Università di Roma Tor Vergata

Partenariato cybersecurity privacy

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

2ª EDIZIONE
FEBBRAIO 2019 - FEBBRAIO 2020
FORMULA EXECUTIVE
ROMA

CON IL PATROCINIO DI:

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

CON LA COLLABORAZIONE DI:

intertek Total Quality. Assured.

CSQA

ISACA Sistemi informativi: averne fiducia e trarne valore
Capitolo di Milano

SOGGETTI ORGANIZZATORI

Università di Roma Tor Vergata

Partenariato cybersecurity privacy

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

Università di Roma Tor Vergata · clariter · GT 50 VISIONARY INNOVATORS · IGS · Posteitaliane · pragmema · Profice · SUPERCOM

PATROCINI E COLLABORAZIONI

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

PATROCINIO

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*":

PATROCINIO

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

COLLABORAZIONI

intertek Total Quality. Assured. · CSQA · ISACA Sistemi informativi: averne fiducia e trarne valore Capitolo di Milano

IL MASTER IN SINTESI

REQUISITI

- ✓ Laurea di II livello o
- ✓ Laurea quadriennale

IMPEGNO

- ✓ frequenza 1 settimana *full immersion* al mese
- ✓ Inizio lezioni 18 febbraio 2019

ISCRIZIONI

- ✓ entro il 18 gennaio 2019

DURATA

- ✓ lezioni in aula: 12 mesi + project work fino a febbraio 2020

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

QUALIFICHE E CERTIFICAZIONI

ESPERTO IN CYBERSICUREZZA, *DATA PROTECTION* E *PRIVACY*

Specializzazione giuridico normativa	Specializzazione gestionale aziendalistica	Specializzazione tecnologico digitale
per la *cybersecurity* e l' *information security*	della protezione dei dati, *cybersecurity* e *privacy*	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*, *COBIT5 for NIST cybersecurity* di *APMG international*, ISO27001 (sistemi di *info security*), ISO20000-1 (servizi *IT*) e ISO22301 (sistemi di *business continuity*), etc.

ENTI CERTIFICANTI

ISACA — Sistemi informativi: averne fiducia e trarne valore

APMG International — Accrediting Professionals

aicq sicev

ISACA **APMG** **AICQ-SICEV**

INDICE

CONTESTO

SCENARIO DI RIFERIMENTO

Aziende, pubbliche amministrazioni, istituzioni e infrastrutture critiche richiedono con urgenza sempre maggiore di presidiare in modo strutturato le necessità di cybersicurezza, 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 NIS** del 2016 sulla protezione dei dati per gli enti e le aziende che erogano servizi essenziali e servizi digitali;
- il nuovo **Regolamento GDPR 679/2016 sulla *privacy*,** 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.

OBIETTIVO DEL MASTER

Questo Master dà risposta alla carenza di esperti nelle tematiche di cybersicurezza, 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 *cybersecurtity 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 *cybersicurezza* 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:

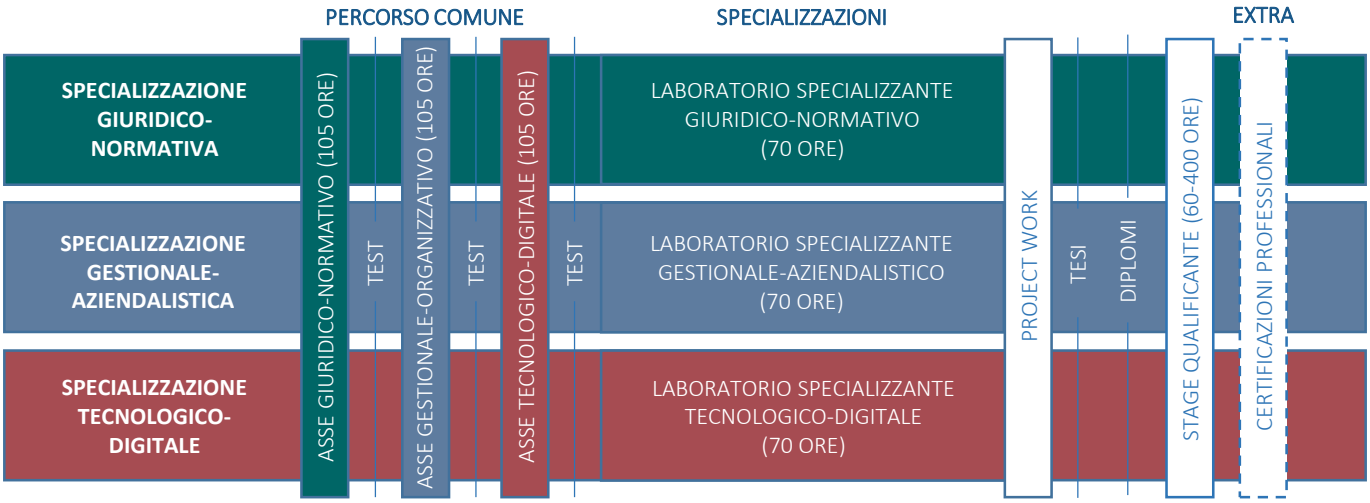
- 315 ore, [+25 ore per i beneficiari dei bandi INPS] (45 CFU) di attività **didattica frontale multidisciplinare sui temi giuridico-normativi (105 ore), gestionali-aziendalistici (105 ore) e tecnologico-digitali (105 ore**)
- 70 ore (10 CFU) di **specializzazione verticale tramite laboratori interattivi 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-curriculari e *project work* finale** (5 CFU) a copertura delle ore restanti.

