Università degli Studi del Molise

Dipartimento di Bioscienze e Territorio

C.da Fonte Lappone – Pesche (IS)

Consultazione con il Comitato di Indirizzo del
Corso di Laurea Magistrale in Sicurezza dei Sistemi Software
Art. 11 DM 270/04

Consultazione n. 1 del 31 maggio 2018

L'anno 2018, il giorno 31 del mese di maggio il Comitato di Indirizzo del Corso di Laurea in Sicurezza dei Sistemi Software, istituito nella seduta n. 3 del 6 febbraio 2017 del Consiglio di Corso di Studio Unificato in Informatica e così composto:

- Prof. Rocco Oliveto (Presidente del Consiglio di Corso di Studio)
- Prof.ssa Anna Lisa Ferrara (Docente esperta di sicurezza informatica)
- Dott. Pasquale Lavorgna (Responsabile funzioni didattiche del Dipartimento)
- Sig. Davide Placella (Rappresentante degli Studenti)
- Dott. Pasquale Sorgonà (Dirigente Compartimento Regionale Polizia Postale e Comunicazioni "Abruzzo")
- Dott. Alessandro Vallega (Security Business Development Director at Oracle, Milano)
- Dott. Saverio Abbatiello (co-Founder della iForensics s.n.c di Isernia)

è stato convocato, attraverso procedura telematica, dal Presidente del Consiglio di Corso di Studio per valutare l'efficacia del percorso formativo del Corso di Laurea Magistrale in Sicurezza dei Sistemi Software dell'Università degli Studi del Molise.

Assume le funzioni di segretario verbalizzante il Dott. Pasquale Lavorgna, in qualità di Responsabile delle funzioni didattiche del Dipartimento di Bioscienze e Territorio.

Il Presidente, prima di sottoporre all'attenzione del Comitato la suddetta proposta, riporta ai componenti del Comitato di Indirizzo i risultati della terza edizione dell'Osservatorio delle Competenze Digitali, presentato a giugno 2017 e condotto dalle principali associazioni ICT AICA, Assinform, Assintel e Assinter Italia e promosso da MIUR e AgID. Dati alla mano, l'Osservatorio delle Competenze Digitali dimostra che sia nella Pubblica Amministrazione sia nelle imprese cresce la domanda di nuovi profili legati all'innovazione dei processi, dei prodotti e delle strategie in ottica digitale. Quelli più critici sono il Business Analyst, il **Project Manager** e il **Security Analyst**. Nelle

aziende utenti, invece, i profili comuni più critici da reperire sono il Responsabile Sistemi Informativi, e ancora una volta l'**ICT Security Manager** e il **Project Manager**. E' chiara quindi la necessità di avere professionalità specifiche nell'ambito della sicurezza informatica, come anche dimostrato da uno studio dell'Osservatorio "*Information security & privacy*" della School of management del Politecnico di Milano: un'impresa italiana su due (51%), contro il 9% di un anno fa, ha in corso progetti strutturati per adeguarsi al nuovo regolamento europeo sulla protezione dei dati (GDPR), che diventerà applicabile dal 25 maggio 2018, e il 58% (rispetto al 15% del 2016) ha un budget dedicato. Insieme al mercato, cresce anche la consapevolezza della necessità di un approccio di lungo periodo nella gestione della sicurezza: nel 50% delle imprese è in corso un piano di investimenti pluriennale, anche se il 21% dichiara di stanziare un budget in sicurezza solo in caso di necessità. Inoltre, quattro grandi imprese su dieci (39%) prevedono un aumento in organico dei ruoli dedicati alla cybersecurity e quasi la metà intende incrementare le figure preposte alla gestione della privacy, mentre, il 28% ha già un "Data protection officer" (che ha il compito di facilitare il rispetto delle disposizioni del GDPR). Tutto ciò porterà nel 2020 ad avere 3 milioni di posti di lavoro vacanti nel settore della sicurezza informatica.

Tali risultati suggeriscono da un lato la necessità di continuare ad investire nella formazione di manager della sicurezza e dall'altro che l'attuale percorso formativo del Corso di Laurea Magistrale in Sicurezza dei Sistemi Software, caratterizzato non solo da un ambito tecnologico, ma anche da un ambito giuridico ed uno sociale ed economico, è in linea con le attuali esigenze del mercato.

Il Presidente comunica inoltre al Comitato di Indirizzo che il Consiglio di Corso di Studio Unificato di Informatica, tenendo conto i) delle esigenze del mercato del lavoro; ii) delle opinioni degli Studenti; iii) delle osservazioni ricevute dai Docenti che erogano attività didattica nell'ambito del Corso di Studio, ha deciso di revisionare, rispetto all'anno precedente, il piano di studio.. Nello specifico, le modifiche apportate al piano di studio sono:

1. cambio della denominazione del modulo "Sicurezza dei sistemi software" dell'insegnamento "Sicurezza delle reti e dei sistemi software" in "Metodi formali per la sicurezza" per meglio

rispecchiare gli obiettivi formativi del corso, con relativo cambio del SSD da INF/01 a ING-INF/05;

2. erogazione del corso di "Organizzazione e pianificazione aziendale" in un unico modulo da 9 CFU;

3. introduzione del corso "Profili giuridici dei social network" (6 CFU, 48 ore) – organizzato in due moduli (3 CFU SSD IUS/01 e 3 CFU IUS/04) – come corso caratterizzante a scelta vincolata nell'area giuridica, correlativamente rendendo a scelta vincolata anche il corso caratterizzante "Informatica e diritto" (6 CFU, SSD IUS/20, 48 ore). Tale modifica è giustificata dall'esigenza di voler sperimentare, per il momento solo nell'area giuridica, la possibilità di prevedere percorsi formativi ulteriormente specializzanti e di approfondimento e, contestualmente, rispondere ad una esplicita proposta della Commissione Paritetica Docenti-Studenti, formulata nel quadro B della Relazione annuale 2017, di incrementare in tale Corso di Studio magistrale i corsi d'insegnamento a scelta quali "*importanti e auspicabili opportunità*" di apprendimento fruibili dagli studenti, anche "*mediante l'attivazione altrettanto auspicabile di corsi a scelta vincolata, particolarmente adatti ad assicurare la coerenza degli insegnamenti opzionali con gli obiettivi formativi programmati*".

