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 E STUDENTI
SERVIZIO ALTA FORMAZIONE

D.R. n. 173

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 28.02.2017 relative alle procedure per l'accesso degli studenti stranieri richiedenti il visto ai corsi di formazione superiore per l'a.a. 2017/2018;
- 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. 2173 del 19.06.2017 con il quale è stata proposta l'attivazione del Master Universitario di II livello in "Cybersecurity and Critical Infrastructure Protection*"* I Edizione;
- 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. 2178 del 19.06.2017 con il quale è stata approvata la sopra citata proposta di attivazione del Master Universitario di II livello in "Cybersecurity and Critical Infrastructure Protection*"* I Edizione, in quanto Dipartimento associato;
- Visto il Decreto d'urgenza del Preside della Scuola Politecnica dell'Università degli Studi di Genova n. 2187 del 19.06.2017 con cui è stata approvata l'attivazione del Master Universitario di II livello in "Cybersecurity and Critical Infrastructure Protection*"* I Edizione;
- Viste le delibere, in data 04.07.2017 del Senato Accademico e in data 05.07.2017 del Consiglio di Amministrazione, con le quali è stato ratificato il decreto d'urgenza n. 2271 del 22.06.2017 che istituiva l'attivazione di Master in risposta all'Avviso pubblico di cui alla D.G.R. n. 361 del 05.05.2017;
- Visto il Decreto del Direttore Generale della Regione Liguria n. 240 del 14.11.2017 "Approvazione esiti selezione e ammissione a finanziamento delle operazioni presentate ai sensi dell'Avviso di cui alla D.G.R. 361 del 05.05.2017";
- Visto l'atto costitutivo di ATS stipulato in data 14.12.2017 tra l'Università degli Studi di Genova e Fondazione Ansaldo (Gruppo Leonardo) per la realizzazione del progetto Master Universitario di II livello in "Cybersecurity and Critical Infrastructure Protection" I Edizione;

D E C R E T A

Art. 1
Norme Generali

E' attivato per l'anno accademico 2017/2018, 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) dell'Università degli Studi di Genova, il Master Universitario di II livello in *"***Cybersecurity and Critical infrastructure protection"**, I Edizione.

Il Master è realizzato sulla base di Associazione Temporanea di Scopo (ATS) con: Fondazione Ansaldo (Gruppo Leonardo).

Il Master è finanziato dal F.S.E. nell'ambito di progetti per l'attuazione di Master universitari di I e II livello a valere sull'asse 3 "Istruzione e Formazione" del POR FSE 2014-2020.

Aderiscono al progetto le seguenti aziende e enti, anche attraverso la disponibilità di docenza diretta nell'attività didattica:

ABB S.p.A.
AITEK
Aizoon
Ansaldo Energia
Ansaldo STS
Deloitte
Gruppo SIGLA
IREN
Kaspersky
Leonardo
RINA
UniCredit

e contribuiscono con possibile attività di docenza diretta e/o offerta di stage/project work le seguenti aziende o enti:

Consiglio Nazionale delle Ricerche
ConsiQ
DASTech
ENEL
Fondazione Bruno Kessler
FortiNet
IBM
LRQA
Minded Security
Piaggio AeroSpace
Protivity
RealityNet
TALOS
Vodafone

I soggetti esterni partecipano alla realizzazione dei progetti sia come membri dell'ATS sia come sostenitori.
Il master rientra in un più ampio programma di alta formazione e accompagnamento al lavoro finanziato da Regione Liguria con fondi comunitari e finalizzato a sviluppare nelle imprese e nelle istituzioni capitale umano critico per sostenere la domanda di ricerca e innovazione espressa dal sistema economico, sociale e istituzionale e il rafforzamento delle attività di trasferimento tecnologico e di diffusione dell'innovazione.

La partecipazione al master è gratuita.

