MASTER DI 2º LIVELLO in
CYBERSECURITY & PRIVACY

COMPETENZE DIGITALI PER LA PROTEZIONE DEI DATI, LA *CYBERSECURITY* E LA *PRIVACY*

Master multidisciplinare con specializzazione giuridica, gestionale e tecnologica

8ª EDIZIONE
2024 - 2025
FORMULA EXECUTIVE
ROMA

PATROCINI

Per il Piano di formazione nazionale in *cybersecurity, cyberthreat* e *privacy*:

AGENZIA PER L'ITALIA DIGITALE
PRESIDENZA DEL CONSIGLIO DEI MINISTRI

Per il Master di II livello in "Competenze digitali per la protezione dei dati, la *cybersecurity* e la *privacy*":

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

IL MASTER IN SINTESI

IMPEGNO

- ✓ frequenza 1 settimana *full immersion* al mese

REQUISITI

- ✓ Laurea di II livello o
- ✓ Laurea quadriennale

ISCRIZIONI

- ✓ entro il 15 marzo 2025

DURATA

- ✓ lezioni in aula: 12 mesi + *project work*, fino a marzo 2026

COSTO

- ✓ 8.000,00 € per candidato
- ✓ disponibili borse di studio

SEDE

- ✓ Roma, presso Università degli Studi di Roma «Tor Vergata», Facoltà di Economia

QUALIFICHE E CERTIFICAZIONI

PERCHE' PARTECIPARE

Il Master universitario di II livello "Competenze digitali per la protezione dei dati, la *cybersecurity* e la *privacy*" rappresenta un'opportunità di crescita e specializzazione professionale unica perché:

- la *faculty* dei docenti annovera i rappresentanti delle principali istituzioni nazionali ed europee in tema di *privacy* e *cybersecurity* (*es. Garante privacy, ENISA, DIS, ABI, ACN, Guardia di Finanza, etc.*), i dirigenti delle aziende di riferimento per i settori critici e per la consulenza tecnologica e, infine, professionisti esperti e *opinion leader* riconosciuti a livello internazionale
- il percorso si sviluppa in modo multidisciplinare, formando profili esperti congiuntamente in ambito giuridico, manageriale e tecnologico
- i corsi del Master abilitano gli allievi a sostenere gli esami per l'acquisizione di certificazioni professionali specialistiche riconosciute a livello internazionale in ambito cybersecurity, data protection e privacy (DPO-Data Protection Officer, ISACA CSX cybersecurity fundamentals, COBIT5 for NIST cybersecurity di APMG international, ISO27001 (sistemi di info security), ISO20000-1 (servizi IT) e ISO22301 (sistemi di business continuity) auditor/lead auditor, etc.)

COME PARTECIPARE

Nel sito dell'università:

- il bando per la partecipazione ai Master
- la tabella, in cui nella prima pagina è presente il master "Competenze digitali per la protezione dei dati, la cybersecurity e la privacy" , con gli importi da versare e le relative date di scadenza

PROGRAMMA

ASSE 1 GIURIDICO-NORMATIVO

MODULO INTRODUTTIVO

- Lo stato dell'arte della minaccia cibernetica
- Le norme di contesto italiano dell'innovazione digitale: il nuovo CAD
- Le tematiche giuridiche del diritto Internet (monopoli, concorrenza, *privacy*)
- *Cybersecurity*, *data protection*, *privacy*: UE, Nato, USA

MODULO 1

- La disciplina di settore in materia di *privacy* e *cybersecurity*
- La gestione dei dati e della *cybersecurity* nei servizi di rilievo pubblico (servizi di utilità generale, infrastrutture critiche)
- Le nuove figure professionali in materia di sicurezza e le competenze degli uffici legali e legislative
- Le filiere di specificità del settore privato: i casi del settore finanziario, bancario e assicurativo

MODULO 2

- Le strategie nazionali e internazionali, strutture e apparati di gestione
- Procedure d'implementazione dei processi e metodologie di gestione dell'innovazione nel settore pubblico: il caso del PCP e del PPI
- Le filiere di specificità del settore pubblico

MODULO 3

- Le norme di contesto: il Codice *Privacy* e il Regolamento generale sulla protezione dei dati del 2016; la direttiva NIS 2 e il decreto nazionale attuativo (d.lgs. n. 138/2024) ; DORA
- La componente del CERT e dei CSIRT secondo la normativa

MODULO 4

- Le autorità e le competenze nazionali. Profili di tutela giurisdizionale e amministrativa

