

MASTER DI 2° LIVELLO

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

Master multidisciplinare con specializzazione giuridica, gestionale e tecnologica

3^a EDIZIONE
APRILE 2020 - APRILE 2021
FORMULA EXECUTIVE
ROMA

CON IL PATROCINIO DI:



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

CON LA COLLABORAZIONE DI:



AGENZIA PER L'ITALIA DIGITALE
PRESIDENZA DEL
CONSIGLIO DEI MINISTRI

SOGGETTI ORGANIZZATORI



Membri del Partenariato *cybersecurity privacy* (www.cybersecurityprivacy.it)



PATROCINI E COLLABORAZIONI

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

PATROCINIO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

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

COLLABORAZIONI



AGENZIA PER L'ITALIA DIGITALE
PRESIDENZA DEL
CONSIGLIO DEI MINISTRI

IL MASTER IN SINTESI

REQUISITI

- ✓ Laurea di II livello o
- ✓ Laurea quadriennale

IMPEGNO

- ✓ frequenza nei week-end
- ✓ Laboratori specialistici
formula una settimana
continuativa per 70 ore
- ✓ Inizio lezioni aprile 2020

ISCRIZIONI

- ✓ entro il 10/02/2020

DURATA

- ✓ lezioni in aula: 12 mesi + *project work*
fino ad aprile 2021

COSTO

- ✓ 8.000,00 € per candidato
- ✓ 4.000,00 € per uditori
- ✓ disponibili borse di studio

SEDE

- ✓ Roma, presso Università degli Studi di Roma «Tor Vergata», Facoltà di Economia, Via Columbia 2, 00133 Roma

QUALIFICHE E CERTIFICAZIONI

ESPERTO IN CYBERSICUREZZA, DATA PROTECTION E PRIVACY

Specializzazione
giuridico
normativa

per la *cybersecurity* e
l' *information security*

Specializzazione
gestionale
aziendalistica

della protezione dei dati,
cybersecurity e *privacy*

Specializzazione
tecnologico
digitale

per la
cybersecurity competence

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 docenti universitari specialisti della materia, rappresentanti delle principali istituzioni nazionali ed europee in tema di *privacy* e *cybersecurity* (es. Garante per la protezione dei dati personali, AgID, MISE, Ministero dell'Interno, Ministero della Difesa, ENISA, DIS, ABI, etc.), 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
- Alcuni cicli didattici sono finalizzati a consentire ai partecipanti di sostenere esami di certificazione. Sono previsti, su richiesta, seminari specifici esterni al Master e connessi con lo stesso per specifiche **certificazioni professionali specialistiche riconosciute a livello internazionale in ambito *cybersecurity*, *data protection* e *privacy***: DPO Data Protection Officer, ISACA CSX *cybersecurity fundamentals*, COBIT 2019 for NIST *cybersecurity* di APMG international, ISO27001 (sistemi di *info security*), ISO20000-1 (servizi IT) e ISO22301 (sistemi di *business continuity*), etc.

INDICE

CONTESTO

Scenario di riferimento	6
Obiettivi del Master	6
Sbocchi occupazionali	6

STRUTTURA DEL MASTER

Articolazione Master	7
Percorso comune	8
Specializzazioni selezionabili	9
<i>Project work</i>	9
Stage qualificante	9
Certificazioni conseguibili	10

ORGANIZZATORI E DOCENTI

Coordinamento Master	11
Corpo docente	11
Soggetti organizzatori	12
Patrocinio e collaborazioni	13

ISCRIZIONE

Requisiti di ammissione	14
Quota di partecipazione	14
Domanda di ammissione	14
Contatti e informazioni	15
Logistica	15

CONTESTO

SCENARIO DI RIFERIMENTO

Aziende, pubbliche amministrazioni, istituzioni e infrastrutture critiche richiedono con urgenza sempre maggiore di presidiare in modo strutturato le necessità di *cybersecurity*, di *privacy* e di *IT risk governance*. Lo squilibrio tra queste esigenze e la carenza di competenze specialistiche in grado di gestirne la complessità sempre crescente sono amplificati dalla recente introduzione di nuove norme comunitarie e nazionali nonché di standard internazionali, tra cui, a solo titolo d'esempio:

- la **Direttiva UE 2016/1148** (c.d. **Direttiva NIS**) sulla protezione di reti e sistemi informativi per gli enti e le aziende che erogano servizi essenziali e servizi digitali;
- Il **Regolamento UE 2016/679** (c.d. **GDPR**) in materia di protezione dei dati personali, la cui adozione è obbligatoria a decorrere da maggio 2018;
- Il **Cybersecurity Framework del NIST**, ormai assunto a modello di riferimento per la *cybersecurity* nei settori finanziari e industriali;
- Il **Regolamento UE 2019/881** (c.d. **Cyber Act**) che ha introdotto un *framework* unico di certificazione per i prodotti, processi e servizi ICT all'interno dell'Unione Europea;
- Il **Decreto Legge n. 105/2019** convertito con modificazioni dalla Legge 18 novembre 2019, n. 133 recante **Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica**.

