# REGOLAMENTO DIDATTICO DEL

*Corso di Studio Magistrale in*

# Sicurezza Informatica (sede di Taranto)

Anno Accademico 2023-2024

Regolamento didattico del Corso di Studio Magistrale in

# Sicurezza Informatica (sede di Taranto) – LM-66

## SOMMARIO

Regolamento didattico del Corso di Studio Magistrale in

# Sicurezza Informatica (sede di Taranto) – LM-66

## ART. 1 – INDICAZIONI GENERALI DEL CORSO DI STUDIO

| | |
|---|---|
| **Nome Corso di Studi** | Sicurezza Informatica |
| **Classe di Laurea (DD.MM. 16 marzo 2007 e s.m.i.)** | LM-66 – Sicurezza Informatica |
| **Struttura didattica di riferimento** | Dipartimento di Informatica |
| **Sede di svolgimento delle attività didattiche** | Dipartimento di Informatica (sede di Taranto)<br>Ex II Facoltà di Scienze - Quartiere Paolo VI<br>Via Alcide de Gasperi - 74123 - Taranto |
| **Indirizzo Internet** | https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica |
| **Anno di Ordinamento** | 2019 (D.M. 270/2004) |
| **Organo di gestione del Corso di Studi** | CICSI<br>Consiglio di Interclasse dei Corsi di Studio in Informatica |
| **Coordinatore del CICSI** | Prof. Giovanni Dimauro |
| **Lingua di erogazione** | Italiano |

## ART. 2 – OBIETTIVI FORMATIVI SPECIFICI, RISULTATI DI APPRENDIMENTO ATTESI E SBOCCHI OCCUPAZIONALI

### OBIETTIVI FORMATIVI SPECIFICI

La Laurea Magistrale in Sicurezza Informatica, in coerenza con gli obiettivi formativi specifici della Classe delle Lauree LM-66, fornisce vaste e approfondite competenze teoriche, metodologiche, sperimentali e applicative nelle aree fondamentali della Sicurezza Informatica.

Il laureato magistrale ha conoscenze e competenze riguardanti le metodologie informatiche e gli strumenti tecnologici fondamentali per svolgere attività di ricerca, progettazione, sviluppo, testing, coordinamento e gestione di sistemi informatici sicuri. Obiettivo della sua attività è anche l'innalzamento e il miglioramento costante dei livelli di sicurezza e di protezione in comprensione degli scopi applicativi e dei contesti specifici del sistema nel suo complesso. Le conoscenze e le competenze non si esauriscono a quelle metodologiche e tecnologiche proprie dell'informatica, ma sono estese anche alla gestione aziendale e agli aspetti giuridici relativi al trattamento dei dati sensibili, da un punto di vista della loro conservazione e trasmissione.

I laureati devono in particolare:

1. possedere solide conoscenze relative alle metodologie e agli strumenti tecnologici per la gestione dell'intero ciclo di vita di un sistema informatico sicuro;
2. conoscere il metodo scientifico di indagine, comprendere e utilizzare metodi, tecniche e strumenti per l'analisi dei dati;
3. conoscere i principi, le strutture e l'utilizzo di sistemi di elaborazione, reti e infrastrutture informatiche sicuri e protetti;
4. conoscere le tecniche, i metodi di progettazione e la realizzazione di sistemi informatici sicuri, sia di base sia applicativi;

5. avere conoscenza dei diversi contesti nei quali è fondamentale la sicurezza dei sistemi informatici;
6. possedere conoscenza di cultura aziendale e professionale;
7. conoscere gli aspetti giuridici che regolamentano il trattamento sicuro di dati sensibili;
8. possedere una approfondita conoscenza della lingua inglese comparabile al livello B2.

Gli obiettivi da 1 a 5 sono raggiunti tramite gli insegnamenti negli ambiti scientifico e tecnologico, gli obiettivi 6 e 7 sono raggiunti tramite gli insegnamenti nell'ambito giuridico, sociale ed economico. L'obiettivo 8 è raggiunto tramite un insegnamento nell'ambito linguistico.

Il corso di studio prevede insegnamenti che coprono l'area informatica rispetto alla sicurezza nelle reti, nei sistemi distribuiti e nelle basi di dati, alla realizzazione di architetture sicure orientate ai servizi, alla progettazione e gestione di sistemi complessi sicuri e protetti, all'identificazione biometrica, al data mining e ai metodi formali per la verifica di protocolli, al rapporto tra l'informatica e le modalità di investigazione previste dagli ordinamenti giuridici.

Per l'area giuridica, il corso di laurea in Sicurezza Informatica prevede insegnamenti che riguardano la regolamentazione giuridica circa l'utilizzo di soluzioni informatiche e la gestione e il trattamento dei dati sensibili (dalla loro acquisizione alla loro analisi ed elaborazione).

Per l'area socio-economica, il corso di laurea in Sicurezza Informatica prevede insegnamenti che riguardano i processi di divisione e di coordinamento del lavoro all'interno delle aziende, le dinamiche di team eterogenei di professionisti, la sicurezza interna ed esterna e i processi per la valutazione del rischio e le tecniche per la sua mitigazione.

Il laureato magistrale sarà quindi in grado di:

- collaborare all'analisi e alla valutazione tecnica dello stato di sicurezza attuale di un sistema informatico;
- collaborare all'analisi e alla valutazione delle caratteristiche di sicurezza necessarie per un sistema informatico rispetto al suo ambito di applicazione sociale, aziendale, tecnologico e normativo;
- proporre, negli ambiti operativi in cui opera, continue innovazioni che contraddistinguono la disciplina;
- supportare la realizzazione, gestione e manutenzione di sistemi sicuri per mezzo di tecniche e metodi informatici avanzati;
- gestire dati sensibili in contesti pubblici e privati;
- gestire il rischio derivante da falle di sicurezza;
- svolgere ruoli manageriali in contesti nazionali e internazionali.

Il percorso formativo prevede l'attività di tirocinio che può svolgersi presso aziende del settore, enti pubblici o privati e laboratori dell'Università e alla quale sono dedicati 20 CFU.

All'attività di tirocinio deve seguire lo sviluppo di un elaborato finale, in italiano o in inglese, redatto secondo la struttura di una pubblicazione scientifica che deve riguardare un'esperienza scientifica originale sui temi della sicurezza informatica. L'elaborato finale, al quale sono dedicati 10 CFU, è prodotto sotto la supervisione di un docente-relatore.

## RISULTATI DI APPRENDIMENTO ATTESI

Le competenze specifiche sviluppate dal corso di laurea in Sicurezza Informatica possono essere utilmente elencate, nel rispetto dei principi dell'armonizzazione europea, mediante il sistema dei descrittori di Dublino:

### A: CONOSCENZA E CAPACITÀ DI COMPRENSIONE (KNOWLEDGE AND UNDERSTANDING)

Il laureato magistrale del corso di studio di questa classe si caratterizza per la conoscenza dei fondamenti essenziali della sua disciplina, quali, per esempio, la gestione della complessità, i metodi e le tecniche per la sicurezza nelle reti, nei sistemi distribuiti e nelle basi di dati, i metodi e le tecniche per il data mining applicato alla sicurezza informatica, i metodi e le tecniche per l'autenticazione in sistemi biometrici oltre che per una competenza approfondita della lingua inglese.

