

Informazioni generali



Università	Università Telematica "Universitas MERCATORUM"
Nome del corso in italiano	SICUREZZA INFORMATICA (IdSua:1636161)
Nome del corso in inglese	CYBERSECURITY
Classe	LM-66 R - Sicurezza informatica
Lingua in cui si tiene il corso	italiano
URL del corso	http://www.unimercatorum.it
Modalità di erogazione	d. Corso di studio integralmente a distanza
Riepilogo Caratteristiche Cds	🌐 1° anno in SUA: 2024

Programmazione Accessi

Programmazione nazionale (art.1 Legge 264/1999)	No
Programmazione locale	No

Sede del Corso

Sede	ROMA (Cod.058091)
Codice interno all'Ateneo del Corso	066
Utenza sostenibile	400

Scheda SUA - Date creazione e aggiornamenti

Data di istituzione del corso	da determinare
Data Ultimo aggiornamento Scheda SUA	15/06/2026 11:27
Data Ultimo aggiornamento RAD	15/02/2024 10:54

Referenti e Strutture

Presidente (o Referente o Coordinatore) del CdS

SARDELLITTI Stefania

Organo Collegiale di gestione del corso di studio

Consiglio di Corso di Studio

Struttura didattica di riferimento ai fini amministrativi

Facoltà di SCIENZE
TECNOLOGICHE e
dell'INNOVAZIONE

Requisiti di Docenza e Docenti di riferimento

DOCENTI DI RIFERIMENTO

INCF	COGNOME	NOME	SETTORE	GSD	QUANTITÀ INSEGNAMENTI ASSOCIATI
1RSGPP57P12D969I	CORASANITI	Giuseppe	GIUR-17/A	12/GIUR-17	10
2LTLTZ85A69H926X	D'ALTILIA	Letizia	GIUR-14/A	12/GIUR-14	10
3SIMHL70S13F912X	DIIESU	Michele	GIUR-14/A	12/GIUR-14	10
4RNLSSE86P62A783S	FIORENZA	Elisa	STAT-01/A	13/STAT-01	10
5HRMLK	GHARBA	Molka	IINF-	09/IINF-	10

83D44Z3 52K	OUI		05/A	05	A
MRTBBR 71P60D 612P	MARTINI	Barbara	INFO- 01/A	01/INFO -01	P O
8GRNGL 73A30H 501G	SGROI	Angelo	INFO- 01/A	01/INFO -01	ti D

 È necessario indicare 4 tutor

 Tutti i requisiti docenti soddisfatti per il corso

Figure specialistiche aggiuntive			
COGNOME	NOME	QUALIFICA	ANNO INIZIO COLLABORAZIONE
Figure specialistiche del settore non indicati			

Tutor			
Nessuna Tipologia			
COGNOME	NOME	EMAIL	TIPO DOC./TIR.
Di Gennaro	Pellegrino	pellegrino.digenaro@multiverscity.it	Tutor tecnici 
LATORRE ALICE	FRANCESCA		Tutor dei corsi di studio 
MASTRANGELO	GIOVANNI		Tutor disciplinari 

Gruppo di gestione AQ

COGNOME	NOME
Bracchitta	Giorgia
D'Altilia	Letizia
Sardellitti	Stefania

Rappresentanti degli Studenti

COGNOME	NOME	EMAIL
Bracchitta	Giorgia	giorgia.bracchitta@studenti.unimercatorum.it

Il Corso di Studio in breve

Il Corso di Laurea magistrale in Sicurezza Informatica si propone di formare 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. Il corso di studio si caratterizza per un'offerta didattica interdisciplinare che raccoglie contributi dell'informatica, dell'ingegneria, della statistica, delle scienze giuridico-economiche e organizzative, insieme a conoscenze specifiche dei principali domini applicativi di protezione contro i cyber-attacchi, assicurando alle proprie laureate e ai propri laureati una formazione avanzata e completa in relazione alle fondamenta, alle metodologie, alle soluzioni scientifiche e tecnologiche relative alla sicurezza informatica. In particolare, la laurea magistrale in Sicurezza Informatica offre le conoscenze professionali adeguate, sia dal punto di vista tecnologico che normativo, per supervisionare e coordinare le politiche di sicurezza nell'ambito di complessi sistemi informatici, organizzare la protezione da cyber-attacchi, e gestire il recupero in caso di attacco avvenuto con successo. Il corso di laurea copre tutti gli argomenti fondamentali per la preparazione culturale di una laureata e di un laureato magistrale del settore, ed è progettato per essere seguito proficuamente da studentesse e studenti offrendo un ampio percorso formativo comune e garantendo l'omogeneità e la coerenza della formazione.

Progettazione del CdS

Si veda il "Documento di Progettazione del CdS".

Link inserito:

<https://www.unimercatorum.it/corso-di-studio-lm66-sicurezza-informatica-2025-2026>

Sintesi della relazione tecnica del nucleo di valutazione

Relazione Nucleo di Valutazione per accreditamento

Pdf inserito: [VERBALE NUCLEO DI VALUTAZIONE CON PARERE](#) 

Parere del comitato regionale di coordinamento

Non pertinente per i Corsi erogati in modalità 'D'

Consultazione con le organizzazioni rappresentative - a livello nazionale e internazionale - della produzione di beni e servizi, delle professioni (Istituzione del corso)



L'Ateneo ha strutturato un percorso organico e variegato per l'interlocuzione con le parti economiche e sociali, volto a:

- selezionare gli ambiti di competenza carenti;
- raccogliere i fabbisogni formativi;
- intercettare fabbisogni di professionalità collegati a futuri inserimenti nel mondo del lavoro.

Il metodo impostato, desumibile dalla Road Map inserita nel link a fondo pagina, consente di verificare come si sia inteso dar vita ad una vera e propria co-progettazione che accompagnerà il Corso di studio anche nella fase di avvio ed erogazione. L'Ateneo ha avviato una serie di azioni ulteriori di accompagnamento alla progettazione delle schede insegnamento, attraverso convegni e seminari ad hoc, che consentiranno di proseguire il lavoro di co-progettazione e consultazione delle Parti Sociali.

Il metodo di lavoro prevede la costituzione di un Comitato Proponente e di un Comitato di Indirizzo.

Il COMITATO PROPONENTE (CP) composto da professori Universitari di settore in servizio presso l'Ateneo e/o in quiescenza, ha il compito di:

- sovrintendere alle attività di progettazione e di assicurazione della qualità dei CdS;
- preparare e sottoporre agli Organi accademici le pratiche relative alla programmazione, coordinamento e verifica delle attività formative ivi compreso la proposta di RAD (Ordinamento Didattico);
- proporre alle strutture di Ateneo il calendario accademico, i programmi d'insegnamento e i programmi d'esame degli insegnamenti con i relativi

CFU, l'elenco delle attività didattiche elettive approvate, l'attribuzione dei compiti didattici ai singoli docenti.

Il lavoro del Comitato Proponente si interseca, si completa e si anima grazie alla interlocuzione con il COMITATO DI INDIRIZZO (CI). Il CI assume un ruolo fondamentale in fase progettuale al fine di assicurare il collegamento con il Mondo del Lavoro, valutare l'andamento dei Corsi, elaborare proposte di definizione e progettazione dell'offerta formativa e proposte di definizione degli obiettivi di apprendimento e suggerire indirizzi di sviluppo.

L'Ateneo si è dotato di Linee Guida per l'attivazione del Comitato di Indirizzo e ha elaborato anche un documento identificativo di ruoli, funzioni e timing di lavoro.

Il COMITATO DI INDIRIZZO dell'istituendo Corso di Laurea in "Sicurezza Informatica" ha operato:

- nel mese di novembre e dicembre 2023 attraverso consultazioni informali;
- tra dicembre 2023 e gennaio 2024 attraverso la compilazione di uno specifico questionario;
- 5 febbraio 2024 attraverso una prima riunione aperta di confronto e validazione delle figure professionali previste, degli sbocchi lavorativi e delle competenze associate alle singole funzioni;
- 13 febbraio 2024 attraverso una seconda riunione per discutere e approfondire i temi emersi nel primo incontro.

Le attività proseguiranno:

- ai fini della istituzione del corso nei mesi di febbraio e marzo 2024 per contribuire alla definizione dei contenuti formativi nelle schede insegnamento e per raccogliere le proposte in merito agli insegnamenti a scelta da attivare;
- con cadenza semestrale per aggiornare le istanze e i fabbisogni e contribuire alla manutenzione del corso.

In particolare, compongono il CI del Corso di Laurea "Sicurezza Informatica"

Il Segretario Generale di Eurispes, il Digital Advisor di Monrif.net, il Country Manager di VMware Italy, il Direttore Affari Generali della Fondazione Ugo Bordoni, il Direttore dell'Ufficio di vigilanza TIM, il Direttore Generale di Aci Informatica, il CEO di CYBHORUS, il Direttore generale di INFOCAMERE, il Direttore Generale del Centro Studi G. Tagliacarne, il già Prefetto della Prefettura di Alessandria e Consulente di Aci Informatica, il Già responsabile Cybersecurity dell'Agenzia Spaziale Europea (ESA), il già responsabile sicurezza di ISTINFORM, il Già responsabile della Scuola TLC e Cyberdefence della Marina Militare Centro Studi, il Già direttore dell'Istituto superiore comunicazioni e tecnologie dell'informazione, il già DG delegato della Segreteria per le Infrastrutture Critiche (Presidenza Consiglio Ministri 2010-13) e la Senior

Expert di FEDERTERZIARIO.

L'intensa collaborazione tra i due Comitati - Indirizzo e Proponente - ha portato alla progettazione della parte ordinamentale della SUA CdS, in seguito sottoposta alla valutazione delle Parti Sociali attraverso l'invio di un questionario di valutazione volto a identificare le componenti del Corso che le imprese valutano di interesse maggiore in termini di occupabilità futura, ovvero la domanda del mercato del lavoro, i profili professionali che ritengono di maggior interesse per le proprie attività, la loro reperibilità e quindi la necessità di tali profili professionali nel breve e lungo periodo.