Sono previsti test per la verifica dell'apprendimento al termine di ogni asse tematico e di ogni percorso laboratoriale di specializzazione.

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 e i laboratori prevedono una frequenza concentrata mediamente in una settimana al mese (5 giornate da 7 ore), in modo da conciliare eventuali esigenze di spostamento degli studenti e la continuità degli impegni.



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

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

MODULO 3
- Le norme di contesto: il Codice *Privacy* e il Regolamento generale sulla protezione dei dati del 2016
- Le competenze dei CERT e dei CSIRT secondo la normativa

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
- 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

MODULO 4
- 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*
- CSX Cybersecurity Fundamentals di ISACA
- 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 - AZIENDALISTICA (ASSI 4.1 , 4.2)	• Laboratori di approfondimento di IT *governance*, *data protection* e *cybersecurity* nelle banche e nelle assicurazioni • Gestione CERT banche e coordinamento ABI Lab • 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 • Tecniche di IT *auditing* secondo la norma ISO19011 • Laboratorio di applicazione tecniche di *risk management* • Laboratorio implementazione *privacy* secondo gli standard ISO 29134, ISO29151, ISO27018 • *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

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 OBBLIGATORIO

A conclusione, è previsto l'obbligo 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 *privacy*, che prevede esperienza e competenze avanzate di *privacy* in ambito giuridico, organizzativo, tecnologico
CSX – *Cybersecurity Fundamentals*	Livello di certificazione di base previsto da ISACA per le competenze in ambito *cybersecurity*, in accordo alla classificazione del *Cybersecurity framework* del NIST
COBIT5 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 *cybersecurity* in accordo col *framework* internazionale COBIT5

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 *auditing* necessarie ad eseguire le verifiche di *compliance* di un sistema di gestione aziendale
UNI CEI ISO IEC 27001:2014 A/LA	Certificazione internazionale che crea profili di *auditor* ufficiali in grado di coordinare l'implementazione e verificare la *compliance* di un sistema di gestione per la sicurezza delle informazioni e *data protection* rispetto alla norma ISO 27001:2014
UNI EN ISO 20000-1:2018 A/LA	Certificazione internazionale che crea profili di ***auditor*** ufficiali in grado di coordinare l'implementazione e verificare la *compliance* di un sistema di gestione dei servizi IT rispetto alla norma ISO 20000-1:2018
ISO 22301:2012 A/LA	Certificazione internazionale che crea profili di ***auditor*** ufficiali in grado di coordinare l'implementazione e verificare la *compliance* di un sistema di gestione per la continuità operativa e il *disaster recovery* 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'

- G. Bianchi (Professore ordinario Università degli Studi Roma "Tor Vergata")
- M. Bonola (Ingegnere, Ph. D. Università degli Studi Roma "Tor Vergata")
- G. Bruno (Professore ordinario Università degli Studi Roma "Tor Vergata")
- A.Caponi (Ricercatore Consorzio naz. interuniversitario per le TLC)
- 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")
- U. Pomante (Professore ordinario e Direttore Dipartimento Management e diritto, Università degli Studi Roma "Tor Vergata")
- 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")