OBIETTIVO DEL MASTER

Questo Master dà risposta alla carenza di esperti nelle tematiche di *cybersecurity*, *IT risk governance*, *data protection* e *privacy*, attraverso un percorso multidisciplinare di alta formazione finalizzato a preparare professionisti e manager dotandoli:

- dei **requisiti di competenza trasversali previsti dagli standard internazionali** (es. DPO per la *privacy*, *auditor* dei sistemi di gestione della sicurezza delle informazioni o per la continuità operativa, esperti in *cybersecurity risk management*, etc.);
- di **professionalità specialistiche** in termini di conoscenze e prassi operative in ambito:
 - **giuridico-normativo**, di particolare interesse per gli uffici legali e legislativi;
 - **gestionale-aziendalistico**, per applicare gli strumenti di *IT risk & security governance*;
 - **tecnologico-digitale**, per presidi tecnologie della sicurezza.

SBOCCHI OCCUPAZIONALI

Specializzazione giuridico-normativa: responsabili e addetti negli uffici legali e legislativi e in settori sensibili, quali istituzioni economico-finanziarie, servizi di utilità generale, infrastrutture critiche, sanità e previdenza, AAPP.

Specializzazione gestionale-aziendalistica: *consulenti/advisor in cybersecurity e privacy*; responsabili e addetti alla *privacy* e alla *data protection* nelle pubbliche amministrazioni e nelle aziende italiane ed estere; professionisti e manager esperti nella *governance* del rischio IT, della *cybersecurity* e della *privacy*.

Specializzazione tecnologico-digitale: specialista *cybersecurity* in ambito altamente tecnico (es. livello CERT-CSIRT) per pubbliche amministrazioni ed aziende italiane ed europee; nuove professionalità inerenti la prevenzione e la resilienza negli attacchi informatici, le applicazioni di sistemi automatici e semiautomatici di protezione e controllo tecnologico.

STRUTTURA DEL MASTER

ARTICOLAZIONE DEL MASTER

Il **Master universitario di II livello** “Competenze digitali per la protezione dei dati, la *cybersecurity* e la *privacy*” richiede 1.500 ore di impegno complessivo per lo studente nell’arco di un anno accademico, pari a 60 crediti formativi (CFU), articolate in:

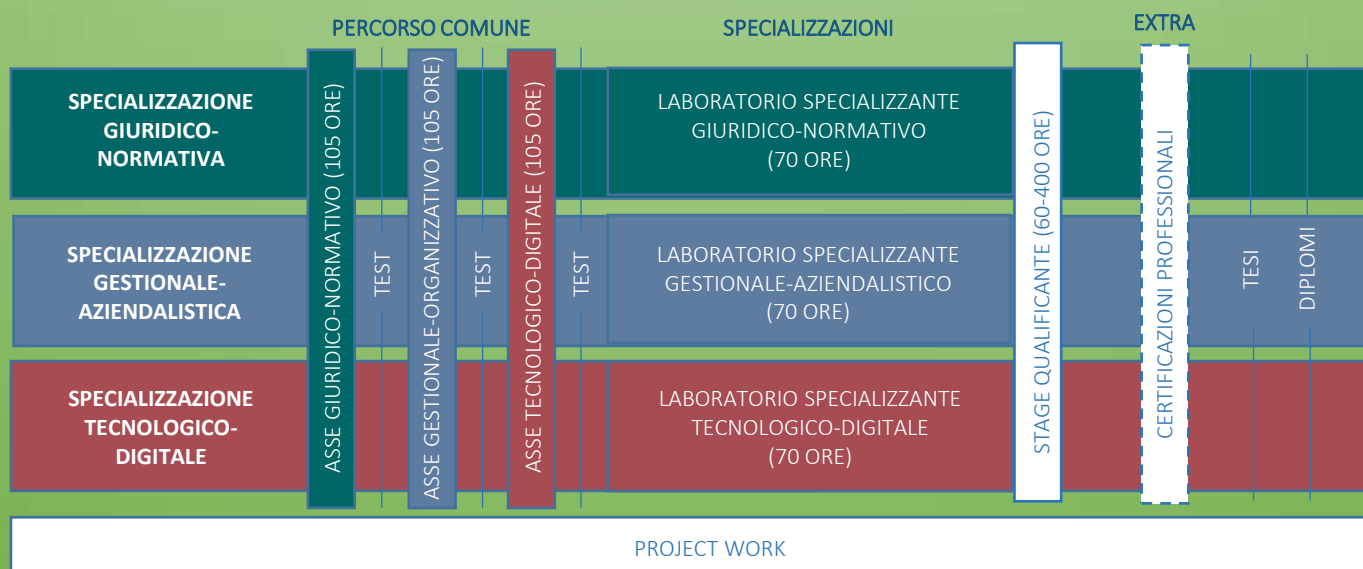
- 315 ore, [+25 ore per i beneficiari dei bandi INPS] (45 CFU) di attività **didattica frontale multidisciplinare** sui temi **giuridico-normativi (105 ore)**, **gestionali-aziendalistici (105 ore)** e **tecnologico-digitali (105 ore)**
- 70 ore (10 CFU) di **specializzazione verticale** tramite **laboratori interattivi ed esercitazioni pratiche** individuali e di gruppo con la supervisione del docente
 - **l’ambito di specializzazione viene scelto dallo studente** all’inizio del Master tra 3 indirizzi alternativi:
 - giuridico-normativo
 - gestionale-aziendalistico
 - tecnologico-digitale
- **studio individuale, eventi extra-curricolari e *project work* finale** (5 CFU) a copertura delle ore restanti.
- elaborazione di ***project work* di gruppo**

