# Scheda Unica del Corso di alta formazione (SU-AF) in
# DATA PROTECTION, CYBERSECURITY E DIGITAL FORENSICS

## Informazioni Generali

**Nome del Corso:** DATA PROTECTION, CYBERSECURITY E DIGITAL FORENSICS
**Link al regolamento didattico:**
https://www.unipg.it/files/pagine/195/regolamento_data_protection.pdf
**Titolo e/o certificazione rilasciata**: Master di primo livello
**Bando/Avviso:**
https://ginko.unipg.it/ws/concorsi/scaricadocumento.php?iddocumento=27628
**Struttura proponente**: Dipartimento di Giurisprudenza
**Anno accademico**: 2019/2020
**Area disciplinare**: 12
**Livello**: Primo
**Direttore/Coordinatore**: Prof.ssa Stefania Stefanelli
**Durata**: 1 anno
**Modalità di erogazione della didattica**: Frontale
**Lingua**: Italiano
**Costo**: 3.500 Euro
**Scadenza bando/avviso**: 31.10.2019
**Inizio e fine immatricolazione/iscrizione**: v. bando
**Periodo di svolgimento**: Novembre 2019/Aprile 2021
**Sito del Corso**: https://www.unipg.it/didattica/accesso-corsi-numero-programmato/master?layout=concorso&idConcorso=19416
**Eventuali borse**: n. 1 offerta da Studio legale Avv. Giuseppe Serafini

## Caratteristiche

**Obiettivi formativi e finalità**: Il Master di primo livello in «Data protection, cybersecurity e digital forensics», di durata annuale, si articola in 60 crediti formativi e si propone di fornire competenze specifiche nell'ambito della Data protection, cybersecurity e digital forensics, ai laureati di primo livello nell'ambito della protezione dei dati personali, della sicurezza informatica e dell'acquisizione delle prove digitali.
Il master ha ottenuto il patrocinio dell'Autorità Garante per la Protezione dei Dati Personali e della FIIF – Fondazione per l'innovazione forense del Consiglio Nazionale Forense, ed è in corso l'accreditamento presso il CNF per la formazione professionale degli avvocati. Il Master ha l'obiettivo di creare competenze specifiche nel:
a) garantire la protezione, la sicurezza, la conservazione ed il corretto trattamento dei dati personali, assicurando al contempo la riservatezza dei titolari, il rispetto della base giuridica, l'efficienza e la minimizzazione del trattamento rispetto agli scopi che si prefigge;
b) gestire, con adeguate competenze tecnologiche, di informatica giuridica e manageriali, il coordinamento strategico dello sviluppo dei sistemi informativi di telecomunicazione e fonia, per realizzare la transizione della pubblica amministrazione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di una P.A. digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;
c) svolgere attività di indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture;

| | |
|---|---|
| | d) comprendere come affrontare e gestire ogni fase del procedimento probatorio avente ad oggetto fonti di prove digitali, sia sulla scorta della disciplina vigente che delle più recenti interpretazioni giurisprudenziali (digital forensics).<br>Le conoscenze e le capacità teorico-pratiche, che saranno acquisite al termine del corso, prevedono altresì l'approfondimento della modalità per una corretta redazione di registri dei trattamenti, valutazioni di impatto sulla protezione dei dati (DPIA), segnalazioni e comunicazioni di data breach e gestione delle istanze costituenti esercizio dei diritti degli interessati rispetto al trattamento dei propri dati personali, nonché di gestione di ricorsi, reclami e azioni di risarcimento danni per illegittimo trattamento.<br>Le conoscenze e le capacità teorico-pratiche, che saranno acquisite al termine del corso, prevedono l'approfondimento della disciplina di protezione dei dati personali, aggiornata alle fonti di adeguamento al GDPR, alla prassi ed all'interpretazione dottrinale e giudiziaria; del contrasto al cybercrime e dell'acquisizione delle prove informatiche; della system, social and mobile security; del diritto amministrativo, con particolare riguardo al ruolo ed alle funzioni delle autorità di controllo e dei confini tra trasparenza e privacy; del diritto europeo della privacy e della sicurezza informatica.<br>Le conoscenze e le capacità teorico-pratiche, che saranno acquisite al termine del corso, prevedono altresì l'approfondimento della modalità per una corretta redazione di registri dei trattamenti, valutazioni di impatto sulla protezione dei dati (DPIA), segnalazioni e comunicazioni di data breach e gestione delle istanze costituenti esercizio dei diritti degli interessati rispetto al trattamento dei propri dati personali, nonché di gestione di ricorsi reclami e azioni di |

risarcimento danni per illegittimo trattamento.

