U N I V E R S I T A' D E G L I S T U D I D I G E N O V A
AREA DIDATTICA, SERVIZI AGLI STUDENTI, ORIENTAMENTO E INTERNAZIONALIZZAZIONE
SERVIZIO ALTA FORMAZIONE

IL RETTORE

- Vista la Legge 15 maggio 1997, n. 127, pubblicata nel supplemento ordinario alla G.U. n. 113 del 17 maggio 1997 e successive modifiche, in merito alle misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo;
- Visto il Decreto del Ministro dell'Università e della Ricerca Scientifica e Tecnologica del 22 ottobre 2004 n. 270 recante **"***Modifiche al regolamento recante norme concernenti l'autonomia didattica degli atenei, approvato con decreto del Ministro dell'Università e della Ricerca Scientifica e Tecnologica 3 novembre 1999, n. 509*" ed in particolare l'art. 3, comma 9;
- Vista la Legge 12 aprile 2022, n. 33, recante "*Disposizioni in materia di iscrizione contemporanea a due corsi di istruzione superiore*";
- Visto il Decreto Ministeriale 29 luglio 2022, n. 930, recante "*Disposizioni per consentire la contemporanea iscrizione a due corsi universitari*";
- Viste le disposizioni del Ministero dell'Università e della Ricerca relative alle procedure per l'ingresso, il soggiorno e l'immatricolazione degli studenti stranieri/internazionali ai corsi di formazione superiore in Italia per l'a.a. 2023/2024;
- Visto il Regolamento dei Corsi di Perfezionamento, di aggiornamento professionale e di formazione permanente e dei corsi per Master Universitari di primo e secondo livello dell'Università degli Studi di Genova emanato con D.R. n. 511 del 10 febbraio 2015;
- Visto il Regolamento per la disciplina dei contratti di ricerca, di consulenza e di formazione per conto terzi, emanato con D.R. n. 5321 del 31 ottobre 2018;
- Viste le delibere, in data 4 luglio 2017 del Senato Accademico e in data 5 luglio 2017 del Consiglio di Amministrazione, con le quali è stato istituito il Master Universitario di II livello in *"Cybersecurity and Critical Infrastructure Protection";*
- Vista la delibera del Consiglio di Dipartimento di informatica, bioingegneria, robotica e ingegneria dei sistemi – DIBRIS del 12 giugno 2024, con la quale è stata proposta la VII edizione del Master Universitario di II livello in *"Cybersecurity and Critical Infrastructure Protection"* per l'a.a. 2023/2024;
- Visto il Decreto d'urgenza del Preside della Scuola Politecnica del 26 giugno 2024 con il quale è stata proposta l'attivazione della VII edizione del Master Universitario di II livello in *"Cybersecurity and Critical Infrastructure Protection"* per l'a.a. 2023/2024.

D E C R E T A

Art. 1
Norme Generali

È istituito per l'anno accademico 2023/2024 presso il Dipartimento di informatica, bioingegneria, robotica e ingegneria dei sistemi – DIBRIS dell'Università degli Studi di Genova il **Master Universitario di II livello in *"Cybersecurity and Critical Infrastructure Protection"* – VII Edizione**

Strutture che collaborano alla realizzazione del Master:
Strutture Università di Genova: Area ricerca, trasferimento tecnologico e terza missione - Servizio per il trasferimento tecnologico e delle conoscenze
Enti esterni: Centro di competenza per la sicurezza e l'ottimizzazione delle infrastrutture strategiche - Start 4.0

Art. 2
Finalità del Corso

Destinatari dell'azione formativa: Il Master universitario si rivolge ai Laureati magistrali o specialistici con un background informatico che intendano approfondire la preparazione su tematiche verticali nell'ambito della cybersecurity e della protezione delle infrastrutture critiche.

