Patrocini

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Master universitario di 2°livello in

Competenze digitali per la protezione dei dati, la cybersecurity e la privacy- Digital competences in data protection, cybersecurity and privacy

Anno accademico 2017-2018

Soggetti organizzatorl

L'**Università degli Studi di Roma "Tor Vergata"/Dipartimento di Management e diritto**, su iniziativa e in collaborazione con le **Parti contraenti l'accordo di Partenariato per il Piano nazionale di formazione in Cybersecurity, Cyberthreat e Privacy** (Università degli Studi di Roma "Tor Vergata", Poste Italiane, Clariter Texi, Pragmema, Profice, Supercom, Istituto per il diritto societario), stipulato in data 5.12.2016, propone il Master universitario di 2°livello in *Competenze digitali per la protezione dei dati, la cybersecurity e la privacy- Digital competences in data protection, cybersecurity and privacy.*

Titolo del Master

Master universitario di 2°livello in Competenze digitali per la protezione dei dati, la cybersecurity e la privacy- Digital competences in data protection, cybersecurity and privacy.

Settori scientifico disciplinari

IUS/04, IUS/05, IUS/07, IUS/09, IUS/10, IUS/13, IUS/14, IUS/17

SECS-P/07, SECS-P/08, SECS-P/10, SECS-P/11

L-LIN/01, ING-INF/01, ING-INF/03, ING-INF/05

Siti internet di riferimento del master

www.cresec.com

www.cybersecurityprivacy.it

Contatti 348 3333682

presidente@eCReSEC.uniroma2.it

elisabetta.zuanelli@uniroma2.it

Costo del Master

Euro 8.000,00 per candidato

Sede didattica del master

Università degli Studi di Roma "Tor Vergata Macroarea di Economia

Durata

Annuale: novembre 2017-novembre 2018

Programma e ore di formazione erogate

Il master avrà la durata di un anno accademico.

L'attività formativa prevede 60 crediti formativi, pari a 1.500 ore di impegno complessivo per lo studente, di cui 385 ore di attività didattica frontale, cioè con la presenza di docenti, lezioni tradizionali, laboratorio guidato, esercitazioni guidate.

Le ore di docenza complessiva nell'ambito del Master saranno ,tuttavia, 525, in quanto inclusive della somma delle ore necessarie per i tre laboratori specialistici che funzioneranno in parallelo ovvero 70 ore moltiplicato per tre di cui solo 70 frequentabili da ciascun studente in base alla specializzazione.

Articolazione

Il Master è articolato in:

- tre assi interdisciplinari di cui è prevista la frequenza comune di tutti i partecipanti, indipendentemente dall'area di specializzazione scelta:

o ASSE 1. La componente giuridico- normativa della protezione dei dati, della privacy e della cybersecurity (105 ORE, 15 crediti)

o ASSE 2. La componente gestionale - aziendalistica della protezione dei dati, cybersecurity e privacy (105 ORE, 15 crediti)

o ASSE 3. La componente tecnologico-digitale per la cybersecurity competence (105 ORE, 15 crediti)

- un quarto asse laboratoriale, specifico per la specializzazione scelta:

o I percorsi laboratoriali specifici di approfondimento saranno 3, uno per Asse (normativo-giuridica, gestionale-aziendalistica, tecnologico-digitale), da 70 ore e 10 crediti ciascuno, frequentabili alternativamente in base all'asse di specializzazione scelto.

o Le ore di docenza totali per l'ASSE 4 saranno complessivamente 210, date dalla somma dei 3 percorsi laboratoriali specialistici di cui al punto precedente.

- La tesi finale, che si aggiunge ai quattro assi di cui sopra, per un massimo di 5 crediti.

- Tirocini da 60 a 120 a 320 ore in istituzioni, aziende ed enti specifici (es. Poste Italiane, NXC, Accademia Nazionale del Notariato, Leonardo, etc.)

- Nel Master sono inclusi moduli rispondenti ai requisiti formativi previsti per le figure professionali definite dalle istituzioni in materia (Garante privacy, Accredia, ISACA, etc), e propedeutici, previo superamento del test di modulo, al sostenimento degli esami per l'acquisizione di certificazioni specialistiche Vendor-Indipendent in ambito Cybersecurity, Data Protection e Privacy. Tali esami non sono inclusi nell'ambito del Master.