Gli esiti del questionario sono stati confrontati ulteriormente con l'analisi documentale parallelamente condotta dal CP. Il questionario è stato indirizzato a incrociare le attitudini e le competenze previste per ogni professione individuata nella Scheda SUA con le esigenze espresse dai soggetti coinvolti.

Più in dettaglio, il CI ha portato avanti il dialogo con le Parti Sociali, richiedendo loro l'opinione in merito ai seguenti aspetti:

- a) adeguatezza degli obiettivi formativi del Corso di Studi;
- b) adeguatezza delle abilità /competenze fornite dal Corso di Studi ed eventuali modifiche da apportare;
- c) grado di rilevanza sulle conoscenze/competenze/abilità possedute dalle laureate e dai laureati;
- e) rispondenza dei risultati di apprendimento attesi, disciplinari/specifici e generici, in relazione al percorso formativo offerto, con richiesta di suggerimenti e critiche;
- f) rispondenza dei risultati di apprendimento attesi rispetto alle competenze richieste dalle figure professionali di riferimento.

Il risultato complessivo rispetto alle interazioni effettuate con le parti sociali è stato di grande soddisfazione, sia rispetto all'adeguatezza degli obiettivi formativi, alle conoscenze/abilità /competenze che si andranno a formare, all'adeguata rispondenza dei risultati di apprendimento attesi in relazione al percorso formativo offerto, sia in relazione alla soddisfacente rispondenza dei risultati di apprendimento attesi rispetto alle richieste di figure professionali di riferimento. In particolare sono state colte le nuove esigenze, anche connesse alle opportunità del Recovery Plan.

A partire da una ricognizione sulla figura dell'Esperta/o in Sicurezza Informatica in termini di conoscenze, competenze e prospettive, il Comitato di Indirizzo evidenzia, anche sulla base dei questionari raccolti, la assoluta necessità di tale figura professionale.

Suggerisce, inoltre, il Comitato di Indirizzo i seguenti spunti a cui si è dato seguito:

- prevedere che la laureata e il laureato magistrale abbiano la capacità di

saper gestire in maniera sicura i dati sensibili;

- opportunità di prevedere insegnamenti che permettano alla laureata e al laureato di interagire con figure professionali non afferenti al proprio settore di competenza.

L'analisi della domanda svolta seguendo le Linee guida di Ateneo proposte del Presidio di Qualità - è stata quindi indirizzata in tre direzioni:

- 1) consultazioni dirette attraverso la somministrazione di questionari;
- 2) giornate di co-progettazione anche attraverso la costituzione di un Comitato di Indirizzo;
- 3) analisi documentale e studi di settore.

La consultazione dei due Comitati - Indirizzo e Proponente - è stata effettuata dal Rettore, con il supporto del Direttore Generale, del Preside di Facoltà e degli Uffici Amministrativi preposti.

Viene reso disponibile il documento 'CONSULTAZIONE CON LE PARTI ECONOMICHE E SOCIALI PER L'ISTITUZIONE DEL CORSO DI LAUREA SICUREZZA INFORMATICA' che comprende i seguenti documenti:

- VERBALI DELLE RIUNIONI DEL COMITATO PROPONENTE E DEL COMITATO DI INDIRIZZO
- FORMAT DI QUESTIONARIO DI CONSULTAZIONE CON LE ORGANIZZAZIONI RAPPRESENTATIVE DELLA PRODUZIONE, DEI SERVIZI, DELLE PROFESSIONI
- SLIDE "LA PROGETTAZIONE DEL NUOVO CORSO DI LAUREA"
- ROAD MAP

Tutto l'iter è anche visionabile, per trasparenza, al seguente link:
<https://www.unimercatorum.it/lm-66-sicurezza-informatica>

Consultazione con le organizzazioni rappresentative - a livello nazionale e internazionale - della produzione di beni e servizi, delle professioni (Consultazioni successive)

Come evidenziato nel quadro A1.a, l'Ateneo ha intrapreso un percorso strutturato con le parti economiche e sociali, con l'obiettivo di individuare le esigenze formative e cogliere i fabbisogni di professionalità collegati a futuri inserimenti nel mondo del lavoro.

Dopo la fase iniziale di collaborazione progettuale, il Comitato di Indirizzo (CI) ha avuto un ruolo determinante suggerendo, a seguito delle consultazioni con le Parti Sociali, validi indirizzi di sviluppo per il Corso e promuovendo i contatti per gli stage degli studenti presso le aziende.

Il processo di consultazione prevede la somministrazione e la compilazione di specifici questionari da parte dei componenti del Comitato di Indirizzo. Il Coordinatore del corso di studi provvede in

seguito alla raccolta e alla sintesi dei risultati emersi, ponendoli all'attenzione del CI durante riunioni formali volte alla loro discussione e analisi.

I componenti del CI, l'elenco delle organizzazioni consultate, il format del questionario utilizzato per raccogliere pareri e le risultanze ottenute sono disponibili nel documento allegato ANALISI DELLA DOMANDA E VERBALI CI.

Sono stati, inoltre, formulati diversi commenti e/o suggerimenti, che si riportano per punti:

- a) Implementare una didattica multidisciplinare equilibrata tra insegnamenti giuridici e insegnamenti tecnici;
- b) Verificare attualità delle lauree richieste per l'ammissione al Cds ampliando eventualmente la platea dei laureati STEM;
- c) Avviare esperienze di laboratorio mirate a situazioni di crisi informatica e di resilienza;

Allegati allo stesso documento sono presenti i verbali delle riunioni tenute dal CI, svoltesi per valutare l'andamento della progettazione del Corso e discutere le opinioni raccolte durante le varie consultazioni. L'Ateneo ha avviato una serie di azioni ulteriori di accompagnamento alla progettazione delle schede insegnamento, attraverso convegni e seminari ad hoc, che consentiranno di proseguire il lavoro di co-progettazione e consultazione delle Parti Sociali.

Il Comitato di Indirizzo ha pianificato inoltre iniziative di orientamento, come Summer School, che mirano a favorire la consapevolezza dei discenti in ambito formativo. La proposta delle iniziative di orientamento del CdS è stata condivisa con tutti gli attori della progettazione del corso al fine di predisporre attività mirate e in linea con i profili culturali del CdS.

È stato predisposto infine un piano di monitoraggio e feedback che prevede un riesame annuale di ciascuna attività.

Certificazione sul materiale didattico e servizi offerti [corsi telematici]

Pdf inserito: 

Istituzione di più corsi nella classe



Gruppo di affinità

Gruppo: 1

**Delibera di ateneo relativa all'istituzione di ulteriori corsi nella
classe - 73**

Parte Testuale

Obiettivi formativi specifici del Corso e descrizione del percorso formativo, anche con riferimento ai descrittori di Dublino



La laurea magistrale in Sicurezza Informatica si propone di fornire conoscenze avanzate che contribuiscono a sviluppare capacità professionali necessarie sia allo svolgimento di attività di ricerca, progettazione, realizzazione, verifica, coordinamento e gestione di sistemi informatici, riferibili ai diversi campi di applicazione delle scienze e delle tecnologie informatiche nell'ambito della sicurezza e protezione dei sistemi, delle reti e delle infrastrutture informatiche, e al trattamento sicuro e riservato dei dati. La laureata e il laureato magistrale in Sicurezza Informatica sono anche in grado di svolgere attività di progettazione, realizzazione, verifica, manutenzione, monitoraggio 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 corso di laurea magistrale in Sicurezza Informatica si propone dunque di formare professionisti dotati di competenze scientifiche e tecnologiche di alto livello, di capacità metodologiche e operative e di visione aperta e critica delle problematiche connesse all'adozione e all'uso delle tecnologie informatiche.

Il corso di studi intende fornire a studentesse e studenti una preparazione di tipo multidisciplinare nel settore della cybersecurity, includendo tematiche di tipo economico, giuridico, statistico, informatico e dell'ingegneria dell'informazione, oltre a tematiche riguardanti la psicologia (se opzionato il relativo insegnamento dalle studentesse e dagli studenti).

Le competenze che la laureata e il laureato magistrale in Sicurezza Informatica acquisirà sono:

- capacità di progettare, implementare, validare e mantenere infrastrutture e sistemi informatici e di comunicazione sicuri, così

come gestire basi di dati e sistemi informativi evoluti in modo efficiente e sicuro;

- capacità di lavorare sia in autonomia che in gruppo, guidando progetti e prendendo decisioni;
- conoscenza dei principi di sicurezza dell'informazione, che includano quindi i principi e le pratiche di base della cybersecurity, nonché i principi e protocolli crittografici;
- conoscenza di metodi e tecniche di analisi dati basate su apprendimento automatico e modelli statistici, includendo le tecniche di machine/deep learning e processi stocastici;
- conoscenza di applicazioni ed aspetti avanzati della cybersecurity insieme ad aspetti di sicurezza di tecnologie quali mobile device, IoT, social network e impianti industriali;
- conoscenza di principi base di ambito giuridico, economico e psicologico (quest'ultimo nel caso in cui venga opzionato dalle studentesse e dagli studenti), quali: il rapporto tra processi cognitivi e computazione; interazione uomo- macchina; aspetti legali attinenti ai dati, al loro utilizzo, all'identità digitale e al diritto all'oblio;
- competenze di base per comprendere i processi di digital transformation delle imprese con particolare attenzione ai business model basati sui servizi (digital servitization);
- conoscenza di metodi e tecniche di prevenzione e gestione del rischio;
- capacità di comunicazione, sia in forma scritta che orale, in lingua inglese, con riferimento ai lessici disciplinari e tecnici.

Per tutti gli insegnamenti è prevista attività progettuale svolta attraverso la didattica interattiva, finalizzata allo sviluppo ed al test di soluzioni avanzate per problemi di complessità simili a quelli che la laureata e il laureato potrebbero affrontare nel mondo del lavoro.

