UNIVERSITA' DEGLI STUDI DI GENOVA
AREA DIDATTICA E STUDENTI
SERVIZIO ALTA FORMAZIONE

D.R. n. 406

IL RETTORE

- Vista la L. 15.5.1997, n. 127, pubblicata nel supplemento ordinario alla G.U. n. 113 del 17.5.1997 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. 551 del 10.02.2015;
- Viste le disposizioni del Ministero dell'Università e della Ricerca del 22.03.2016 relativa alle procedure per l'accesso degli studenti stranieri richiedenti il visto ai corsi di formazione superiore per l'a.a. 2016/2017;
- Visto il Regolamento recante la disciplina dei contratti di ricerca e di consulenza, delle convenzioni di ricerca per conto terzi nonché del procedimento di conferimento di incarichi interni retribuiti ai docenti emanato con D.R. n. 417 del 3.10.2011;
- Visto il parere favorevole espresso dal Senato Accademico in data 18.11.2014;
- Visto il parere favorevole espresso dal Consiglio di Amministrazione in data 19.11.2014;
- Visto il Decreto d'urgenza del Direttore del Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS) dell'Università degli Studi di Genova n. 5 del 26.01.2017 con il quale è stato proposto il rinnovo del Master Universitario di II livello in "Cyber-Security and Data Protection" III edizione;
- Visto il Decreto d'urgenza del Direttore del Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni (DITEN) dell'Università degli Studi di Genova n. 259 del 27.01.2017 con il quale è stato proposto il rinnovo del Master Universitario di II livello in "Cyber-Security and Data Protection" III edizione;
- Visto il Decreto d'urgenza del Preside della Scuola Politecnica n. 320/2017 del 03.02.2017 con il quale esprime parere favorevole al rinnovo del Master Universitario di II livello in "Cyber-Security and Data Protection" III edizione;

D E C R E T A

Art. 1
Norme Generali

È attivato per l'anno accademico 2016/2017 presso il Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni (DITEN) (capofila) e il Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS) (associato) il Master Universitario di II livello in "**Cyber-Security and Data Protection**" III edizione.
Il Master è realizzato in collaborazione con: ISICT, Fondazione Ansaldo.

Art. 2
Finalità del Master

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) preposti alla tutela della sicurezza e alla protezione del patrimonio informativo di un'organizzazione.

Se nel recente passato la rilevanza strategica dell'Information Technology comportava rischi legati alla protezione dei dati aziendali, oggi la nascita di un nuovo mondo virtuale, il Cyber-Space, formato dall'interazione di persone, organizzazioni, software e servizi che condividono lo stesso ambiente di comunicazione Internet mediante dispositivi e reti di connessione di molteplice natura, richiede non solo lo sviluppo di sistemi di protezione e di segregazione ancora più raffinati per migliorare la sicurezza dei prodotti e la qualità dei servizi ma anche la definizione di un modello integrato ed efficace di gestione della sicurezza complessivo.

In base all'evoluzione degli scenari, delle minacce e dei rischi, in ogni infrastruttura di ICT, sia essa mezzo con cui le organizzazioni gestiscono i propri processi di business oppure componente di impianti di automazione industriale, due sono le discipline che devono essere ben conosciute e correttamente applicate al fine di assicurarne adeguata protezione: Cyber-Security e Data Protection.

L'unificazione del Cyber-Space richiede che queste due discipline diventino pervasive e patrimonio di tutti coloro che sono chiamati a proteggere i sistemi informativi, in settori anche molto diversi: il commercio elettronico, i servizi di Internet banking, le frodi informatiche, la privacy delle comunicazioni interpersonali, la difesa dal furto di identità digitale, la difesa informatica di grandi infrastrutture (es. ferrovie, porti e aeroporti), l'investigazione digitale, la prevenzione antiterrorismo fino al supporto alle forze dell'ordine per la risposta alle cyber-minacce, la conformità a normative internazionali di settore e la certificazione.

