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
SERVIZIO SEGRETERIE STUDENTI

DR n 1450 del 15 aprile 2021

IL RETTORE

- Vista la L. 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 "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;
- 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 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. 2020/2021;
- Visto il Regolamento recante la disciplina dei contratti di ricerca e di consulenza, delle convenzioni di ricerca per conto terzi emanato con D.R. n. 1551 del 5 maggio 2017;
- Vista la delibera del Consiglio di Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi- DIBRIS del 10 marzo 2021 con il quale è stato proposto il rinnovo del Master Universitario di II livello in "Cybersecurity and Critical Infrastructure Protection" – IV Edizione per l'a.a. 2021/2021;
- Visto il D.U. del Direttore del Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni – DITEN n 887 del 4 marzo 2021 con il quale esprime parere favorevole per il rinnovo del Master Universitario di II livello in "Cybersecurity and Critical Infrastructure Protection" – IV Edizione per l'a.a. 2020/2021;
- Vista la delibera del Consiglio di Scuola Politecnica del 16 marzo 2021 con il quale è stato proposto il rinnovo del Master Universitario di II livello in "Cybersecurity and Critical Infrastructure Protection" – IV Edizione per l'a.a. 2020/2021;

D E C R E T A

Art. 1
Norme Generali

È istituito per l'anno accademico 2020/2021 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" – IV Edizione per l'a.a. 2020/2021 .**

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:
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. In particolare, il Master si pone i seguenti obiettivi strategici:

- Fornire un insieme completo di nozioni fondamentali di Cybersecurity a laureati magistrali in materie legate all'ICT, al fine di incrementare la preparazione dei laureati su tali tematiche emergenti.
- Fornire competenze sulla governance della Cybersecurity e delle relative procedure a livello aziendale o di infrastruttura critica, in modo da potenziare la formazione professionale degli studenti anche con conoscenze approfondite sulle "best practice", con l'obiettivo di agevolare un inserimento rapido ed efficace degli studenti stessi in un contesto aziendale.

- Fornire nozioni in ambito legale sulla Cybersecurity, affinché lo studente sappia prendere decisioni in tale contesto non solo dal punto di vista tecnico ma anche considerando l'impatto legale che le scelte fatte possano avere sull'azienda nelle sedi legali.
- Fornire capacità pratiche e padronanza operativa di soluzioni e prodotti allo stato dell'arte nello scenario moderno di Cybersecurity. A tal fine, molti moduli del Master includono parti pratiche finalizzate ad incrementare le capacità pratiche dello studente. Lo scopo di questa dimensione operativa è di colmare il gap con l'attuale preparazione universitaria che tende, anche in ambito Cybersecurity, ad essere sbilanciata verso la teoria a scapito della applicazione pratica. Anche in questo caso la preparazione su strumenti e tool allo stato dell'arte ha lo scopo di migliorare la facilità di inserimento in azienda.
- Fornire conoscenze e competenze sulla protezione delle Infrastrutture Critiche in termini sia teorici sia pratici. Questo ambito include aspetti emergenti quali le tecnologie SCADA, Web Security, Mobile Security, IoT Security, ecc. Lo scopo è rendere lo studente operativo in un elevato e svariato numeri di scenari attuali, in modo che sia flessibile e facilmente inseribile nella realtà aziendale in cui verrà coinvolto.

Il raggiungimento dei precedenti obiettivi formativi permette di colmare il gap di formazione e preparazione evidenziato nella sezione precedente, permettendo, con un solo anno di formazione aggiuntiva, di creare professionisti di Cybersecurity pronti all'inserimento in un contesto aziendale, alleviando le aziende o le istituzioni dalla necessità di formare internamente le persone, con costi aggiuntivi e spesso tempi di formazione insostenibili.

