U N I V E R S I T À D E G L I S T U D I D I G E N O V A
AREA FORMAZIONE PERMANENTE E POST LAUREAM
SERVIZIO ALTA FORMAZIONE

D.R. n. 1656

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. 1250 del 27.12.2013;
- Vista la nota del Ministero dell'Università e della Ricerca prot. n. 7802 del 24 marzo 2014 relativa alle norme per l'accesso degli studenti stranieri ai corsi per l'a.a. 2014/2015;
- 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 Decreto d'Urgenza del Direttore del Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni dell'Università degli Studi di Genova n.104 del 29.10.2014 con il quale è stato proposta l'attivazione del Master Universitario di II livello in "Cyber-Security and Data Protection";
- Visto il Decreto d'Urgenza del Direttore del Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi dell'Università degli Studi di Genova n.100 del 30.10.2014 con il quale è stato proposta l'attivazione del Master Universitario di II livello in "Cyber-Security and Data Protection";
- Visto il parere favorevole espresso dalla Commissione scientifica di Ateneo per i master universitari in data 30.10.2014;
- Visto il verbale del consiglio della Scuola Politecnica del 11.11.2014 con cui si rettifica il Decreto d'urgenza n.16 del 08.09.2014;
- 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;

D E C R E T A

Art. 1

Norme Generali

È attivato per l'anno accademico 2014/2015 presso il Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni (capofila) e il Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi il **Master Universitario di II livello in "Cyber-Security and Data Protection"**

Il Master è realizzato in collaborazione con: ISICT, Fondazione Ansaldo.

Il Master sarà realizzato con il patrocinio del Consorzio Nazionale Interuniversitario per le Telecomunicazione (CNIT) e del Laboratorio Nazionale di Cyber Security del Consorzio Interuniversitario Nazionale per l'Informatica (CINI).

Art. 2

Finalità del Master

Obiettivi:

Il Master si propone di formare la figura di un esperto nella progettazione e gestione dei sistemi 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 la stessa rete Internet richiede non solo lo sviluppo di sistemi di protezione e di segregazione ancora più raffinati ma anche la definizione di un modello integrato di gestione della sicurezza.

In base all'evoluzione degli scenari, delle minacce e dei rischi, in ogni infrastruttura ICT, due sono le discipline che devono essere ben approfondite 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.
Obiettivo specifico del Master è la preparazione interdisciplinare di un esperto nella CyberSecurity 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 essere gestite 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.
Particolare attenzione è dedicata a due specializzazioni verticali, approfondite nella parte conclusiva del Master: "Incident Response and Computer Forensics" e "Critical Infrastructure and Industrial Automation Protection". 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/Network Forensics.
Tutte queste figure professionali devono avere un'approfondita conoscenza 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 dai cogenti.
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, 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.

Il Master fornisce inoltre stumenti concreti per conseguire diverse certificazioni inerenti la sicurezza informatica prevedendo:

- Supporto formativo specifico ed un voucher gratuito per 3 studenti particolarmente meritevoli per sostenere un "GIAC Certification Attempt" ovvero un esame in modalità "challenge" del SANS Institute per una delle Certificazioni Accreditate ANSI/ISO/IEC 17024
- La partecipazione gratuita per tutti gli studenti ad un corso per la certificazione ISO/IEC 27001 (Information Security Management) e l'iscrizione gratuita all'esame finale per 3 studenti particolarmente meritevoli.

Sbocchi occupazionali:

Il rapporto CLUSIT del 2014 sulla Sicurezza ICT in Italia (https://clusit.it/rapportoclusit/) indica che il 67% delle aziende italiane ha aumentato la sensibilità ai problemi di sicurezza informatica e che le stesse imprese prevedono un aumento del 25% delpersonale che si occupano di sicurezza informatica. Prevalgono, tra le figure professionali richieste, quelle a forte contenuto tecnico: Security Architect, Security Developer, Security Admin, Security DBA, che rappresentano il 42,5% delle nuove figure professionali richieste.