L'importanza crescente della disciplina di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, alla luce del Regolamento europeo n. 679/2016, e dell'evoluzione normativa in materia, con l'adeguamento al GDPR attraverso il d.lgs. n. 101/2018 ed i provvedimenti delle Autorità nazionali ed europee, dei profili di effettività della tutela, ai confini di applicazione del Regolamento e delle sfide che si aprono in tema di sicurezza informatica, del contrasto al crimine informatico e dell'acquisizione della prova digitale, impone, nella realtà contemporanea, la necessità di disporre di figure professionali con competenze interdisciplinari, correttamente formate e soprattutto aggiornate, capaci di svolgere sempre al meglio la loro professione, sia in ambito pubblico, sia in ambito privato.

Ruolo chiave per la formazione dei discenti svolge la compenetrazione tra insegnamenti giuridici e tecnico-informatici, affidati a docenti universitari e ad esperti di chiara fama, selezionati dal Consiglio dei docenti e dagli enti che partecipano al master.

Infine, la possibilità di svolgere un periodo di stage presso strutture di enti pubblici, professionisti, aziende ed enti non profit, garantisce una formazione completa per un professionista con qualifiche rispondenti alle esigenze delle aziende, dei professionisti, degli enti senza scopo di lucro, ed alle amministrazioni pubbliche.

**Sbocchi (profilo) professionali**:

- assumere l'incarico di DPO
- Data Protection Officer (responsabile della protezione dei dati personali), ai sensi del Regolamento europeo n. 2016/679 in enti pubblici e nel settore privato, di consulente privacy e di altre figure specialistiche privacy anche in

ambito sanitario, giudiziario e di ricerca scientifica;
- assumere l'incarico di RTD (responsabile della transizione digitale), ai sensi della circolare Ministero dell'interno n 3 del 1° ottobre 2018 e dell'art. 17 del Codice dell'Amministrazione digitale, adottato con d.lgs. n. 82/2005, successive modificazioni e integrazioni;
- svolgere le funzioni di consulente professionale con competenze interdisciplinari per attività di commercio elettronico, digitalizzazione, sicurezza informatica e trustworthiness come affidabilità, correttezza, e robustezza delle reti e dei sistemi nelle imprese, nelle pubbliche amministrazioni e per le infrastrutture critiche, attraverso l'organizzazione, la gestione e l'assunzione di responsabilità nei contesti della sicurezza informatica aziendale, intelligenza artificiale e sanità elettronica;
- svolgere le funzioni di consulente tecnico di parte o di perito del giudice, ovvero supervisionare l'attività degli esperti in metodologie per l'acquisizione, il trattamento e la gestione delle fonti di prova informatiche, e adottare le più idonee misure per preservare inalterata la genuinità della fonte di prova informatica sia con riferimento ad ogni fase del procedimento penale avente ad oggetto anche ipotesi di criminalità informatica, sia con riferimento alle controversie civili, commerciali, gius-lavoristiche e fiscali o alle indagini difensive e stragiudiziali.

