MASTER UNIVERSITARIO DI II LIVELLO
in
“Competenze digitali per la protezione dei dati, la cybersecurity e la privacy”
“Digital competences in data protection, cybersecurity and privacy”

STATUTO

Art. 1 - Istituzione
È istituito presso il Dipartimento di Management e Diritto dell’Università degli Studi di Roma “Tor Vergata” 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 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 protezioine, controllo tecnologico e l’addestramento comportamentale degli addetti).
Il Master propone pertanto soluzioni di alta formazione professionale 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.

Art. 3 - Requisiti di ammissione
Possono iscriversi candidati provvisti di laurea di 2° livello o laurea quadriennale in materie giuridiche, economiche e ingegneristico-elettroniche. 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.
Sono ammessi iscritti alla frequenza dei singoli Moduli del Master con riconoscimento dei crediti formativi previsti per ciascun modulo.
E’ possibile l’ammissione di uditori, cioè di partecipanti che non possiedono il titolo necessario per l’accesso ma che sono in possesso di una solida esperienza professionale nell’ambito degli argomenti trattati nel master. Agli uditori verrà rilasciato un certificato di partecipazione senza l’attribuzione di crediti formativi universitari.

Art. 4 - Durata
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.

Art. 5 – 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:
    - ASSE 1. La componente giuridico- normativa della protezione dei dati, della privacy e della cybersecurity (105 ORE, 15 crediti)
    - ASSE 2. La componente gestionale - aziendalistica della protezione dei dati, cybersecurity e privacy (105 ORE, 15 crediti)
    - ASSE 3. La componente tecnologico-digitale per la cybersecurity competence (105 ORE, 15 crediti)
- **un quarto asse laboratoriale**, specifico per la specializzazione scelta:
    - 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.
    - 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 ore in istituzioni, aziende ed enti specifici** (es. Poste Italiane, HPE, 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 ultimi esami per il conseguimento delle predette certificazioni specialistiche 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).*
    - 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)*
    - 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)*
    - 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)*
    - 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)*
    - 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)*
    - 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)*
    - 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)*
    - Minacce, attacchi, modelli APT, tassonomie CERT/CSIRT/ENISA
- **MODULO 3.2** *(49 ORE – ING-INF/01, ING-INF/03)*
    - 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)*
    - 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)***:**
    - **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)***:**

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

Art. 6 - Verifica del profitto

Alla fine di ciascun asse sarà somministrato un test scritto di profitto sotto forma di quesiti a scelta multipla e/o tesina e/o esercitazione pratica. Ogni prova si intenderà superata al raggiungimento di almeno 18 punti su 30. La prova finale, consistente nella discussione di una tesi, sarà valutata invece su una scala di 110, con votazione minima di 66/110.

Art. 7 - Sede amministrativa

La sede amministrativa sarà il Dipartimento di Management e Diritto / Macroarea Economia / Università di degli Studi di Roma "Tor Vergata".

Art. 8 - Sede delle attività didattiche

La sede delle attività didattiche sarà il Dipartimento di Management e Diritto / Macroarea Economia / Università degli Studi di Roma "Tor Vergata".

Art. 9 – Docenti del Master

I docenti del Master sono nominati dal Consiglio del Dipartimento.

Art. 10 - Organi del Master

Sono organi del Master: il Collegio dei docenti del Master, il Coordinatore e il Comitato Scientifico.

Art. 11 - Collegio dei docenti del Master

1. Il Collegio dei docenti del Master è costituito dai professori dell'Ateneo, di prima o seconda fascia o ricercatori, in numero non inferiore a tre, che siano titolari di insegnamenti impartiti nel corso o di altre attività di insegnamento esplicitamente previste dallo statuto del master. Alle sedute del Collegio dei docenti partecipano, senza che la loro presenza concorra alla formazione del numero legale e senza diritto di voto, i docenti esterni.
2. Il Collegio dei docenti del Master ha compiti di indirizzo programmatico, sovrintende al coordinamento delle attività didattiche e determina, inoltre, nei limiti delle risorse finanziarie disponibili, il compenso per i docenti interni ed esterni e per il personale tecnico-amministrativo dei Dipartimenti o dei Centri interessati, nonché le spese per seminari, conferenze e convegni ed ogni altro costo di gestione, predisponendo preventivamente un piano di spese.

Può proporre di attivare, convenzioni con lo Stato, la Regione, il Comune ed altri enti pubblici e privati, ed in particolare associazioni, fondazioni ed imprese con o senza scopo di lucro e di accettare liberalità da parte di soggetti pubblici, privati e da persone fisiche.

Art. 12 - Coordinatori del Master

1. Il Coordinatore ha la responsabilità didattica del Master**,** sovrintende al suo funzionamento, coordina le attività e cura i rapporti esterni.

