



UNIVERSITÀ DEGLI STUDI
DI SALERNO

Area III – Didattica e Ricerca

UOR: Ufficio Formazione Post Laurea

IL RETTORE

- VISTI** gli artt. 17 e 39 dello Statuto dell'Università degli Studi di Salerno;
- VISTO** il D.M. 22 ottobre 2004, n° 270, contenente modifiche al regolamento recante norme concernenti l'autonomia didattica degli atenei approvato con D.M. 3 novembre 1999, n° 509;
- VISTO** l'art. 38, comma 1, della Legge Regionale 3 settembre 2002, n° 21, pubblicato nel Bollettino Ufficiale della Regione Campania del 21 dicembre 2002, n° 42, con il quale la Tassa Regionale per il Diritto allo Studio Universitario è stata riconosciuta come tributo proprio della Regione Campania, e ne è stato determinato l'importo;
- VISTO** l'art. 18, comma 8, del D. Lgs. 29 marzo 2012, n° 68, pubblicato nella Gazzetta Ufficiale della Repubblica Italiana del 31 maggio 2012, n° 126, con il quale è stato disposto che le Regioni e le Province Autonome rideterminino l'importo della Tassa Regionale per il Diritto allo Studio Universitario articolandolo in tre fasce;
- VISTO** l'art. 1, comma 19–24, della Legge Regionale 7 agosto 2014, n° 16, pubblicato nel Bollettino Ufficiale della Regione Campania del 7 agosto 2014, n° 57, con il quale la Giunta Regionale della Campania ha rideterminato della Tassa Regionale per il Diritto allo Studio Universitario articolandolo in tre fasce;
- VISTO** l'art. 8 del Regolamento Didattico di Ateneo, emanato con D.R. 1° aprile 2008, Rep. n° 1043, Prot. n° 19161, e successive modificazioni ed integrazioni;
- VISTO** il D.R. 25 settembre 2020, Rep. n° 1580, Prot. n° 249901, con il quale è stato emanato il Regolamento di Ateneo per la disciplina dei Corsi di Master;
- VISTA** la deliberazione con la quale il Consiglio di Amministrazione, nella seduta del 22 febbraio 2024, ha approvato l'adesione dell'Ateneo alla manifestazione di interesse finalizzata all'avvio di una partnership con la allora Business School24 S.p.A., oggi Digit'Ed S.p.A., avente ad oggetto la realizzazione e gestione congiunta di una proposta formativa post-laurea e di alta formazione, demandandone al Rettore la formalizzazione;
- RILEVATO** che la collaborazione proposta è volta alla ideazione, progettazione, realizzazione, e commercializzazione di Master Universitari di alta qualificazione su specifiche aree tematiche da definirsi tra le Parti, e che pertanto l'obiettivo della collaborazione consiste nel raggiungere elevati livelli di qualità dell'offerta formativa, avvalendosi anche delle collaudate, avanzatissime tecnologie informatiche, di cui dispone Digit'Ed S.p.A., per la formazione certificata a distanza, nonché della capillare diffusione sul territorio del brand "24ORE Business School";
- ATTESO** che, in esito alla manifestazione di interesse, si è addivenuti alla possibilità della sottoscrizione di uno specifico Accordo Quadro in forza del quale l'Ateneo e Digit'Ed S.p.A. potranno definire l'attivazione di uno o più Master;
- VISTE** le deliberazioni con le quali il Senato Accademico ed il Consiglio di Amministrazione, rispettivamente nelle sedute del 19 novembre 2024 e del 21 novembre 2024, hanno approvato la sottoscrizione del suddetto Accordo Quadro relativo all'ideazione, progettazione, realizzazione, e commercializzazione di Master Universitari;



UNIVERSITÀ DEGLI STUDI DI SALERNO

PRESO ATTO che la proposta di sottoscrizione di Accordo Quadro, formalizzata dall'Ateneo in data 28 gennaio 2025, è stata accettata in data 29 gennaio 2025;

VISTO l'Accordo Quadro 31 gennaio 2025, Rep n° 228, Prot. n° 37450;

CONSIDERATO che, ai sensi dell'articolo 2, comma 2.1, del suddetto Accordo Quadro, le Parti si impegnano fin d'ora a concordare e definire, per ciascun Master che intenderanno attivare in collaborazione, apposita scheda prestazionale contenente le caratteristiche di tali Master e le condizioni e modalità di esecuzione che, sottoscritta da entrambe le Parti, andrà a formare parte integrante dell'Accordo;

ACQUISITA la scheda prestazionale per l'istituzione ed attivazione di un Corso di Master Universitario, di II livello, denominato CYBER INTELLIGENCE & SECURITY come sottoscritta dalle Parti;

ATTESO che, al fine di dare prima attuazione all'Accordo Quadro, completo di relativa scheda prestazionale, si rende necessario procedere all'istituzione ed attivazione del predetto Corso di Master Universitario;

DECRETA

Per le motivazioni descritte in premessa, è disposta l'istituzione, per l'anno accademico 2024/2025, con durata annuale, del Corso di Master Universitario, di II livello, denominato "CYBER INTELLIGENCE & SECURITY", in partnership con Digit'Ed S.p.A., e ne è attivata la I edizione.

E' Direttore del Corso il prof. Vincenzo LOIA, professore ordinario per il settore scientifico-disciplinare INFO-01/A (Informatica) presso il Dipartimento Scienze Aziendali - Management & Innovation Systems/DISA-MIS dell'Ateneo.

E' emanato il bando di concorso per l'ammissione al predetto Corso di Master Universitario, nel testo di seguito indicato:

Art. 1

Disposizioni generali

E' indetto, per l'Anno Accademico 2024/2025, un concorso pubblico, per **titoli ed esame**, a n. **40** posti per l'ammissione alla I edizione del Corso di Master Universitario, di II livello, denominato "CYBER INTELLIGENCE & SECURITY", istituito presso l'Università degli Studi di Salerno in partnership con Digit'Ed S.p.A.

Per l'attivazione del Corso è necessario un numero di iscritti non inferiore a **25**.

E' prevista anche l'iscrizione, fino ad un numero massimo di **4** partecipanti, a singoli moduli didattici del Master nel limite di 24 crediti formativi universitari corrispondenti alla fase d'aula. Al termine della frequenza dei moduli singoli, viene rilasciato un attestato di frequenza a cura del Direttore del Master. Nel caso in cui sia stata effettuata la verifica del profitto, il suddetto certificato indicherà la valutazione conseguita e i crediti formativi maturati

Ai sensi dell'art. 3, comma 9, del D.M. 22 ottobre 2004, n° 270, il Master si configura come Corso di Perfezionamento Scientifico e di Alta Formazione Permanente e Ricorrente, al termine del quale, previo superamento di un esame finale, è rilasciato il diploma di Master Universitario di II livello.

Art. 2

Destinatari dell'azione



UNIVERSITÀ DEGLI STUDI DI SALERNO

Il Corso di Master Universitario, di II livello, denominato “CYBER INTELLIGENCE & SECURITY” è rivolto ai laureati in possesso dei requisiti di cui al successivo articolo 3.

Art. 3

Requisiti generali di ammissione

Possono partecipare al concorso i cittadini italiani e stranieri che, alla scadenza del termine per la presentazione della domanda di partecipazione allo stesso, siano in possesso di una Laurea Magistrale, oppure Laurea Specialistica, oppure Laurea vecchio ordinamento, conseguito in Italia o all'estero purchè riconosciuto idoneo in base alla normativa vigente, preferibilmente in Informatica, Ingegneria, Data Science, Economia, Consulenza e Management Aziendale, Giurisprudenza, Psicologia e altre discipline tecnico/scientifiche.

La Commissione si riserva la facoltà di valutare la possibilità di ammettere ulteriori classi di laurea non esplicitamente menzionate in precedenza.

Possono, inoltre, partecipare al concorso anche coloro i quali conseguiranno il titolo di studio di cui al comma precedente **entro e non oltre il 30 settembre 2025**. In tal caso l'ammissione al concorso verrà disposta “con riserva” e il candidato sarà tenuto a presentare ovvero a spedire, a pena di decadenza, entro e non oltre quindici giorni dalla scadenza del predetto termine, la dichiarazione sostitutiva di certificazione, resa ai sensi dell'art. 46 del D.P.R. 28 dicembre 2000, n° 445, che attesti il conseguimento del diploma di laurea.

