



Informazioni generali sul Corso di Studi

Università	Università degli Studi di BARI ALDO MORO
Nome del corso in italiano	Sicurezza Informatica(<i>IdSua:1571202</i>)
Nome del corso in inglese	Cyber Security
Classe	LM-66 - Sicurezza informatica
Lingua in cui si tiene il corso	italiano
Eventuale indirizzo internet del corso di laurea	https://www.uniba.it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica
Tasse	Pdf inserito: visualizza
Modalità di svolgimento	b. Corso di studio in modalità mista



Referenti e Strutture

Presidente (o Referente o Coordinatore) del CdS	DIMAURO Giovanni
Organo Collegiale di gestione del corso di studio	CICSI - Consiglio di Interclasse dei Corsi di Studio in Informatica
Struttura didattica di riferimento	Informatica

Docenti di Riferimento

N.	COGNOME	NOME	SETTORE	QUALIFICA	PESO	TIPO SSD
1.	DESOLDA	Giuseppe	INF/01	RD	1	Caratterizzante
2.	IMPEDOVO	Donato	ING-INF/05	PA	1	Caratterizzante

3.	LISI	Francesca Alessandra	INF/01	PA	1	Caratterizzante
4.	MIGNONE	Paolo	ING-INF/05	RD	1	Caratterizzante
5.	PIRLO	Giuseppe	ING-INF/05	PO	1	Caratterizzante
6.	BUONO	Paolo	INF/01	PA	1	Caratterizzante

Rappresentanti Studenti	Petruzzellis Flavio f.petruzzellis6@studenti.uniba.it Villano Giorgia g.villano@studenti.uniba.it Dimaggio Michele m.dimaggio18@studenti.uniba.it Abbinante Alessandro a.abbinante14@studenti.uniba.it Parisi Matteo m.paris39@studenti.uniba.it Zizza Vincenzo v.zizza2@studenti.uniba.it Ianne Alessandro a.ianne3@studenti.uniba.it Ungaro Marco m.ungaro15@studenti.uniba.it De Palma Antonio a.depalma54@studenti.uniba.it Manfredi Walter w.manfredi@studenti.uniba.it Luceri Matteo m.luceri3@studenti.uniba.it Calore Giammarco g.calore2@studenti.uniba.it Caputo Francesco f.caputo45@studenti.uniba.it Pizzolla Anna a.pizzolla3@studenti.uniba.it
Gruppo di gestione AQ	MARCELLA CIVES GIOVANNI DIMAURO DONATO IMPEDOVO FEDERICA NITTI VERONICA ROSSANO
Tutor	Donato IMPEDOVO Annalisa APPICE Paolo BUONO Venere ALTAMURA



12/05/2021

Il Corso di Laurea Magistrale intende far acquisire ai futuri laureati conoscenze e competenze specifiche nell'ambito della Sicurezza Informatica. Più precisamente, il percorso di studio è teso a formare professionisti che abbiano conoscenze e competenze di tipo teorico, metodologico, sperimentale e applicativo che consentano di svolgere attività sia di progettazione, sviluppo, test come pure di ricerca, coordinamento e gestione riguardo sistemi informatici complessi dove è fondamentale il tema della sicurezza e della protezione da molteplici punti di vista: infrastrutturale, organizzativo, tecnologico, applicativo e normativo.

Il laureato in Sicurezza Informatica dovrà essere in grado non solo di sviluppare e gestire sistemi informatici complessi sicuri ma dovrà anche conoscere gli aspetti giuridici che regolamentano il trattamento dei dati informatici, la registrazione e la trasmissione dei dati sensibili. Il laureato acquisirà anche conoscenze e competenze che consentiranno di ricoprire ruoli manageriali presso imprese, aziende di servizi e istituzioni.

Il percorso formativo è strutturato in modo tale da fornire ai laureati una formazione avanzata e in linea con lo stato dell'arte in relazione alle metodologie e soluzioni in ambito Sicurezza Informatica.

Le attività formative sono svolte prevalentemente attraverso lezioni frontali, esercitazioni, prove di laboratorio e mediante ulteriori strumenti di supporto alla didattica. Il corso prevede anche l'erogazione in modalità e-learning di alcuni insegnamenti quali Organizzazione aziendale e Trattamento dei dati sensibili. Questi insegnamenti non prevedendo Crediti Formativi dedicati specificatamente ad attività laboratoriali e, quindi, possono essere fruiti efficacemente anche in modalità asincrona favorendo una didattica flessibile maggiormente incentrata sui bisogni degli studenti.

Sono previste attività individuali e di gruppo sotto la guida del docente e il tirocinio presso aziende del settore, enti pubblici o privati e laboratori dell'Università al fine non solo di redigere l'elaborato finale da presentare in seduta di laurea, ma anche di condurre una esperienza formativa significativa.

Il laureato in Sicurezza Informatica potrà proseguire gli studi nell'ambito di Dottorati di Ricerca o Master di secondo livello.



QUADRO A1.a

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

10/01/2017

Dipartimento di Informatica - 24 novembre 2016 - ore 10.00 - Sala Consiglio

La prof.ssa Roselli, Coordinatore dell'Interclasse dei CdS in Informatica ha convocato Enti e Aziende di rilievo che quotidianamente si trovano a fronteggiare le problematiche della Sicurezza Informatica.

Nell'ambito dell'incontro, sono stati posti i seguenti quesiti:

1) Ritenete utile, per lo sviluppo del territorio, formare la figura professionale dell'Esperto in Sicurezza Informatica che abbia competenze in:

- progettazione, realizzazione, verifica e manutenzione di infrastrutture e sistemi informatici sicuri e protetti;
- trattamento sicuro e riservato dei dati informatici, bio-sanitari e bioetici con particolare attenzione agli aspetti giuridici;
- organizzazione del lavoro, con particolare attenzione agli elementi critici relativi alla sicurezza delle infrastrutture e dei sistemi informatici ed alla protezione dei dati informatici.

2) Tali conoscenze/competenze ritenete siano sufficienti o ritenete che debbano essere ampliate per formare e rendere competitiva sul mercato del lavoro la figura dell'Esperto in Sicurezza Informatica?

3) Siete interessati ad una collaborazione con l'Università degli Studi di Bari Aldo Moro nell'offrire opportunità di formazione/stage presso la vostra azienda/ente?

I soggetti consultati

- Aeronautica Militare – Referente Comscuole A.M.
- Autorità Portuale di Taranto – Referenti Direzione Affari Generali e Direzione Operativo e Sicurezza
- Carabinieri Legione Puglia – Referente del Comando Provinciale dei Carabinieri
- Comando Esercito Puglia – Referente Scuola Cavalleria
- Marina Militare – Direttore Studi della Scuola sottufficiali della Marina Militare di Taranto
- Electronic's Time - Martina Franca (TA) – Responsabile Formazione
- Exprivia S.p.A. Molfetta (BA) - Direttore Area Application & Infrastructure Management
- Masvis S.r.L. – Conversano (BA) – Amministratore Unico
- SOGET S.p.A. Taranto – Responsabile servizi

hanno non solo espresso parere positivo rispetto alle questioni poste ma, soprattutto, hanno dichiarato che la figura professionale che si intende formare andrebbe a soddisfare un'esigenza fortemente sentita.

Alla luce di questi elementi la laurea magistrale LM66 costituisce una possibile risposta per la formazione di figure qualificate negli aspetti di rilievo della sicurezza informatica.

Per la definizione puntuale della corrispondenza ed una sempre migliore adesione tra la figura professionale formata dal CdS e le esigenze del territorio, si prevede, in concomitanza con le diverse fasi del processo di valutazione, una interazione successiva ed ampliata con le parti sociali.

