

AMMINISTRAZIONE CENTRALE
 AREA DIDATTICA E SERVIZI AGLI STUDENTI
 UFFICIO OFFERTA FORMATIVA ED
 ASSICURAZIONE DELLA QUALITA'

1222·2022
 800
 A N N I



UNIVERSITÀ
 DEGLI STUDI
 DI PADOVA

Decreto Rep. Prot. n.
 Anno 2020 Tit. III Cl. 2 Fasc. 4 All. n. 2

OGGETTO: Regolamento Didattico di Ateneo – Istituzione di ordinamenti didattici di Corso di studio.

IL RETTORE

Vista la legge 19 novembre 1990, n. 341, art. 11 c. 1;

Visto il decreto del Ministro dell'Istruzione, dell'Università e della Ricerca (MIUR) del 22 ottobre 2004 n. 270, "Modifiche al regolamento recante norme concernenti l'autonomia didattica degli atenei, approvato con decreto del Ministro dell'Università e della Ricerca scientifica e tecnologica 3 novembre 1999, n. 509";

Visto il decreto MIUR del 16 marzo 2007, relativo alla determinazione delle Classi delle Lauree Magistrali;

Visto il decreto MIUR del 7 gennaio 2019, n. 6, avente ad oggetto "Autovalutazione, valutazione, accreditamento iniziale e periodico delle sedi e dei corsi di studio";

Viste le note MIUR del 12 novembre 2019 "Banche Dati RAD e SUA-CdS per accreditamento corsi a.a. 2020-21. Indicazioni operative" e del 27 dicembre 2019 "Banche Dati RAD e SUA-CdS per accreditamento corsi a.a. 2020-2021 – chiarimenti e integrazioni alle indicazioni operative";

Viste la delibera del Consiglio della Scuola di Scienze del 24 ottobre 2019 e la comunicazione del Presidente del Consiglio della Scuola di Scienze del 21 novembre 2019 con le quali è stata proposta agli Organi Centrali l'istituzione degli ordinamenti didattici dei Corsi di Laurea Magistrali in Cybersecurity LM-66 e in Geophysics for natural risks LM-79;

Vista la delibera del Senato Accademico n. 1 del 21 gennaio 2020, con la quale è stata approvata l'istituzione degli ordinamenti didattici dei Corsi di Laurea Magistrali in Cybersecurity LM-66 e in Geophysics for natural risks LM-79;

Vista la proposta di integrazione del Regolamento Didattico di Ateneo contenente i suddetti ordinamenti didattici, trasmessa al MIUR dal Rettore dell'Università degli Studi di Padova con nota prot.14662 del 21 gennaio 2020;

Visti i rilievi resi dal CUN nell'adunanza del 29 gennaio 2020 in merito ai corsi di studio di nuova istituzione e il successivo parere favorevole espresso dal CUN nell'adunanza del 19 febbraio 2020, a seguito della riformulazione dell'ordinamento didattico;

Vista la nota MUR del 20 febbraio 2020 con la quale si trasmette il provvedimento direttoriale che all'art. 2 decreta che il Rettore provvederà ad emanare con proprio decreto la modifica del Regolamento Didattico di Ateneo relativamente ai corsi di studio di nuova istituzione per l'a.a. 2020/21;

La/II Responsabile del procedimento amministrativo Cristina Stocco	La/II Dirigente Andrea Grappeggia	Il Direttore Generale Alberto Scuttari
--	--	---

Richiamato lo Statuto dell'Università degli Studi di Padova, emanato con decreto rettorale rep. n. 3276/2011, e modificato con decreto rettorale rep. n. 1664/2012, e in particolare l'art. 10 co. 2 lett. c;

Preso atto che la struttura proponente ha accertato la conformità del provvedimento alla legislazione vigente e ai Regolamenti di Ateneo;

DECRETA

1. di procedere ad integrare il Regolamento Didattico dell'Università degli Studi di Padova - Parte seconda, con i seguenti ordinamenti didattici:

LM-66 – Sicurezza informatica

- Cybersecurity

LM-79 – Scienze geofisiche

- Geophysics for natural risks

Gli ordinamenti didattici dei Corsi di studio sono quelli risultanti sul sito MIUR Banca Dati RAD. Sono inoltre allegati al presente decreto e ne costituiscono parte integrante;

2. che i Corsi di studio con i suddetti ordinamenti didattici possano essere attivati a partire dall'Offerta formativa 2020/2021;
3. di incaricare l'Ufficio Offerta formativa ed Assicurazione della qualità dell'esecuzione del presente provvedimento, che verrà registrato nel Repertorio Generale dei Decreti;