ASSE 2 GESTIONALE-AZIEDALISTICO

MODULO 1

- La governance nel *cyber* rischio, nella *cyber threat* e nella *privacy*: livelli di strutturazione aziendale e compiti specifici
- Il DPO e le altre figure professionali per la *privacy* (GDPR:2016) e la *cybersecurity* (NIS:2016), responsabilità gestionali e adempimenti organizzativi
- Il *Cybersecurity Framework* del NIST nel contesto europeo e nazionale
- Il *Cyber-Security Maturity Model*
- Modelli di *governance* per *data protection*, *risk management* e IT *security* per il *cloud*

MODULO 2

- Metodi e tecniche e professionalità di IT *risk* & *security governance* e *management*, *assessment* ricorrenti e strumenti tecnologici di rilevazione degli attacchi e dei rischi
- Correlazione tra assetti di gestione, innovazione tecnologica e rischi: Infrastrutture critiche

MODULO 3

- I CERT/CSIRT nella struttura aziendale e istituzionale
- I SIEL aziendali: infrastrutture critiche (Enel, Eni, Terna, etc.)
- Aspetti contrattuali dell'offerta e della domanda di servizi digitali in chiave *cybersecurity* e *privacy*

ASSE 3 TECNOLOGICO-DIGITALE

MODULO 1

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

MODULO 2

- 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.)

MODULO 3

- Sicurezza comportamentale e *social engineering*
- Tecniche e strumenti di IT *risk assessment* & *mitigation*
- Monitoraggio e *intrusion detection*, sicurezza perimetrale, *firewall, policies*
- La certificazione CSX Cybersecurity Fundamentals di ISACA
- La certificazione COBIT5 for NIST Cybersecurity di APMG

SPECIALIZZAZIONI SELEZIONABILI

SPECIALIZZAZIONE GIURIDICO – NORMATIVA (ASSE 4.1)	• *Law-regulatory* LAB for *data protection, privacy and cybersecurity* • *Privacy Lab*: applicazione del GDPR • *Cybersicurezza* e protezione dati negli studi legali e professionali • La *privacy* nella sanità: forme di attuazione e soluzioni gestionali • La *privacy* nel bancario e nell'assicurativo • La *privacy* nelle IoT e *big data analytics*
SPECIALIZZAZIONE GESTIONALE - AZIEDALISTICA (ASSE 4.2)	• Principi, *tool* e *framework* a disposizione del *board* delle organizzazioni per pianificare e controllare il rischio *cyber* • Laboratorio ISO27001 e *information security risk assessment*: come farlo in pratica e come collegarlo alla governance aziendale e alla *compliance* • Laboratorio ISO20000-1: IT *service management*: implementare un sistema di gestione dei servizi IT • Laboratorio ISO22301 di *business continuity*, *disaster recovery* e *crisis & incident management*: applicazione pratica • Laboratorio di applicazione tecniche di *risk management* • *Framework* NIST e verticalizzazioni di settore
SPECIALIZZAZIONE TECNOLOGICO – DIGITALE (ASSE 4.3)	• Laboratorio di *malware analysis* • Laboratorio di *penetration testing* • Laboratorio di *network security* • Tecniche operative di prevenzione e di intervento in esempi di casi reali • *Vulnerability Assessment*: laboratorio di attività di difesa

PROJECT WORK

Al fine di consentire agli studenti di applicare ad un contesto reale le competenze e gli strumenti acquisiti durante il percorso didattico, negli ultimi mesi del Master ogni studente viene chiamato a sviluppare un progetto con la supervisione e la guida di un mentore.
Il *project work* prevede l'assegnazione di un progetto di consulenza da implementare presso il proprio datore di lavoro o appoggiandosi a una delle organizzazioni partner dell'Università degli Studi di Roma «Tor Vergata».
L'ambito del progetto viene individuato insieme al mentore, considerando le eventuali proposte da parte dello studente e dell'organizzazione di appoggio, e verte necessariamente su un tema connesso all'ambito di specializzazione scelto dallo studente.

STAGE QUALIFICANTE (facoltativo)

A conclusione, per gli studenti che lo richiedono, è possibile accedere alle selezioni per essere inseriti in uno *stage* qualificante da 60 a 120 ore presso istituzioni, aziende partner ed enti specifici, al fine di perfezionare l'applicazione sul campo delle competenze acquisite.