Pdf inserito: [visualizza](#)

Descrizione Pdf: Verbale consultazione organizzazioni rappresentative

11/05/2021

Il 20 marzo 2018 l'Ufficio Placement del Dipartimento di Informatica ha organizzato una giornata di confronto con le realtà aziendali di settore presso la sede di Taranto per gli studenti del Corso di Studi Triennale in Informatica e Comunicazione Digitale e del Corso Magistrale in Sicurezza Informatica, attivo da quest'anno accademico.

La giornata è stata strutturata in due momenti differenti.

Nella mattinata, la Elmec Informatica S.p.A. ha proposto agli studenti un seminario dal titolo 'Ethical Hacking' nel quale ha illustrato alcune tra le più frequenti tecniche di attacco e come prevenire e sfruttare le vulnerabilità.

Ha poi coinvolto i ragazzi in un business game in modalità Capture the Flag con premialità finale per il vincitore.

Gli studenti hanno risposto in modo molto positivo all'invito anche per l'attinenza dell'argomento trattato con i profili che i due corsi di studio vanno a formare.

Da parte sua, l'azienda ha espressamente dichiarato di aver riscontrato una realtà d'eccellenza dove gli studenti, insieme alle competenze specifiche, hanno dimostrato di avere curiosità, entusiasmo e voglia di mettersi in gioco. Queste caratteristiche consentono loro di rispondere alla richiesta del mercato di oggi che punta sulla verticalizzazione delle competenze digitali, ovvero la necessità di conoscere, di un determinato ambito/argomento dagli aspetti basilari ai risvolti più spiccatamente specialistici e sulla disponibilità alla formazione continua, necessaria data la rapida evoluzione delle IT. Nel pomeriggio si è tenuto un secondo momento di confronto con la Fincons S.p.A. e l'Exprivia S.p.A., aziende di notevoli dimensioni presenti sul mercato internazionale e con la Klopotek Software & Technology Services Italia S.r.L., società che fornisce soluzioni software e servizi di consulenza nel campo dell'editoria e che, quindi, ha espresso grande interesse per il profilo del laureato/laureando in Informatica e Comunicazione Digitale.

Nella prima parte dell'incontro, le aziende hanno presentato la propria mission e dato una panoramica dei profili professionali ricercati. Si è poi lasciato spazio alle domande formulate dagli studenti (laureandi/laureati) e dai docenti e all'esplicitazione delle modalità di selezione messe in atto dalle aziende.

Tutte le aziende hanno manifestato l'interesse ad avviare progetti di tirocinio curriculare come primo momento di sinergia tra il mondo accademico e il mercato del lavoro.

Il giorno 25 ottobre 2018 alle ore 9:30, nell'Aula Magna del Dipartimento di Informatica, si è tenuto l'incontro di consultazione con le parti sociali con lo scopo di verificare la validità dell'offerta formativa del Dipartimento di Informatica e capire le prospettive e le scelte da attuare nel lungo termine. E' stata l'occasione anche per presentare la nuova modalità didattica del Corso di Laurea in Sicurezza Informatica che riguarda alcuni insegnamenti che si intendono erogare in e-learning.

All'incontro erano presenti:

- il Direttore del Dipartimento di Informatica, Prof. Donato Malerba;
- il Coordinatore del Consiglio di Interclasse dei Corsi di Studio in Informatica, Prof.ssa Teresa Roselli;
- il Responsabile dell'Agenzia per il Placement dell'Università Aldo Moro, dott.ssa Teresa Fiorentino;
- il Presidente del Distretto Produttivo dell'Informatica, dott. Salvatore Latronico;
- il Comandante del Comando Scuole A.M./3^a Regione Aerea, tenente colonnello Daniele Ortensio;
- il Vice Presidente e Tesoriere dalla Sezione Terziario Innovativo e Comunicazione di Confindustria Bari-Bat.

• i rappresentanti delle seguenti Aziende:

Accenture, Altran, Eusoft Srl, Everis, Experis, Exprivia SpA, Fincons SpA, Gruppo ISC Srl, HCL Technologies, IBM, Omnitech, Planetek, Randstad, Revevol.

Erano inoltre presenti i docenti dei corsi di studio e gli studenti sia della sede di Bari sia della sede di Taranto.

Durante l'incontro la prof.ssa Roselli ha sottolineato che la scelta di adottare la 'modalità mista' risponde alle esigenze di chi chiede maggiore flessibilità nello studio, per motivi di lavoro o familiari, consente di supportare chi ha difficoltà a seguire con regolarità i corsi in presenza e a sostenere i relativi esami e offre la possibilità di sperimentare nuove forme di didattica universitaria centrata sull'attività e la partecipazione dello studente al suo processo di acquisizione della conoscenza.

I convenuti hanno condiviso la modalità innovativa di erogazione di parte del Corso di Sicurezza Informatica anche nell'ottica di favorire la formazione permanente e l'aggiornamento di figure professionali già presenti sul mercato.

Il 4 dicembre 2019, nell'ambito del Career Day, si è tenuto un nuovo tavolo di consultazione con le parti sociali.

All'incontro erano presenti:

- il Direttore del Dipartimento di Informatica;
- il Coordinatore del Consiglio di Interclasse dei Corsi di Studio in Informatica;

- le seguenti Aziende nelle persone dei loro rappresentanti:
Applicazioni di Ingegneria ed Informatica Srl – Operating Manager
Auriga SpA – Responsabile HR e HR assistant
BurdaForward Italia – Branch Principal Manager
BV Tech SpA – ICT Recruiter
Euris – Responsabile Business Unit Prodotti
Exprivia SpA – Recruiting specialist
Iconconsulting SpA – Business Consultant – HR
KLOPOTEK SOFTWARE E TECH. – HR Senior Consultant e Direttore di filiale
LINKS MANAGEMENT AND TECHNOLOGY – Talent Acquisition Coordinator
Maggioli SpA – HR - Talent Acquisition Specialist
MAINSTREAMING SPA – Account Manager HR
Openjobmetis SpA – Responsabile Ufficio Comunicazione e Marketing
RGI SpA – HR Employer Branding
Scai Synteg Srl – HR Specialist
Security Architect Srl – Marketing & Sales Representative

Erano inoltre presenti i docenti dei corsi di studio e gli studenti. Per gli studenti della sede di Taranto è stato messo a disposizione il trasporto in pullman gratuito.

Nel mese di Aprile 2021 è stata effettuata una consultazione non presenziale (tramite questionario) con le parti interessate (imprese di settori affini a quelli dei CdS, Enti di Ricerca, etc.), la cui sintesi è riportata nel Pdf di seguito.

Pdf inserito: [visualizza](#)

Descrizione Pdf: Sintesi consultazioni con le parti sociali non presenziali



QUADRO A2.a

Profilo professionale e sbocchi occupazionali e professionali previsti per i laureati

Specialista in Sicurezza Informatica

funzione in un contesto di lavoro:

Lo specialista in Sicurezza Informatica potrà svolgere funzioni di analista, progettista, programmatore e project manager di sistemi informatici avanzati ad alto contenuto di sicurezza. Potrà, inoltre, ricoprire i ruoli di amministratore di Sistema e consulente in ambito di Sicurezza Informatica avendo acquisito conoscenze relative sia alla gestione di progetti e di processi aziendali sia agli aspetti normativi e giuridici che regolamentano il trattamento di dati sensibili.

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.

sbocchi occupazionali:

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



QUADRO A2.b

Il corso prepara alla professione di (codifiche ISTAT)

1. Analisti e progettisti di software - (2.1.1.4.1)
2. Analisti di sistema - (2.1.1.4.2)
3. Specialisti in reti e comunicazioni informatiche - (2.1.1.5.1)
4. Specialisti in sicurezza informatica - (2.1.1.5.4)
5. Ricercatori e tecnici laureati nelle scienze matematiche e dell'informazione - (2.6.2.1.1)



17/01/2017

Il Corso di studi è a numero aperto. Possono 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 CdS.

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 CdS 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, devono accedere alla verifica personale della preparazione che è obbligatoria e avviene tramite un colloquio orale e/o una prova scritta.