L'impostazione didattica prevede che la formazione teorica sia accompagnata da: una rilevante attività sperimentale, lo svolgimento di progetti individuali e di gruppo, esercitazioni ed attività individuali in laboratorio virtuale, seminari, analisi di casi aziendali, il tutto al fine di stimolare la partecipazione attiva, l'attitudine propositiva, la capacità di elaborazione autonoma e di comunicazione dei risultati del lavoro svolto.

In ogni insegnamento previsto nel piano di studio il 25% della didattica erogata sarà sotto forma di laboratori virtuali per lo svolgimento di lezioni ed esercitazioni di laboratorio, attività progettuali autonome, e/o attività individuali in laboratorio virtuale.

Nell'ambito del corso di laurea magistrale in Sicurezza Informatica è previsto che la studentessa o lo studente segua, oltre ai tradizionali insegnamenti, anche altre attività individuali di specializzazione in laboratori virtuali utili per il Mondo del Lavoro. Queste attività mirano a creare competenze trasversali utili a completare il percorso formativo della studentessa e dello studente e a favorire il loro inserimento nel mondo del lavoro.

Il percorso formativo prevede innanzitutto l'apprendimento di strumenti e metodi di gestione di sistemi distribuiti, reti di comunicazioni, basi di dati e sistemi informativi evoluti e dei fondamenti di cybersecurity, anche con riferimento agli aspetti giuridici e economici. Grande importanza è data all'acquisizione di appropriati strumenti di ottimizzazione combinatoria per la gestione di infrastrutture di reti e alla conoscenza dei modelli computazionali dei processi cognitivi. Su queste tematiche nel I ANNO vengono erogati insegnamenti caratterizzanti INF/01 Informatica e ING-INF/03 Telecomunicazioni, oltre a SECS-S/01 Statistica, IUS/17 - Diritto penale, SECS-P/07 - Economia degli intermediari finanziari e ING-IND/35. Completano il primo anno il modulo di Altre attività per il mondo del lavoro e lo studio di una lingua straniera.

La preparazione viene approfondita negli ambiti informatici, di elaborazione delle informazioni e in quelli giuridici con l'erogazione nel II ANNO di insegnamenti di ING-INF/05 Sistemi di elaborazione delle informazioni, INF/01 Informatica e IUS/20 Filosofia del diritto. Completano la seconda annualità le attività formative affini e integrative, le attività a scelta dello studente e infine la prova finale.

Da ex QUADRO A4.b.1: Conoscenza e comprensione, e Capacità di applicare conoscenza e comprensione: Sintesi

Le laureate e i laureati magistrali del corso di Laurea Magistrale in Sicurezza Informatica devono:

- possedere le conoscenze informatiche adeguate ad operare efficientemente su infrastrutture e sistemi informatici;
- saper gestire basi di dati e sistemi informativi evoluti in modo efficiente e protetto, anche dal punto di vista giuridico,
- conoscere i principi di sicurezza dell'informazione, che includano quindi i principi e le pratiche di base della cybersecurity, nonché i principi e protocolli crittografici;
- conoscere gli strumenti di apprendimento automatico e modellazione statistica di processi, includendo le tecniche di machine/deep learning e processi stocastici;
- conoscere le applicazioni ed aspetti avanzati della cybersecurity, aspetti di sicurezza di tecnologie quali mobile device, IoT, social network e impianti industriali.
- possedere conoscenze in almeno uno dei seguenti ambiti giuridico, psicologico ed economico, quali ad esempio: il rapporto tra processi cognitivi e computazione; interazione uomo- macchina; aspetti legali legati ai dati, al loro utilizzo, all'identità digitale e al diritto all'oblio; competenze teoriche e tecniche di base per comprendere i processi di digital transformation delle imprese con particolare attenzione ai business model basati sui servizi (digital servitization);

- possedere conoscenze di prevenzione e gestione del rischio.

Le conoscenze e la capacità di comprenderne le problematiche sottostanti, sono acquisite dalle studentesse e dagli studenti attraverso:

- lezioni teoriche, esercitazioni e analisi di casi di studio;
- attività di didattica interattiva (che le studentesse e gli studenti devono essere capaci di completare operando anche autonomamente);
- attività di laboratorio virtuale, nonché moduli di Altre Conoscenze per il Mondo del Lavoro.

La verifica della conoscenza e della capacità di comprensione raggiunta avviene entro ogni insegnamento, sia nelle prove di esame individuale che in verifiche in itinere basate su colloquio integrato da prove pratiche e/o scritte e su attività progettuali e di laboratorio virtuale. Per le attività di didattica interattiva la verifica avviene anche in occasione della presentazione di una relazione sull'attività o progetto svolto.

Le laureate e i laureati magistrali del corso di studi dovranno essere in grado di applicare le conoscenze e le competenze acquisite all'analisi, al progetto, alla realizzazione e alla valutazione di sistemi informatici sicuri e protetti operanti in diversi ambiti applicativi quali ad esempio: commerciale, industriale, pubblica amministrazione, assicurativo, bancario, finanziario, ospedaliero, ambientale, energetico, ricerca.

Essi dovranno altresì essere in grado di impiegare gli strumenti conoscitivi sviluppati durante il corso di studi per analizzare e valutare da un punto di vista professionale e nell'ambito di imprese, di centri di ricerca pubblici e privati, di organismi governativi, nonché di autorità di controllo e di garanzia la correttezza e la conformità di scelte progettuali nonché gli effetti di decisioni sul corretto funzionamento di sistemi informatici e le necessarie garanzie di protezione dei dati, operando nell'ambito di imprese, centri di ricerca, etc...

Le laureate e i laureati magistrali del corso dovranno quindi essere in grado di integrare le conoscenze acquisite in insegnamenti e contesti diversi, valutare criticamente e scegliere modelli e metodi di soluzione.

Queste capacità sono fornite alle studentesse e agli studenti attraverso lo studio critico di testi avanzati, supportato da attività curriculari e complementari. Tali attività, guidate dai docenti mediante le ore dedicate alla didattica interattiva, includono la discussione di casi di studio, l'attività di laboratorio virtuale, l'elaborazione di progetti anche di gruppo, la discussione di problemi di frontiera, le attività di tipo seminariale su argomenti di ricerca.

La tesi di laurea magistrale, che può essere svolta anche in contesti aziendali o centri di ricerca avanzata, consente alla studentessa e allo

studente di applicare le conoscenze acquisite a problemi concreti e lo abitua ad un processo di valutazione di soluzioni caratterizzato da tempi ristretti di realizzazione e da specifici vincoli di progetto.

La verifica della capacità di applicare conoscenza e comprensione avviene attraverso la valutazione della documentazione prodotta a corredo di tali attività.

Da ex QUADRO A4.c: Autonomia di giudizio, Abilità comunicative, Capacità di apprendimento

Le laureate e i laureati magistrali del corso dovranno acquisire una piena capacità di formulare giudizi autonomi e consapevoli in merito alle decisioni ed alle scelte progettuali delle imprese, delle organizzazioni e degli enti in cui si trovassero a operare. Essi dovranno anche assimilare appieno i principi di deontologia professionale che guidano le relazioni interpersonali nei contesti occupazionali di riferimento nei quali potranno imbattersi nella vita professionale successiva al conseguimento della laurea magistrale. Inoltre, le laureate e i laureati magistrali dovranno essere consapevoli dei principi di etica professionale somministrati al fine di utilizzare le tecniche di attacco apprese solo al fine di migliorare il livello di sicurezza informatica di una organizzazione.

Risultati di apprendimento attesi:

- capacità di ragionare criticamente e di porre in discussione scelte progettuali e implementative;
- capacità di sviluppare ragionamenti e riflessioni autonome e indipendenti;
- consapevolezza dell'esistenza di diversi approcci metodologici alternativi per la progettazione e realizzazione di sistemi, comprensione della rilevanza di tale pluralità;
- capacità di valutare criticamente rilevanza e meriti di progetti di un sistema tra loro alternativi;
- capacità di valutare e interpretare criticamente il comportamento di sistemi complessi.

Lo sviluppo della capacità critica di giudizio delle studentesse e degli studenti avviene durante le lezioni e le esercitazioni, nell'ambito delle attività di didattica interattiva, delle attività di laboratorio virtuale ed, in particolar modo, durante il periodo di tesi.

La verifica della capacità di giudizio avviene attraverso le prove d'esame, anche in itinere, e la valutazione della documentazione prodotta a corredo delle attività di didattica interattiva e della prova finale.

Le laureate e i laureati magistrali del corso di laurea magistrale in Sicurezza Informatica dovranno essere in grado di argomentare le proprie posizioni e di comunicare gli esiti delle proprie analisi e

valutazioni in modo chiaro ed efficace, utilizzando la lingua di lavoro più diffusa nei contesti lavorativi internazionali di riferimento (inglese) e avvalendosi, con piena padronanza tecnica, dei più aggiornati strumenti informatici, nonché degli strumenti più avanzati (informatici, matematici, statistici, econometrici) per l'analisi, l'elaborazione e la presentazione di dati.

Risultati di apprendimento attesi:

1. capacità di comunicazione scritta, fondata sull'impiego di terminologia e linguaggi tecnici appropriati.
2. capacità di presentare e valutare criticamente per iscritto in maniera chiara, coerente e concisa idee e argomentazioni tecniche e metodologiche.
3. capacità di formulare ed esprimere oralmente, anche in contesti pubblici, argomentazioni complesse in campo tecnico e metodologico.
4. 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.

Lo sviluppo delle abilità comunicative avviene nell'arco di tutto il corso di studio: in occasione di webinar tra studentesse/studenti e docenti, nelle attività di didattica interattiva, nonché durante l'attività relativa alla prova finale.

La verifica di tali abilità avviene attraverso la valutazione di ciò che viene espresso dalle studentesse e dagli studenti in forma orale e/o scritta sia durante le prove intermedie e la prova d'esame dei singoli insegnamenti che in occasione delle attività di didattica interattiva e della prova finale.