Art. 3
Organizzazione didattica dei Corsi

Il corso della durata di 12 mesi si svolge **da febbraio 2015 a gennaio 2016**. Il Master prevede 1500 ore di formazione così suddivise:

- 464 ore di attività didattica in aula o in laboratorio
- 886 ore si studio e approfondimento individuale
- 150 ore di tirocinio o project work da svolgersi presso l'azienda di appartenenza per gli occupati e preparazione della tesi finale

Al corso sono attribuiti 60 CFU.

Articolazione didattica:

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

Le sedi di svolgimento delle attività formative sono la scuola Politecnica, la scuola di Scienze Matematiche Fisiche e Naturali e Fondazione Ansaldo

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

Il programma è articolato nei seguenti moduli didattici (per il dettaglio vedere l'allegato 1):

materie di base

1. Introduzione generale
2. Introduzione alla crittografia moderna
3. Protocolli crittografici
4. Computer security
5. Network security
6. Host Security
7. Web security
8. Social Cyber Security and Advanced Topics
9. Sicurezza dei Dispositivi Mobili

materie professionalizzanti e specialistiche

1. Security Management
2. Seminari Specialistici: Tecnologia
3. Seminari Specialistici Governance
4. Informatica Legale, Privacy e Crimine Informatico
5. Introduzione ai Profili Professionali
6. Indirizzo 1 e 2

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.

L'articolazione delle attività formative, per il cui dettaglio si rimanda all'allegato 1, si struttura in tre parti principali:
Parte I: Le Basi (I.1 - I.12)
Parte II: La Professionalità (II.1 - II.3)
Parte III: Specializzazioni (III.1) e gli indirizzi specialistici (IN1 e IN2)
La tabella seguente riporta il Piano Didattico previsto. Le Basi sono costituite dai primi 12 moduli, la Professionalità dal modulo di Security Management, dai moduli sui Seminari Specialistici riguardanti la Governance e dal modulo di Informatica Legale, Privacy e Crimine Informatico. Le Specializzazioni dal modulo dal modulo di introduzione ai profili professionali e dai due indirizzi specialistici. La scelta dell'indirizzo specialistico verrà effettuata dagli studenti al termine della Parte I del Master.

Programma didattico:

N.	Modulo	SSD	CFU	h Università	h Esterni	Docenti	Tot. h Docenza
	Parte I: Le Basi						
I.1	Introduzione generale	ING-INF/05	1	3	3	Docenti del Comitato di Gestione	6
I.2	Introduzione alla crittografia moderna	INF01	5	42	0	Chiola, Lagorio, Zunino	42
I.3	Protocolli Crittografici	ING-INF/05	3	24	0	Armando, Costa	24
I.4	Computer Security	ING-INF/05	3	24	0	Armando. Chiola, Lagorio	24
I.5	Network Security	ING-INF/03	3	24	0	Aiello, Chiola, Marchese, Papaleo	24
I.6	Host Security	INF01	3	14	10	Chiola, Lagorio, Massa, Zunino	24
I.7	Web security	ING-INF/05	3	24	0	Armando, Merlo	24
I.8	Social Cyber Security and Advanced Topics	ING-INF/01	3	24	0	Zunino	24
I.9	Sicurezza dei Dispositivi Mobili	ING-INF/05	3	24	0	Armando, Costa	24
I.10	Seminari Specialistici: Tecnologia 1	INF/01	1	0	8	FNM	8
I.11	Seminari Specialistici: Tecnologia 2	ING-INF/01	3	0	32	Wellcomm, Digipoint	32
I.12	Seminari Specialistici: Tecnologia 3	ING-INF05	3	0	24	WellComm, DigiPoint	24
	Parte II: La Professionalita' nel management della cyber security						
II.1	Security Management	ING-INF/01	5	0	40	Meda	40
II.2a	Seminari Specialistici: Governance 1	INF/01	4	0	32	FNM, Protiviti, NISPro	32
II.2b	Seminari Specialistici: Governance 2	ING-INF/01	1	0	8	Fastweb	8
II.3	Informatica Legale, Privacy e Crimine Informatico	IUS/01	2	0	32	Bassoli, Losengo, Polizia Postale	32
	Parte III: Specializzazioni						
III.1	Introduzione ai profili professionali	ING-INF/01	3	12	12	Zunino, ABB, RealityNet	24
IN1	**Indirizzo 1: Incident Response and Computer Forensics**						