Padova, data della registrazione

Il Rettore
Rosario Rizzuto
firmato digitalmente ai sensi del d.lgs. 82/2005

La/Il Responsabile del procedimento amministrativo Cristina Stocco	La/Il Dirigente Andrea Grapppeggia	Il Direttore Generale Alberto Scuttari
---	---------------------------------------	---

Università	Università degli Studi di PADOVA
Classe	LM-66 - Sicurezza informatica
Nome del corso in italiano	Sicurezza Informatica <i>riformulazione di: Sicurezza Informatica (1391703)</i>
Nome del corso in inglese	Cybersecurity
Lingua in cui si tiene il corso	inglese
Codice interno all'ateneo del corso	SC2542^2020^000ZZ^ 028060
Data di approvazione della struttura didattica	15/10/2019
Data di approvazione del senato accademico/consiglio di amministrazione	21/01/2020
Data della consultazione con le organizzazioni rappresentative a livello locale della produzione, servizi, professioni	13/09/2019 -
Data del parere favorevole del Comitato regionale di Coordinamento	20/12/2019
Modalità di svolgimento	a. Corso di studio convenzionale
Eventuale indirizzo internet del corso di laurea	http://didattica.unipd.it/didattica/2020/SC2542/2020
Dipartimento di riferimento ai fini amministrativi	MATEMATICA "TULLIO LEVI-CIVITA" - DM
Altri dipartimenti	INGEGNERIA DELL'INFORMAZIONE - DEI
EX facoltà di riferimento ai fini amministrativi	
Massimo numero di crediti riconoscibili	DM 16/3/2007 Art 4 Nota 1063 del 29/04/2011

Obiettivi formativi qualificanti della classe: LM-66 Sicurezza informatica

I laureati magistrali nei corsi di laurea della classe devono:

- conoscere gli aspetti scientifici relativi alle fondamenta della progettazione, realizzazione, verifica e manutenzione di infrastrutture e sistemi informatici sicuri e protetti
- conoscere le metodologie e gli strumenti tecnologici attraverso i quali si progettano, realizzano, verificano e mantengono infrastrutture e sistemi informatici sicuri e protetti, con attenzione sia alle tecniche formali che sperimentali
- conoscere gli aspetti relativi alla organizzazione del lavoro ed alle problematiche di carattere psicologico e sociale come elementi critici rispetto alla sicurezza delle infrastrutture e dei sistemi informatici ed alla protezione dei dati informatici, nonché gli aspetti giuridici relativi al trattamento sicuro e riservato dei dati informatici e quelli bio-sanitari e bio-etici relativi alle tecniche biometriche ed al trattamento, conservazione e trasmissione dei dati sensibili riguardanti la salute
- essere capaci di comunicare efficacemente, in forma scritta e orale, in almeno una lingua dell'Unione Europea, oltre l'italiano, anche con riferimento ai lessici disciplinari
- possedere gli strumenti cognitivi di base per l'aggiornamento continuo delle proprie conoscenze
- essere in grado di lavorare con ampia autonomia, anche assumendo responsabilità di progetti e strutture, ed evidenziando capacità relazionali e decisionali.

I principali sbocchi occupazionali e professionali dei laureati magistrali di questa classe sono negli ambiti della sicurezza di infrastrutture e sistemi informatici e del trattamento di dati sensibili per imprese, aziende di servizi, enti della pubblica amministrazione e, più in generale, per qualunque organizzazione utilizzi sistemi informatici complessi.

Ai fini indicati, i curricula dei corsi di laurea magistrale della classe:

- prevedono lezioni ed esercitazioni di laboratorio oltre ad attività progettuali autonome e attività individuali in laboratorio per non meno di 10 crediti;
- prevedono, in relazione a obiettivi specifici, attività esterne come tirocini formativi presso aziende, strutture della pubblica amministrazione e laboratori, oltre a soggiorni di studio presso altre università italiane ed europee, anche nel quadro di accordi internazionali.

In considerazione della valenza sia scientifica che professionalizzante di questo percorso formativo, l'ammissione ai corsi di laurea magistrale della classe richiede il possesso di requisiti curriculari che prevedano, comunque, un'adeguata padronanza di metodi e contenuti scientifici propedeutici a quelli di almeno uno degli ambiti disciplinari caratterizzanti l'ordinamento della presente classe di laurea magistrale.