Profili funzionali:
L'inizio di questo millennio ha visto affermarsi l'Information Technology e, con essa, le prime problematiche di sicurezza, con rischi perlopiù inizialmente legati alla protezione dei dati aziendali. Da allora, il continuo sviluppo tecnologico ha portato l'Information Technology a diventare fruibile sia a livello di utenza personale (smartphone, wearable devices, ...) che professionale (e.g., BYOD). Inoltre, negli ultimi anni l'Information Technology è diventata completamente pervasiva nella collettività (e.g., Smart Cities) e nell'industria (e.g., Industria 4.0) e nuovi paradigmi architetturali continuano ad emergere, come l'Internet of Things (IoT).
Se da un lato l'avvento di tali nuove tecnologie nella vita privata e lavorativa di tutti i giorni è stato molto rapido, dall'altro ha costituito inedite problematiche di sicurezza che devono essere gestite adeguatamente. La caratteristica di tali nuovi problemi di (cyber-) sicurezza è di essere trasversali coinvolgendo diverse tecnologie, dispositivi e contesti. Al tempo stesso, una mancanza di consapevolezza o una debolezza in termini di Cybersecurity può comportare impatti molto più devastanti che in passato: ad esempio, un attacco informatico perpetrato ai danni di un'infrastruttura critica (e.g., fornitore di energia elettrica) potrebbe portare alla sospensione della fornitura per giorni ed in diverse regioni di un paese. Pertanto, le Istituzioni e le aziende percepiscono sempre più il bisogno di nuovi esperti di sicurezza, pronti per sviluppare soluzioni efficaci per la protezione delle infrastrutture strategiche aziendali e, di conseguenza, anche del business ad esse collegato.
Tutto il comparto produttivo odierno è in qualche modo legato al mondo dell'Information and Communication Technology (ICT), avendo nelle proprie infrastrutture digitali e soprattutto nei propri dati un valore e un asset strategico. Le aziende hanno quindi assunto la consapevolezza di essere costantemente esposte a minacce cyber e, al contempo, hanno chiara evidenza del fatto che il loro comparto di esperti ICT debba essere incrementato con esperti di sicurezza aggiornati e affidabili. Una recente dimostrazione di questo è stata la diffusione di malware che attaccano direttamente le aziende e le loro infrastrutture critiche (e.g., Mirai, WannaCry, ...) ed il cui impatto in molte realtà aziendali è stato devastante. Tali malware riescono a raggiungere le reti aziendali a causa di: a) una ridotta sensibilità alle minacce informatiche da parte del personale aziendale, e b) inadeguate conoscenze e competenze di Cybersecurity da parte degli amministratori di sistema e del personale aziendale addetto alla sicurezza.
Per questo motivo, 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:
La natura varia e molteplice delle Aziende che aderiscono al Master evidenzia l'ampio spettro di ricadute occupazionali legate al conseguimento del titolo del Master. Indagini indipendenti (Capital, Nro 447-448, sett/ott 2017) a livello nazionale evidenziano l'alto assorbimento di personale con profonde conoscenze in ambito Cybersecurity da parte di tutto il comparto produttivo. 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 Corso

Il corso, della durata di 12 mesi, si svolge **da luglio 2021 a giugno 2022**.
Al corso sono attribuiti 60 CFU.

Sede di svolgimento dell'attività didattica: Università degli Studi di Genova. a causa della situazione pandemica, il master sarà erogato online tramite la piattaforma Microsoft Teams. Un'eventuale erogazione parziale in presenza potrà essere presa in considerazione durante l'anno, in relazione all'evoluzione pandemica e la relativa normativa nazionale

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.

Numero minimo per l'attivazione: 12 iscrizioni.
Il Comitato di Gestione valuterà la possibilità di ridurre i costi di gestione ad un livello corrispondente a quello dei proventi, come condizione per svolgere il Master.

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. L'esame consisterà in un test scritto e/o orale nella forma più consona al modulo a discrezione del docente (prova scritta, test a risposta multipla, esercizio, interrogazione orale). Ciascun test si articola al massimo su tre ore ed è programmato almeno una settimana dopo la chiusura del modulo, al fine di permettere agli allievi di studiare ed assimilare i contenuti.
Per ogni esame di modulo sarà formata una commissione d'esame composta dal titolare del modulo (o suo delegato) e da un altro docente o esperto della materia nominato dal Comitato di Gestione su proposta del titolare del modulo. I membri della commissione saranno presenti al momento dell'esame. 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.
L'attività svolta sarà documentata in una relazione che introduce l'argomento e il problema affrontato, delinea il metodo seguito per la soluzione ovvero il percorso seguito per estendere le metodologie, e descrive i risultati ottenuti. Ogni progetto sarà seguito da un relatore, di norma docente del Master; eventuali eccezioni con relatori non inclusi fra i docenti del master dovranno essere approvate dal Comitato di Gestione.
La votazione finale sarà in centodecimi.

Monitoraggio e valutazione
Al termine di ogni insegnamento sarà sottoposto ad ogni studente un questionario valutativo. Inoltre, è prevista la compilazione di un questionario generale sul Master a fine percorso, con specifiche domande sul gradimento delle attività di stage e tesi.
Infine, un tutor sarà messo a disposizione degli studenti durante tutta la durata del Master. Il tutor seguirà lo svolgimento del Master ed interagirà costantemente con gli studenti e con i docenti, al fine di gestire eventuali problematiche e valutare l'andamento del percorso di studi.

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 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: € 6.766,00 (per occupati) o € 2.766,00 (per inoccupati)
€ 6.500,00+ contributo universitario € 250,00 e marca da bollo (€ 16,00) per occupati per l'intero Master
€ 2.500,00+ contributo universitario € 250,00 e marca da bollo (€ 16,00) per inoccupati per l'intero Master

Rateizzazione
E' possibile richiedere la rateizzazione dell'importo in 3 tranche, di cui una contestuale all'iscrizione. Eventuali richieste sono da inviare a popia@perform.unige.it.

