



Informazioni generali sul Corso di Studi

Università	Università di PISA
Nome del corso in italiano	SICUREZZA INFORMATICA (<i>IdSua:1581775</i>)
Nome del corso in inglese	CYBERSECURITY
Classe	LM-66 - Sicurezza informatica
Lingua in cui si tiene il corso	inglese
Eventuale indirizzo internet del corso di laurea	https://cysec.unipi.it/
Tasse	Pdf inserito: visualizza
Modalità di svolgimento	a. Corso di studio convenzionale



Referenti e Strutture

Presidente (o Referente o Coordinatore) del CdS	CHESSA Stefano
Organo Collegiale di gestione del corso di studio	Consiglio di Corso di Studio
Struttura didattica di riferimento	INGEGNERIA DELL'INFORMAZIONE
Eventuali strutture didattiche coinvolte	INFORMATICA

Docenti di Riferimento

N.	COGNOME	NOME	SETTORE	QUALIFICA	PESO	TIPO SSD
1.	ANASTASI	Giuseppe		PO	0,5	
2.	BACCI	Giacomo		RD	0,5	

3.	BARONTI	Federico	PA	0,5
4.	CHESSA	Stefano	PO	1
5.	FERRARI	Gian-Luigi	PO	1
6.	GARROPPO	Rosario Giuseppe	PA	0,5
7.	MARCELLONI	Francesco	PO	0,5
8.	PAGANELLI	Federica	PA	0,5
9.	ROSSI	Daniele	PA	0,5
10.	SALETTI	Roberto	PO	0,5

Rappresentanti Studenti	Rappresentanti degli studenti non indicati
Gruppo di gestione AQ	STEFANO BARONTI SOFIA BONAPACE STEFANO CHESSA BARBARA CONTE TEODORICO PACINI
Tutor	Stefano CHESSA



Il Corso di Studio in breve

29/04/2022

L'obiettivo del Corso di Laurea Magistrale in Cybersecurity è quello di rispondere alla crescente esigenza di formazione di specialisti dotati di elevate competenze scientifiche e tecnologiche nell'ambito della sicurezza informatica e dei dati. A questo fine assicura ai propri laureati una profonda conoscenza dei fondamenti scientifici, delle metodologie di questo ambito, che permette loro di contribuire al progresso delle conoscenze e di saper affrontare problematiche di sicurezza informatica nei più diversi ambiti applicativi. Il corso di laurea copre tutti gli argomenti fondamentali per la preparazione culturale di un laureato magistrale del settore, ed è progettato per essere seguito proficuamente da studenti provenienti da lauree delle classi di Ingegneria dell'Informazione e di Scienze e Tecnologie Informatiche, offrendo un ampio percorso formativo comune e garantendo l'omogeneità e la coerenza della formazione. In particolare, il corso di laurea offre conoscenze specialistiche di notevole impatto innovativo, all'interno di un'offerta che include tutti i principali ambiti della sicurezza informatica (sicurezza e affidabilità nelle reti di comunicazione, nei sistemi, nell'hardware e nel software, e aspetti della sicurezza legati ai linguaggi di programmazione e all'applicazione di tecniche crittografiche e di intelligenza artificiale) più conoscenze relative all'organizzazione aziendale e degli aspetti giuridici della sicurezza informatica e dei dati. Per questi motivi, il laureato magistrale in cybersecurity è dotato di una preparazione culturale, scientifica e metodologica che gli permette di accedere ai livelli di studio universitario successivi al magistrale, quali i dottorati di ricerca in informatica e ingegneria informatica o dottorati di ricerca in discipline affini.

Gli obiettivi formativi specifici della Laurea Magistrale in Cybersecurity sono:

- conoscere gli aspetti scientifici e tecnologici relativi alla sicurezza informatica e le soluzioni allo stato dell'arte per la progettazione, realizzazione, verifica e manutenzione di infrastrutture e sistemi informatici sicuri e protetti;
- conoscere gli aspetti relativi all'organizzazione delle aziende e degli aspetti di rischio connessi all'uso di tecnologie informatiche nella realizzazione delle loro infrastrutture e nella gestione dei dati;

- conoscere gli aspetti giuridici in merito alla protezione dei sistemi informatici e alla protezione e trattamento dei dati gestiti con strumenti digitali, e saper progettare sistemi informatici e di gestione dei dati in accordo con la legislazione vigente;
- essere in grado di aggiornare le proprie conoscenze anche attingendo alle pubblicazioni scientifiche nell'ambito della cybersecurity;
- saper progettare e valutare soluzioni innovative per la sicurezza informatica.

Link: <http://>



QUADRO A1.a

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

19/12/2019

La proposta di Laurea Magistrale in Sicurezza Informatica - Cybersecurity è stata portata all'attenzione e alla valutazione di diversi portatori di interesse:

- Direttore Centro di Competenza Toscana in CyberSecurity (27 Giugno 2019)
- Vicepresidente Confindustria Firenze con delega a Industria 4.0 (11 Novembre 2019)
- Portavoce Nazionale ICT di CNA (11 Novembre 2019)
- Portavoce Regionale ICT di CNA (11 Novembre 2019)
- Direttore Consorzio QUINN - Consorzio Universitario in Ingegneria per la Qualità e l'Innovazione (12 Novembre 2019)
- Managing Director Glass Industry Italy (12 Novembre 2019)
- Rappresentanti Studenti nel Consiglio Dipartimento di Informatica (12 Novembre 2019)

Le parti interessate consultate hanno concordato sulla necessità di attivare dei percorsi formativi specializzati in cybersecurity e hanno valutato positivamente e espresso parere favorevole alla proposta.

Le analisi di mercato sulle tecnologie dell'informazione e della comunicazione e sulla sicurezza informatica in particolare confermano un'elevata domanda di formazione di laureati con competenze nel settore, in particolare negli ambiti in cui è maggiormente presente l'innovazione tecnologica (fonti: rapporto Assinform, rapporto Assintel, rapporti ISTAT ed EUROSTAT, Manifesto e-skills, libro bianco del CINI sulla cybersecurity, ricerche ISFOL sui fabbisogni professionali). Tutti gli studi esaminati concordano sull'esigenza di formare figure scientifiche e professionali in grado di contribuire al processo di innovazione del paese nel settore della sicurezza informatica.

Al fine di monitorare ulteriormente le esigenze formative avanzate dalle organizzazioni rappresentative della produzione di beni e servizi, i dipartimenti di Informatica e di Ingegneria dell'Informazione si occupano dell'orientamento universitario, dell'elaborazione e diffusione di informazione sui percorsi di studio

universitario, dei rapporti col mondo del lavoro, dell'internazionalizzazione dei corsi di studio, dell'elaborazione e della diffusione di informazione su risultati delle attività di ricerca e innovazioni realizzati dai due dipartimenti.

Il corso di studio, nell'intento di verificare e valutare gli interventi mirati al miglioramento del corso stesso effettuerà consultazioni periodiche con le organizzazioni maggiormente rappresentative nel settore di interesse.



QUADRO A1.b

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

29/04/2022

Il corso di studio è stato istituito da meno di due anni, ha iniziato ad erogare i corsi nel Settembre 2020, ed è nato per venire incontro ad esigenze espresse da diverse organizzazioni in diverse sedi, come documentato nel documento di progettazione. Il corso di studio svolge azioni di consultazione periodiche, con cadenza annuale, sotto la diretta responsabilità del suo presidente. Le consultazioni con le organizzazioni esterne avvengono principalmente tramite studi di settore. Il corso di studio inoltre organizza seminari e altri eventi che prevedono incontri con esponenti del mondo

professionale, delle pubbliche amministrazioni e delle aziende. Infine, non avendo ancora laureati nel corso del 2021 il corso di studio non ha, al momento, attivato tirocini e tesi con relatori aziendali o questionari da sottoporre alle aziende che hanno assunto laureati del corso di studio, come pure attività di monitoraggio e job placement, ma queste sono iniziative pianificate per il futuro.