Il corso di laurea magistrale si propone di condurre le proprie studentesse e i propri studenti, sia pure in maniera graduale, sino alla frontiera della ricerca negli ambiti disciplinari di riferimento. Proprio per questa ragione il corso intende favorire in maniera prioritaria lo sviluppo di capacità di ulteriore apprendimento da parte delle studentesse e degli studenti, nonché l'acquisizione di abilità e competenze metodologiche e teoriche che consentano alle proprie laureate e ai propri laureati magistrali di intraprendere in maniera autonoma attività di approfondimento e ricerca scientifica secondo standard internazionali, anche al fine di un'eventuale prosecuzione degli studi nell'ambito di programmi di dottorato in campo Informatico e in altri campi affini.

Risultati di apprendimento attesi:

- capacità di organizzare le proprie idee in maniera critica e sistematica;
- capacità di identificare, selezionare e raccogliere informazioni mediante l'uso appropriato delle fonti rilevanti;
- capacità di utilizzare biblioteche, banche dati, archivi e repertori cartacei ed elettronici per accedere alle informazioni scientifiche e

documentarie rilevanti;

- capacità di organizzare e realizzare un piano di studio indipendente;
- capacità di riflettere sulla propria esperienza di apprendimento e di adattarla in risposta a suggerimenti e stimoli da parte dei docenti o dei colleghi;
- capacità di riconoscere la necessità di ulteriori studi e di apprezzare il ruolo di modalità di apprendimento innovative e di attività aggiuntive di ricerca;
- capacità di progettare ed elaborare un lavoro di ricerca indipendente, ancorché guidato da un supervisore.

Lo sviluppo delle capacità di apprendimento avviene nell'arco di tutto il corso di studio, difatti tutte le attività previste (lezioni, esercitazioni, attività di laboratorio, attività di didattica interattiva da soli o in gruppo, tesi di laurea) concorrono al progressivo aumento delle capacità di apprendimento.

La verifica a sua volta avviene in tutte le fasi del corso di studio, iniziando dalle prove d'esame, passando dalle verifiche delle attività di didattica interattiva e in occasione della prova finale.

Profilo e sbocchi



Profilo professionale e sbocchi occupazionali e professionali previsti per i laureati

Nome della figura professionale formata: ESPERTA/O IN SICUREZZA INFORMATICA

Funzione in un contesto di lavoro e competenze:

L'Esperta/o in Sicurezza Informatica supervisiona e coordina le politiche di sicurezza informatica, in particolare quelle legate al sistema di gestione dell'informazione di una azienda, alla comunicazione, all'aspetto normativo, e all'individuazione di standard di sicurezza. Si tratta quindi di un esperta/o tecnologica/o che opera all'interno di una organizzazione per la protezione da attacchi informatici nelle varie fasi di prevenzione, scoperta, mitigazione e recupero da un attacco. La sua specializzazione include anche la conoscenza di tecniche di sicurezza attiva per poter operare eventualmente in modo appropriato nella mitigazione. In concreto si occupa di:

- Definire strategia e standard della sicurezza informatica

aziendale;

- Contribuire alla stesura delle policy di sicurezza;
- Valutare rischi, minacce e possibili conseguenze;
- Stabilire e gestire il piano di Incident Response.

COMPETENZE

L'Esperta/o in Sicurezza Informatica deve possedere le seguenti competenze per svolgere le funzioni nel contesto di lavoro nel quale andrà ad operare:

- competenze nella definizione e implementazione di programmi di governance e controllo della sicurezza delle informazioni;
- competenze nella gestione del rischio, continuità operativa e disaster recovery;
- competenze nella prevenzione dallo spionaggio industriale e in materia di privacy e protezione dei dati;
- competenze e conoscenza dei principali sistemi informatici e infrastrutture aziendali;
- competenze nell'identificazione dei processi operativi e nella definizione del livello di tolleranza al rischio;
- competenze manageriali di definizione delle attività da svolgere e delle risorse a cui assegnarle;
- capacità di monitorare la spesa per i progetti di sicurezza e il relativo ROI- Return on investment.

Sbocchi occupazionali:

La laureata e il laureato magistrale possono ricoprire il ruolo di Esperta/o in Sicurezza Informatica in:

- aziende di prodotti e servizi;
- enti della pubblica amministrazione;
- ambiti di consulenza per l'erogazione di servizi per la PA e i privati;
- enti di ricerca pubblici e privati.

Il corso prepara alla professione di (codifiche ISTAT)

1. Analisti di sistema - (2.7.1.1.2.)
2. Analisti e progettisti di applicazioni web - (2.7.1.1.3.)
3. Analisti e progettisti di basi dati - (2.7.2.1.2.)
4. Amministratori di sistemi - (2.7.2.1.3.)
5. Analisti e progettisti di software - (2.7.1.1.1.)
6. Specialisti in reti e comunicazioni informatiche - (2.7.2.1.1.)
7. Specialisti in sicurezza informatica - (2.7.2.1.4.)

Conoscenze richieste per l'accesso



L'accesso al corso è diretto per le laureate e i laureati nelle classi L8 (Ingegneria dell'Informazione) e L31 (Scienze e Tecnologie Informatiche), o di altro titolo di studio conseguito all'estero, riconosciuto idoneo.

Le laureate e i laureati in altre discipline devono aver acquisito almeno 66 CFU nell'insieme dei seguenti settori:

27 CFU tra:

ING-INF/05 - Sistemi di elaborazione delle informazioni; INF/01 - Informatica.

33 CFU tra:

ING-INF/01 - Elettronica;
ING-INF/02 - Campi elettromagnetici;
ING-INF/03 - Telecomunicazioni;
ING-INF/04 - Automatica;
ING-IND/31 - Elettrotecnica;
FIS/01 - Fisica sperimentale;
MAT/02 - Algebra;
MAT/03 - Geometria;
MAT/05 - Analisi matematica;
MAT/06 - Probabilità e statistica matematica; MAT/08 - Analisi numerica;
MAT/09 - Ricerca Operativa SECS-S/01 – Statistica;
SECS-S/02 – Statistica per la ricerca sperimentale e tecnologica.

6 CFU tra:

ING-IND/35 - Ingegneria Economico-Gestionale; SECS-P/06 Economia Applicata;
SECS-P/07 - Economia aziendale;
SECS-P/08 Economia e Gestione delle Imprese SECS-P/10 Organizzazione Aziendale;
IUS/01 Diritto Privato;
IUS/10 Diritto Amministrativo.

Inoltre, la studentessa e lo studente devono 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).

Il Regolamento Didattico, oltre a stabilire le modalità di ammissione delle studentesse e degli studenti in possesso di titolo di studio estero, identifica le modalità di verifica della personale preparazione.

Modalità di ammissione

L'accesso al Corso di Laurea Magistrale è diretto per le laureate e i laureati nelle classi L8 (Ingegneria dell'Informazione) e L31 (Scienze e Tecnologie Informatiche), o di altro titolo di studio conseguito all'estero, riconosciuto idoneo.

L'iscrizione al Corso di Laurea Magistrale è subordinata al superamento del test d'ingresso. Sono esonerati dallo svolgimento del test gli studenti già laureati (nelle classi di laurea pertinenti) presso Universitas Mercatorum o che abbiano conseguito la Laurea triennale, anche presso altri Atenei, con una votazione non inferiore a 90/110.

Se viene accertata la mancanza di eventuali requisiti curriculari, lo studente potrà acquisirli iscrivendosi a opportuni 'Corsi Singoli' e superando i relativi esami di profitto prima dell'iscrizione al Corso di Laurea Magistrale.

Per approfondimenti consultare il "Regolamento requisiti di ammissione ai corsi di studio" sul sito istituzionale.

Link: <https://www.unimercatorum.it/offerta-formativa-2026-2027>

Caratteristiche della prova finale



La prova finale (tesi di Laurea Magistrale) consiste nella preparazione e discussione di un'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. Il caso sarà sviluppato nell'ambito delle discipline del Corso di Studio.

L'elaborato è corredato da presentazione multimediale, discussa dal candidato durante lo svolgimento della prova finale di fronte ad un'apposita Commissione.

La laureanda o il laureando dovrà dimostrare capacità di operare in modo autonomo, padronanza dei temi trattati e attitudine alla sintesi nel comunicare i contenuti e nel sostenere una discussione.

Modalità di svolgimento della prova finale

Le modalità di svolgimento della prova finale con le indicazioni operative, la struttura della commissione e le modalità di attribuzione del voto finale sono definite nel "Regolamento del Corso di Studio" e nel "Regolamento della Prova Finale e della Tesi di Laurea e determinazione del voto di Laurea".

Link: <https://www.unimercatorum.it/offerta-formativa-2026-2027>

Parte Tabellare

Attività caratterizzanti



Ambito Disciplinare	Settore	CFU		min da D.M. per l'ambito
		min	MAX	
Formazione scientifica	MATH-01/A Logica matematica MATH-06/A Ricerca operativa PHYS-03/A Fisica sperimentale della materia e applicazioni PHYS-04/A Fisica teorica della materia, modelli, metodi matematici e applicazioni STAT-01/A Statistica STAT-01/B Statistica per la	6	15	-

	ricerca sperimentale e tecnologica			
Formazione informatica	IINF-05/A Sistemi di elaborazione delle informazioni INFO-01/A Informatica	24	36	24
Formazione tecnologica, aziendale, economica, giuridica, etica, psicologica e sociale	ECON-06/A Economia aziendale ECON-08/A Organizzazione aziendale GIUR-01/A Diritto privato GIUR-02/A Diritto commerciale GIUR-09/A Diritto internazionale GIUR-14/A Diritto penale GIUR-17/A Filosofia del diritto GSPS-06/A Sociologia dei processi culturali e comunicativi IEGE-01/A Ingegneria economico-gestionale IINF-03/A Telecomunicazioni	30	42	-
Minimo di crediti riservati dall'ateneo minimo da D.M. 48:		-		

Totale Attività Caratterizzanti	60 - 93
--	---------

Attività affini



Ambito Disciplinare

CFU

Ambito Disciplinare	CFU	
	min	MAX
Attività formative affini o integrative	12	18
Minimo di crediti riservati dall'ateneo:	-	

Totale Attività Affini	12 - 18
-------------------------------	---------

Descrizione sintetica delle attività affini o integrative



Le attività affini relative all'ambito SECS-S/03 Statistica Economica sono poste al fine di formare specialisti in grado di utilizzare sistemi analitici e telematici per raccogliere informazioni, elaborarle, ricavarne indicazioni economico-strategiche, distribuirle ai giusti livelli di dettaglio e con le modalità tecnologiche più opportune.