Art. 4
Comitato di Gestione e Presidente

Presidente: Alessio Merlo
Vice Presidente: Rodolfo Zunino
Componenti Unige del Comitato di Gestione: Alessio Merlo (DIBRIS); Alessandro Armando (DIBRIS), Rodolfo Zunino (DITEN), Giovanni Chiola (DIBRIS), Paola Girdinio (DITEN), Giovanni Lagorio (DIBRIS), Mario Marchese (DITEN), Enrico Russo (DIBRIS).
Componenti esterni del Comitato di Gestione: Cocurullo Fabio (Leonardo), Mattia Epifani (RealityNet), Ermete Meda (Cyber Security Information Expert), Massa Danilo (RCS), Silvio Ranise (FBK), Antonio Rebora (Ansaldo Energia), Danilo Moresco (ABB), Gaetano Sanacore (A2A).
Delegato della struttura cui è affidata la gestione amministrativa, organizzativa e finanziaria: Alessia Popia (Settore Gestione Progetti)
Struttura Unige cui è affidata la gestione amministrativa, organizzativa e finanziaria del Master: Università degli Studi di Genova, Area Internazionalizzazione, Ricerca e Terza missione, Servizio Rapporti con imprese e territorio, Settore Gestione progetti

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).

Eventuali altri requisiti: possono accedere altresì coloro che, 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.

Modalità di ammissione:
L'ammissione al corso avverrà in conformità a una procedura di selezione effettuata da un'apposita Commissione nominata dal Comitato di Gestione.

Contribuiranno alla valutazione del candidato:

- **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. In caso di candidato dipendente pubblico che intenda accedere alle agevolazioni INPS, descritte all'articolo 6 del presente bando, la relazione dovrà pervenire dall'amministrazione di appartenenza e deve contenere le motivazioni a supporto della candidatura, anche con riferimento alle particolari caratteristiche professionali del dipendente.
- 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.

La graduatoria finale dei candidati idonei, 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 riportati nella valutazione delle esperienze formative e nella prova orale.

Il calendario delle selezioni sarà pubblicato a cura della Segreteria del master entro la chiusura del bando.
La selezione non verrà effettuata nel caso in cui il numero di candidati sia inferiore o pari al numero minimo dei posti disponibili

Nel caso di pari merito verrà data preferenza al più giovane di età.

Eventuali agevolazioni economiche e/o borse

Borse di studio INPS (ex I.N.P.D.A.P.) e SNA
Il Master ha ottenuto l'accreditamento INPS e SNA. Sono state erogate **n. 4 Borse INPS** a sostegno di attività di qualificazione, riqualificazione e aggiornamento professionale dei dipendenti pubblici e di **1 Borsa SNA** per dipendenti pubblici che abbiano la qualifica di dirigenti o funzionari e siano appartenenti ai ruoli ed in servizio presso una delle seguenti amministrazioni pubbliche: a) Organi costituzionali e di rilievo costituzionale; b) Presidenza del Consiglio dei ministri e Ministeri; c) Agenzie fiscali; d) Autorità amministrative indipendenti; e) Istituto nazionale infortuni sul lavoro -INAIL; f) Istituto nazionale previdenza sociale - INPS; g) Istituto nazionale di statistica -ISTAT
L'importo unitario della Borsa è di € 6.500,00 a copertura dell'iscrizione al Master (escluse le tasse universitarie).
Le borse saranno erogate a coloro in possesso dei requisiti, in ordine di graduatoria.
Il Bando sarà reperibile sul sito internet dell'INPS al link che verrà indicato sul sito https://www.perform.unige.it/master/master-cybersecurity

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 dell'11 giugno 2021.**
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 equipollenza 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.
4. solo per i dipendenti pubblici che intendono accedere all'agevolazione INPS: nulla osta da parte dell'Amministrazione di appartenenza, una relazione della stessa amministrazione in cui sono esposte le motivazioni che supportano la candidatura, anche con riferimento alle particolari caratteristiche professionali del dipendente e la dichiarazione con cui esprimono un ordine di preferenza per l'assegnazione del contributo INPS o SNA.

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.

Nel caso di titolo di studio conseguito all'estero, qualora il titolo non sia già stato riconosciuto equipollente, l'interessato deve chiederne l'equipollenza 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 equipollenza 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 equipollenza 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. 2020/2021.

I cittadini stranieri non ancora in possesso del codice fiscale, lo potranno ottenere rivolgendosi al Servizio Internazionalizzazione-Settore Accoglienza Studenti Stranieri (SASS): Telefono: (+39) 010 209 51525, E-mail: sass@unige.it.