Il Master si contraddistingue con un progetto formativo innovativo sia per i contenuti sia per le metodologie didattiche adottate e particolarmente adatto a soddisfare le esigenze delle imprese. Per questo motivo si è fatta particolare attenzione nel coniugare l'esperienza di realtà aziendali d'avanguardia e di professionisti di provata esperienza con la rigorosità concettuale, la capacità di modellizzazione e sistematizzazione dei problemi propria del mondo accademico.

La terza edizione del Master mira a consolidare il presidio del nostro Ateneo su temi di così grande rilevanza, attirando anche risorse e discenti al di fuori della realtà locale. Infatti nell'edizione qui proposta si integrano contributi di grandi realtà di rilievo nazionale interessanti il settore bancario ed energetico, aumentando in tal modo il palinsesto di competenze offerte ai discenti per una professionalizzazione più efficace e approfondita.

Obiettivo specifico del Master è infatti la preparazione interdisciplinare di un esperto nella Cyber Security e nella Protezione dei Dati che, avendo acquisito nella prima parte del corso conoscenze approfondite di base teorico/pratiche per la protezione delle informazioni, possa apprendere, nella seconda parte, come applicarle correttamente, adottando e gestendo contromisure e strumenti adeguati alle necessità, in conformità con le migliori pratiche e le normative vigenti.

Profili funzionali:
Il Master forma esperti nella progettazione di strumenti e contromisure di Cyber Security e Data Protection in grado di applicare le conoscenze acquisite nell'ambito di un Sistema di Gestione della Sicurezza delle

Informazioni che comprende dunque, come discipline complementari, i modelli organizzativi, gli aspetti legali, i requisiti di conformità e certificazione.

Il Master è dedicato a chi intende ricoprire il ruolo di Information/ICT Security Manager o Chief Info Security Manager e a chi desidera diventare specialista e consulente in quest'area: pertanto destinatari naturali del Master sono tutti coloro che, occupati e non, dovranno operare come specialisti e/o consulenti per piccole, medie e grandi imprese industriali, di servizi e della Pubblica Amministrazione.

Alcune importanti caratteristiche di rilievo della terza edizione qui proposta consistono, da un lato, nella copertura di aspetti di Cyber Security nel sistema Bancario, di grande attualità e rilevanza per la criticità delle tematiche e della casistica coinvolte; dall'altro, nell'approfondimento di aspetti di Cyber Intelligence che rivestono una importanza sia dal punto di vista della protezione infrastrutture critiche (threat intelligence e early prevention) sia nel settore professionale e commerciale, dove gli strumenti di Open Source Intelligence ormai costituiscono una dotazione professionale standard.

Particolare attenzione è dedicata a due specializzazioni verticali, approfondite nella parte conclusiva del Master: " Vulnerability Assessment & Penetration Testing" e "Critical Infrastructure Protection and Security Assurance". Questa doppia valenza permette di estendere l'utilità del Master anche a ulteriori figure professionali, quali esperti di sicurezza per sistemi ICT appartenenti ad infrastrutture critiche ed esperti di Computer Forensics e Networking.
Queste figure professionali devono avere padronanza delle tecnologie ICT e delle vulnerabilità e minacce a cui queste sono esposte. Devono saper stimare gli effetti potenziali di tali attacchi sulle infrastrutture tecnologiche e sul patrimonio informativo ed essere in grado di individuare i sistemi di prevenzione più adatti e le contromosse più appropriate, considerando sia requisiti interni all'organizzazione, sia opportunità suggerite dalle best practice, sia vincoli imposti dagli *stakeholders*.

Al termine del percorso formativo lo specialista sarà quindi in grado di analizzare in dettaglio la situazione "as is" riguardante gli aspetti tecnologici, organizzativi e legali in modo da poter valutare le necessarie e sostenibili contromisure da adottare per la prevenzione, il monitoraggio e la gestione degli incidenti.

In particolare il Master fornisce gli strumenti concettuali e le competenze tecnico/scientifiche adatte a soddisfare le esigenze di diverse figure professionali:

- i laureati in scienze matematiche e fisiche per completare il proprio profilo con conoscenze e competenze più legate all'ingegneria ed alla ricerca tecnologica;
- i laureati in informatica e ingegneria per verticalizzare la loro specializzazione su specifiche tematiche ritenute "core business" dalle aziende leader del settore nonché per avere la possibilità di essere immediatamente allocati su progetti di rilevante complessità tecnologica.