Art. 4

Obiettivi formativi, profili professionali e sbocchi occupazionali

Il Corso di Master Universitario, di II livello, denominato “CYBER INTELLIGENCE & SECURITY” ha l'obiettivo di formare i discenti in merito ai temi della Cyber Intelligence & Security e, in maniera particolare, alla loro applicazione per governare e gestire scenari di crisi caratterizzati da rischio, incertezza e volatilità delle informazioni. Sono scenari e casi rappresentativi della attuale situazione internazionale e che, di recente, sono resi più complessi a causa delle evoluzioni di tipo generativo della intelligenza artificiale, come ad esempio il deep fake ed il disordine informativo che possono essere considerati come strategie di guerra cognitiva. A tal fine, i proponenti del Master ritengono utile formare una nuova classe di analisti e decisori che possa combinare una profonda conoscenza verticale delle discipline della Cyber Intelligence & Security con competenze di data science e intelligenza artificiale, e con conoscenze ed abilità (inclusi soft-skills), di tipo orizzontale, che permettano di acquisire maggiore consapevolezza delle situazioni di crisi e del loro governo e gestione.

Il progetto di questo Master si basa dunque su due pilastri fondamentali che si appoggiano ad una Teoria Cognitiva ed una metodologia di formazione che permette lo sviluppo di capacità e soft-skill utili al decision making informato ed alla gestione delle crisi.

I due pilastri fondamentali sono relativi a: 1) metodologie e tecnologie di Data Science, Computational ed Artificial Intelligence, e 2) metodologie, tecnologie ed architetture a supporto di Cyber Intelligence & Security. Il Master, su questi due pilastri, fornirà insegnamenti tali da far acquisire ai discenti una profonda conoscenza dei modelli, metodi e tecnologie allo stato dell'arte ed emergenti e delle attuali sfide e problematiche aperte che caratterizzano l'infrastruttura più complessa finora realizzata dall'uomo: il cyberspazio.

Due elementi orizzontali appaiono utili in questo percorso in aggiunta, ovviamente, all'approfondimento verticale summenzionato. Il primo fa riferimento all'utilizzo della Teoria della Situation Awareness di Mica Endsley. La Situation Awareness fornisce un modello cognitivo ed un approccio metodologico alla progettazione dei sistemi software che permette ad analisti e decisori di acquisire un maggiore consapevolezza di una situazione per poter prendere decisioni informate minimizzando i bias cognitivi che portano ad errori decisionali. Tale teoria, ampiamente usata negli USA, vede ancor'oggi una scarsa applicazione nel nostro paese. Il secondo elemento è relativo all'utilizzo di una metodologia di formazione che permetta lo sviluppo di capacità e soft-skill utili alla gestione delle crisi. Ciò è tipico di percorsi



UNIVERSITÀ DEGLI STUDI DI SALERNO

di formazione di Crisis Management, Response and Simulation che, però, sono tipicamente offerti in maniera stand-alone. La Situation Awareness, inoltre, diventa infine un elemento fondamentale nell'ambito della cybersecurity per fronteggiare con successo la velocità di azione, il polimorfismo e la capacità di coordinamento delle recenti minacce malware, che rendono la gestione tradizionale della sicurezza "statica" e "decontestualizzata" completamente inefficace.

Con questo Master si intende integrare, in maniera pervasiva, questi due elementi nelle attività di formazione sulle tematiche di Data Science, Computational & Artificial Intelligence, Cyber Intelligence & Security al fine di formare professionisti che possono fare leva sui recenti sviluppi tecnologici a supporto dell'intelligence e della sicurezza, inclusi i modelli di intelligenza artificiale generativa, per analizzare, gestire e governare situazioni di crisi o potenziale conflitto che coinvolgano sistemi e/o organizzazioni complesse ed infrastrutture critiche. Tali situazioni presentano numerose istanze che includono: *a)* istanze "tradizionali" come analisi di situazioni aziendali per supportare la readiness ad evoluzioni di mercato (tipico della Business Intelligence), analisi di infrastrutture critiche in ottica di resilienza (tipico della Cyber security) e *b)* istanze "emergenti" come analisi della resilienza di comunità, gruppi sociali, paesi ad attacchi di guerra cognitiva.

Le figure professionali formate attraverso le conoscenze/competenze acquisite durante il Master saranno in grado di affrontare questioni nell'ambito della Cyber Intelligence & Security e, in maniera particolare, alla loro applicazione per governare e gestire scenari di crisi caratterizzati da rischio, incertezza e volatilità delle informazioni. Saranno, altresì, in grado di applicare tali conoscenze ai crimini informatici, alla violazione della riservatezza e alle moderne indagini con strumenti tecnologicamente molto avanzati. Le figure professionali formate avranno anche la possibilità di ricoprire ruoli fortemente richiesti dal mercato come quelli di Data Analyst e Data Scientist.

Art. 5

Articolazione del percorso formativo

Il Corso di Master Universitario, di II livello, denominato "CYBER INTELLIGENCE & SECURITY" si articola in un unico ciclo della durata di un anno, per complessivi 60 crediti formativi (C.F.U), pari ad un numero di 1500 ore di attività.

La frequenza al Corso è obbligatoria ed eventuali assenze dovranno essere adeguatamente giustificate.

Gli insegnamenti saranno impartiti *in modalità blended* attraverso:

- a) ATTIVITÀ D'AULA (didattica online, attività formative di sostegno volte alla socializzazione dei saper minimi, gruppi di studio);
- b) ATTIVITÀ APPLICATIVE (laboratori online, tirocinio e supervisione del tirocinio, attività di valutazione dell'apprendimento).

Sia per le attività d'aula online che per quelle applicative è richiesto un congruo numero di ore riservate allo studio o ad altre attività formative di tipo individuale.

I crediti acquisibili per ciascuna attività e per la prova finale sono di seguito riassunti:

| Progetto generale di articolazione delle attività formative e relativi contenuti | ATTIVITA' | ORE | CFU |
|--|--|-----|-----|
| | DIDATTICA FRONTALE | 300 | 42 |
| | STUDIO INDIVIDUALE E GUIDATO ANCHE ON LINE | 750 | |
| | TIROCINIO | 150 | 6 |



UNIVERSITÀ DEGLI STUDI DI SALERNO

| | | | |
|--|-------------------------------------|-------------|-----------|
| | VERIFICHE INTERMEDIE E PROVA FINALE | 300 | 12 |
| | TOTALE | 1500 | 60 |

Il Master sarà erogato in modalità blended. Per quanto riguarda la didattica d'aula, alle lezioni tradizionali saranno affiancate lezioni svolte in modalità on line. Inoltre, in funzione di esigenze logistiche e/o didattiche, le lezioni possono essere erogate anche in modalità mista (distance learning/presenza). È possibile prevedere anche web conference, al fine di facilitare lo svolgimento di lezioni/seminari tenuti da docenti appartenenti ad altre università o organizzazioni geograficamente distanti. Sono inoltre previste forme di didattica attiva: discussione di casi, lavori di gruppo, esercitazioni, formazione esperienziale, role playing, seminari e incontri con manager ed esperti. Il ricorso alla formazione integrata, inoltre, consente di valorizzare le soft skills dei discenti e di attivarne le potenzialità in scenari complessi.

I discenti non lavoratori partecipanti al Master potranno realizzare l'attività di tirocinio previo collocamento presso primarie aziende nazionali e internazionali che svolgono attività coerenti con la figura in uscita prevista dal percorso formativo, ovvero previo utilizzo di piattaforme applicative già in uso presso le strutture dipartimentali di Ateneo (es: eduopen , federica web learning e altre).

I discenti lavoratori potranno, invece, realizzare l'attività di tirocinio presso la propria Amministrazione di appartenenza ovvero presso altra Amministrazione, sia pubblica sia privata; tale modalità rappresenta una sperimentazione attiva dei contenuti appresi durante il percorso formativo frontale e a distanza.

Le attività formative inizieranno il giorno 19 settembre 2025.

Art. 6

Termini per la presentazione della domanda telematica di ammissione al concorso

La presentazione della domanda di ammissione al concorso è articolata nelle fasi di seguito indicate:

PRIMA FASE

REGISTRAZIONE AL SISTEMA INFORMATIVO DI ATENEO

Non sono tenuti alla registrazione al sistema informatico di Ateneo i candidati già precedentemente iscritti presso l'Università degli Studi di Salerno. Essi potranno accedere direttamente all'Area Riservata esclusivamente con le credenziali SPID (Sistema Pubblico di Identità Digitale) selezionando <LOGIN> dal menù in alto a destra.