ISTITUZIONI

- E. Albamonte (Presidente ANM - Associazione nazionale magistrati)
- L. Bolognini (Presidente Istituto italiano per la *privacy* e la valorizzazione dei dati)
- G. Busia (Segretario generale Autorità Garante per la protezione dei dati personali)
- N. Ciardi (Direttore Polizia postale – Min. interno)
- R. Forsi (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)
- P. Poletti (Presidente Securitalia - *Security Solutions*)
- F. Silvestrini (Direzione centrale Sistemi informativi e dell'innovazione - MEF)
- R. Stasi (Direttore generale ABI Lab)
- F. Vestito (Responsabile Comando Interforze Operazioni Cibernetiche – CIOC – Min. Difesa)

AZIENDE e PROFESSIONISTI

- R. Abeti (Avvocato *ICT*, professore incaricato di Diritto e Informatica Giuridica, Partner EXP *Legal*)
- L. Aglieri (Presidente Associazione *Cloud for Defence*)
- M.S. Busico (Consulente esperto in ICT e sistemi *open source*)
- F. Di Resta (Avvocato, esperto *privacy*)
- R. Mammoliti (Responsabile sicurezza - Poste italiane)
- F. Marazzi (Avvocato esperto *privacy*, professore incaricato di Diritto Internazionale – Marazzi & Associati)
- N. Martini (*Privacy officer* certificato, *Associate Partner Head of Data Protection Roedl & Partners*)
- L. Nobile (*Security Principal* Italia - DXC *Technology*)
- F. Pacchiarotti (Cyber*security consultant* - Bl4ckSwan)
- C. Pomodoro (*Partner Info Security* - HSPI)
- R. Randazzo (IT/Info *Security Consultant – Auditor* CSQA)
- S. Rubini (Ingegnere elettronico, esperto di *ICT* e *cybersecurity*)
- F. Santi (*Security Principal* Sud Europa - DXC *Technology*)

SOGGETTI ORGANIZZATORI

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. Al suo interno ospita anche il CNR, (Centro Nazionale delle Ricerche), l'ASI (Agenzia Spaziale Italiana) e il Policlinico universitario.

Il Partenariato *cybersecurity* e *privacy* (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 *cybersecurity*, *cyberthreat* e *privacy* 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 *cybersecurity* ha attivato l'osservatorio sulla *cybersecurity* dal 2013 e promosso il Partenariato *cybersecurity* e *privacy* nel 2016, realizzato un ciclo di tavole rotonde su ***cybersecurity*** e ***privacy*** 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: *cybersecurity* (*vulnerability assessment*, *application security*, *hybrid cloud security*, SIEM, APT, *security analytics*); portali multicanale (*order management*, *enterprise billing reporting*); tecnologie e metodologie di SW *testing*; CRM operativo e applicativo; gestione infrastrutture IT e TLC.

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 condivisi tra una pluralità di soggetti aderenti che operano in ordini professionali, imprese, istituzioni e Università.

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 *Campus* tecnologico che tutela, 24 ore su 24, la sicurezza delle comunicazioni e delle transazioni finanziarie. Oggi l'intero sistema postale è governato da una serie di cabine di regia che utilizzano le più evolute soluzioni tecnologiche.

Pragmema (www.pragmema.it) è una società che eroga servizi di architettura cognitiva logico-semantica e di interattività nel campo della comunicazione digitale, della formazione ICT/sicurezza informatica e dell'organizzazione in *Internet* e *intranet* (*business intelligence*, motori di ricerca, tassonomie e indicizzazioni di dominio, valutatori automatici di interattività, *big data analytics*).

Profice (www.profice.it) è una società di formazione *executive* e di editoria specialistica B2B con particolare riferimento ai temi di *compliance & innovation* in ambito IT *governance*, *privacy*, *cybersecurity*. E' partner di formazione con AIEA, DNVGL, CSQA e altre organizzazioni per l'erogazione di corsi per le certificazioni internazionali ISACA, COBIT5, ITIL,, ISO A/LA, DPO, etc.

Supercom (www.supercom.it), è la piattaforma di *business relations* che offre servizi avanzati di comunicazione, eventi, relazioni istituzionali e *content management*, come strumenti di sostegno alle attività delle aziende e delle pubbliche amministrazioni centrali e locali, per rafforzare la *reputation* e consolidare rapporti con il sistema di relazioni del mondo delle istituzioni, dei decisori politici, delle autorità di regolazione, dei *leader* d'opinione, dei media.

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.