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) e di Cybersecurity (Mobile, Web, Cloud, SCADA, ...) 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, mentre gli indirizzi di specializzazione contemplano cyber-esercizi finalizzati 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, Cloud Security ecc. Lo scopo è rendere lo studente operativo in un elevato e variato numeri di scenari, 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).

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 nell'attuale contesto Information Technology 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 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 del virus WannaCry che ha avuto impatti devastanti in molte realtà anche su scala mondiale. WannaCry è riuscito 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. Un'analisi integrata dell'incidente WannaCry mostra che l'efficacia dell'attacco è imputabile sia al fatto che i PC aziendali non fossero aggiornati (o neppure messi in sicurezza in modo opportuno), sia alla impreparazione del personale nella gestione dell'incidente.

Per questo motivo, le aziende hanno urgente bisogno di inserire rapidamente personale esperto di Cybersecurity e protezione delle proprie infrastrutture all'interno del loro staff. Va sottolineato che la domanda di tali figure professionali supera di molto l'offerta attualmente disponibile; al tempo stesso, i laureati magistrali attuali non dispongono del livello di competenze necessario.

Sbocchi occupazionali:

La natura variata e molteplice delle Aziende che aderiscono al Master evidenzia l'ampio spettro di ricadute occupazionali legate al conseguimento del titolo del Master. Recenti indagini indipendenti (Capital, Nro 447-448, sett/ott 2017) a livello nazionale evidenziano l'alto assorbimento di personale skilled in 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 Master

Il Master della durata di 12 mesi, si svolge **da maggio 2018 a aprile 2019**.
Il Master si articola in 1500 ore di cui:
- 464 ore di attività formative d'aula;
- 586 ore di studio individuale;
- 450 ore stage/project work;

Al Master sono attribuiti 60 CFU.

Il piano didattico è riportato nell'Allegato 1 che fa parte integrante del presente bando.

La frequenza è a tempo parziale per un ammontare massimo di 32 ore settimanali, con tolleranza del 34% delle assenze.
Il Master NON prevede ore di docenza telematica.

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 corso, 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 corso. Il tutor seguirà lo svolgimento del corso ed interagirà costantemente con gli studenti e con i docenti, al fine di gestire eventuali problematiche e valutare l'andamento del percorso di studi.

Verifiche intermedie e prove finali

Ciascun modulo didattico prevede un esame intermedio 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 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: 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, 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.
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, che sarà espresso in centodecimi, 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.

Sede di svolgimento dell'attività didattica: Università degli Studi di Genova - Scuola Politecnica, con possibilità di visite e attività di laboratorio presso aziende contributrici al Master.

Art. 4
Requisiti di Ammissione

Al Master sono ammessi un numero **massimo di 20 allievi** (il numero minimo per l'attivazione è di 15 allievi).

Titoli di studio richiesti:

- 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).

Potranno tuttavia essere ammessi laureati di classi di laurea diverse purché in possesso di un background sufficiente per affrontare le tematiche del 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. La procedura di selezione prevede una prova scritta con la garanzia dell'anonimato dell'autore fino a valutazione avvenuta, e una prova orale individuale, in cui la Commissione si baserà anche sull'analisi del Curriculum di ogni candidato, attribuendo a ciascuno i seguenti punti:

- Prova scritta (max 30 punti) che consisterà in un test finalizzato al rilevamento del possesso delle competenze di base per la frequenza del Master; i candidati dal 1° al 40° posto presenti nella graduatoria saranno ammessi alla prova orale. In caso di parità di punteggio verrà data la precedenza al candidato con minore età anagrafica.
- Prova orale individuale: saranno valutati il Curriculum del candidato, comprendente la tipologia di laurea conseguita, la votazione di laurea, pubblicazioni, esperienze professionali ed eventuali altri titoli (max 25 punti), nonché i suoi interessi ed elementi motivazionali per la valutazione delle attitudini professionali e alle relazioni umane (max 25 punti). La prova orale si intende superata dai candidati che avranno ottenuto un punteggio pari o superiore a 30.