I candidati italiani che non siano già registrati al sistema informatico di Ateneo dovranno, invece, preliminarmente, registrarsi allo stesso come nuovo utente utilizzando esclusivamente lo SPID (Sistema Pubblico di Identità Digitale) con le seguenti modalità:

1. collegarsi al sito internet di Ateneo: www.unisa.it ; selezionare i link di seguito indicati: SERVIZI ON LINE - SERVIZI PER STUDENTI- AREA UTENTE (ESSE3) - per accedere all'Area Riservata;
2. accedere all'Area Riservata selezionando dal menù sulla destra della pagina l'opzione: "Registrazione con SPID", completare la registrazione con SPID e, quindi, compilare in ogni sua parte il modulo che verrà proposto.

I candidati minorenni e stranieri che non siano già titolari dei codici di accesso dovranno, invece, preliminarmente, registrarsi al sistema informatico di Ateneo, con le seguenti modalità:



UNIVERSITÀ DEGLI STUDI DI SALERNO

1. collegarsi al sito internet di Ateneo: www.unisa.it ; selezionare i link di seguito indicati: SERVIZI ON LINE – SERVIZI PER STUDENTI – AREA UTENTE (ESSE3) – per accedere all’Area Riservata;
2. entrati nell’area riservata, selezionare dal menù sulla destra della pagina l’opzione: “Registrazione studenti stranieri e minorenni” e compilare in ogni sua parte il modulo che verrà proposto. In fase di registrazione verrà richiesto un indirizzo e-mail personale da utilizzare per il recupero della password.
3. al termine della registrazione il candidato riceverà una coppia di codici (“nome utente” e “password”) da stampare o annotare con cura nel rispetto dei caratteri maiuscoli. Tale coppia di codici consentirà, in seguito, di accedere all’Area Riservata (“Login”).

La procedura on-line descritta è accessibile da qualunque postazione informatica connessa alla rete web.

SECONDA FASE ISCRIZIONE AL CONCORSO

(DOMANDA DI AMMISSIONE + PAGAMENTO CONTRIBUTO + CARICAMENTO TITOLI)

Una volta effettuata la procedura di registrazione, il candidato dovrà iscriversi al concorso, implementando le attività di seguito indicate:

- A. compilazione per via telematica della domanda di ammissione al concorso,
- B. pagamento del contributo per la partecipazione al concorso tramite la modalità elettronica denominata PagoPA,
- C. caricamento nella piattaforma dei titoli valutabili.

A tal fine, dovrà:

1. collegarsi al sito internet di Ateneo: www.unisa.it ; selezionare i link di seguito indicati: SERVIZI ON LINE – SERVIZI PER STUDENTI – AREA UTENTE (ESSE3) – per accedere all’Area Riservata;
2. entrati nell’Area Riservata,
 - per i candidati stranieri o minorenni che abbiano acquisito i predetti codici: selezionare dal menu alla destra della pagina l’opzione: “Login”: la procedura proporrà una maschera nella quale inserire la predetta coppia di codici;
 - per i candidati italiani che si siano registrati o autenticati utilizzando lo SPID (Sistema Pubblico di Identità Digitale): selezionare dal menu alla destra della pagina l’opzione: “Login” e fare accesso con lo SPID;
3. effettuato l’accesso, alla destra della nuova pagina, verrà indicato un elenco completo di tutte le operazioni che è possibile effettuare nella sezione <Area Studenti>: selezionare “Test per corsi ad accesso programmato” e compilare la domanda di ammissione seguendo le istruzioni fornite dalla procedura. Sarà richiesto, tra l’altro, di inserire i dati del proprio documento di riconoscimento, che dovrà essere lo stesso che sarà portato in sede di concorso per l’identificazione.
Si ricorda che per i dati dichiarati in fase di iscrizione si applicano le sanzioni penali previste nel caso di dichiarazioni non veritiere, di formazione o uso di atti falsi, richiamate dall’articolo 76 del D.P.R. 28 dicembre 2000, n° 445, e si decade dai benefici conseguenti al provvedimento eventualmente emanato sulla base della dichiarazione non veritiera, qualora dal controllo effettuato emerga la non veridicità del contenuto di taluna delle dichiarazioni rese (art.75 D.P.R. 28 dicembre 2000, n° 445);
4. terminato l’inserimento dei dati richiesti, cliccando il pulsante <Stampa domanda di Ammissione>, stampare la domanda di ammissione al concorso compilata on line



UNIVERSITÀ DEGLI STUDI DI SALERNO

completandone la compilazione, ed **effettuare il pagamento del contributo per la partecipazione al concorso, per un importo di € 30,00.**

Il pagamento del suddetto contributo dovrà essere effettuato tramite la modalità elettronica denominata PagoPA, utilizzando alternativamente una delle seguenti modalità:

- A): **direttamente online**, cliccando il pulsante <Pagamenti> e successivamente il pulsante <Paga con PagoPA>, scegliendo tra i seguenti strumenti disponibili: carta di credito o debito o prepagata, oppure bonifico bancario nel caso si disponga di un conto corrente presso banche e altri prestatori di servizio di pagamento aderenti all'iniziativa, o scegliendo un canale alternativo di pagamento.
- B): **di persona**, cliccando il pulsante <Pagamenti> e successivamente il pulsante <Stampa Avviso per PagoPA>, in modo da ottenere la stampa del relativo Avviso di pagamento riportante il **Codice di Avviso di Pagamento (IUV)**, da utilizzare presso tutte le banche e gli altri **Prestatori di Servizi di Pagamento (PSP)** aderenti all'iniziativa tramite i canali da questi messi a disposizione (sportello fisico, ATM), ovvero presso le tabaccherie con circuito Banca 5, i punti vendita di SISAL e LIS PAGA di Lottomatica.

Il Contributo per la partecipazione al concorso non verrà restituito in nessun caso.

I soli cittadini stranieri residenti all'estero sono esonerati dal pagamento del predetto Contributo.

5. terminate le suddette attività, cliccando il pulsante <Modifica Titoli di Valutazione>, **caricare nella piattaforma gli atti e/o i documenti attestanti il possesso dei titoli valutabili di cui al successivo articolo 9.**

Tale documentazione, completa dell'elenco generale degli atti e documenti caricati e della scansione del documento di riconoscimento che sarà portato in sede di concorso, dovrà essere caricata utilizzando alternativamente una delle seguenti modalità:

- unico file PDF non modificabile,
- più files PDF non modificabili per ciascun titolo.

L'iscrizione al concorso, previa compilazione per via telematica della domanda di ammissione, pagamento del contributo per la partecipazione e caricamento dei titoli valutabili, dovrà essere perfezionata entro il termine perentorio del giorno 28 agosto 2025, ore 15:00 (ora italiana). A tal fine, la procedura informatizzata di cui al presente articolo sarà improrogabilmente chiusa entro il termine perentorio di cui al presente comma.

Si precisa che la domanda di ammissione al concorso di cui al presente articolo non dà diritto a sostenere le prove concorsuali, se non si è provveduto ad effettuare il pagamento del contributo per la partecipazione al concorso entro il termine perentorio previsto dal presente articolo.

Inoltre, la domanda di ammissione al concorso, debitamente compilata e sottoscritta, e la ricevuta del pagamento del contributo per la partecipazione al concorso **non** dovranno essere consegnate all'Ufficio Formazione Post-Laurea dell'Ateneo, ma conservate a cura del candidato ed esibite, se richieste, alla Commissione Esaminatrice di cui al successivo articolo 9.

Non saranno, infine, accettate domande di ammissione trasmesse a mezzo fax, a mezzo posta elettronica (semplice o certificata), ovvero consegnate a mano o spedite a mezzo posta.

Art.7

Contenuto della domanda telematica di ammissione al concorso



UNIVERSITÀ DEGLI STUDI DI SALERNO

Nella domanda, da compilarsi per via telematica con la procedura informatizzata di cui al precedente articolo 6, il candidato dovrà dichiarare, a pena di esclusione e sotto la propria responsabilità:

1. cognome e nome, luogo e data di nascita;
2. cittadinanza;
3. residenza;
4. possesso del titolo di studio di cui al precedente articolo 3, l'Istituzione universitaria presso la quale lo stesso è stato conseguito, la votazione e la data del conseguimento.