Sono previsti test per la verifica dell’apprendimento al termine di ogni asse, comprensivi della valutazione in *progress* del *project work*.

Il percorso di Master si conclude con una sessione finale di presentazione delle tesi risultanti dal *project work* a una commissione giudicatrice.

A tutti gli studenti che avranno frequentato il Master, superato le prove di verifica del profitto e presentato con successo la tesi finale viene rilasciato il **diploma di Master universitario di II Livello in “Competenze digitali per la protezione dei dati, la *cybersecurity* e la *privacy*”, con specializzazione giuridico-normativa, gestionale-aziendalistica o tecnologico-digitale** in base alla scelta di studi fatta.

Le lezioni degli Assi teorici prevedono una frequenza concentrata mediamente nel venerdì e nel sabato. Le lezioni degli Assi laboratoriali saranno erogate in una settimana continuativa (dal lunedì al venerdì, 5 giornate da 7 ore). Il totale di ciascun Asse laboratoriale è di 70 ore (due settimane totali).



PERCORSO COMUNE

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, Cina

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 legislativi
- 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
- Le filiere di specificità del settore pubblico e privato

MODULO 3

- Le norme di contesto: il Codice *Privacy*, il Regolamento UE 2016/679 e il d.lgs. n. 231/2001.
- Le competenze dei CERT e dei CSIRT secondo la normativa
- La direttiva NIS, il *Cyber Act*, il Perimetro Nazionale di sicurezza cibernetica, 5G e *Golden Power*

MODULO 4

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

ASSE 2
GESTIONALE-AZIENDALISTICO
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
- CSX *Cybersecurity Fundamentals* di ISACA
- COBIT 2019 for NIST *Cybersecurity* di APMG
- Il *Cyber-Security Maturity Model*
- Modelli di *governance* per *data protection*, *risk management* e *IT security* per il cloud

MODULO 2

- Metodi, 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

- Standard di prodotti e servizi digitali e *framework* europeo ENISA
- Struttura e compiti delle Autorità NIS, del punto unico di contatto CSIRT, del coordinamento nazionale ed europeo
- I centri di valutazione

MODULO 4

- I CERT/CSIRT nella struttura aziendale e istituzionale
- I SIEL/SOC 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*