Attesta e autorizza tutti gli atti di gestione anche inerenti alla liquidazione delle spese, ove delegato dal Direttore del Dipartimento. Al termine del Master riferisce al Collegio dei docenti circa le iniziative

effettuate. Convoca e presiede gli organi del master. Predispone, sulla base delle direttive del Collegio dei docenti, la relazione finale del master. Può adottare provvedimenti di urgenza sottoponendoli a ratifica del Collegio dei docenti del Master.
2. Il Coordinatore dura in carica, 3 anni ed è nominato dal Collegio dei Docenti del Master tra i professori dell'Ateneo di prima o seconda fascia o ricercatori che assicurino un numero di anni di servizio almeno pari alla durata del mandato prima della data di collocamento a riposo.
3. Il Coordinatore può delegare l'esercizio di talune funzioni a docenti componenti il Collegio dei docenti del Master.

Art. 13 - Comitato Scientifico
Il Comitato Scientifico ha funzioni di indirizzo generale del Master e di proposta. Ne fanno parte docenti dell'Ateneo, eminenti personalità nel panorama delle discipline impartite nel master, esperti designati anche da altre Università, da Organismi Internazionali e dell'Unione Europea.

Art. 14 - Iscrizione al Master universitario
Il numero massimo di partecipanti al master è fissato in 30 e il numero minimo in 10, esclusi gli iscritti ai singoli assi.
La quota di iscrizione è pari ad 8.000 Eu, da versare secondo le seguenti modalità:

- 50% all'atto dell'iscrizione
- 50% all'avvio del Master.

Sono previste borse di studio per neolaureati.
La contribuzione per gli uditori è di 4.000,00 Eu.
E' prevista l'iscrizione ai singoli Moduli, per un importo riproporzionato rispetto al numero di ore del modulo rispetto all'intero Master, con riconoscimento dei relativi crediti formativi previsti, previa verifica del profitto, che darà luogo ad un certificato di frequenza.

Il certificato di frequenza e il superamento del test saranno, altresì, correlati al riconoscimento dei profili professionali previsti dalle Autorità in materia (Garante Privacy, Accredia, ISACA, etc.), previo superamento degli esami previsti dai relativi schemi di certificazione e non inclusi nel Master.

I moduli ad iscrizione singola previsti sono:

- **MODULO 1.1** *(35 ORE, 5 CFU - IUS/01, IUS/04, IUS/05, IUS/07):*
  - 1.050 Eu
- **MODULO 1.2** *(35 ORE, 5 CFU - IUS/10, IUS/17):*
  - 1.050 Eu
- **MODULO 1.3** *(28 ORE, 4 CFU – IUS 13, IUS/14):*
  - 840 Eu
- **MODULO 1.4** *(7 ORE, 1 CFU – IUS/09):*
  - 250 Eu
- **MODULO 2.1** *(35 ORE, 5 CFU - SECS-P/07, SECS-P/11):*
  - 1.050 Eu
- **MODULO 2.2** *(35 ORE, 5 CFU - SECS-P/08):*
  - 1.050 Eu
- **MODULO 2.3** *(35 ORE, 5 CFU - SECS-P/10):*
  - 1.050 Eu

- **MODULO 3.1** *(14 ORE, 2 CFU – L-LIN/01):*
  - 500 Eu
- **MODULO 3.2** *(49 ORE, 7 CFU – ING-INF/01, ING-INF/03):*
  - 1.470 Eu
- **MODULO 3.3** *(42 ORE, 6 CFU ING-INF/05):*
  - 1.260 Eu
- **MODULO 4.1** *(70 ORE, 10 CFU, IUS/01, IUS/04, IUS/05, IUS/07, IUS/09, IUS/13, IUS/14)***:**
  - 1.800 Eu
- **MODULO 4.2** *(70 ORE, 10 CFU, SECS-P/07, SECS-P/08, SECS-P/10, SECS-P/11)***:**
  - 1.800 Eu
- **MODULO 4.3** *(70 ORE, 10 CFU, ING-INF/01, ING-INF/03, ING-INF/05)***:**
  - 1.800 Eu

Art. 15 - Obbligo di frequenza
I partecipanti al master hanno un obbligo di frequenza non inferiore al 70% delle ore di attività didattica. La frequenza sarà verificata tramite la raccolta delle firme di presenza.

Art. 16 - Conseguimento del titolo
L'attività formativa svolta nell'ambito del Master è pari a 60 crediti formativi. A conclusione del Master agli iscritti che abbiano adempiuto agli obblighi didattico-amministrativi e superato le prove di verifica del profitto e la prova finale viene rilasciato il diploma di Master universitario di II. livello in "**Competenze digitali per la protezione dei dati, la cybersecurity e la privacy" -** "Digital competences in Data Protection, Cybersecurity and Privacy".

Art. 17 - Risorse Finanziarie
Le risorse finanziarie disponibili per il funzionamento del Master sono costituite dai proventi delle iscrizioni e dai finanziamenti derivanti da contratti e convenzioni con enti pubblici e privati e da liberalità dei medesimi Enti o persone fisiche.

Art. 18 - Rinvio
Per quanto non contemplato nel presente statuto si rinvia al Regolamento per l'attivazione e l'organizzazione dei Master Universitari e dei Corsi di perfezionamento.