Relativamente agli studi di settore, viene preso in considerazione il rapporto sul digitale in Italia a cura di Confindustria Digitale, Anitec-Assinform e promosso dal Ministero dell'Istruzione, Università e Ricerca, e dall'Agenzia per l'Italia Digitale (<https://ildigitaleinitalia.it/>) e l'Osservatorio delle Competenze Digitali a cura di Aica, Anitec-Assinform, Assintel, Assinter Italia, <https://competenzedigitali.org/>.

Nel corso del 2021 si sono inoltre svolti i seguenti eventi, che hanno portato ad un confronto tra il corso di studi (nella figura del suo presidente e/o docenti del corso) ed esponenti del mondo professionale, delle pubbliche amministrazioni e delle aziende:

- incontro con il Prof. Gabriele Oligeri, HBKU Qatar, tenuto il 22 Dicembre 2021 in concomitanza con il seminario per gli studenti su "BrokenStrokes: on the (in)security of wireless keyboards"
- incontri con Marelli Powertrain (Ing. Fabio Ghigo, Ing. Francesco Barletta e Ing. Andrea Nicolo), tenuti il 3/6/21 e il 5/10/21
- incontro con Prof. Roberto Guanciale, KTH Royal Institute of Technology Stockholm University, Sweden, tenuto il 10/6/2021 in concomitanza con il seminario per gli studenti su "InSpectre: Breaking and Fixing Microarchitectural Vulnerabilities by Formal Analysis"
- incontro con Huawei (Ing. Fabrizio Tronci), 25/5/2021, in concomitanza con il seminario per gli studenti su "Synergy between functional safety and cybersecurity in complex automotive systems"
- incontro con Prof. Maria Grazia Porcedda, Trinity College Dublin, tenuto il 13/5/2021 in concomitanza con il seminario per gli studenti su "Cascade and Chain Effects in Big Data Cybercrime: Lessons from the TalkTalk hack"
- incontro con IUSINTECH (avv. Rita Eva Cresci) tenuto il 6 Maggio 2021 in concomitanza con il seminario per gli studenti su "Cloud computing: security and data protection"
- incontro con Avv. Maria Concetta Causarano tenuto il 5 Maggio 2021 in concomitanza con il seminario per gli studenti su "Online (transaction) platforms: the applicable legal framework and the remedies available for the protection of digital users".

Link : <http://>



QUADRO A2.a

Profilo professionale e sbocchi occupazionali e professionali previsti per i laureati

Progettista di sistemi e applicazioni informatiche sicure

funzione in un contesto di lavoro:

Funzioni di elevata responsabilità nella progettazione, lo sviluppo, la valutazione, la verifica e la gestione di sistemi e di infrastrutture di comunicazione complessi per far fronte alle esigenze di sicurezza più stringenti.

competenze associate alla funzione:

Profonda conoscenza delle metodologie e delle tecnologie relative alla sicurezza informatica e degli aspetti giuridici legati al trattamento dei dati e alla loro sicurezza; capacità di comprendere e di integrare nuove tecnologie; spiccata capacità di analisi critica e di valutazione di problemi complessi, anche in relazione ai molteplici ambiti applicativi in cui si rende necessaria la presenza di sistemi informatici sicuri; comprensione dell'organizzazione aziendale dal punto di vista della sicurezza informatica.

sbocchi occupazionali:

Imprese, enti pubblici e pubbliche amministrazioni operanti nell'ambito della produzione e dei servizi informatici.

Ricercatore in sicurezza informatica

funzione in un contesto di lavoro:

Attività di ricerca e di innovazione metodologica ed applicativa, nell'ambito di tutti i settori della sicurezza informatica.

competenze associate alla funzione:

Profonda conoscenza delle basi scientifiche e tecnologiche della sicurezza informatica e della gestione sicura dei dati, capacità di astrazione e di modellazione di sistemi e reti informatiche complesse e conoscenza delle problematiche proposte dall'interazione tra la sicurezza informatica e le altre discipline scientifiche/tecnologiche.

sbocchi occupazionali:

Enti pubblici e privati operanti nel settore della ricerca in sicurezza informatica, e più in generale, della ricerca scientifica. È inoltre possibile accedere ai livelli di studio universitario successivi, quali il Dottorato di Ricerca in Informatica, in Ingegneria dell'Informazione e dottorati in discipline affini.

Specialista in sicurezza informatica

funzione in un contesto di lavoro:

Attività di supervisione, coordinamento e gestione delle politiche e delle attività di sicurezza informatica per aziende e pubbliche amministrazioni relative all'analisi, progettazione, gestione e manutenzione dei sistemi informativi e delle reti.

competenze associate alla funzione:

Lo specialista in sicurezza informatica è dotato di competenze specialistiche relative alle tecnologie e alle metodologie per la sicurezza informatica e per la gestione sicura e affidabile dei dati, e di conoscenze relative all'organizzazione aziendale e degli aspetti giuridici della sicurezza informatica che gli consentono di far fronte alle diverse esigenze in merito alla sicurezza informatica di aziende e pubbliche amministrazioni. Competenze specifiche riguardano la capacità di analisi per la prevenzione, scoperta, mitigazione e recupero da un attacco informatico, e la capacità di progettare o di rimodellare le infrastrutture informatiche esistenti di imprese e di pubbliche amministrazioni per far fronte a specifiche esigenze di sicurezza.

sbocchi occupazionali:

Imprese, enti pubblici e pubbliche amministrazioni operanti nell'ambito della produzione e dei servizi informatici.



QUADRO A2.b

Il corso prepara alla professione di (codifiche ISTAT)

1. Analisti e progettisti di software - (2.1.1.4.1)
2. Specialisti in reti e comunicazioni informatiche - (2.1.1.5.1)
3. Specialisti in sicurezza informatica - (2.1.1.5.4)



22/01/2020

Requisito generale per l'ammissione è il possesso di una laurea triennale delle classi delle lauree in Scienze e tecnologie informatiche (L-31) o in Ingegneria dell'informazione (L-8), o lauree equipollenti nelle corrispondenti classi di cui al D.M. 509/1999. Possono essere ammessi studenti in possesso di una laurea triennale di un'altra classe conseguita in Italia, o di equivalente titolo di studio conseguito all'estero, che abbiano acquisito almeno 54 CFU così ripartiti:

- almeno 36 CFU nei settori ING-INF/01, ING-INF/03, ING-INF/05, INF/01
- almeno 18 CFU nei settori MAT/*, FIS/*

Il Consiglio del corso di laurea valuterà per l'ammissione la congruità dei crediti acquisiti da studenti con il titolo estero; inoltre, per tutti gli studenti appurerà l'adeguatezza della preparazione personale secondo procedure definite nel regolamento didattico.

È inoltre richiesta una adeguata conoscenza della lingua inglese equiparabile almeno di livello B2 del Quadro Comune Europeo di riferimento per le lingue. Il possesso di tale requisito potrà essere certificato dagli studenti in fase di iscrizione o, in assenza di una certificazione, sarà verificato tramite colloquio o esame del curriculum durante la verifica della preparazione personale dello studente.



11/05/2021

Requisito generale per l'ammissione è il possesso di una laurea triennale delle classi delle lauree in Scienze e tecnologie informatiche (L-31) o in Ingegneria dell'informazione (L-8) e nelle corrispondenti classi di cui al D.M. 509/1999. Possono essere ammessi studenti in possesso di una laurea triennale di un'altra classe conseguita in Italia, o di equivalente titolo di studio conseguito all'estero, che abbiano acquisito almeno 54 CFU così ripartiti:

- almeno 36 CFU nei settori ING-INF/01, ING-INF/03, ING-INF/05, INF/01
- almeno 18 CFU nei settori MAT/*, FIS/*

Il Consiglio del corso di laurea valuterà per l'ammissione la congruità dei crediti acquisiti da studenti con il titolo estero e appurerà l'adeguatezza della preparazione personale tramite un colloquio individuale.