Le conoscenze che il laureato magistrale acquisisce riguardano gli aspetti fondamentali della disciplina che rimangono inalterati rispetto alla continua evoluzione tecnologica.

Il laureato magistrale al termine del percorso formativo possiede conoscenze e competenze disciplinari di livello avanzato riguardanti le aree di apprendimento relative all'ambito scientifico-tecnologico, in particolare rispetto alla sicurezza nelle reti e nei sistemi distribuiti, alla crittografia, all'analisi dei dati per la sicurezza, ai sistemi biometrici, ai metodi formali per la sicurezza, alla sicurezza delle architetture orientate ai servizi, nelle applicazioni e negli ambienti mobile.

Riguardo alle aree di apprendimento relative all'ambito giuridico e socio-economico, il laureato magistrale possiede conoscenze e competenze disciplinari di livello avanzato quali l'informatica giuridica, il trattamento dei dati sensibili, l'organizzazione aziendale e l'analisi e la gestione del rischio.

Possiede inoltre approfondita conoscenza della lingua inglese, acquisita attraverso attività formative ulteriori nell'ambito linguistico, per comprendere e produrre testi complessi e comunicare in modo appropriato in contesti di settore.

*Risultati di apprendimento attesi*

Le conoscenze e le competenze disciplinari del corso di studio sono essenzialmente le seguenti:

1. conoscenze e competenze di crittografia relative alle metodologie e caratteristiche degli approcci per la segretezza delle informazioni ed integrità dei dati;
2. conoscenze e competenze inerenti la complessità, i rischi della complessità, le decisioni e le strategie nella sua gestione;
3. conoscenze e competenze relative ai metodi formali per la sicurezza, ai metodi per individuare le caratteristiche del sistema da analizzare, ai principali domini applicativi e alle algebre di processo;
4. conoscenze e competenze inerenti i metodi e le tecniche per la sicurezza delle reti e nei sistemi distribuiti, riguardo le minacce, le tipologie di attacchi, le tecnologie per la sicurezza e il rilevamento delle intrusioni, il controllo degli accessi, i protocolli, l'operating system security;

5. conoscenze e competenze relative ai metodi e alle tecniche per la sicurezza in architetture orientate ai servizi, alle architetture SoA ed attacchi, alle tecniche per sistemi distribuiti;
6. conoscenze e competenze inerenti le principali tecniche di data mining per Cyber Security (cyber-terrorismo e violazioni della sicurezza), tecniche di Intrusion detection, tecniche di auditing, tecniche di Link analysis, tecniche di classificazione;
7. conoscenze e competenze relative alle principali tecniche biometriche, ai fondamenti della biometria e alle caratteristiche dei principali tratti biometrici, alla struttura e all'organizzazione dei sistemi biometrici, alle strategie di valutazione e agli indicatori di performance dei sistemi biometrici, alle problematiche legate alla sicurezza ed alla vulnerabilità dei sistemi biometrici, alla normativa e agli standard dei sistemi biometrici, agli aspetti sociali e culturali legati all'uso dei sistemi biometrici;
8. conoscenze e competenze inerenti le tecniche per la sicurezza nelle basi di dati, l'integrità, la verificabilità, la riservatezza, l'autenticazione, la disponibilità;
9. conoscenze e competenze inerenti il trattamento di dati sensibili, la disciplina del trattamento dei dati nella pubblica amministrazione e in ambiti privati, le disposizioni relative a specifici settori, tutela e sanzioni;
10. conoscenze e competenze relative ai principali aspetti di organizzazione aziendale, ai processi di divisione e coordinamento del lavoro.

*Metodi didattici*

Il laureato magistrale acquisisce le conoscenze suddette attraverso lezioni, esercitazioni, attività di laboratorio e mediante ulteriori strumenti di supporto alla didattica. Tali attività possono essere condotte anche in modalità e-learning. Il corso prevede lo svolgimento di attività individuali e di gruppo sotto il tutorato del docente nella forma di casi di studio.

Il corso prevede anche lo svolgimento di un tirocinio presso aziende del settore, enti pubblici o privati o laboratori dell'Università al fine di redigere un elaborato finale da presentare in seduta di laurea.

*Modalità di verifica*

La verifica del conseguimento dei risultati attesi è effettuata durante l'anno accademico, in base alle caratteristiche degli insegnamenti, mediante prove in itinere ed esami che prevedono prove scritte e/o prove pratiche e/o colloqui orali.

La predisposizione dell'elaborato finale, conseguente all'attività di tirocinio, consente allo studente di dimostrare, rispetto al problema affrontato, capacità di analisi, di sviluppo del progetto e della sua realizzazione nonché di saper collocare il tema trattato nel panorama attuale delle conoscenze relative alla Sicurezza Informatica.

Le conoscenze e competenze disciplinari del corso di studio che lo studente magistrale deve possedere sono pertanto oggetto di continua verifica.

## B: CAPACITÀ DI APPLICARE NELLA PRATICA CONOSCENZE E COMPRENSIONE (APPLYING KNOWLEDGE AND UNDERSTANDING)

Il laureato magistrale sarà in grado di applicare le conoscenze acquisite per:

- analizzare e valutare lo stato di sicurezza attuale di un sistema informatico sia attraverso l'utilizzo di modelli che di evidenze empiriche;
- analizzare e valutare le caratteristiche di sicurezza necessarie per un sistema informatico rispetto al suo ambito di applicazione;
- progettare, implementare e coordinare lo sviluppo di sistemi sicuri per mezzo di tecniche e metodi informatici avanzati;
- proporre e valutare soluzioni alternative e selezionare le tecnologie più appropriate, ma anche gli oneri economici e la forza lavoro richiesta;
- organizzare e gestire (anche a livello manageriale) lo sviluppo di progetti software sicuri di grandi dimensioni o che coinvolgano grossi team di progettazione/sviluppo in ambiti applicativi eterogenei quali pubblica amministrazione, banche, assicurazioni e finanza, industrie, sanità, ambiente, energia ed utilities, ricerca;
- gestire e manutenere il sistema informatico sicuro;
- comprendere gli ambiti di applicabilità di norme e soluzioni tecniche rispetto agli scenari di interesse;
- trattare dati sensibili in maniera conforme alle norme;
- valutare i modelli organizzativi e gestionali in essere o da adottare, con riferimento allo scenario aziendale e sociale dell'ente/impresa in cui opera;
- valutare il contesto (sociale, economico e di mercato) dell'ente/impresa in cui opera;
- effettuare valutazioni di sicurezza interna ed esterna dell'ente/impresa in cui opera e porre in essere tecniche per la attenuazione del rischio;

produrre elaborati chiari e dettagliati in lingua inglese su un'ampia gamma di argomenti per essere in grado di esprimere opinioni indicando vantaggi e svantaggi in riferimento a diverse opzioni; saper argomentare con scioltezza e spontaneità interagendo in modo naturale in contesti internazionali.