Il candidato è, altresì, tenuto ad indicare la casella di posta elettronica presso la quale intende ricevere il link di accesso per la prova di ammissione nonché le eventuali comunicazioni relative al concorso, e ad impegnarsi a segnalare tempestivamente le variazioni che dovessero intervenire successivamente.

Nella domanda di partecipazione al concorso i candidati portatori di handicap sono tenuti, ai sensi dell'art. 20 della L. 5 febbraio 1992, n° 104, a richiedere l'ausilio necessario e a indicare gli eventuali tempi aggiuntivi per l'espletamento delle prove.

Agli studenti con invalidità uguale o superiore al 66%, che potranno usufruire della partecipazione gratuita al master, viene richiesto di inoltrare opportuna certificazione già in fase di ammissione al concorso, così da non essere inseriti nelle liste per l'attribuzione delle borse di studio, che consentono la riduzione del costo di iscrizione per gli altri partecipanti.

L'esclusione dal concorso può essere disposta in qualsiasi momento, per difetto dei requisiti di ammissione, per pagamento effettuato decorsi i termini di cui al presente articolo, con provvedimento motivato del Rettore.

Articolo 8 Partecipanti a singoli moduli didattici

La domanda di partecipazione al Corso da parte di partecipanti a singoli moduli didattici cui al precedente articolo 1 dovrà essere compilata secondo l'apposito modulo (cfr. Allegato A), e dovrà essere indirizzata a:

Direttore del Master Universitario, di II livello, denominato "CYBER INTELLIGENCE & SECURITY – Università degli Studi di Salerno – Via Giovanni Paolo II, 132 – 84084 Fisciano (SA)

Essa dovrà pervenire **entro il termine perentorio del giorno 31 dicembre 2025, ore 15:00 (ora italiana)**, alla seguente casella di posta elettronica: cyber@unisa.it.

Alla domanda d'iscrizione dovrà essere allegata, a pena di esclusione, la seguente documentazione:

- 1) dichiarazione sostitutiva di certificazione, resa ai sensi del D.P.R. 28 dicembre 2000 n. 445, relativa all'avvenuto conseguimento del titolo di studio posseduto, in cui riportare l'Istituzione presso il quale è stato conseguito, la votazione e la data in cui è stato sostenuto l'esame finale;
- 2) *curriculum vitae et studiorum*;
- 3) fotocopia della carta d'identità (fronte/retro) o di un documento equipollente e del codice fiscale.

Nell'oggetto dell'e-mail dovrà essere specificato: **Corso di Master Universitario, di II livello, denominato "CYBER INTELLIGENCE & SECURITY"**.

La **Tassa di partecipazione** annuale, versata da ciascun iscritto, ammonta rispettivamente ad **€ 2.400,00**. Essa dovrà essere corrisposta alle scadenze di seguito indicate:



UNIVERSITÀ DEGLI STUDI
DI SALERNO

| Anno Accademico | Anno di corso | Rata | Importo | Scadenza |
|-----------------|---------------|---------------------|--------------------------|---------------------------------------|
| 2024/2025 | 1 | 1 ^a rata | €. 1.216,00 ¹ | all'atto dell'immatricolazione |
| | | 2 ^a rata | €. 1.200,00 | entro e non oltre il 28 febbraio 2026 |

¹ di cui € 16 a titolo di imposta di bollo assolta in modo virtuale

Il pagamento delle suddette Tasse dovrà essere effettuato utilizzando esclusivamente la modalità elettronica denominata PagoPA, scegliendo alternativamente una delle seguenti modalità:

- A): **direttamente online**, cliccando il pulsante <Pagamenti> e successivamente il pulsante <Paga con PagoPA>, scegliendo tra i seguenti strumenti disponibili: carta di credito o debito o prepagata, oppure bonifico bancario nel caso si disponga di un conto corrente presso banche e altri prestatori di servizio di pagamento aderenti all'iniziativa, o scegliendo un canale alternativo di pagamento.
- B): **di persona**, cliccando il pulsante <Pagamenti> e successivamente il pulsante <Stampa Avviso per PagoPA>, in modo da ottenere la stampa del relativo Avviso di pagamento riportante il **Codice di Avviso di Pagamento (IUV)**, da utilizzare presso tutte le banche e gli altri **Prestatori di Servizi di Pagamento (PSP)** aderenti all'iniziativa tramite i canali da questi messi a disposizione (sportello fisico, ATM), ovvero presso le tabaccherie con circuito **Banca 5**, i punti vendita di **SISAL** e **LIS PAGA di Lottomatica**.

Al termine della frequenza dei moduli singoli, verrà rilasciato un attestato di partecipazione a cura della Direttrice del Master, con l'indicazione dei temi e del rispettivo numero di ore di partecipazione alle attività.

L'esclusione dal concorso può essere disposta in qualsiasi momento e con apposito provvedimento per difetto dei requisiti di ammissione.

Art.9

Titoli valutabili

Ai fini della procedura concorsuale di cui al successivo articolo 11, sono considerati titoli valutabili:

1. dichiarazione sostitutiva di certificazione, resa ai sensi dell'art. 46 del D.P.R. 28 dicembre 2000, n° 445, relativa al possesso del titolo di studio di cui al precedente articolo 3, completa dell'indicazione dell'Istituzione universitaria presso la quale lo stesso è stato conseguito, della data del conseguimento, della votazione riportata, delle votazioni riportate nei singoli esami di profitto;
2. *curriculum vitae et studiorum* completo di indicazione della casella di posta elettronica presso la quale intende ricevere il link di accesso per la prova di ammissione;
3. tesi di laurea;
4. atti e/o documenti attestanti l'esperienza certificata nel settore del Master;
5. pubblicazioni a stampa o lavori in extenso attinenti al Master.

Art.10

Commissione Esaminatrice



UNIVERSITÀ DEGLI STUDI DI SALERNO

La Commissione Esaminatrice viene nominata, su proposta del Comitato Scientifico del Corso di Master, dal Rettore con proprio Decreto.

Essa è composta da tre professori di ruolo dell'Ateneo.

Essa definisce la graduatoria finale di merito di cui al successivo articolo 11 secondo l'ordine decrescente delle votazioni complessive riportate da ciascun candidato.

Tale graduatoria verrà resa pubblica a mezzo pubblicazione all'Albo Ufficiale di Ateneo alla voce <https://web.unisa.it/amministrazione-trasparente/albo>.

La suddetta graduatoria sarà, altresì, pubblicata, a soli fini di pubblicità-notizia, nel sito web di Ateneo all'indirizzo: <http://web.unisa.it/didattica/master/bandi>.

Art. 11

Prove concorsuali e graduatoria finale di merito

Il concorso pubblico per l'ammissione al Corso di Master Universitario, di II livello, denominato "CYBER INTELLIGENCE & SECURITY" è per **titoli ed esame**. La valutazione complessiva è espressa in centesimi.

L'esame di ammissione consta di una **prova orale**, diretta ad accertare la cultura generale nelle aree di formazione e la motivazione alla partecipazione al percorso formativo.

Il punteggio massimo attribuibile alla prova d'esame è di 70/100. La votazione minima per il superamento della prova d'esame è di 40/70.

I **titoli** sono valutabili secondo i criteri di seguito indicati. A tal fine, la valutazione massima è di 30 punti, così suddivisi:

a) VOTO DI LAUREA – Punteggio massimo: punti 5.

La Commissione esaminatrice attribuirà al voto di laurea un punteggio in base al seguente prospetto:

voto 110 e lode – 5 punti

voto da 104 a 110 – 4 punti

voto da 97 a 103 – 3 punti

voto da 90 a 96 – 2 punti

< di 90 – 1 punto

Nel caso, di conseguimento di una o più titoli di laurea, nell'attribuzione del punteggio verrà presa in considerazione la votazione più alta conseguita.

b) CURRICULUM VITAE ET STUDIORUM – Punteggio massimo: punti 5.

La Commissione esaminatrice potrà attribuire, a suo insindacabile giudizio, un punteggio fino ad un massimo di 5 punti, al curriculum vitae et studiorum del candidato, con particolare riferimento al possesso di altri titoli di studio quali Dottorato di Ricerca, Specializzazioni e Corsi di perfezionamento universitario post-laurea, purché attinenti al Master.

c) TESI LAUREA ATTINENTE AL MASTER– Punteggio massimo: punti 5.