È inoltre richiesta una adeguata conoscenza della lingua inglese equiparabile almeno di livello B2 del Quadro Comune Europeo di riferimento per le lingue. Il possesso di tale requisito potrà essere certificato dagli studenti in fase di iscrizione o, in assenza di una certificazione, sarà verificato tramite colloquio o esame del curriculum durante la verifica della personale preparazione dello studente.

L'adeguatezza della personale preparazione, in particolare sui fondamenti delle scienze e delle tecnologie dell'informazione e della lingua Inglese è verificata mediante la valutazione del curriculum formativo ed eventualmente con una prova di verifica su argomenti specifici.

Nel caso non vengano rispettati i requisiti curriculari, la Commissione a ciò delegata (Presidente o vice-presidente del corso di laurea, delegato ai PdS) può indicare agli studenti quali specifici singoli corsi di transizione sono adatti al

completamento dei requisiti curriculari, in ogni caso in misura non superiore a 40 CFU. Il soddisfacimento dei requisiti curriculari deve comunque precedere l'iscrizione.



QUADRO A4.a

Obiettivi formativi specifici del Corso e descrizione del percorso formativo

09/12/2019

Il Corso di Laurea Magistrale in Cybersecurity risponde alla crescente esigenza di formazione di specialisti dotati di elevate competenze scientifiche e tecnologiche nell'ambito della sicurezza informatica e dei dati. A questo fine assicura ai propri laureati una profonda conoscenza dei fondamenti scientifici e delle metodologie di questo ambito, che permette loro di contribuire al progresso delle conoscenze e di saper affrontare problematiche di sicurezza informatica nei più diversi ambiti applicativi.

Il corso di laurea copre tutti gli argomenti fondamentali per la preparazione culturale di un laureato magistrale del settore, ed è progettato per essere seguito proficuamente da studenti provenienti da lauree delle classi di Ingegneria dell'Informazione e di Scienze e Tecnologie Informatiche, offrendo un ampio percorso formativo comune e garantendo l'omogeneità e la coerenza della formazione. In particolare, il corso di laurea offre conoscenze specialistiche di notevole impatto innovativo, all'interno di un'offerta che include tutti i principali ambiti della sicurezza informatica (sicurezza e affidabilità nelle reti di comunicazione, nei sistemi, nell'hardware e nel software, e aspetti della sicurezza legati ai linguaggi di programmazione e all'applicazione di tecniche crittografiche e di intelligenza artificiale) più conoscenze relative all'organizzazione aziendale e degli aspetti giuridici della sicurezza informatica e dei dati.

Per questi motivi, il laureato magistrale in cybersecurity è dotato di una preparazione culturale, scientifica e metodologica che gli permette di accedere ai livelli di studio universitario successivi, quali i dottorati di ricerca in informatica e ingegneria informatica o dottorati di ricerca in discipline affini.

Il Corso di Laurea Magistrale in Informatica forma le seguenti figure professionali:

- a) Progettista di sistemi e applicazioni informatiche sicure
- b) Ricercatore in informatica/ingegneria dell'informazione
- c) Specialista in sicurezza informatica

STRUTTURA DEL PERCORSO DI STUDIO

Il percorso di studio, definito nel regolamento didattico, prevede nel primo anno di corso insegnamenti obbligatori negli ambiti scientifico e tecnologico che forniscono i fondamenti della sicurezza informatica. Nel primo anno è inoltre previsto un insegnamento affine volto al consolidamento della preparazione di base dello studente nelle discipline informatiche, di telecomunicazioni e di elettronica.

Nel secondo anno di corso lo studente affronterà insegnamenti obbligatori nell'ambito giuridico, sociale ed economico e potrà specializzare/approfondire il proprio percorso scegliendo tra insegnamenti affini o integrativi, e svolgerà le attività relative alla prova finale.



QUADRO

A4.b.1

Conoscenza e comprensione, e Capacità di applicare conoscenza e comprensione: Sintesi

Conoscenza e capacità di comprensione	<p>Il laureato magistrale ha conoscenza specialistiche nelle discipline inerenti la sicurezza informatica e dei dati, anche dal punto di vista degli aspetti giuridici e di organizzazione aziendale. Dato che questa disciplina si interseca con i più diversi aspetti dell'informatica, il percorso formativo fornisce ai laureati competenze 'orizzontali' delle problematiche inerenti alla sicurezza e all'affidabilità a tutti i livelli di un sistema informatico, dall'hardware, reti, sistemi, dati, software e linguaggi, combinate con competenze relative all'utilizzo delle tecniche più evolute di intelligenza artificiale e crittografia. Le conoscenze acquisite vengono verificate in tutte le prove finali degli insegnamenti.</p>	
Capacità di applicare conoscenza e comprensione	<p>Il laureato magistrale in Cybersecurity ha la capacità di lavorare in autonomia, è in grado di progettare, sviluppare, validare e gestire sistemi informatici sicuri, e di definire e gestire le politiche di sicurezza informatica e di protezione dei dati sensibili di aziende, enti e pubbliche amministrazioni. Le capacità di applicare le conoscenze acquisite negli insegnamenti sono sviluppate dagli studenti tramite attività progettuali/laboratoriali svolte negli insegnamenti stessi. La verifica di tali capacità avviene tramite specifiche prove di progetto o di laboratorio che affiancano le prove finali degli insegnamenti, e tramite la prova finale.</p>	

Cybersecurity

Conoscenza e comprensione

Il laureato magistrale ha conoscenza specialistiche nelle discipline inerenti la sicurezza informatica e dei dati, anche dal punto di vista degli aspetti giuridici e di organizzazione aziendale. Dato che questa disciplina si interseca con i più diversi aspetti dell'informatica e dell'ingegneria dell'informazione, il percorso formativo fornisce ai laureati competenze "orizzontali" delle problematiche inerenti alla sicurezza e l'affidabilità a tutti i livelli di un sistema digitale. In particolare, il laureato magistrale conosce lo stato dell'arte ed è in grado di comprenderne l'evoluzione negli aspetti della progettazione e ingegnerizzazione di hardware e software sicuro e affidabile, sia negli aspetti di sistema, dati, di comunicazione e di linguaggio, e nella comprensione di tecniche evolute di intelligenza artificiale e crittografia. Ha inoltre la capacità di capire, di modellare e analizzare sistemi complessi dal punto di vista della sicurezza informatica.

Le conoscenze e la capacità di comprensione degli argomenti trattati vengono promosse con insegnamenti aventi sia carattere metodologico sia attività progettuali e laboratoriali. La verifica del raggiungimento di questi obiettivi avverrà tramite le prove finali degli insegnamenti.

Capacità di applicare conoscenza e comprensione

Il laureato magistrale in Cybersecurity ha competenze tecnico scientifiche per lavorare con ampia autonomia, assumere responsabilità di progetti, per mantenersi aggiornato rispetto all'evoluzione delle conoscenze e delle tecnologie del settore e per promuovere innovazione nell'ambito della cybersecurity. In particolare, possiede le conoscenze scientifiche e tecniche necessarie per:

- comprendere e modellare sistemi informatici complessi dal punto di vista della sicurezza e affidabilità, tenendo conto degli aspetti giuridici e di organizzazione aziendale;
- progettare e sviluppare soluzioni sicure e affidabili per sistemi informatici complessi;
- progettare e gestire la sicurezza informatica e dei dati di aziende, enti e pubblica amministrazione;
- gestire situazioni di emergenza in caso di attacchi ad infrastrutture informatiche;
- comprendere e produrre documentazione scientifica e tecnica in italiano e in inglese;
- valutare la correttezza e l'efficienza delle soluzioni proposte.