Le attività affini riguardanti PSI/03 Psicometria offrono la possibilità di formare specialisti in grado di individuare le tecniche appropriate per l'analisi dei dati in diversi contesti di ricerca e di usare tale capacità, con l'ausilio degli appropriati strumenti informatici, per giungere a conclusioni sulla base dei dati disponibili.

Altre attività



Ambito Disciplinare		CFU	
		min	MAX
A scelta dello studente		9	12
Per la prova finale		12	15
Ulteriori attività formative (art. 10, comma 5, lettera d)	Ulteriori conoscenze linguistiche	3	6
	Abilità informatiche e telematiche	-	-

	Tirocini formativi e di orientamento	-	-
	Altre conoscenze utili per l'inserimento nel mondo del lavoro	3	6
Minimo di crediti riservati dall'ateneo alle Attività art. 10, comma 5 lett. d			
Per stages e tirocini presso imprese, enti pubblici o privati, ordini professionali		-	-
Totale Altre Attività		27 - 39	

Raggruppamento settori


Per modificare il raggruppamento dei settori

Riepilogo CFU


CFU totali per il conseguimento del titolo	120
Range CFU totali del corso	99 - 150

Massimo numero di crediti riconoscibili (D.M. n. 931/2024)	24
---	-----------

Eventuale articolazione curriculare inclusi eventuali orientamenti/indirizzi
(ex Eventuali Curriculum)

Non sono previsti curricula

Offerta Didattica Programmata

Attività caratterizzanti	Settore	CFU Ins	CFU Off	CFU Rad
Formazione scientifica	STAT-01/A Statistica <i>Statistical Learning e Analisi dei Big Data (1 anno) - 9 CFU - obbl</i>	9	9	6 - 15
Formazione informatica	IINF-05/A Sistemi di elaborazione delle informazioni <i>Cybersecurity (2 anno) - 9 CFU - obbl</i> <i>Informatica Forense e Sicurezza dell'IA (2 anno) - 9 CFU - obbl</i> INFO-01/A Informatica <i>Sicurezza e protezione dei dati e dei sistemi informatici (1 anno) - 9 CFU - obbl</i> <i>Principi e Metodi di Crittografia (2 anno) - 6 CFU - obbl</i>	33	33	24 - 36
Formazione tecnologica, aziendale, economica,	ECON-06/A Economia aziendale <i>Gestione del rischio e continuità</i>	39	39	30 - 42

giuridica, etica, psicologica e sociale	<i>operativa (1 anno) - 6 CFU - obbl</i>			
	GIUR-14/A Diritto penale			
	<i>Elementi di diritto penale e criminalità informatica (1 anno) - 9 CFU - obbl</i>			
	GIUR-17/A Filosofia del diritto			
	<i>Informatica giuridica ed etica digitale (2 anno) - 6 CFU - obbl</i>			
	IEGE-01/A Ingegneria economico-gestionale			
	<i>Economia e gestione dell'innovazione (1 anno) - 9 CFU - obbl</i>			
	IINF-03/A Telecomunicazioni			
	<i>Tecnologie e sicurezza delle reti di comunicazione (1 anno) - 9 CFU - obbl</i>			
Minimo di crediti riservati dall'ateneo: -				
(minimo da D.M. 48)				
Totale attività caratterizzanti		81	60	- 93

Attività affini	Settore	CFU Ins	CFU Off	CFU Rad
Attività		24	12	12

formative affini o integrative	PSIC-01/C Psicometria		-
	<i>Modelli multidimensionali per l'analisi dei dati (2 anno) - 12 CFU</i>		18
			mi n
			12
	STAT-02/A Statistica economica		
	<i>Metodi Statistici per l'Economia Digitale (2 anno) - 12 CFU</i>		
Totale attività Affini		12	12 - 18

Altre attività		CFU	CFU Rad
A scelta dello studente		9	9 - 12
Per la prova finale		12	12 - 15
Ulteriori attività formative (art. 10, comma 5, lettera d)	Ulteriori conoscenze linguistiche	3	3 - 6
	Abilità informatiche e telematiche	-	-
	Tirocini formativi e di orientamento	-	-
	Altre conoscenze utili per l'inserimento nel mondo del lavoro	3	3 - 6
Minimo di crediti riservati dall'ateneo alle Attività art. 10, comma 5 lett. d			
Per stages e tirocini presso imprese, enti pubblici o privati, ordini professionali		-	-
Totale Altre Attività		27	27 - 39

CFU totali per il conseguimento del titolo	120	
CFU totali inseriti	120	99 - 150

Regolamento Didattico del CdS

Pdf inserito: 

Indicazione dei piani di studio offerti agli studenti

Pdf inserito: 

Matrice di Tuning

Area Informatica

Conoscenza e comprensione

La laureata e il laureato acquisiscono un solido bagaglio di conoscenze di Area informatica relative a:

- tecniche crittografiche di base per la protezione dei dati da agenti non autorizzati
- protocolli per l'identificazione e la comunicazione sicura
- gestione della sicurezza per reti cablate e wireless
- tecnologie di sicurezza più utilizzate in Internet e nelle reti aziendali
- gestione della vulnerabilità della sicurezza nell'ambito delle basi di dati, e della protezione e privacy dei dati
- principali caratteristiche degli attacchi informatici contro i principali sistemi operativi
- metodologie di secure software engineering
- secure software deployment basato su cloud e su container, e sicurezza nell'edge e fog computing
- architetture e tecnologie di sviluppo di moderni sistemi di gestione dell'informazione, modelli e metodi per la gestione di dati non relazionali, semistrutturati e non strutturati.

Capacità di applicare conoscenza e comprensione

Le conoscenze di Area informatica consentono di:

- applicare i principali algoritmi di sicurezza informatica, e impiegare meccanismi protettivi in contesti applicativi
- applicare le tecniche crittografiche per la protezione dei dati, e comprendere i protocolli per l'identificazione e la comunicazione sicura
- contribuire alla progettazione di reti informatiche sicure
- valutare la sicurezza delle reti esistenti
- applicare le soluzioni tecnologiche per garantire la privacy e la protezione dati in diversi scenari
- scegliere il metodo di analisi più adeguato a comprendere le funzionalità di un programma malevolo
- valutare il codice software e le applicazioni al fine di identificare le vulnerabilità
- implementare opportune attività che garantiscano la sicurezza nel corso di tutte le fasi del ciclo di vita del software
- applicare le nuove modalità di organizzazione, integrazione, gestione e reperimento di informazioni per la realizzazione di applicazioni in vari domini inclusi il Web of Data, il Semantic Web.

Curriculum di riferimento:

Statutario

Le conoscenze e capacità sono conseguite e verificate nelle seguenti attività formative:

Anno di corso 1 - Sicurezza e protezione dei dati e dei sistemi informatici (cfu 9 - 0662509INF01 - E82616626002) [url](#)

Anno di corso 1 - Tecnologie e sicurezza delle reti di comunicazione (cfu 9 - 0662509INGINF03 - E82616626004) [url](#)

Anno di corso 2 - Cybersecurity (cfu 9 - 0662509INGINF05 - E82616626009) [url](#)

Anno di corso 2 - Informatica Forense e Sicurezza dell'IA (cfu 9 - 0662509INGINF05I - E82616626012) [url](#)

Anno di corso 2 - Principi e Metodi di Crittografia (cfu 6 - 0662506INF01 - E82616626011) [url](#)

Area Economico-Analitica e Gestionale

Conoscenza e comprensione

La laureata e il laureato acquisiscono un solido bagaglio di conoscenze che si collocano nell'Area economico-analitica e gestionale relative a:

- attendibilità del dato informatico, e sua individuazione, raccolta, trasporto, acquisizione e conservazione ai fini della analisi forense digitale
- gestione di dati e elaborazione di modelli per l'analisi organizzativa di un sistema aziendale e per l'analisi competitiva dell'ambiente in cui l'azienda opera

- framework concettuali e regolamentari in materia di rischio, della composizione del capitale e della gestione delle banche

Capacità di applicare conoscenza e comprensione

Le conoscenze nell'Area economico-analitica e gestionale consentono di:

- applicare modelli concettuali per l'indagine conoscitiva e la diagnosi funzionale di sistemi organizzativi semplici, con particolare attenzione ai sistemi aziendali ed al settore dell'ICT
- applicare sistemi di gestione innovativa dei progetti all'organizzazione dei processi di sviluppo di nuovi prodotti e servizi
- applicare le principali misure dei rischi quantificabili relativi alla gestione delle banche
- analizzare le varie prospettive ed i metodi della ricerca e dell'analisi di dati, in modo da comprenderne non soltanto gli aspetti teorici ma anche i possibili risvolti applicativi

Curriculum di riferimento:
Statutario

Le conoscenze e capacità sono conseguite e verificate nelle seguenti attività formative:

Anno di corso 1 - Economia e gestione dell'innovazione (cfu 9 - 0662609INGIND35 - E82616626003) [url](#)

Anno di corso 1 - Gestione del rischio e continuità operativa (cfu 6 - 0662506SECSP07 - E82616626006) [url](#)

Anno di corso 1 - Statistical Learning e Analisi dei Big Data (cfu 9 - 0662509SECSS01 - E82616626001) [url](#)

Anno di corso 2 - Metodi Statistici per l'Economia Digitale (cfu 12 - 0662512SECSS03 - E82616626014) [url](#)

Anno di corso 2 - Modelli multidimensionali per l'analisi dei dati (cfu 12 - 0662512MPSIO3 - E82616626013) [url](#)

Area Etico-Giuridica

Conoscenza e comprensione

La laureata e il laureato acquisiscono un solido bagaglio di conoscenze che si collocano nell'Area etico-giuridica relative a:

- problemi giuridici legati all'uso e allo sviluppo delle tecnologie informatiche nel contesto normativo internazionale
- comprensione dei dati che risultano di interesse nei processi forensi e individuazione dell'ordine di importanza degli stessi da presentare all'autorità giudiziaria
- categorie generali dell'innovazione applicata al diritto e alla formazione del ragionamento giuridico, con particolare riferimento alle tematiche della logica giuridica nella transizione digitale
- l'uso responsabile degli strumenti digitali nell'ambito delle professioni giuridiche, con particolare riferimento all'etica, alla resilienza e alla sicurezza digitale

Capacità di applicare conoscenza e comprensione

Le conoscenze nell'Area etico-giuridica consentono di:

- gestire le principali problematiche connesse all'utilizzazione e allo sviluppo di tecnologie informatiche: copyright/diritto d'autore, proprietà industriale, stipula di contratti software, regolamentazione di privacy e sicurezza, firme elettroniche/digitali e documenti informatici, commercio elettronico, reati informatici
- seguire con consapevolezza situazioni dibattimentali nell'ambito dell'analisi forense digitale, con comprensione dei ruoli e delle dinamiche processuali.