IN1.1	Incident Response and Forensics Analysis	ING-INF/05	4	10	22	Massa, Epifani, Scarito,Picasso, Meda, Zunino, Milani, Lawyer Court	32
IN1.2	Seminari Specialistici: Cyber Crime Investigation	ING-INF/01	1	0	16	Min.Interno, Lawyer Court, ROS	16
IN2	**Indirizzo 2: Critical Infrastructure and Industrial Automation Protection**						
IN2.1.1	Critical Infrastructure Protection	ING-INF/01	2	16	0	Zunino	16
IN2.1.2	SCADA Protection System	ING-INF/01	2	0	16	ABB	16
IN2.2	Seminari Specialistici: Protezione di Infrastrutture Critiche	ING-INF/05	1	0	16	Selex ES, Digi	16
17	Stage e tesi finale		6	0	0		0
	Totale		65	241	271		512
	Totale Indirizzo 1		60	225	239		464
	Totale Indirizzo 2		60	231	233		464

Docenti: Prof Alessandro Armando, Prof. Giovanni Chiola, Prof. Gabriele Costa, Prof. Mario Marchese, Prof. Alessio Merlo, Prof. Rodolfo Zunino.
Docenti esterni: Dott. Maurizio Aiello (CNR), Ing. Angeloluca Barba (Selex), Ing. Marco Biancardi (ABB), Ing. Mattia Epifani (RealityNet), Ing. Danilo Massa (Aizoon), Ing. Ermete Meda (Ansaldo STS), Ing. Matteo Meucci (MindedSecurity), Ing. Marco Morana (MindedSecurity).

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.
Al termine ogni candidato conseguirà una votazione finale complessiva espressa in centodecimi.
A conclusione del Master, agli iscritti che a giudizio del Comitato abbiano superato con esito positivo la prova finale, verrà rilasciato il diploma di Master Universitario di 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 dell'Ateneo genovese.

Art. 4
Comitato di Gestione e il Presidente

Presidente Prof. Alessandro Armando
Comitato di gestione: Prof Alessandro Armando, Prof. Giovanni Chiola, Prof. Mario Marchese, Prof. Sebastiano B. Serpico, Prof. Rodolfo Zunino e dai seguenti esperti in materia: Dott. Maurizio Aiello, Ing. Angeloluca Barba, Ing. Marco Biancardi, Ing. Mattia Epifani, Ing. Ermete Meda, Ing. Danilo Massa.

La strutture 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 11/A - 16145 Genova, tel. +39 0103532733/2160, fax +39 0103532700/2777, e-mail: 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: 010209 270.

Art. 5
Modalità di accesso

Al Master saranno ammessi un numero **massimo di 35 allievi** (il numero minimo per l'attivazione è di 17 allievi).
Titoli di studio richiesti:

- Laurea in Fisica, Ingegneria, Informatica e Matematica conseguita secondo l'ordinamento previgente 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;

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.
L'ammissione avverrà sulla base della valutazione dei titoli e di una prova orale.
La commissione, per la valutazione dei titoli, ha a disposizione fino a un massimo di 50 punti che verranno assegnati in conformità ai seguenti criteri:

- valutazione della laurea conseguita in relazione alla preparazione di base richiesta per una proficua frequenza del Master (max punti 20)
- punteggio proporzionale alla votazione di laurea tra 60/100 e 101/100, dopo aver normalizzato i punteggi in centesimi e considerato il punteggio massimo con lode pari a 101/100. (max punti 15)
- pubblicazioni valutate sulla base della pertinenza rispetto alle tematiche del Master, della numerosità e della collocazione editoriale; esperienze valutate sulla base della pertinenza rispetto alle tematiche del Master, della durata complessiva e del prestigio degli ente e/o aziende presso cui sono state svolte. (max punti 15)

Potranno accedere alla prova orale i candidati i cui titoli hanno conseguito un punteggio pari o superiore a 25.
Per la prova orale, la commissione ha a disposizione fino ad un massimo di 50 punti.
Sarà valutato il profilo del candidato, suoi interessi e elementi motivazionali. 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