L'impostazione degli insegnamenti prevede che la formazione teorica sia accompagnata da esempi, applicazioni, lavori individuali e di gruppo e verifiche che sollecitino la partecipazione attiva, l'attitudine propositiva, la capacità di elaborazione autonoma e di comunicazione dei risultati del lavoro svolto. Gli insegnamenti possono a tal fine integrare valutazioni intermedie in itinere e valutazione finale.

La parte di approfondimento ed elaborazione delle conoscenze demandata allo studio personale dello studente assume a questo proposito una rilevanza notevole. Infatti solo tramite una congrua rielaborazione personale delle informazioni introdotte durante le ore di lezione lo studente può misurare concretamente il livello di padronanza delle conoscenze, delle competenze e delle abilità raggiunte.

Le capacità applicative sono raggiunte dallo studente attraverso attività progettuali e attraverso la preparazione della tesi di laurea, e sono verificate con prove scritte e orali e con discussione dei risultati ottenuti.

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

929II APPLIED CRYPTOGRAPHY 9 CFU
931II ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY 6 CFU
934II BIOMETRICS SYSTEMS 6 CFU
713AA DATA AND SYSTEM SECURITY 9 CFU
932II DEPENDABILITY 6 CFU
935II ELECTROMAGNETIC SECURITY 6 CFU
930II HARDWARE AND EMBEDDED SECURITY 9 CFU
714AA LANGUAGE-BASED TECHNOLOGY FOR SECURITY 9 CFU
933II NETWORK SECURITY 9 CFU
005PN ORGANIZATIONAL SCIENCES AND INFORMATION AND TECHNOLOGY LAW 12 CFU
937II PENETRATION AND DEFENCE LABORATORY 6 CFU
715AA SECURE SOFTWARE ENGINEERING 9 CFU

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

[Visualizza Insegnamenti](#)

[Chiudi Insegnamenti](#)

APPLIED CRYPTOGRAPHY [url](#)

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY [url](#)

BIOMETRICS SYSTEMS [url](#)

DATA AND SYSTEM SECURITY [url](#)

DEPENDABILITY [url](#)

ELECTROMAGNETIC SECURITY [url](#)

HARDWARE AND EMBEDDED SECURITY [url](#)

LANGUAGE-BASED TECHNOLOGY FOR SECURITY [url](#)

NETWORK SECURITY [url](#)

ORGANIZATIONAL SCIENCES AND INFORMATION AND TECHNOLOGY LAW (OL) [url](#)

PENETRATION AND DEFENCE LABORATORY [url](#)

**Autonomia di giudizio**

Il laureato magistrale in Cybersecurity ha la capacità di determinare, valutare e elaborare in modo autonomo gli aspetti critici del sapere e delle tecnologie della sicurezza informatica e del loro impatto giuridico, sociale ed etico.

In particolare è in grado di raccogliere, interpretare, e valutare dati e fabbisogni informativi per determinare e specificare soluzioni informatiche sicure e affidabili da utilizzare ai vari livelli architetturali di un sistema o di una rete di comunicazione.

Gli insegnamenti introdotti nel piano di studio enfatizzano, attraverso esercitazioni e attività pratiche condotte sia individualmente che in gruppo, la capacità di selezionare, elaborare ed interpretare problemi di sicurezza informatica complessi. Il piano di studi comprende attività di esercitazione autonoma e di gruppo affinché lo studente sia in grado di valutare autonomamente i risultati ottenuti da questo tipo di attività didattica. Tra le finalità di queste attività ci sono lo sviluppo della capacità di lavorare in gruppo, la competenza di selezionare le informazioni rilevanti per l'analisi e la risoluzione di un problema e lo sviluppo delle capacità di esprimere giudizi.

Il raggiungimento di questi obiettivi sarà valutato in tutte le prove finali degli insegnamenti.

Abilità comunicative

I laureati magistrali saranno in grado di comunicare con altri specialisti tecnico scientifici per interagire e cooperare con loro. Inoltre saranno in grado di documentare gli aspetti di sicurezza dei sistemi informatici di interesse producendo relazioni scritte utilizzando un linguaggio tecnico scientifico appropriato. Saranno anche in grado di comunicare a non specialisti le varie caratteristiche dei sistemi informatici sicuri oggetto della loro attività sia in forma scritta che orale.

Nel percorso formativo, alcuni degli insegnamenti prevedono lo svolgimento, da parte degli studenti, di attività di progetto a cui deve seguire una discussione per favorirne il coinvolgimento e prepararli al confronto pubblico con gli interlocutori.

La valutazione finale degli insegnamenti (esami di profitto) è un ulteriore strumento di

elaborazione e comunicazione del lavoro svolto: la valutazione finale dell'insegnamento è normalmente composta da una prova scritta e una prova orale. La prova finale è un'ulteriore opportunità di approfondimento e di verifica delle capacità di analisi, elaborazione e comunicazione del lavoro svolto. Essa prevede infatti, di norma, la discussione, innanzi ad una commissione, di un elaborato, con contenuti di originalità, preparato dallo studente. La tesi deve essere relativa ad un argomento o progetto a carattere innovativo, svolta in autonomia dallo studente. La tesi dovrà documentare i risultati innovativi ottenuti nonché i collegamenti del lavoro svolto con lo stato delle conoscenze nel settore della scienza e delle tecnologie informatiche.

<p>Capacità di apprendimento</p>	<p>Il laureato magistrale in Cybersecurity è dotato di una preparazione culturale, scientifica e metodologica di base che gli permette di accedere ai livelli di studio universitario successivi al magistrale, quali il Dottorato di Ricerca in Informatica o in Ingegneria Informatica. La suddivisione delle ore di lavoro complessive previste per lo studente dà un forte rilievo alle ore di lavoro personale proprio per offrire allo studente la possibilità di verificare e migliorare la propria capacità di apprendimento autonomo. Analogo obiettivo viene perseguito con il rigore metodologico dell'impostazione degli insegnamenti, che deve portare lo studente a sviluppare l'attitudine a un ragionamento orientato alla risoluzione di problemi (problem solving) con solide basi scientifiche e metodologiche che, sulla base di precise ipotesi, porti alla conseguente risoluzione di un problema ed alla dimostrazione della correttezza ed adeguatezza della soluzione prodotta. Gli strumenti utili al conseguimento di questa abilità sono anche le attività progettuali e laboratoriali, e la prova finale. Le capacità di apprendimento sono verificate in tutte le prove finali degli insegnamenti.</p>	
---	--	--

 **QUADRO A4.d** | **Descrizione sintetica delle attività affini e integrative**

05/05/2022

Le attività affini indicate nel Regolamento didattico permettono di approfondire in senso multidisciplinare e interdisciplinare le conoscenze caratterizzanti fornite nel CdS, già di per sé profondamente interdisciplinari, e permettono anche di consolidare le conoscenze di base in materie informatiche ed ingegneristiche tramite insegnamenti di informatica, ingegneria informatica, elettronica e delle telecomunicazioni.

Per gli studenti che provengono da un percorso formativo precedente in aree non informatiche, l'attivazione di insegnamenti "affini" intende favorire l'acquisizione di competenze multidisciplinari legate ai linguaggi e ai sistemi informatici, mentre per gli studenti provenienti da aree informatiche gli insegnamenti di tipologia "affine" favoriscono l'acquisizione di competenze legate alle reti di telecomunicazione e alle piattaforme elettroniche digitali.

Inoltre, l'inserimento di un insegnamento affine di SSD ING-INF/01 legato alla sicurezza nell'hardware e nei sistemi embedded offre un significativo complemento e rafforzamento del percorso formativo su tematiche sempre legate alla cybersecurity e ritenute rilevanti per la formazione degli studenti, anche in vista dell'inserimento nel mondo del lavoro.