E' evidente come l'impatto del Master sul percorso di carriera degli allievi debba essere valutato in una prospettiva di medio-lungo periodo, ovvero in termini di:

- auto-realizzazione, negli anni successivi al diploma di Master, rispetto alle proprie vocazioni tecniche e professionali;
- maggior velocità nel processo di maturazione da "junior" a "senior";
- capacità di mantenimento di un elevato livello di specializzazione tecnica e di un agevole auto-rinnovamento delle conoscenze tecnologiche negli anni successivi;
- capacità di conversione professionale per personale già occupato.

Sbocchi occupazionali:
Le edizioni precedenti del Master hanno connotato questa iniziativa con un considerevole successo, dal momento che i discenti hanno trovato sbocco occupazionale nelle aziende che hanno supportato il Master stesso, preliminarmente con forma di Project Work poi consolidatosi in alcuni casi con Contratti di Lavoro a tempo indeterminato.

Come evidenziato dai rapporti del CLUSIT (www.clusit.it) le aziende italiane hanno aumentato la loro sensibilità ai problemi di sicurezza informatica, così come gli addetti alla cybersecurity. Prevalgono, tra le figure professionali richieste, quelle a forte contenuto tecnico: Security Architect, Security Developer, Security Admin, Security DBA.

Art. 3
Organizzazione didattica del Corso

Il Corso della durata di 12 mesi si svolge dal 30 marzo 2017 al 30 marzo 2018. Il Master prevede 1500 ore di formazione così suddivise:

1. 428 ore di attività didattica in aula o in laboratorio
2. 922 ore di studio e approfondimento individuale
3. 150 ore tirocinio e preparazione della tesi finale

Al corso sono attribuiti 60 CFU.

Articolazione didattica:

L'articolazione del programma delle attività formative si struttura in tre parti principali:

Parte I - Formazione Culturale:
1. Introduction to Cyber Security
2. Cryptographic Protocols
3. Information Security Management and Legals
4. Network security
5. Computer security

Parte II - Formazione professionale:
6. Information Security Management
7. Business Continuity and Crisis Management
8. Legal Informatics, Privacy and Cyber Crime
9. Fundamentals of Computer Forensics
10. Cryptography
11. Cyber Security in Credit System, Management in Incident Response
12. Cybersecurity of SCADA Systems
13. Social Engineering and Intelligence for Cyber Security
14. Mobile and Cloud Security

Parte III – Specializzazioni:
Indirizzo 1: Vulnerability Assessment & Penetration Testing
Indirizzo 2: Critical Infrastructure Protection and Security Assurance

La tabella seguente riporta il Piano Didattico previsto, suddiviso in tre parti: Formazione Culturale, Formazione Professionale e due possibili Specializzazioni. La scelta dell'indirizzo specialistico verrà effettuata dagli studenti al termine della seconda parte. Ciascuno dei due indirizzi specialistici si concluderà con un'esercitazione pratica di Cybersecurity (Cyber Exercise).

Sono previsti percorsi personalizzati per l'eventuale recupero di conoscenze di base relative al settore ICT e rendere omogenee le conoscenze di base nell'elettronica, l'informatica e le telecomunicazioni a seconda delle esigenze dei singoli partecipanti. Verrà reso disponibile materiale didattico da discutere singolarmente con un docente di ogni settore a cui chiedere chiarimenti e spiegazioni.