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 graduatoria degli ammessi sarà pubblicata sul sito https://www.perform.unige.it/master/master-cybersecurity **entro il 24 giugno 2021.**

I candidati che non riporteranno nella domanda tutte le indicazioni richieste saranno esclusi dalle prove.
L'Università può adottare anche successivamente all'espletamento del concorso, provvedimenti di esclusione nei confronti dei candidati privi dei requisiti richiesti.

Non sono previsti rimborsi spese per gli iscritti.

Art. 7
Perfezionamento dell'iscrizione

I candidati ammessi al Master Universitario devono perfezionare l'iscrizione **entro il 29 giugno 2021** 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. n. 1 foto tessera in formato jpg.
2. ricevuta comprovante il versamento dell'importo dovuto, comprensivo dell'imposta di bollo e del contributo universitario per l'a.a. 2020/2021 deliberato dagli Organi accademici.

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.

Successivamente all'iscrizione, i cittadini stranieri non ancora in possesso di **codice fiscale italiano** sono tenuti ad ottenerlo, rivolgendosi al Servizio Internazionalizzazione-Settore Accoglienza Studenti Stranieri (SASS): Telefono: (+39) 010 209 51525, e-mail: sass@unige.it.

Ai sensi dell'art. 11 comma 3 del Regolamento per gli Studenti emanato con D.R. 228 del 25.09.2001 e successive modifiche, lo studente iscritto ad un corso universitario non ha diritto alla restituzione delle tasse e dei contributi versati, anche se interrompe gli studi o si trasferisce ad altra Università.

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

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

I dati personali forniti dai candidati saranno raccolti dall'Università degli Studi di Genova, Area Didattica, e trattati per le finalità di gestione della selezione e delle attività procedurali correlate, secondo le disposizioni del Regolamento UE 2016/679 (GDPR – General Data Protection Regulation) e D.L.vo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali".

IL RETTORE
Firmato digitalmente

Responsabile del procedimento: Dott.ssa Ilaria Mantegazza
Per informazioni: 0102099691 – 0102099636

Allegato 1 – Piano didattico

Modulo	SSD	CFU	Ore di didattica
PARTE I - FORMAZIONE CULTURALE			
Introduction to Cybersecurity	ING-INF/01	0,8	8
Computer Security	INF/01	3	30
Information Security Management and Legals	ING-INF/01	2,4	24
Network Security	ING-INF/03	3	30
Cryptography	INF/01	2,4	24
Totale		**11,6**	**116**
PARTE II - FORMAZIONE PROFESSIONALE			
Security and Threats to Critical Infrastructure	ING-IND/31	1,2	12
Cryptographic Protocols & Blockchain Technologies	ING-INF/05	2,4	24
Web Security	ING-INF/05	2	20
Information Security & Risk Management	ING-INF/01	2,8	28
Business Continuity and Crisis Management	ING-INF/05	1,6	16
Informatica Legale, Privacy and Cyber Crime	IUS/01	3,6	36
Fundamentals of Computer Forensics	ING-INF/05	0,8	8
Cyber Security in Financial and Credit Systems	ING-INF/05	0,4	4
Cybersecurity in SCADA Systems, Industry, Power, and Energy	ING-INF/01, ING-INF/03	3	30
IoT Applications Security	ING-INF/05	2	20
Defense-in-Depth Strategies for Critical Infrastructures	ING-INF/05	1,2	12
Standards and Best Practices for Security and Safety	ING-IND/31	1,8	18
Social Engineering and Intelligence for Cyber Security	ING-INF/01	1,6	16
Totale:		**24,4**	**244**
PARTE III - SPECIALIZZAZIONI - INDIRIZZO I: Cyber Defence of IT/OT Systems			
Incident Response and Forensics Analysis	ING-INF/05	2,4	24
Malware Analysis	INF/01	2,4	24
Mobile Security	ING-INF/05	1,2	12
Cloud Security	ING-INF/05	1,2	12
Totale:		**7,2**	**72**
PARTE III - SPECIALIZZAZIONI - INDIRIZZO II: GRC for Critical Infrastructure Protection and the Enterprise			
Cyber Defense and Cyber Intelligence	ING-INF/01	2,4	24
Standards for ISMS and BCMS Certification: ISO/IEC 27001, ISO 22301	ING-INF/05, ING-IND/31	2,4	24
Physical Security	ING-INF/01	1,2	12
Risk Propagation in Interconnected Infrastructures	ING-IND/31	1,2	12
Totale:		**7,2**	**72**
ATTIVITÀ	**N. ORE**	**CFU**	
Lezioni	432	43,2	
Studio individuale	648		
Project work	420	16,8	
TOTALE	1500	60	