 **QUADRO A5.a** | **Caratteristiche della prova finale**

09/12/2019

La laurea magistrale in Cybersecurity si consegue con il superamento di una prova finale consistente nella discussione di una tesi con contenuti di originalità, preparata in autonomia dallo studente sotto la supervisione di uno o più relatori (almeno uno dei quali interno al corso di studi).

La tesi deve essere relativa ad un argomento o progetto a carattere innovativo, svolta in autonomia. E può essere anche

svolta presso un'azienda o un ente esterno. Dovrà inoltre documentare i risultati innovativi ottenuti nonché i collegamenti del lavoro svolto con lo stato delle conoscenze nel settore della scienza e delle tecnologie della sicurezza informatica. Lo svolgimento della tesi consente al laureato magistrale di acquisire ulteriori conoscenze che gli permetteranno un adeguato inserimento nel mondo del lavoro, ed anche eventualmente la prosecuzione del percorso formativo in un dottorato di ricerca.



27/12/2019

La prova finale del corso di studio è sostenuta dinanzi ad una commissione che esprime un voto in centodecimi. Il voto viene determinato sommando alla media degli esami, pesata rispetto al numero di CFU, la valutazione del curriculum e della discussione della tesi.

Fatte salve le prerogative di legge della Commissione di laurea, le modalità di calcolo del voto di laurea sono le seguenti:

- le attività formative con voto, presenti nel piano di studio approvato, contribuiscono a formare una media pesata che viene trasformata in centodecimi, arrotondandola all'intero più vicino;
- le attività senza voto e quelle non presenti nel piano di studi, non contribuiscono a tale media;
- nel calcolo della media gli esami con lode vengono valutati 32/30;
- la prova finale non contribuisce alla media, ma viene valutata collegialmente dalla Commissione di Laurea per determinare un incremento che può andare da 1 a 7 punti, considerando sia la qualità che l'originalità della tesi, sia la presentazione orale, sia il curriculum globale del candidato.

Se la somma S della media arrotondata e dell'incremento:

- è minore o uguale a 110, S è il voto di laurea;
- è uguale a 111, il voto di laurea è 110;
- è maggiore o uguale a 112 e il candidato ha ottenuto meno di 5 punti di incremento per la prova finale, il voto di laurea è 110;
- è maggiore o uguale a 112 e il candidato ha ottenuto almeno 5 punti di incremento per la prova finale, il voto di laurea è 110 e lode.



▶ QUADRO B1

Descrizione del percorso di formazione (Regolamento Didattico del Corso)

Pdf inserito: [visualizza](#)

Descrizione Pdf: Percorso formativo corso di Laurea Magistrale in Cybersecurity (WCY-LM)

Link: <https://www.unipi.it/index.php/lauree/corso/11291>

▶ QUADRO B2.a

Calendario del Corso di Studio e orario delle attività formative

<http://www.ing.unipi.it/it/studiare-a-ingegneria/orario-delle-lezioni>

▶ QUADRO B2.b

Calendario degli esami di profitto

<http://www.ing.unipi.it/it/studiare-a-ingegneria/esami-e-prove-in-itinere/calendari-esami>

▶ QUADRO B2.c

Calendario sessioni della Prova finale

<http://www.ing.unipi.it/it/studiare-a-ingegneria/sedute-di-laurea/date-di-laurea>

▶ QUADRO B3

Docenti titolari di insegnamento

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.	ING-INF/05	Anno di	APPLIED CRYPTOGRAPHY link			9		

		corso 1							
2.	ING- INF/03	Anno di corso 1	COMMUNICATION TECHNOLOGIES (modulo di <i>ELECTRONICS AND COMMUNICATION TECHNOLOGIES</i>) link	LUISE MARCO	PO	6	24		
3.	ING- INF/03	Anno di corso 1	COMMUNICATION TECHNOLOGIES (modulo di <i>ELECTRONICS AND COMMUNICATION TECHNOLOGIES</i>) link	BACCI GIACOMO	RD	6	24		
4.	INF/01	Anno di corso 1	DATA AND SYSTEM SECURITY link	CHESSA STEFANO	PO	9	72		
5.	ING- INF/01 ING- INF/03	Anno di corso 1	ELECTRONICS AND COMMUNICATION TECHNOLOGIES link			12			
6.	ING- INF/01	Anno di corso 1	ELECTRONICS SYSTEMS (modulo di <i>ELECTRONICS AND COMMUNICATION TECHNOLOGIES</i>) link	SALETTI ROBERTO	PO	6	24		
7.	ING- INF/01	Anno di corso 1	ELECTRONICS SYSTEMS (modulo di <i>ELECTRONICS AND COMMUNICATION TECHNOLOGIES</i>) link	BARONTI FEDERICO	PA	6	24		
8.	ING- INF/01	Anno di corso 1	HARDWARE AND EMBEDDED SECURITY link	ROSSI DANIELE	PA	9	32		
9.	ING- INF/01	Anno di corso 1	HARDWARE AND EMBEDDED SECURITY link	SAPONARA SERGIO	PO	9	40		
10.	IUS/01	Anno di corso 1	INFORMATION AND TECHNOLOGY LAW (modulo di <i>ORGANIZATIONAL SCIENCES AND INFORMATION AND TECHNOLOGY LAW (OL)</i>) link	CASAROSA FEDERICA		6	24		
11.	IUS/01	Anno di corso 1	INFORMATION AND TECHNOLOGY LAW (modulo di <i>ORGANIZATIONAL SCIENCES AND INFORMATION AND TECHNOLOGY LAW (OL)</i>) link	000000 00000		6	24		
12.	INF/01	Anno di corso 1	LANGUAGE-BASED TECHNOLOGY FOR SECURITY link	BODEI CHIARA	PA	9	24		

13.	INF/01	Anno di corso 1	LANGUAGE-BASED TECHNOLOGY FOR SECURITY link	FERRARI GIAN-LUIGI	PO	9	48	
14.	INF/01	Anno di corso 1	LANGUAGES FOR INFORMATICS (modulo di SYSTEMS AND LANGUAGES FOR INFORMATICS) link	PAGANELLI FEDERICA	PA	6	48	
15.	SECS-P/10	Anno di corso 1	ORGANIZATIONAL SCIENCES (modulo di ORGANIZATIONAL SCIENCES AND INFORMATION AND TECHNOLOGY LAW (OL)) link	NICCOLINI FEDERICO	PA	6	48	
16.	IUS/01 SECS-P/10	Anno di corso 1	ORGANIZATIONAL SCIENCES AND INFORMATION AND TECHNOLOGY LAW (OL) link				12	
17.	INF/01 ING-INF/05	Anno di corso 1	SYSTEMS AND LANGUAGES FOR INFORMATICS link				12	
18.	ING-INF/05	Anno di corso 1	SYSTEMS FOR INFORMATICS (modulo di SYSTEMS AND LANGUAGES FOR INFORMATICS) link	ANASTASI GIUSEPPE	PO	6	48	



QUADRO B4

Aule

Descrizione link: Sistema informatico di gestione delle aule (Gestione Aule Poli - GAP)

Link inserito: <http://gap.adm.unipi.it/GAP-SI/>

Pdf inserito: [visualizza](#)

Descrizione Pdf: Scuola di Ingegneria - Aule didattiche



QUADRO B4

Laboratori e Aule Informatiche

Pdf inserito: [visualizza](#)

Descrizione Pdf: Dipartimento di Ingegneria dell'informazione - Laboratori e aule informatiche



QUADRO B4

Sale Studio

Descrizione link: Sale studio dell'Università di Pisa

Link inserito: <https://www.unipi.it/index.php/servizi-e-orientamento/item/1300-sale-studio>



