	SECS-S/01	6	1	2
	Formazione Informatica	Intelligenza artificiale per la sicurezza e la privacy	INF/01	6	1	1
		Crittografia	INF/01	6	1	1
		Gestione sicura dei dati	INF/01	6	1	1
		Privacy e protezione dei dati	INF/01	6	1	1



		Sicurezza nelle architetture data intensive	INF/01	6	1	1
		Sicurezza nelle reti	INF/01	6	1	1
		Tecniche di protezione del software	INF/01	6	1	1
	Formazione tecnologica, aziendale, economica, giuridica, etica, psicologica e sociale	Fondamenti giuridici per la sicurezza e la privacy	IUS/20	6	1	2
Totale Attività Caratterizzanti				54	9	

Attività Affini

TAF*	Insegnamento	SSD	CFU	Nr. esami
C	Insegnamenti a scelta guidata (vedi tabella sotto)	INF/01, SECS-P/08	12	2
Totale Attività Affini			12	2

Altre Attività Formative

TAF*			Attività formative	CFU	Anno di corso
D	A scelta dello studente		-	12	1 e 2
E	Per la prova finale e la lingua straniera (art.10, comma 5, lettera c)	Prova finale	-	39	2
		Per la conoscenza di almeno una lingua straniera	-		
F	Ulteriori attività formative (art. 10, comma 5, lettera d)	Ulteriori conoscenze	Lingua inglese	3	
Totale				54	



Insegnamenti a scelta guidata

Per i 12 CFU a scelta guidata, lo studente deve scegliere fra gli insegnamenti della seguente tabella.

Insegnamento	SSD	CFU	Anno di corso
Affidabilità dei sistemi	INF/01	6	1
Gestione della sicurezza nelle imprese	SECS-P/08	6	1
Digital forensics	INF/01	6	1
Machine learning per la sicurezza dei sistemi e delle reti	INF/01	6	1
Progettazione di sistemi operativi sicuri	INF/01	6	2
Quantum e post-quantum computing	INF/01	6	2
Specifiche e verifica di sistemi critici	INF/01	6	1
Tecniche di protezione dei sistemi	INF/01	6	2
Tecniche e applicazioni biometriche	INF/01	6	1

***TAF** (Tipo Attività formativa) secondo la seguente legenda:

A=base

B=caratterizzante

C=affine

D=A scelta dello studente (art.10, comma 5, lettera a)

E=Per la prova finale e la lingua straniera (art.10, comma 5, lettera c)

F=Ulteriori attività formative (art.10, comma 5, lettera d)

S=Per stages e tirocini presso imprese, enti pubblici o privati, ordini professionali (art.10, comma 5, lettera e)

Gli obiettivi e i programmi dei singoli insegnamenti sono pubblicati sul sito del corso.

Propedeuticità

Non sono previste propedeuticità.

Caratteristiche prova finale

La prova finale consiste nella redazione di un elaborato finale relativo ad un'attività di carattere teorico o sperimentale svolta in autonomia dallo studente, sotto la supervisione di uno o più docenti, presso gruppi di ricerca o imprese; l'elaborato dovrà documentare gli aspetti progettuali e realizzativi dell'attività svolta nonché i collegamenti del lavoro con lo stato corrente delle conoscenze nel settore della Sicurezza Informatica.



Art.6 - Organizzazione della Assicurazione della Qualità (Scheda Sua - Quadro D2)

I processi di gestione del CdS sono coordinati dal Presidente del Collegio Didattico, al cui lavoro contribuiscono: un Coordinatore per ogni CdS, il Collegio Didattico, la Commissione Paritetica Docenti-Studenti (CPDS), un insieme di Commissioni e Gruppi di Lavoro dipartimentali e le Unità per l'Assicurazione della Qualità (Referenti AQ).

Il Presidente del Collegio Didattico ha il compito di monitorare lo svolgimento delle attività didattiche gestite dal Collegio e verificare il pieno assolvimento degli impegni di competenza dei singoli docenti. Il Coordinatore del CdS coadiuva il Presidente nella gestione del CdS. Insieme si occupano di:

- monitorare l'andamento del CdS attraverso l'esame delle statistiche relative al percorso degli studenti (CFU acquisiti, abbandoni, etc.),
- avanzare proposte di modifica al piano formativo,
- contribuire alla stesura delle schede SUA e delle schede del riesame,
- contribuire alla stesura dei regolamenti e dei manifesti,
- contribuire alla stesura del piano didattico delle coperture.

Il Collegio didattico approva la scheda di monitoraggio annuale, il rapporto di riesame ciclico ed esamina la Relazione finale della CPDS, collaborando al buon funzionamento dei processi di AQ del CdS.

In accordo con il piano strategico del Dipartimento di Informatica, ci si ripropone di riunire fino a due volte l'anno il collegio didattico di corso di studio, composto dai soli docenti coinvolti nel corso di Laurea Magistrale in Sicurezza Informatica. Il collegio didattico del corso di studio coopera, in forma consultiva con il coordinatore del CdS, nella compilazione della scheda di monitoraggio annuale ed, eventualmente, del rapporto di riesame ciclico. Esamina inoltre la Relazione finale della CPDS, formulando, sempre in modo consultivo, proposte migliorative al coordinatore di CdS.

La Facoltà di Scienze e Tecnologie svolge funzioni di coordinamento delle attività didattiche nelle aree di Biotecnologie Industriali, Scienze Biologiche, Scienze della Terra, Scienze e politiche ambientali, Scienze e tecnologie chimiche, Scienze e tecnologie fisiche, Scienze e tecnologie informatiche, Scienze e tecnologie per la conservazione dei beni culturali, Scienze e tecnologie per l'ambiente e la natura, Scienze matematiche.

La Commissione paritetica docenti-studenti (CPDS), che può essere qualificata come osservatorio permanente delle attività didattiche, è preposta alla funzione di primo valutatore interno delle attività formative che si svolgono nell'ambito dell'Ateneo ed espleta un'attività di controllo complessivo sull'Assicurazione della Qualità.

Il Gruppo di riesame è incaricato di redigere la Scheda di monitoraggio annuale secondo le scadenze ministeriali. Inoltre, redige il rapporto di Riesame ciclico tramite il quale si analizza in modo approfondito il CdS e si evidenziano i punti di forza e le possibilità di miglioramento. Il rapporto di Riesame ciclico viene redatto con cadenza quinquennale, fatta eccezione per i



seguenti casi: preparazione di una visita di Accreditamento Periodico, ovvero in presenza di modifiche sostanziali dell'ordinamento del CdS.

Le Unità per l'Assicurazione della Qualità (Referenti AQ) sono designate per ciascuno dei CdS afferenti al Dipartimento e hanno il compito di promuovere i processi locali di AQ, monitorandone gli esiti e supportando il PQA (Presidio della Qualità di Ateneo) nell'attività di comunicazione e sensibilizzazione circa le Politiche della Qualità d'Ateneo. Il referente per la gestione AQ supporta il Presidente di collegio nel coordinare il sistema della qualità del CdS, assicurando che le azioni intraprese siano conformi alle politiche dell'Ateneo e alle Linee guida del PQA. Il referente AQ svolge azioni di monitoraggio dell'andamento del CdS e verifica la corretta esposizione del sistema di AQ nella Scheda SUA-CdS. Infine, il referente partecipa al gruppo del riesame nella stesura delle schede di riesame annuale e ciclico, promuovendo il recepimento delle indicazioni della CPDS in tali documenti.