Sintesi della consultazione con le organizzazioni rappresentative a livello locale della produzione, servizi, professioni

La progettazione della Laurea Magistrale in Cybersecurity è stata sin dal principio stimolata dalle numerose collaborazioni che i Dipartimenti coinvolti hanno con aziende, enti pubblici e centri di ricerca, dai quali è emersa l'urgenza di formare figure professionali e scientifiche in cui le competenze fondamentali, principalmente di Informatica e Ingegneria Informatica, siano contestualizzate in una formazione multidisciplinare, motivata dalla straordinaria varietà dei contesti in cui è necessaria la cybersecurity.

La crescente necessità a livello internazionale di profili professionali specializzati nella cybersecurity è testimoniata da studi recentissimi:

- dal rapporto redatto dall'Enterprise Strategy Group (ESG) congiuntamente con l'Information Systems Security Association che riporta i risultati di una indagine a livello mondiale condotta a cavallo fra il 2018 e il 2019. Da tale indagine risulta che la carenza di competenze in materia di cybersecurity sta peggiorando per il terzo anno consecutivo e ha avuto un impatto su quasi tre quarti (74%) delle organizzazioni intervistate;
 - da un'indagine condotta da Hays, uno dei leader globali nel recruitment specializzato IT, nel 2018 su di un campione di 300 professionisti italiani relativamente alle professioni del futuro. Da tale indagine risulta che entro il 2025 i profili tradizionali IT più ricercati vedranno al secondo posto gli "IT security specialist", e al terzo posto i "guardiani della privacy online".
- È indubbio che i risultati di queste indagini siano indice di una tendenza globale, come certificato anche dal recente rapporto "The Future of Jobs Report" 2018 del World Economic Forum (<https://www.weforum.org/reports/the-future-of-jobs-report-2018>).

Conferma all'interesse suscitato dall'iniziativa è venuta dall'incontro con le parti sociali, tenutosi presso il Dipartimento di Ingegneria dell'Informazione (DEI) il 13 settembre 2019, che ha visto un'ampia e attiva partecipazione di rappresentanti del mondo del lavoro.

Oltre ad associazioni (Assindustria, Associazione Alumni UniPD) e forze dell'ordine (quali la Polizia di Stato; nello specifico il Compartimento Polizia Postale e delle Telecomunicazioni), erano presenti circa 40 aziende sia locali, nazionali, che Internazionali (es. IBM, NTT, PWC). Le aziende presenti operano in molti settori, sia strettamente legate all'ambito della sicurezza (es. Yarix), così come più in generale nell'IT (IBM) ma anche alla consulenza (es. PWC) e di produzione (es. BFT) e servizi, incluse aziende bancarie (Intesa).

Durante la discussione sono emerse varie necessità delle aziende, che spaziano dalla conoscenza della compliance normativa, delle certificazioni, dell'analisi dei rischi, della geopolitica, del cybercrime, di architettura applicativa e di sistema, fino alle dinamiche di human-computer interaction e ai soft skills. Inoltre le aziende hanno offerto spunti sugli insegnamenti che secondo loro sono essenziali al profilo professionale e hanno sottolineato come sia comunque indispensabile fornire e salvaguardare delle basi solide.

In seguito all'incontro, che ha evidenziato un interesse generalizzato e molto sentito per il tema della cybersecurity e per le sue applicazioni in vari settori produttivi e dei servizi, è stato prodotto un documento/verbale che riepiloga i risultati della giornata: il documento è disponibile nel sito web della Scuola di Scienze <http://www.scienze.unipd.it>, alla pagina http://www.scienze.unipd.it/index.php?id=parti_sociali insieme all'ulteriore documentazione di supporto al progetto di attivazione del nuovo Corso di Studio, e viene qui allegato.

Ulteriori incontri con le parti sociali saranno fondamentali visto lo stretto legame tra questa Laurea Magistrale e le aziende, pronte a cogliere le opportunità offerte dalle nuove tecnologie.

Vedi allegato

Sintesi del parere del comitato regionale di coordinamento

Il Comitato Regionale di Coordinamento delle Università del Veneto riunitosi il giorno 20 dicembre 2019, presso L'Università degli Studi di Padova