Una descrizione di sintesi del nuovo percorso formativo, riportata nell'**Allegato 1** del presente verbale, è stata già inviata, tramite posta elettronica, ai componenti del Comitato di Indirizzo con la mail di convocazione.

Il Presidente, concede quindi ai Componenti del Comitato di Indirizzo, di comunicare telematicamente (e-mail da inviare al Presidente del CCS unificato di Informatica ed al Segretario verbalizzante) entro il 6 giugno 2018, sempre, eventuali commenti e suggerimenti in merito all'efficacia del progetto formativo.

Sono pervenute quindi le seguenti osservazioni:

- **Dott. Alessandro Vallega, Manager – Security Business Development Director at Oracle (Milano).** Il giorno 05.06.2018 il Dott. Vallega conferma la validità dell'offerta formativa,

rinnovando l'apprezzamento, già manifestato all'epoca della costituzione del Corso di Studio, per la volontà di insegnare Sicurezza e Diritto insieme. Il Dott. Vallega sottolinea gli impatti del GDPR e la necessità di avere figure specializzate in grado non solo di dominare la tecnologia ma anche di operare nel rispetto della normativa vigente in merito al trattamento dell'informazione. Il Dott. Vallega sottolinea come da più di un anno si stia occupando solo di GDPR e gli investimenti effettuati dai suoi clienti per adeguare la sicurezza e la privacy dei loro sistemi informativi. Il Dott. Vallega, inoltre, condivide con il Comitato le future tendenze del mondo ICT: nel suo ambiente si fa un gran parlare di automazione, machine learning e intelligenza artificiale, del software utilizzato per la difesa di reti e infrastrutture. L'analista del SOC (Security Operation Center) deve essere assistito dalle più moderne tecnologie per proteggere gli asset aziendali. Gli attacchi procedono ad un ritmo che solo le macchine possono contrastare: macchine attaccano e macchine difendono.

- **Dott. Pasquale Sorgonà, Dirigente Compartimento Regionale Polizia Postale e delle Comunicazioni "Abruzzo".** Il giorno 06.06.2018 il Dott. Sorgonà, dopo aver confermato l'efficacia dell'offerta formativa, sottolinea la validità dell'inserimento di materie, quali "Profili giuridici dei social network", "Cultura della protezione dei dati personali" e "Sistemi video per la sicurezza", che, pur apportando un rilevante contributo all'area giuridica, sicuramente arricchiscono notevolmente il patrimonio di conoscenze multitematico reso necessario dall'imprescindibile necessità di armonizzare la tecnologia con le leggi. Il Dott. Sorgonà suggerisce, inoltre, di modificare il nome dell'insegnamento "Cultura della protezione dei dati personali" in "Privacy e sicurezza dei dati personali o delle informazioni" con la contestuale aggiunta di alcuni argomenti di oggettiva rilevanza per chi volesse valutare l'opportunità di aprirsi uno sbocco lavorativo nel settore della privacy.

- **Dott. Saverio Abbatiello, Docente del Corso di Laurea in Informatica e referente dell'area giuridica.** Il giorno 06.05.2018 il Dott. Abbatiello suggerisce, alla luce dell'importanza che ha e che assumerà per l'avvenire il DPO ("Data Protection Officer") con l'entrata in vigore del GDPR, di erogare il corso "Cultura della Protezione dei Dati personali" come "Caratterizzate",

curando, in modo particolare, la formazione di DPO. Inoltre, il Dott. Abbatiello auspica che sia dato ampio spazio alla pratica, all'uso delle diverse strumentazioni di Digital Forensics – in modo particolare, a quelle dedicate all'acquisizione e all'analisi dei dispositivi mobili – e allo studio e alla compilazione di perizie e pareri tecnici professionali.

Il giorno 07.06.2018 il Presidente dichiara chiusa la procedura di consultazione telematica e ringrazia tutti partecipanti per i loro suggerimenti puntuali e sicuramente indispensabili per valutare l'efficacia dell'offerta formativa e migliorare ulteriormente il progetto formativo del Corso di Laurea Magistrale in Sicurezza dei Sistemi Software.

Il verbale è redatto, letto e approvato seduta stante.

Pesche (IS), 07 giugno 2018.

Il Segretario verbalizzante
Dott. Pasquale Lavorgna

Il Presidente del CCS di Informatica
Prof. Rocco Oliveto

UNIVERSITÀ
DEGLI STUDI
DEL MOLISE

DIPARTIMENTO DI BIOSCIENZE E TERRITORIO

Descrizione Piano degli Studi e Ordinamento Didattico del Corso di Laurea Magistrale in Sicurezza dei Sistemi Software

Aggiornato al 31 maggio 2018

INTRODUZIONE

Il Corso di Laurea Magistrale in Sicurezza dei Sistemi Software dell'Università degli Studi del Molise nasce nell'a.a. 2016/2017. A luglio 2018, molto probabilmente, ci saranno i primi laureati in tale percorso di studio.