In particolare la preparazione personale richiede 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.

Il superamento delle prove è condizione necessaria per l'accettazione della domanda di immatricolazione al corso di studi.



12/05/2021

Nel Regolamento del CdS sono specificate le modalità di ammissione: una commissione appositamente nominata dal CICS I provvede in primo luogo alla verifica dei requisiti curriculari minimi, basata sull'analisi del curriculum progressivo dello studente che può essere integrato, se ritenuto necessario, con i programmi dei corsi seguiti. Accertata la presenza dei requisiti curriculari, si passa all'accertamento della personale preparazione che è obbligatoria ed è effettuata tramite prove orali e/o scritte. Date, tipologia e argomenti di tali prove sono indicati nel Regolamento del CdS.

Pdf inserito: [visualizza](#)

Descrizione Pdf: Art. 3 Regolamento Didattico del CdS

14/01/2019

La Laurea Magistrale in Sicurezza Informatica, in coerenza con gli obiettivi formativi specifici della Classe delle Lauree LM66, fornisce vaste e approfondite competenze teoriche, metodologiche, sperimentali ed 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 agli aspetti giuridici relativi al trattamento dei dati sensibili, da un punto di vista della loro conservazione e trasmissione, e alla gestione aziendale.

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 orientata 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 le 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.

**Conoscenza e
capacità di
comprensione**

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 CdS 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 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

11. Conoscenze e competenze comunicative nell'ambito della lingua inglese dei linguaggi settoriali.

Metodi didattici

Il laureato magistrale acquisisce le conoscenze suddette prevalentemente attraverso lezioni frontali, esercitazioni, attività di laboratorio e mediante ulteriori strumenti di supporto alla didattica. Alcuni insegnamenti sono erogati 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 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 capacità di analisi del problema affrontato, di sviluppo del progetto e della sua realizzazione e di saper collocare il tema affrontato nel panorama attuale delle conoscenze nell'ambito della Sicurezza Informatica.

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

Capacità di applicare conoscenza e comprensione

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 mantenere 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.

Metodi didattici

Sono previste lezioni prevalentemente frontali, esercitazioni, attività di laboratorio e utilizzo anche di ulteriori strumenti di supporto alla didattica. Alcuni insegnamenti sono erogati in modalità e-learning. Lo studente applica la conoscenza e la comprensione acquisite svolgendo casi di studio in modo individuale e/o in gruppo sotto la guida del docente. Il percorso di studi si completa con un periodo di tirocinio da svolgere presso aziende del settore, enti pubblici o privati o laboratori dell'Università al fine di redigere l'elaborato finale oggetto della discussione in seduta di laurea.

Modalità di verifica

La verifica del conseguimento dei risultati attesi, e quindi le conoscenze e le competenze disciplinari acquisite nel corso di studio, è effettuata costantemente durante tutto l'anno accademico. Vengono effettuate prove in itinere ed esami, che prevedono prove scritte e/o prove pratiche e/o colloqui orali, secondo le caratteristiche degli insegnamenti. L'elaborato finale, conseguente all'attività di tirocinio, consente allo studente di dimostrare di possedere capacità di analisi rispetto al problema affrontato, di essere in grado di sviluppare e realizzare il progetto oltre a saper collocare il tema affrontato nel panorama attuale delle conoscenze relative alla Sicurezza Informatica.

Conoscenza e comprensione

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;
- principi e metodi per la realizzazione di architetture sicure orientate ai servizi;
- metodi e tecniche per la sicurezza nelle reti e nei sistemi distribuiti;
- metodi e tecniche per l'analisi della sicurezza;
- metodi e tecniche per l'autenticazione in sistemi biometrici;
- metodi e tecniche per il data mining per cyber security;
- metodi e tecniche per la sicurezza nelle basi di dati;
- fondamenti di sicurezza informatica in sistemi complessi;
- principali risultati di ricerca nei diversi ambiti della sicurezza informatica;
- relazione tra informatica e diritto nelle investigazioni.

Le attività formative correlate alle precedenti competenze sono articolate in insegnamenti quali:

- Sicurezza nelle reti e nei sistemi distribuiti
- Crittografia
- Analisi dei dati per la sicurezza
- Sistemi biometrici
- Sicurezza nelle applicazioni
- Logica
- Metodi formali per la sicurezza
- Sicurezza delle architetture orientate ai servizi
- Progettazione di sistemi sicuri
- Informatica forense.

Capacità di applicare conoscenza e comprensione

Il laureato magistrale sarà in grado di:

- 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 e a stato dell'arte;
- gestire e mantenere il sistema informatico sicuro.

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

[Visualizza Insegnamenti](#)

[Chiudi Insegnamenti](#)

ANALISI DEI DATI PER LA SICUREZZA [url](#)

CRITTOGRAFIA [url](#)

METODI FORMALI PER LA SICUREZZA [url](#)

SICUREZZA DELLE ARCHITETTURE ORIENTATE AI SERVIZI [url](#)

SICUREZZA IN AMBIENTI MOBILE [url](#)

SICUREZZA NELLE APPLICAZIONI [url](#)

SICUREZZA NELLE RETI E NEI SISTEMI DISTRIBUITI [url](#)

SISTEMI BIOMETRICI [url](#)

Conoscenza e comprensione

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

- Regolamentazione giuridica circa l'utilizzo di soluzioni informatiche
- Gestione e trattamento dei dati sensibili (dalla loro acquisizione alla loro analisi ed elaborazione)

Le attività formative correlate alle precedenti competenze sono articolate in insegnamenti quali:

- Informatica giuridica
- Trattamento dei dati sensibili

Capacità di applicare conoscenza e comprensione

Il laureato magistrale sarà in grado di:

- comprendere gli ambiti di applicabilità di norme e soluzioni tecniche rispetto agli scenari di interesse;
- trattare dati sensibili in maniera conforme alle norme.

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

[Visualizza Insegnamenti](#)

[Chiudi Insegnamenti](#)

TRATTAMENTO DEI DATI SENSIBILI [url](#)

Area Socio-Economica

Conoscenza e comprensione

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

- 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.

Le attività formative correlate alle precedenti competenze sono articolate in insegnamenti quali:

- Organizzazione aziendale
- Analisi e gestione del rischio

Capacità di applicare conoscenza e comprensione

Il laureato magistrale sarà in grado di:

- 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.

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

[Visualizza Insegnamenti](#)

[Chiudi Insegnamenti](#)

ANALISI E GESTIONE DEL RISCHIO [url](#)

ORGANIZZAZIONE AZIENDALE [url](#)

Area Linguistica

Conoscenza e comprensione

Le competenze che si intendono sviluppare vertono sulla conoscenza e la comprensione della comunicazione in linguaggi settoriali della lingua inglese sviluppate attraverso attività formative ulteriori nel settore scientifico disciplinare L-LIN/12.

Capacità di applicare conoscenza e comprensione

Il laureato magistrale sarà in grado di:

- Comprendere argomenti chiave di un testo complesso in lingua inglese
- Produrre elaborati chiari e dettagliati 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.

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

[Visualizza Insegnamenti](#)

[Chiudi Insegnamenti](#)

LINGUA INGLESE [url](#)



QUADRO A4.c

Autonomia di giudizio
Abilità comunicative
Capacità di apprendimento

Autonomia di giudizio

Il laureato magistrale dovrà acquisire la capacità di formulare giudizi autonomi, nonché 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 curriculari verranno, ove necessario, segnalate agli studenti 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 infine, in occasione della discussione della tesi di laurea.

Le abilità comunicative saranno sviluppate per consentire ai laureati magistrali di interloquire sia con professionisti specialisti che non specialisti. A tal fine, verranno proposti agli studenti 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 anche mediante strumenti di interazione sincrona e asincrona (forum, chat, instant messaging, etc.).
- lo studio da testi e fonti anche in lingua inglese.
- l'analisi, sintesi, esposizione e discussione di dati di letteratura.
- l'elaborazione e 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.