Nello specifico, la struttura del master avrà la seguente articolazione per competenze:

ASSE 1: La componente giuridico- normativa della protezione dei dati, della privacy e della cybersecurity (105 ore, 15 crediti, IUS/01, IUS/04, IUS/05, IUS/07, IUS/09, IUS/10, IUS/13, IUS/14, IUS/17) – (LINE 1: Law-regulatory component for Data Protection, Privacy and Cybersecurity)

- MODULO 1.1 (35 ORE - IUS/01, IUS/04, IUS/05, IUS/07).

o La disciplina di settore in materia di cybersecurity e privacy. Le nuove figure professionali in materia di sicurezza e le competenze degli Uffici legali e legislativi. Le filiere di specificità del settore privato: i casi del settore finanziario, bancario e assicurativo. Le strategie nazionali e internazionali, le strutture e gli apparati di gestione.

- MODULO 1.2 (35 ORE - IUS/10, IUS/17)

o Le strategie nazionali e internazionali, le strutture e gli apparati di gestione. Procedure d'implementazione dei processi e metodologie di gestione dell'innovazione nel settore pubblico: il caso del PCP e del PPI. La gestione dei dati e della cybersecurity nei servizi di rilievo pubblico (servizi di utilità generale, infrastrutture critiche). Le filiere di specificità del settore pubblico: i casi della sanità, della previdenza e dei tributi.

- MODULO 1.3 (28 ORE – IUS 13, IUS/14)

o Le norme di contesto: dal CAD alla Direttiva NIS 2016 al Regolamento sulla privacy 2016. Le competenze dei CERT e dei CSIRT secondo la normativa. L'assetto giuridico normativo e le competenze internazionali in materia di cybersecurity e privacy.

- MODULO 1.4 (7 ORE – IUS/09)

o Le Autorità e le competenze nazionali. Profili di tutela giurisdizionale e ammnistrativa.

ASSE 2: La componente gestionale - aziendalistica della protezione dei dati, cybersecurity e Privacy (105 ore, 15 crediti, SECS-P/07, SECS-P/08, SECS-P/10, SECS-P/11) – (LINE 2: Managing-Organizational component for Data Protection, Cybersecurity and Privacy)

- MODULO 2.1 (35 ORE - SECS-P/07, SECS-P/11)

o La gestione del cyber rischio, della cyber threat e della privacy: livelli di strutturazione aziendale e compiti specifici. Modelli di Governance per Data Protection, Risk Management e IT Security secondo gli standard internazionali ISO. Il Cybersecurity framework del NIST nel contesto europeo e nazionale. Il Privacy e Cyber-Security Maturity Model.

- MODULO 2.2 (35 ORE - SECS-P/08)

o Metodi e Tecniche di IT Risk Governance e Management e relazioni con le istituzioni e gli intermediari; assessment ricorrenti e strumenti tecnologici di rilevazione degli attacchi e dei rischi; Correlazione tra assetti di gestione, innovazione tecnologica e rischi: CMS e KMS, Cloud, Mobile, WoT, Industry 4.0, Infrastrutture critiche.

- MODULO 2.3 (35 ORE - SECS-P/10)

o I CERT/CSIRT nella struttura aziendale e istituzionale e i SIEL aziendali. Il DPO e le altre professionalità/responsabilità gestionali per la Cybersecurity. Gli schemi di certificazione personale nazionali ed internazionale e i piani di formazione per la sicurezza e la Privacy: livelli e figure professionali. Aspetti contrattuali dell'offerta e della domanda di servizi digitali in chiave Cybersecurity e Privacy.

ASSE 3: La componente tecnologico-digitale per la cybersecurity competence (105 ore, 15 crediti, L-LIN/01, ING-INF/01, ING-INF/03, ING-INF/05) – (LINE 3: Technologic-Digital Component for Cybersecurity competences)

- MODULO 3.1 (14 ORE – L-LIN/01)

o Minacce, attacchi, modelli APT, tassonomie CERT/CSIRT/ENISA

- MODULO 3.2 (49 ORE – ING-INF/01, ING-INF/03)

o Elementi di crittografia e protezione dei dati; Protocolli per autenticazione, autorizzazione, e sicurezza del trasporto delle informazioni e analisi delle relative vulnerabilità. Sicurezza della rete e dei relativi sistemi (routing, DNS, etc). Monitoraggio e intrusion detection, sicurezza perimetrale, firewall, policies

- MODULO 3.3 (42 ORE ING-INF/05)

o Sicurezza comportamentale e social engineering; Tecniche e strumenti di IT Risk assessment & mitigation secondo lo schema operativo NIST: Identify, Protect, Detect, Respond, Recover

ASSE 4: La componente di specializzazione, composta dai seguenti 3 percorsi laboratoriali alternativi:

- MODULO 4.1 (70 ore, 10 crediti, IUS/01, IUS/05, IUS/07, IUS/09, IUS/13, IUS/14):

o Laboratorio specialistico giuridico-normativo per la protezione dei dati, la privacy e la cybersecurity – (LINE 4.1: Law-regulatory LAB for Data Protection, Privacy and Cybersecurity)