Obiettivi e profili funzionali: Il Master si propone di formare la figura di un esperto nella progettazione e gestione dei sistemi basati sull'Information and Communications Technology (ICT) e di Cybersecurity (Mobile, Web, Cloud, SCADA, IoT, ...) preposti alla tutela della sicurezza e alla protezione del patrimonio informativo ed architetturale di un'azienda, una infrastruttura critica o un'organizzazione.
Le aziende hanno urgente bisogno di inserire personale esperto di Cybersecurity e protezione delle proprie infrastrutture all'interno del loro staff. Va inoltre sottolineato come la domanda di tali figure professionali super di molto l'offerta attualmente disponibile; al tempo stesso, i laureati magistrali attuali non dispongono del livello di competenze necessario.

Sbocchi occupazionali: fra i numerosi profili, sebbene in senso non esclusivo, si possono comunque delineare alcuni sbocchi professionali di riferimento, sottolineando tuttavia che la rapidissima evoluzione dello scenario odierno offre prospettive e potenzialità ben ulteriori rispetto a quelle evidenziate:

- *Information Security Officer* in aziende o Corporate
- Operatore di *Cybersecurity* in infrastrutture critiche (comparto energia, banche e finanza)
- Consulente di *Cybersecurity* per aziende
- Sviluppatore e analista professionale per aziende legate ad automazione nei sistemi SCADA
- Analista e operatore di Intelligence preventiva
- Esperto e consulente legale di *Incident Handling* e *Computer/Digital Forensics*
- Responsabile/componente di CERT aziendale
- Auditor e esperto di Governance della (*Cyber*) Security per analisi di conformità a standard ISO
- Sviluppatore di tool e metodi per aziende ad alto contenuto tecnologico

Art. 3
Organizzazione didattica del Master

Il Master, della durata di 12 mesi, si svolge **da ottobre 2024 a ottobre 2025.**

Il Master si articola in 1500 ore di cui:

- 432 ore di attività formative d'aula e laboratori;
- 648 ore di studio individuale e verifiche di apprendimento;
- 420 ore stage/project work;

Per il dettaglio del piano didattico si rimanda all'**allegato 1**, che è parte integrante del presente bando.

Al Master sono attribuiti 60 CFU.

Sede di svolgimento dell'attività didattica: il master sarà erogato online tramite la piattaforma Microsoft Teams.

La frequenza è a tempo parziale: 16 ore alla settimana divise tra il giovedì pomeriggio (4h), il venerdì (8h) ed il sabato mattina (4h).
Assenze consentite: 34%.
La lingua di insegnamento e di verifica del profitto è l'ITALIANO.
È richiesto un livello di certificazione B2 della lingua italiana per gli studenti stranieri.

Tipologia verifiche intermedie: Ciascun modulo didattico prevede un esame di accertamento per l'attribuzione dei relativi crediti formativi universitari. La votazione attribuita sarà in trentesimi.

Tipologia prova finale: Al termine delle attività formative, il partecipante al Master dovrà preparare e discutere un elaborato (tesi finale) relativo alle attività svolte. L'attività potrà essere: a) di ricerca, sia teorica sia sperimentale, tipicamente orientata all'analisi critica di argomenti trattati nei moduli, allo studio di temi scientifici del settore e alla produzione di risultati sperimentali innovativi; b) di approfondimento, tipicamente relativa all'analisi di argomenti trattati nei moduli, all'applicazione di metodi studiati nei moduli per la soluzione di particolari problemi e casi specifici e all'eventuale produzione di risultati sperimentali; c) di indagine bibliografica, comprendente una ricerca bibliografica su argomenti specifici relativi alle tematiche studiate nel Master.

Certificazione delle competenze pregresse apprese durante il corso di perfezionamento o insegnamenti nell'ambito di precedenti edizioni: Per coloro che hanno frequentato insegnamenti o l'intero corso di perfezionamento in ***"Cybersecurity and Critical Infrastructure Protection"*** in edizioni precedenti sarà possibile fare esplicita richiesta al Comitato di Gestione (master.cybersecurity@unige.it) che valuterà il riconoscimento delle conoscenze pregresse e predisporrà un piano personalizzato per il conseguimento del titolo. Le richieste dovranno contenere i seguenti dati:

- Nome, cognome, numero di matricola, denominazione percorso formativo frequentato (corso oppure elenco insegnamenti) e punteggio conseguito nella valutazione di ciascun insegnamento.