La graduatoria finale dei candidati idonei, cioè che avranno superato la prova orale, sarà stilata sulla base della somma dei punteggi riportati nella prova scritta e nella prova orale. Saranno ammessi al corso i primi candidati in graduatoria fino a un massimo di 20. Gli eventuali candidati idonei oltre il ventesimo in graduatoria costituiscono le riserve da cui attingere, secondo l'ordine della graduatoria stessa, in caso si verifichino rinunce da parte dei candidati ammessi.
In caso di parità di punteggio verrà data preferenza al candidato con minore età anagrafica.

Art. 5
Comitato di Gestione e Presidente

Presidente: Prof. Rodolfo Zunino;
Comitato di Gestione: Prof. Alessandro Armando, Prof. Riccardo Bozzo, Prof. Giovanni Chiola, Prof. Paolo Gastaldo, Prof.ssa Paola Girdinio, Ing. Lorenzo Ivaldi, Prof. Giovanni Lagorio, Prof. Mario Marchese, Prof. Alessio Merlo, Prof. Paolo Pinceti, Dr. Enrico Russo, Prof. Sebastiano B. Serpico; Dott. Maurizio Aiello (CNR), Ing. Stefano Cocurullo (Leonardo), Dott. Mattia Epifani (RealityNet), Ing. Ermete Meda (Ansaldo STS), Ing. Danilo Massa (Aizoon), Ing. Danilo Moresco (ABB), Ing. Daniele Patuelli (ABB), Ing. Silvio Ranise (Fondazione Bruno Kessler), Ing. Antonio Rebora (Ansaldo Energia), Ing. Gaetano Sanacore (Ansaldo Energia), Dott.ssa Patrizia Queirolo (Leonardo), Gen. B. A. Francesco Vestito (Stato Maggiore della Difesa - Comando Interforze per le Operazioni Cibernetiche).

Rappresentanti della struttura cui è affidata la gestione amministrativa, organizzativa e finanziaria: Dott.ssa Isa Traverso, Responsabile Amministrativo, Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni (DITEN).
La struttura cui sarà affidata la segreteria organizzativa e amministrativo-contabile e la funzione di sportello informativo del corso è: il Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni (DITEN) Via all'Opera Pia 11A - 16145 Genova, tel. +39 0103532733, fax +39 0103532700, email: 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. 6
Presentazione della domanda di ammissione

La domanda di ammissione al concorso deve essere presentata mediante la procedura on-line disponibile all'indirizzo https://servizionline.unige.it/studenti/post-laurea/master, entro **le ore 12:00 del 30 marzo 2018.**

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.

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 28.02.2017 relative alle procedure per l'accesso degli studenti stranieri richiedenti visto ai corsi di formazione superiore del 2017/2018, disponibile all'indirizzo http://www.studiare-in-italia.it/studentistranieri.
Ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, alle dichiarazioni rese nella domanda di ammissione, nel caso di falsità in atti e dichiarazioni mendaci si applicano le sanzioni penali previste dall'art. 76 del decreto n. 445/2000 sopra richiamato. Nei casi in cui non sia applicabile la normativa in materia di dichiarazioni sostitutive (D.P.R. n. 445/2000 e ss.mm.ii), il candidato si assume comunque la responsabilità (civile, amministrativa e penale) delle dichiarazioni rilasciate.

L'Amministrazione si riserva di effettuare i controlli e gli accertamenti previsti dalle disposizioni in vigore. I candidati che renderanno dichiarazioni mendaci decadranno automaticamente dall'iscrizione, fatta comunque salva l'applicazione delle ulteriori sanzioni amministrative e/o penali previste dalle norme vigenti.
L'Amministrazione universitaria non assume alcuna responsabilità per il caso di smarrimento di comunicazioni dipendente da inesatte indicazioni della residenza e del recapito da parte dell'aspirante o da mancata oppure tardiva comunicazione del cambiamento degli stessi, né per eventuali disguidi postali o telegrafici non imputabili a colpa dell'Amministrazione medesima.