Inoccupati o disoccupati: **€ 2.717,00** (**inclusi € 217,00 di tassa di iscrizione all'università**) da pagare al momento dell'iscrizione

Per tutti gli altri: **€ 6.717,00 (inclusi € 217,00 di tassa di iscrizione all'università) suddivise in tre rate:**

- **€ 2.717,00** (inclusa la tassa di iscrizione) I rata da pagare al momento dell'iscrizione;
- **€ 2.000,00** II rata da pagare entro il 31 maggio 2015;
- **€ 2.000,00** III rata da pagare entro il 31 ottobre 2015.

Art. 6
Presentazione delle domande

La domanda di ammissione al concorso deve essere presentata mediante la procedura on-line disponibile all'indirizzo https://servizionline.unige.it/studenti/post-laurea/master, entro **le ore 12:00 del 16.01.2015**

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. 5;
d. autocertificazione relativa allo status di occupazione/inoccupazione-disoccupazione.

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

1. copia fronte/retro del documento di identità;
2. curriculum vitae;
3. eventuale documentazione attestante il livello di conoscenza delle lingue straniere prescelte e della lingua italiana per studenti stranieri
4. autocertificazione relativa alla veridicità delle dichiarazioni rese e all'autenticità dei documenti allegati alla domanda. Tale dichiarazione dovrà essere resa attraverso il modulo disponibile sulla pagina web della procedura on-line, che dovrà essere stampato, compilato e sottoscritto dall'interessato e allegato attraverso la procedura on-line.

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 dalla nota del Ministero dell'Università e della Ricerca prot. n. 7802 del 24 marzo 2014 (Norme per l'accesso degli studenti stranieri ai corsi per l'a.a. 2014/2015),, 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 DITEN - Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni, Via all'Opera Pia 11/A - 16145 Genova, il giorno 23.01.2015 secondo il calendario pubblicato sul sito internet www.MasterCyberSecurity.it

La graduatoria degli ammessi sarà affissa presso la sede degli esami e presso il sito web del Master (www.MasterCyberSecurity.it) entro il 26.01.2015

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. 7
Perfezionamento iscrizione

I candidati ammessi al Master universitario di II livello in "Cyber Security and Data Protection" devono perfezionare l'iscrizione entro il 09.02.2015 mediante presentazione dei seguenti documenti all'Università degli Studi di Genova, **–** Area formazione permanente e post lauream - Servizio alta formazione **–** Via Bensa, 1 **–** 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. modulo richiesta tesserino magnetico (*);
3. fotocopia fronte/retro del documento di identità;
4. n. 1 fotografia formato tessera;
5. contratto formativo (*);
6. ricevuta comprovante il versamento della quota d'iscrizione di importo pari a **2.717,00 €** da effettuarsi **online** tramite il servizio bancario disponibile nell'area dei servizi online agli studenti, 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 **2000,00 €**, dovrà essere effettuato secondo le modalità sopracitate entro il **31 maggio 2015**
Il pagamento della **III rata** di importo pari a **2000,00 €**, dovrà essere effettuato secondo le modalità sopracitate entro il **31 ottobre 2015**

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

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 di iscrizione 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. 8
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. 9
Trattamento dei dati personali

I dati personali forniti dai candidati saranno raccolti dall'Università degli Studi di Genova Area formazione permanente e post lauream 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, 10.12.2014

IL RETTORE
Prof. Paolo Comanducci
F.to Paolo Comanducci

Responsabile del procedimento:
Dott. Aldo Spalla
Tel. 010/2095795

Allegato 1

PARTE I: Le Basi

I.1. Introduzione generale (6h) (Tutti) 1CFU - ING-INF/05

1. Le 4 facce della sicurezza: confidenzialità, integrità, disponibilità, affidabilità
2. come si realizza la sicurezza: livello fisico/hardware, livello software base/applicativo, livello organizzativo (fattore umano - cognitivo, psicologico, sociale, ecc.)
3. Un po' di storia ... (da dove viene la cybersecurity)
4. Principi di Denning: accesso mediato alle risorse, anello debole della catena, economia/ridondanza di controllo, minimo privilegio, sessioni di lavoro e cambio di contesto
5. Principali vulnerabilita` dei sistemi attuali, tipici esempi di attacchi
6. Tecniche base di difesa: crittografia, host security, network security, organizzazione/governance dei processi