- MODULO 4.2 (70 ore, 10 crediti, SECS-P/07, SECS-P/08, SECS-P/10, SECS-P/11):

o Laboratorio specialistico gestionale-aziendalistico per la protezione dei dati, la privacy e la cybersecurity – (LINE 4.2: Managing-Organizational LAB for Data Protection, Cybersecurity and Privacy)

- MODULO 4.3 (70 ore, 10 crediti, ING-INF/01, ING-INF/03, ING-INF/05):

o Laboratorio specialistico tecnologico-digitale per la cybersecurity competence – (LINE 4.3: Technologic-Digital LAB for Cybersecurity

Stage/Tirocinio formativo

(con esclusione dei corsi di perfezionamento e dei corsi esteri equiparati) Art. 6 dell'avviso.

Indicare la durata e il n. ore dello stage, l'azienda, gli studi professionali o le PP.AA. presso cui gli studenti potranno effettuare il tirocinio nell'ambito del master. Tirocini da 60 a 120 a 320 ore in istituzioni, aziende ed enti specifici (es. Poste Italiane, NXC, Accademia Nazionale del Notariato, Leonardo, etc.)

Direttore/Coordinatore Didattico

Prof. Giorgio Lener: Coordinatore Master e direttore sezione Diritto nel Dip. di Management e diritto Un.Tor Vergata

Prof. Elisabetta Zuanelli: Presidente CReSEC/Un. Tor Vergata, Coordinatore del Partenariato per un Piano di formazione nazionale in cybersecurity, cyberthreat e privacy

Professori ordinari Un. Tor Vergata con esperienza ultra decennale

Corpo docente

Professori ordinari I° fascia e Associati, Ricercatori Università Tor Vergata Proff. G. Lener Coord. Master, E. Zuanelli (Coord. Met.did Master), U. Pomante, Direttore Dip. Management e diritto, R. Lener, G. Bruno, G. Bianchi, G. Loreti, A. Detti

Proff. Esterni altre università): Un. Foggia (ass.) , Un. Sannio (ric.), Un. Luiss (inc.), Lumsa (inc.), Un.Link (inc.)

C.Tedeschi, A. Visaggio, S.Mazzantini, G.Crea, F.Di Resta

Esperti istituzionali esterni: Garante privacy, ABI Lab. Min Difesa, Gat (Guardia di Finanza/ Osservatorio Cybersecurity CReSEC/Tor Vergata), Leonardo (Confindustria. Digitale), CERT

G.Busia (Segr.Generale Aut. Privacy, Comitato strategico CReSEC Tor Vergata), R.Stasi (Dir Gen. ABI Lab rete esterna), S.Gagliano (Gen. Difesa Com.strategico CReSEC/Tor Vergata), G.Parascandolo (Col. GAT in Osservatorio cybersecurity CReSEC/Tor Vergata), G.Mosca (Resp. cibersecurity Conf.digitale, rete esterna Tor Vergata)

Esperti aziendali e partenariato Un. Tor Vergata/ aziende Piano nazionale di formazione in cybersecurity, cyberthreat e privacy: Poste italiane, Profice, Clariter, Pragmema, IGS R.Mammoliti (partenariato Tor Vergata), F. Silvestrini, F.Busico, S.Rubini (docenti esterni Master CReSEC Tor Vergata e partenariato)

Esperti Osservatorio sulla Cybersecurity Un. Tor Vergata, Studi professionali e Aziende F. Marazzi (Marazzi & Partners rete esterna), Martini, F.Santi (DXC/HPE osservatorio cybersecurity CReSEC/Tor Vergata) L.Nobile (DXC/HPE Profice partenariato Tor Vergata) L. Aglieri Cloud Security Alliance rete esterna

Logistica e dotazioni strumentali

Aule didattiche attrezzate e laboratori informatici Macroarea economia/ Un. Tor Vergata

Obiettivo del Master

Art. 1 - Istituzione

È istituito, presso il Dipartimento di Management e Diritto dell'Università degli Studi di Roma "Tor Vergata", su iniziativa ed in collaborazione con le Parti contraenti l'accordo di Partenariato per il Piano nazionale di formazione in Cybersecurity, Cyberthreat e Privacy (Università degli Studi di Roma "Tor Vergata", Poste Italiane, Clariter Texi, Pragmema, Profice, Supercom), stipulato in data 5.12.2016, il Master universitario di 2°livello in Competenze digitali per la protezione dei dati, la cybersecurity e la privacy- Digital competences in data protection, cybersecurity and privacy.