## C: AUTONOMIA DI GIUDIZIO (MAKING JUDGEMENTS)

Il laureato magistrale dovrà acquisire la capacità di formulare giudizi autonomi, nonché di esprimere valutazioni collegiali (maturate attraverso le prove di gruppo), con riferimento alle politiche gestionali e scelte tecnico-progettuali degli enti nei quali potrà operare. Il laureato sarà in grado di proporre soluzioni volte al miglioramento della sicurezza del sistema informatico.

In tutti i corsi curricolari verranno segnalate agli studenti, ove necessario, le possibili implicazioni etiche delle ricerche e degli studi in oggetto anche con riferimento alla deontologia professionale tra le diverse figure che operano nel settore della sicurezza informatica. Il laureato sarà, pertanto, consapevole delle responsabilità relative alla propria professione.

Nello specifico, l'autonomia di giudizio riguarda:

- capacità di analisi individuale;

- capacità di confronto in team;
- capacità di analisi multidisciplinare rispetto alle soluzioni progettuali;
- capacità di comparazione tra soluzioni diverse e/o alternative;
- capacità di valutare obiettivamente risultati empirici.

*Metodi didattici*

Il Corso di studio prevede lo sviluppo di casi di studio (singoli e/o in team anche mediante l'uso di piattaforme di e-learning) e la redazione di elaborati.

*Modalità di verifica*

La verifica dell'autonomia di giudizio sarà effettuata attraverso la valutazione della capacità di discutere in gruppo o con i singoli docenti, attraverso la valutazione di elaborati e in occasione della discussione della tesi di laurea.

## D: ABILITÀ NELLA COMUNICAZIONE (COMMUNICATION SKILLS)

Le abilità comunicative saranno sviluppate per consentire ai laureati magistrali di interloquire sia con professionisti specialisti sia con professionisti non specialisti.

A tal fine, saranno adottati metodi di didattica e di valutazione atti a stimolare le capacità di comunicazione e sintesi dei contenuti appresi e dei temi elaborati, favorendo in particolare lo svolgimento di presentazioni sia in lingua italiana sia in lingua inglese. Sarà inoltre favorita la partecipazione attiva a seminari e workshop organizzati con la collaborazione di professionisti ed esperti del settore.

L'approccio interdisciplinare dei corsi e la loro strutturazione e organizzazione mirano a stimolare la capacità del laureato magistrale di utilizzare un linguaggio scientifico, legale ed economico per l'analisi, l'elaborazione e la presentazioni di dati.

Il laureato magistrale sarà in grado di:

- comunicare ed esprimere verbalmente in modo chiaro ed efficace le conoscenze apprese, presentare i casi di studio trattati e discutere le soluzioni adottate adeguando il contenuto al target professionale dell'uditorio;
- redigere elaborati scritti chiari, sintetici e coerenti;
- lavorare in team con diverse professionalità.

*Metodi didattici*

Il corso di studio prevede:

- l'elaborazione e discussione di relazioni su esercitazioni in laboratorio e in aula, condotte in piccoli gruppi o singolarmente;
- la partecipazione a gruppi di lavoro per lo sviluppo di attività progettuali nell'ambito di specifici insegnamenti;
- lo studio da testi e fonti anche in lingua inglese;
- l'analisi, la sintesi, l'esposizione e la discussione di dati di letteratura;
- l'elaborazione e la discussione della tesi di laurea.

*Modalità di verifica*

Saranno determinanti al fine della valutazione delle competenze acquisite:

- le prove di esame scritte e orali;
- la verifica effettuata durante lo svolgimento delle attività connesse con il tirocinio formativo e durante la preparazione della tesi di laurea;

la discussione della tesi durante la seduta di laurea

## E: CAPACITÀ DI APPRENDERE (LEARNING SKILLS)

Il laureato magistrale sarà in grado di procedere in autonomia alla ricerca, selezione e approfondimento delle fonti da consultare al fine di documentarsi riguardo uno specifico scenario/tema di interesse. Gli studenti saranno incoraggiati ad approfondire tematiche di loro interesse e, conseguentemente, a esporle in forma scritta e/o orale.

Anche con riferimento alla scelta del tirocinio professionalizzante e della tesi, pur mettendo a disposizione degli studenti un ampio ventaglio di possibili opzioni, sarà favorita una scelta autonoma.

Tale approccio consentirà al laureato magistrale di apprendere metodologie e modus operandi utili a mantenere aggiornate le proprie competenze in un settore in continua evoluzione anche con riferimento a nuovi scenari applicativi. Il laureato magistrale sarà anche in grado di intraprendere e affrontare percorsi di studio superiori (dottorato, master).

Il laureato magistrale sarà quindi in grado di:

- individuare, elaborare e organizzare informazioni appropriate per soluzioni di problemi caratterizzanti la propria attività professionale;
- elaborare e organizzare idee in modo critico e sistematico.

*Metodi didattici*

Le capacità suddette saranno sviluppate prevalentemente quando lo studente, per lo svolgimento dei casi di studio e dell'elaborato finale, avrà bisogno della consultazione di materiale bibliografico tradizionale o reperibile via internet o attraverso piattaforme di e-learning.

*Modalità di verifica*

La verifica delle capacità di apprendimento sarà effettuata in maniera continuativa durante le varie attività formative, durante lo sviluppo di casi di studio/progetti e durante lo svolgimento sia del tirocinio sia della preparazione della tesi di laurea.

## SBOCCHI OCCUPAZIONALI E PROFESSIONALI PREVISTI

Tutti gli ambiti del settore pubblico e privato che utilizzano tecnologie informatiche sono contesti lavorativi in cui la figura professionale dello specialista in Sicurezza Informatica trova collocazione. Si elencano, di seguito, alcuni esempi:

- banche
- assicurazioni

- logistica e trasporti
- sanità
- pubbliche amministrazioni
- telecomunicazioni e media
- società di servizi
- industria
- enti di ricerca
- aziende specializzate in cyber security

Competenze associate alla funzione

Le competenze che si intendono sviluppare vertono sulla conoscenza e comprensione di:

- approcci per la segretezza delle informazioni ed integrità dei dati;
- metodologie per la gestione della complessità;
- metodi e principi per la realizzazione di architetture sicure orientate ai servizi;
- tecniche per la sicurezza nelle reti e nei sistemi distribuiti;
- tecniche e metodi per l'analisi della sicurezza;
- tecniche e metodi per l'autenticazione in sistemi biometrici;
- tecniche e metodi di data mining per cyber security;
- tecniche e metodi per la sicurezza nelle basi di dati;
- sicurezza informatica in sistemi complessi;
- principali risultati di ricerca nei diversi ambiti della sicurezza informatica;
- relazione tra Informatica e diritto nelle investigazioni;
- regolamentazione giuridica circa l'utilizzo di soluzioni informatiche;
- gestione e trattamento dei dati sensibili (dalla loro acquisizione alla loro analisi ed elaborazione);
- caratteristiche delle moderne aziende;
- processi di divisione e coordinamento del lavoro;
- aspetti inerenti le dinamiche di un team eterogeneo di professionisti sicurezza interna ed esterna dell'azienda;
- processi per la valutazione e tecniche per la mitigazione del rischio.