Curriculum di riferimento:
Statutario

Le conoscenze e capacità sono conseguite e verificate nelle seguenti attività formative:

Anno di corso 1 - Elementi di diritto penale e criminalità informatica (cfu 9 - 0662509IUS17 - E82616626005) [url](#)

Anno di corso 2 - Informatica giuridica ed etica digitale (cfu 6 - 0662506IUS20 - E82616626010) [url](#)

Offerta Didattica Erogata

N.	Sede	Coorte	CUIN	Insegnamento	Settori insegnamento	Docente	Settore docente	Ore di didattica assistita
1		2026	E826 1662 6015	A scelta a dello studente	Non e' stato indicato il settore dell'attività formativa	Docente non specificato		72
2		2026	E826 1662 6008	Altre conoscenze utili per l'inserimento nel mondo del lavoro	Non e' stato indicato il settore dell'attività formativa	Docente non specificato		24
3		2026	E826 1662 6009	Cybersecurity	IINF-05/A	Docente di riferimento Barbara	INFO - 01/A	72

						MAR TINI <i>Profe ssore Ordin ario (L. 240/ 10)</i>		
4		2026	E826 1662 6003	Econ omia e gesti one dell'i nnov azion e	IEGE - 01/A	Doce nte non speci ficat o		72
5		2026	E826 1662 6005	Elem enti di diritt o pena le e crimi nalit à infor mati ca	GIUR - 14/A	Doce nte di riferi ment o Letizi a D'AL TILIA <i>Ricer cator e a t.d.- t.pien o (L. 79/2 022)</i>	GIUR - 14/A	72
6		2026	E826 1662 6005	Elem enti di diritt o pena le e crimi nalit à infor	GIUR - 14/A	Doce nte di riferi ment o Mich ele DIIES U <i>Attivi</i>	GIUR - 14/A	72

				matematica		<i>ta' di insegnamento (art. 23 L. 240/10)</i>		
7		2026	E826 1662 6006	Gestione del rischio e continuità operativa	ECON-06/A	Docente non specificato		48
8		2026	E826 1662 6012	Informatica Forense e Sicurezza dell'IA	IINF-05/A	Docente di riferimento Molka GHARRBA OUI Professore Associato (L. 240/10)	IINF-05/A	72
9		2026	E826 1662 6010	Informatica giuridica ed etica digitale	GIUR-17/A	Docente di riferimento Giuseppe CORASANI Professore	GIUR-17/A	48

						ssore Ordin ario (L. 240/ 10)		
10		2026	E826 1662 6014	Meto di Stati stici per l'Eco nomi a Digit ale	STAT - 02/A	Doce nte non speci ficat o		96
11		2026	E826 1662 6013	Mod elli multi dime nsio nali per l'ana lisi dei dati	PSIC - 01/C	Doce nte non speci ficat o		96
12		2026	E826 1662 6011	Princ ipi e Meto di di Critt ograf ia	INFO - 01/A	Doce nte di riferi ment o Ange lo SGR OI Attivi ta' di inseg name nto (art. 23 L. 240/ 10)	INFO - 01/A	48

13		2026	E826 1662 6016	Prova finale	Non e' stato indicato il settore dell'attivita' formativa	Docente non specificato		96
14		2026	E826 1662 6002	Sicurezza protezione dei dati e dei sistemi informatici	INFO - 01/A	Docente non specificato		72
15		2026	E826 1662 6001	Statistica I Learning e Analisi dei Big Data	STAT - 01/A	Docente di riferimento Elisa FIORENZA <i>Ricercatore a t.d.-t.defin. (L. 79/2022)</i>	STAT - 01/A	72
16		2026	E826 1662 6001	Statistica I Lear	STAT - 01/A	Docente non speci		72

				ning e Anali si dei Big Data		ficat o		
17		2026	E826 1662 6007	Ulter iori cono scen ze lingu istic he	Non e' stato indic ato il setto re dell'a ttivit a' form ativa	Doce nte non speci ficat o		24
							ore totali	1128

Didattica programmata per coorte

Sono garantiti i collegamenti informatici alle pagine del portale di ateneo dedicate a queste informazioni.

N.	Settori	Anno di corso	Insegnamento	Cognome Nome	Ruolo	Crediti	Ore	Docente di riferimento per corso
1.	NN	Anno di corso 1	Altre cono scen ze utili per l'inse rime nto nel mon do del			3	24	

			lavoro link					
2.	IEGE - 01/A	Anno di corso 1	Economia e gestione dell'innovazione link			9	72	
3.	GIUR - 14/A	Anno di corso 1	Elementi di diritto penale e criminalità informatica link	D'ALTILIA LETIZIA	RD	9	72	
4.	GIUR - 14/A	Anno di corso 1	Elementi di diritto penale e criminalità informatica link	DIIES UMICHELE	ID	9	72	
5.	ECON- 06/A	Anno di corso 1	Gestione del rischio e continuità			6	48	

			oper ativa link					
6.	INFO - 01/A	Anno di corso 1	Sicur ezza e prote zione dei dati e dei siste mi infor mati ci link			9	72	
7.	STAT - 01/A	Anno di corso 1	Stati stical Lear ning e Anali si dei Big Data link			9	72	
8.	STAT - 01/A	Anno di corso 1	Stati stical Lear ning e Anali si dei Big Data link	FIOR ENZ A ELIS A	RD	9	72	
9.	IINF- 03/A	Anno di corso 1	Tecn ologi e e sicur ezza delle reti di com			9		

			unica zione link					
10.	NN	Anno di corso 1	Ulteri ori cono scen ze lingui stich e link			3	24	
11.	NN	Anno di corso 2	A scelt a dello stud ente link			9	72	
12.	IINF- 05/A	Anno di corso 2	Cybe rsecu rity link	MAR TINI BAR BAR A	PO	9	72	
13.	IINF- 05/A	Anno di corso 2	Infor mati ca Fore nse e Sicur ezza dell'I A link	GHA RBA OUI MOL KA	PA	9	72	
14.	GIUR - 17/A	Anno di corso 2	Infor mati ca giuri dica ed etica digit ale link	COR ASA NITI GIUS EPPE	PO	6	48	
15.	STAT - 02/A	Anno di	Metodi di Stati			12	96	

		corso 2	stici per l'Eco nomi a Digit ale link					
16.	PSIC - 01/C	Anno di corso 2	Mod elli multi dime nsion ali per l'anal isi dei dati link			12	96	
17.	INFO - 01/A	Anno di corso 2	Princ ipi e Meto di di Critt ograf ia link	SGR OI ANG ELO	ID	6	48	
18.	NN	Anno di corso 2	Prov a final e link			12	96	

Calendario del Corso di Studio e orario delle attività formative

Calendario del Corso di Studio e orario delle attività formative

<https://www.unimercatorum.it/offerta-formativa-2026-2027>

Data di inizio dell'attività didattica

01/08/2026

Calendario degli esami di profitto

<https://www.unimercatorum.it/offerta-formativa-2026-2027>

Calendario sessioni della Prova finale

<https://www.unimercatorum.it/offerta-formativa-2026-2027>

Infrastrutture

Aule

Pdf inserito: 

Laboratori e Aule Informatiche

Pdf inserito: 

Sale Studio

Pdf inserito: 

Biblioteche

Pdf inserito: 

Servizi a supporto

Orientamento in ingresso e in itinere

Pdf inserito: 

Tutorato

Pdf inserito: 

Assistenza per lo svolgimento di periodi di formazione all' esterno (tirocini e stage)

Pdf inserito: 

Assistenza per la mobilità internazionale I compiti principali del servizio di assistenza e degli accordi per la mobilità internazionale degli studenti comprendono la promozione, l'organizzazione e la gestione dei programmi di mobilità in uscita e il supporto all'accoglienza degli studenti stranieri in ingresso.

L'Ufficio Erasmus si occupa della gestione degli aspetti amministrativi della mobilità, tra cui la richiesta delle sovvenzioni comunitarie, la stipula dell'accordo finanziario con lo studente, il riconoscimento dei crediti formativi e la gestione dell'Online Linguistic Support.

Viene inoltre garantita un'assistenza continua agli studenti prima della partenza, durante la permanenza all'estero e al rientro, con supporto nelle principali procedure amministrative e informazioni utili per il soggiorno all'estero.

L'Ateneo ha stipulato un totale di n. 55 accordi interistituzionali riportati nella tabella sottostante.

Durante il periodo di formazione all'estero per gli studenti sono previste due tipologie di attività:

- ☐ Mobilità ai fini di studio (Student Mobility for Studies);
- ☐ Mobilità per tirocinio (Student Mobility for Traineeships).