La prova scritta sarà effettuata il 9 aprile 2018 alle ore 16 presso i locali (aula B2) della Scuola Politecnica dell' Università di Genova – Via Opera Pia 15 A – 16145 Genova. L'elenco degli ammessi alla prova orale, la sede delle prove orali e il relativo calendario saranno resi disponibili mediante affissione presso il Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni (DITEN), Via all'Opera Pia 11A - 16145 Genova e sul sito web del Dipartimento (www.diten.unige.it) entro il giorno **11 aprile 2018**.

La prova orale di ammissione avrà luogo a partire dal 18 aprile 2018 alle ore 9.

La graduatoria degli ammessi verrà pubblicata presso il Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni (DITEN), Via all'Opera Pia 11A - 16145 Genova e sul sito web del Dipartimento (www.diten.unige.it) **entro il 23 aprile 2018.**

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.

Art. 7
Perfezionamento dell'iscrizione

I candidati ammessi al Master devono perfezionare l'iscrizione entro il 30 aprile 2018 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;

Il Master è interamente finanziato da Regione Liguria con fondi comunitari. Gli oneri di iscrizione al corso, comprensivi della tassa di iscrizione all'Università sono coperti da tale finanziamento, quindi nulla è dovuto dallo studente iscritto.

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 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 studenti – Servizio alta formazione, e trattati per le finalità di gestione della selezione e delle attività procedurali correlate, secondo le disposizioni D.L.vo 30.06.2003 n. 196 "Codice in materia di protezione di dati personali".

Genova, 17 gennaio 2018

F. TO IL RETTORE

Il responsabile del procedimento:
…….
Per informazioni: Tel. ……

Allegato 1

Piano didattico

Modulo	SSD	CFU	Tot. h insegnamento frontale	h. docenza UNIGE	h. docenza esterna
Parte I: Formazione Culturale					
Introduction to Cybersecurity	ING-INF/01	1,5	16	8	8
Cryptographic Protocols	ING-INF/05	1,5	16	8	8
Information Security Management and Legals	ING-INF/01	2	24	0	24
Network Security	ING-INF/03	3	32	9	23
Computer Security	INF/01	3	32	24	8
TOTALE		**11**	**120**	**49**	**71**
Parte II: Formazione Professionale					
Information Security Management	ING-INF/01	3	32	0	32
Business Continuity and Crisis Management	ING-INF/05	2	24	0	24
Legal Informatics, Privacy and Cyber Crime	IUS/01	3	32	8	24
Fundamentals of Computer Forensics	ING-INF/05	1	8	0	8
Cryptography	INF/01	3	32	32	0
Cybersecurity in Credit System, Management in Incident Response	ING-INF/01	1	16	0	16
Cybersecurity of SCADA Systems	ING-INF/01	1	12	0	12
Social Engineering and Intelligence for Cybersecurity	ING-INF/01	2	20	20	0
Mobile and Cloud Security	ING-INF/05	2	20	20	0
Security and Threats to Critical Infrastructures	ING-IND/31	1	16	8	8
Cybersecurity of Power and Energy Systems	ING-INF/03	1,5	16	8	8
Seminario Confindustria	ING-INF/05	0,5	4	0	4
TOTALE		**21**	**232**	**96**	**136**
Parte III: Specializzazioni					