## ART. 3 – REQUISITI DI AMMISSIONE E MODALITÀ DI VERIFICA DELL'ADEGUATEZZA DELLA PREPARAZIONE INIZIALE

Il corso di studio è a numero aperto. Potranno presentare direttamente domanda di iscrizione al corso di laurea magistrale in Sicurezza Informatica coloro che sono in possesso di una laurea conseguita presso questo o altro Ateneo nell'ambito della classe delle lauree di informatica (classe 26 o classe L-31) e nella classe delle lauree dell'Ingegneria dell'informazione (classe 9 o L-08), nonché coloro che sono in possesso di altro titolo di studio conseguito in Italia o all'estero e riconosciuto idoneo dal corso di studio.

Le certificazioni rilasciate da enti e/o aziende del settore non saranno considerate nella valutazione e acquisizione dei crediti formativi della laurea magistrale.

È comunque condizione per l'ammissione al corso di studio aver conseguito almeno:

- 18 CFU complessivi in uno o più dei settori scientifico-disciplinari MAT/01, MAT/02, MAT/03, MAT/05, MAT/06, MAT/07, MAT/08, MAT/09, FIS/01, FIS/02, FIS/03, FIS/07;
- 48 CFU complessivi in uno o più dei settori scientifico-disciplinari INF/01, ING-INF/05, ING-INF/03;
- conoscenza della lingua Inglese a livello B1.

Gli studenti in possesso di tali requisiti curriculari potranno accedere alla verifica personale della preparazione che sarà obbligatoria e avverrà tramite un colloquio orale e/o una prova scritta.

In particolare, la preparazione personale richiederà conoscenze e competenze relative a: algoritmi e strutture dati, architetture degli elaboratori, basi di dati, ingegneria del software, linguaggi di programmazione, sistemi operativi, reti di calcolatori e conoscenza della lingua Inglese a livello B1.

Una commissione appositamente nominata dal Corso di Studi provvederà in primo luogo alla verifica dei requisiti curriculari minimi, basata sull'analisi del curriculum pregresso dello studente che potrà essere integrato, se ritenuto necessario, con i programmi dei corsi seguiti. Accertata la presenza dei requisiti curriculari, si passerà all'accertamento della personale preparazione che sarà obbligatoria e sarà effettuata tramite prove orali e/o scritte.

La valutazione della preparazione personale verrà effettuata tramite test che si terrà entro il mese di settembre. La data del test e la scadenza per la prenotazione saranno comunicate mediante pubblicazione sul sito web del Dipartimento di Informatica.

Ulteriori sessioni di test, potranno essere organizzate entro aprile dell'anno successivo e saranno comunicate successivamente alla pubblicazione degli esiti della prima sessione di settembre.

Il superamento del test di verifica dell'adeguata preparazione è obbligatorio per effettuare l'immatricolazione al corso di studi.

## ART. 4 – DESCRIZIONE DEL PERCORSO FORMATIVO E DEI METODI DI ACCERTAMENTO

### DESCRIZIONE DEL PERCORSO FORMATIVO

Il corso di studi Magistrale in Sicurezza Informatica è articolato in un unico curriculum. La frequenza ai corsi non è obbligatoria, ma è fortemente raccomandata. Per l'iscrizione agli anni successivi al primo non è richiesta l'acquisizione di un numero minimo di CFU.

L'attività didattica è svolta secondo diverse possibili tipologie di insegnamento in corrispondenza delle quali si acquisiscono crediti formativi e, per consentire l'applicazione delle nozioni apprese, il Corso di Laurea Magistrale in Sicurezza Informatica prevede una intensa attività di laboratorio e un significativo numero di Crediti Formativi Universitari (CFU) per tirocini da svolgere presso aziende, enti pubblici o privati al fine di favorire il trasferimento delle competenze dal mondo universitario al mondo del lavoro. In particolare, sono previste:

- lezioni tradizionali in aula, supportate da strumenti audio-visivi multimediali;
- lezioni ed esercitazioni di laboratorio a piccoli gruppi;
- attività didattiche integrative e di sostegno mediante collaboratori ed esperti linguistici (CEL);

- progetti individuali e di gruppo supportati da tutor;
- seminari ed altro.

Queste tipologie di forme didattiche possono essere integrate da didattica a distanza e da laboratori per l'auto-apprendimento.

In conformità al D.M. 3 Nov. 1999, ogni credito formativo corrisponde ad un carico standard di impegno didattico - formativo pari a 25 ore, e può essere articolato secondo la seguente tipologia:

**T1.** 8 h di lezione in aula/in modalità e-learning e 17 di studio individuale;

**T2.** 15 h di laboratorio ed esercitazioni guidate/ in modalità e-learning e 10 di rielaborazione personale;

**T3.** 25 h di esercitazioni di progetto;

**T4.** 25 h di studio individuale.

In riferimento alla tabella relativa alla distribuzione dei crediti con la indicazione dei settori disciplinari, come appare nell'ordinamento didattico della Università degli Studi di Bari, le attività formative sono classificabili come segue:

a. attività formative caratterizzanti;
b. attività formative affini;
c. attività formative autonomamente scelte dallo studente (tali attività devono essere certificate dal superamento di un esame con voto in trentesimi);
d. attività formative relative alla preparazione della prova finale e alla verifica della conoscenza della lingua straniera;
e. attività formative di tirocinio (seminari, stage).

La certificazione dei crediti acquisiti dallo studente avviene sostenendo prove scritta e/o orale e/o di laboratorio. Le specifiche modalità di svolgimento di ciascun esame sono indicate nel programma di ogni insegnamento pubblicato sul sito web del Corso di Studi. Tali modalità possono comunque prevedere che l'ammissione ad una prova sia subordinata all'esito delle prove precedenti e che possano essere esentati da una parte delle prove di esame gli studenti che abbiano positivamente sostenuto prove in itinere con valore esonerante, secondo quanto indicato nei programmi degli insegnamenti.

I crediti formativi corrispondenti a ciascuna attività formativa sono acquisiti dallo studente previo il superamento dell'esame o a seguito di altra forma di verifica della preparazione o delle competenze conseguite.

## METODI DI ACCERTAMENTO

La verifica del profitto ha lo scopo di accertare l'adeguata preparazione degli studenti iscritti al corso di studio ai fini della prosecuzione della loro carriera universitaria e della acquisizione da parte loro dei crediti corrispondenti alle attività formative seguite.

La verifica del profitto individuale dello studente ed il conseguente riconoscimento dei CFU maturati nelle varie attività formative sono effettuati mediante prove scritte e/o orali e/o di laboratorio, secondo le modalità definite dal docente titolare dell'insegnamento e riportate nel programma dell'anno accademico corrente. Tutti gli esami danno luogo a votazione (esami di profitto), eccetto l'esame di Lingua Inglese che dà luogo ad un giudizio di idoneità.