Gli studenti possono dunque confrontarsi con realtà universitarie e lavorative di tipo internazionale, seguendo corsi e sostenendo i relativi esami o svolgendo un tirocinio in un'azienda all'estero.

Gli studenti e i neolaureati di Universitas Mercatorum possono candidarsi partecipando ai bandi di mobilità previsti per studio e per tirocinio.

Universitas Mercatorum ha ricevuto dalla Commissione Europea il riconoscimento della Erasmus Charter for Higher Education (ECHE), che permette all'Università di partecipare a tutte le attività di cooperazione e mobilità europea e internazionale nell'ambito del nuovo Programma Erasmus+ per l'istruzione e formazione 2021/2027.

L'Ateneo ha aderito all'iniziativa della Commissione europea "Erasmus Without Paper", sviluppando numerosi Inter-Institutional Agreements e

Online Learning Agreements attraverso la piattaforma EWP Dashboard. L'Ateneo promuove attivamente i Blended Intensive Programmes (BIP), favorendo la partecipazione di studenti e docenti. In particolare, sono stati avviati progetti consolidati in collaborazione con la Universidad de León e l'Instituto Superior de Ciências Sociais e Políticas della Universidade de Lisboa (ISCSP), partner con cui si è instaurata una relazione solida e continuativa. Grazie a queste collaborazioni, l'Ateneo è diventato un punto di riferimento nell'implementazione dei BIP, integrando la mobilità fisica con le componenti virtuali in un contesto internazionale e interdisciplinare. Le testimonianze di studenti e docenti confermano il valore aggiunto di queste esperienze, evidenziando il rafforzamento del legame formativo e la natura collaborativa e intensiva dei BIP.

Link inserito: <https://www.unimercatorum.it/offerta-formativa-2026-2027>

Inserimento atenei in convenzione 

N.	Nazione	Ateneo in convenzione	Codice EACEA	Data convenzione	Titolo
1	Albania	UNIVERSITETI ALEKSANDER MOISIU DURRE		30/08/2024	solo italiano
2	Albania	University of Vlora		03/09/2025	solo italiano
3	Algeria	UNIVERSITE DE BISKRA		01/08/2025	solo italiano
4	Algeria	University Center of Tipaza		03/09/2025	solo italiano
5	Armenia	Armenian State University of Economics (ASUE)		07/11/2024	solo italiano

6	Cambogia	National University of Battambang		26/11/2024	solo italiano
7	Cambogia	National University of Chea Sim Kamchaymear		26/11/2024	solo italiano
8	Cina	Shanghai University of political science and law		07/11/2024	solo italiano
9	Cossovo	International University for Business and Technology (UBT)		15/07/2025	solo italiano
10	Francia	Université de Lorraine		25/04/2024	solo italiano
11	Georgia	ST. Andrews Georgian University - (SANGU)		29/10/2024	solo italiano
12	Germania	RUPRECHT-KARLS-UNIVERSITÄT HEIDELBERG		08/10/2025	solo italiano
13	Grecia	Università		20/05/2024	solo

		ty of West Attica		025	italiano
14	Lettonia	Riga Technica l Universi ty Liepaja Academ y		20/08/2 025	solo italiano
15	Lituania	KlaipĀdo s valstybi nĀ koelgija		04/06/2 024	solo italiano
16	Lituania	VILNIAU S GEDIMI NO TECHNI KOS UNIVER SITETAS		20/06/2 025	solo italiano
17	Lituania	Vilniaus Universi tetas		21/11/2 023	solo italiano
18	Madaga scar	Universi tĀ© d'Antsira nana		07/11/2 024	solo italiano
19	Madaga scar	Universi tĀ© de Mahajan ga		26/11/2 024	solo italiano
20	Moldavi a	Universi tatea de Stat din Moldova		10/06/2 025	solo italiano
21	Monten egro	Univerzit et Mediterr an		14/09/2 023	solo italiano

		Podgorica			
22	Paesi Bassi	Erasmus School of Law, Erasmus University Rotterdam		10/09/2025	solo italiano
23	Paesi Bassi	Utrecht University		12/09/2025	solo italiano
24	Polonia	Adam Mickiewicz University in Poznań		21/07/2025	solo italiano
25	Polonia	Rzeszów University of Technology		04/06/2025	solo italiano
26	Polonia	UNIWER SYTET EKONOMICZNY W POZNANIU		01/12/2025	solo italiano
27	Polonia	Uniwersytet Ekonomiczny w Krakowie		14/01/2026	solo italiano
28	Portogallo	Instituto Politecnico Do Porto		14/06/2023	solo italiano
29	Portogallo	Instituto		17/04/2	solo

	lo	Superior de Ci�ncias Sociais e Politicas da Universidade de Lisboa (ISCSP)		024	italiano
30	Portogal lo	Iscte-Instituto Universit�rio de Lisboa		24/10/2024	solo italiano
31	Portogal lo	UNIVERSIDADE DE LISBOA		29/08/2024	solo italiano
32	Portogal lo	Universidade Aberta		14/07/2022	solo italiano
33	Repubbli ca Ceca	UNIVERZITA OBRANY		29/08/2024	solo italiano
34	Romania	UNIVERSITATEA NATIONALA DE STIINTA SI TEHNOLOGIE POLITEHNICA BUCURESTI		26/03/2025	solo italiano
35	Romania	UNIVERSITATEA PETROL - GAZEDI N		29/08/2024	solo italiano

		PLOIEST I			
36	Romania	Universi ta' Ovidius di Costanz a		15/07/2 022	solo italiano
37	Senegal	Universi te' Cheikh Anta Diop de Dakar		22/11/2 023	solo italiano
38	Spagna	UNIVER SIDAD DE CANTAB RIA		27/08/2 024	solo italiano
39	Spagna	UNIVER SIDAD REY JUAN CARLOS		27/06/2 025	solo italiano
40	Spagna	Universi dad a distanci a de Madrid		15/07/2 022	solo italiano
41	Spagna	Universi dad de Granada		09/11/2 021	solo italiano
42	Spagna	Universi dad de La Laguna		05/04/2 023	solo italiano
43	Spagna	Universi dad de Salaman ca		20/09/2 023	solo italiano
44	Spagna	Universi dad de Valencia		07/03/2 023	solo italiano

45	Spagna	Universi dade de Vigo		20/09/2 023	solo italiano
46	Spagna	Universi ta' del Valladoli d		20/12/2 022	solo italiano
47	Spagna	Universi tÃ di Leon		24/06/2 022	solo italiano
48	Turchia	BASKEN T UNIVER SITESI		14/01/2 026	solo italiano
49	Turchia	Kadir Has Ãniversit esi		10/01/2 025	solo italiano
50	Ucraina	Dnipro universit y of technolo gy - Ucraina		26/11/2 024	solo italiano
51	Ucraina	Lviv Polytech nic National Universi ty		03/09/2 025	solo italiano
52	Ucraina	NATION AL AEROSP ACE UNIVER SITY		10/09/2 025	solo italiano
53	Ucraina	National Technica l Universi ty â âKharkiv Polytech nic		07/11/2 024	solo italiano

		Institute â			
54	Ucraina	V.N.Kara zin Kharkiv National Universi ty		29/10/2 024	solo italiano
55	Ungheri a	Universi ty of Gyor		01/08/2 022	solo italiano

Accompagnamento al lavoro

Pdf inserito: 

Eventuali altre iniziative

Opinioni studenti

Universitas Mercatorum sottopone agli studenti la compilazione dei seguenti questionari:

- Questionario per la rilevazione dell'opinione degli studenti sugli insegnamenti ('Questionario insegnamenti');
- Questionari per la rilevazione delle opinioni degli studenti sui tirocini curriculari ('Questionario tirocini studenti').

I questionari posti sono riportati in allegato alle 'Linee Guida per la gestione dei questionari compilati da studenti e tutori aziendali, laureandi, laureati, dottorandi e dottori di ricerca, personale docente e di ricerca e personale non docente e la pubblicizzazione e utilizzazione dei relativi risultati' (LG Questionari).

Per quanto riguarda la rilevazione dell'opinione degli studenti sugli insegnamenti, l'Università Mercatorum utilizza un questionario sviluppato internamente ('Questionario insegnamenti'), composto da 11 domande finalizzato a rilevare l'opinione degli studenti sull'insegnamento, sulla docenza e il loro interesse relativamente agli argomenti trattati nell'insegnamento.

Il Questionario insegnamenti è compilato on line dagli studenti in forma anonima.

La compilazione riguarda soltanto gli insegnamenti previsti dal piano di studio per l'anno di corso in cui lo studente è iscritto ed è collegata all'iscrizione agli esami di profitto.

Gli studenti possono compilare il questionario dopo lo svolgimento di almeno due terzi delle lezioni.

L'elaborazione dei dati è effettuata dall'Ufficio AQ una volta all'anno entro il mese di ottobre e, quindi, dopo la conclusione del precedente A.A., che, per le Università telematiche, è convenzionalmente stabilita alla data del 31 luglio di ogni anno, e in largo anticipo rispetto alla scadenza per la redazione della relazione annuale del NdV relativa, appunto, all'analisi dei questionari compilati dagli studenti.

Sono presi in considerazione solo i questionari degli insegnamenti per i quali sono state raccolte almeno 5 rilevazioni, non considerando significativi, in caso contrario, i dati raccolti.

I risultati sono resi disponibili con tre differenti livelli di aggregazione: Ateneo, Corso di Studio, singolo insegnamento.

L'AQ richiede che, in presenza di criticità, queste vengano analizzate e, nel caso l'analisi confermi la presenza di criticità, vengano individuati e adottati gli interventi opportuni per risolverle e le modalità di verifica dell'efficacia di tali interventi.

Sono da considerare 'critici' e, pertanto, da prendere certamente in considerazione ai fini della individuazione di opportune azioni correttive o

di miglioramento, i risultati attinenti a ogni singola domanda per i quali la somma delle risposte 'Decisamente sì' e 'Più sì che no' è inferiore al 60% delle risposte complessive e/o le risposte 'Decisamente no' sono superiori al 25% delle risposte complessive.