Abilità comunicative

Capacità di apprendimento

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, necessiterà 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.



QUADRO A5.a

Caratteristiche della prova finale

13/01/2017

La prova finale deve costituire un'importante occasione formativa individuale a completamento del percorso. 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, anche in concomitanza con lo stage presso un'azienda, una pubblica amministrazione, o un laboratorio 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;

Al superamento di tale prova vengono assegnati 10 CFU che permettono il conseguimento della Laurea.



QUADRO A5.b

Modalità di svolgimento della prova finale

12/05/2021

Per conseguire la laurea lo studente dovrà discutere, di fronte ad una commissione di laurea nominata secondo le

disposizioni di legge vigenti, un elaborato finale.

L'elaborato finale preparato dallo studente 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 deve 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. L'elaborato finale può essere redatto in lingua inglese, ma la presentazione deve essere in lingua italiana.

Il conferimento del titolo avviene ad opera della commissione di laurea composta da almeno sette docenti del CICS. Tale commissione è presieduta di norma dal Coordinatore del CICS. In assenza di questo, potrà essere presieduta dal docente più anziano in ruolo.

La commissione esprimerà la propria valutazione tenendo conto dei seguenti criteri: carriera dello studente, esami di profitto, contenuto ed esposizione, diligenza nella attività di tesi. Sono previste premialità relative allo svolgimento della tesi in Erasmus e al completamento del corso di studi entro i due anni (durata legale).

I termini di consegna della documentazione per l'accesso alla prova finale sono disponibili sul sito web dell'Università di Bari o possono essere richiesti alla segreteria studenti. La domanda per il conseguimento del titolo deve 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, deve essere consegnata alla segreteria didattica almeno 3 mesi prima della seduta di laurea. Tale modulistica è disponibile sul sito web del Dipartimento.



▶ QUADRO B1

Descrizione del percorso di formazione (Regolamento Didattico del Corso)

Pdf inserito: [visualizza](#)

Descrizione Pdf: Regolamento Didattico e Manifesto 2021-2022

▶ QUADRO B2.a

Calendario del Corso di Studio e orario delle attività formative

<http://www.uniba.it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica>

▶ QUADRO B2.b

Calendario degli esami di profitto

http://www.studenti.ict.uniba.it/esse3/ListaAppelliOfferta.do?jsessionid=7545E923F27D0836EACA4683C1EC9845.jvm2b?menu_opened_cod=navbox_didattica_Esami

▶ QUADRO B2.c

Calendario sessioni della Prova finale

<http://www.uniba.it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica>

▶ QUADRO B3

Docenti titolari di insegnamento

Sono garantiti i collegamenti informatici alle pagine del portale di ateneo dedicate a queste informazioni.

N.	Settori	Anno di corso	Insegnamento	Cognome Nome	Ruolo	Crediti	Ore	Docente di riferimento per corso
1.	ING-INF/05	Anno di corso 1	ANALISI DEI DATI PER LA SICUREZZA link	APPICE ANNALISA	PA	6	47	
2.	SECS-S/01	Anno di corso 1	ANALISI E GESTIONE DEL RISCHIO link			6	48	
3.	INF/01	Anno di corso 1	CRITTOGRAFIA link	CARUSO COSTANTINA		6	62	
4.	L-LIN/12	Anno di corso 1	LINGUA INGLESE link	BAGNARDI ANTONIETTA		3	24	
5.	SECS-P/10	Anno di corso 1	ORGANIZZAZIONE AZIENDALE link	BARLETTA VITA SANTA		6	48	

6.	ING-INF/05	Anno di corso 1	SICUREZZA NELLE APPLICAZIONI link	MALERBA DONATO	PO	9	48	
7.	ING-INF/05	Anno di corso 1	SICUREZZA NELLE APPLICAZIONI link	MIGNONE PAOLO	RD	9	15	
8.	INF/01	Anno di corso 1	SICUREZZA NELLE RETI E NEI SISTEMI DISTRIBUITI link			6	47	
9.	ING-INF/05	Anno di corso 1	SISTEMI BIOMETRICI link	IMPEDOVO DONATO	PA	9	93	
10.	IUS/04	Anno di corso 1	TRATTAMENTO DEI DATI SENSIBILI link			9	72	
11.	INF/01	Anno di corso 2	METODI FORMALI PER LA SICUREZZA link			6		
12.	PROFIN_S	Anno di corso 2	PROVA FINALE link			10		
13.	ING-INF/05	Anno di corso 2	SICUREZZA DELLE ARCHITETTURE ORIENTATE AI SERVIZI link			6		
14.	INF/01	Anno di corso 2	SICUREZZA IN AMBIENTI MOBILE link			6		
15.	NN	Anno di corso 2	TIROCINIO, STAGE link			20		

▶ QUADRO B4 | Aule

Pdf inserito: [visualizza](#)

Descrizione Pdf: Aule CdS in Sicurezza Informatica

▶ QUADRO B4 | Laboratori e Aule Informatiche

Pdf inserito: [visualizza](#)

Descrizione Pdf: Laboratori e Aule Informatiche Sede di Taranto

▶ QUADRO B4 | Sale Studio

Pdf inserito: [visualizza](#)

Descrizione Pdf: Sale studio sede di Taranto

▶ QUADRO B4 | Biblioteche

Pdf inserito: [visualizza](#)

Descrizione Pdf: Biblioteca sede di Taranto

▶ QUADRO B5

Orientamento in ingresso

16/04/2021

ORIENTAMENTO IN INGRESSO

Responsabile: Prof.ssa Claudia d'Amato

Supporto amministrativo: Ida Mastroviti

Le iniziative organizzate dal Dipartimento in coordinamento con il CAOT e riservate all'orientamento in ingresso per le lauree magistrali, sono le seguenti:

- Attività di sportello di orientamento per studenti presso il Dipartimento di Informatica; aula virtuale su piattaforma Microsoft Teams <https://teams.microsoft.com/join/19%3a9c936682f8b94be491e77cc56eccccea%40thread.tacv2/1590400545270?context=%7b%22id%22%3a%22c6328dc3-afdf-40ce-846d-326eead86d49%22%2c%22oid%22%3a%224c550362-9366-46de-b424-c7d7bb550c50%22%7d>. Il servizio si svolge ogni mercoledì dalle 10:30 alle 12:00.
 - Giornate di Orientamento Live di Ateneo 'UniBa è Magistrale': si sono svolte il 22 e 23 Luglio le due sessioni di orientamento per le lauree magistrali erogate da UniBa. Le attività sono state articolate in Macroaree. Per la macroarea di Scienze di cui il Dipartimento è parte, è stato registrato un picco di partecipazione di 48 studenti in prossimità della presentazione dei corsi di Laurea magistrale del Dipartimento di Informatica il 22 Luglio e circa 14 studenti il 23 Luglio. L'evento è stato registrato. Le registrazioni sono disponibili sul sito Web del Dipartimento (sezione Orientamento) al link <https://www.uniba.it/ricerca/dipartimenti/informatica/notizie-eventi/eventi/uniba-e-magistrale>
 - Organizzazione periodica di seminari in cui i docenti presentano i loro corsi e come questi si inquadrano nel percorso di studi.
 - Incontri con le aziende del settore durante i quali i dirigenti illustrano in modo dettagliato le prospettive di carriera offerte ad un laureato magistrale rispetto ad un laureato triennale.
- Gli eventi vengono pubblicizzati sul sito web del DIB sia nella sezione delle Notizie che nell'apposita pagina dedicata all'Orientamento e Tutorato.

Link inserito: <https://www.uniba.it/ricerca/dipartimenti/informatica/tutorato/orientamento-e-tutorato-1>

▶ QUADRO B5

Orientamento e tutorato in itinere

16/04/2021

Tutti gli iscritti ai corsi di laurea afferenti al Dipartimento di Informatica, partecipando agli incontri con le aziende organizzati dal Consiglio di Interclasse, hanno la possibilità di acquisire costantemente informazioni dirette sul settore di riferimento, sull'organizzazione delle diverse aziende, sui profili professionali maggiormente richiesti e sulle modalità di recruiting.