- Visto il DPR 25 del 27 gennaio 1998, "Regolamento recante disciplina dei procedimenti relativi allo sviluppo ed alla programmazione del sistema universitario, nonché ai comitati regionali di coordinamento, a norma dell'articolo 20, comma 8, lettere a) e b), della legge 15 marzo 1997, n. 59", e in particolare l'art. 3;
- Visto il D.M. 30 gennaio 2013, n. 47, che disciplina l'autovalutazione, l'accreditamento iniziale e periodico delle sedi e dei corsi di studio e la valutazione periodica;
- Visto il decreto MIUR del 23 dicembre 2013, n. 1059: "Autovalutazione, accreditamento iniziale e periodico delle sedi e dei corsi di studio e valutazione periodica Adegamenti e integrazioni al D.M. 30 gennaio 2013, n. 47";
- Visto il Decreto Ministeriale n. 194 del 27/03/2015, "Requisiti accreditamento corsi di studio";
- Decreto Ministeriale n. 6 del 7/01/2019, "Decreto Autovalutazione, Valutazione, Accredimento iniziale e periodico delle sedi e dei corsi di studio".
- Esaminate le proposte di istituzione dei nuovi corsi di studio formulate dall'Università degli studi di Padova;
- Sentite ed accolte le motivazioni addotte per l'istituzione dei corsi.

esprime parere favorevole

subordinatamente all'approvazione da parte dei competenti organi di ciascun Ateneo, in merito all'istituzione del seguente nuovo corso di studio ai sensi del D.M.270/2004:

Cybersecurity (LM-66)
Dipartimento di Matematica
Scuola di Scienze

Obiettivi formativi specifici del corso e descrizione del percorso formativo

Le competenze richieste a un esperto di CyberSecurity, e che sono alla base di questo progetto di Laurea Magistrale, includono:
capacità di progettare, implementare, validare e mantenere infrastrutture e sistemi informatici e di comunicazione sicuri, assieme alla confidenzialità dei loro dati
conoscenza di metodi e strumenti a supporto di progettazione, implementazione, validazione e manutenzione di infrastrutture e sistemi informatici e di comunicazione sicuri, assieme ai loro dati, con attenzione sia alle tecniche formali che sperimentali
conoscenza delle basi delle aree non prettamente informatiche ma che si interfacciano direttamente con la Cybersecurity: area Economica, Giuridica e Sociale
capacità di comunicazione, sia in forma scritta che orale, in lingua inglese, con riferimento ai lessici disciplinari e tecnici
capacità di continuo apprendimento al fine di aggiornare di continuo le proprie conoscenze
capacità di lavorare sia in autonomia che in gruppo, guidando progetti e prendendo decisioni
capacità di comunicare con chiarezza i risultati e le linee strategiche più opportune risultanti dall'analisi della sicurezza dei sistemi.
Il percorso formativo è caratterizzato da una forte vocazione interdisciplinare tra l'Informatica e l'Ingegneria dell'Informazione, ed è strutturato in modo da poter accogliere studenti di varia provenienza. Gli insegnamenti riguarderanno rispettivamente:
i principi di sicurezza dell'informazione, che includono quindi i principi e le pratiche di base della cybersecurity, nonché i principi e protocolli crittografici.
strumenti di apprendimento automatico e modellazione di processi, includendo le tecniche di machine/deep learning e processi stocastici.
applicazioni ed aspetti avanzati della cybersecurity, es. biometria, aspetti di sicurezza di tecnologie quali mobile devices, IoT, social networks e impianti industriali.
nozioni di ambito giuridico, psicologico ed economico, quali: 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).
Una congrua offerta di insegnamenti opzionali permette infine la progettazione di percorsi rivolti ad ambiti specifici, quali la sicurezza del software, delle reti e dei sistemi cyber-physical.

Risultati di apprendimento attesi, espressi tramite i Descrittori europei del titolo di studio (DM 16/03/2007, art. 3, comma 7)

Conoscenza e capacità di comprensione (knowledge and understanding)

Il laureato magistrale in CyberSecurity ha solide radici nelle discipline classiche dell'Informatica e dell'Ingegneria dell'Informazione, relazionando queste con la sicurezza dei sistemi, delle infrastrutture e dei dati che l'Informatica e l'Ingegneria dell'Informazione permettono di progettare, gestire, e validare. Le discipline classiche a cui ci si riferisce includono l'algoritmica, l'ingegneria del software, le architetture dei calcolatori, i sistemi operativi, i sistemi di gestione di basi di dati e di reperimento dell'informazione, le reti di comunicazione, i sistemi distribuiti e Web, l'elaborazione di grandi moli di dati e l'elaborazione dei segnali multimediali, che si intrecciano con argomenti più avanzati come l'intelligenza artificiale, il machine learning (apprendimento automatico), le comunicazioni e il calcolo quantistico. Oltre a conoscere gli aspetti scientifici e tecnologici della cybersecurity, il laureato magistrale in CyberSecurity sa relazionare questi aspetti con l'area della psicologia, in quanto i fattori umani sono importanti sia dal punto di vista dell'interazione con i sistemi informatici (e non), che da quello delle motivazioni e dei pattern comportamentali legati agli attacchi. Sono inoltre presenti legami con l'ambito giuridico (aspetti attinenti alla regolamentazione della privacy e della sicurezza dei sistemi, nonché alle loro ricadute legali e penali) ed economico (gestione del rischio, motivazione, fattibilità e impatto degli attacchi, quali ad esempio i recenti ransomware).