Il costo dell'iscrizione sarà ponderato in considerazione del piano personalizzato.

Costo complessivo del Master: € 5.282,00 (per occupati) o € 2.782,00 (per inoccupati)
€ 5.000,00 + contributo universitario € 250,00+ 2 marche da bollo (€ 16,00+€ 16,00) per occupati per l'intero Master
€ 2.500,00+ contributo universitario € 250,00+ 2 marche da bollo (€ 16,00+€ 16,00) per inoccupati per l'intero Master

Art. 4
Comitato di Gestione e Presidente

Presidente: Luca Verderame.
Vice Presidente: Rodolfo Zunino.
Docenti Unige del Comitato di Gestione: Luca Verderame (DIBRIS), Rodolfo Zunino (DITEN), Alessandro Armando (DIBRIS), Giovanni Chiola (DIBRIS), Paola Girdinio (DITEN), Giovanni Lagorio (DIBRIS), Mario Marchese (DITEN), Enrico Russo (DIBRIS).
Docenti esterni del Comitato di Gestione: Alessio Merlo (CASD), Cocurullo Fabio (Leonardo), Mattia Epifani (RealityNet), Ermete Meda (Cyber Security Information Expert), Massa Danilo (RCS), Silvio Ranise (FBK), Antonio Rebora (Leonardo), Danilo Moresco (ABB), Gaetano Sanacore (A2A).

Art. 5
Requisiti di Ammissione

Il numero minimo per l'attivazione è 12 iscritti, il numero massimo è 25.

Titoli di studio richiesti:

- Laurea in Fisica, Informatica, Ingegneria e Matematica conseguita secondo il previgente ordinamento o titoli equipollenti;
- Laurea magistrale in Fisica (classe LM-17), Informatica (classe LM-18), Ingegneria biomedica (classe LM-21), Ingegneria dell'automazione (classe LM-25), Ingegneria delle telecomunicazioni (classe LM-27), Ingegneria elettrica (classe LM-28), Ingegneria elettronica (classe LM-29), Ingegneria informatica (classe LM-32), Matematica (classe LM-40), Modellistica matematico-fisica per l'ingegneria (classe LM-44) conseguita secondo l'ordinamento vigente o titoli equipollenti (incluse lauree conseguite secondo il previgente ordinamento o all'estero).

Altri requisiti: Possono accedere studenti in possesso di un titolo di studio di secondo livello diverso da quello specificato: il Comitato di Gestione si riserva di decidere l'ammissione sulla base dell'analisi del curriculum formativo e professionale che i candidati dovranno presentare con la domanda di ammissione al Master.
Inoltre, per i candidati stranieri è richiesta la conoscenza della lingua italiana, attestata da un certificato da allegare al momento della presentazione della domanda di ammissione.

Modalità di selezione: Per titoli e colloquio
L'ammissione avverrà sulla base di una graduatoria di merito formata attraverso i seguenti criteri di valutazione:

- **Breve relazione motivazionale** (max 1 cartella) a supporto della candidatura da inviare in fase di domanda di ammissione **(massimo 20 punti)**
- **Esperienze formative e professionali (massimo 25 punti)**
- **Prova orale (massimo 55 punti).**

L'accertamento delle competenze in ingresso e in uscita dal Master Universitario è affidato al Comitato di Gestione. L'ammissione al Master avverrà in conformità a una procedura di selezione effettuata da un'apposita Commissione nominata dal Comitato di Gestione.
Nel caso di pari merito verrà data preferenza al più giovane di età.