Le figure dei tutor docenti assegnati al CdS garantiscono un supporto costante allo studente durante la carriera.

▶ QUADRO B5

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

16/04/2021

Responsabile Tirocini e Stage: Prof.ssa Annalisa APPICE

Supporto amministrativo: Ida Mastroviti

Il consiglio di interclasse promuove l'attività svolta dal Job Placement del Dipartimento di Informatica e finalizzata alla stipula di convenzioni tra

il Dipartimento di Informatica e le Aziende, dislocate sul territorio regionale e nazionale, che operano nel settore ICT.

I referenti di tali aziende sono invitati a delineare, in concomitanza con docenti del consiglio di interclasse, progetti formativi di valenza industriale, che possano essere portati avanti dagli studenti dei corsi di laurea in Informatica durante stage/tirocini. Questi progetti formativi, realizzati presso le sedi aziendali, oltre a essere oggetto della prova finale del percorso di studi, sono finalizzati all'inserimento rapido nel mondo del lavoro dei tirocinanti. I progetti formativi spesso sono anche utilizzati, durante la ricerca di lavoro, dai neo-laureati come testimonianze di esperienze acquisite e sono molto apprezzati dalle imprese.

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. Scopo del portale è principalmente quello di rendere maggiormente fruibile l'accesso alle informazioni sulle offerte di lavoro o semplicemente sulla possibilità di accedere a tirocini di varia natura fornendo un'ampia rosa di scelta agli studenti o ai neo laureati riguardo alle aziende disponibili. Tutte le informazioni sono reperibili sul sito del Dipartimento di Informatica nella sezione 'Tirocini'.

Link inserito: <http://www.uniba.it/ricerca/dipartimenti/informatica/didattica/tirocini/tirocini-informatica>



QUADRO B5

Assistenza e accordi per la mobilità internazionale degli studenti

i

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

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

I corsi di studio che rilasciano un titolo doppio o multiplo con un Ateneo straniero risultano essere internazionali ai sensi del DM 1059/13.

Responsabile: Prof.ssa Berardina De Carolis

Supporto amministrativo: Dott.ssa Marianna Calò - Procedura Accordi

Dott.ssa Marcella Cives - Procedura Learning Agreements

Erasmus+ è il programma dell'Unione europea per l'Istruzione, la Formazione, la Gioventù e lo Sport 2014-2020.

Il programma, approvato con il Regolamento UE N 1288/2013 del Parlamento europeo e del Consiglio, combina e integra tutti i meccanismi di finanziamento attuati dall'Unione Europea fino al 2013:

- il Programma di apprendimento permanente (Comenius, Erasmus, Leonardo da Vinci, Grundtvig)
- Gioventù in azione
- i cinque programmi di cooperazione internazionale (Erasmus Mundus, Tempus, Alfa, Edulink e il programma di cooperazione bilaterale con i paesi industrializzati). Comprende inoltre le Attività Jean Monnet e include per la prima volta un sostegno allo Sport.

Il programma integrato permette di ottenere una visione d'insieme delle opportunità di sovvenzione disponibili, mira a facilitare l'accesso e promuove sinergie tra i diversi settori rimuovendo le barriere tra le varie tipologie di progetti. Vuole inoltre attrarre nuovi attori dal mondo del lavoro e dalla società civile e stimolare nuove forme di cooperazione.

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.

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

Per quanto riguarda l'aspetto economico, oltre alla borsa Erasmus e al rimborso del biglietto aereo, ogni anno l'Ateneo distribuisce fondi in maniera equa fra gli studenti che hanno preso parte al programma.

Di notevole rilievo per la formazione internazionale degli studenti è anche il Progetto Global Thesis (DM 29.12.2014 n. 976) che consente agli

studenti della magistrale o del ciclo unico di ricevere una borsa di studio per svolgere l'attività di tesi all'estero.

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).

Un'ulteriore offerta di internazionalizzazione è rappresentata dal 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).

Descrizione link: Informazioni per la mobilità

Link inserito: <https://www.uniba.it/internazionale>

n.	Nazione	Ateneo in convenzione	Codice EACEA	Data convenzione	Titolo
1	Austria	JOHANNES KEPLER UNIVERSITAET LINZ		23/03/2016	solo italiano
2	Cipro	Cyprus University of Technology		26/10/2016	solo italiano
3	Finlandia	University of Oulu - Oulun Yliopisto		17/04/2014	solo italiano
4	Germania	Universitaet Hamburg		15/02/2018	solo italiano
5	Germania	Universitat Ausburg		25/03/2014	solo italiano
6	Grecia	PANEPISTIMIO PATRON		12/05/2015	solo italiano
7	Lettonia	Latvia University of Life Science and Technologies		15/11/2018	solo italiano
8	Paesi Bassi	Technische Universiteit Eindhoven		10/12/2015	solo italiano
9	Polonia	University of Lodz		24/10/2017	solo italiano
10	Romania	Univeritatea din Bucuresti		06/03/2014	solo italiano
11	Spagna	Universidad de Castilla-La-Mancha Ciudad Real		28/11/2014	solo italiano
12	Spagna	Universidade da Coruna		27/11/2017	solo italiano

▶ QUADRO B5

Accompagnamento al lavoro

16/04/2021

L'Università degli Studi di Bari aderisce alle disposizioni ministeriali relative a 'Collegato al lavoro' tramite il portale di Ateneo. Selezionando la voce 'Placement', l'Università consente l'incontro fra domanda, offerta ed istituzione, rendendo fruibili i servizi offerti dalla Agenzia del Placement.

Il consiglio di interclasse organizza, in collaborazione con il Job Placement di Dipartimento e con il Job Placement di Ateneo, incontri periodici degli studenti con le aziende al fine di agevolare l'inserimento dei laureati nel mondo del lavoro, nell'anno 2020 questo non è stato possibile per il periodo prolungato di quarantena sociale dovuta al COVID-19.

Dopo un primo periodo di stasi dovuto al blocco di ogni attività in presenza, si è riusciti ad organizzare con alcune aziende momenti seminariali, di giochi virtuali e conoscitivi su piattaforma, soprattutto rivolti agli studenti del terzo anno delle triennali e delle magistrali.

Tali eventi si sono tenuti con le aziende:

- Bip (Cyber turbo Game su piattaforma zoom): challenge per gli studenti appassionati alla cyber security tenutosi l'8 luglio 2020
- Ariston (Programma ICT e career su piattaforma Teams) iniziativa di recruiting organizzata in un primo momento seminariale di presentazione dell'azienda ed un secondo momento di colloqui 'one to one' online tra studenti e l'HR dell'area ICT dell'azienda; 8 settembre 2020
- Dxc (Simulazione di assessment su piattaforma Teams) per gli studenti del secondo e terzo anno delle triennali e delle magistrali, 5 novembre 2020
- Accenture (webinar online per conoscere le aree di innovazione e le competenze professionali correlate) per gli studenti del secondo e terzo anno delle triennali e delle magistrali, dall'11 marzo al 27 aprile 2021
- Auriga (Virtual assessment su Teams) per gli studenti del secondo e terzo anno delle triennali e delle magistrali, 19 marzo 2021

È stato organizzato un ciclo di laboratori per l'acquisizione di competenze trasversali in collaborazione con l'Agenzia per il Placement finalizzato alla progettazione e costruzione del futuro professionale degli studenti delle triennali e delle magistrali. L'attività ha visto l'erogazione di 5 seminari su piattaforma Teams dal 1 al 9 luglio con esercitazioni pratiche.