La Commissione esaminatrice stabilirà preliminarmente se la tesi del candidato, compilativa o sperimentale, sia stata svolta in disciplina attinente al percorso formativo del Master. In caso affermativo l'elaborato potrà essere valutato, ad insindacabile giudizio della Commissione, fino ad un massimo di 5 punti, secondo la qualità del lavoro svolto dal candidato e l'attinenza alle discipline del Master.

d) ESPERIENZE CERTIFICATE NEL SETTORE – Punteggio massimo: punti 10.



UNIVERSITÀ DEGLI STUDI DI SALERNO

La Commissione esaminatrice potrà attribuire, a suo insindacabile giudizio, un punteggio fino ad un massimo di 10 punti.

e) PUBBLICAZIONI ATTINENTI AL MASTER – Punteggio massimo: punti 5.

La Commissione esaminatrice potrà attribuire, a suo insindacabile giudizio, un punteggio fino ad un massimo di 5 punti, alle pubblicazioni attinenti al Master. La tesi di laurea, se pubblicata, potrà essere valutata una sola volta, come tesi o come pubblicazione.

Ai sensi dell'art. 3, comma 7, della L. 15 maggio 1997, n° 127, come modificato dall'art. 2 della L. 16 giugno 1998, n° 191, se due o più candidati ottengono, a conclusione delle operazioni di valutazione dei titoli, pari punteggio, è preferito il candidato più giovane d'età.

La Commissione Esaminatrice definirà la graduatoria finale di merito secondo l'ordine decrescente delle votazioni complessive riportate da ciascun candidato.

Con Decreto del Rettore saranno approvati gli atti concorsuali nonché la **graduatoria finale di merito**, e proclamati i vincitori del concorso. Avverso tale provvedimento è possibile proporre ricorso all'autorità giudiziaria competente entro il termine di legge, decorrente dalla data di pubblicazione del provvedimento medesimo all'Albo Ufficiale dell'Ateneo.

In caso di rinuncia o decadenza dei vincitori, si procederà allo scorrimento della graduatoria finale di merito in favore di coloro che risultino utilmente collocati nella stessa.

Art.12

Data della prova orale

La prova orale per l'ammissione al Corso di Master Universitario, di II livello, denominato "CYBER INTELLIGENCE & SECURITY" si svolgerà per via telematica, previo utilizzo della piattaforma audio-video di Ateneo denominata Microsoft Teams, il giorno **5 settembre 2025, ore 12:00**.

Ai partecipanti verrà inviato, il giorno precedente quello fissato per la prova concorsuale, alla casella di posta elettronica indicata con le modalità di cui ai precedenti articoli 7 ed 8, il link di accesso alla suddetta piattaforma. Per eventuali informazioni, si può contattare la casella di posta elettronica dedicata ciber@unisa.it

La presente comunicazione ha valore legale di notifica a tutti gli effetti di legge.

Art. 13

Documentazione per l'immatricolazione

I candidati che risultino utilmente collocati nella graduatoria finale di merito dovranno presentare domanda di immatricolazione, a pena di decadenza, **a partire dal giorno 12 settembre 2025 fino al giorno 16 settembre 2025**, utilizzando **esclusivamente** la procedura informatizzata, attivata previo accesso al sito internet di Ateneo: www.unisa.it, ed avvalendosi della coppia di codici ("nome utente" e "password") ottenuti con la registrazione.

In particolare, dovranno:

1. collegarsi al sito internet di Ateneo: www.unisa.it ; selezionare i link di seguito indicati: SERVIZI ON LINE – SERVIZI PER STUDENTI– AREA UTENTE (ESSE3) – per accedere all'Area Riservata;
2. entrati nell'Area Riservata,



UNIVERSITÀ DEGLI STUDI DI SALERNO

- per i candidati stranieri o minorenni che abbiano acquisito i predetti codici: selezionare dal menu alla destra della pagina l'opzione: "Login": la procedura proporrà una maschera nella quale inserire la predetta coppia di codici;
 - per i candidati italiani che si siano registrati o autenticati utilizzando lo SPID (Sistema Pubblico di Identità Digitale): selezionare dal menu alla destra della pagina l'opzione: "Login" e fare accesso con lo SPID;
3. effettuato l'accesso, alla destra della nuova pagina, nella sezione <Area Studente> verrà indicato un elenco completo di tutte le operazioni che è possibile effettuare: selezionare "Immatricolazione", compilando la relativa domanda avvalendosi delle istruzioni fornite dalla procedura informatizzata.
Se i dati sono corretti, cliccare sul bottone <conferma i dati inseriti> per confermarli; altrimenti, qualora si intenda modificare qualche dato, cliccare sul bottone <Modifica i dati inseriti>;
4. terminare l'inserimento dei dati richiesti, cliccando il pulsante <Stampa Domanda di Immatricolazione>, stampare la domanda di immatricolazione e provvedere al pagamento della Tassa Regionale per il Diritto allo Studio Universitario ed alla prima rata delle Tasse di iscrizione al Master, seguendo le istruzioni di cui al successivo articolo 13.

Il pagamento delle predette Tasse dovrà essere effettuato, a pena di decadenza dall'immatricolazione, entro il termine perentorio di cui al comma 1 del presente articolo.

Una volta contabilizzati dal sistema informativo di Ateneo i predetti importi, lo studente ha l'obbligo di **allegare**, nella sezione "Allegati carriera" della propria area riservata dei servizi studenti on line, la scansione della domanda di immatricolazione comprensiva di:

- autocertificazione del possesso dei requisiti di ammissione debitamente sottoscritta,
- autocertificazione relativa all'eventuale iscrizione contemporanea a due corsi di studio universitari reperibile nella pagina internet dell'Ufficio al link: <https://web.unisa.it/uploads/rescue/68/21/domanda-di-doppia-iscrizione-corsi-universitari-2022-compilabile-copia.pdf>
- fotocopia fronte e retro di un documento di riconoscimento in corso di validità,
- fotocopia del codice fiscale.

Per l'invio telematico della documentazione sopra indicata dovranno essere utilizzati formati statici e non direttamente modificabili, preferibilmente PDF.

Gli studenti portatori di handicap con invalidità uguale o superiore al 66% sono tenuti al rispetto della medesima procedura di immatricolazione on line, dichiarando lo stato di studente portatore di handicap.

I predetti sono tenuti al solo pagamento della Tassa Regionale per il Diritto allo Studio Universitario, di cui al successivo articolo 14.

Si informa, infine, che sulla domanda di immatricolazione e sul relativo bollettino di versamento è riportato il numero di matricola assegnato a ciascuno studente.

I candidati stranieri devono anche presentare:

- diploma originale di Laurea con traduzione, legalizzazione e dichiarazione di valore del Consolato o Ambasciata Italiana del Paese ove lo stesso è stato conseguito;
- documento di soggiorno:
- per i cittadini comunitari: carta di soggiorno;
- per i cittadini extracomunitari: permesso di soggiorno per lavoro subordinato o lavoro autonomo, per motivi familiari, per asilo politico, per asilo umanitario, per motivi religiosi e di studio per il periodo di almeno un anno, rinnovabile sino al termine degli studi.



UNIVERSITÀ DEGLI STUDI DI SALERNO

I candidati ammessi che non avranno provveduto all'immatricolazione entro il termine previsto saranno considerati rinunciatari. Si procederà, quindi, ad ammettere al Corso i candidati immediatamente successivi secondo l'ordine della graduatoria finale di merito; a tal fine, l'iscrizione dei subentranti dovrà avvenire **entro 5 giorni dalla pubblicazione del relativo provvedimento all'Albo Ufficiale di Ateneo**. Tale pubblicazione costituirà notifica ufficiale ai vincitori dei risultati concorsuali; conseguentemente, non verranno inviate comunicazioni personali.

In caso di rinuncia non è consentito il rimborso delle tasse già corrisposte.

Art. 14

Tasse universitarie

L'importo della Tassa Regionale per il Diritto allo Studio Universitario è graduato, per tutti gli studenti iscritti al Master, su tre fasce di contribuzione. Per determinare la propria fascia di contribuzione occorre fare riferimento all'attestazione I.S.E.E. per "Prestazioni per il diritto allo studio universitario", in corso di validità, risultante negli archivi I.N.P.S.

Al momento dell'immatricolazione online, la procedura informatica preleverà in automatico i dati ISEE, se presenti, dal sito web dell'INPS. Nel caso in cui non sia rilevata un'attestazione ISEE di tipo universitario, lo studente sarà collocato nella fascia contributiva cd. **SENZA ISEE**.

