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
SETTORE MASTER, TFA ED ESAMI DI STATO

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. 2025/2026;
- 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;
- 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 15 luglio 2025, con la quale è stata proposta la VIII edizione del Master Universitario di II livello in *"Cybersecurity and Critical Infrastructure Protection"* per l'a.a. 2025/2026;
- Visto il Decreto d'urgenza del Preside della Scuola Politecnica del 31 luglio 2025 con il quale è stata proposta l'attivazione della VIII edizione del Master Universitario di II livello in *"Cybersecurity and Critical Infrastructure Protection"* per l'a.a. 2025/2026;
- Viste le delibere del Senato Accademico in data 23 settembre 2025 e del Consiglio di Amministrazione in data 24 settembre 2025, con le quali è stata approvata la modifica della proposta istitutiva del Master universitario di secondo livello in *"Cybersecurity and Critical Infrastructure Protection";*

D E C R E T A

Art. 1
Norme Generali

È istituito per l'anno accademico 2025/2026 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"* – VIII Edizione**

Strutture che collaborano alla realizzazione del Master:
Strutture Università di Genova: Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni (DITEN) - Area ricerca, trasferimento tecnologico e terza missione - Servizio per il trasferimento tecnologico e delle conoscenze
Partner: Camelot *Biomedical System* – HWG Sababa – Leonardo *Cyber & Security Solutions – txOne networks*

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 gennaio 2026 a fine gennaio 2027.**

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.

Costo complessivo del Master: € 5.432,00 (per occupati) o € 2.932,00 (per inoccupati)
€ 5.000,00 + contributo universitario € 400,00 + 2 marche da bollo (€ 16,00 + € 16,00) per occupati per l'intero Master
€ 2.500,00 + contributo universitario € 400,00 + 2 marche da bollo (€ 16,00 + € 16,00) per disoccupati/inoccupati per l'intero Master

Agevolazioni economiche:
È stata fatta richiesta per rientrare tra i corsi di studio individuati nel Protocollo di intesa tra il Ministero per la Pubblica Amministrazione e l'Università degli Studi di Genova (PA110eLode), finalizzato a dare attuazione all'offerta formativa dedicata al personale in servizio presso le pubbliche amministrazioni. Pertanto, per i dipendenti in servizio presso una Pubblica Amministrazione, nel caso tale richiesta venisse accettata, sarà previsto l'esonero parziale del contributo universitario pari a € 330,00.
Gli aventi diritto devono compilare apposita autocertificazione, ai sensi del D.P.R. 445/2000, inerente il possesso del requisito, redatta secondo il modello disponibile nella procedura online (denominato "REQUISITO PA 110 E LODE").

Art. 4
Comitato di Gestione e Presidente

Presidente: Luca Verderame.
Vice Presidente: Rodolfo Zunino.
Docenti Unige del Comitato di Gestione: Luca Verderame, Rodolfo Zunino, Alessandro Armando, Marina Ribaudo, Paola Girdinio, Giovanni Lagorio, Mario Marchese, Enrico Russo.
Docenti esterni del Comitato di Gestione: Alessio Merlo, Cocurullo Fabio, Mattia Epifani, Ermete Meda, Massa Danilo, Antonio Rebora, Gaetano Sanacore.

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.

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.

<u>Nel dettaglio:</u>

- **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 **27 e 28 novembre 2025**, il calendario e gli orari dei colloqui individuali saranno pubblicati a cura della Segreteria del master https://cybersecurity.master.unige.it/ entro il **21 novembre 2025**.

Agevolazioni economiche e/o borse

Borse di studio INPS: il Master è accreditato al programma "Master INPS Executive" per l'ottenimento di borse di studio 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. Per le informazioni circa le modalità di accesso alle borse, ai criteri di eleggibilità, e ai bandi attivi, si rimanda al sito ufficiale INPS.

Borse di studio per Studenti Disoccupati/Inoccupati: sono disponibili **n.1 borse di studio offerta dall'azienda HWG Sababa e n.4 borse di studio offerte dall'azienda Leonardo.** Le borse di studio per studenti disoccupati/inoccupati a copertura dei costi di iscrizione verranno assegnate dalla Commissione Giudicatrice agli studenti in possesso del requisito di disoccupazione/inoccupazione secondo la graduatoria emessa sulla base della somma dei punteggi del processo di selezione. Gli studenti selezionati per le borse dovranno sostenere il solo costo delle marche da bollo (€ 16,00+€ 16,00) e del contributo universitario deliberato dagli Organi di Ateneo (ove dovuto) per l'anno accademico 2025/2026 (€ 400,00).

