INPS
Istituto Nazionale Previdenza Sociale

ALL. 1

- **Master universitari "Executive" professionalizzanti**

Spett.le INPS

Direzione Regionale Liguria	
Indirizzo	P.zza Borgo Pila, 40 16129 Genova

Proposta di accredito e convenzionamento per Master Executive professionalizzanti per l'anno accademico 2015-2016.

In riscontro all'avviso di selezione pubblicato da codesto Istituto trasmettiamo la presente candidatura:

Soggetto proponente	Università degli Studi di Genova – DIBRIS - Dip.to di Informatica, bioingegneria, robotica e ingegneria dei sistemi
Codice fiscale	00754150100
Indirizzo	Via Balbi, 5 – 16126 Genova
Titolo del percorso formativo proposto	Master Universitario di II livello in "Cyber-Security and Data Protection" II edizione – a.a. 2015/2016
Tipologia del corso (selezionare con una X una o entrambe le tipologie)	master di I livello ☒ master di II livello
Contatti	Rodolfo Zunino Telefono: 010 353 2269 (2650)
	e-mail: rodolfo.zunino@unige.it

Alleghiamo la Scheda Tecnica, debitamente compilata, al fine di comprovare e descrivere il possesso dei requisiti minimi previsti dall'Avviso.

Data, 25 novembre 2015

Firma e timbro del Legale Rappresentante

UNIVERSITA' DI GENOVA

INPS
Istituto Nazionale Previdenza Sociale

La presente scheda, che illustra il progetto formativo presentato, è compilata avendo a riferimento i requisiti minimi per l'accreditamento dei master executive, così come previsti dall'Avviso pubblicato sul sito istituzionale

Soggetti proponenti (specificare l'appartenenza alle categorie di cui all'art. 4 dell'Avviso)	Università degli Studi di Genova – DIBRIS - Dipartimento di Informatica, bioingegneria, robotica e ingegneria dei sistemi L'Università degli Studi di Genova appartiene alle categorie di cui all'art. 4 dell'Avviso.
Titolo e livello del Master	Master universitario di II livello in Cyber-Security and Data Protection II edizione a.a. 2015/2016
Numero massimo di posti di cui si chiede il finanziamento	10
Durata (indicare le date presunte di inizio e termine del master)	1/03/2016 – 28/02/2017
Contenuti formativi (specificare quale delle tematiche definite all'art. 3 dell'Avviso)	***ICT e progettazione*** ***Articolazione dei moduli formativi:*** Parte I: Formazione Culturale Crittografia moderna Protocolli Crittografici Information Security Management and Legals Computer Security Network Security Web Security Parte II: Formazione Professionale Information Security Governance Continuità Operativa e Gestione della Crisi Informatica Legale, Privacy e Crimine Informatico Fondamenti di Computer forensics Critical Infrastructure Protection Cyber Sec nel sistema creditizio, Management in Incident Response La Security nei sistemi SCADA Mobile Security Social Engineering and Intelligence for Cyber Security Cloud Security Parte III: Specializzazioni Incident Response and Forensics Analysis Host Security ICT per Critical Infrastructure Protection CyberDefense e CyberIntelligence SCADA and Industrial system protection

INPS
Istituto Nazionale Previdenza Sociale

Ore di formazione erogate e crediti formativi (indicare il n. ore complessivo di attività didattica e il n. di corrispondenti crediti formativi rilasciati)	Il master della durata di 12 mesi prevede 1500 ore di formazione di cui - 432 ore didattica in aula e laboratorio - 150 ore project work presso Amministrazione di appartenenza o altra Amministrazione - studio individuale Al master sono attribuiti 60 crediti formativi L'orario delle lezioni terrà conto delle indicazioni dell'art. 5.4 dell'Avviso. L'apprendimento verrà monitorato alla fine delle lezioni di ciascun modulo mediante specifiche prove d'esame. Il/la tutor verificherà in modo continuativo il buon andamento del Master, raccogliendo eventuali segnalazioni dagli allievi e facendo da tramite verso il corpo docente ed il Comitato di Gestione.
Titolo del Master svolto nelle 3 precedenti edizioni (art. 5 dell'Avviso - indicare, inoltre, gli AA.AA. in cui sono stati svolti i suddetti corsi e, nel caso di nuovo master, le specifiche materie nell'ambito della relativa tematica disciplinare)	***- Progettisti Sistemi Informatici A.A. 2013-14*** Progettazione orientata agli oggetti Basi dati Ingegneria del Software Reti di Telecomunicazioni Reti telematiche e Servizi di telecomunicazioni Sicurezza delle informazioni in rete e Crittografia ***- Telecomunicazioni A.A. 2011-2012*** Codifica di immagini e di sequenze video Elaborazione numerica dei segnali Reti di telecomunicazioni Comunicazioni mobili Sicurezza delle telecomunicazioni ***- Telecomunicazioni A.A. 2010-2011*** Stesse materie dell'edizione A.A. 2011-2012 ***Nota**: La I Edizione del Master qui proposto (A.A. 2014-2015) non è ancora conclusa: sono terminati le lezioni e gli esami; stanno per iniziare i project work. Si concluderà nel mese di marzo 2016.*
Numero massimo di partecipanti al Master (art. 5.6 dell'Avviso)	***30***
Requisiti richiesti ai candidati per la partecipazione alla selezione	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;