L'esame di profitto dà luogo ad una votazione espressa in trentesimi. L'esito della votazione si considera positivo ai fini dell'attribuzione dei CFU se si ottiene un punteggio di almeno diciotto trentesimi (18/30). L'attribuzione della lode nel caso di una votazione pari a trenta trentesimi (30/30) è a discrezione della commissione d'esame e richiede l'unanimità dei suoi componenti.

Gli esami di profitto sono pubblici e pubblica è la comunicazione del voto finale. La trasparenza della valutazione delle prove scritte è garantita dall'accesso ai propri elaborati prima della prova orale o della registrazione del voto d'esame, nel caso in cui la valutazione si svolga solo in forma scritta.

Ogni titolare di insegnamento è tenuto ad indicare prima dell'inizio dell'anno accademico e contestualmente alla programmazione didattica il programma e le specifiche modalità di svolgimento dell'esame previsto per il suo insegnamento.

Le commissioni d'esame sono costituite da almeno due docenti, di cui uno è il titolare dell'insegnamento. Alle commissioni di esame di lingua inglese partecipano i collaboratori ed esperti linguistici (CEL). I docenti titolari dell'insegnamento potranno anche avvalersi di verifiche in itinere per valutare l'andamento del corso. Tali verifiche in itinere possono avere valore esonerante, a discrezione del docente titolare dell'insegnamento. Le prove in itinere non potranno mai sostituire l'esame finale.

Le date degli esami e delle verifiche in itinere non dovranno normalmente essere sovrapposte ai periodi di svolgimento delle lezioni.

Gli esami si svolgono successivamente alla conclusione del periodo delle lezioni, esclusivamente nei periodi previsti per gli appelli di esame. Le date sono comunicate dai titolari e disponibili sul sistema ESSE3 raggiungibile, tramite link, anche dal sito del Dipartimento di Informatica.

La data di un appello di esame non può essere anticipata rispetto a quella pubblicata e può essere posticipata solo per un grave e giustificato motivo. In ogni caso deve essere data opportuna comunicazione agli studenti.

Il CICSI favorisce lo svolgimento di tirocini formativi presso aziende pubbliche o private, nazionali o estere; sono inoltre possibili attività di progetto da svolgersi presso i laboratori dei Dipartimenti Universitari. Il CICSI sulla base dello specifico programma di lavoro previsto definirà, in conformità a quanto previsto dal Piano di Studi, il numero di crediti formativi da assegnare a questa tipologia di attività formativa.

Lo svolgimento del tirocinio/attività di progetto è attività formativa obbligatoria; i risultati ottenuti vengono verificati attraverso attestati di frequenza e/o relazioni sulla attività svolta.

I risultati di eventuali periodi di studio all'estero verranno esaminati dal CICSI in base ai programmi presentati dallo studente, cui verrà riconosciuto un corrispettivo in CFU coerente con l'impegno sostenuto per le attività formative frequentate all'estero ed una votazione in trentesimi equivalente a quella riportata eventualmente con diversi sistemi di valutazione.

Si terrà comunque conto della coerenza complessiva dell'intero piano di studio conseguito all'estero con gli obiettivi formativi del Corso di Laurea Magistrale in Sicurezza Informatica, piuttosto che la perfetta corrispondenza dei contenuti tra le singole attività formative.

I CFU acquisiti hanno, di norma, validità per un periodo di 8 (otto) anni dalla data dell'esame. Dopo tale termine il CICSI dovrà verificare l'eventuale obsolescenza dei contenuti conoscitivi provvedendo eventualmente alla determinazione di nuovi obblighi formativi per il conseguimento del titolo.

## ATTIVITÀ A SCELTA DELLO STUDENTE

Per quanto riguarda le attività formative a scelta (tipologia d), gli studenti possono inserire nel proprio piano di studi tutti gli insegnamenti attivati nell'Ateneo, comprese le attività per l'acquisizione di competenze trasversali, purché coerenti con gli obiettivi formativi; la coerenza viene stabilita dal CICSI. Gli ulteriori insegnamenti attivabili, elencati in coda al piano di studi, sono consigliati dal CICSI e si intendono coerenti per il raggiungimento degli obiettivi formativi.

Lo studente può comunque proporre al CICSI un piano di studi individuale nei termini previsti dal Regolamento Didattico di Ateneo. I piani di studio individuali, contenenti insegnamenti diversi da quelli previsti nel piano di studi ufficiale, saranno sottoposti alla valutazione del CICSI che verificherà se essi, come prescritto dall'art. 10 del DM 270/2004, siano coerenti con il progetto formativo. Il piano di studi individuale, può essere approvato o rigettato; nel secondo caso lo studente sarà tenuto a seguire:

- il piano di studi ufficiale nel caso in cui non sia stato proposto in precedenza un piano individuale accettato dal CICSI;

oppure

- l'ultimo piano di studi individuale proposto ed approvato dal CICSI.

I crediti acquisiti a seguito di esami eventualmente sostenuti con esito positivo per insegnamenti aggiuntivi rispetto a quelli conteggiabili ai fini del completamento del percorso che porta al titolo di studio rimangono registrati nella carriera dello studente e possono dare luogo a successivi riconoscimenti ai sensi della normativa in vigore. Le valutazioni ottenute non rientrano nel computo della media dei voti degli esami di profitto.

## CERTIFICAZIONI LINGUA INGLESE

Agli studenti in possesso di certificazioni internazionali di Lingua Inglese di livello B2 o superiore saranno interamente riconosciuti i 3 CFU per la Lingua Inglese.

Regolamento didattico del Corso di Studio Magistrale in

# Sicurezza Informatica (sede di Taranto) – LM-66

## PROGRAMMAZIONE DIDATTICA

Il periodo per lo svolgimento di lezioni, esercitazioni, seminari, attività di laboratorio è stabilito, annualmente. Ciascun anno di corso è articolato in due semestri, ognuno dei quali comprende almeno 12 settimane di lezioni.

Gli esami di profitto e ogni altro tipo di verifica soggetta a registrazione previsti per il corso di laurea possono essere sostenuti solo successivamente alla conclusione dei relativi insegnamenti.

Lo studente in regola con l'iscrizione e i versamenti relativi può sostenere, senza alcuna limitazione numerica, tutti gli esami e le prove di verifica che si riferiscano a corsi di insegnamento conclusi e nel rispetto delle eventuali propedeuticità.

L'orario delle lezioni, da fissarsi tenendo conto delle specifiche esigenze didattiche e delle eventuali propedeuticità, è stabilito con almeno 30 giorni di anticipo rispetto allo svolgimento lezioni. Le date degli esami di profitto e delle prove di verifica sono stabilite con almeno 60 giorni di anticipo rispetto allo svolgimento delle prove e delle lezioni. Il numero degli appelli, non inferiori a otto nell'anno accademico per ciascun esame, e la loro distribuzione sono stabiliti evitando, possibilmente, la sovrapposizione con i periodi di lezioni.