La **Tassa d'iscrizione** annuale, versata da tutti gli studenti iscritti al Corso di Master, ammonta rispettivamente ad **€ 7.500,00**. Essa dovrà essere corrisposta alle scadenze di seguito indicate:

| Anno Accademico | Anno di corso | Rata | Importo | Scadenza |
|-----------------|---------------|---------------------|--------------------------|---------------------------------------|
| 2024/2025 | 1 | 1 ^a rata | €. 2.516,00 ¹ | all'atto dell'immatricolazione |
| | | 2 ^a rata | €. 2.500,00 | entro e non oltre il 31 dicembre 2025 |
| | | 3 ^a rata | €. 2.500,00 | entro e non oltre il 30 aprile 2026 |

¹ di cui € 16 a titolo di imposta di bollo assolta in modo virtuale

Il pagamento delle suddette Tasse dovrà essere effettuato utilizzando esclusivamente la modalità elettronica denominata PagoPA, scegliendo alternativamente una delle seguenti modalità:

- A): **direttamente online**, cliccando il pulsante <Pagamenti> e successivamente il pulsante <Paga con PagoPA>, scegliendo tra i seguenti strumenti disponibili: carta di credito o debito o prepagata, oppure bonifico bancario nel caso si disponga di un conto corrente presso banche e altri prestatori di servizio di pagamento aderenti all'iniziativa, o scegliendo un canale alternativo di pagamento.
- B): **di persona**, cliccando il pulsante <Pagamenti> e successivamente il pulsante <Stampa Avviso per PagoPA>, in modo da ottenere la stampa del relativo Avviso di pagamento riportante il **Codice di Avviso di Pagamento (IUV)**, da utilizzare presso tutte le banche e gli altri **Prestatori di Servizi di Pagamento (PSP)** aderenti all'iniziativa tramite i canali da questi messi a disposizione (sportello fisico, ATM), ovvero presso le tabaccherie con circuito **Banca 5**, i punti vendita di **SISAL** e **LIS PAGA di Lottomatica**.



UNIVERSITÀ DEGLI STUDI DI SALERNO

I termini di cui al presente articolo sono perentori: gli studenti che non corrispondono le rate entro le scadenze previste sono tenuti al pagamento di un'**indennità di mora** per un importo di **€ 50,00**.

Gli studenti che non risultano in regola con il pagamento delle tasse universitarie di cui al presente articolo non possono compiere atti di carriera scolastica né richiedere certificati.

Lo studente che ha ottenuto l'iscrizione al Corso non ha diritto in alcun caso alla restituzione delle tasse e dei contributi universitari corrisposti.

Art. 15 **Incentivi a sostegno del merito**

In base ai finanziamenti disponibili, il Comitato Scientifico potrà deliberare l'assegnazione di incentivi a sostegno del merito, consistenti in un esonero parziale o totale dal versamento delle tasse di iscrizione.

L'incentivo sarà assegnato ai candidati, utilmente classificati nella graduatoria finale di merito, secondo l'ordine della stessa, che sarà formulata a seguito della valutazione degli esiti di apprendimento conseguiti al termine delle attività didattiche d'aula.

Gli studenti non devono presentare alcuna domanda d'esonero per merito: l'Università verifica d'ufficio il possesso dei requisiti di merito

Art. 16 **Piano degli studi**

Il piano degli studi previsto per il Corso di Master Universitario, di II livello, denominato "CYBER INTELLIGENCE & SECURITY" è allegato al presente bando di concorso (ALLEGATO A), del quale costituisce parte integrante e sostanziale.

Art. 17 ***Facoltà di iscrizione contemporanea e incompatibilità***

È consentita l'**iscrizione contemporanea** a un corso di laurea o di laurea magistrale e a un corso di master, di dottorato di ricerca o di specializzazione, ad eccezione dei corsi di specializzazione medica, nonché l'iscrizione contemporanea a un corso di dottorato di ricerca o di master e a un corso di specializzazione medica.

È altresì consentita l'**iscrizione contemporanea** a un corso di dottorato di ricerca o di master e a un corso di specializzazione non medica.

Qualora uno dei due corsi di studio, secondo quanto disciplinato nel rispettivo regolamento didattico, sia a frequenza obbligatoria, è consentita l'iscrizione ad un secondo corso di studio che non presenti obblighi di frequenza.

L'iscrizione contemporanea è consentita presso Istituzioni italiane ovvero italiane ed estere.

Art. 18 **Gestione amministrativo-contabile**

La gestione amministrativo - contabile dei fondi compete ai competenti Uffici dell'Università degli Studi di Salerno.



UNIVERSITÀ DEGLI STUDI
DI SALERNO

Articolo 19

Copertura assicurativa

L'Università degli Studi di Salerno garantisce agli studenti, per tutta la durata del Corso, la copertura assicurativa per infortuni e responsabilità civile durante ed in occasione della frequenza di attività didattiche, durante ed in occasione dell'espletamento di attività formative di studio e di ricerca connesse allo stesso.

La copertura assicurativa è, altresì, garantita durante ed in occasione del tirocinio anche pratico svolto al di fuori dei locali dell'Ateneo nonché durante ed in occasione di eventuali periodi di soggiorno all'estero, purché tali attività siano preventivamente autorizzate dal Direttore del Corso.

Art. 20

Pubblicità

Il presente bando di concorso è affisso all'Albo Ufficiale di Ateneo alla voce: <https://web.unisa.it/amministrazione-trasparente/albo> e consultabile nella pagina internet dell'Ufficio alla voce: <http://web.unisa.it/didattica/master/bandi>.

Art. 21

Trattamento dei dati personali

In attuazione del Regolamento UE del Parlamento Europeo e del Consiglio in data 27 aprile 2016, l'Università degli Studi di Salerno, in quanto Pubblica Amministrazione, ai sensi dell'art. 1, comma 2, del Decreto Legislativo 165/2001 e sue successive modifiche ed integrazioni, persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche. Pertanto, il trattamento dei dati personali, nell'esercizio dei suoi compiti istituzionali, trova il fondamento di liceità nella condizione prevista dall'art. 6, par. 1, del suddetto Regolamento, ed il fondamento giuridico nell'apposito Regolamento di Ateneo emanato con Decreto Rettorale 18 luglio 2019, Rep. n° 7327, Prot. n° 201636.

Al riguardo, l'Università degli Studi di Salerno garantisce che il trattamento dei dati personali sarà improntato a principi di liceità, correttezza e trasparenza nei confronti dell'interessato.

In particolare, i dati personali saranno raccolti in maniera adeguata, pertinente e limitata alle finalità connesse e strumentali al presente bando di concorso ed all'eventuale gestione del rapporto con l'Ateneo, e successivamente trattati in modo compatibile con tale finalità. Essi saranno, se necessario, aggiornati, e conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle suddette finalità, nonché per fini statistici, previa adozione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato.

Il trattamento dei dati personali sarà effettuato con le seguenti modalità: informatizzato e cartaceo. Il consenso al trattamento dei suddetti dati è obbligatorio per l'espletamento della procedura concorsuale di cui al presente bando di concorso, e per l'eventuale gestione della carriera accademica dello studente; conseguentemente, l'eventuale rifiuto a fornire i dati non consentirà lo svolgimento della predetta procedura concorsuale e la gestione della carriera accademica. I dati potranno essere comunicati a soggetti pubblici o privati, anche mediante inserimento nel sito internet di Ateneo, per adempimenti imposti da disposizioni di legge; a tal fine, il trattamento sarà curato da personale dell'Ateneo.

I candidati hanno diritto a: ottenere la conferma dell'esistenza o meno dei dati personali che li riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;



UNIVERSITÀ DEGLI STUDI DI SALERNO

ottenere l'accesso, la rettifica, la cancellazione nonché presentare opposizione al trattamento; esercitare il diritto alla limitazione del trattamento non solo in caso di violazione dei presupposti di liceità del trattamento, e quale alternativa alla cancellazione dei dati stessi, bensì anche nelle more che sia riscontrata da parte del titolare una richiesta di rettifica dei dati o di opposizione al trattamento; esercitare il diritto di opposizione alla profilazione; esercitare il diritto alla portabilità dei dati solo qualora il trattamento si basi sul consenso ai sensi dell'art. 6, par. 1, lettera a), o dell'art. 9, par. 2, lettera a) del Regolamento UE o su un contratto ai sensi dell'art. 6, par. 1, lettera b) del Regolamento UE e sia effettuato con mezzi automatizzati; esercitare il diritto all'oblio chiedendo la cancellazione dei propri dati personali nel caso questi siano stati resi pubblici on-line.