Piano didattico

	Modulo	SSD	CFU	h Univ	h Esterni	Docenti	Tot. h Docenza
	Parte I: Formazione Culturale						
I.1	Introduction to Cyber Security	ING-INF/01	2	8	8	Zunino(8), Meda(8)	16
I.2	Cryptographic Protocols	ING-INF/05	2	8	8	Armando, Carbone	16
I.3	Information Security Management and Legals	ING-INF/01	3	0	24	Meda, Bassoli	24
I.4	Network Security	ING-INF/03	4	16	16	Aiello, Chiola, Marchese, Fortinet, Digipoint	32
I.5	Computer Security	INF/01	4	32	0	Chiola, Lagorio, Ranise	32
	TOTALE		**15**	**64**	**56**		**120**
	Parte II: Formazione Professionale						
II.1	Information Security Management	ING-INF/01	4	0	32	Meda, Ferretti	32
II.2	Business Continuity and Crisis Management	ING-INF/05	3	0	24	Buson, Cerasoli, Vodafone, BT	24
II.3	Legal Informatics, Privacy and Cyber Crime	IUS/01	4	4	28	Bassoli, Losengo, Pol.Postale, Zunino, Bosco	32
II.4	Fundamentals of Computer Forensics	ING-INF/05	1	0	8	Aizoon, RealityNet	8
II.5	Cryptography	INF/01	4	32	0	Chiola, Lagorio, Zunino	32
II.6	Cyber Security in Credit System, Management in Incident Response	ING-INF/01	2	0	16	Protiviti, UniCredit	16
II.7	Cybersecurity of SCADA Systems	ING-INF/01	1	0	12	AEN, Deloitte-Intellium	12
II.9	Social Engineering and Intelligence for Cyber	ING-INF/01	2	20	0	Zunino	20

	Security						
II.10	Mobile and Cloud Security	ING-INF/05	2	20	0	Digipoint, Zunino, Costa	20
	TOTALE		**23**	**76**	**120**		**196**
	Parte III: Specializzazioni						
IN1	**Indirizzo 1: Vulnerability Assessment & Penetration Testing**						
IN1.1	Incident Response and Forensics Analysis	ING-INF/05	4	0	32	Massa, Epifani, Picasso, Meda	32
IN1.2	Malware Analysis	INF/01	3	12	12	Massa, Lagorio	24
IN1.3	Web Security	ING-INF/05	3	16	8	Meucci, Valenza, Merlo	24
IN1.4	Mobile Security	ING-INF/05	3	16	8	Costa, Verderame, Aonzo	24
IN1.5	Cyber Exercise	ING-INF/05	3	8		Valenza	8
	TOTALE		**16**	**52**	**60**		**112**
IN2	**Indirizzo 2: Critical Infrastructure Protection and Security Assurance**						
IN2.1	ICT for Critical Infrastructure Protection	ING-INF/01	2	12	4	Zunino, Meda, DIGI	16
IN2.2	Cyber Defense and Cyber Intelligence	ING-INF/01	2	4	12	Zunino, AEN, TigerSecurity	16
IN2.3	SCADA and Industrial Systems Protection	ING-INF/01	4	0	32	ABB, AEN, Papaleo, Pinceti	32
IN2.4	The ISO27001 Standard	ING-INF/01	2	0	16	Cerasoli, IBM	16
IN2.5	Governance Finance	ING-INF/05	1		8	Deloitte	8
IN2.6	Security Assurance	ING-INF/05	2	0	16	Deloitte-Intellium, Meda, HP, IFINET	16
IN2.7	Cyber Exercise	ING-INF/01	3	8		Zunino	8
	TOTALE		**16**	**24**	**88**		**112**
	Stage and Thesis		6	0	0		0
	Totale Indirizzo 1		**60**	**192**	**236**		**428**
	Totale Indirizzo 2		**60**	**164**	**208**		**428**

Le lezioni si svolgeranno il giovedì , venerdì e sabato mattina.

Le sedi di svolgimento delle attività formative sono la Scuola Politecnica e Fondazione Ansaldo, con possibilità di visite e attività di laboratorio presso Aziende contributrici del Master.

E’ prevista un frequenza obbligatoria alle attività didattiche con tolleranza del 34% delle assenze.

Verifiche intermedie, verifiche finali e conseguimento del titolo:

È previsto un esame intermedio di accertamento per l’attribuzione dei relativi crediti formativi universitari per ciascun modulo didattico.

In particolare l’esame consisterà in un test scritto e/o orale nella forma più consona al modulo e preferita dal docente (prova scritta, test a risposta multipla, esercizio, interrogazione orale). In media, ciascun test dovrebbe articolarsi al massimo su tre ore e dovrebbe essere svolto almeno una settimana dopo la chiusura del modulo al fine di permettere agli allievi di studiare/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 in aula al momento dell’esame.