INPS
Istituto Nazionale Previdenza Sociale

Modalità di selezione dei partecipanti (strumenti e metodologia)	***valutazione dei titoli (max. 50 punti):*** laurea conseguita (max.20 punti); votazione di laurea (max. 15 punti); pubblicazioni ed esperienze pregresse (max. 15 punti); ***prova orale (max. 50 punti:*** valutazione del profilo del candidato, suoi interessi ed elementi motivazionali
Direttore/Coordinatore Didattico (nominativo, dichiarazione di esperienza pregressa e incarico attualmente rivestito)	***Presidente del Master: ZUNINO Rodolfo*** ***Professore associato dal 2000*** ***Settore ING-INF/01 Elettronica*** La responsabilità del master è affidata al Comitato di gestione. Compete al Presidente del Master la direzione delle attività. Il Comitato di gestione è costituito dal Presidente del Master, da docenti dei corsi e rappresentanti delle aziende partner.
Corpo docente (nominativi, esperienza maturata, incarico attualmente rivestito, rapporto con il soggetto proponente)	**ZUNINO Rodolfo** - Docente presso l'Università di Genova. Professore Associato dal 2000, è titolare del corso "Cyber Security" (Corso di Laurea in Ingegneria Elettronica) , è coordinatore e responsabile del Laboratorio Sistemi Elettronici Avanzati (SEA Lab). Membro del collegio dei docenti di vari Master di I e II livello nel settore ICT, in particolare: Master SIIT su Sistemi Elettronici Intelligenti Integrati, Master di Ingegneria dei Sistemi Complessi (Scuola FFAA – Chiavari), Master in Cyber-Security and D.P. **ARMANDO Alessandro** - Docente presso l'Università di Genova. Professore Associato, dal 2004, è titolare del corso "Computer Security" (Corso di Laurea Magistrale in Ingegneria Informatica); dirige il Computer Security Laboratory (CSEC). Egli ha inoltre contribuito alla scoperta di una seria vulnerabilità nel SAML-based Single Sign-On for Google Apps e in una vulnerabilità in Android. A partire dal 2010 è responsabile dell'Unità di Ricerca "Security & Trust" del Centro per le Tecnologie dell'Informazione della Fondazione Bruno Kessler a Trento.