PATROCINIO E COLLABORAZIONI

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

PATROCINIO

Il Garante per la protezione dei dati personali (www.gpdp.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 disporne 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.

intertek

COLLABORAZIONE

Intertek (www.intertek.it) fornisce servizi di certificazione accreditati nel settore *Data Protection* e *ICT* per le norme UNI 11697:2017 (Valutatore *Privacy* e *DPO*) e UNI 11506:2017 (*Security Specialist* e *Security Manager*). E' una tra le aziende leader nel fornire soluzioni di *Total Quality Assurance* per le industrie di tutto il mondo, offre soluzioni innovative e su misura di *Assurance* (Servizi per identificare e ridurre i rischi connessi alle vostre attività, *supply chain* e sistemi di gestione), *Testing* (Servizi per dimostrare la conformità dei vostri prodotti/servizi alle norme di qualità, sicurezza, sostenibilità e performance), Ispezioni (Servizi per convalidare le specifiche tecniche, il valore e la sicurezza delle vostre materie prime, prodotti e assets.) e Certificazioni (Servizi per certificare che i vostri prodotti/servizi siano conformi rispetto ai relativi standard, siano essi di mercato o specifici di un'azienda) per le attività e le supply chains dei nostri clienti.

CSQA

COLLABORAZIONE

CSQA Certificazioni (www.csqa.it) fornisce a livello internazionale servizi di certificazione e ispezione accreditati nel settore *ICT* e *Digital Market* per le norme ISO 9001:2015, UNI CEI ISO IEC 27001:2014, UNI EN ISO 20000-1:2018, ISO 22301:2012, UNI EN ISO 19011:2018 . CSQA inoltre è ente di certificazione accreditato:

- per la certificazione dei Conservatori a Norma secondo le disposizioni dell'AgID, e CAB.
- per la certificazione eIDAS (Reg. UE 910/2014) dei Trust Service Providers.
- per la certificazione degli operatori SPID.

Tramite il proprio Centro Formazione, CSQA eroga numerosi percorsi di formazione e di qualifica per Auditor Interni, Lead Auditor, ITIL, COBIT5 ed altri, riconosciuti a livello nazionale e internazionale.

AIEA ISACA Sistemi informativi: averne fiducia e trarne valore Milano Chapter

COLLABORAZIONE

Fondata nel 1969 con oltre 100.000 associati in 180 Paesi, ISACA® (www.isaca.org), di cui AIEA incarna il Capitolo di Milano (www.aiea.it), è *leader* mondiale nello sviluppo di modelli di IT *audit* & *compliance*, IT *governance*, IT *security* e *cyber-security*, IT *risk* & *control*.
Favorisce, inoltre, l'acquisizione delle competenze e delle conoscenze IT e le attesta mediante le certificazioni riconosciute a livello internazionale quali: CISA® (*Certified Information Systems Auditor*™), CISM® (*Certified Information Security Manager*®), CGEIT™ (*Certified in the Governance of Enterprise* ITTM), CRISC™ (*Certified in Risk and Information Systems Control*™) e CSX ™ (*Cybersecurity Certification*). ISACA aggiorna continuamente COBIT® che assiste i professionisti dell'IT e i manager delle imprese ad adempiere le proprie responsabilità relativamente all'IT *governance* e alla gestione manageriale.

ISCRIZIONE

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.
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:

- € 4.146,00 all'immatricolazione, entro il 08/02/2019 (comprensivi dell'importo di € 16,00 della marca da bollo virtuale e del contributo di € 130,00 per il rilascio della pergamena finale);
- € 4,000,00 entro il 05/03/2019.

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

- € 2.146,00 all'immatricolazione, entro il 08/02/2019 (comprensivi dell'importo di € 16,00 della marca da bollo virtuale e del contributo di € 130,00 per il rilascio della pergamena finale);
- € 2.000,00 entro il 05/03/2019.

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 18/01/2019** 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 18/01/2019, all'indirizzo e-mail jessica.chiavari@uniroma2.it, la seguente documentazione:
   - ricevuta del pagamento del contributo di pre-iscrizione di € 30,00 convalidato con il codice AUTH;
   - Curriculum vitae;
   - Ripartizione Master, Corsi di Perfezionamento, Scuole di Specializzazione area non sanitaria
   - 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 24/01/2019 sul sito web http://www.uniroma2.it.