Pur essendo un corso di Laurea di recente istituzione, il Consiglio di Corso di Studio ha ritenuto opportuno procedere ad una valutazione dell'efficacia dell'attuale offerta formativa coinvolgendo i Portatori di Interesse. Inoltre, per l'a.a. 2018/2019 sono stati pianificati dei piccoli cambiamenti al piano di studio, di seguito descritti, per cercare di soddisfare alcune richieste del mercato del lavoro.

Il Presente documento riporta le modifiche dell'attuale piano degli studi del Corso di Laurea Magistrale in Sicurezza dei Sistemi Software dell'Università degli Studi del Molise, nonché la descrizione dettagliata del nuovo percorso formativo.

ATTUALE PIANO DEGLI STUDI DEL CORSO DI LAUREA MAGISTRALE IN SICUREZZA DEI SISTEMI SOFTWARE

I anno - I semestre	Moduli	Docente	SSD	CFU	Tipo attività
Sicurezza delle reti e dei sistemi software	Sicurezza delle reti	F. Mercaldo	INF/01	6	Caratterizzante
Informatica e diritto		B. Troncarelli	IUS/20	6	Caratterizzante
Cryptography*		A. L. Ferrara	INF/01	6	Caratterizzante
Organizzazione e pianificazione aziendale		F. Di Virgilio	SECS-P/10	9	Caratterizzante
Inglese avanzato (idoneità)		I. Innato	L-LIN/12	3	Altre
				30	
I anno - II semestre	**Moduli**	**Docente**	**SSD**	**CFU**	**Tipo attività**
Sicurezza delle reti e dei sistemi software	Sicurezza dei sistemi sw	A. Santone	INF/01	6	Caratterizzante
Statistical learning and big data*		F. Divino	SECS-S/02	6	Affine
Gestione progetti software		F. Fasano	INF/01	6	Affine
Computer forensics e investigazioni	Computer forensics	P. Sorgona	INF/01	3	Caratterizzante
	Investigazioni	M. Giacci	INF/01	3	Caratterizzante
Metodi di ottimizzazione		C. Cerrone	MAT/09	6	Caratterizzante
				30	
II anno - I semestre	**Moduli**	**Docente**	**SSD**	**CFU**	**Tipo attività**
Software reliability and testing*		R. Oliveto	ING-INF/05	6	Caratterizzante
Biometric systems*		S. Ricciardi	INF/01	6	Caratterizzante
Semantic intelligence for cybersecurity*		R. Pareschi	INF/01	6	Caratterizzante
Attività a scelta dello studente				12	Altre
				30	
II anno - II semestre	**Moduli**	**Docente**	**SSD**	**CFU**	**Tipo attività**
Prova finale				30	Altre
				30	

* Corso erogato in lingua inglese

PROPOSTE DI MODIFICA AL PIANO DEGLI STUDI DEL CORSO DI LAUREA MAGISTRALE IN SICUREZZA DEI SISTEMI SOFTWARE

In estrema sintesi, le modifiche che si intende apportare all'attuale percorso formativo sono:

1. cambio della denominazione del modulo "Sicurezza dei sistemi software" dell'insegnamento "Sicurezza delle reti e dei sistemi software" in "Metodi formali per la sicurezza" per meglio rispecchiare gli obiettivi formativi del corso, con relativo cambio del Settore Scientifico Disciplinare (SSD) da INF/01 a ING-INF/05;
2. introduzione del corso "Profili giuridici dei social network" (6 CFU, 48 ore) – organizzato in due moduli (3 CFU SSD IUS/01 e 3 CFU IUS/04) – come corso caratterizzante a scelta vincolata nell'area giuridica, correlativamente rendendo a scelta vincolata anche il corso caratterizzante "Informatica e diritto" (6 CFU, SSD IUS/20, 48 ore). Tale modifica è giustificata dall'esigenza di voler sperimentare, per il momento solo nell'area giuridica, la possibilità di prevedere percorsi formativi ulteriormente specializzanti e di approfondimento e, contestualmente, rispondere ad una esplicita proposta della Commissione Paritetica Docenti-Studenti, formulata nel quadro B della Relazione annuale 2017, di incrementare in tale Corso di Studio magistrale i corsi d'insegnamento a scelta quali "*importanti e auspicabili opportunità*" di apprendimento fruibili dagli studenti, anche "*mediante l'attivazione altrettanto auspicabile di corsi a scelta vincolata, particolarmente adatti ad assicurare la coerenza degli insegnamenti opzionali con gli obiettivi formativi programmati*".
3. spostamento del corso "Informatica e diritto" dal primo al secondo semestre e, correlativamente, spostamento del corso "Metodi di ottimizzazione" dal secondo al primo semestre.

NUOVO PIANO DEGLI STUDI DEL CORSO DI LAUREA MAGISTRALE IN SICUREZZA DEI SISTEMI SOFTWARE

I anno - I semestre	Moduli	Docente	SSD	CFU	Tipo attività
Sicurezza delle reti e dei sistemi software	Sicurezza delle reti	F. Mercaldo	INF/01	6	Caratterizzante
Cryptography*		A. L. Ferrara	INF/01	6	Caratterizzante
Organizzazione e pianificazione aziendale		Da definire	SECS-P/10	9	Caratterizzante
Metodi di ottimizzazione		C. Cerrone	MAT/09	6	Caratterizzante
Inglese avanzato (idoneità)		Da definire	L-LIN/12	3	Altre
				30	
I anno - II semestre	**Moduli**	**Docente**	**SSD**	**CFU**	**Tipo attività**
Sicurezza delle reti e dei sistemi software	Metodi formali per la sicurezza	A. Santone	INF/01	6	Caratterizzante
Statistical learning and big data*		F. Divino	SECS-S/02	6	Affine
Gestione progetti software		F. Fasano	INF/01	6	Affine
Computer forensics e investigazioni	Computer forensics	P. Sorgonà	INF/01	3	Caratterizzante
	Investigazioni	M. Giacci	INF/01	3	Caratterizzante
Uno a scelta tra:					
Informatica e diritto		B. Troncarelli	IUS/20	6	Caratterizzante
Profili giuridici dei social network	Primo modulo	S. Giova	IUS/01	3	Caratterizzante
	Secondo modulo	G. P. La Sala	IUS/04	3	Caratterizzante
				30	
II anno - I semestre	**Moduli**	**Docente**	**SSD**	**CFU**	**Tipo attività**
Software reliability and testing*		R. Oliveto	ING-INF/05	6	Caratterizzante
Biometric systems*		S. Ricciardi	INF/01	6	Caratterizzante
Semantic intelligence for cybersecurity*		R. Pareschi	INF/01	6	Caratterizzante
Attività a scelta dello studente				12	Altre
				30	
II anno - II semestre	**Moduli**	**Docente**	**SSD**	**CFU**	**Tipo attività**
Prova finale				30	Altre
				30	