La votazione attribuita sarà in trentesimi.

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: di ricerca, sia teorica che sperimentale, tipicamente relativa all’analisi critica di argomenti trattati nei moduli, allo studio di tematiche di ricerca e alla produzione di risultati sperimentali innovativi; di approfondimento, tipicamente relativa all’approfondimento 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; di indagine bibliografica (ricerca bibliografica su argomenti specifici relativi alle tematiche studiate nel Master).

L’attività svolta verrà 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, descrive i risultati ottenuti. Ogni progetto sarà seguito da un relatore, di norma docente del Master. Eventuali eccezioni (relatori non docenti del master) dovranno essere approvate dal Comitato di Gestione.

Ogni candidato si presenterà alla discussione dell’elaborato finale, in sessione plenaria, con un voto di partenza risultante dalla media dei voti ottenuti durante gli esami intermedi, ponderata sui crediti formativi universitari corrispondenti ai vari moduli didattici. Per determinare il voto di discussione la Commissione esaminatrice potrà attribuire alla prova finale un punteggio che varierà tra 0 e 6 punti a seconda della qualità dell’elaborato, dipendente anche dal tipo di attività svolta (ricerca, approfondimento, o indagine bibliografica) e della capacità di esposizione dello stesso.

Art. 4
Comitato di Gestione e il Presidente

Presidente: Prof. Alessandro Armando

Comitato di gestione: Prof. Alessandro Armando, Prof. Giovanni Chiola, Prof. Gabriele Costa, Prof. Giovanni Lagorio, Prof. Mario Marchese, Prof. Alessio Merlo, Prof. Paolo Pinceti, Prof. Sebastiano B. Serpico, Prof. Rodolfo Zunino e dai seguenti esperti in materia: Dott. Maurizio Aiello, Dott. Andrea Rigoni, Ing. Marco Biancardi, Ing. Mattia Epifani, Ing. Ermete Meda, Ing. Danilo Massa, Ing. Silvio Ranise, Ing. Gaetano Sanacore.

Docenti: Proff. Alessandro Armando, Giovanni Chiola, Gabriele Costa, Mario Marchese, Alessio Merlo, Paolo Pinceti, Rodolfo Zunino, Dott. Simone Aonzo, Andrea Valenza.

Docenti esterni: Dott. Maurizio Aiello (CNR), Andrea Rigoni (Deloitte-Intellium), Matthew Holt (Deloitte-Intellium), Marco Biancardi (ABB), Roberto Carbone (FBK), Mattia Epifani (RealityNet), Danilo Massa (Aizoon), Ermete Meda (Ansaldo STS), Matteo Meucci (MindedSecurity), Marco Morana (MindedSecurity),

Gianluca Papaleo (Dastech), Silvio Ranise (FBK), Alessandro Scoscia (TigerSecurity), Gaetano Sanacore (Ansaldo Energia), Luca Verderame (Talos).

Struttura cui è affidata la gestione amministrativa, organizzativa e finanziaria del corso:
Il Master è affidato ai Dipartimenti DITEN (in qualità di Dipartimento capofila) e DIBRIS (in qualità di Dipartimento associato) e a ISICT e a Fondazione Ansaldo, d'intesa con il Presidente ed il Comitato di Gestione, sarà affidata la gestione amministrativa, la programmazione operativa, l'organizzazione del corso, l'individuazione dei tutor.
La struttura a cui sarà affidata la segreteria organizzativa e amministrativo-contabile e la funzione di sportello informativo del Master è il DITEN - Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni Via all'Opera Pia 11A - 16145 Genova, tel. +39 0103532733, fax +39 0103532700, email: segreteria@isict.it,diten@diten.unige.it; indirizzo internet: www.diten.unige.it.
Referente: Dott.ssa Isa Traverso, e-mail: Isa.Traverso@unige.it, telefono: 010353 2703.