SPECIALIZZAZIONI SELEZIONABILI

SPECIALIZZAZIONE GIURIDICO – NORMATIVA (ASSE 4.1)	• <i>Law-regulatory LAB for data protection, privacy and cybersecurity</i> • <i>Privacy Lab</i>: applicazione del GDPR • <i>Cybersecurity</i> e protezione dati negli studi legali e professionali • La <i>privacy</i> nella sanità: forme di attuazione e soluzioni gestionali • La <i>privacy</i> nel bancario e nell'assicurativo • La <i>privacy</i> nelle IoT e <i>big data analytics</i>
SPECIALIZZAZIONE GESTIONALE - AZIENDALISTICA (ASSI 4.1 , 4.2)	• Laboratori di approfondimento di IT <i>governance</i>, <i>data protection</i> e <i>cybersecurity</i> nelle banche e nelle assicurazioni • Gestione CERT banche e coordinamento ABI Lab • Laboratorio ISO27001 e <i>information security risk assessment</i>: come farlo in pratica e come collegarlo alla governance aziendale e alla <i>compliance</i> • Laboratorio ISO20000-1: IT <i>service management</i>: implementare un sistema di gestione dei servizi IT • Laboratorio ISO22301 di <i>business continuity</i>, <i>disaster recovery</i> e <i>crisis&incident management</i>: applicazione pratica • Tecniche di IT <i>auditing</i> secondo la norma ISO19011 • Laboratorio di applicazione tecniche di <i>risk management</i> • Laboratorio implementazione <i>privacy</i> secondo gli standard ISO 29134, ISO 29151, ISO 27017 e 27018 • <i>Framework NIST</i> e verticalizzazioni di settore
SPECIALIZZAZIONE TECNOLOGICO – DIGITALE (ASSE 4.3)	• Laboratorio di <i>malware analysis</i> • Laboratorio di <i>penetration testing</i> • Laboratorio di <i>network security</i> • Tecniche operative di prevenzione e di intervento in esempi di casi reali

PROJECT WORK

Al fine di consentire agli studenti di applicare ad un contesto reale le competenze e gli strumenti che acquisiscono durante il percorso didattico, ogni studente viene chiamato a sviluppare un progetto di gruppo (*project work*) con la supervisione e la guida di un mentore.

Il *project work* prevede la possibilità di implementazione 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

A conclusione è prevista, per i partecipanti interessati, la possibilità di frequentare un tirocinio formativo da 60 a 400 ore presso istituzioni, aziende partner ed enti specifici, al fine di perfezionare l'applicazione sul campo delle competenze acquisite.

CERTIFICAZIONI CONSEGUIBILI

Nel Master sono inclusi cicli didattici rispondenti ai requisiti formativi previsti per le figure professionali definite dalle istituzioni in materia (Accredia/AICQ-SICEV, ISACA, APMG, etc.) e propedeutici al sostenimento degli esami per l'acquisizione delle certificazioni in ambito *cybersecurity*, *data protection* e *privacy* precedentemente elencate.

Gli esami per il conseguimento delle certificazioni non sono inclusi nell'ambito del Master e sono facoltativi.

Per gli studenti che intendano avvalersi dell'opportunità di conseguire alcune o tutte le certificazioni disponibili, vengono messi a disposizione seminari complementari esterni al Master e su richiesta, insieme alle sessioni d'esame ufficiali con la supervisione degli enti di certificazione o di organizzazioni da questi riconosciute.

Certificazioni connesse con il percorso comune

DPO – Data Protection Officer secondo le UNI 11697:2017	Certificazione conforme ai requisiti del Profilo dirigenziale richiesto dal GDPR 679/2016 a supporto obbligatorio delle aziende europee più coinvolte dai rischi <i>privacy</i> , che prevede esperienza e competenze avanzate di <i>privacy</i> in ambito giuridico, organizzativo, tecnologico	
CSX – Cybersecurity Fundamentals	Livello di certificazione di base previsto da ISACA per le competenze in ambito <i>cybersecurity</i> , in accordo alla classificazione del <i>Cybersecurity framework</i> del NIST	
COBIT 2019 for NIST Cybersecurity	Certificazione di APMG International che fornisce le competenze fondamentali per definire gli obiettivi di controllo di IT Governance e IT Audit per la <i>cybersecurity</i> in accordo col <i>framework</i> internazionale COBIT 2019	

Certificazioni connesse con la specializzazione gestionale-aziendalistica

UNI EN ISO 19011:2018 A/LA	Certificazione internazionale che fornisce le competenze riconosciute dagli standard internazionali ISO 19011:2018 sulle tecniche di <i>auditing</i> necessarie ad eseguire le verifiche di <i>compliance</i> di un sistema di gestione aziendale	
UNI CEI ISO IEC 27001:2017 A/LA	Certificazione internazionale che crea profili di <i>auditor</i> ufficiali in grado di coordinare l'implementazione e verificare la <i>compliance</i> di un sistema di gestione per la sicurezza delle informazioni e <i>data protection</i> rispetto alla norma ISO 27001:2017	
UNI EN ISO 20000-1:2018 A/LA	Certificazione internazionale che crea profili di <i>auditor</i> ufficiali in grado di coordinare l'implementazione e verificare la <i>compliance</i> di un sistema di gestione dei servizi IT rispetto alla norma ISO 20000-1:2018	
ISO 22301:2019 A/LA	Certificazione internazionale che crea profili di <i>auditor</i> ufficiali in grado di coordinare l'implementazione e verificare la <i>compliance</i> di un sistema di gestione per la continuità operativa e il <i>disaster recovery</i> rispetto alla norma ISO 22301:2012	