Art. 6
Presentazione della domanda di ammissione

La domanda di ammissione al concorso deve essere presentata mediante la procedura on-line, entro **le ore 12:00 del 17.11.2025.**
I candidati GIA' IN POSSESSO di credenziali UniGePass (matricola e password) potranno presentare domanda utilizzando il seguente *link*: https://servizionline.unige.it/studenti/post-laurea/master/domanda
I candidati che non hanno MAI POSSEDUTO le credenziali UniGePass (matricola e password) prima di utilizzare la procedura presente al *link* indicato precedentemente dovranno creare un utente utilizzando il seguente *link*: https://servizionline.unige.it/web-esterni2/it/#/registrazioneutente
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'equivalenza stessa oppure l'istanza di richiesta di equivalenza ai soli fini del concorso;
d. stato occupazione/disoccupazione/inoccupazione;

Alla domanda di ammissione al master devono essere allegati, mediante la procedura online:
1. fotocopia fronte/retro del documento di identità;
2. *curriculum vitae*;
3. breve relazione di cui all'art.5;
4. eventuale documentazione a supporto della richiesta di esonero totale dal versamento del contributo universitario deliberato dagli Organi di Ateneo per l'anno accademico 2025/2026, di cui all'art. 8 del presente bando.
5. Eventuale autocertificazione attestante requisito per Progetto PA 110 e lode redatta secondo il modello denominato "REQUISITO PA 110 E LODE". ATTENZIONE: Il modello di autocertificazione si trova all'interno della procedura informatica di presentazione della domanda di ammissione: selezionando la relativa voce nel menù a tendina della pagina in cui è richiesto di inserire gli allegati, comparirà una sezione in cui è presente il modello stesso.

Per confermare la domanda sarà necessario attestare la veridicità delle dichiarazioni rese spuntando l'apposita sezione prima della conferma della domanda.

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 o, in alternativa, può essere accettato l'attestato di verifica (*statement of verification*) rilasciato dal CIMEA;
- "dichiarazione di valore" del titolo di studio resa dalla stessa rappresentanza o, in alternativa, può essere accettato l'Attestato di comparabilità (*statement of comparability*) rilasciato dal CIMEA.

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'accesso degli studenti stranieri richiedenti visto ai corsi di formazione superiore per l'a.a. 2025/2026, disponibile all'indirizzo https://www.studiare-in-italia.it/studentistranieri/

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.

La pubblicazione della graduatoria sarà affissa presso https://cybersecurity.master.unige.it/ entro il **5 dicembre 2025.**
L'Università può adottare, anche successivamente all'espletamento del concorso, provvedimenti di esclusione nei confronti dei candidati privi dei requisiti richiesti.

Art. 7
Perfezionamento dell'iscrizione

I candidati ammessi al Master Universitario devono perfezionare l'iscrizione **entro le 23:59 del 16.12.2025** mediante procedura online all'indirizzo https://servizionline.unige.it/studenti/post-laurea/confermaPL 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 € 432,00,** comprensiva delle **marche da bollo** (€ 16,00+€ 16,00) e del contributo universitario deliberato dagli Organi accademici per l'anno accademico 2025/2026 (€ 400,00), qualora l'importo pagato non risultasse già nella procedura.

Il versamento può essere effettuato online utilizzando il Servizio pagoPA, oppure utilizzando i servizi offerti dalla Banca Popolare di Sondrio, istituto cassiere dell'Università di Genova. Non è possibile effettuare alcun pagamento mediante bonifico.
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 30.01.2026**
il pagamento della III rata di importo pari a **€ 2.500,00** dovrà essere effettuato secondo le modalità sopracitate **entro il 29.05.2026**

Per gli inoccupati:
Il pagamento della II rata di importo pari a **€ 1.250,00** dovrà essere effettuato secondo le modalità sopracitate **entro il 30.01.2026**
Il pagamento della III rata di importo pari a **€ 1.250,00** dovrà essere effettuato secondo le modalità sopracitate **entro il 29.05.2026**

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

Esoneri per disabilità

L'Ateneo riconosce l'esonero dal versamento del contributo universitario deliberato dagli Organi di Ateneo per l'anno accademico 2025/2026 (€ 400,00) agli studenti con disabilità, con riconoscimento di handicap ai sensi dell'art.3, Legge 104/1992 o con invalidità pari o superiore al 66%.
Lo studente dovrà allegare documentazione idonea a comprovare il diritto all'esonero, come previsto nell'art. 6 del presente bando.