Indirizzo 1: Vulnerability Assessment & Penetration Testing					
Incident Response and Forensics Analysis	ING-INF/05	3	32	0	32
Malware Analysis	INF/01	2	24	12	12
Web Security	ING-INF/05	2	24	16	8
Mobile Security	ING-INF/05	2	24	24	0
Cyber Exercise	ING-INF/05	1	8	8	0
TOTALE		**10**	**112**	**60**	**52**
Indirizzo 2: Cybersecurity for Industrial Systems					
ICT for Critical Infrastructure Protection	ING-INF/01	1	8	4	4
Cyber Defense and Cyber Intelligence	ING-INF/01	1	16	8	8
Standards and Best Practices in Security and Safety for Industry	ING-INF/01	2	24	0	24
SCADA and Industrial Systems Protection	ING-INF/01	3	32	0	32
Governance Finance	ING-INF/05	1	8	0	8
Security Assurance	ING-INF/05	1	16	0	16
Cyber Exercise	ING-INF/01	1	8	8	0
TOTALE		**10**	**112**	**20**	**92**
Indirizzo 3: Security by Design for Critical Infrastructure Protection					
ICT for Critical Infrastructure Protection	ING-INF/01	1	8	8	0
Cyber Defense and Cyber Intelligence	ING-INF/01	1	16	8	8
Standards and Best Practices in Security and Safety for Industry	ING-INF/05	2	24	0	24
Security-driven Design	ING-INF/05	3	32	0	32
Physical Security	ING-IND/31	1	8	8	0
Risk Propagation in Interconnected Infrastructures	ING-INF/03	1	12	12	0
Crisis Management for Critical Infrastructures	ING-IND/31	1	12	12	0
TOTALE		**10**	**112**	**48**	**64**
Stage e Tesi		**18**	**0**	**0**	**0**

Totale Indirizzo 1		**60**	**464**	**205**	**259**
Totale Indirizzo 2		**60**	**464**	**165**	**299**
Totale Indirizzo 3		**60**	**464**	**193**	**271**

ATTIVITÀ	**N. ORE**	**CFU**
Lezioni frontali e laboratori di gruppo	464	42
Studio individuale; Verifiche di apprendimento	586	
Stage, Project work	450	18
TOTALE	**1500**	**60**

Unione Europea
Fondo Sociale Europeo

REGIONE LIGURIA

Alfa
Agenzia regionale per il lavoro
la formazione e l'accreditamento

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 E STUDENTI
SERVIZIO ALTA FORMAZIONE

D.R. n. 508

IL RETTORE

- Visto il Decreto Rettorale n. 173 del 17.01.2018 con il quale è stato emanato il bando di concorso per l'ammissione al **Master Universitario di II livello in "CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION" I edizione",** attivato per l'anno accademico 2017/2018, presso il Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni" (capofila) e il Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (associato) dell'Università degli Studi di Genova;

- Vista la nota in data 08.02.2018 del Presidente del Master Prof. Rodolfo Zunino, con la quale chiede di apportare le seguenti modifiche ed integrazioni al Decreto n. 173 del 17.01.2018;

D E C R E T A

il Decreto Rettorale n. 173 del 17.01.2018 con il quale è stato emanato il bando di concorso per l'ammissione al Master Universitario II livello in "CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION" I edizione, è modificato come di seguito indicato:

- L'elenco delle aziende che contribuiscono al Master, riportate all'Art. 1, è modificato prevedendo la sostituzione di LRQA le seguenti aziende: Axerta, Eni Gas e Luce, Novotek, SIA;

- Le ore di attività formative d'aula, indicate all'Art. 3, sono modificate da 464 a 460 e le ore di studio individuale e verifiche di apprendimento da 586 a 590. È conseguentemente rettificato il il Piano Didattico di cui all'allegato 1 del Bando;

- Le assenze consentite sul totale di ore corso, indicate all'Art. 3, sono modificate dal 34% al 20% per i non occupati e al 30% per gli occupati;

- Il Comitato di Gestione di cui all'Art. 5 è modificato prevedendo il nominativo di Fabio Cocurullo invece di Stefano Cocurullo;

- L'Art. 6 è integrato con la seguente previsione: "Per ulteriori informazioni consultare la Scheda Informativa validata da Alfa Liguria sul sito https://www.perform.unige.it/master/masterfse/master-cyber-security.html.".

Genova, 13.02.2018

F.TO IL RETTORE

Per informazioni: altaformazione@unige.it (Tel. 010209 5795)