ORGANIZZATORI E DOCENTI

COORDINAMENTO MASTER

Prof. GIORGIO LENER

coordinatore Master e
vice direttore del dip. di Management e Diritto, Università
degli Studi Roma "Tor Vergata"

Prof.ssa ELISABETTA ZUANELLI

responsabile scientifico Master, pres. CReSEC, Università degli
Studi Roma "Tor Vergata", coordinatore Partenariato per il Piano di
formazione nazionale in *cybersecurity*, *cyberthreat* e *privacy*

CORPO DOCENTE

UNIVERSITA'	ISTITUZIONI	AZIENDE e PROFESSIONISTI
• G. Bianchi (Professore ordinario Università degli Studi Roma "Tor Vergata") • M. Bonola (Ingegnere, Ph. D. Università degli Studi di Roma "Tor Vergata") • G. Bruno (Professore ordinario Università degli Studi Roma "Tor Vergata") • A. Caponi (Ricercatore Consorzio naz. interuniversitario per le TLC) • M. Cataudella (Professore ordinario e Capo dipartimento di management e diritto Università degli Studi Roma "Tor Vergata") • C. Cilli (Professore incaricato Università degli Studi Roma "La Sapienza") • G. Crea (Professore incaricato Università Europea di Roma) • C. Cupelli (Professore associato Università degli Studi Roma "Tor Vergata") • V. Farina (Professore associato Università degli Studi di "Tor Vergata") • G. Lener (Professore ordinario Università degli Studi Roma "Tor Vergata") • R. Lener (Professore ordinario Università degli Studi Roma "Tor Vergata") • S. Mazzantini (Avvocato, professore incaricato Università degli Studi Roma "LUISS") • C. Tedeschi (Professore associato Università degli Studi Roma "La Sapienza") • C.A. Visaggio (Professore associato Università del Molise "Unisannio") • E. Zuanelli (Professore ordinario/Emerito Università degli Studi Roma "Tor Vergata")	• E. Albamonte (Presidente ANM - Associazione nazionale magistrati) • L. Bolognini (Presidente Istituto italiano per la <i>privacy</i> e la valorizzazione dei dati) • G. Busia (Coordinatore del Comitato europeo per la protezione dei dati (EDPB, UE)) • N. Ciardi (Direttore Polizia postale – Min. interno) • G. Contristano (Capo Uff. Ops. CIOC) • R. Forsi (già Direttore generale ISCOM - Istituto Superiore Comunicazioni e Tecnologie dell'Informazione - Mise) • S. Gagliano (Generale Divisione Aerea, docente Sicurezza e Difesa) • C. Giustozzi (Esperto di sicurezza cibernetica - AgID) • S. Mari (Ingegnere - CERT Nazionale Italiano) • F. Martinelli (CNR - ESCO) • S. Ramacciotti (Capo ufficio Sicurezza Difesa) • G. Reccia (Comandante del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza) • F. Silvestrini (Direzione centrale Sistemi informativi e dell'innovazione - MEF) • R. Stasi (Direttore generale ABI Lab) • F. Tortorelli (già dirigente Agid) • M. Trinchera (<i>Technical Coordinator</i> Cert Fin)	• R. Abeti (Avvocato <i>ICT</i>, professore incaricato di Diritto e Informatica Giuridica, Partner EXP <i>Legal</i>) • D. Benedetti (<i>Security solution architect</i> – DXC Technology) • M. S. Busico (Consulente esperto in <i>ICT</i> e sistemi <i>open source</i>) • A. Capobianco (CEO Fata informatica) • F. Di Resta (Avvocato, esperto <i>privacy</i>) • R. Mammoliti (Responsabile sicurezza - Poste italiane) • N. Martini (<i>Privacy officer</i> certificato, <i>Associate Partner</i> Head of <i>Data Protection</i> Roedl & Partners) • L. Nobile (<i>Security Principal</i> Italia - DXC Technology) • F. Pacchiarotti (<i>Cybersecurity consultant</i> - Bl4ckSwan) • R. Randazzo (<i>IT/Info Security Consultant</i> – Auditor CSQA) • S. Rubini (Ingegnere elettronico, esperto di <i>ICT</i> e <i>cybersecurity</i>) • F. Santi (<i>Security Principal</i> Sud Europa - DXC Technology) • A. Toma (Responsabile «<i>Incident Prevention and Management</i>» di Poste Italiane)