Nel dettaglio:

- **Breve relazione motivazionale** (max 1 cartella) a supporto della candidatura **(max 20 punti)** da inviare in fase di domanda di ammissione
  Il candidato dovrà presentare una relazione in cui vengano esposte le sue motivazioni a supporto della candidatura, con riferimento al progetto professionale che egli intende perseguire.
- E**sperienze formative e professionali (max 25 punti)**
  Valutazione della laurea (massimo 8 punti):
  - 5 punti per il voto di laurea pari a 110 e lode
  - 4 punti per il voto di laurea compreso tra 110 e 107
  - 3 punti per il voto di laurea compreso tra 106 e 103
  - 2 punti per il voto di laurea compreso tra 102 e 100
  - 1 punto per il voto di laurea pari o inferiore a 99
  - massimo 3 punti per la pertinenza della laurea

  Massimo 4 punti per altre esperienze formative pertinenti
  Massimo 3 punti per il possesso di ulteriori certificazioni (es. conoscenza dell'inglese e competenze informatiche di base)
  Valutazione delle esperienze professionali (max 10 punti)
  - 5 punti per le competenze specifiche acquisite attraverso attività professionali/di ricerca/stage
  - 5 punti per la pertinenza del settore di attività e/o il ruolo professionale per le persone occupate
- **Prova orale (max 55 punti).** La prova orale consisterà in un colloquio individuale volto ad individuare il possesso delle competenze di base per la frequenza del Master, nonché l'interesse e la motivazione rispetto agli obiettivi formativi del Master, le competenze eventualmente già possedute nel settore di riferimento, le attitudini professionali, le relazioni umane e la propensione a lavorare in team.

L'elenco ammessi al Master, ovvero coloro che avranno totalizzato **almeno 60 punti** tra la relazione, la valutazione delle esperienze formative e professionali e la prova orale, sarà stilata sulla base della somma dei punteggi.
Le selezioni si terranno nei giorni **24-25-26 settembre 2024**, il calendario e gli orari dei colloqui individuali saranno pubblicati a cura della Segreteria del master https://cybersecurity.master.unige.it/ entro il **20 settembre 2024**.
La selezione non verrà effettuata nel caso in cui il numero di candidati sia inferiore o pari al numero minimo dei posti disponibili.

Agevolazioni economiche e/o borse

Borse di studio INPS: il Master è accreditato al programma "Master INPS Executive" per l'ottenimento di 3 borse a copertura dei costi di iscrizione rivolte ai dipendenti della Pubblica Amministrazione, iscritti alla Gestione unitaria delle prestazioni creditizie e sociali di cui all'art. 1, comma 245, della legge 662/96 e in forza del D.M. 45/2007. Il Bando per accedere alle borse è reperibile sul sito INPS.

Qualora si rendessero disponibili ulteriori borse di studio, le informazioni saranno pubblicate nella sezione news della pagina del Master: https://cybersecurity.master.unige.it/.

Art. 6
Presentazione della domanda di ammissione

La domanda di ammissione al concorso deve essere presentata mediante la procedura on-line disponibile all'indirizzo https://servizionline.unige.it/studenti/post-laurea/master, entro **le ore 12:00 del 16 settembre 2024.**
La data di presentazione della domanda di partecipazione al concorso è certificata dal sistema informatico che, allo scadere del termine utile per la presentazione, **non permetterà più l'accesso e l'invio della domanda**.
Nella domanda il candidato deve autocertificare sotto la propria responsabilità, pena l'esclusione dal concorso:

a. il cognome e il nome, il codice fiscale, la data e il luogo di nascita, la residenza, il telefono ed il recapito eletto agli effetti del concorso. Per quanto riguarda i cittadini stranieri, si richiede l'indicazione di un recapito italiano o di quello della propria Ambasciata in Italia, eletta quale proprio domicilio. Può essere omessa l'indicazione del codice fiscale se il cittadino straniero non ne sia in possesso, evidenziando tale circostanza;
b. la cittadinanza;
c. tipo e denominazione della laurea posseduta con l'indicazione della data, della votazione e dell'Università presso cui è stata conseguita ovvero il titolo equipollente conseguito presso un'Università straniera nonché gli estremi dell'eventuale provvedimento con cui è stata dichiarata l'equipollenza stessa oppure l'istanza di richiesta di equivalenza ai soli fini del concorso di cui all'art. 4;

Alla domanda di ammissione al master devono essere allegati, mediante la procedura online:

1. fotocopia fronte/retro di un documento di identità;
2. curriculum vitae.
3. breve relazione di cui all'art.5.