I.2. Introduzione alla crittografia moderna (42h) (UniGE) 5 CFU - INF01

1. Teoria dell'informazione e concetto di entropia, con esercizi numerici ed esempi pratici in aula.
2. Cifratura con chiave simmetrica.
    a. One-time pad e perfect secrecy, con esempio pratico ed esercizio in laboratorio di attacco COA in caso di riuso della stessa chiave per produrre ciphertext diversi
    b. Attacchi passivi ed attivi: COA, KPA, CPA, CCA; indistinguibilità IND-CPA, INC-CCA; avversario efficiente, parametro di sicurezza, sicurezza semantica. Malleabilità. Teoria in aula con esempi pratici
    c. Cifrari a blocchi: DES, AES; applicazione a messaggi di lunghezza arbitraria: ECB, CBC, OFB, CTR; caratteristiche e confronto in casi pratici
    d. Stream ciphers: RC4, con esperienza in laboratorio per determinare la velocita` di esecuzione in confronto con block cipher
    e. Diffie-Hellman key exchange
3. Funzioni hash
    a. Collision resistence, paradosso del compleanno, costruzione di Merkel, MD5, SHA-1, SHA-256, lezione in aula con esempi pratici
4 Message authentication code: CBC-MAC, HMAC
5. Cifratura a chiave pubblica
    a. El Gamal (derivato da Diffie-Hellman) cifratura, e firma DSA
    b. Textbook RSA con esempi numerici
    c. Padding: PKCS#1, OAEP, sicurezza rispetto a CPA/CCA, con esempi pratici di attacchi a padding insicuri
6. Firme e certificati digitali
    a. Schemi di firma RSA e DSA; ASN.1, formati DER e PER, X509v3, PKI vs. Web of Trust; lezione in aula con esempi pratici
    b. Esperienza in laboratorio di creazione e uso di una CA
7. Elliptic curve Cryptography
    a. Algebra per curve Ellittiche - GF(p) e GF(2^n)
    b. Protocolli ECDH e ECDSA

I.3. Protocolli Crittografici (24h) (UniGE) 3 CFU - ING-INF05

1. Basic notions (protocol execution, assumptions and goals, attacker model)

2. Reply protection (timestamps, nonces)
3. Examples of protocols and attacks (NSPK, Otway-Rees, Andrew Secure RPC, Denning & Sacco)
4. Prudent engineering of security protocols
5. Kerberos (architecture, protocol, inter-realm communication, limitations)
6. SSL/TLS, SSH
7. GPG, SMIME, PEC, con laboratorio e/o IPSec, con laboratorio

I.4. Computer Security (24h) (UniGE) 3 CFU - ING-INF05

1. 3.1 Autenticazione degli utenti
   a. Password gestite da un utente, PIN, one-time password, hash chain
2. 3.2 Autorizzazione
   a. Modelli, Meccanismi e Linguaggi per il Controllo degli Accessi
   b. ACL vs capability; confuse deputy problem
   c. Discretionary vs Mandatory Access Control
   d. Role-Based Access Control (RBAC) e Administrative Role-Based Access Control (ARBAC)
   e. Attribute-based Access Control
   f. I modelli di Bell-LaPadula, Harrison-Ruzzo-Ullman, Chinese Wall, Biba, Clark-Wilson
   g. Laboratorio su XACML
   h. Laboratorio su ACL in Linux, SELinux