Art. 2 – Finalità

IL Master "Competenze digitali per la protezione dei dati, la cybersecurity e la privacy" (Digital competences in data protection, cybersecurity and privacy) propone un approccio alla sicurezza, alla privacy e alla protezione dei dati inerenti l'uso delle nuove tecnologie digitali (sistemi informativi istituzionali e aziendali pubblici e privati, cloud, applicazioni mobile, IoT, ecc.) fortemente auspicati dall'Unione europea per uno sviluppo e un utilizzo confidente del cyberspazio.

Il Master realizza per la prima volta una dimensione formativa interdisciplinare che verte sulla attivazione di competenze e professionalità inedite in prospettiva giuridico-normativa (addetti e responsabili in uffici legali e legislativi), gestionale-aziendalistica (professionalità di gestione istituzionale e aziendale di analisi e valutazione del rischio attraverso l'istituzione obbligatoria dei profili previsti dalla normativa comunitaria e nazionale (Direttiva NIS e Regolamento privacy da attivare obbligatoriamente a partire dal 2018 per tutti gi Enti, Aziende e Amministrazioni pubblici e privati) segnatamente, il DPO e connessi) e tecnologico-digitale (nuove professionalità inerenti la prevenzione e la resilienza negli attacchi informatici, le applicazioni di sistemi automatici e semiautomatici di protezione, controllo tecnologico e l'addestramento comportamentale degli addetti).

Prospettive occupazionali

Il Master propone soluzioni di alta formazione relative all'istituzione obbligatoria dei profili previsti dalla normativa comunitaria e nazionale (Direttiva NIS e Regolamento privacy da attivare obbligatoriamente a partire dal 2018 per tutti gi Enti, Aziende e Amministrazioni pubblici e privati) segnatamente, il DPO e connessi) e tecnologico-digitale (nuove professionalità inerenti la prevenzione e la resilienza negli attacchi informatici, le applicazioni di sistemi automatici e semiautomatici di protezione, controllo tecnologico e l'addestramento comportamentale degli addetti) ai diversi livelli e per la dirigenza pubblica e privata in materia di Cybersecurity e Privacy, interventi che implicano conoscenze e prassi nei comportamenti singoli e corporate adeguati nell'analisi, nella valutazione e nella gestione del rischio cibernetico.

Requisiti richiesti agli studenti per l'iscrizione

Possono iscriversi candidati provvisti di laurea di 2° livello o laurea quadriennale in materie giuridiche, economiche e ingegneristico-informatiche.

Sono ammesse iscrizioni alla frequenza dei singoli Moduli del Master con riconoscimento dei crediti formativi previsti per ciascun modulo, propedeutici agli esami di certificazione internazionali.

All'atto dell'iscrizione ai candidati sarà somministrato un test di pre-assessment di ingresso per la scelta della specializzazione specifica di uno tra i tre assi del Master: giuridico-normativo,gestionale-aziendalistico, tecnologico-digitale

Registrazione delle presenze

Presenze per giornate e lezioni su registro firme rilevate dai tutor d'aula.

Attività di promozione

Pubblicìzzazione su sito specifico www.cybersecurityprivacy.it , sul sito dell'Università www.uniroma2.it e di Cresec/ Tor Vergata www.cresec.com, sui siti del partenariato, e sui siti di rete esterna.

Il Master gode del patrocinio di AGiD/PCM e Autorità garante della privacy. Con essi, con le istituzioni ed enti sponsor e le istituzioni di sistema (Difesa, Sviluppo economico, MEF, ecc. ABI, Associazioni di Rete, naz. e internazionali) sarà organizzata una Conferenza di presentazione del Master stesso.

E' prevista una pubblicizzazione guidata nei social.

Rilevazione soddisfazione partecipanti

Il Master prevede un sistema di rilevazione e gradimento su schede annotate e statistica per:

- qualità didattica
- clima d'aula

- qualità dei materiali
- soddisfazione generale in prospettiva professionale

secondo i modelli universitari previsti dal Nucleo di valutazione dei Master dell'Università di Tor Vergata.

Azioni di contatto professionale

Sarà organizzata un'attività di placement con invito ad Enti ed aziende e indirizzario fornito ai partecipanti.

Specifiche sessioni di contatto aziendale/istituzionale saranno avviate durante la formazione e in connessione con i laboratori.

Metodologie didattiche

- Lezioni frontali con applicazioni d'aula, studi di caso e lavori di gruppo.
- Applicazioni formative su apprendimento collaborativo d'aula e online.
- Laboratori di specializzazione di 70 ore per asse con tecnologie ICT, modelli/framework europei e nazionali e standard internazionali COBIT, ISO, ecc.
- Simulazioni di ruolo aziendale in materia giuridico-normativa, manageriale economica e ingegneristico-informatica.