Corpo docente (nominativi, esperienza maturata, incarico attualmente rivestito, rapporto con il soggetto proponente)	**CHIOLA Giovanni** - Docente presso l'Università di Genova. Professore ordinario in Sistemi di Elaborazione dell'Informazione, dal 1994, dove insegna corsi di sicurezza informatica, architettura dei calcolatori, sistemi operativi, reti, programmazione, sistemi distribuiti e peer-to-peer, simulazione e valutazione delle prestazioni. È stato inoltre per 3 anni direttore scientifico della Sezione Informatica per le Telecomunicazioni del Consorzio CINI e Principal Ingestigator per il progetto nazionale FIRB WebMINDS. **AIELLO Maurizio** – Docente esterno. Tecnologo presso il Consiglio Nazionale delle Ricerche dal 2001. Membro di Comitati Scientifici e consigli d'Amministrazione; relatore sulle tematiche della Sicurezza Informatica (Senato della Repubblica Italiana, convegni e workshop). Responsabile della Commessa CNR sulla Sicurezza delle Reti. Nomina del Ministro dell'Interno come rappresentante CNR gruppo di lavoro su tematiche inerenti la Sicurezza Nazionale. Docente di "Network Security" presso Università degli studi di Genova e di "Cybercrime Investigation" presso lo University College of Dublin. Collaborazioni tecniche con Procure della Repubblica, Forze di Polizia nazionali ed internazionali, Europol. Delegato del Governo italiano presso UE nel comitato di Horizon 2020 "Secure societies - Protecting freedom and security of Europe and its citizens". **BIANCARDI Marco** – Docente esterno. Ha acquisito diverse esperienze lavorative, prima nel campo delle telecomunicazioni per Ericsson Telecomunicazioni; attualmente è Renewable Automation Sales Support & Cyber Security Business Development Specialist in ABB, ove opera nel campo dei sistemi di controllo SCADA. E' specializzato nell'automazione per le energie rinnovabili e nella Cyber Security per i sistemi di controllo. Ha partecipato a diversi convegni internazionali come relatore su temi relativi alla Sicurezza Informatica **EPIFANI Mattia** - Docente esterno. Attualmente è socio e CEO della REALITY NET - System Solutions di Genova, azienda di consulenza informatica che si occupa di informatica forense e sicurezza informatica. Ha ottenuto diverse certificazione in materia di sicurezza informatica e digital forensics come Certified Forensics Analyst (GCFA), Mobile Device Security Specialist (GMOB), Certified Information Forensics Investigator (CIFI), Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), Certified Computer Examiner (CCE), AccessData Certified Examiner (ACE), AccessData Mobile Examiner (AME), Mobile Phone Seizure Certification (MPSC), Europen Certificate on Cybercrime and Digital Evidence (ECCE). Membro del team di sviluppo degli applicativi opensource iPhone Backup Analyzer, Whatsapp Xtract, SkypeXtractor.

INPS
Istituto Nazionale Previdenza Sociale

Corpo docente (nominativi, esperienza maturata, incarico attualmente rivestito, rapporto con il soggetto proponente)	**MASSA Danilo** – Docente esterno. È un esperto di sicurezza con oltre 12 anni di esperienza nel ruolo e 20 anni nel campo infomatico. Oggi è il CISO di aizoOn Consulting, realtà multinazionale, in cui opera anche come Service Line Manager del settore CyberSecurity. E' quindi responsabile dei servizi di sicurezza erogati dalla Service Line nell'ambito di attività quali vulnerability assessment, penetration testing, progettazione architetture sicure, reverse engineering del malware e consulenze tecniche di parte. Possiede diverse certificazioni GIAC quali GPEN, GCIH, GCFA e GREM. **MEDA Ermete** – Docente esterno. Attualmente è Information Security Manager di Ansaldo STS, Responsabile della Sicurezza delle Informazioni della Corporate. Dal 2000 si occupa di Sicurezza ICT, di risk assessment/management, business continuity e disaster recovery nell'ambito dei progetti di Segnalamento Ferroviario. E' membro del Gruppo di Lavoro Uninfo ISO27000 dedicato alla revisione delle normative internazionali della famiglia ISO27000 per l'Italia. Lead Auditor ISO27001 ed ISO20000, possiede le certificazione ITIL Foundation V.3 e SANS GCFA in Computer Forensics.
Sede didattica e dotazioni strumentali di cui all'art.9 dell'avviso	***Polo didattico di Genova Albaro – Scuola Politecnica dell'Università di Genova*** La Scuola Politecnica metterà a disposizione un'Aula adeguata al numero di partecipanti e a norma di legge. Saranno inoltre disponibili aule informatiche e laboratori didattici attrezzati con apparecchiature e pacchetti software specifici per le materie del Master. Verranno offerti servizi di accesso gratuito ad internet ed alle risorse delle biblioteche dell'Università di Genova.
Registro presenze (*indicare modalità di rilevazione delle presenze)*	Per ogni lezione in aula e in laboratorio, i partecipanti firmano il registro in corrispondenza dell'ora di inizio e di fine presenza.
Descrizione modelli Customer Satisfaction (art.20 dell'avviso)	Questionari per singolo modulo didattico e questionario globale compilati dai partecipanti in merito alla qualità della didattica e all'organizzazione del Master. I questionari verranno somministrati con cadenza almeno quadrimestrale e a conclusione del Master. Il/la tutor consentirà un monitoraggio continuo dell'andamento del Master.
Attività di promozione (art. 12 dell'avviso - modalità e strumenti)	Attività avviata e coordinata con INPS. Pubblicità tramite il Sito web del Master, pieghevole, poster, comunicati dei soci di ISICT (inclusi Confindustria, CCIAA), pubblicità su siti internet a larga diffusione tra i giovani. Giornata dedicata alla presentazione pubblica del Master, giornata dedicata alla consegna dei diplomi.