SOGGETTI ORGANIZZATORI

  Partenariato cybersecurity privacy	L'Università degli Studi di Roma "Tor Vergata" (www.uniroma2.it), ispirata al modello dei campus anglosassoni, è articolata in 6 macroaree (Economia, Giurisprudenza, Ingegneria, Lettere e Filosofia, Medicina e Chirurgia, Scienze matematiche, fisiche e naturali), 18 dipartimenti, 29 laboratori informatici, 108 corsi di laurea, di cui 16 internazionali e 150 percorsi post-laurea. Il Partenariato <i>cybersecurity</i> e <i>privacy</i> (www.cybersecurityprivacy.it) è una forma di partenariato pubblico-privato promosso nel 2016 dall'Università degli Studi di Roma "Tor Vergata" attraverso il CReSEC (Centro di Ricerca e Sviluppo sull'E-Content, www.cresec.it) per attivare collaborazioni con una rete di aziende, al fine di creare un piano nazionale di formazione in materia di <i>cybersecurity</i>, <i>cyberthreat</i> e <i>privacy</i> con il patrocinio dell'AgID - Agenzia per l'Italia Digitale. Il Master è una delle attività concepite e progettate dal Partenariato.
--	--

MEMBRI DEL PARTENARIATO

	Il CReSEC (www.cresec.com) organizza, promuove e coordina attività di alta formazione, ricerca e sviluppo sull'e-content. Nella <i>cybersecurity</i> ha attivato l'osservatorio sulla <i>cybersecurity</i> dal 2013 e promosso il Partenariato <i>cybersecurity</i> e <i>privacy</i> nel 2016, realizzato un ciclo di tavole rotonde su <i>cybersecurity</i> e <i>privacy</i> in collaborazione con il GAT della Guardia di finanza e altri soggetti pubblici e privati.
	Gruppo Clariter (www.clariter.it) fornisce supporto ICT presso aziende di rilievo nazionale e internazionale in ambito: <i>cybersecurity</i> (<i>vulnerability assessment</i>, <i>application security</i>, <i>hybrid cloud security</i>, SIEM, APT, <i>security analytics</i>); portali multicanale (<i>order management</i>, <i>enterprise billing reporting</i>); tecnologie e metodologie di SW <i>testing</i>.
	L'Istituto per il Governo Societario (www.istitutogovernosocietario.it) è un'associazione con l'obiettivo di promuovere l'approfondimento e lo sviluppo di soluzioni e modelli di governo societario.
	Poste Italiane è la più grande infrastruttura in Italia nel recapito, nella logistica, nel settore del risparmio, nei servizi finanziari e assicurativi. Poste Italiane è stata tra le prime aziende a dotarsi di un <i>Campus</i> tecnologico che tutela, 24 ore su 24, la sicurezza delle comunicazioni e delle transazioni finanziarie.
	Pragmema (www.pragmema.it) è una società che eroga servizi di architettura cognitiva logico-semantiche e di interattività nel campo della comunicazione digitale, della formazione ICT/sicurezza informatica e dell'organizzazione in <i>Internet</i> e <i>intranet</i> (<i>business intelligence</i>, motori di ricerca, tassonomie e indicizzazioni di dominio, valutatori automatici di interattività, <i>big data analytics</i>).
	Profice (www.profice.it) è una società di formazione <i>executive</i> e di editoria specialistica B2B con particolare riferimento ai temi di <i>compliance & innovation</i> in ambito IT <i>governance</i>, <i>privacy</i>, <i>cybersecurity</i> (ISACA, COBIT5, ITIL, ISO A/LA, DPO, etc).
	Supercom (www.supercom.it), è la piattaforma di <i>business relations</i> che offre servizi avanzati di comunicazione, eventi, relazioni istituzionali e <i>content management</i>, come strumenti di sostegno alle attività delle aziende e delle pubbliche amministrazioni centrali e locali.
	GT50 (www.gt50.org) è una Azienda Innovativa. E' focalizzata nel trasformare la tecnologia in applicazioni reali. GT50 ha più di 30 anni di esperienza in sicurezza e protezione digitale. E' impegnata ad associare diverse tecnologie esistenti e consolidate, come il Timbro Digitale e il QR Code, per migliorare la sicurezza e creare soluzioni nell'applicazione di certificazioni digitali.
	Fata Informatica S.r.l è una società che opera dal 1994 nel campo delle tecnologie dell'informatica e delle telecomunicazioni fornendo servizi specialistici ad alto valore aggiunto riguardanti la progettazione, la realizzazione, l'integrazione e la gestione dei sistemi e delle infrastrutture informatiche complesse.

PATROCINIO E COLLABORAZIONI



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

PATROCINIO

Il Garante per la protezione dei dati personali (www.gdpd.it) è un'autorità amministrativa indipendente istituita dalla legge n. 675 del 31 dicembre 1996 (cosiddetta legge sulla *privacy*), per assicurare la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali.