Descrizione link: Placement di Ateneo - Agenzia per il Placement

Link inserito: <http://www.uniba.it/studenti/orientamento/lavoro>

▶ QUADRO B5

Eventuali altre iniziative

Sul sito del Dipartimento è presente una Sezione Job Placement che viene continuamente aggiornata con pubblicazioni di offerte di lavoro e stage che pervengono dalle aziende. 16/04/2021

A partire dal Mese di marzo 2020 lo Sportello dedicato al Job Placement che garantisce a tutti gli studenti dei corsi di studio in Informatica assistenza e consulenza personalizzate è stato portato avanti con consulenze via email e telefoniche e da ottobre 2020 anche su Teams ogni mercoledì.

Descrizione link: Job Placement di Dipartimento

Link inserito: <http://www.uniba.it/ricerca/dipartimenti/informatica/job-placement>

▶ QUADRO B6

Opinioni studenti

12/04/2021

Descrizione link: Opinione studenti 2019/20

Link inserito: <http://reportanvur.ict.uniba.it:443/birt/run?>

[_report=Anvur_2019_CorsoBackup_rptdesign&_format=html&RP_Fac_id=1012&RP_Cds_id=10594&_locale=it_IT&_svg=true&_designer=fa](http://reportanvur.ict.uniba.it:443/birt/run?_report=Anvur_2019_CorsoBackup_rptdesign&_format=html&RP_Fac_id=1012&RP_Cds_id=10594&_locale=it_IT&_svg=true&_designer=fa)

▶ QUADRO B7

Opinioni dei laureati

13/09/2021

Giudizio dei laureati sul percorso di studi

Link inserito: <http://>

Pdf inserito: [visualizza](#)



▶ QUADRO C1

Dati di ingresso, di percorso e di uscita

Scheda di Monitoraggio Annuale

13/09/2021

Link inserito: <http://>

Pdf inserito: [visualizza](#)

▶ QUADRO C2

Efficacia Esterna

Dati sull'occupazione relativi alla prima coorte di laureati

13/09/2021

Link inserito: <http://>

Pdf inserito: [visualizza](#)

▶ QUADRO C3

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

Gli studenti dei CdS in Informatica triennali e magistrali possono svolgere i loro tirocini curricolari presso aziende esterne all'Università e questo offre loro l'opportunità di vivere un primo approccio con il mondo del lavoro e comprendere l'interazione dipendente/datore di lavoro.

Ad oggi, nell'anno 2021, sono state coinvolte 29 aziende per lo svolgimento di 39 tirocini esterni e tutte hanno compilato la relazione/questionario finale.

Il questionario presenta una sezione libera, riguardante la descrizione delle attività di tirocinio espletate dallo studente e una sezione con domande specifiche riferite alla preparazione ed il coinvolgimento del tirocinante, all'interazione con l'ufficio che gestisce i tirocini e all'esperienza complessiva del tirocinio in azienda.

La documentazione viene poi analizzata al fine di comprendere meglio quanto gli studi in Informatica siano rispondenti alle richieste del mercato del lavoro.

In particolare, dal monitoraggio effettuato, risulta che gli studenti hanno una preparazione medio/alta, le aziende sono pienamente soddisfatte dell'esperienza nel suo complesso, ma esprimono qualche perplessità circa la durata dei tirocini.

Inoltre, è da rilevare che numerosi studenti che hanno espletato tirocini aziendali hanno poi sottoscritto un contratto con le stesse aziende alla fine del percorso di studi.

Non abbiamo evidenze riguardanti i punti di forza, né suggerimenti da parte delle aziende coinvolte, ma intendiamo modificare i nostri questionari in modo da poter reperire anche queste informazioni.

13/09/2021

Link inserito: <https://www.uniba.it/ricerca/dipartimenti/informatica/didattica/tirocini/tirocini-informatica>

Pdf inserito: [visualizza](#)



▶ QUADRO D1

Struttura organizzativa e responsabilità a livello di Ateneo

09/04/2021

Il Sistema di Assicurazione della Qualità (SAQ) dell'Università degli Studi di Bari Aldo Moro (UNIBA) descrive le modalità attraverso cui gli organi di governo e tutti gli attori dell'Assicurazione della Qualità (AQ) interagiscono fra loro per la realizzazione delle politiche, degli obiettivi e delle procedure di AQ. Il coordinamento e la verifica dell'attuazione del processo di AQ dei Corsi di Studio sono in capo al Presidio della Qualità di Ateneo (PQA), organo statutario di UNIBA (art. 14 dello Statuto, emanato con D.R. n. 423 del 04.02.2019). Ad esso sono attribuite le funzioni relative alle procedure di AQ, per promuovere e migliorare la qualità della didattica, ricerca e terza missione, nonché le altre funzioni attribuite dalla Legge, dallo Statuto e dai Regolamenti in vigore in UNIBA. Le modalità di funzionamento del PQA sono disciplinate da apposito Regolamento. Nello svolgimento dei suoi compiti, il PQA gode di piena autonomia operativa e riferisce periodicamente agli Organi di governo sullo stato delle azioni relative all'AQ. Il processo di AQ è trasparente e condiviso con tutta la comunità attraverso apposite pagine web, gestite dallo stesso PQA (link <https://www.uniba.it/ateneo/presidio-qualita>).

Descrizione link: Documentazione AQ

Link inserito: <https://www.uniba.it/ateneo/presidio-qualita/pqa/documentazione-ufficiale>

Pdf inserito: [visualizza](#)

Descrizione Pdf: Struttura organizzativa e responsabilità a livello di Ateneo

▶ QUADRO D2

Organizzazione e responsabilità della AQ a livello del Corso di Studio

13/05/2021

Il CdS ha provveduto a nominare il Gruppo di AQ costituito dal Coordinatore del CdS, dal referente del CdS e dalla rappresentanza studentesca.

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 in Sicurezza Informatica.

Il Team di AQ è costituito da:

Prof. Giovanni Dimauro (Coordinatore dell'Interclasse)

Dr.ssa Veronica Rossano (Docente Responsabile Assicurazione della Qualità del CdS)

Prof. Donato Impedovo (Docente Referente del CdS)

Dr.ssa Marcella Cives (Tecnico amministrativo con funzione Manager didattico)

Sig.ra Federica Nitti (Studente)

▶ QUADRO D3

Programmazione dei lavori e scadenze di attuazione delle iniziative

12/05/2021

La commissione di AQ esaminerà:

- le statistiche sull'andamento degli studi;
- i risultati dei questionari, compilati dagli studenti, sulla qualità dei corsi;
- la laureabilità in Sicurezza Informatica.

Il team di assicurazione di qualità avrà il compito di effettuare rilevazioni qualitative e quantitative. Le misurazioni si effettueranno a metà ed alla fine di ogni semestre. Nelle rilevazioni a metà semestre si potranno valutare le frequenze dei corsi, in quello di fine semestre si potrà valutare la numerosità degli esami superati dagli studenti. Sulla base dei dati rilevati il team di AQ proporrà delle iniziative di miglioramento. Queste saranno presentate al CdS che le discuterà, le emenderà, eventualmente, e le approverà. Dopo l'approvazione, tutti i docenti interessati contribuiranno alla realizzazione delle iniziative.

I risultati di questi audit costituiranno le informazioni del processo di riesame.

▶ QUADRO D4

Riesame annuale

▶ QUADRO D5

Progettazione del CdS

08/03/2017

Descrizione link: Progettazione CdS Sicurezza Informatica

Pdf inserito: [visualizza](#)

▶ QUADRO D6

Eventuali altri documenti ritenuti utili per motivare l'attivazione del Corso di Studio



Informazioni generali sul Corso di Studi

Università	Università degli Studi di BARI ALDO MORO
Nome del corso in italiano	Sicurezza Informatica
Nome del corso in inglese	Cyber Security
Classe	LM-66 - Sicurezza informatica
Lingua in cui si tiene il corso	italiano
Eventuale indirizzo internet del corso di laurea	https://www.uniba.it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica
Tasse	Pdf inserito: visualizza
Modalità di svolgimento	b. Corso di studio in modalità mista



Corsi interateneo R²D



Questo campo dev'essere compilato solo per corsi di studi interateneo,

Un corso si dice "interateneo" quando gli Atenei partecipanti stipulano una convenzione finalizzata a disciplinare direttamente gli obiettivi e le attività formative di un unico corso di studi, che viene attivato congiuntamente dagli Atenei coinvolti, con uno degli Atenei che (anche a turno) segue la gestione amministrativa del corso. Gli Atenei coinvolti si accordano altresì sulla parte degli insegnamenti che viene attivata da ciascuno; deve essere previsto il rilascio a tutti gli studenti iscritti di un titolo di studio congiunto, doppio o multiplo.