Titolare del trattamento dei dati personali è l'Università degli Studi di Salerno, con sede legale in Fisciano (SA) alla via Giovanni Paolo II, 132, in persona del suo legale rappresentante, Rettore Pro-tempore, PEC: ammicent@pec.unisa.it.

Responsabile della protezione dei dati personali è il Dirigente autorizzato dal Titolare al trattamento, in relazione alle proprie funzioni e competenze, alla protezione dei dati: PEC: protezionedati@pec.unisa.it.

Responsabile esterno del trattamento dei dati personali è il Consorzio Interuniversitario CINECA, nella qualità di fornitore del relativo servizio - con sede in via Magnanelli 6/3 - 40033 Casalecchio di Reno (BO), PEC: cineca@pec.cineca.it

Responsabile interno del trattamento dei dati personali è il Capo dell'Ufficio Formazione Post Laurea - dott. Giovanni SALZANO, e-mail: gsalzano@unisa.it.

Responsabile amministrativo del procedimento, secondo quanto previsto dagli artt. 4 e ss. della L. 7 agosto 1990, n° 241, e successive modificazioni, è il Capo dell'Ufficio Formazione Post Laurea - dott. Giovanni SALZANO, e-mail: gsalzano@unisa.it.

Art. 22

Norme finali

Per tutto quanto non previsto dal presente bando di concorso, si applicano le norme contenute nel Regolamento di Ateneo per la disciplina dei Corsi di Master, nel D.P.R. 9 maggio 1994, n° 487, e le altre disposizioni vigenti in materia.

IL RETTORE

Vincenzo LOIA

firmato digitalmente ai sensi del D. Lgs n° 82/2005



UNIVERSITÀ DEGLI STUDI
DI SALERNO

Allegato A

PIANO DIDATTICO DEL MASTER

Modulo 1 – Governare le crisi (30 ore)

Questo modulo è dedicato ad illustrare come le tecnologie emergenti (Data Science, AI, Cyber Intelligence e Cyber Security) possono essere applicate per il governo delle crisi. Con il termine crisi, si intende un conflitto (anche potenziale) che comporta scenari di rischio ed incertezza. Due tipologie di crisi saranno illustrate, insieme alle soluzioni tecnologiche ed applicative che possono aumentare la consapevolezza di analisti e decisori che devono governare tali situazioni. Gli scenari di crisi riguardano la sfera economico-sociale (come attacchi a banche, ospedali ed organizzazioni/sistemi complessi in generale, attacchi ad infrastrutture critiche, fomentazione di sommosse popolari con disordine informativo) e la sfera geo-politica (come conflitti di differente natura: economica, tecnologica, militare). In questo modulo, pertanto, sono previste lezioni per far apprendere ai discenti come analizzare le vulnerabilità di un cyber sistema e/o di sistemi complessi interconnessi in rete (banche, multinazionali), analizzare un incident report, implementare politiche di cyber protection (passive e pro-attive), utilizzare metodologie e schemi di attacco, anche basti sul disordine informativo, come pratica di deterrenza. Analogamente, saranno fornite le competenze necessarie ad analizzare i punti di forze e debolezza di un sistema paese e le leve (diplomazia, informativa, militare, economica, tecnologica) che possono essere messe in campo per la gestione delle crisi geo-politiche.

| Unità Didattica | Tipologia | SSD | Ore | Docenti |
|---|------------------------------|------------------|-----|-----------------------|
| Metodologie, Strumenti e Tecniche gestione e governo di crisi e conflitti | Lezione Frontale | SPS/04, | 10 | C.Grelle/A.Manfredini |
| Scenari di crisi economico-sociale | Lezione Frontale/Laboratorio | INF/01 SPS/04 | 10 | R.Volpi/R.Di Biase |
| Scenari di crisi Geo-Politica | Lezione Frontale/Laboratorio | INF/01 SPS/04 | 10 | R.Volpi/R.Di Biase |

Modulo 2 – Data Analysis (30 ore)

Il modulo ha l'obiettivo di fornire le conoscenze attuali sulla disciplina della Data Science. Il modulo inizia con un insegnamento di perfezionamento informatico, basato sul linguaggio di programmazione Python, che permetterà a tutti i discenti, indipendentemente dal loro percorso di provenienza, di imparare il linguaggio e le librerie di data analysis utili allo sviluppo delle differenti fasi di un progetto di data science.

| Unità Didattica | Tipologia | SSD | Ore | Docenti |
|---|----------------------------------|----------------------|-----|------------|
| Perfezionamento Informatico e Coding | Lezione Frontale/ Laboratorio | INF/01 ING-INF/05 | 10 | C. De Maio |
| Programmazione Avanzata in Python Data Base e Data Mining | Lezione Frontale/ Laboratorio | INF/01 ING-INF/05 | 10 | D. Parente |
| Data Analysis & Visualization Laboratorio di Data Analysis | Lezione Frontale | INF/01 ING-INF/05 | 10 | A. Gaeta |

Modulo 3 – Computational intelligence (30 ore)

Il modulo ha l'obiettivo di condurre i discenti alla comprensione dei metodi attuali ed emergenti di Computational. Faranno parte di tale modulo anche approcci e tecniche basate su logiche di tipo fuzzy o rough set per supportare il reasoning approssimato. Saranno, inoltre, approfonditi i modelli di machine learning, deep learning

| Unità Didattica | Tipologia | SSD | Ore | Docenti |
|--|------------------|----------------------|-----|-------------|
| Computational Intelligence e Reasoning Approssimato | Lezione Frontale | INF/01 ING-INF/05 | 15 | M. Nappi |
| Machine Learning Deep Learning | Lezione Frontale | INF/01 ING-INF/05 | 15 | F. Narducci |



UNIVERSITÀ DEGLI STUDI DI SALERNO

Modulo 4 – Artificial Intelligence (30 ore)

Il modulo ha l'obiettivo di condurre i discenti alla comprensione dei metodi attuali ed emergenti di Artificial Intelligence. Saranno, inoltre, approfonditi i modelli di intelligenza artificiale generativa.

| Unità Didattica | Tipologia | SSD | Ore | Docenti |
|-------------------|------------------|----------------------|-----|---------------------|
| Generative AI | Lezione Frontale | INF/01 ING-INF/05 | 15 | F. Orciuoli |
| Laboratorio di AI | Laboratorio | INF/01 ING-INF/05 | 15 | Aniello Castiglione |

Modulo 5 – Situation Awareness e Decision Making (30 ore)

Il modulo ha l'obiettivo di fornire un approfondimento sulle teorie ed i modelli più usati di Situation Awareness e sulla loro relazione/integrazione con le tecniche di Cyber Security e Cyber Intelligence.

| Unità Didattica | Tipologia | SSD | Ore | Docenti |
|---|------------------|----------------------|-----|----------|
| La Situation Awareness | Lezione Frontale | INF/01 ING-INF/05 | 15 | A. Gaeta |
| Fonti e strumenti a supporto di sistemi della Situation Awareness data-driven | Lezione Frontale | INF/01 ING-INF/05 | 15 | G. Fenza |

Modulo 6 – Information disorder (30 ore)

Il modulo ha l'obiettivo di fornire un approfondimento sulle modalità di conflitto emergenti basate, su disordine informativo e strategie di Guerra Cognitiva.

| Unità Didattica | Tipologia | SSD | Ore | Docenti |
|---|---------------------------------|--------|-----|------------------|
| Information Disorder Analysis e Detection | Lezione Frontale laboratorio | INF/01 | 30 | V. Loia/G. Fenza |

Modulo 7 – Metodi, Tecnologie ed Architetture di Cyber Intelligence & Security (120 ore)

