



CORSO DI PERFEZIONAMENTO E AGGIORNAMENTO PROFESSIONALE

UNICUSANO

LA GESTIONE DELL'INNOVAZIONE DIGITALE NELLA SANITÀ:

**Data protection officer, cybersecurity
and information security specialist**



**UNIVERSITÀ
CUSANO**



L'Università degli Studi Niccolò Cusano attiva il Corso di Perfezionamento e Aggiornamento Professionale in “LA GESTIONE DELL'INNOVAZIONE DIGITALE NELLA SANITÀ: DATA PROTECTION OFFICER, CYBERSECURITY AND INFORMATION SECURITY SPECIALIST” afferente alla Facoltà di Giurisprudenza, di durata pari a 1000 h.

Agli iscritti che avranno superato le eventuali prove di verifica intermedie e la prova finale verrà rilasciato il Diploma di Corso di Perfezionamento e Aggiornamento Professionale in “LA GESTIONE DELL'INNOVAZIONE DIGITALE NELLA SANITÀ: DATA PROTECTION OFFICER, CYBERSECURITY AND INFORMATION SECURITY SPECIALIST”.





Obiettivi

Nel contesto attuale di una forte spinta verso la digitalizzazione anche nel settore della sanità, il Corso in “LA GESTIONE DELL'INNOVAZIONE DIGITALE NELLA SANITÀ: DATA PROTECTION OFFICER, CYBERSECURITY AND INFORMATION SECURITY SPECIALIST” mira a formare nuovi professionisti nell'ambito della sanità pubblica e privata, tra i quali in particolare la figura del Data Protection Officer (RPD/DPO), che svolge anche un ruolo di sensibilizzazione dell'organizzazione e altre figure di consulenza con abilità in ambito cybersecurity. Pertanto, durante il corso verranno illustrati dei casi di studio e dei metodi di lavoro di tali figure, unendo la parte teorica di analisi della normativa agli aspetti pratici della professione. Accanto al RPD/DPO vi è la necessità impellente di formare altre figure di supporto privacy, inclusi i componenti dei gruppi di lavoro privacy e degli uffici dedicati. Gli specialisti privacy, che hanno compiti più o meno operativi all'interno delle Aziende Ospedaliere, Asl, ma anche all'interno di Ospedali e strutture sanitarie private accreditati o meno, hanno la necessità di acquisire conoscenze e competenze specifiche.

Per la figura del Data Protection Officer l'esperienza effettiva nel settore e la conoscenza approfondita della normativa sulla protezione dei dati applicata nel quotidiano, sono dei requisiti normativi necessari per ricoprire tale incarico unitamente all'obbligo di aggiornamento continuo. Analogamente, con l'aumento esponenziale di attacchi informatici, che sta colpendo in particolare il nostro Paese, non meno importanti appaiono la formazione e le nuove competenze delle figure tecniche IT, amministratori di sistema e impiegati informatici che necessitano di aggiornarsi e formarsi nell'ambito della sicurezza informatica e della cybersecurity. Infatti, un modulo rilevante sarà dedicato al ruolo di specialista di cybersecurity, modulo utile, sia per chi abbia una conoscenza base e la necessità di approfondire questo ambito, sia per chi abbia già acquisito una buona conoscenza di sicurezza informatica e di cybersecurity e abbia necessità di aggiornarsi sulle nuove tecniche e metodologie di attacco e difesa. Infine, per l'organizzazione dell'impresa pubblica e soprattutto privata, anche al fine di partecipare a bandi di gara, diventa sempre più



importante dimostrare che i propri processi aziendali e i sistemi di gestione siano conformi agli standard internazionali con l'ottenimento di certificazioni riconosciute sul mercato, sia in base agli standard ISO che in base agli altri standard di settore. A tale tema, anch'esso di estrema rilevanza, è stato dedicato un intero modulo, coinvolgendo docenti con esperienza internazionale e altamente qualificati.



Destinatari e ammissione

Il Corso è rivolto a tutti i diplomati e ai laureati in tutte le discipline del nuovo e vecchio ordinamento (ex art. 6 comma 2 lettera c della legge 341/90).