INPS
Istituto Nazionale Previdenza Sociale

Costo del Master (art. 19 dell'avviso - indicare il costo complessivo del corso; specificare se, e in che misura sussistono, eventuali altre tasse e se sono incluse nel costo del corso).	***€ 6.500 + € 217 di tassa iscrizione all'Università***
Costo di frequenza per privati	***Occupati: € 6.500*** ***Disoccupati o inoccupati: € 2.500*** ***Tutti: € 217 di tassa iscrizione all'Università***
Community on-line (Art. 6 dell'avviso - elencare, dandone sintetica descrizione, i servizi/strumenti utilizzati a supporto dell'ambiente virtuale. Specificare per quanto tempo la Community resterà attiva dopo il master)	**Aula Web:** È attiva una pagina dedicata su AulaWeb – il portale per la didattica on-line dell'Università degli Studi di Genova - che ospita la community on-line. L'accesso è riservato ai partecipanti al Master che accedono al portale con le loro credenziali UniGePASS. I docenti utilizzano la piattaforma per condividere i materiali didattici e per interagire in tempo reale con gli studenti. ***LinkedIn:*** Verrà usato da docenti, allievi ed ex-allievi per offrire opportunità lavorative dopo il conseguimento del titolo e come forum di discussione su argomenti "hot" sulla tematica del Master. ***WhatsApp:*** Strumento on-line per l'interazione immediata tra docenti e allievi e per gli allievi tra di loro. ***La community su LinkedIn resterà attiva almeno fino a 24 mesi dopo la conclusione del Master.***
Project Work (Indicare la durata, specificando il n. di ore, le modalità di svolgimento previste, l'attività di assistenza individuale del tutor, le risorse strutturali; specificare se è prevista la pubblicazione del documento finale del lavoro)	***Durata: 150 ore.*** Esperienza professionalizzante presso l'Amministrazione di provenienza o altra Amministrazione scelte in modo da garantire la disponibilità di apparecchiature informatiche e pacchetti software adeguati (per gli allievi privati si svolgerà presso laboratori universitari o aziendali); a ciascun allievo verranno assegnati un tutor accademico ed uno dell'Amministrazione (o azienda) ospitante; è prevista la pubblicazione on-line del documento finale o di un suo estratto, in relazione alla valutazione della criticità dei temi trattati ed all'autorizzazione a divulgarli.

INPS
Istituto Nazionale Previdenza Sociale

Metodologie didattiche innovative (elencare, dandone adeguata definizione e descrizione, le azioni di didattica innovativa impiegate nel percorso formativo)	***Modulo professionalizzante svolto interamente in azienda.*** Il Master ha una forte connotazione professionalizzante, testimoniata dalla presenza quasi paritaria di docenti esterni da Aziende specializzate. Questo consente di personalizzare la formazione di ogni discente, su tematiche che da un lato sono certamente di alto profilo tecnologico, e dall'altro consentono di incontrare le specifiche preferenze dell'allievo. ***Visita al centro "Security Operation Center" (Fastweb).*** La Cyber Security è connessa in modo imprescindibile con il mondo degli Internet Providers, che da erogatori di servizi TLC sono ora parte attiva nel processo di Security. L'incontro è programmato in un momento inoltrato del Master, affinché la disponibilità di un operatore di primaria grandezza consenta agli allievi di verificare "sul campo" le conoscenze già apprese, e confrontarsi con esperti operativi in materia di protezione e controllo del cyber space. ***Sperimentazione su apparati professionali.*** Per offrire una conoscenza aggiornata degli strumenti professionali, il Master si avvale dei contatti industriali e ospita, nelle attività di laboratorio, apparati 'stato dell'arte' messi a disposizione da primarie industrie, per consentire sperimentazioni. Nel settore networking, queste prevedono configurazioni di Firewall, deployment di Intrusion Detection Systems. Nel settore Forensic, gli allievi sperimenteranno tool di computer forensics quali Encase FTK per simulare acquisizione e incident handling realistici. Nel settore intelligence gli allievi potranno accedere a tecnologie di Text Mining semantico per Open Source Intelligence.

Quanto sopra esposto rappresenta una dichiarazione e corrisponde a quanto presente agli atti del Soggetto Proponente e a manifestazioni di volontà per attività poste in essere e propedeutiche all'attivazione del percorso formativo proposto.

Data, 25 novembre 2015

Firma e timbro del Legale Rappresentante

UNIVERSITA' DI GENOVA