Art. 5
Modalità di accesso

Al Master sono ammessi un numero massimo di 30 allievi. Il numero minimo per l'attivazione è di 12 (8 occupati e 4 inoccupati o occupati con forma di lavoro flessibile).
Saranno ammessi al Corso:

Prioritariamente laureati in Informatica, Fisica, Matematica ed Ingegneria (laurea di secondo livello (magistrale o specialistica) o laurea a ciclo unico secondo il vecchio ordinamento).

In particolare i titoli di studio richiesti sono:

-Laurea in Fisica, Ingegneria, Informatica e Matematica conseguita secondo l'ordinamento pre-vigente;
-Laurea specialistica in Fisica (classe 20/S), Informatica (classe 23/S), Ingegneria biomedica (classe 26/S), Ingegneria dell'automazione (classe 29/S), Ingegneria delle telecomunicazioni (classe 30/S), Ingegneria elettrica (classe 31/S), Ingegneria elettronica (classe 32/S), Ingegneria informatica (classe 35/S), Matematica (classe 45/S), Modellistica matematico-fisica per l'ingegneria (classe 50/S), secondo l'ordinamento pre-vigente;
-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.

Il Comitato di Gestione del Master si riserva di ammettere candidati in possesso di un titolo di studio universitario diverso da quello specificato, sulla base dell'analisi del curriculum formativo e professionale ritenuto affine al profilo del corso. In tale caso sarà necessaria una richiesta al Comitato, a cui dovrà essere allegato il certificato di laurea, con gli esami sostenuti, ed eventuali altri titoli acquisiti che il candidato ritiene pertinenti al Master.
Il Comitato di Gestione del Master si riserva di ammettere candidati anche non in possesso dei requisiti necessari all'acquisizione del Master in qualità di uditori.

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. La commissione baserà la propria attività sull'analisi del Curriculum dei candidati ed un colloquio attribuendo a ciascuno i seguenti punti:

- Titoli (max 50 punti): saranno valutati la tipologia di laurea conseguita, la votazione di laurea, eventuali pubblicazioni e/o esperienze professionali;

- Prova orale (max 50 punti): sarà valutato il profilo psico-attitudinale del candidato e i suoi interessi e elementi motivazionali. Particolare rilevanza avrà la valutazione delle attitudini alla leadership e alle relazioni umane.

Potranno accedere alla prova orale i candidati i cui titoli hanno conseguito un punteggio pari o superiore a 25. La graduatoria finale sarà stilata sulla base della somma dei punteggi riportati nella prova orale e nei titoli.
La prova orale potrà svolgersi anche per via telematica (tramite collegamento Skype con video per la verifica dell'identità) previa richiesta al Presidente del Comitato di Gestione del Master, Prof. Alessandro Armando, per posta elettronica all'indirizzo: alessandro.armando@unige.it, inserendo nella richiesta il proprio identificativo Skype.
Nel caso di pari merito viene data preferenza al più giovane di età.

Contributi a carico dei partecipanti

€ 2.718,00 (**inclusa la tassa di iscrizione**) per inoccupati, disoccupati o occupati con forma di lavoro flessibile, da pagare al momento dell'iscrizione.
€ 6.718,00 (inclusa la tassa di iscrizione) per tutti gli altri, **suddivise in tre rate.**

Art. 6
Eventuali agevolazioni economiche e/o borse

Borse di studio INPS (ex I.N.P.D.A.P.)

Il Master ha ottenuto l'accreditamento INPS. Sono state erogate n. 5 Borse a sostegno di attività di qualificazione, riqualificazione e aggiornamento professionale dei dipendenti pubblici. L'importo unitario della Borsa è di € 6.500,00 a copertura dell'iscrizione al Master (escluse le tasse universitarie).

Il Bando sarà reperibile sul sito internet dell'INPS al link che verrà indicato sul sito www.MasterCyberSecurity.it o sul sito www.diten.unige.it

Art. 7
Presentazione delle domande

La domanda di ammissione al corso 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 giorno 8 marzo 2017.**

La data di presentazione della domanda di partecipazione al corso 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 corso:

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 della procedura valutativa di cui all'art. 5;

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. autocertificazione relativa allo status di occupazione/inoccupazione-disoccupazione.