CONTATTI E INFORMAZIONI

Per le **informazioni didattiche** rivolgersi a:

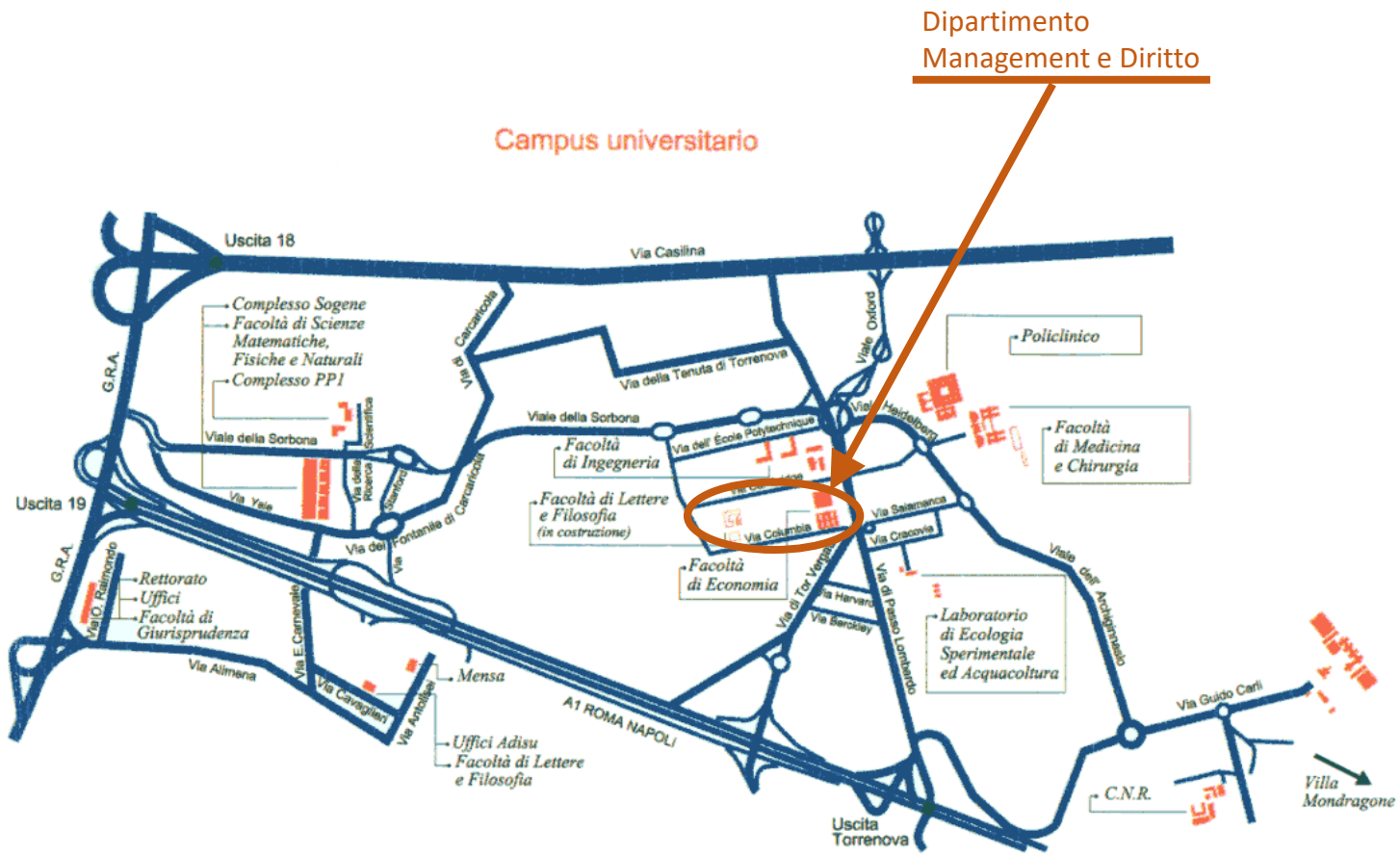
- **segreteria didattica del Master:**
  - tel.: (+39) 339 373 5020
  - e-mail jessica.chiavari@uniroma2.it
  - web: http://www.cybersecurityprivacy.it/master/master-in-cybersecurity-e-privacy.html

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 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

PARTNER PROMOTORI

Università di Roma Tor Vergata

pragmema hyper-interactive net solutions

Profice

Posteitaliane

IGS Istituto per il Governo Societario

GT 50 改善 VISIONARY INNOVATORS

clariter proposals being delivered

SUPERCOM strategie d'impresa

PATROCINIO

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

COLLABORAZIONI

intertek Total Quality. Assured.

CSQA

ISACA Sistemi informativi: averne fiducia e trarne valore

Capitolo di Milano