QUADRO B4

Biblioteche

Descrizione link: Biblioteca di Ingegneria

Link inserito: <http://www.sba.unipi.it/it/biblioteche/polo-5/ingegneria>



QUADRO B5

Orientamento in ingresso

04/05/2021

Descrizione link: Sito web di ateneo sull'Orientamento in ingresso

Link inserito: <https://orientamento.unipi.it/>

Pdf inserito: [visualizza](#)

Descrizione Pdf: Orientamento in ingresso



QUADRO B5

Orientamento e tutorato in itinere

10/02/2020

Descrizione link: Sito web di ateneo sull'Orientamento

Link inserito: <https://www.unipi.it/index.php/servizi-e-orientamento>

Pdf inserito: [visualizza](#)

Descrizione Pdf: Orientamento e tutorato in itinere



QUADRO B5

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

04/02/2020

Descrizione link: Sito web di ateneo sui Tirocini

Link inserito: <https://www.unipi.it/index.php/tirocini-e-job-placement>

Pdf inserito: [visualizza](#)

Descrizione Pdf: Assistenza per periodi di formazione all'esterno



QUADRO B5

Assistenza e accordi per la mobilità internazionale degli studenti



In questo campo devono essere inserite tutte le convenzioni per la mobilità internazionale degli studenti attivate con Atenei stranieri, con l'eccezione delle convenzioni che regolamentano la struttura di corsi interateneo; queste ultime devono invece essere inserite nel campo apposito "Corsi interateneo".

Per ciascun Ateneo straniero convenzionato, occorre inserire la convenzione che regola, fra le altre cose, la mobilità degli studenti, e indicare se per gli studenti che seguono il relativo percorso di mobilità sia previsto il rilascio di un titolo doppio o multiplo. In caso non sia previsto il rilascio di un titolo doppio o multiplo con l'Ateneo straniero (per esempio, nel caso di convenzioni per la mobilità Erasmus) come titolo occorre indicare "Solo italiano" per segnalare che gli studenti che seguono il percorso di mobilità conseguiranno solo il normale titolo rilasciato dall'ateneo di origine.

Pdf inserito: [visualizza](#)

Descrizione Pdf: Mobilità internazionale degli studenti

Descrizione link: Mobilità internazionale degli studenti

Link inserito: <https://www.unipi.it/index.php/internazionale>

n.	Nazione	Ateneo in convenzione	Codice EACEA	Data convenzione	Titolo
1	Austria	Universitaet Graz	A GRAZ01	22/03/2022	solo italiano
2	Belgio	Katholieke Universiteit Leuven	B LEUVEN01	22/03/2022	solo italiano
3	Belgio	Universite Catholique De Louvain	B LOUVAIN01	22/03/2022	solo italiano
4	Belgio	Universite De Liege	B LIEGE01	22/03/2022	solo italiano
5	Belgio	Universite De Namur Asbl	B NAMUR01	22/03/2022	solo italiano

6	Belgio	Universiteit Hasselt	B DIEPENB01	22/03/2022	solo italiano
7	Belgio	Vrije Universiteit Brussel	B BRUSSEL01	22/03/2022	solo italiano
8	Bulgaria	St. Cyril And St. Methodius University Of Veliko Turnovo	BG VELIKO01	22/03/2022	solo italiano
9	Danimarca	Kobenhavns Universitet	DK KOBENHA01	22/03/2022	solo italiano
10	Estonia	Tartu Ulikool	EE TARTU02	22/03/2022	solo italiano
11	Finlandia	Helsingin Yliopisto	SF HELSINK01	22/03/2022	solo italiano
12	Finlandia	Lappeenrannan Teknillinen Yliopisto	SF LAPPEEN01	22/03/2022	solo italiano
13	Francia	Association Isep - Edouard Branly	F PARIS376	22/03/2022	solo italiano
14	Francia	Association L'Éonard De Vinci	F PARIS270	22/03/2022	solo italiano
15	Francia	Ecole Nationale De L Aviation Civile	F TOULOUS18	22/03/2022	solo italiano
16	Francia	Ecole Nationale Superieure D'Arts Et Metiers	F PARIS062	22/03/2022	solo italiano
17	Francia	Ecole Nationale Superieure De Mecanique Et D'Aerotechnique	F POITIER05	22/03/2022	solo italiano
18	Francia	Eurecom	F CANNES09	22/03/2022	solo italiano
19	Francia	Groupe 3il	F LIMOGES20	22/03/2022	solo italiano
20	Francia	Institut Polytechnique De Bordeaux	F BORDEAU54	22/03/2022	solo italiano
21	Francia	Institut Polytechnique De Grenoble	F GRENOBL22	22/03/2022	solo italiano
22	Francia	Institut Superieur De L'Aeronautique Et De L'Espace	F TOULOUS16	22/03/2022	solo italiano
23	Francia	SORBONNE UNIVERSITE		22/03/2022	solo italiano
24	Francia	UNIVERSITE' PARIS-SACLAY		22/03/2022	solo italiano
25	Francia	Universite Charles De Gaulle Lille3	F LILLE03	22/03/2022	solo italiano

26	Francia	Universite Paris Descartes	F PARIS005	22/03/2022	solo italiano
27	Francia	Yncrea Mediterranee	F TOULON19	22/03/2022	solo italiano
28	Germania	Christian-Albrechts-Universitaet Zu Kiel	D KIEL01	22/03/2022	solo italiano
29	Germania	Freie Universitaet Berlin	D BERLIN01	22/03/2022	solo italiano
30	Germania	Friedrich-Alexander-Universitaet Erlangen Nuernberg	D ERLANGE01	22/03/2022	solo italiano
31	Germania	Gottfried Wilhelm Leibniz Universitaet Hannover	D HANNOVE01	22/03/2022	solo italiano
32	Germania	Heinrich-Heine-Universitaet Duesseldorf	D DUSSELD01	22/03/2022	solo italiano
33	Germania	Hochschule Anhalt	D KOTHE01	22/03/2022	solo italiano
34	Germania	Hochschule Esslingen	D ESSLING03	22/03/2022	solo italiano
35	Germania	Johann Wolfgang Goethe Universitaet Frankfurt Am Main	D FRANKFU01	22/03/2022	solo italiano
36	Germania	Otto-Von-Guericke-Universitaet Magdeburg	D MAGDEBU01	22/03/2022	solo italiano
37	Germania	Rheinisch-Westfaelische Technische Hochschule Aachen	D AACHEN01	22/03/2022	solo italiano
38	Germania	Stiftung Universitaet Hildesheim	D HILDESH01	22/03/2022	solo italiano
39	Germania	Technische Hochschule Deggendorf	D DEGGEND01	22/03/2022	solo italiano
40	Germania	Technische Hochschule Ingolstadt	D INGOLST01	22/03/2022	solo italiano
41	Germania	Technische Universitaet Muenchen	D MUNCHEN02	22/03/2022	solo italiano
42	Germania	Technische Universitaet Braunschweig	D BRAUNSC01	22/03/2022	solo italiano
43	Germania	Universitaet Bielefeld	D BIELEFE01	22/03/2022	solo italiano
44	Germania	Universitaet Leipzig	D LEIPZIG01	22/03/2022	solo italiano
45	Germania	Universitaet Des Saarlandes	D SAARBRU01	22/03/2022	solo italiano