I.5. Network Security (24h) (UniGE, CNR) 3 CFU - ING-INF03

1. Vulnerabilita` dei protocolli Internet
   a. Lo stack protocollare : IPv4 e IPv6, ICMP, TCP/UDP, DNS, FTP/HTTP/SMTP/POP3/IMAP, SSH/SSL/TLS
   b. Laboratorio Wireshark
   c. Principali attacchi: virus e Botnet, DoS e DDoS, Worm, Email SPAM/Physhing, DNS Cache Poisoning, Web SPAM, sniffing; lezione in aula
   d. Presentazione dell'attacco di Mitnick contro Shimomura; lezione in aula con esempi pratici
   e. Port scanning, fingerprinting, uso di NMAP; lezione pratica in laboratorio
2. WiFi and Bluetooth security
   a. - minacce e contromisure
   b. esperienza di laboratorio su WiFi Security e hacking tools
3. Firewall
   a. Reti pubbliche e private, NAT/PAT, port forwarding, VLAN; lezione in aula con esempi pratici
   b. Packet filtering: principio del collo di bottiglia, IPtables, default permit/deny, esempi di regole per consentire o vietare servizi, regole antispoofing, statefull packet filtering, deep packet inspection; lezione in aula con esempi pratici
   c. Esperienza pratica di configurazione di firewall, in laboratorio
   d. Firewall bypassing, tunneling; lezione teorico/pratica

I.6. Host Security (24h) (UniGE) 3 CFU - INF01

1. Integrita` del sistema
   a. minacce: virus/worm, troyan, keylogger, backdoor, rootkit; esempio di Ken Thompson; lezione in aula
   b. difese: antivirus, host-based IDS, signature/anomaly based detection, virtual machine, honeypot
   c. Network IDS;
   d. Esperienza di installazione e uso di IDS, in laboratorio
2. Stack Overflow
   a. vulnerabilita` nel codice applicativo, concetto di exploit, con esempi semplificati; lezione in aula (4h)
   b. esperienza di applicazione di un attacco di tipo stack overflow su una macchina vulnerabile; in laboratorio

3. Malware analysis
    a. Static vs/ dynamic malware analysis, uso di sandbox per malware analysis
    b. Metodi intelligenti per dynamic malware analysis, machine learning per classificazione dei malware
    c. Esperienza in laboratorio di malware classification
4. OS Hardening
    a. Esecuzione sicura di applicazioni: kernel Unix/Linux, processi POSIX, memoria sicura, accesso controllato ai file, vulnerabilità a sistema spento e durante la fase di bootstrap; lezione in aula con esempi pratici in ambiente POSIX
    b. Configurazione e operazione sicura di un sistema Linux: sudo, /etc, gestione dei log, cron, ecc.; pratica in laboratorio

I.7. Web Security (24h) (UniGE) 3 CFU - ING-INF05

1. Introduzione al Web: il protocollo http, il modello client –server, HTML, cookies
2. Server-side Scripting (PHP)
3. DOM e Client-side Scripting (Javascript)
4. Cross-site Scripting
5. Database Security and SQL-injection
6. Browser-based Security protocols: SAML SSO , OpenID, OAuth
7. Security of HTML5
8. OWASP Testing Framework
9. Web Application Penetration Testing

I.8. Social Cyber Security & advanced topics (24h) (UniGE) 3 CFU - ING-INF01

1. Social Engineering
    a. impersonation attacks, furto di identità, phishing e oltre, smishing, etc., best practices comportamentali
    b. social networks, user profiling
    c. esperienza pratica in laboratorio di social profiling
2. Advanced Persistent Threat
    a. configurazione degli attacchi, strutturazione in squadre specialistiche, Inserimento, Diffusione, Mantenimento dell'attacco, metodi di prevenzione e rilevazione, e terapie di rimozione
    b. procedure di comportamento in presenza di APT
    c. dimostrazione pratica in laboratorio di APT

I.9. Mobile Security (24h) (UniGE) 3 CFU - ING-INF05

1. Introduzione ai dispositivi mobili: storia, evoluzione, caratteristiche
2. Mobile OSes e sicurezza: struttura e caratteristiche dei SO più diffusi (Android, iOS, Windows)
3. Mobile code: modelli di distribuzione delle applicazioni, problematiche e rischi (e.g., integrità e autenticità del codice), pratiche comuni (mutuate/ereditate da tecnologie precedenti -- isolation/sandboxing)
4. Malware detection: tecniche di ispezione e riconoscimento del codice malevolo, panoramica sul numero e il tipo di malware per dispositivi mobili
5. Modelli di sicurezza: access control, usage control e history-based security (specifica e prevenzione dei comportamenti indesiderati), language-based security
6. NFC e Host-based Card Emulation
7. Remote Attestation
8. Trusted Execution Environments
9. Caso di studio/progetto: Soluzioni per il paradigma Bring Your Own Device (BYOD) OPPURE Soluzioni per il mobile/proximity payment