Per confermare la domanda sarà necessario attestare la veridicità delle dichiarazioni rese spuntando l'apposita sezione prima della conferma della domanda.
I candidati che non riporteranno nella domanda tutte le indicazioni richieste saranno esclusi dalle procedure concorsuali.
L'Università può adottare anche successivamente all'espletamento del concorso, provvedimenti di esclusione nei confronti dei candidati privi dei requisiti richiesti.

Tutti gli allegati devono essere inseriti in formato PDF (la dimensione di ogni pdf non deve superare i 2 Megabyte).

Nel caso di titolo di studio conseguito all'estero, qualora il titolo non sia già stato riconosciuto equipollente, l'interessato deve chiederne l'equivalenza ai soli fini del concorso, allegando alla domanda i seguenti documenti:

- titolo di studio tradotto e legalizzato dalla competente rappresentanza diplomatica o consolare italiana del paese in cui è stato conseguito il titolo;
- "dichiarazione di valore" del titolo di studio resa dalla stessa rappresentanza.

Il provvedimento di equivalenza sarà adottato ai soli fini dell'ammissione al concorso e di iscrizione al corso.
Nel caso in cui la competente rappresentanza diplomatica o consolare italiana non abbia provveduto a rilasciare tale documentazione in tempo utile per la presentazione della domanda di ammissione, è necessario allegare alla domanda tutta la documentazione disponibile. L'eventuale provvedimento di equivalenza sarà adottato sotto condizione che la traduzione legalizzata e la "dichiarazione di valore" siano presentate entro il termine previsto per l'iscrizione ai corsi da parte dei candidati ammessi.
Il rilascio della suddetta documentazione e dell'eventuale permesso di soggiorno per la frequenza del corso ai cittadini stranieri è disciplinato dalle disposizioni del Ministero dell'Università e della Ricerca relative alle procedure per l'ingresso, il soggiorno e l'immatricolazione degli studenti stranieri/internazionali ai corsi di formazione superiore in Italia per l'a.a. 2023/2024.

Ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, alle dichiarazioni rese nella domanda di ammissione, nel caso di falsità in atti e dichiarazioni mendaci si applicano le sanzioni penali previste dall'art. 76 del decreto n. 445/2000 sopra richiamato. Nei casi in cui non sia applicabile la normativa in materia di dichiarazioni sostitutive (D.P.R. n. 445/2000 e ss.mm.ii), il candidato si assume comunque la responsabilità (civile, amministrativa e penale) delle dichiarazioni rilasciate.

L'Amministrazione si riserva di effettuare i controlli e gli accertamenti previsti dalle disposizioni in vigore. I candidati che renderanno dichiarazioni mendaci decadranno automaticamente dall'iscrizione, fatta comunque salva l'applicazione delle ulteriori sanzioni amministrative e/o penali previste dalle norme vigenti.

L'Amministrazione universitaria non assume alcuna responsabilità per il caso di smarrimento di comunicazioni dipendente da inesatte indicazioni della residenza e del recapito da parte dell'aspirante o da mancata oppure tardiva comunicazione del cambiamento degli stessi, né per eventuali disguidi postali o telegrafici non imputabili a colpa dell'Amministrazione medesima.

L'elenco degli ammessi sarà pubblicata sul sito cybersecurity.master.unige.it **entro il 30 settembre 2024.**
Non sono previsti rimborsi spese per gli iscritti.