Modalità e strumenti didattici per raggiungere l'obiettivo

Le conoscenze e la capacità di comprendere le problematiche ad esse correlate, sono fornite agli studenti attraverso:

- lezioni teoriche ed esercitazioni in aula;
- attività di laboratorio, che gli studenti devono essere capaci di completare operando anche autonomamente.

Strumenti per verificare che l'obiettivo sia stato raggiunto

Le modalità di verifica delle conoscenze acquisite e dei livelli di comprensione raggiunti sono in larga parte riferibili ai singoli insegnamenti e in tal caso consistono nelle prove di esame individuale finale e in verifiche in itinere basate su colloquio integrato da prove pratiche e/o scritte e su attività progettuali e di laboratorio.

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

L'esperto di CyberSecurity, formato in questa Laurea Magistrale, grazie alla interdisciplinarietà della sua formazione, saprà coordinare progetti di CyberSecurity in svariati ambiti applicativi. In particolare, sarà in grado di identificare gli elementi di sicurezza essenziale di un sistema informatico o cibernetico. Sarà in grado di identificare vulnerabilità negli stessi sistemi. Sarà capace di disegnare ed implementare contromisure e soluzioni di sicurezza complesse, anche facendo uso di strumenti avanzati quali tecniche di machine learning e strumenti statistici.

La sua forma mentis gli consentirà di mantenersi continuamente aggiornato, approfondendo gli aspetti connessi alle applicazioni specifiche del settore di competenza, e di entrare in contatto con le realtà nazionali e internazionali più avanzate nel settore.

Modalità e strumenti didattici per raggiungere l'obiettivo

Queste capacità sono fornite agli studenti attraverso lo studio critico di testi avanzati, supportato da attività curricolari e complementari. Tali attività, guidate dai docenti durante le ore di lezione, vanno dalla discussione di casi di studio alla elaborazione di progetti anche di gruppo, alle attività di laboratorio, alla discussione di problemi di frontiera, alle attività di tipo seminariale su argomenti di ricerca.

Strumenti per verificare che l'obiettivo sia stato raggiunto

La capacità di applicare conoscenza e comprensione dello studente è monitorata con attività di laboratorio, formazione individuale, verifiche in itinere, ed è valutata con gli esami scritti e/o orali e con attività progettuali gestite dagli studenti individualmente e/o in gruppo.

Autonomia di giudizio (making judgements)

I laureati in Cybersecurity devono essere in grado di gestire e di formulare giudizi personali su problemi e tecnologie per la loro soluzione. Devono inoltre essere in grado di proporre soluzioni anche in caso di problemi complessi e con informazioni incomplete. Inoltre, 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.

Modalità e strumenti didattici per raggiungere l'obiettivo

Lo sviluppo della capacità critica di giudizio degli studenti avviene durante le lezioni e le esercitazioni, nell'ambito delle attività di laboratorio ed, in particolare modo, durante il periodo di tesi. Inoltre, diversi insegnamenti prevedono lo sviluppo di casi di studio, e la redazione di elaborati, e sviluppo di sistemi (attività da svolgersi singolarmente e/o in team anche mediante l'uso di piattaforme di e-learning), permettendo allo studente di acquisire capacità di giudizio e confrontarsi con docenti e colleghi.

Strumenti per verificare che l'obiettivo sia stato raggiunto

La verifica di queste capacità verrà effettuata nella valutazione delle prove scritte, dei colloqui orali e delle documentazioni prodotte a corredo delle attività progettuali vengono analizzati le vulnerabilità che emergono. Il laureato in Cybersecurity, deve inoltre essere in grado di comunicare con chiarezza i risultati e le linee strategiche più opportune risultanti dall'analisi dei dati, anche attraverso adeguate visualizzazioni dei risultati. La verifica della abilità comunicative avviene nella valutazione del progetto di tesi e nelle attività progettuali degli insegnamenti che le prevedono.