CONTATTI E INFORMAZIONI

Per informazioni didattiche rivolgersi a:

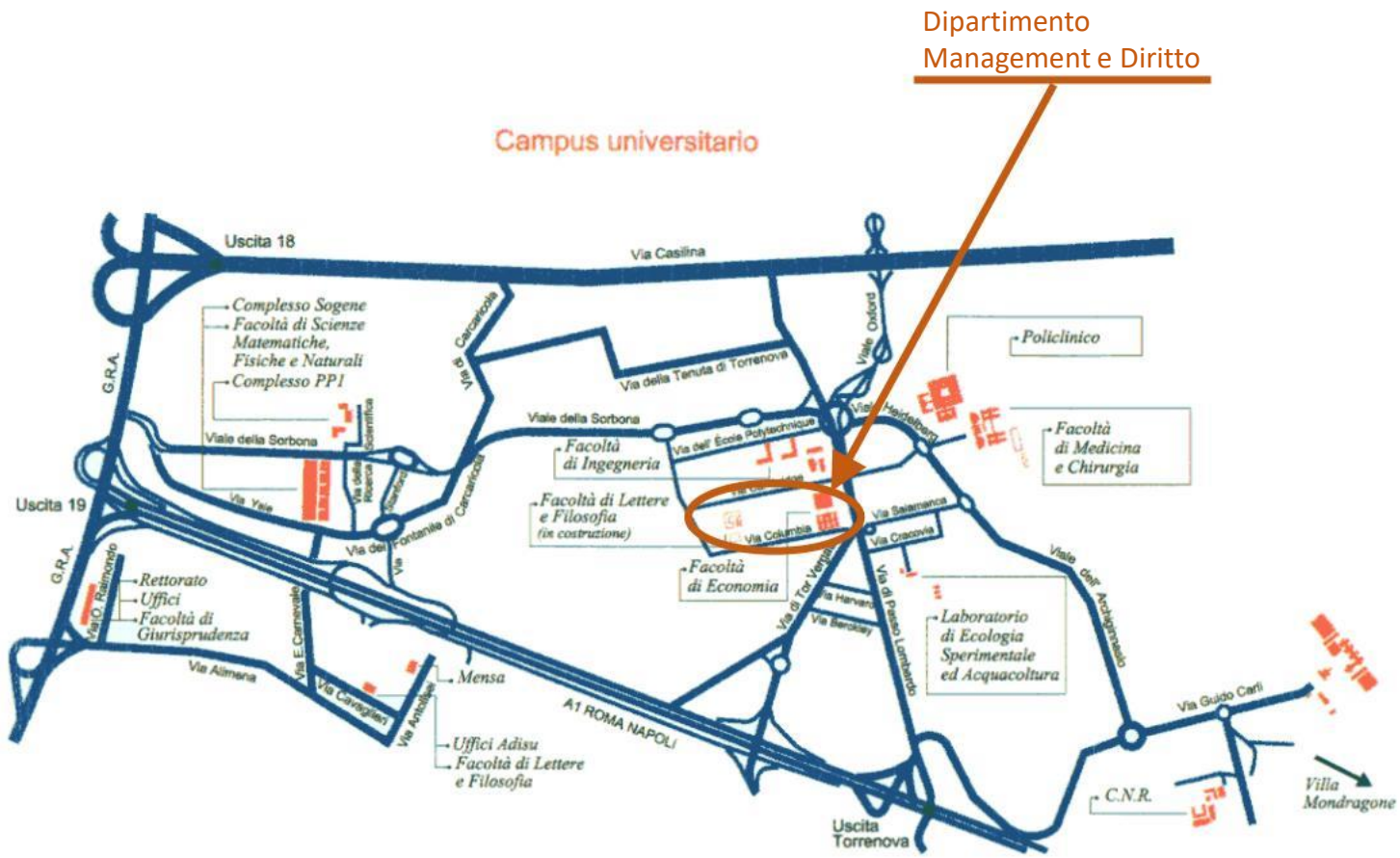
- segreteria didattica del Master:
  - tel.: (+39) 349 144 3152
  - e-mail catherinecappelli@hotmail.com
  - web: http://www.cybersecurityprivacy.it/master/master-in-cybersecurity-e-privacy.html

Per informazioni di tipo amministrativo rivolgersi a:

- sportello Master e corsi di perfezionamento dell'Università degli Studi di Roma "Tor Vergata":
  - tel.: (+39) 06 7259 2223
  - e-mail segreteriamaster@uniroma2.it
  - web: http://web.uniroma2.it/module/name/Content/newlang/italiano/navpath/SEG/section_parent/5996

LOGISTICA

La sede del Master è il Dipartimento di Management e Diritto / Macroarea Economia dell'Università degli Studi di Roma "Tor Vergata", Via Columbia 2, 00133 Roma



TOR VERGATA
UNIVERSITA' DEGLI STUDI DI ROMA