CORSI A SCELTA DELLO STUDENTE

N.	Titolo	Docente	SSD	CFU	Sem.
1	Cultura della Protezione dei Dati Personali (GDPR)	Da definire	IUS/01	3	I
2	Logistica	**CERRONE** Carmine	MAT/09	3	I
3	Sistemi video per la sicurezza	**RICCIARDI** Stefano	INF/01	3	I

OBIETTIVI FORMATIVI SPECIFICI DEL CORSO

Il Corso di Laurea Magistrale in "Sicurezza dei sistemi software" è orientato a formare laureati che abbiano vaste ed approfondite competenze teoriche, metodologiche, sperimentali ed applicative nelle aree fondamentali della sicurezza informatica. Il dottore magistrale in "Sicurezza dei sistemi software" sarà in grado di affrontare, con il giusto livello di astrazione, problemi informatici, con particolare riferimento alla sicurezza, e di utilizzare tutti gli strumenti messi a disposizione dall'informatica e dalle discipline connesse.

Il laureato avrà competenze e conoscenze relative alle metodologie e agli strumenti tecnologici per la gestione dell'intero ciclo di vita di un sistema informatico sicuro, a partire dalla sua progettazione, passando per la sua implementazione e la sua verifica, fino ad arrivare alla sua manutenzione. Oltre alle competenze metodologiche e tecnologiche relative alla sicurezza, il laureato magistrale in "Sicurezza dei sistemi software" acquisirà conoscenze sugli aspetti giuridici relativi al trattamento sicuro e riservato dei dati informatici, nonché alla conservazione e trasmissione dei dati sensibili.

Inoltre, il laureato sarà in grado di applicare metodologie e tecnologie per condurre indagini al fine di identificare reati e crimini informatici, nonché valutare il grado di sicurezza di un sistema software e proporre negli ambiti applicativi in cui esso opera, le innovazioni che continuamente caratterizzano la disciplina al fine di migliorare costantemente la sicurezza nei sistemi informatici. In tali scenari, il laureato non solo sarà in grado di adattare in specifici contesti le soluzioni già presenti in letteratura, ma sarà anche in grado di definire tecniche e soluzioni originali utilizzabili in diversi contesti. Infine, il laureato acquisirà capacità di lavoro in autonomia, con buone capacità direttive, comunicative e manageriali nella conduzione di gruppi di lavoro in contesti sia nazionali sia internazionali formati da persone con livelli, settori di competenza e cultura diversi.

RISULTATI DI APPRENDIMENTO ATTESI

Le successive sezioni descrivono i risultati di apprendimento attesi organizzati secondo le tre aree di studio che caratterizzano il corso, cioè l'area Matematica, Fisica e Statistica, l'area Informatica e l'area Giuridica. La descrizione dei risultati di apprendimento attesi sono espressi tramite i descrittori di Dublino.

Conoscenza e capacità di comprensione

Area Giuridica. Le conoscenze e competenze che si intende fornire in questo ambito sono di fondamentale importanza per creare manager esperti di sicurezza in grado non solo di progettare sistemi software sicuri e di valutare il livello di sicurezza di un sistema software complesso, ma di utilizzare, nel rispetto della normativa vigente, tecnologie informatiche per l'analisi e la gestione dei cosiddetti dati sensibili.

Nello specifico, il percorso formativo del Corso di Laurea Magistrale in "Sicurezza dei sistemi software" intende fornire:

- conoscenza e comprensione del rapporto intercorrente tra informatica e diritto;
- conoscenza e comprensione della regolamentazione relativa all'utilizzo delle tecnologie informatiche;
- conoscenza e comprensione dei principali aspetti civilistici dei social network;
- conoscenza e comprensione delle modalità di investigazione alla luce dell'ordinamento giuridico italiano;

- conoscenza e comprensione dei princìpi generali in materia di trattamento dei dati, con particolare riferimento alle norme per le tecniche di acquisizione, conservazione, analisi e produzione dei dati digitali rinvenuti nei computer e dei flussi telematici per la loro utilizzabilità nell'ambito dei vari tipi di processi.

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

- Informatica e diritto
- Profili giuridici dei social network
- Computer forensics e investigazioni

Area Sociale ed Economica. Il percorso formativo del Corso di Laurea Magistrale in "Sicurezza dei sistemi software" intende creare dei manager in grado di coordinare la progettazione, lo sviluppo, il collaudo e la manutenzione di sistemi software complessi, con particolare riferimento ad aspetti legati alla sicurezza. Le conoscenze e le competenze che si intende fornire in questo ambito contribuiscono alla formazione manageriale degli studenti. Nello specifico, il percorso formativo del Corso di Laurea Magistrale in "Sicurezza dei sistemi software" intende fornire:

- conoscenza e comprensione dei contesti socio-economici, che influenzano il funzionamento delle organizzazioni;
- conoscenza e comprensione delle metodologie per la pianificazione strategica e la redazione del business plan;
- conoscenza degli aspetti inerenti la struttura, le dinamiche e i processi di gruppo (comunicativi, decisionali, di conflitto e negoziazione);
- conoscenza e comprensione di metodi e tecniche per l'analisi dei dati.