Abilità comunicative (communication skills)

Per un esperto di CyberSecurity è indispensabile essere in grado di comunicare con chiarezza le vulnerabilità presenti in un sistema informatico e i meccanismi di protezione degli stessi. Queste abilità vengono fornite e verificate nei corsi che prevedono progetti, relativi a implementazione di sistemi informatici sicuri, in cui vengono analizzati le vulnerabilità che emergono. Il laureato in Cybersecurity, deve inoltre essere in grado di comunicare con chiarezza i risultati e le linee strategiche più opportune risultanti dall'analisi dei dati, anche attraverso adeguate visualizzazioni dei risultati. La verifica della abilità comunicative avviene nella valutazione del progetto di tesi e nelle attività progettuali degli insegnamenti che le prevedono.

Capacità di apprendimento (learning skills)

I laureati devono aver sviluppato capacità di apprendimento che consentano loro di continuare a studiare in modo autonomo e di adeguarsi ai cambiamenti rapidi nel mondo della CyberSecurity. Anche grazie alla formazione interdisciplinare, l'esperto di CyberSecurity è in grado di apprendere rapidamente e in profondità nozioni relative a nuove metodologie e tecnologie utilizzate in ambito CyberSecurity.

Modalità e strumenti didattici per raggiungere l'obiettivo

La capacità di apprendimento viene guidata e stimolata attraverso la proposta di compiti individuali e l'interazione con docenti e colleghi. 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 da soli o in gruppo, attività formative complementare, tesi di laurea) concorrono al progressivo aumento delle capacità di apprendimento. Infine, lo sviluppo di queste capacità avviene in maniera significativa anche con la preparazione della prova finale, dove sarà richiesta una sostanziale rielaborazione e un approfondimento personale delle conoscenze fornite dai docenti.

Strumenti per verificare che l'obiettivo sia stato raggiunto

La capacità di apprendimento viene monitorata in maniera continuativa durante le varie attività formative, con frequenti colloqui; viene verificata in sede d'esame e soprattutto con la valutazione dell'attività di tesi e di altre attività progettuali dove allo studente è dato un problema da risolvere, ma è lasciato libero sulla scelta delle metodologie e tecnologie da usare.

Conoscenze richieste per l'accesso

(DM 270/04, art 6, comma 1 e 2)

Gli studenti che intendono iscriversi al Corso di Laurea Magistrale in Cybersecurity devono essere in possesso di un diploma di Laurea o di altro titolo conseguito all'estero, riconosciuto idoneo in base alla normativa vigente.

Per l'ammissione al Corso di laurea magistrale in Cybersecurity sarà verificato il possesso di requisiti curriculari minimi, definiti in termini di crediti in gruppi di settori omogenei, e di un'adeguata preparazione personale.

I requisiti curriculari richiesti per l'accesso sono i seguenti:

- 24 CFU acquisiti nei SSD INF/01 - ING-INF/05 - ING-INF-03

- 18 CFU acquisiti nei SSD MAT/01-09

E' inoltre richiesta una buona conoscenza della lingua inglese, almeno di livello B2 abilità ricettive (lettura e ascolto) del quadro di riferimento CEFR.

L'adeguata preparazione personale è definita in termini di conoscenze, competenze e abilità nelle discipline fondamentali dell'Informatica e dell'Ingegneria dell'Informazione, quali le basi della programmazione, delle reti di comunicazione e dei sistemi informativi.

La verifica del possesso di tali conoscenze, competenze e abilità avviene attraverso modalità definite nel Regolamento Didattico del Corso di Studio.

Per i candidati in possesso di un titolo italiano con ordinamento diverso da quelli disciplinati dal DM 509/99 o dal DM 270/2004 o in possesso di un titolo conseguito all'estero, la verifica del possesso dei requisiti curriculari sarà svolta dalla commissione di ammissione.

Caratteristiche della prova finale

(DM 270/04, art 11, comma 3-d)

La prova finale consiste nella discussione di un elaborato inerente alle tematiche del corso di studio con caratteristiche di originalità. La preparazione dell'elaborato si svolgerà sotto la supervisione di un tutore con l'eventuale coinvolgimento di altri docenti di discipline inerenti al tema prescelto. Fermo restando il ruolo del relatore, la tesi di laurea potrà essere elaborata anche nell'ambito di soggiorni di studio presso altre università o Aziende, sia in Italia che all'estero. Nello svolgimento dell'attività per la prova finale l'allievo dovrà dimostrare, oltre alla padronanza degli argomenti trattati con sviluppi interdisciplinari la capacità di operare in modo autonomo, scientificamente rigoroso e concretamente efficace.