Art. 7
Perfezionamento dell'iscrizione

I candidati ammessi al Master Universitario devono perfezionare l'iscrizione **entro le 23.59 del 10 ottobre 2024** mediante procedura online collegandosi alla pagina **https://servizionline.unige.it/studenti/post-laurea** cliccando su <<Conferme iscrizione post-laurea>> e scegliendo il Master la cui iscrizione deve essere confermata.
Alla conferma online dovranno essere allegati i seguenti documenti:

1. una fotografia a colori, formato tessera in formato JPG di dimensioni non superiori a 50Kb;

2. Ricevuta comprovante il versamento della **prima rata pari a € 282,00,** comprensiva delle **marche da bollo** (€ 16,00+€ 16,00) e del contributo universitario deliberato dagli Organi accademici per l'anno accademico 2023/2024 (€ 250,00).

Il pagamento è da effettuarsi online tramite il servizio bancario disponibile nell'Area dei Servizi online agli Studenti (https://servizionline.unige.it/studenti/unigepay20/), utilizzando una delle carte di credito appartenenti ai circuiti Visa, Visa Electron, CartaSì, MasterCard, Maestro o tramite "avviso di pagamento" cartaceo (pago PA).
Si invita a leggere attentamente la pagina web https://www.studenti.unige.it/tasse/pagamento_online/ (modalità di pagamento).
Nota bene: Il solo pagamento del contributo universitario non costituisce iscrizione al Master.

I candidati, che non avranno provveduto ad iscriversi entro il termine sopraindicato, di fatto saranno considerati rinunciatari.

Per gli occupati:
il pagamento della II rata di importo pari a **€ 2.500,00** dovrà essere effettuato secondo le modalità sopracitate **entro il 20 dicembre 2024**.
il pagamento della III rata di importo pari a **€ 2.500,00** dovrà essere effettuato secondo le modalità sopracitate **entro il 14 marzo 2025**

Per gli inoccupati:
Il pagamento della II rata di importo pari a **€ 1.250,00** dovrà essere effettuato secondo le modalità sopracitate **entro il 20 dicembre 2024**.
Il pagamento della III rata di importo pari a **€ 1.250,00** dovrà essere effettuato secondo le modalità sopracitate **entro il 14 marzo 2025.**

Successivamente all'iscrizione, i cittadini stranieri non ancora in possesso di codice fiscale italiano sono tenuti ad ottenerlo, rivolgendosi al Servizio Internazionalizzazione-Settore Welcome Office-Accoglienza Studenti e Utenti Internazionali: Telefono: (+39) 010 209 51525, E-mail: sass@unige.it.
Ai sensi dell'art. 8 comma 5 del Regolamento di Ateneo per gli Studenti, emanato con D.R. 641 del 9 febbraio 2023, pubblicato nell'albo informatico di Ateneo il 9 febbraio 2023, *"lo studente iscritto non ha diritto alla restituzione della contribuzione studentesca versata, anche se interrompe gli studi o si trasferisce ad altra Università, fatte salve le disposizioni del regolamento contribuzione studentesca e benefici universitari e delle delibere dell'Ente regionale per il diritto allo studio universitario".*

Art. 8
Rilascio del Titolo

A conclusione del Master, agli iscritti che a giudizio del Comitato di gestione abbiano superato con esito positivo la prova finale, verrà rilasciato il diploma di Master Universitario di II livello in *"Cybersecurity and Critical Infrastructure Protection"* come previsto dall'art. 19 del Regolamento dei Corsi di Perfezionamento, di aggiornamento professionale e di formazione e dei corsi per Master Universitari di primo e secondo livello.