I.10 Seminari Specialistici: Tecnologia

1. *Cyber Security: Panoramica* **(8h)** (Finmeccanica) 1CFU - INF01
2. *Perimeter Defense (Lab)* **(24h)** (Wellcomm) 2CFU - ING-INF01
3. Content Filtering *(Lab)* **(8h)** (Digipoint) 1CFU - ING-INF01
4. *Funzioni hash crittografiche* **(8h)** (ST Micro) 1CFU - ING-INF05
5. *Web Security* **(8h)** (OWASP Italia) 1CFU - ING-INF05
6. *Threat Modeling* **(8h)** (MindedSecurity) 1CFU - ING-INF05

PARTE II: La Professionalità nel Management della CyberSecurity

II.1 Security Management (40h) (Ansaldo-STS) 5 CFU - ING-INF01

1. Necessità di un ISMS (Information Security Management System) e PIMS (Personal Information Management System) – Scenario Globale
   a. L'evoluzione dell'ICT e la Cyber Security
   b. L'evoluzione delle minacce: breve storia degli attacchi ed incidenti informatici
   c. I difetti della tecnologia: le vulnerabilità di reti e sistemi – Il fattore umano
   d. Il Budget ICT e Cyber Security - Relazioni con l'Alta Direzione
2. Natura di un ISMS e PIMS
   a. Governo della sicurezza e processi aziendali, le 5 fasi di ITIL, Ruoli e Responsabilità, Tabella RACI
   b. Ciclo PDCA di Deming - Fasi di Prevention, Monitoring and Reaction
   c. I Domini della Cyber Security
   d. Componente Tecnologica :panoramica Tipologie, Metodi e Strumenti
   e. Componente Organizzativa: Modelli , Policy, Corpus Documentale (Direttive, Procedure, Istruzioni Operative), SOC, IRT/CERT
   f. Componente Legale: Cogenti (262, 231,196, successivi provvedimenti garante privacy), ambiti UE (Trattato di Budapest, direttiva protezione infrastrutture critiche), adempimenti
   g. Cenni su Computer & Network Forensics: la preservazione della prova digitale. La norma ISO27037
   h. Data Security: Classificazione Informazione, DLP, IRM, Secure Disposal and Wiping
   i. La progettazione di un ISMS secondo la ISO27001/27002 e di un PIMS secondo la BS10012
   j. Lab.n Esercizi in Aula
3. Gestione del Rischio
   a. Scope, Asset e Classificazione dell'Informazione
   b. Risk Assessment, Gap Analysis, Risk Reduction
   c. L'Analisi del Rischio secondo lo standard ISO27005
   d. Lab.n Esercizio in Aula
4. Continuità Operativa e Gestione della Crisi
   a. Business Continuity e Disaster Recovery – Redazione di BCP e DRP
   b. Business Impact Analysis
   c. La Continuità Operativa secondo la BS7799 e la ISO22301
   d. Lab.n Esercizio in Aula
5. Conformità e Audit
   a. Standard Internazionali e Best Practice di riferimento
   b. Il processo di Certificazione (volontaria) e di Audit

II.2 Seminari Specialistici: Governance

1. *Information Security Governance: Panoramica* **(8h)** (Finmeccanica) 1CFU - INF01
2. *Information Security Governance in azienda* **(8h)** (Protiviti) 1CFU - INF01
3. *Il SOC/CERT e la Security Operation* **(8h)** (Fastweb) 1CFU - ING-INF01
4. *La Continuità Operativa (Lab)* **(8h)** (Finmeccanica) 1CFU - INF01
5. *Le nome ISO27001/ISO22301, la Certificazione e l'Audit* **(8h)** (NISPro) 1CFU - INF01

II.3 Informatica Legale, Privacy e Crimine Informatico (32h) (Studio Legale Bassoli & Losengo Soliani, Polizia Postale) 2CFU – IUS/01