Sbocchi occupazionali e professionali previsti per i laureati

Chief Security Officer

funzione in un contesto di lavoro:

Il Security Officer supervisiona e coordina le politiche di sicurezza, 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.

competenze associate alla funzione:

Il Security Officer è dotato sia di competenze specifiche nel campo delle tecnologie e dei metodi per la sicurezza informatica sia di conoscenze interdisciplinari e di gestione, indispensabili per padroneggiare non solo gli aspetti più tecnici ma anche le esigenze derivanti dalla gestione dei sistemi informativi. Il Security Officer è uno specialista di livello avanzato in modo particolare sugli aspetti di dettaglio di alcune tecnologie per la cybersecurity. Competenze avanzate di questo tipo possono essere richieste in tutte le aree tipiche della sicurezza informatica, dalla programmazione sicura, alle tecniche avanzate di crittografia, alle metodologie di test e di monitoraggio di applicazioni sicure.

sbocchi occupazionali:

I principali sbocchi occupazionali e professionali dei laureati magistrali di questa classe sono negli ambiti della sicurezza di infrastrutture e sistemi informatici e del trattamento di dati sensibili per aziende di prodotti e servizi, enti della pubblica amministrazione e, più in generale, per qualunque organizzazione utilizzi sistemi informatici sicuri. Grandi, medie e piccole aziende, pubblica amministrazione, amministrazioni locali, enti di ricerca pubblici e privati, istituti di analisi economico-sociale. Il laureato in Cybersecurity può inoltre svolgere attività libero professionale iscrivendosi all'Albo degli Ingegneri, Settore Ingegneria dell'Informazione (sezione A, per chi ha conseguito una laurea magistrale), previo superamento del corrispondente esame di Stato.

Cybersecurity Officer

funzione in un contesto di lavoro:

Il Cybersecurity Officer è esperto tecnologico all'interno di una organizzazione della 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.

competenze associate alla funzione:

Il Cybersecurity Officer è dotato sia di competenze specifiche nel campo delle tecnologie e dei metodi per la sicurezza informatica sia di conoscenze interdisciplinari e di gestione, indispensabili per padroneggiare non solo gli aspetti più tecnici ma anche le esigenze derivanti dal posizionamento di mercato, e dalle necessità commerciali e di strategia aziendale nel contesto ampio del settore dell'information technology mondiale. Il Cybersecurity Officer possiede un'ottima conoscenza di base ed un ampio spettro di conoscenze e competenze nei vari settori dell'informatica, ha elevate capacità di modellazione e sa comprendere e utilizzare gli strumenti matematici di supporto, è in grado di gestire attività di gruppo, di operare con autonomia e di inserirsi prontamente negli ambienti di lavoro.

sbocchi occupazionali:

I principali sbocchi occupazionali e professionali dei laureati magistrali di questa classe sono negli ambiti della sicurezza di infrastrutture e sistemi informatici e del trattamento di dati sensibili per aziende di prodotti e servizi, enti della pubblica amministrazione e, più in generale, per qualunque organizzazione utilizzi sistemi informatici sicuri. Grandi, medie e piccole aziende, pubblica amministrazione, amministrazioni locali, enti di ricerca pubblici e privati, istituti di analisi economico-sociale. Il laureato in Cybersecurity può inoltre svolgere attività libero professionale iscrivendosi all'Albo degli Ingegneri, Settore Ingegneria dell'Informazione (sezione A, per chi ha conseguito una laurea magistrale), previo superamento del corrispondente esame di Stato.

Information Officer

funzione in un contesto di lavoro:

L'information officer è impegnato nella guida di analisi e re-engineering dei processi di business esistenti garantendo appropriate politiche di sicurezza, individuando e sviluppando la capacità di utilizzare nuovi strumenti, rimodellando le infrastrutture fisiche dell'impresa e l'accesso alla rete, e di identificare e sfruttare le risorse di conoscenza dell'impresa. Si occupa anche della gestione di progetti orientati alla sicurezza informatica all'interno dei sistemi informativi aziendali.

competenze associate alla funzione:

L'Information Officer è dotato sia di competenze specifiche nel campo delle tecnologie e dei metodi per la sicurezza informatica sia di conoscenze interdisciplinari e di gestione, indispensabili per padroneggiare non solo gli aspetti più tecnici ma anche le esigenze derivanti dalla gestione dei sistemi informativi. Partendo da una formazione di tipo tecnico-scientifico, tali figure professionali approfondiscono tematiche trasversali che includono competenze di gestione di progetto, aspetti economici, competenze giuridiche, gestione dei rischi connessi col ciclo di vita di un progetto.

sbocchi occupazionali:

I principali sbocchi occupazionali e professionali dei laureati magistrali di questa classe sono negli ambiti della sicurezza di infrastrutture e sistemi informatici e del trattamento di dati sensibili per aziende di prodotti e servizi, enti della pubblica amministrazione e, più in generale, per qualunque organizzazione utilizzi sistemi informatici sicuri. Grandi, medie e piccole aziende, pubblica amministrazione, amministrazioni locali, enti di ricerca pubblici e privati, istituti di analisi economico-sociale. Il laureato in Cybersecurity può inoltre svolgere attività libero professionale iscrivendosi all'Albo degli Ingegneri, Settore Ingegneria dell'Informazione (sezione A, per chi ha conseguito una laurea magistrale), previo superamento del corrispondente esame di Stato.

Il corso prepara alla professione di (codifiche ISTAT)

- Specialisti in reti e comunicazioni informatiche - (2.1.1.5.1)
- Amministratori di sistemi - (2.1.1.5.3)
- Specialisti in sicurezza informatica - (2.1.1.5.4)

Il corso consente di conseguire l'abilitazione alle seguenti professioni regolamentate:

- ingegnere dell'informazione

Il rettore dichiara che nella stesura dei regolamenti didattici dei corsi di studio il presente corso ed i suoi eventuali curricula differiranno di almeno 30 crediti dagli altri corsi e curriculum della medesima classe, ai sensi del DM 16/3/2007, art. 1 §2.

Attività caratterizzanti

ambito disciplinare	settore	CFU		minimo da D.M. per l'ambito
		min	max	
Ambito Scientifico	FIS/03 Fisica della materia INF/01 Informatica MAT/01 Logica matematica MAT/02 Algebra MAT/03 Geometria MAT/09 Ricerca operativa	18	24	18
Ambito Tecnologico	INF/01 Informatica ING-INF/03 Telecomunicazioni ING-INF/05 Sistemi di elaborazione delle informazioni	18	30	18
Ambito Giuridico, Sociale ed Economico	IUS/01 Diritto privato IUS/04 Diritto commerciale IUS/07 Diritto del lavoro IUS/10 Diritto amministrativo IUS/13 Diritto internazionale IUS/14 Diritto dell'unione europea IUS/20 Filosofia del diritto M-PSI/01 Psicologia generale M-PSI/05 Psicologia sociale M-PSI/06 Psicologia del lavoro e delle organizzazioni SECS-P/08 Economia e gestione delle imprese SECS-P/10 Organizzazione aziendale SECS-S/01 Statistica SPS/08 Sociologia dei processi culturali e comunicativi SPS/09 Sociologia dei processi economici e del lavoro	12	18	12
Minimo di crediti riservati dall'ateneo minimo da D.M. 48:		48		

Totale Attività Caratterizzanti

48 - 72

Attività affini

ambito disciplinare	settore	CFU		minimo da D.M. per l'ambito
		min	max	
Attività formative affini o integrative	ING-INF/01 - Elettronica ING-INF/04 - Automatica IUS/17 - Diritto penale MAT/05 - Analisi matematica MAT/06 - Probabilità e statistica matematica MAT/08 - Analisi numerica	12	18	12

Totale Attività Affini

12 - 18

Altre attività

ambito disciplinare		CFU min	CFU max
A scelta dello studente		12	15
Per la prova finale		30	39
Ulteriori attività formative (art. 10, comma 5, lettera d)	Ulteriori conoscenze linguistiche	0	3
	Abilità informatiche e telematiche	-	-
	Tirocini formativi e di orientamento	0	3
	Altre conoscenze utili per l'inserimento nel mondo del lavoro	0	3
Minimo di crediti riservati dall'ateneo alle Attività art. 10, comma 5 lett. d		1	
Per stages e tirocini presso imprese, enti pubblici o privati, ordini professionali		-	-
Totale Altre Attività		43 - 63	

Riepilogo CFU

CFU totali per il conseguimento del titolo	120
Range CFU totali del corso	103 - 153

Motivazioni dell'inserimento nelle attività affini di settori previsti dalla classe o Note attività affini

(Settori della classe inseriti nelle attività affini e non in ambiti di base o caratterizzanti : MAT/05 , MAT/06)

I SSD MAT/05 e MAT/06 sono da considerarsi affini per questa laurea magistrale in quanto il taglio dell'offerta didattica è prevalentemente applicativo: i fondamenti matematici alla base degli strumenti per la cybersecurity rappresentano conoscenze di tipo integrativo.

Note relative alle altre attività

Note relative alle attività caratterizzanti

RAD chiuso il 18/02/2020