## CALENDARIO DIDATTICO

Nell'a.a. 2023-2024, le date dei semestri sono:

| | | |
|---|---|---|
| I Semestre | 25 settembre 2023 | 12 gennaio 2024 |
| | Interruzione lezioni: | 13-17 novembre 2023 |
| II Semestre | 1 marzo 2024 | 7 giugno 2024 |
| | Interruzione lezioni: | 29 marzo -12 aprile 2024 |

Le sessioni d'esame per il corso di studi (valide per l'a.a. cui fa riferimento il presente regolamento/manifesto) sono così definite:

***Insegnamenti del I semestre***

3 appelli nei mesi di gennaio e febbraio 2024

1 appello a giugno/luglio 2024

2 appelli nel mese di settembre 2024

1 appello nel mese di novembre 2024

1 appello marzo / aprile 2025 (nel periodo di sospensione delle lezioni).

***Insegnamenti del II semestre***

3 appelli nei mesi di giugno e luglio 2024

2 appelli nel mese di settembre 2024

1 appello nel mese di novembre 2024

1 appello a gennaio/febbraio 2025

1 appello marzo / aprile 2025 (nel periodo di sospensione delle lezioni).

Eventuali prove in itinere si svolgono normalmente nel periodo di interruzione delle lezioni.

Le prove finali per il conseguimento della laurea si svolgono sull'arco di almeno tre appelli distribuiti nei seguenti periodi: da giugno a luglio, da settembre a dicembre, da febbraio ad aprile.

## ART. 5 – TRASFERIMENTI IN INGRESSO E PASSAGGI DI CORSO

Il CICSI delibera sul riconoscimento dei crediti nei casi di trasferimento da altro ateneo, di passaggio ad altro corso di studio o di svolgimento di parti di attività formative in altro ateneo italiano o straniero, anche attraverso l'adozione di un piano di studi individuale.

I crediti nei settori INF/01 oppure ING-INF/05 conseguiti presso i Corsi di Laurea della stessa classe LM-66 vengono integralmente riconosciuti.

Il CICSI delibera altresì sul riconoscimento della carriera percorsa da studenti che abbiano già conseguito il titolo di studio presso l'Ateneo o in altra Università italiana o che siano contemporaneamente iscritti ad altro corso di studi ai sensi della legge n. 33/2022 e del DM 930/2022 e che chiedano, contestualmente all'iscrizione, l'abbreviazione degli studi. Questa può essere concessa previa valutazione e convalida dei crediti formativi considerati riconoscibili in relazione al corso di studio prescelto.

Esclusivamente nel caso in cui il trasferimento dello studente sia effettuato tra corsi di studio appartenenti alla medesima classe, la quota dei crediti relativi al medesimo settore scientifico disciplinare direttamente riconosciuti allo studente non potrà essere inferiore al 50% di quelli già maturati. Nel caso in cui il corso di provenienza sia svolto in modalità a distanza, la quota minima del 50% è riconosciuta solo se il corso di provenienza risulta accreditato ai sensi del Regolamento Ministeriale di cui all'art. 2 comma 148 del decreto legge 3 ottobre 2006, n. 262, convertito dalla legge 24 novembre 2006 numero 286.

I crediti eventualmente conseguiti non riconosciuti ai fini del conseguimento del titolo di studio rimangono, comunque, registrati nella carriera universitaria dell'interessato.

Possono essere riconosciuti come crediti, nella misura e secondo i criteri stabiliti dagli ordinamenti didattici dei corsi di studio, le conoscenze e le abilità professionali certificate ai sensi della normativa vigente in materia, nonché altre conoscenze e abilità maturate in attività formative di livello post secondario alla cui progettazione e realizzazione l'Ateneo abbia concorso.

Per il riconoscimento di CFU maturati dagli studenti in esperienze precedenti, ad esempio a seguito di esami sostenuti in altro Corso di Laurea dell'Università di Bari o altra Università o Accademia italiana o straniera, è necessario fare domanda al CICSI fornendo adeguata documentazione, certificata dalla struttura formativa di provenienza, che riporti:

- il programma seguito;
- l'impegno impiegato dallo studente, per acquisire le conoscenze o le abilità di cui si richiede il riconoscimento, espresso in termini di ore di lezione/laboratorio valutabili come CFU;
- le modalità di accertamento/valutazione (esame scritto, orale, prova di laboratorio, etc. scale di valutazione) e la eventuale votazione riportata.

Agli studenti in possesso di certificazioni internazionali di Lingua Inglese di livello B2 o superiore saranno interamente riconosciuti i 3 CFU per la Lingua Inglese.

Lo studente, proveniente da altri corsi di laurea, è iscritto al primo anno di corso se il numero di CFU riconosciuti non è maggiore di 29; è iscritto al secondo anno di corso se il numero di CFU riconosciuti è almeno uguale a 30.

Il riconoscimento degli studi compiuti all'estero è regolato da specifiche norme del Regolamento Didattico di Ateneo (articolo 20).

## ART. 6 – OPPORTUNITÀ OFFERTE DURANTE IL PERCORSO FORMATIVO

### MOBILITÀ INTERNAZIONALE

Tra le opportunità di studio/formazione all'estero disponibili al link:

https://www.uniba.it/it/internazionale/mobilita-in-uscita/studenti/studenti

segnaliamo, in particolare, le seguenti:

- **Erasmus+ STUDIO**: il programma comunitario Erasmus Plus consente agli studenti regolarmente iscritti all'Università degli Studi di Bari Aldo Moro di ottenere un contributo finanziario per trascorrere all'estero un periodo di studio (corsi, esami, preparazione tesi di laurea) presso un'università di uno dei paesi indicati nel bando, in base agli accordi stipulati.
- **Erasmus+ Traineeship**: Il nuovo programma europeo ERASMUS+ a supporto dell'istruzione, della formazione, della gioventù e dello sport, ha sostituito ed integrato il Lifelong Learning Programme per il periodo 2014-2020. La Key action 1 del programma medesimo permette agli studenti di primo, secondo e terzo ciclo di svolgere dei periodi di formazione in imprese, centri di formazione, centri di ricerca, atenei ed altre organizzazioni che sono presenti in uno dei Paesi partecipanti al Programma. Il Programma prevede l'erogazione di un contributo finanziario (borsa) per la copertura parziale delle spese sostenute dai beneficiari durante il periodo di mobilità per tirocinio all'estero.
- **Premio di studio Global Thesis** (DM 29.12.2014 n. 976): consente agli studenti della magistrale o del ciclo unico di ricevere una borsa di studio per svolgere l'attività di tesi all'estero.
- **Progetto S.E.M.I.N.A.R.E.**: Scambi in Europa e nel Mediterraneo per Internazionalizzare gli Atenei della Regione Puglia – in cui l'Unimed mette a disposizione degli studenti dell'Ateneo barese borse di studio per recarsi presso l'Università di Istanbul – Aydin (Turchia) e di Tampere (Finlandia).