Art. 9
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. 10
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
Prof. Federico DELFINO
Firmato digitalmente

Firmato digitalmente da FEDERICO DELFINO
Data: 02.10.2025 19:47:51 CEST
Organizzazione: Università degli Studi di Genova

Responsabile del procedimento: Sig.ra Marianna MODICA
Per informazioni: altaformazione@unige.it – Call center attivo lunedì, mercoledì e venerdì, ore 9–11. Tel.: 010 33 55 000 - digitare 6

Allegato 1 – Piano didattico

Modulo	Insegnamento	SSD	CFU Desiderati	CFU Verifica	UNIGE h docenza			Esterni h docenza			h studio individuale	Tot h docenza e Studio indiv.	H verifica apprendimento Modulo	
					Frontale	Distanza*		Frontale	Distanza*					
						Sincrone	Asincrone		Sincrone	Asincrone			Doc. UniGE	Doc. Esterna
Totali	-	-	**43,2**	**43,2**	**0**	**186**	**0**	**0**	**318**	**0**	**648**	**1080**	**0**	**0**
PARTE I – FORMAZIONE CULTURALE	1) Introduction to Cybersecurity	ING-INF/01	1,2	1,2		4			8		**18**	30		
	2) Computer Security	INF/01	2,4	2,4		16			8		**36**	60		
	3) Information Security Management and Legals	ING-INF/01	2,4	2,4					24		**36**	60		
	4) Network Security	ING-INF/03	2,8	2,8		28					**42**	70		
	5) Cryptography	INF/01	2,4	2,4		24					**36**	60		
PARTE II – FORMAZIONE PROFESSIONALE	6) Security and Threats to Critical Infrastructure	ING-IND/31	1,2	1,2		8			4		**18**	30		
	7) Cryptographic Protocols	ING-INF/05	1,6	1,6		12			4		**24**	40		
	8) Blockchain Tecnologies	ING-INF/05	1,6	1,6		12			4		**24**	40		
	9) Web Security	ING-INF/05	2	2,0		4			16		**30**	50		
	10) Information Security & Risk Management	ING-INF/01	2,8	2,8					28		**42**	70		
	11) Business Continuity and Crisis Management	ING-INF/05	1,6	1,6		0			16		**24**	40		
	12) Informatica Legale, Privacy and Cyber Crime	IUS/01	3,6	3,6		8			28		**54**	90		
	13) Fundamentals of Computer Forensics	ING-INF/05	0,8	0,8					8		**12**	20		
	14) Cyber Security in Financial and Credit Systems	ING-INF/05	0,4	0,4					4		**6**	10		
	15) Cybersecurity in SCADA Systems, Industry, Power, and Energy	ING-INF/01, ING-INF/03	3,2	3,2		8			24		**48**	80		

	16) IoT Security	ING-INF/05	2	2,0		8			12		**30**	50		
	17) Defense-in-Depth Strategies for Critical Infrastructures	ING-INF/05	0,8	0,8		8					**12**	20		
	18) Standards and Best Practices for Security and Safety	ING-IND/31	1,6	1,6					16		**24**	40		
	19) Social Engineering and Intelligence for Cybersecurity	ING-INF/01	1,6	1,6		16					**24**	40		
PARTE III SPECIALIZZAZIONI – INDIRIZZO I: Cyber Defence of IT/OT systems	20) Incident Response and Forensics Analysis	ING-INF/05	2,4	2,4					24		**36**	60		
	21) Malware Analysis	INF/01	2,4	2,4		4			20		**36**	60		
	22) Mobile Security	ING-INF/05	1,2	1,2		6			6		**18**	30		
	23) Cloud Security	ING-INF/05	1,2	1,2		6			6		**18**	30		
oppure (Gli allievi si suddividono in due aule dopo aver scelto l'indirizzo professionale di 72 ore da seguire) Il totale delle ore di didattica per ciascuno rimane di 432 ore.														
PARTE III SPECIALIZZAZIONI – INDIRIZZO II: GRC for Critical Infrastructure Protection and the Enterprise	20) Cyber Defense and Cyber Intelligence	ING-INF/01	2,4	2,4		10			14		**36**	60		
	21) Standards for ISMS and BCMS Certification: ISO/IEC 27001, ISO 22301	ING-INF/05, ING-IND/31	2,4	2,4					24		**36**	60		
	22) Physical Security	ING-INF/01	1,2	1,2					12		**18**	30		
	23) Risk Propagation in Interconnected Infrastructures	ING-IND/31	1,2	1,2		4			8		**18**	30		