Non sono presenti atenei in convenzione



Referenti e Strutture



Presidente (o Referente o Coordinatore) del CdS	DIMAURO Giovanni
Organo Collegiale di gestione del corso di studio	CICSI - Consiglio di Interclasse dei Corsi di Studio in Informatica
Struttura didattica di riferimento	Informatica



Docenti di Riferimento

N.	COGNOME	NOME	SETTORE	QUALIFICA	PESO	TIPO SSD	Incarico didattico
1.	DESOLDA	Giuseppe	INF/01	RD	1	Caratterizzante	1. SICUREZZA IN AMBIENTI MOBILE
2.	IMPEDOVO	Donato	ING- INF/05	PA	1	Caratterizzante	1. SISTEMI BIOMETRICI
3.	LISI	Francesca Alessandra	INF/01	PA	1	Caratterizzante	1. METODI FORMALI PER LA SICUREZZA
4.	MIGNONE	Paolo	ING- INF/05	RD	1	Caratterizzante	1. SICUREZZA NELLE APPLICAZIONI
5.	PIRLO	Giuseppe	ING- INF/05	PO	1	Caratterizzante	1. SICUREZZA DELLE ARCHITETTURE ORIENTATE AI SERVIZI
6.	BUONO	Paolo	INF/01	PA	1	Caratterizzante	1. SICUREZZA IN AMBIENTI MOBILE

✓ requisito di docenza (numero e tipologia) verificato con successo!

✓ requisito di docenza (incarico didattico) verificato con successo!



Rappresentanti Studenti

COGNOME	NOME	EMAIL	TELEFONO
Petruzzellis	Flavio	f.petruzzellis6@studenti.uniba.it	
Villano	Giorgia	g.villano@studenti.uniba.it	
Dimaggio	Michele	m.dimaggio18@studenti.uniba.it	
Abbinante	Alessandro	a.abbinante14@studenti.uniba.it	
Parisi	Matteo	m.parisi39@studenti.uniba.it	
Zizza	Vincenzo	v.zizza2@studenti.uniba.it	
Ianne	Alessandro	a.ianne3@studenti.uniba.it	
Ungaro	Marco	m.ungaro15@studenti.uniba.it	
De Palma	Antonio	a.depalma54@studenti.uniba.it	
Manfredi	Walter	w.manfredi@studenti.uniba.it	
Luceri	Matteo	m.luceri3@studenti.uniba.it	
Calore	Giammarco	g.calore2@studenti.uniba.it	
Caputo	Francesco	f.caputo45@studenti.uniba.it	
Pizzolla	Anna	a.pizzolla3@studenti.uniba.it	



Gruppo di gestione AQ

COGNOME	NOME
CIVES	MARCELLA
DIMAURO	GIOVANNI
IMPEDOVO	DONATO
NITTI	FEDERICA
ROSSANO	VERONICA



Tutor

COGNOME	NOME	EMAIL	TIPO
IMPEDOVO	Donato		
APPICE	Annalisa		
BUONO	Paolo		
ALTAMURA	Venere		

▶ Programmazione degli accessi 

Programmazione nazionale (art.1 Legge 264/1999)	No
Programmazione locale (art.2 Legge 264/1999)	No

▶ Sedi del Corso 

[DM 6/2019](#) Allegato A - requisiti di docenza

Sede del corso: - TARANTO	
Data di inizio dell'attività didattica	27/09/2021
Studenti previsti	65

▶ Eventuali Curriculum 

Non sono previsti curricula



Altre Informazioni



Codice interno all'ateneo del corso	8972^2019^PDS0-2019^2174
Massimo numero di crediti riconoscibili	12 DM 16/3/2007 Art 4 Nota 1063 del 29/04/2011



Date delibere di riferimento



Data di approvazione della struttura didattica	21/09/2018
Data di approvazione del senato accademico/consiglio di amministrazione	06/03/2019
Data della consultazione con le organizzazioni rappresentative a livello locale della produzione, servizi, professioni	24/11/2016
Data del parere favorevole del Comitato regionale di Coordinamento	30/01/2017



Sintesi della relazione tecnica del nucleo di valutazione

Il Nucleo di Valutazione nella riunione del 16 gennaio 2017, valutati i requisiti richiesti, esprime parere favorevole alla proposta di nuova istituzione del Corso di laurea magistrale "SICUREZZA INFORMATICA" – classe LM-66. Si allega la Relazione tecnico-illustrativa ai sensi dell'art. 8 comma 4 del Decreto Legislativo 27 gennaio 2012, n. 19.

Pdf inserito: [visualizza](#)

Descrizione Pdf: Relazione NdV su proposta di nuova istituzione del Corso di laurea magistrale Sicurezza Informatica



Relazione Nucleo di Valutazione per accreditamento



La relazione completa del NdV necessaria per la procedura di accreditamento dei corsi di studio deve essere inserita nell'apposito spazio all'interno della scheda SUA-CdS denominato "Relazione Nucleo di Valutazione per accreditamento" entro la scadenza del 15 febbraio 2021 **SOLO per i corsi di nuova istituzione**. La relazione del Nucleo può essere redatta seguendo i criteri valutativi, di seguito riepilogati, dettagliati nelle linee guida ANVUR per l'accREDITAMENTO iniziale dei Corsi di Studio di nuova attivazione, consultabili sul sito dell'ANVUR

Linee guida ANVUR

1. Motivazioni per la progettazione/attivazione del CdS
2. Analisi della domanda di formazione
3. Analisi dei profili di competenza e dei risultati di apprendimento attesi
4. L'esperienza dello studente (Analisi delle modalità che verranno adottate per garantire che l'andamento delle attività formative e dei risultati del CdS sia coerente con gli obiettivi e sia gestito correttamente rispetto a criteri di qualità con un forte impegno alla collegialità da parte del corpo docente)
5. Risorse previste
6. Assicurazione della Qualità

La Relazione tecnico-illustrativa sulle proposte di nuova istituzione dei Corsi di Studio per l'a.a. 2017/18 approvata dal Nucleo di Valutazione nella riunione del 16.01.2017 ed allegata nel campo (Sintesi della relazione tecnica del nucleo di valutazione) esamina i requisiti previsti dalla normativa. Tale relazione esprime il parere favorevole del Nucleo di Valutazione all'istituzione dei nuovi Corsi di Studio.