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

- Big data analysis (in lingua inglese)
- Gestione progetti software
- Metodi di ottimizzazione
- Organizzazione e pianificazione aziendale

Area Informatica. Le conoscenze e competenze che si intende fornire in questo ambito rappresentano il cuore dell'intero percorso formativo. I laureati del Corso di Laurea Magistrale in "Sicurezza dei sistemi software" saranno in grado di progettare, sviluppare, valutare e gestire sistemi software sicuri. Di conseguenza, il percorso formativo intende fornire:

- conoscenza e comprensione delle problematiche e delle soluzioni organizzative relative alla sicurezza informatica;
- conoscenza e comprensione dei metodi matematici alla base delle tecnologie informatiche per la crittografia dei dati;
- conoscenza e comprensione delle metodologie di sviluppo dei sistemi software complessi, con particolare riferimento alla sicurezza e alla gestione dei progetti software;
- conoscenza e comprensione di modelli di ottimizzazione connessi allo sviluppo di sistemi software complessi e sicuri;
- conoscenza e comprensione delle architetture software basate su servizi (service-oriented architecture) e/o su cloud computing;
- conoscenza e comprensione delle metodologie per garantire la sicurezza in architetture basate su servizi e/o cloud computing;

- conoscenza e comprensione delle tecnologie informatiche (hardware e software) per svolgere indagini informatiche o investigazioni difensive;
- conoscenza e comprensione delle metodologie per il recupero di dati;
- conoscenza e comprensione delle metodologie e delle tecniche per l'individuazione e la rimozione di vulnerabilità all'interno di sistemi software complessi;
- conoscenza e comprensione delle tecniche di autenticazione e riconoscimento basate su sistemi biometrici;
- conoscenza e comprensione di tecniche di business intelligence per gestire la sicurezza e la criminalità informatica.

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

- Networking avanzato
- Gestione progetti software
- Computer forensics e investigazioni
- Metodi di ottimizzazione
- Metodi matematici per la crittografia
- Biometric systems (in lingua inglese)
- Semantic intelligence for cybersecurity (in lingua inglese)
- Software reliability and testing (in lingua inglese)

Capacità di applicare conoscenza e comprensione

Area Giuridica. Sulla base delle conoscenze e competenze acquisite lo studente sarà in grado di:

- applicare le tecnologie informatiche in accordo alla normativa vigente in materia;
- svolgere, nel rispetto della normativa vigente, un'indagine informatica o un'investigazione difensiva nel campo dei crimini informatici e dei crimini comuni la cui prova sia costituita da dati digitali o veicolati da sistemi informatici;
- trattare dati sensibili in accordo alla normativa vigente in materia.

Area Sociale ed Economica. Sulla base delle conoscenze e competenze acquisite lo studente sarà in grado di:

- analizzare efficacemente i contesti socio-economici, che influenzano il funzionamento delle organizzazioni, con particolare riferimento ai processi della comunicazione nelle loro diverse forme e livelli, sia dal punto di vista teorico, metodologico e applicativo;
- analizzare il comportamento individuale e di gruppo, le condizioni di efficacia dei gruppi di lavoro, dei ruoli e della leadership nei team;
- valutare le performance di gruppo;
- comprendere l'ambiente competitivo in cui l'impresa opera e le risorse a sua disposizione per affrontare con successo la sfida competitiva;
- redigere un business plan, dalla definizione della missione e degli obiettivi strategici fino alla predisposizione del piano economico e finanziario;
- gestire in maniera efficace gruppi di lavoro formati da persone con livelli, settori di competenza e cultura diversi in contesti sia nazionali sia internazionali;
- analizzare dati provenienti da diverse sorgenti al fine di fornire al management aziendale le informazioni utili ad assumere decisioni e disegnare strategie.

Area Informatica. Sulla base delle conoscenze e competenze acquisite lo studente sarà in grado di:

- gestire le problematiche legate alla sicurezza di sistemi software complessi e sintetizzare soluzioni organizzative a tali problemi;
- comprendere i modelli matematici alla base della crittografia dei dati con l'obiettivo di valutarne punti di forza e debolezza;
- coordinare lo sviluppo e la manutenzione di un sistema software complesso;
- applicare modelli di ottimizzazione per migliorare l'efficacia e l'efficienza del processo di sviluppo e del processo evolutivo di un sistema software;
- progettare architetture software sicure basate su servizi (service-oriented architecture) e su cloud computing;
- svolgere indagini informatiche o investigazioni difensive attraverso l'uso delle più recenti tecnologie hardware e software;
- valutare e confrontare tecnologie hardware e software per indagini informatiche o investigazioni difensive;
- recuperare dati da computer o dispositivi mobili;
- individuare e rimuove vulnerabilità all'interno di sistemi software complessi;
- sviluppare soluzioni software sicure e robuste;
- progettare e sviluppare moduli di autenticazione e di riconoscimento basati su sistemi biometrici;
- utilizzare tecniche di business intelligence per gestire la sicurezza e la criminalità informatica.