Gli studenti possono fare domanda e partire per una destinazione straniera 1 volta per ogni ciclo di laurea (di I livello, II livello, dottorato). Il periodo previsto è da 2 a 12 mesi. I neolaureati possono partire entro un anno dalla laurea per stage sia presso centri di ricerca che presso aziende straniere. Questa esperienza è considerata molto importante anche nell'ottica del trasferimento delle know-how acquisito alle nostre realtà aziendali.

La permanenza all'estero, l'organizzazione e le modalità di verifica sono regolate da esplicite norme del Regolamento Didattico d'Ateneo (Art. 33) e dal Regolamento per la mobilità degli studenti Erasmus+ (D.R. 1160).

Nell'ottica di stimolare ed incentivare i nostri studenti ad andare all'estero attraverso le possibilità offerte, il Consiglio di Interclasse ha deliberato di riconoscere una premialità nel contesto dell'esame di laurea (premio internazionalizzazione).

## TIROCINIO E STAGE

Il servizio di Job Placement del Dipartimento di Informatica promuove e stipula convenzioni con aziende, dislocate sul territorio regionale e nazionale, che operano nel settore dell'ICT.

Le aziende propongono, in accordo con docenti del corso di studio, progetti formativi di valenza industriale, che possano essere svolti nell'ambito delle attività di stage/tirocinio curriulari. Questi progetti formativi, realizzati presso le sedi aziendali, possono essere oggetto della prova finale del percorso di studi e sono finalizzati all'inserimento rapido nel mondo del lavoro.

Tramite il portale dell'Agenzia per il Placement (www.portiamovalore.uniba.it), tutte le aziende che si interfacciano con l'Università di Bari per offrire lavoro, tirocini curriculari e post laurea, si iscrivono e possono sottoscrivere convenzioni con le varie strutture universitarie.

Tutte le informazioni sono reperibili sul sito del Dipartimento di Informatica nella sezione «Tirocini».

http://www.uniba.it/ricerca/dipartimenti/informatica/didattica/tirocini/tirocini-informatica

## TUTORATO

Sul portale del Dipartimento sono disponibili le informazioni relative al tutorato, aggiornate costantemente per informare gli studenti sulle iniziative disponibili, pubblicizzare i calendari degli incontri e rendere nota la disponibilità di nuovi Bandi.

http://www.uniba.it/ricerca/dipartimenti/informatica/tutorato

## DIDATTICA PERSONALIZZATA E INDIVIDUALIZZATA

L'ufficio per i servizi agli studenti disabili e DSA di Ateneo garantisce, attraverso l'attivazione di servizi specifici, la tutela e il supporto al diritto allo studio in presenza di disabilità e Disturbo Specifico dell'Apprendimento (DSA) e la piena inclusione nella vita universitaria, in ottemperanza alla legge 17/99 che integra la precedente legge 104/92 e alla legge 170/2010.

https://www.uniba.it/it/studenti/servizi-per-disabili

## ART. 7 – PROVA FINALE

La prova finale deve costituire un'importante occasione formativa individuale a completamento del percorso.

Alla prova finale si accede previa acquisizione di almeno 110 CFU, secondo quanto previsto dal piano didattico. Al superamento di tale prova vengono assegnati 10 CFU che permettono il conseguimento della Laurea.

Per conseguire la laurea lo studente dovrà discutere un elaborato finale di fronte ad una commissione di laurea nominata in conformità all' Art. 6 del DPR 2/1/2001.

Tale elaborato dovrà collocare il tema affrontato nel panorama attuale delle conoscenze nel settore della Sicurezza Informatica e documentare tutti gli aspetti inerenti l'analisi del/i problema/i affrontato/i, il progetto e la sua realizzazione, nonché eventuali aspetti di ricerca. Il progetto dovrà essere svolto sotto la guida di un relatore mediante lo stage presso un'azienda, una pubblica amministrazione, o un Dipartimento dell'Università degli Studi di Bari.

Per accedere alla prova finale lo studente dovrà:

- aver superato tutti gli esami previsti dal piano di studi;
- aver ottenuto, complessivamente 90 CFU articolati in 2 anni di corso;
- aver svolto un tirocinio professionalizzante di 20 CFU;

L'elaborato finale potrà essere redatto in lingua inglese, ma la presentazione dovrà essere in lingua italiana.

Il titolo è conferito dalla commissione di laurea composta dai docenti del CICSI.

La commissione esprimerà la propria valutazione tenendo conto dei seguenti criteri: carriera dello studente, media ponderata esami di profitto, contenuto ed esposizione, diligenza nella attività di tesi, per un massimo di 10 punti. Sono previste ulteriori premialità relative ad attività svolte in programmi di mobilità internazionale (2 punti) e al completamento del corso di studi entro i due anni (durata legale) (2 punti).

La valutazione dell'esame di laurea verrà espressa in 110mi. In caso di conseguimento della valutazione massima, per decisione unanime della Commissione, può essere conferita la lode.

I termini di consegna della documentazione per l'accesso alla prova finale saranno disponibili sul sito web dell'Università di Bari o potranno essere richiesti alla segreteria studenti. La domanda per il conseguimento del titolo dovrà essere debitamente compilata on-line sul sistema ESSE3. La proposta di argomento di tesi e di tirocinio, completa della dichiarazione del relatore di disponibilità a seguire l'attività di tesi, dovrà essere consegnata in segreteria didattica almeno 3 mesi prima della seduta di laurea. Tale modulistica sarà disponibile sul sito web del Dipartimento.

## ART. 8 – ASSICURAZIONE DELLA QUALITÀ

Regolamento didattico del Corso di Studio Magistrale in

## Sicurezza Informatica (sede di Taranto) – LM-66

Il Corso di Studi aderisce alla politica di Assicurazione della Qualità di Ateneo.

Specifica commissione nominata dal Consiglio Interclasse dei Corsi di Studio Magistrale in Sicurezza Informatica per l'Assicurazione della Qualità viene nominata ogni anno.

La commissione esamina:

- le statistiche sull'andamento degli studi;
- i risultati dei questionari, compilati dagli studenti, sulla qualità dei corsi;
- le statistiche sugli occupati tra i laureati alla laurea Magistrale in Sicurezza Informatica.

Il Team di Assicurazione della Qualità è costituito dalle seguenti figure:

- Il Coordinatore dell'Interclasse
- Il Docente Responsabile Assicurazione della Qualità del Corso di Studi
- Il Docente Referente del Corso di Studi
- Il Manager didattico
- Lo Studente

Le segnalazioni da parte degli studenti/esse vengono gestiti dal Coordinatore e dalla U.O. Didattica.

### ART. 9 – NORME FINALI

Il presente Regolamento è applicato a decorrere dall'a.a. 2023-2024 e rimane in vigore per l'intera coorte di studi.

Per tutto quanto non espressamente previsto dal presente Regolamento si rinvia allo Statuto, al Regolamento Didattico di Ateneo e alla normativa vigente, nonché alle disposizioni dell'Università.