46	Germania	Universitat Passau	D PASSAU01	22/03/2022	solo italiano
47	Grecia	Aristotelio Panepistimio Thessalonikis	G THESSAL01	22/03/2022	solo italiano
48	Grecia	Athens University Of Economics And Business - Research Center	G ATHINE04	22/03/2022	solo italiano
49	Grecia	University Of Macedonia	G THESSAL02	22/03/2022	solo italiano
50	Norvegia	Hogskolen I Ostfold	N HALDEN02	22/03/2022	solo italiano
51	Norvegia	Norges Teknisk-Naturvitenskapelige Universitet Ntnu	N TRONDHE01	22/03/2022	solo italiano
52	Norvegia	Universitetet I Agder	N KRISTIA01	22/03/2022	solo italiano
53	Norvegia	Universitetet I Stavanger	N STAVANG01	22/03/2022	solo italiano
54	Paesi Bassi	Stichting Christelijke Hogeschool Windesheim	NL ZWOLLE05	22/03/2022	solo italiano
55	Paesi Bassi	Stichting Vu	NL AMSTERD02	22/03/2022	solo italiano
56	Paesi Bassi	Technische Universiteit Delft	NL DELFT01	22/03/2022	solo italiano
57	Paesi Bassi	Technische Universiteit Eindhoven	NL EINDHOV17	22/03/2022	solo italiano
58	Paesi Bassi	Universiteit Leiden	NL LEIDEN01	22/03/2022	solo italiano
59	Paesi Bassi	Universiteit Twente	NL ENSCHED01	22/03/2022	solo italiano
60	Polonia	Akademia Gorniczo-Hutnicza Im. Stanislaw Staszica W Krakowie	PL KRAKOW02	22/03/2022	solo italiano
61	Polonia	Politechnika Lodzka	PL LODZ02	22/03/2022	solo italiano
62	Polonia	Politechnika Slaska	PL GLIWICE01	22/03/2022	solo italiano
63	Polonia	Politechnika Wroclawska	PL WROCLAW02	22/03/2022	solo italiano
64	Polonia	Szkola Glowna Gospodarstwa Wiejskiego	PL WARSZAW05	22/03/2022	solo italiano
65	Portogallo	Instituto Politecnico Do Porto	P PORTO05	22/03/2022	solo italiano

66	Portogallo	Universidade De Coimbra	P COIMBRA01	22/03/2022	solo italiano
67	Portogallo	Universidade De Evora	P EVORA01	22/03/2022	solo italiano
68	Portogallo	Universidade De Lisboa	P LISBOA109	22/03/2022	solo italiano
69	Portogallo	Universidade Do Minho	P BRAGA01	22/03/2022	solo italiano
70	Portogallo	Universidade Do Porto	P PORTO02	22/03/2022	solo italiano
71	Portogallo	Universidade Nova De Lisboa	P LISBOA03	22/03/2022	solo italiano
72	Repubblica Ceca	Vysoke Uceni Technicke V Brne	CZ BRNO01	22/03/2022	solo italiano
73	Romania	Universitatea Babes Bolyai	RO CLUJNAP01	22/03/2022	solo italiano
74	Romania	Universitatea De Vest Din Timisoara	RO TIMISOA01	22/03/2022	solo italiano
75	Romania	Universitatea Politehnica Din Bucuresti	RO BUCURES11	22/03/2022	solo italiano
76	Romania	Universitatea Transilvania Din Brasov	RO BRASOV01	22/03/2022	solo italiano
77	Slovenia	Univerza Na Primorskem Universita Del Litorale	SI KOPER03	22/03/2022	solo italiano
78	Spagna	Universidad Autonoma De Madrid	E MADRID04	22/03/2022	solo italiano
79	Spagna	Universidad Carlos Iii De Madrid	E MADRID14	22/03/2022	solo italiano
80	Spagna	Universidad De Alcala	E ALCAL-H01	22/03/2022	solo italiano
81	Spagna	Universidad De Cadiz	E CADIZ01	22/03/2022	solo italiano
82	Spagna	Universidad De La Iglesia De Deusto	E BILBAO02	22/03/2022	solo italiano
83	Spagna	Universidad De Malaga	E MALAGA01	22/03/2022	solo italiano
84	Spagna	Universidad De Oviedo	E OVIEDO01	22/03/2022	solo italiano
85	Spagna	Universidad De Sevilla	E SEVILLA01	22/03/2022	solo italiano

86	Spagna	Universidad De Valladolid	E VALLADO01	22/03/2022	solo italiano
87	Spagna	Universidad Politecnica De Cartagena	E MURCIA04	22/03/2022	solo italiano
88	Spagna	Universidad Politecnica De Madrid	E MADRID05	22/03/2022	solo italiano
89	Spagna	Universidad Pontificia Comillas	E MADRID02	22/03/2022	solo italiano
90	Spagna	Universidad Rey Juan Carlos	E MADRID26	22/03/2022	solo italiano
91	Spagna	Universitat Autonoma De Barcelona	E BARCELO02	22/03/2022	solo italiano
92	Spagna	Universitat De Barcelona	E BARCELO01	22/03/2022	solo italiano
93	Spagna	Universitat De Les Illes Balears	E PALMA01	22/03/2022	solo italiano
94	Spagna	Universitat Politecnica De Catalunya	E BARCELO03	22/03/2022	solo italiano
95	Spagna	Universitat Politecnica De Valencia	E VALENCI02	22/03/2022	solo italiano
96	Spagna	Universitat Rovira I Virgili	E TARRAGO01	22/03/2022	solo italiano
97	Svezia	Hoegskolan I Boras	S BORAS01	22/03/2022	solo italiano
98	Turchia	Bahcesehir Universitesi Foundation	TR ISTANBU08	22/03/2022	solo italiano
99	Turchia	Kocaeli Universitesi	TR KOCAELI02	22/03/2022	solo italiano
100	Ungheria	Szegedi Tudomanyegyetem	HU SZEGED01	22/03/2022	solo italiano



QUADRO B5

Accompagnamento al lavoro

04/02/2020

Descrizione link: Il servizio di Career Service di Ateneo

Link inserito: <https://www.unipi.it/index.php/career-service>

Pdf inserito: [visualizza](#)

Descrizione Pdf: Accompagnamento al lavoro



QUADRO B5

Eventuali altre iniziative

29/04/2022

La LM in Cybersecurity si appoggia alla Scuola di Ingegneria e alle strutture del Dipartimento di Ingegneria dell'Informazione per le varie iniziative in tema di orientamento. In particolare, la Scuola di Ingegneria nomina un referente per l'orientamento per ciascun dipartimento. Inoltre, gli studenti possono richiedere un colloquio di orientamento rivolgendosi direttamente al presidente del CdS o tramite richiesta al responsabile dell'Unità Didattica di Ingegneria dell'Informazione.

Il CdS partecipa inoltre all'evento di orientamento 'Open Day' organizzato dalla Scuola di Ingegneria, e nel quale il CdS è stato presentato agli studenti delle lauree triennali il 17 Maggio 2021.

Descrizione link: Pagina dell'Orientamento della Scuola di Ingegneria

Link inserito: <http://www.ing.unipi.it/it/entrare-a-ingegneria/orientamento-in-entrata>



QUADRO B6

Opinioni studenti

14/09/2022

Si riassumono i dati ricavati dai questionari di valutazione della didattica relativi all'A.A. 2021/22, che è il secondo anno nel quale il corso di studi è stato fino ad ora attivo. I risultati sono stati elaborati dall'Ufficio Programmazione, Valutazione e Statistica dell'Ateneo e si riferiscono ad un totale di 438 questionari compilati dagli studenti.

Dal quadro riassuntivo, rappresentato dalle medie per singola domanda a livello di corso di studio, riportato nella prima tabella (vedi PDF allegato) estratta dal rapporto, emerge un giudizio positivo su tutti gli indicatori. In particolare, rispetto all'unico altro anno nel quale esistono dati, l'A.A. 2020/21, si evince un netto miglioramento delle valutazioni medie del corso di studio su quasi tutte le domande. L'unica eccezione è relativa alla domanda BV_A5 sull'adeguatezza delle aule virtuali, dove la valutazione dell'A.A. 21/22 è stata inferiore all'A.A. 20/21. C'è però da considerare che a differenza dell'anno precedente, nel A.A. 21/22 le lezioni sono state erogate in modalità mista e quindi con maggiori problematiche nell'uso delle aule virtuali.