Autonomia di giudizio

Capacità che si intendono trasmettere. Il laureato magistrale in "Sicurezza dei sistemi software" sarà in grado di lavorare in completa autonomia per comprendere le necessità di innovazione delle imprese e delle pubbliche amministrazioni e gestirle, nell'ambito dei processi organizzativi, proponendo soluzioni di tipo ICT sicure. Sarà, quindi, in grado di analizzare, valutare e proporre adeguate soluzioni innovative in un'ottica di efficacia e di efficienza organizzativa volte al miglioramento continuo. Al termine del suo percorso formativo, il laureato sarà in grado di:

- analizzare problemi in diversi contesti applicativi, con particolare riferimento alla sicurezza del software e dei sistemi informatici, definire e formalizzare strategie di risoluzione efficaci ed efficienti;
- pianificare la raccolta di dati appropriata per gli obiettivi proposti e interpretare criticamente i dati raccolti al fine di derivarne giudizi autonomi suffragati da analisi oggettive e quantitative;
- valutare la qualità e il rapporto costo/beneficio delle soluzioni proposte in relazione agli obiettivi e ad altre soluzioni;
- lavorare con un alto grado di autonomia;
- coordinare lo sviluppo di sistemi informatici complessi e sicuri;
- coordinare piccoli team di lavoro composti anche da persone con culture diverse e competenze in discipline diverse e a diversi livelli.

Il laureato magistrale sarà inoltre consapevole delle responsabilità sociali, etiche, giuridiche e deontologiche relative alla sua professione.

Metodi didattici. Lo sviluppo delle capacità sopra elencate avviene attraverso molteplici attività:

- partecipazione a gruppi di lavoro per lo sviluppo di sistemi informativi e analisi di sistemi informativi esistenti nell'ambito delle attività progettuali di specifici insegnamenti;
- analisi di casi di studio nelle attività di esercitazione e di laboratorio;
- redazione di elaborati personali;
- elaborazione della tesi di laurea.

Modalità di verifica. La verifica dell'acquisizione delle capacità di giudizio autonomo ed obiettivo avviene attraverso la valutazione delle prove scritte, dei colloqui orali e delle documentazioni prodotte a corredo delle attività progettuali previste dai singoli insegnamenti e dalla prova finale.

Abilità comunicative

Abilità che si intendono trasmettere. Il laureato magistrale in "Sicurezza dei sistemi software" sarà in grado di sintetizzare e comunicare in modo chiaro ed efficace le proprie posizioni e gli esiti delle proprie analisi e valutazioni, utilizzando la lingua di lavoro più diffusa nei contesti lavorativi internazionali di riferimento (inglese) e avvalendosi, con piena padronanza tecnica, dei più aggiornati strumenti informatici. Il laureato sarà inoltre in grado di usare in maniera adeguata il "linguaggio" matematico, statistico ed economico per l'analisi, l'elaborazione e la presentazione di dati. Più in dettaglio, il laureato sarà in grado di:

- comunicare in modo chiaro ed efficace, anche attraverso l'uso di strumenti informatici, le proprie conoscenze, idee, problemi, soluzioni e il razionale ad esse sottese, adeguando le modalità di espressione alle caratteristiche culturali e professionali dei destinatari della comunicazione;
- comunicare in italiano o in inglese con tecnici ed esperti con proprietà di linguaggio e mostrando padronanza della terminologia tecnica;
- lavorare in gruppi multidisciplinari e multiculturali con adeguate capacità relazionali e decisionali;
- relazionare sulla propria attività lavorativa.

Metodi didattici. Lo sviluppo delle capacità sopra elencate avviene attraverso molteplici attività:

- colloqui e preparazioni di relazioni, nonché discussioni in aula guidate dal docente;
- partecipazione a gruppi di lavoro per lo sviluppo di sistemi informativi e analisi di sistemi informativi esistenti nell'ambito delle attività progettuali di specifici insegnamenti;
- redazione di elaborati personali;
- seminari su argomenti avanzati;
- studio da testi e fonti in lingua inglese e partecipazione a programmi di mobilità;
- elaborazione e discussione della tesi di laurea.

Modalità di verifica. La verifica dell'acquisizione delle abilità comunicative avviene sia attraverso le prove orali previste dalla maggior parte delle attività formative sia nell'ambito della presentazione di elaborati individuali o di gruppo. La prova finale, discussa davanti ad una commissione, rappresenta un ulteriore momento di verifica delle suddette abilità.

Capacità di apprendimento

Capacità che si intendono trasmettere. Il laureato magistrale in "Sicurezza dei sistemi software" sarà in grado di studiare in modo autonomo, integrando in modo efficace le conoscenze ricevute. Ciò consentirà al laureato magistrale di mantenere aggiornate le proprie

competenze in un settore in continua evoluzione come l'Informatica, di apprendere le problematiche di nuovi settori applicativi, di intraprendere efficacemente percorsi formativi di livello superiore (Dottorato di Ricerca o master di II livello) e affrontare carriere manageriali che richiedono una elevata capacità di aggiornamento e un alto grado di autonomia. Più in dettaglio, il laureato sarà in grado di:

- organizzare e realizzare un piano di studio indipendente;
- organizzare le proprie idee in maniera critica e sistematica;
- progettare ed elaborare un lavoro di ricerca indipendente, ancorché guidato da un supervisore;
- identificare, selezionare e raccogliere informazioni mediante l'uso appropriato delle fonti rilevanti.

Metodi didattici. Lo sviluppo delle capacità sopra elencate avviene durante i corsi e soprattutto durante la preparazione della prova finale, dove sarà richiesta una sostanziale rielaborazione e un approfondimento personale delle conoscenze fornite dai docenti.

Modalità di verifica. La verifica dell'acquisizione delle capacità di apprendimento avviene attraverso la verifica continua durante le attività formative, nel corso dello svolgimento assistito di progetti e nella prova finale. Quest'ultima prova permetterà di verificare l'attitudine dello studente ad un autonomo approfondimento sui temi specifici trattati.