Regolamento didattico del Corso di Studio Magistrale in

## Sicurezza Informatica (sede di Taranto) – LM-66

ALLEGATO 1 – OBIETTIVI FORMATIVI DEGLI INSEGNAMENTI

# Corso di Studio Magistrale in Sicurezza Informatica (sede di Taranto) – LM-66 Anno Accademico 2023-2024

| Attività formativa | Obiettivi formativi |
|---|---|
| **Attività obbligatoria** | |
| Analisi dei dati per la sicurezza | Il corso si propone di fornire gli strumenti algoritmici per lo sviluppo di competenze teoriche in merito al metodo scientifico di indagine, metodi, tecniche e strumenti per l'analisi dei cyber dati |
| Analisi e gestione del rischio | Acquisizione di adeguate conoscenze relative all'analisi e gestione del rischio delle informazioni nei contesti organizzativi di piccole, medie e grandi dimensioni. |
| Crittografia | Acquisizione delle competenze crittografiche, raggiungimento della piena consapevolezza e capacità di distinzione tra algoritmo e protocollo crittografico, dei singoli algoritmi e protocolli, delle loro proprietà, peculiarità, debolezze e delle modalità di applicazione. Valutazione di ciascun elemento nei termini di riservatezza, autenticazione delle parti, integrità e non ripudio. Ottenimento della massima competenza e conoscenza dei limiti della crittografia e delle sue debolezze intrinseche. Acquisizione delle capacità di determinare i limiti e le debolezze di ciascun algoritmo attraverso una conoscenza basilare della crittanalisi e dei concetti legati allo spazio delle chiavi. |
| Lingua Inglese | Il corso mira a fornire agli studenti di Sicurezza Informatica degli strumenti che saranno loro utili per acquisire una buon padronanza della lingua inglese tale da consentire loro di esprimere e interpretare concetti, in forma sia orale che scritta e di adottare un registro tecnico linguistico appropriato al loro campo di studio. |
| Metodi formali per la sicurezza | Acquisizione di competenze nei metodi formali, in particolare quelli basati sulla logica, utilizzati in informatica per progettare sistemi che soddisfino i requisiti di sicurezza |
| Organizzazione aziendale | Il corso fornisce elementi di organizzazione dei processi e dei servizi dell'impresa nella direzione della difesa e protezione delle proprie reti ed informazioni. Definizione e strutturazione operativa di SOC e CSIRT. |
| Sicurezza delle architetture orientate ai servizi | Acquisizione delle competenze in materia di sicurezza dei sistemi distribuiti, raggiungimento della consapevolezza sulle tipologie di attacco DDoS per le architetture orientate ai servizi e delle tecniche di mitigazione. Acquisizione delle capacità di determinare i limiti e le debolezze delle architetture orientate ai |

Regolamento didattico del Corso di Studio Magistrale in

## Sicurezza Informatica (sede di Taranto) – LM-66

| Attività formativa | Obiettivi formativi |
|---|---|
| | servizi Ottenimento delle competenze e conoscenza dei sistemi avanzati per la gestione della sicurezza e degli eventi. |
| Sicurezza in ambienti mobile | Acquisizione delle conoscenze sulla sicurezza in ambienti mobile, in particolare, sull'architettura, gli strumenti e le tecniche di verifica della sicurezza in ambienti protetti. Capacità di effettuare l'analisi di sicurezza di app mobile in ambienti Android e di realizzare report che descrivono tali attività. |
| Sicurezza nelle applicazioni | Acquisizione di adeguate conoscenze relative a ambiti progettuali strategici sulla sicurezza informatica. Comprensione delle criticità nello sviluppo di applicazioni software. Acquisizione di competenza nello sviluppo di applicazioni sicure in linguaggio Java. |
| Sicurezza nelle reti e nei sistemi distribuiti | Lo studente apprenderà i concetti fondamentali della sicurezza delle reti di calcolatori e nei sistemi distribuiti, con particolare riferimento ai livelli applicativi della pila di protocolli TPC/IP. |
| Sistemi biometrici | Il corso prevede lo studio di soluzioni e tecniche di intelligenza artificiale per progettare e sviluppare soluzioni in ambito di sistemi biometrici. A tali concetti sono affiancati quelli inerenti aspetti normativi in ambito GDPR per la protezione dei dati. Il corso intende anche fornire elementi generali per la individuazione e comparazione delle diverse tecnologie e delle diverse soluzioni. |
| Trattamento dei dati sensibili | L'insegnamento, che riguarda la tutela del dato personale, in particolare in ambito sicurezza informatica, ha come obiettivo quello di rendere lo studente edotto circa l'importanza della "privacy", concetto inquadrabile sia sotto il profilo giuridico, sia sotto quello informatico, nell'analisi dei dati. Lo studente apprenderà la normativa risultante dal Reg. UE 2016/679 (GDPR) e dal D.lgs. n. 196/2003, e ss.mm.ii., acquisendo la capacità di effettuare scelte in ordine al rispetto dei principi del trattamento dei dati di cui all'art. 5 del GDPR. |
| **Attività a scelta dello studente** | |
| Informatica e Diritto | Fornire agli studenti le conoscenze relative alle problematiche giuridiche che potrebbero sorgere utilizzando le nuove tecnologie ed alle opportune soluzioni rapportate al caso di specie. |
| Informatica Forense | Il corso si propone di formare i futuri professionisti della Digital Forensics, mettendoli in grado di conoscere modelli teorici e applicare tecniche scientifiche e rigorose, con un approccio metodologico conforme alle normative vigenti che cristallizzi gli elementi probatori digitali preservandone l'efficacia ai fini legali. |
| Logica applicata | Gli studenti conosceranno i fondamenti, i principali compiti ed approcci della Logica Applicata. Conosceranno anche nel dettaglio i principali algoritmi presenti in letteratura. Saranno quindi in grado di |

Regolamento didattico del Corso di Studio Magistrale in

## Sicurezza Informatica (sede di Taranto) – LM-66

| Attività formativa | Obiettivi formativi |
|---|---|
| | applicare tecniche di rappresentazione ed inferenza logica a problemi specifici, e di impostare correttamente le tecniche per un proficuo utilizzo. |
| Progettazione di Sistemi Sicuri | Sviluppare competenze sulla capacità di individuare le vulnerabilità di un sistema software che possono essere sfruttate dagli attaccanti, e le possibili soluzioni per prevenire e mitigare gli attacchi software. |
| Quantum Computing | Il corso mira a sviluppare competenze teoriche e metodologiche sulle tecniche di calcolo quantistico che possono essere utilizzate per supportare la risoluzione di problemi irrisolvibili con il calcolo classico o di problemi nuovi per qualsiasi paradigma computazionale |
| Teoria dell'informazione | Il corso si propone di introdurre alcuni concetti fondamentali inerenti all'Informatica, attingendo dalla Teoria Generale dei Sistemi, la Cibernetica, la Teoria della Comunicazione di Shannon e la Teoria dell'Informazione Algoritmica. Lo scopo dell'insegnamento è di fissare i concetti fondamentali e di saperli riconoscere e utilizzare nell'esercizio professionale dell'Informatica. |