Art. 9
Trattamento dei dati personali

Con riferimento alle disposizioni di cui al Regolamento UE 2016/679 (GDPR – *General Data Protection Regulation*) e al Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" concernente la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali i dati personali forniti dai candidati sono raccolti presso l'Università degli Studi di Genova per le finalità di gestione del concorso e sono trattati anche in forma automatizzata. Il trattamento degli stessi, per gli ammessi al corso, proseguirà anche successivamente all'avvenuta immatricolazione per le finalità inerenti alla gestione della carriera universitaria.
Il conferimento di tali dati è obbligatorio ai fini della valutazione dei requisiti di partecipazione, pena l'esclusione dal concorso.
Le informazioni fornite possono essere comunicate unicamente alle amministrazioni pubbliche direttamente interessate alla posizione universitaria dei candidati o allo svolgimento del concorso.
Gli interessati sono titolari dei diritti di cui agli artt. 16, 17, 18, 19 e 21 del Regolamento (UE) 2016/679, tra i quali figura il diritto di accesso ai dati che li riguardano, nonché alcuni diritti complementari tra cui il diritto di rettificare, aggiornare, completare o cancellare i dati erronei, incompleti o raccolti in termini non conformi alla legge, nonché il diritto di opporsi al loro trattamento per motivi legittimi.
Tali diritti possono essere fatti valere nei confronti dell'Università degli Studi di Genova – Via Balbi, 5 – 16126 Genova - Legale rappresentante: Rettore Prof. Federico Delfino titolare del trattamento.

IL RETTORE
Firmato digitalmente

Responsabile del procedimento: Sig.ra Marianna Modica
Per informazioni su procedure amministrative: Email: carrieremaster@unige.it
Per informazioni sulla didattica: master.cybersecurity@unige.it

Allegato 1 – Piano didattico

PARTE I – FORMAZIONE CULTURALE	Ore	CFU	SSD
Introduction to Cybersecurity	8	0,8	ING-INF/01
Computer Security	24	2,4	INF/01
Information Security Management and Legals	24	2,4	ING-INF/01
Network Security	28	2,8	ING-INF/03
Cryptography	24	2,4	INF/01
Totale Parte I		**10,80**	
PARTE II – FORMAZIONE PROFESSIONALE			
Security and Threats to Critical Infrastructure	12	1,2	ING-IND/31
Cryptographic Protocols	16	1,6	ING-INF/05
Blockchain Tecnologies	16	1,6	ING-INF/05
Web Security	20	2	ING-INF/05
Information Security & Risk Management	28	2,8	ING-INF/01
Business Continuity and Crisis Management	16	1,6	ING-INF/05
Informatica Legale, Privacy and Cyber Crime	36	3,6	IUS/01
Fundamentals of Computer Forensics	8	0,8	ING-INF/05
Cyber Security in Financial and Credit Systems	4	0,4	ING-INF/05
Cybersecurity in SCADA Systems, Industry, Power, and Energy	32	3,2	ING-INF/01, ING-INF/03
IoT Security	20	2	ING-INF/05
Defense-in-Depth Strategies for Critical Infrastructures	12	1,2	ING-INF/05
Standards and Best Practices for Security and Safety	16	1,6	ING-IND/31
Social Engineering and Intelligence for Cybersecurity	16	1,6	ING-INF/01
Totale Parte II		**25,2**	

PARTE III - SPECIALIZZAZIONI – INDIRIZZO I: Cyber Defence of IT/OT systems	**Ore**	**CFU**	**SSD**
Incident Response and Forensics Analysis	24	2,4	ING-INF/05
Malware Analysis	24	2,4	INF/01
Mobile Security	12	1,2	ING-INF/05
Cloud Security	12	1,2	ING-INF/05
Totale Parte III (Indirizzo I)		**7,2**	
PARTE III - SPECIALIZZAZIONI – INDIRIZZO II: *GRC for Critical Infrastructure Protection and the Enterprise*			
Cyber Defense and Cyber Intelligence	24	2,4	ING-INF/01
Standards for ISMS and BCMS Certification: ISO/IEC 27001, ISO 22301	24	2,4	ING-INF/05, ING-IND/31
Physical Security	12	1,2	ING-INF/01
Risk Propagation in Interconnected Infrastructures	12	1,2	ING-IND/31
Totale Parte III (Indirizzo II)		**7,2**	
TOTALE ORE DIDATTICA	**432**		
Project Work		**16,8**	
Totale CFU		**60**	

ATTIVITÀ	N. ORE	CFU
Lezioni	432	**43,2**
Studio individuale	648	
Project work	420	**16,8**
TOTALE	1500	**60**