SBOCCHI OCCUPAZIONALI E PROFESSIONALI PREVISTI PER I LAUREATI

Di seguito sono descritti profili professionali e gli sbocchi occupazionali e professionali previsti per i laureati.

Consulente per la progettazione di sistemi software sicuri e per la gestione del rischio

Funzione in un contesto di lavoro. Operano nel vasto settore della consulenza rivolta alla direzione di sistemi informativi e alla direzione aziendale. Coniugano la conoscenza approfondita delle tecnologie informatiche con conoscenze di gestione di progetti e di processi aziendali, un'approfondita conoscenza delle tematiche proprie della sicurezza informatica, degli aspetti normativi e giuridici pertinenti e dei principali trend di sviluppo sia tecnologici sia in discipline correlate come la privacy e l'analisi del rischio. Propongono soluzioni volte a garantire un livello di sicurezza complessivo per il sistema informativo che risulti adeguato alle specifiche esigenze. Forniscono supporto per l'applicazione di tali soluzioni e la definizione di procedure organizzative che permettano la piena efficacia dei sistemi di sicurezza realizzati.

Competenze associate alla funzione. Sono figure professionali dotate 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, dal posizionamento di mercato, e dalle necessità commerciali e di strategia aziendale nel contesto ampio del settore dell'information technology.

Sbocchi occupazionali. Tali figure svolgono attività professionali altamente specializzate nell'ambito della consulenza aziendale rivolta alle imprese e alla pubblica amministrazione presso le quali supportano la direzione d'azienda e quella dei sistemi informativi dedicandosi alla gestione di progetti o alla partecipazione a progetti strategici che richiedono non solo competenze tecniche specialistiche, ma anche conoscenze di livello gestionale, giuridico e interdisciplinare. Nello specifico i principali sbocchi sono:

- grandi aziende di produzione software (consulenza alla direzione di progetti di sviluppo complessi e critici);
- microimprese e PMI di produzione software;
- aziende che forniscono servizi di consulenza informatica;
- imprese, enti ed amministrazioni, sia pubbliche sia private, che devono sviluppare e gestire sistemi informatici sicuri;
- PMI che forniscono servizi di consulenza informatica ad utenti finali;
- aziende che forniscono servizi di formazione e training professionale;
- pubblica amministrazione;
- libero professionismo nell'ambito della consulenza.

Progettisti di sistemi con requisiti avanzati di sicurezza informatica

Funzione in un contesto di lavoro. Esperti di problematiche avanzate di sicurezza informatica relative sia allo sviluppo di software affidabile, sia alla gestione di dinamiche complesse nell'ambito della progettazione di tale software. Tali figure professionali affrontano aspetti tecnologici per i quali è richiesta una conoscenza estremamente approfondita delle tecnologie, dei processi aziendali riguardanti lo sviluppo di sistemi complessi e della pianificazione delle risorse. Sono quindi indispensabili in casi nei quali sia richiesta capacità di analisi di scenari tecnologici di elevata complessità e criticità e l'applicazione di determinate tecnologie per implementare soluzioni ottimali.

Competenze associate alla funzione. Tali figure professionali sono degli specialisti di livello avanzato nello sviluppo di software sicuri per aver approfondito, in modo particolare, tutti gli aspetti, anche di maggior dettaglio, di alcune tecnologie innovative. Le competenze associate a questa figura professionale spaziano in tutte le aree tipiche della sicurezza informatica, dalla programmazione sicura con l'applicazione di metodologie avanzate di analisi statica e dinamica del codice sorgente, l'analisi di codice malevolo, progettazione di architetture basate su servizi, tecniche avanzate di crittografia, tecniche avanzate di protezione dei dati (biometria).

Sbocchi occupazionali. Il solido background posseduto nell'ambito della programmazione di sistemi affidabili e nella gestione di processi aziendali complessi, permette l'inserimento in contesti lavorativi pubblici e privati dove si progettano, implementano, testano e gestiscono sistemi software critici o con requisiti avanzati di sicurezza. Più in particolare è possibile ricoprire ruoli altamente specializzati nei seguenti ambiti:

- grandi aziende di sviluppo software (progettazione, sviluppo, testing, manutenzione) con elevati requisiti di affidabilità;
- imprese, enti ed amministrazioni, sia pubbliche sia private, che sviluppano e gestiscono sistemi informatici critici con particolare attenzione alla vulnerabilità e alla protezione di dati;
- aziende che forniscono contenuti e servizi su rete (sistemi distribuiti e basati su cloud).

Project manager di sistemi informatici

Funzione in un contesto di lavoro. Specialisti nella progettazione di sistemi informatici, e servizi web con requisiti avanzati di sicurezza informatica e di gestione sicura dei dati in contesti aziendali e pubblici. Le tipiche funzioni sono quelle di esperto di tecnologie che deve saper strutturare un progetto, organizzarlo in fasi, coordinare le attività e il personale tecnico, gestire un budget dedicato, selezionare risorse e strumenti, gestire rapporti con fornitori e consulenti e operare nel rispetto delle scadenze previste. Nell'ambito di un contesto di

progetto definito crea le condizioni per un efficiente lavoro di squadra finalizzato al raggiungimento degli obiettivi e per un'efficace comunicazione a tutti i livelli.

Competenze associate alla funzione. Tali figure professionali dispongono di competenze interdisciplinari, tecniche e gestionali, in grado di orientare e organizzare un'attività complessa sia per gli aspetti tecnologici sia per quelli di gestione. Sulla base di una formazione di tipo tecnico-scientifico, tali figure professionali possiedono conoscenze trasversali, quali la gestione di progetti, degli aspetti economici, delle competenze giuridiche e della gestione dei rischi connessi alla realizzazione di sistemi software critici.