1. Informatica Legale e Privacy
2. Il Crimine Informatico

PARTE III: Specializzazioni

III. 1 – Introduzione ai profili professionali

1. *Tecnologie ICT in Critical Infrastructure Protection - Basi* **(8h)** (UniGE) 1 CFU - ING-INF01
   a. Aspetti professionali specifici nella CIP (minacce, strumenti di alerting e contromisure)
   b. Normativa e Enti preposti
   c. Introduzione ad aspetti di CyberDefense e Cyber War

2. *La Security nei sistemi SCADA* **(8h)** (ABB) 1 CFU - ING-INF01
   a. Industrial Control System overview: difference between SCADA and DCS, components, protocols, functionalities and differences between ICS and ICT (4h)
   b. Security in Automation products (SD3 approach for product development, Principle of least privilege, Patch Validation, Hardening, Event log, etc.) (4h)

3. *Aspetti fondamentali di Computer forensics* **(8h)** (UniGE, RealityNet) 1 CFU - ING-INF01
   a. Definizione ambiti e scopi della Forensics
   b. Aspetti tecnici e legali della computer Forensics
   c. Procedure e strumenti tipici della Computer Forensics

Indirizzo 1: "Incident response and Computer Forensics"

IN1.1 Incident Response and Forensic Analysis (32h) (Aizoon, RealityNet, Lawyer, Court, Ansaldo-STS- Unige) 4 CFU - ING-INF05

1. Manage response, Investigation and Analysis
   a. Incident Preparation
   b. Incident Detection and Analysis
   c. Containment, Eradication, and Recovery
   d. Proactive and Post Incident Cyber Services
   e. Forensic Technologies
   f. Digital Evidence Collection
   g. Evidentiary Reporting

2. Forensic Analysis of Compromised Systems
   a. Analysis methodologies
   b. File system-level forensic analysis
   c. Operating system-level forensic analysis
   d. Application-level forensic analysis
   e. Network forensic analysis
   f. Timeline analysis

3. Practical Session: CyberCop Simulation
   a. Comprhensive Simulation o fan Incident
   b. Discovery
   c. Investigation
   d. Evidence collection

e. Reporting
f. Trial

IN1.2 – Seminari specialistici: Cyber Crime Investigation (16h) (Polizia Postale, Min. degli Interni, ROS) 1CFU - ING-INF01

Indirizzo 2: "Critical Infrastructure and Industrial Automation Protection"

IN2.1 Critical Infrastructure Protection

1. **Tecnologie ICT in Critical Infrastructure Protection – Approfondimenti** (**16h**) (UniGE) 2 CFU – ING INF01
   a. Aspetti professionali specifici nella CIP (minacce, strumenti di alerting e contromisure)
   b. Normativa e Enti preposti
   c. CyberDefense e Cyber War
   d. definizione e caratteristiche; metodi e strumenti per cyber defense, strutture nazionali e internazionali
   e. Esemplificazione pratica di casi di cyberwar
   f. Definizione del contesto: un problema in n dimensioni interdipendenza ed effetto domino
   g. Sicurezza IT, sicurezza delle informazioni: aspetti tecnologici (system level), aspetti organizzativi (business process).
   h. Le policy di sicurezza nazionale

2. **SCADA system protection (16h)** (ABB) 2 CFU - ING-INF01
   a. Security Standards and Regulation for ICS: IEC-62351, IEC-62443, NERC-CIP
   b. ENEL Experience in CS protection
   c. Test bed and R&D laboratories visit: a real SCADA and its protection features
   d. Guide to Industrial Control Systems (ICS) Security (NIST 800-82),
   e. Countermeasures for SCADA: Data Diode and Unidirectional Gateways, Perimeter Segregation, whitelisting, SIEM.
   f. Case Studies: Stuxnet and related vulnerabilities

IN2.2 - Seminari Specialistici: Protezione di Infrastrutture Critiche (16h) (Selex-ES, DIGI)

1 CFU - ING-INF05

1. *La protezione delle infrastrutture critiche nazionali*

2. *Vulnerability Exposure – Skybox*