Il modulo nasce dall'esigenza di rispondere in modo strutturato alle esigenze di protezione e governo della sicurezza informatica dei sistemi interconnessi nel cyberspazio, e mira a formare esperti nella gestione di tutte le problematiche di intelligence/security nonché di governo del patrimonio informativo nonché delle infrastrutture critiche per l'erogazione di servizi su larga scala. Nell'epoca della trasformazione digitale, la sicurezza informatica si posiziona al centro delle strategie di successo per le aziende di ogni dimensione e settore. Con l'aumento degli attacchi informatici, diventa imperativo per ogni organizzazione implementare misure per proteggere i propri asset digitali. L'obiettivo è costruire l'ecosistema delle competenze per gestire strumenti ed architetture a supporto della cybersicurezza, partendo dai suoi principi di base ed aggiungendo man mano elementi di maggiore sofisticazione e tecnologie avanzate, applicando gli stessi all'analisi critica ed alla valutazione della sicurezza e del rischio di sistemi complessi. Ciò risulterà nella capacità di identificare le principali vulnerabilità dei sistemi interconnessi, riconoscere i meccanismi di attacco/difesa e le strategie per la protezione, applicando le stesse per disegnare/valutare contromisure ed architetture sicure. Infine, questo modulo si concentrerà sulla concreta applicazione di tali tecnologie per la progettazione e realizzazione di sistemi a supporto degli analisti e decisori. In particolare, sarà presentato un nuovo approccio alla protezione, olistico, coordinato e multi-dimensionale, caratterizzato da una totale unitarietà di intenti fra gli attori coinvolti, opportunamente armonizzati in una logica di security fusion in cui vanno orchestrate le varie funzioni di difesa e le controazioni gestite a livello sistemico. Saranno anche presentati in laboratorio scenari pratici di applicazione nonché numerose librerie, basate su python, per la realizzazione di tali sistemi.

Modulo 7 – Metodi, Tecnologie ed Architetture di Cyber Intelligence & Security (30 ore) parte I

| Unità Didattica | Tipologia | SSD | Ore | Docenti |
|--|------------------|-----------------------|-----|--------------|
| Gestione del rischio geopolitico: strategie per modelli di business resilienti | Lezione Frontale | SECS/P-10 SECS/P-7 | 15 | A. Rapisarda |
| Leadership aziendale e cybersecurity | Lezione Frontale | SECS/P-10 SECS/P-7 | 15 | F. Ceraso |



UNIVERSITÀ DEGLI STUDI
DI SALERNO

Modulo 7 – Metodi, Tecnologie ed Architetture di Cyber Intelligence & Security (30 ore) parte II

| Unità Didattica | Tipologia | SSD | Ore | Docenti |
|---|------------------|----------------------|-----|---|
| Elementi di base di Cybersecurity e Network Security | Lezione Frontale | INF/01 ING-INF/05 | 10 | F. Palmieri |
| Architetture e strategie a supporto della CyberSecurity – Ecosistemi di sicurezza | Lezione Frontale | INF/01 ING-INF/05 | 10 | F. Palmieri |
| Modelli e tecniche computazionali per la Cyber Security | Lezione Frontale | INF/01 ING-INF/05 | 10 | F. Palmieri/Arcangelo Castiglione |

Modulo 7 – Metodi, Tecnologie ed Architetture di Cyber Intelligence & Security (30 ore) parte III

| Unità Didattica | Tipologia | SSD | Ore | Docenti |
|---|------------------|----------------------|-----|--------------------------------------|
| Scenari di attacco e difesa nel Cyberspazio | Lezione Frontale | INF/01 ING-INF/05 | 15 | F. Palmieri |
| Tecnologie emergenti per la Cyber Intelligence e Cyber Security | Lezione Frontale | INF/01 ING-INF/05 | 15 | F. Palmieri/Arcangelo Castiglione |

Modulo 7 – Metodi, Tecnologie ed Architetture di Cyber Intelligence & Security (30 ore) parte IV

| Unità Didattica | Tipologia | SSD | Ore | Docenti |
|--|-------------|----------------------|-----|---------------------|
| Laboratorio di Cyber Intelligence & Security | Laboratorio | INF/01 ING-INF/05 | 30 | F. Palmieri/U.Fiore |

STUDIO INDIVIDUALE E GUIDATO

Sono previste 750 ore di studio individuale e guidato. Di queste, 250 saranno lezioni guidate basate sulla metodologia di crisis management, response and simulation. Sono previste attività didattiche finalizzate alla creazione di ambienti virtuali che simulano una realtà socio-economica e geo-politica internazionale. Questi ambienti saranno l'environment su cui si baseranno le lezioni guidate. I discenti saranno divisi in tre gruppi guidati, ognuno, da due tutor esperti (Settori: INF/01/ING-INF/05 e SPS). In queste lezioni, si simulerà una crisi che deve essere gestita. Ogni gruppo dovrà inizialmente effettuare l'assessment dei punti di forza e debolezza del proprio ambiente virtuale (che simula una realtà economico-sociale o geo-politica), proteggere tale ambiente e, contemporaneamente, cercare di scoprire i punti di forza e debolezza degli altri due gruppi. Il risultato sarà sotto forma di report. A valle di ciò, scatta la seconda fase della simulazione. Un ulteriore gruppo (formato da docenti e tutor) innesca un conflitto, andando a minacciare il gruppo di studenti che presenta più debolezze. I tre gruppi di discenti, da ora in poi, saranno coinvolti nelle fasi di governo e gestione del conflitto e dovranno effettuare le azioni necessarie alla comprensione degli effetti di tale conflitto, mitigazione del conflitto (con alleanze, uso di leve, applicazione di politiche di protezione degli asset principali, uso di strategia di deterrenza, etc.) che coinvolgono anche attività di intelligence verso gli altri gruppi ed il gruppo esterno di docenti/tutor. Durante la simulazione, il gruppo di docenti/tutor sarà dedicato a creare nuove azioni di disturbo che possono far scalare il livello della crisi.

VERIFICHE E PROVA FINALE

Sono previste verifiche intermedie della formazione e delle simulazioni.



UNIVERSITÀ DEGLI STUDI
DI SALERNO

Allegato B

Domanda di partecipazione al Corso di Master Universitario, di II livello, denominato “CYBER INTELLIGENCE & SECURITY”

Al Direttore del Corso di Master Universitario
denominato “CYBER INTELLIGENCE & SECURITY”

Il/la sottoscritto/a _____,

C.F. _____, nato/a in _____,

(Prov.) _____ il ____/____/_____, residente in _____,

(Prov.) _____ alla Via _____ n. _____,

tel. _____, cell. _____,

e-mail _____,

chiede

di essere iscritto/a al Corso di Master Universitario denominato “CYBER INTELLIGENCE & SECURITY” in qualità di:

PARTECIPANTE A SINGOLI MODULI DIDATTICI

Selezionare nella tabella sottostante i moduli per i quali si richiede l’iscrizione, barrando la/e cella/e corrispondente/i (nel limite massimo di 4 moduli per i partecipanti a singoli moduli didattici):

| MODULI DIDATTICI | |
|------------------|---|
| 1 | Modulo 1 –Governare le crisi (30 ore) |
| 2 | Modulo 2 – Data Analysis (30 ore) |
| 3 | Modulo 3 – Computational intelligence (30 ore) |
| 4 | Modulo 4 –Artificial Intelligence (30 ore) |
| 5 | Modulo 5 – Situation Awareness e Decision Making (30 ore) |
| 6 | Modulo 6 – Information disorder (30 ore) |
| 7 | Modulo 7 – Metodi, Tecnologie ed Architetture di Cyber Intelligence & Security (30 ore) parte I |
| 8 | Modulo 7 – Metodi, Tecnologie ed Architetture di Cyber Intelligence & Security (30 ore) parte II |
| 9 | Modulo 7 – Metodi, Tecnologie ed Architetture di Cyber Intelligence & Security (30 ore) parte III |
| 10 | Modulo 7 – Metodi, Tecnologie ed Architetture di Cyber Intelligence & Security (30 ore) parte IV |



**UNIVERSITÀ DEGLI STUDI
DI SALERNO**

A tal fine allega la seguente documentazione in carta libera:

- 1) dichiarazione sostitutiva di certificazione, resa ai sensi del D.P.R. 28 dicembre 2000 n. 445, relativa all'avvenuto conseguimento del titolo di studio posseduto, in cui riportare l'Istituzione presso il quale è stato conseguito, la votazione e la data in cui è stato sostenuto l'esame finale;
- 2) *curriculum vitae et studiorum*, ai fini della valutazione dell'adeguata esperienza professionale;
- 3) fotocopia della carta d'identità (fronte/retro) o di un documento equipollente e del codice fiscale.

Luogo: _____

Data: ____/____/____

In fede, _____