OBIETTIVI FORMATIVI SPECIFICI DEL CORSO E DESCRIZIONE DEL PERCORSO FORMATIVO

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.

Grazie ad un accordo di collaborazione con l'Università della Svizzera Italiana, gli studenti avranno la possibilità di partecipare ad un programma di studio comune di alta qualità in "Secure Software and Data Engineering", che prevede lo svolgimento del secondo anno di studio e l'acquisizione di almeno 30 CFU nell'Ateneo svizzero e che porta al rilascio di due certificati di laurea, uno per ciascuna istituzione (*double degree*).

RISULTATI DI APPRENDIMENTO ATTESI, ESPRESSI TRAMITE I DESCRITTORI EUROPEI DEL TITOLO DI STUDIO (DM 16/03/2007, ART 3, COMMA 7)

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 (KNOWLEDGE AND UNDERSTANDING)

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 nuove tecnologie informatiche;
- 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:

- Computer forensics and investigations
- Informatics and law
- Artificial intelligence and law

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 alla struttura, alle dinamiche e ai processi di gruppo (comunicativi, decisionali, di conflitto e negoziazione);
- conoscenza e comprensione delle metodologie per l'analisi automatica dei dati.

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

- Computational statistics and machine learning
- Security governance
- Software project management

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 metodologie per garantire la sicurezza nelle moderne architetture software;

- 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 delle tecniche di software analytics per l'analisi del livello di sicurezza di un sistema software;
- 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:

- Biometric systems
- Computer forensics and investigations
- Cryptography
- Networking security and software security
- Optimization methods for cybersecurity
- Software analytics for cybersecurity
- Software project management
- Semantic intelligence for cybersecurity

CAPACITÀ DI APPLICARE CONOSCENZA E COMPRENSIONE (APPLYING KNOWLEDGE AND UNDERSTANDING)

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 modelli e tecniche per la 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;
- 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;
- effettuare analisi per verificare l'affidabilità di un sistema software;
- utilizzare tecniche di business intelligence per gestire la sicurezza e la criminalità informatica.

AUTONOMIA DI GIUDIZIO (MAKING JUDGEMENTS)

Capacità che si intendono trasmettere. **I**l 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 (COMMUNICATION SKILLS)

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 (LEARNING SKILLS)

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.

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 nuove tecnologie informatiche
C3: modalità di investigazione alla luce dell'ordinamento giuridico italiano
C4: princìpi generali in materia di trattamento dei dati
C5: contesti socioeconomici, che influenzano il funzionamento delle organizzazioni
C6: metodologie per la pianificazione strategica e la redazione del business plan
C7: aspetti inerenti alla struttura, alle dinamiche e ai 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: metodologie per garantire la sicurezza in moderne architetture
C12: metodi e tecniche per la crittografia dei dati
C13: modelli di ottimizzazione connessi allo sviluppo di sistemi software complessi e sicuri
C14: tecnologie informatiche (hardware e software) per svolgere indagini informatiche o investigazioni difensive
C15: metodologie per il recupero di dati
C16: metodologie e delle tecniche per l'individuazione e la rimozione di vulnerabilità all'interno di sistemi software complessi
C17: tecniche di autenticazione e riconoscimento basate su sistemi biometrici
C18: tecniche di business intelligence per gestire la sicurezza e la criminalità informatica
C19: software analytics per l'analisi del livello di sicurezza di un sistema software

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	X	X		X															
A2		X		X															
A3					X	X	X												
A4							X		X	X									
A5										X	X					X			
A6										X		X							
A7										X			X						
A8								X											
A9			X	X										X	X				
A10										X						X			X
A11										X							X		
A12										X								X	

Attività formative

A1: Informatics and law
A2: Artificial intelligence and law
A3: Security governance
A4: Software project management
A5: Networking security and software security
A6: Cryptography
A7: Optimization methods for cybersecurity
A8: Computational statistics and machine learning
A9: Computer forensics and investigations
A10: Software analytics for cybersecurity
A11: Biometric systems
A12: Semantic intelligence for cybersecurity

Conoscenze e competenze

C1: rapporto intercorrente tra informatica e diritto
C2: regolamentazione relativa all'utilizzo delle nuove tecnologie informatiche
C3: modalità di investigazione alla luce dell'ordinamento giuridico italiano
C4: princìpi generali in materia di trattamento dei dati
C5: contesti socioeconomici, che influenzano il funzionamento delle organizzazioni
C6: metodologie per la pianificazione strategica e la redazione del business plan
C7: aspetti inerenti alla struttura, alle dinamiche e ai 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: metodologie per garantire la sicurezza in moderne architetture
C12: metodi e tecniche per la crittografia dei dati
C13: modelli di ottimizzazione connessi allo sviluppo di sistemi software complessi e sicuri
C14: tecnologie informatiche (hardware e software) per svolgere indagini informatiche o investigazioni difensive
C15: metodologie per il recupero di dati
C16: metodologie e delle tecniche per l'individuazione e la rimozione di vulnerabilità all'interno di sistemi software complessi
C17: tecniche di autenticazione e riconoscimento basate su sistemi biometrici
C18: tecniche di business intelligence per gestire la sicurezza e la criminalità informatica
C19: software analytics per l'analisi del livello di sicurezza di un sistema software