Sintesi del parere del comitato regionale di coordinamento

R^{AD}

Pdf inserito: [visualizza](#)

Descrizione Pdf: SINTESI PARERE CURC

Offerta didattica erogata

	coorte	CUIN	insegnamento	settori insegnamento	docente	settore docente	ore di didattica assistita
1	2021	022113202	ANALISI DEI DATI PER LA SICUREZZA <i>semestrale</i>	ING-INF/05	Annalisa APPICE <i>Professore Associato (L. 240/10)</i>	ING-INF/05	47
2	2021	022113203	ANALISI E GESTIONE DEL RISCHIO <i>semestrale</i>	SECS-S/01	Docente non specificato		48
3	2021	022113204	CRITTOGRAFIA <i>semestrale</i>	INF/01	Costantina CARUSO		62
4	2021	022113205	LINGUA INGLESE <i>semestrale</i>	L-LIN/12	Antonietta BAGNARDI		24
5	2020	022110567	METODI FORMALI PER LA SICUREZZA <i>semestrale</i>	INF/01	Docente di riferimento Francesca Alessandra LISI <i>Professore Associato (L. 240/10)</i>	INF/01	47
6	2021	022113206	ORGANIZZAZIONE AZIENDALE <i>semestrale</i>	SECS-P/10	Vita Santa BARLETTA		48
7	2020	022110569	SICUREZZA DELLE ARCHITETTURE ORIENTATE AI SERVIZI <i>semestrale</i>	ING-INF/05	Docente di riferimento Giuseppe PIRLO <i>Professore Ordinario (L. 240/10)</i>	ING-INF/05	47
8	2020	022110570	SICUREZZA IN AMBIENTI MOBILE <i>semestrale</i>	INF/01	Docente di riferimento Paolo BUONO <i>Professore Associato (L. 240/10)</i>	INF/01	39
9	2020	022110570	SICUREZZA IN AMBIENTI MOBILE <i>semestrale</i>	INF/01	Docente di riferimento Giuseppe DESOLDA <i>Ricercatore a t.d. - t.pieno (art. 24 c.3- a L. 240/10)</i>	INF/01	8
10	2021	022113207	SICUREZZA NELLE APPLICAZIONI <i>semestrale</i>	ING-INF/05	Docente di riferimento Paolo MIGNONE <i>Ricercatore a t.d. - t.pieno (art. 24 c.3- a L. 240/10)</i>	ING-INF/05	15
11	2021	022113207	SICUREZZA NELLE APPLICAZIONI <i>semestrale</i>	ING-INF/05	Donato MALERBA <i>Professore Ordinario</i>	ING-INF/05	48
12	2021	022113208	SICUREZZA NELLE RETI E	INF/01	Docente non specificato		47

NEI SISTEMI DISTRIBUITI
semestrale

specificato

13	2021	022113209	SISTEMI BIOMETRICI <i>semestrale</i>	ING-INF/05	Docente di riferimento Donato IMPEDOVO <i>Professore Associato (L. 240/10)</i>	ING-INF/05	93
14	2021	022113210	TRATTAMENTO DEI DATI SENSIBILI <i>semestrale</i>	IUS/04	Docente non specificato		72
						ore totali	645



Offerta didattica programmata

Attività caratterizzanti	settore	CFU Ins	CFU Off	CFU Rad
Ambito Scientifico	INF/01 Informatica	24	24	24 - 24
	↳ SICUREZZA NELLE RETI E NEI SISTEMI DISTRIBUITI (1 anno) - 6 CFU - semestrale - obbl			
	↳ METODI FORMALI PER LA SICUREZZA (2 anno) - 6 CFU - semestrale - obbl			
	ING-INF/05 Sistemi di elaborazione delle informazioni			
	↳ ANALISI DEI DATI PER LA SICUREZZA (1 anno) - 6 CFU - semestrale - obbl			
	↳ SICUREZZA DELLE ARCHITETTURE ORIENTATE AI SERVIZI (2 anno) - 6 CFU - semestrale - obbl			
Ambito Tecnologico	ING-INF/05 Sistemi di elaborazione delle informazioni	18	18	18 - 18
	↳ SICUREZZA NELLE APPLICAZIONI (1 anno) - 9 CFU - semestrale - obbl			
	↳ SISTEMI BIOMETRICI (1 anno) - 9 CFU - semestrale - obbl			
Ambito Giuridico, Sociale ed Economico	IUS/04 Diritto commerciale	21	21	12 - 21
	↳ TRATTAMENTO DEI DATI SENSIBILI (1 anno) - 9 CFU - semestrale - obbl			
	SECS-P/10 Organizzazione aziendale			
	↳ ORGANIZZAZIONE AZIENDALE (1 anno) - 6 CFU - semestrale - obbl			
	SECS-S/01 Statistica			
↳ ANALISI E GESTIONE DEL RISCHIO (1 anno) - 6 CFU - semestrale - obbl				
Minimo di crediti riservati dall'ateneo: - (minimo da D.M. 48)				
Totale attività caratterizzanti			63	54 - 63

Attività affini	settore	CFU Ins	CFU Off	CFU Rad
Attività formative affini o integrative	INF/01 Informatica	12	12	12 - 21 min 12
	↳ CRITTOGRAFIA (1 anno) - 6 CFU - semestrale - obbl			
	↳ SICUREZZA IN AMBIENTI MOBILE (2 anno) - 6 CFU - semestrale - obbl			
Totale attività Affini			12	12 - 21

Altre attività		CFU	CFU Rad
A scelta dello studente		12	12 - 12
Per la prova finale		10	10 - 10
Ulteriori attività formative (art. 10, comma 5, lettera d)	Ulteriori conoscenze linguistiche	3	3 - 3
	Abilità informatiche e telematiche	-	-
	Tirocini formativi e di orientamento	20	20 - 20
	Altre conoscenze utili per l'inserimento nel mondo del lavoro	-	-
Minimo di crediti riservati dall'ateneo alle Attività art. 10, comma 5 lett. d			
Per stages e tirocini presso imprese, enti pubblici o privati, ordini professionali		-	-
Totale Altre Attività		45	45 - 45

CFU totali per il conseguimento del titolo

120

CFU totali inseriti

120

111 - 129



Raggruppamento settori

per modificare il raggruppamento dei settori



Attività caratterizzanti R²D

ambito disciplinare	settore	CFU		minimo da D.M. per l'ambito
		min	max	
Ambito Scientifico	INF/01 Informatica ING-INF/05 Sistemi di elaborazione delle informazioni MAT/06 Probabilità e statistica matematica	24	24	18
Ambito Tecnologico	INF/01 Informatica ING-INF/03 Telecomunicazioni ING-INF/05 Sistemi di elaborazione delle informazioni	18	18	18
Ambito Giuridico, Sociale ed Economico	IUS/01 Diritto privato IUS/04 Diritto commerciale IUS/10 Diritto amministrativo IUS/13 Diritto internazionale IUS/14 Diritto dell'unione europea SECS-P/10 Organizzazione aziendale SECS-S/01 Statistica	12	21	12
Minimo di crediti riservati dall'ateneo minimo da D.M. 48:		-		
Totale Attività Caratterizzanti				54 - 63



Attività affini

R^{AD}

ambito disciplinare	settore	CFU		minimo da D.M. per l'ambito
		min	max	
Attività formative affini o integrative	INF/01 - Informatica			12
	IUS/17 - Diritto penale	12	21	
	MAT/08 - Analisi numerica			
Totale Attività Affini				12 - 21



Altre attività

R^{AD}

ambito disciplinare		CFU min	CFU max
A scelta dello studente		12	12
Per la prova finale		10	10
Ulteriori attività formative (art. 10, comma 5, lettera d)	Ulteriori conoscenze linguistiche	3	3
	Abilità informatiche e telematiche	-	-
	Tirocini formativi e di orientamento	20	20
	Altre conoscenze utili per l'inserimento nel mondo del lavoro	-	-
Minimo di crediti riservati dall'ateneo alle Attività art. 10, comma 5 lett. d			
Per stages e tirocini presso imprese, enti pubblici o privati, ordini professionali		-	-
Totale Altre Attività		45 - 45	



Riepilogo CFU

R^aD

CFU totali per il conseguimento del titolo	120
Range CFU totali del corso	111 - 129



Comunicazioni dell'ateneo al CUN

R^aD



Motivi dell'istituzione di più corsi nella classe

R^aD



Note relative alle attività di base

R^aD



Note relative alle altre attività

R^aD



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

R^aD

(Settori della classe inseriti nelle attività affini e anche/già inseriti in ambiti di base o caratterizzanti : INF/01)

L'inserimento del settore INF/01, già presente nelle attività caratterizzanti di questo corso di studi, è dovuto al necessario approfondimento richiesto dalla vastità del settore in questione.



Note relative alle attività caratterizzanti
R^{ad}