Sbocchi occupazionali. La figura del Project Manager è richiesta principalmente in aziende fornitrici di servizi informatici o di consulenza in progetti presso aziende clienti, in cui è necessario coordinare team per lo sviluppo di software pianificando in modo ottimale tutte le fasi progettuali, fornendo altresì feedback sulle tecnologie necessarie a realizzare software con requisiti di affidabilità e sicurezza.

Il corso prepara alla professione di (codifiche ISTAT):

- Analisti e progettisti di software - (2.1.1.4.1)
- Analisti di sistema - (2.1.1.4.2)
- Analisti e progettisti di applicazioni web - (2.1.1.4.3)
- Specialisti in sicurezza informatica - (2.1.1.5.4)
- Ricercatori e tecnici laureati nelle scienze matematiche e dell'informazione - (2.6.2.1.1).

TRACCIABILITÀ TRA LE FIGURE PROFESSIONALI E I RISULTATI DI APPRENDIMENTO ATTESI (DESCRITTORI DI DUBLINO 1 E 2)

	Area Giuridica				Area Sociale - Economica				Area Informatica										
	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19
F1	X	X	X	X		X			X	X	X	X			X	X	X	X	X
F2		X		X			X		X	X	X	X	X				X	X	
F3		X			X	X	X	X	X		X			X					

Insegnamenti

F1: Consulente per la progettazione di sistemi software sicuri e per la gestione del rischio
F2: Progettisti di sistemi con requisiti avanzati di sicurezza informatica
F3: Project manager di sistemi informatici

Conoscenze e competenze

C1: rapporto intercorrente tra informatica e diritto
C2: regolamentazione relativa all'utilizzo delle tecnologie informatiche con particolare riferimento ai social network
C3: modalità di investigazione alla luce dell'ordinamento giuridico italiano
C4: princìpi generali in materia di trattamento dei dati
C5: contesti socio-economici, che influenzano il funzionamento delle organizzazioni
C6: metodologie per la pianificazione strategica e la redazione del business plan
C7: aspetti inerenti la struttura, le dinamiche e i processi di gruppo
C8: metodi e tecniche per l'analisi dei dati al fine di fornire al management aziendale le informazioni utili ad assumere decisioni e disegnare strategie
C9: metodologie di sviluppo dei sistemi software complessi, con particolare riferimento alla sicurezza e alla gestione dei progetti software
C10: problematiche e soluzioni organizzative relative alla sicurezza informatica
C11: architetture software basate su servizi e/o su cloud computing
C12: metodologie per garantire la sicurezza in architetture basate su servizi e/o cloud computing
C13: metodi e tecniche per la crittografia dei dati
C14: modelli di ottimizzazione connessi allo sviluppo di sistemi software complessi e sicuri
C15: tecnologie informatiche (hardware e software) per svolgere indagini informatiche o investigazioni difensive
C16: metodologie per il recupero di dati
C17: metodologie e delle tecniche per l'individuazione e la rimozione di vulnerabilità all'interno di sistemi software complessi
C18: tecniche di autenticazione e riconoscimento basate su sistemi biometrici
C19: tecniche di business intelligence per gestire la sicurezza e la criminalità informatica

TRACCIABILITÀ TRA LA ATTIVITÀ FORMATIVE PROGRAMMATE E I RISULTATI DI APPRENDIMENTO ATTESI (DESCRITTORI DI DUBLINO 1 E 2)

	Area Giuridica				Area Sociale - Economica				Area Informatica										
	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19
A1-a	X		X	X															
A1-b	X	X																	
A2					X	X	X	X											
A2					X	X	X	X											
A3							X		X	X									
A4										X	X	X							
A5										X			X						
A6										X				X					
A7						X		X											
A8															X	X			
A9										X							X		
A10																		X	
A11										X									X

Attività formative

A1-a: Informatica e diritto
A2-b: Profili giuridici dei social network
A2: Organizzazione e pianificazione aziendale
A3: Gestione progetti software
A4: Advanced networking
A5: Cryptography
A6: Metodi di ottimizzazione
A7: Big Data analysis
A8: Computer forensics e investigazioni
A9: Software reliability and testing
A10: Biometric systems
A11: Semantic intelligence for cybersecutiry

Conoscenze e competenze

C1: rapporto intercorrente tra informatica e diritto
C2: regolamentazione relativa all'utilizzo delle tecnologie informatiche con particolare riferimento ai social network
C3: modalità di investigazione alla luce dell'ordinamento giuridico italiano
C4: princìpi generali in materia di trattamento dei dati
C5: contesti socio-economici, che influenzano il funzionamento delle organizzazioni
C6: metodologie per la pianificazione strategica e la redazione del business plan
C7: aspetti inerenti la struttura, le dinamiche e i processi di gruppo
C8: metodi e tecniche per l'analisi dei dati al fine di fornire al management aziendale le informazioni utili ad assumere decisioni e disegnare strategie
C9: metodologie di sviluppo dei sistemi software complessi, con particolare riferimento alla sicurezza e alla gestione dei progetti software
C10: problematiche e soluzioni organizzative relative alla sicurezza informatica
C11: architetture software basate su servizi e/o su cloud computing
C12: metodologie per garantire la sicurezza in architetture basate su servizi e/o cloud computing
C13: metodi e tecniche per la crittografia dei dati
C14: modelli di ottimizzazione connessi allo sviluppo di sistemi software complessi e sicuri
C15: tecnologie informatiche (hardware e software) per svolgere indagini informatiche o investigazioni difensive
C16: metodologie per il recupero di dati
C17: metodologie e delle tecniche per l'individuazione e la rimozione di vulnerabilità all'interno di sistemi software complessi
C18: tecniche di autenticazione e riconoscimento basate su sistemi biometrici
C19: tecniche di business intelligence per gestire la sicurezza e la criminalità informatica