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 partecipazione alle prove e per la frequenza del corso ai cittadini stranieri è disciplinato dalle disposizioni del Ministero dell'Università e della Ricerca del 22.03.2016 relative alle procedure per l'accesso degli studenti stranieri richiedenti visto ai corsi di formazione superiore per l'a.a. 2016/2017, disponibile all'indirizzo http://www.studiare-in-italia.it/studentistranieri/5.html.

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 prova di ammissione avrà luogo presso il Diten – Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni, Via all'Opera Pia, 11/A – 16145 Genova, il giorno **13 marzo 2017** secondo il calendario pubblicato sul sito internet www.MasterCyberSecurity.it o sul sito www.diten.unige.it

La graduatoria degli ammessi sarà affissa presso la sede degli esami e presso il sito web del Master

(www.MasterCyberSecurity.it) o sul sito web del Diten (www.diten.unige.it) entro il **14 marzo 2017.**

Non saranno inviate comunicazioni individuali ai candidati.
I candidati che non riporteranno nella domanda tutte le indicazioni richieste saranno esclusi dalla graduatoria di ammissione.

L'Università può adottare, anche successivamente alla pubblicazione della graduatoria di ammissione, provvedimenti di esclusione nei confronti dei candidati privi dei requisiti richiesti.

Art. 8
Perfezionamento iscrizione

I candidati ammessi al Master Universitario di II livello devono perfezionare l'iscrizione entro il **20 marzo 2017** mediante presentazione dei seguenti documenti all'Università degli Studi di Genova, **–** Area Didattica e studenti- Servizio alta formazione – Piazza della Nunziata, 6 **–** 16124 Genova (orario sportello: lunedì – mercoledì – giovedì - venerdì ore 9.00 - 12.00 e martedì ore 9.00 – 11.00 e ore 14.30 - 16.00):

1. domanda di iscrizione master universitario (*);
2. contratto formativo (*);
3. modulo richiesta tesserino magnetico (*);
4. fotocopia fronte/retro del documento di identità;
5. n. 1 fotografia formato tessera;
6. ricevuta comprovante il versamento della quota d'iscrizione di importo pari a **€ 2.718,00** da effettuarsi **online** tramite il servizio bancario disponibile nell'area dei servizi online agli studenti (https://servizionline.unige.it/studenti/Anagraficaecarriera/TASSE) utilizzando una delle carte di credito appartenenti ai circuiti Visa, Visa Electron, CartaSì, MasterCard, Maestro, carte prepagate riUnige/riCarige o tramite "avviso di pagamento" cartaceo (bollettino bancario Freccia).

Il pagamento della **II rata** di importo pari a **€ 2.000,00**, dovrà essere effettuato secondo le modalità sopracitate entro il **30 giugno 2017**;
il pagamento della **III rata** di importo pari a **€ 2.000,00**, dovrà essere effettuato secondo le modalità sopracitate entro il **30 novembre 2017**.

(*) disponibile all'indirizzo http://www.studenti.unige.it/master/modmaster

La domanda di iscrizione e i documenti sopra indicati potranno essere anticipati via fax al numero 0039 010 2099539. L'invio a mezzo fax non esime dalla presentazione della domanda e della documentazione in originale.

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 sono considerati rinunciatari.

Art. 9
Rilascio del Titolo

A conclusione del Master, agli iscritti che a giudizio del Comitato di Gestione abbiano superato con esito positivo le prove finali, verrà rilasciato il diploma di Master universitario II livello in "Cyber-Security and Data Protection", come previsto dall'art. 19 del Regolamento dei Corsi di Perfezionamento, di aggiornamento professionale e di formazione permanente e dei corsi per Master Universitari di primo e secondo livello.

Art. 10
Trattamento dei dati personali

I dati personali forniti dai candidati saranno raccolti dall'Università degli Studi di Genova Area Didattica e Studenti e trattati per le finalità di gestione della selezione e delle attività procedurali correlate, secondo le disposizioni del D.L.vo 30.06.2003 n. 196 "Codice in materia di protezione dei dati personali".

Genova, 10.02.2017

F.TO IL RETTORE

Responsabile del procedimento: Dott. ssa Maria Angela Ferrera
Per informazioni: Tel. 0102099636 - 0102099659