Sono inoltre da segnalare:

- l'indicatore BS2 (giudizio complessivo medio sugli insegnamenti) riporta un valore pari a 3,2 (rispetto a 3,0 nell'A.A. precedente)
- l'indicatore BS1 (interesse degli studenti per gli argomenti trattati nel corso) è cresciuto da 3,1 a 3,3
- sono cresciute significativamente le valutazioni per gli indicatori B6 e B7 sulla capacità dei docenti di stimolare interesse e di esporre gli argomenti in modo chiaro
- l'indicatore B2 sul carico didattico non è facilmente confrontabile con l'anno precedente (è cambiata la modalità di valutazione), risulta comunque positivo con una valutazione di 3,1
- è migliorato sensibilmente l'indicatore B3 sul materiale didattico (da 2,7 a 3,2)
- dall'analisi del grafico 1 del rapporto risulta che la percentuale di giudizi completamente negativi è molto bassa, generalmente inferiore rispetto all'anno precedente, e comunque sempre inferiore al 6,4% dell'indicatore B3 (sul carico didattico), ad esclusione dell'indicatore BP che però riguarda la frequenza degli studenti
- relativamente alla presenza degli studenti alle lezioni (indicatore BP), anche questo è in miglioramento rispetto all'A.A.

20/21, con circa il 14% degli studenti dichiara di aver seguito meno del 25% delle lezioni, ma d'altra parte, il 60% degli studenti dichiara la "frequenza completa" e più dell'80% degli studenti dichiara di aver seguito almeno il 50% delle lezioni.

Per quanto riguarda i commenti degli studenti espressi nel campo a testo libero, la maggior parte di questi sono di tipo costruttivo e nella maggior parte dei casi stimolano i docenti a potenziare i contenuti pratici rispetto alla teoria e ad inserire più attività laboratoriali e a migliorare il materiale didattico. Alcuni commenti suggeriscono di migliorare il materiale didattico o di potenziare la trattazione di argomenti di base ritenuti pre-requisiti del corso.

In riferimento ai singoli insegnamenti, le valutazioni sono stratificate su 2 gruppi di rispondenti (gruppi A e B): il primo è relativo agli studenti che hanno dichiarato di aver frequentato il corso nell'A.A. corrente 2021/22, il secondo è composto da coloro che hanno frequentato in A.A. precedenti ma con lo stesso docente.

Dai dati emerge un quadro complessivamente positivo per tutti gli insegnamenti. In particolare si segnala come ogni singolo modulo di insegnamento riceva una valutazione complessivamente positiva (indicatore BS2), con valutazioni comprese tra 2,6 e 3,6. Inoltre gli studenti dichiarano interesse negli argomenti di ogni singolo modulo (indicatore BS1) con valutazioni positive comprese tra 2,5 e 3,9.

In riferimento ai risultati del gruppo A (che sono anche i più numerosi) emergono pochissime criticità:

- per tre moduli di insegnamento emerge una valutazione inferiore al valore di 2,5 relativa al carico didattico (rispettivamente 2,1; 2,3 e 2,3);
- per un modulo di insegnamento risulta una valutazione di 2,4 (appena inferiore al valore soglia 2,5) relativamente all'indicatore B6 (capacità del docente di stimolare interesse verso la disciplina).

Relativamente a queste criticità c'è comunque da considerare il fatto che tre di questi moduli sono nuovi in quanto progettati espressamente per questo Corso di Studio e quindi non derivati o mutuati da altri insegnamenti, e pertanto sono stati tenuti dai docenti per la prima volta. Una valutazione obiettiva sarà possibile nei prossimi anni quando potranno essere analizzate le serie storiche relative a queste valutazioni.

A tal proposito si segnala come tutte le criticità emerse nelle valutazioni dell'A.A. 20/21 per gli insegnamenti nuovi del primo anno siano poi scomparse nelle valutazioni dell'A.A. 201/22, segno che i corsi nuovi avevano bisogno di un adeguato "rodaggio".

In riferimento ai risultati del gruppo B emergono più criticità, ma c'è da osservare che sono dati relativi ad un numero sensibilmente inferiore di questionari e pertanto poco significativi rispetto ai dati del gruppo A. Inoltre, in molti casi questi dati si riferiscono a valutazioni su corsi nuovi, tenuti dai docenti per la prima volta nell'A.A. 20/21, e pertanto anche per questi bisogna attendere per poter effettuare una valutazione più obiettiva.

Pdf inserito: [visualizza](#)



QUADRO B7

Opinioni dei laureati

14/09/2022

Il corso di studio è stato attivato nell'A.A. 2020/21 e al momento tutti gli studenti sono ancora iscritti al primo o al secondo anno. Solo uno studente si laureato nella sessione estiva 2022 e pertanto non è ancora possibile presentare alcun risultato relativo all'opinione dei laureati.



▶ QUADRO C1

Dati di ingresso, di percorso e di uscita

14/09/2022

Il corso di studio è stato attivato nell'A.A. 2020/21, pertanto non esistono serie storiche con le quali poter effettuare un confronto, ma è solo possibile confrontare i dati dell'A.A. in corso con il precedente.

Per quanto riguarda i dati di ingresso, il numero di immatricolati nell'A.A. 2021/2022 è pari a 47, in leggera crescita rispetto all'A.A. precedente:

- il 61,5% proviene da una laurea della classe L-8;
- il 30,8% proviene da una laurea della classe L-31;
- il 2,6% proviene da una laurea della classe 9;
- il 5,1% proviene da una laurea della classe 26.

sempre relativamente agli immatricolati nell'A.A. 21/22, poco più del 40% degli studenti proviene da altri atenei (in significativo aumento rispetto all'A.A. precedente), con una percentuale significativa e in aumento (17%) di studenti stranieri. Da un punto di vista territoriale, solo il 17% (in riduzione) degli studenti proviene dalle province di Pisa, Lucca e Livorno. Per quanto riguarda la distribuzione di genere, la componente femminile risulta minoritaria (4,3%).

Per quanto riguarda invece i dati di percorso, gli studenti attivi sono il 93,9% di quelli iscritti al secondo anno (coorte 2020) e l'80,9% di quelli iscritti al primo anno (coorte 2021).

Il voto medio conseguito agli esami dagli studenti attivi è pari a 26,8 (coorte 2021) e 26,6 (coorte 2020) con una deviazione standard non superiore a 3,0 in entrambi i casi. I dati relativi al numero medio di CFU ottenuti dagli studenti attivi è pari a 56,6 con deviazione standard pari a 22,2 per gli studenti della coorte 2020, e pari a 15,6 con deviazione standard pari a 6,8 per gli studenti della coorte 2021.

Infine, si segnala un numero limitato di rinunce agli studi, pari al 15,8% degli studenti della coorte 2020 e al 2,1% per gli studenti della coorte 2021.

▶ QUADRO C2

Efficacia Esterna

14/09/2022

Il corso di studio è stato attivato nell'A.A. 2020/21 e al momento un solo studente si è laureato nella sessione estiva del 2022 e non è quindi possibile presentare alcun risultato relativo all'efficacia esterna.

▶ QUADRO C3

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

Non sono previste attività di stage o tirocinio in ambito curricolare, ma sono possibili tirocini extra curricolari o tesi in azienda. Al momento sono disponibili i dati relativi ad un'unica tesi svolta in azienda, dal quale risulta che l'azienda ospitante è stata notevolmente soddisfatta della preparazione universitaria dello studente.

Infine, il corso di studio mantiene stretti e continui contatti con le imprese del territorio, nazionali ed internazionali e con gli enti di ricerca, per attività seminariali e collaborazioni per tesi di laurea, al fine di favorire la possibilità di occupazione dei laureati.