**Numero partecipanti: minimo 12, massimo 30**

**Crediti formativi**: 60

## Requisiti d'ammissione

**Titoli d'accesso**: diploma di laurea di primo livello o titolo estero equipollente in Scienze dei servizi giuridici (Classe di laurea L 14 ed equiparate), Scienze e Tecnologie Informatiche (Classe L 31), Scienze dell'Economia e della Gestione Aziendale (Classe L 18 ed equiparate), Scienze economiche (Classe L 33), Scienze della comunicazione (Classe L 20 ed equiparate), Ingegneria dell'informazione (Classe L 08 ed equiparate), Scienze della difesa e della sicurezza (Classe L/DC ed

## Didattica

**Sede di svolgimento delle attività**: Dipartimento di Giurisprudenza

**Programmazione didattica degli insegnamenti con elenco dei docenti e n. CFU**: le attività formative sono articolate in moduli, ed i crediti didattici relativi alle

equiparate), Scienze criminologiche e della sicurezza (Classe L/SC), Scienze dell'educazione e della formazione (Classe L 19 ed equiparate), Scienze politiche e delle relazioni internazionali (Classe L 36), nonché ai rispettivi diplomi di laurea di secondo livello. Il collegio dei docenti del master ha facoltà di ammettere all'iscrizione studenti in possesso di ulteriori diplomi di laurea di primo o di secondo livello, sulla base della valutazione del curriculum formativo e delle competenze acquisite e documentate, anche attraverso attività formative extracurricolari di istruzione superiore o professionale, nonché delle funzioni svolte e degli incarichi ricoperti in pubbliche amministrazioni, imprese o in qualità di libero professionista.

**Criteri di selezione**: selezione per titoli e colloquio, operata da una Commissione nominata dal Collegio dei docenti. Al colloquio saranno attribuiti 30 punti, ai titoli fino a 30 punti.
I criteri di attribuzione dei punteggi per i titoli sono i seguenti:
voto di laurea: fino a 102= 2 punti; da 103 a 105=4 punti; da 106 a 109=8 punti; 110=9 punti; 110 e lode=10 punti;
Pubblicazioni in materie attinenti all'oggetto del master: monografie fino a 10 punti in totale; articoli in riviste scientifiche secondo la classificazione ANVUR o capitoli di libro fino a 5 punti in totale.
Esperienza professionale in ambiti attinenti all'oggetto del master: fino a 5 punti.
**Data di selezione**:v. bando

attività formative, nonché quelli riguardanti la prova finale, sono attribuiti con il superamento dell'esame di profitto dei corsi e rispettivamente della prova finale. Comprenderanno gli insegnamenti di Privacy e data protection (IUS/01-IUS/02), Proff. Giovanni Marini e Stefania Stefanelli; Cybercrime e digital forensics (IUS/16-IUS/17), Proff. Mariangela Montagna, Vico Valentini e esperti esterni; System, social and mobile security (INF/01), Proff. Stefano Bistarelli, Francesco Santini e esperti esterni; Diritto amministrativo (IUS/10), Proff. Annalisa Giusti, Antonio Bartolini, Serenella Pieroni, Giorgio Repetto e esperti esterni; Diritto europeo della privacy e della sicurezza informatica (IUS/14), Prof. Simone Vezzani e esperti esterni.
**Frequenza** (% obbligatorietà): 80%
**Tirocinio** (durata e n. CFU): stage presso aziende, enti non profit, enti pubblici e professionisti garantisce una formazione completa per un professionista con qualifiche rispondenti alle esigenze del mercato del lavoro, in particolare presso il Dipartimento di Giurisprudenza, lo Studio legale Serafini, Enti patrocinanti e ulteriori che verranno determinati dal Dipartimento di Giurisprudenza; n. 13,52 CFU.
**Prova finale** (tipologia e n. CFU): redazione e discussione di un progetto o elaborato scientifico; n. 13,48 CFU.

## Contatti

**Nome e Cognome**: Prof. Stefania Stefanelli
**Indirizzo postale**: Via A. Pascoli n. 33, 06123 Perugia
**Telefono**: 0755852420
**Indirizzo mail**: stefania.stefanelli@unipg.it
**Ufficio Amministrativo di riferimento**: Segreteria del Dipartimento di Giurisprudenza
**Tel., ubicazione, orari**: 0755852401, Via A. Pascoli n. 33, 06123 Perugia; lun., merc., ven. ore 8-14; mar., giov. ore 8-14, 15-17.