Tra i diversi compiti del Garante rientrano quelli di: controllare che i trattamenti siano effettuati nel rispetto delle norme di legge; ricevere ed esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati; vietare i trattamenti illeciti o non corretti ed eventualmente disporre il blocco; promuovere la sottoscrizione di codici di deontologia e buona condotta; curare la conoscenza della disciplina in materia di trattamento dei dati personali e in materia di misure di sicurezza dei dati; denunciare i fatti configurabili come reati perseguibili d'ufficio conosciuti nell'esercizio delle sue funzioni; tenere il registro dei trattamenti.



**AGENZIA PER L'ITALIA
DIGITALE
PRESIDENZA DEL CONSIGLIO
DEI MINISTRI**

COLLABORAZIONE

L'Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica.

AgID ha il compito di coordinare le amministrazioni nel percorso di attuazione del Piano Triennale per l'informatica della Pubblica amministrazione, favorendo la trasformazione digitale del Paese.

AgID sostiene l'innovazione digitale e promuove la diffusione delle competenze digitali anche in collaborazione con le istituzioni e gli organismi internazionali, nazionali e locali (www.agid.gov.it).

ISCRIZIONE

REQUISITI DI AMMISSIONE

Possono iscriversi candidati provvisti di laurea di 2° livello o laurea quadriennale in materie giuridiche, economiche e ingegneristico-elettroniche e, su valutazione del coordinamento scientifico del Master, saranno ammessi laureati di estrazione diversa sulla base dei titoli didattici e professionali presentati. 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.

E' possibile l'ammissione di uditori, limitatamente a coloro 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 sola partecipazione, senza l'attribuzione di crediti formativi universitari.

QUOTA DI PARTECIPAZIONE

La **quota di partecipazione ordinaria** è di **€ 8.000,00**, oltre accessori, da versare come segue:

- **I° quota:** € 4.146,00 all'immatricolazione, **entro il 09/03/2020** (comprensivi dell'importo di € 16,00 della marca da bollo virtuale e del contributo di € 130,00 per il rilascio della pergamena finale);
- **II° quota:** € 4.000,00 **entro il 06/04/2020**.

La **quota di partecipazione per gli uditori** è di **€ 4.000,00**, oltre accessori, da versare come segue:

- **I° quota:** € 2.146,00 all'immatricolazione, **entro il 09/03/2020** (comprensivi dell'importo di € 16,00 della marca da bollo virtuale e del contributo di € 130,00 per il rilascio della pergamena finale);
- **II° quota:** € 2.000,00 **entro il 06/04/2020**.

Il Collegio dei docenti del Master potrà deliberare, nei casi e con le modalità previste dal regolamento, la concessione di benefici economici a titolo di copertura totale o parziale della quota di iscrizione.

DOMANDA DI AMMISSIONE

1. Compilare la domanda di ammissione **entro e non oltre il 10/02/2020** in modalità on-line, seguendo le istruzioni indicate nella sezione PROCEDURA DI PREISCRIZIONE del file "ISTRUZIONI PROCEDURE", nella sezione allegati della pagina web della Segreteria Master e Corsi di Perfezionamento:
 - http://web.uniroma2.it/module/name/Content/newlang/italiano/navpath/SEG/section_parent/5996 (selezionare Facoltà di Economia, Codice Corso PCZ).
2. Versare il pagamento del contributo di pre-iscrizione, convalidato con il codice AUTH apposto dalla banca UNICREDIT sulla ricevuta.
3. Inviare, **entro il 10/02/2020**, all'indirizzo e-mail christianferrari91@gmail.com, la seguente documentazione:
 - Domanda di ammissione scaricata e stampata dal sito <http://delphi.uniroma2.it> ;
 - Curriculum vitae;
 - Autocertificazione di laurea ai sensi del D.P.R 28.12.2000, n. 445, con indicazione dei voti riportati negli esami di profitto e del voto finale di conseguimento del titolo (il modulo è reperibile alla pagina http://web.uniroma2.it/module/name/Content/newlang/italiano/navpath/SEG/section_parent/5996);
 - Eventuali ulteriori titoli.

Il numero massimo di partecipanti al corso è pari a 30, mentre il numero minimo è pari a 10.

Qualora il numero delle domande ecceda la disponibilità massima di posti, l'ammissione avverrà sulla base di graduatorie formate dal Collegio dei docenti. La mancata immatricolazione entro la data di scadenza comporterà rinuncia.

L'elenco degli ammessi sarà pubblicato a partire dal 18/02/2020 sul sito web <http://www.uniroma2.it>.