Possono essere prese in considerazione anche risultati non critici, sulla base dei criteri sopra stabiliti, ma che evidenziano un trend decrescente con riferimento almeno ai due precedenti anni accademici.

I risultati relativi ai singoli insegnamenti non sono pubblici e sono resi disponibili alle parti interessate interne coerentemente a quanto di seguito indicato:

- Docenti: risultanze degli insegnamenti e moduli di competenza
- Docenti responsabili di insegnamenti integrati e articolati in moduli: tutti i moduli
- Coordinatore del CdS, Gruppo di AQD del CdS: risultanze di tutti gli insegnamenti del CdS
- Preside di Facoltà, Commissione Paritetica Docenti-Studenti: risultanze di tutti gli insegnamenti della Facoltà
- Presidente CdA, Rettore, Senato Accademico, Presidio della Qualità, Nucleo di Valutazione: risultanze di tutti gli insegnamenti dell'Ateneo

Una volta resi disponibili i risultati relativi ai singoli insegnamenti:

□ i docenti titolari degli insegnamenti che evidenziano criticità devono fornire un commento a ciascuna di esse, utilizzando un apposito modulo, riportato in allegato alle LG questionari. In particolare, i docenti devono indicare, per ciascuna domanda che evidenzia criticità, le azioni correttive / di miglioramento che intendono adottare/proporre. Il modulo compilato deve essere inviato al Coordinatore di CdS entro 30 giorni dalla ricezione dei risultati dell'elaborazione dei questionari. Tale modulo ha anche lo scopo di stimolare un processo di miglioramento continuo da parte dei docenti e di incentivare la collaborazione tra docente e Ateneo al fine di assicurare il raggiungimento di risultati di qualità nel tempo a beneficio della didattica erogata in Ateneo.

□ I Coordinatori di CdS devono:

- rendicontare al Consiglio di CdS e, quindi, al Consiglio di Facoltà i risultati dell'elaborazione dei questionari a livello CdS, evidenziando in particolare:
 - a) la variazione con riferimento, di norma, al precedente anno accademico;
 - b) i risultati a livello di singoli insegnamenti, evidenziando quanti insegnamenti hanno riportato criticità e quali e quante criticità sono state evidenziate, nel rispetto delle legittime esigenze di privacy (e cioè senza indicare né gli insegnamenti e tantomeno i docenti oggetto di criticità).
 - c) Insieme al Gruppo AQD, esaminare e discutere le indicazioni del docente eventualmente col docente stesso e, quindi, con la CPDS di riferimento (in particolare, con la rappresentanza studentesca) e, se del caso, con altri soggetti ritenuti in grado di poter fornire un utile contributo, per integrarle con eventuali ulteriori considerazioni e proposte da riportare nello stesso modulo compilato dal docente.
- Rendicontare al Consiglio di CdS e, quindi, al Consiglio di Facoltà gli esiti

della fase di analisi delle criticità evidenziate dai questionari e di definizione di azioni per la loro soluzione o almeno per il miglioramento degli aspetti critici evidenziati dai questionari, nel rispetto delle legittime esigenze di privacy.

- Se sono state previste azioni correttive o di miglioramento, effettuare al momento opportuno, eventualmente assieme al docente interessato e col supporto del Gruppo AQD, una verifica degli esiti delle azioni adottate e lasciarne traccia scritta compilando l'apposito quadro nel medesimo modulo.
- Rendicontare al Consiglio di CdS e, quindi, al Consiglio di Facoltà gli esiti delle azioni adottate, nel rispetto delle legittime esigenze di privacy.
- Documentare il tutto nei Verbali del Consiglio di CdS.

Per quanto riguarda la rilevazione delle opinioni degli studenti sui tirocini curriculari, l'Università Mercatorum utilizza un questionario sviluppato internamente ('Questionario tirocini studenti'), composto da 8 domande. Il questionario è finalizzato a verificare, in particolare, la corrispondenza delle attività effettivamente svolte con quanto pianificato, l'opinione degli studenti sull'efficacia del tirocinio e il loro livello di soddisfazione. Il Questionario tirocini studenti è somministrato agli studenti che hanno svolto un tirocinio presso una struttura esterna all'Ateneo.

Il questionario è compilato dagli studenti on line.

I questionari compilati sono elaborati dall'Ufficio AQ, di norma entro il mese di ottobre di ogni anno.

I risultati dell'elaborazione (in particolare: numero di tirocini effettuati, numero di questionari raccolti, risultati delle risposte alle domande poste dal questionario) e i singoli questionari sono trasmessi ai Coordinatori e ai Gruppi di AQD dei CdS, i quali li analizzano allo scopo di identificare eventuali problemi o criticità e, in questo caso, adottare opportune azioni correttive o di miglioramento. Gli esiti dell'analisi e delle eventuali azioni correttive o di miglioramento adottati sono condivisi con il Consiglio del CdS, documentati nei relativi verbali e resi noti al Consiglio di Facoltà.

Pdf inserito: 

Opinioni dei laureati

Universitas Mercatorum sottopone ai laureandi la compilazione del 'Questionario per la rilevazione dell'opinione degli studenti su comunicazione, strutture, servizi e percorso formativo ('Questionario CoSSeP' o 'Questionario laureandi'), sviluppato internamente, composto da 24 domande e riportato in allegato alle LG questionari.

Il Questionario CoSSeP è diviso in quattro sezioni al fine di misurare in modo univoco e sintetico le principali evidenze relative a:

'Comunicazione', 'Strutture', 'Servizi' e 'Percorso formativo'.

La prima sezione – Comunicazione – comprende 6 domande, finalizzate

a rilevare l'opinione degli studenti sull'adeguatezza e l'efficacia della comunicazione.

La seconda sezione – Strutture – comprende 4 domande, finalizzate a rilevare l'opinione degli studenti sull'adeguatezza delle strutture didattiche.

La terza sezione – Servizi – comprende 5 domande, finalizzate a rilevare l'opinione degli studenti sull'adeguatezza dei servizi per gli studenti.

La quarta sezione – Percorso formativo – comprende 9 domande, finalizzate a rilevare l'opinione degli studenti sul processo formativo nel suo complesso.

Il Questionario CoSSeP è somministrato agli studenti all'atto dell'iscrizione alla prova finale.

Il questionario è compilato on line in forma anonima.

I questionari compilati sono elaborati dall'Ufficio AQ, di norma entro il mese di ottobre di ogni anno. Le modalità di elaborazione dei questionari compilati sono le stesse di quelle dei questionari insegnamenti.

I risultati sono resi disponibili con due differenti livelli di aggregazione: Ateneo e Corso di Studio.

Sono da considerare 'critici' e, pertanto, da prendere certamente in considerazione ai fini della individuazione di opportune azioni correttive o di miglioramento, i risultati attinenti a ogni singola domanda per i quali la somma delle risposte 'Sì' e 'Più sì che no' o 'Positiva' e 'Più positiva che negativa' è inferiore al 60% delle risposte complessive e/o le risposte 'No' sono superiori al 25% delle risposte complessive.

Possono essere prese in considerazione anche risultati non critici sulla base dei criteri sopra stabiliti, ma che evidenziano un trend decrescente con riferimento almeno ai due precedenti anni accademici.

I risultati aggregati a livello Ateneo e CdS sono presi in considerazione rispettivamente dal Presidio della Qualità e dai competenti Gruppi di AQD, coordinati dai Coordinatori dei CdS, i quali li analizzano per verificare la loro tendenza negli anni e informare rispettivamente gli Organi di Governo e i Consigli di CdS e, quindi, i Consigli di Facoltà sia dei risultati aggregati sia del loro trend negli anni, documentando il tutto nei rispettivi Verbalì e, per quanto riguarda il Presidio, nella Relazione annuale.

Qualora i risultati evidenziassero criticità comuni a tutti i CdS dell'Ateneo e/o relativi ai singoli CdS, queste saranno prese in considerazione rispettivamente dal Senato Accademico (previa loro identificazione da parte del Presidio della Qualità) e dal competente Gruppo di AQD:

- per avviarne prontamente, se possibile, la soluzione, attraverso l'adozione di opportune azioni correttive o di miglioramento ovvero
- per essere oggetto di riesame in occasione del primo Riesame del Funzionamento del Sistema di Governo e del Sistema di AQ a livello Sede e/o del primo Riesame del Funzionamento del Sistema di AQ a livello CdS (nell'ambito del Riesame percorso formativo e gestione processi AQ CdS) rispettivamente [cfr. 'Linee Guida per il Monitoraggio, la Valutazione e il Riesame del Sistema di Governo e del Sistema di AQ' (LG M&V&R)].

Con riferimento ai problemi e alle criticità relativi a un singolo CdS, il Coordinatore del CdS deve documentare e condividere con il Consiglio di

Corso di Studio prima e con Consiglio di Facoltà di afferenza dopo le criticità evidenziate, le soluzioni adottate, le criticità risolte.

Pdf inserito: 

Dati di ingresso, di percorso e di uscita

I dati di ingresso, di percorso e di uscita presi in considerazione ai fini della valutazione dell'attrattività del CdS e dell'efficacia del processo formativo sono quelli forniti periodicamente dall'ANVUR disponibili nella SUA-CdS 2024– con scadenza al 30/06, al 30/09/e al 31/12 di ogni anno.

I dati relativi agli indicatori al 30 settembre 2025 – e cioè i dati presi in considerazione dall'Ateneo ai fini della compilazione della Scheda di Monitoraggio Annuale (SMA) 2025 – sono disponibili e commentati nella SUA-CdS 2024.

Opinioni enti e imprese con accordi di stage / tirocinio curriculare o extra-curriculare

Il CdS in Sicurezza informatica (LM66) non prevede da ordinamento lo svolgimento di periodi di formazione articolati in tirocini/stage curricolari o extra-curricolari.

Struttura organizzativa e responsabilità a livello di Ateneo

Organizzazione e responsabilità della AQ a livello del Corso di Studio

Riesame annuale