CONTATTI E INFORMAZIONI

Per le informazioni didattiche rivolgersi a:

- **segreteria didattica del Master:**
 - tel.: (+39) 393 154 6225
 - e-mail christianferrari91@gmail.com
 - web <http://www.cybersecurityprivacy.it/master/master-in-cybersecurity-e-privacy.html>

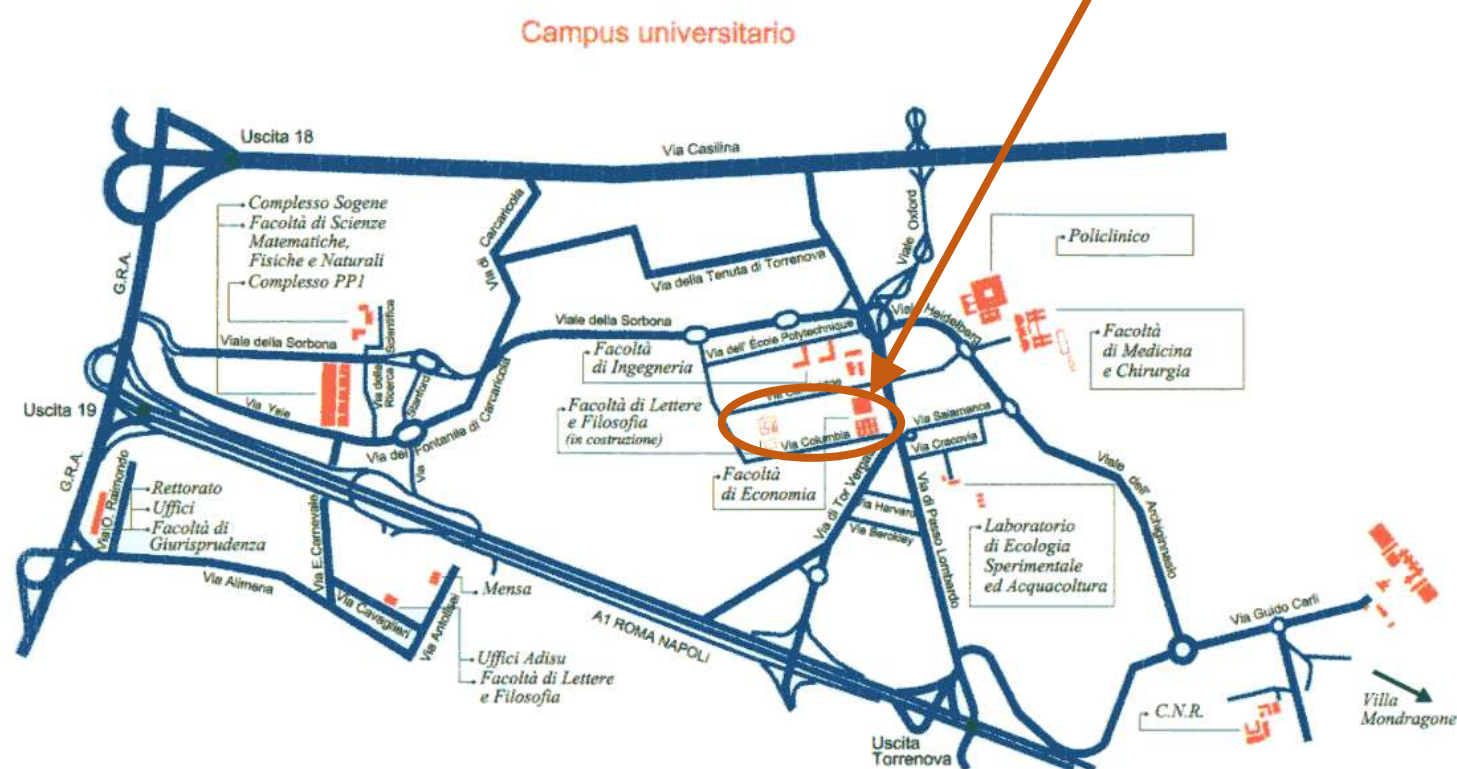
Per le informazioni di tipo amministrativo rivolgersi a:

- **sportello Master e corsi di perfezionamento dell'Università degli Studi di Roma "Tor Vergata":**
 - tel.: (+39) 06 7259 2223
 - e-mail segreteriaamaster@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

Dipartimento
Management e Diritto



TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

PARTNER PROMOTORI



PATROCINIO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

COLLABORAZIONI



AGENZIA PER L'ITALIA
DIGITALE
PRESIDENZA DEL
CONSIGLIO DEI MINISTRI