I candidati in possesso di titolo di studio straniero non preventivamente dichiarato equipollente da parte di una autorità accademica italiana, potranno chiedere al Comitato Scientifico il riconoscimento del titolo ai soli limitati fini dell'iscrizione al Corso. Il titolo di studio straniero dovrà essere corredato da traduzione ufficiale in lingua italiana, legalizzazione e dichiarazione di valore a cura delle Rappresentanze diplomatiche italiane nel Paese in cui il titolo è stato conseguito.

I candidati sono ammessi con riserva previo accertamento dei requisiti previsti dal bando.

I titoli di ammissione devono essere posseduti alla data di scadenza del termine utile per la presentazione per le domande di ammissione.



Durata, organizzazione didattica, verifiche e prova finale

Il Corso ha durata annuale pari a 1000 ore di impegno complessivo per il corsista, corrispondenti a 40 cfu e sarà articolato in:

- lezioni video e materiale fad appositamente predisposto;
- congruo numero di ore destinate all'auto-apprendimento, allo studio individuale e domestico;
- eventuali verifiche intermedie;

Tutti coloro che risulteranno regolarmente iscritti al Corso dovranno sostenere un esame finale che accerti il conseguimento degli obiettivi proposti, presso la sede dell'Università sita in Roma - Via Don Carlo Gnocchi 3.



Ordinamento didattico

Il percorso del Corso prevede i seguenti insegnamenti così articolati:

8 CFU
ING-INF/05

LA GESTIONE DELL'INNOVAZIONE DIGITALE IN SANITÀ'

- La gestione dell'innovazione digitale nella sanità privata e nell'ospedalità privata anche connessa al PNRR
- Il Fascicolo Sanitario Elettronico e il Dossier Sanitario Elettronico
- La telemedicina e il teleconsulto, progetti innovativi in sanità
- Il contesto organizzativo generale nella sanità pubblica e la gestione dell'innovazione digitale
- Il Sistema sanitario nazionale: analisi dell'organizzazione pubblica e del sistema di accreditamento

6 CFU
IUS/01
IUS/14
IUS/10

GDPR IN AMBITO SANITARIO – ANALISI DELLE FONTI E ADEMPIMENTI

- Le carte internazionali e le convezioni internazionali europee (il processo di modernizzazione della convezione n. 108 e il protocollo emendativo)
- La riforma del quadro normativo europeo: la Direttiva 95/46 CE, il regolamento europeo 2016/679 (c.d. GDPR), le direttive 2016/680 e 2016/681
- I soggetti coinvolti nelle operazioni di trattamento nella sanità pubblica e nella sanità privata: interessato, titolare, responsabile, incaricato al trattamento (gli autorizzati e i designati al trattamento), co-titolari rappresentante stabilito
- Il ruolo del responsabile della protezione dei dati nella sanità: presupposti, contesto organizzativo, il codice etico e il conflitto di interessi del RPD
- Il ruolo del responsabile della protezione dei dati nella sanità: compiti e responsabilità
- Analisi della casistica nelle pronunce europee in ordine al Responsabile della protezione dei dati
- Analisi nelle pronunce del Garante italiano in ordine al ruolo del Responsabile della protezione dei dati
- Analisi dei compiti del RPD e casi di studio
- La violazione dei dati (data breach) in ambito sanitario e le procedure di gestione delle violazioni
- Caso di studio per la redazione della notificazione del Garante per la protezione

dei dati

- Caso di studio per la redazione del Registro delle notificazioni interne
 - Analisi delle casistiche di data in sanità e delle sanzioni della autorità di controllo
 - Analisi di casi di studio e simulazioni di data breach notification: chi deve essere coinvolto e fasi di gestione del data breach
 - Ruolo del RPD e gruppo di lavoro privacy nella gestione dei data breach per una corretta minimizzazione dei rischi del titolare del trattamento
 - Analisi del gruppo di supporto privacy rispetto al RPD: conoscenza della normativa, competenze operative
 - Analisi del gruppo di supporto privacy rispetto al RPD: casi di studio
 - Videosorveglianza: aspetti critici
 - Sanzioni e ispezioni: analisi di aspetti particolari
 - Il Registro delle attività di trattamento dei dati: criticità e casi pratici
 - Il Registro delle attività di trattamento nella sanità
-

6 CFU

IUS/01

IUS/14

IUS/10

GDPR IN AMBITO SANITARIO – DISCIPLINA SETTORIALE

- Gestione del rapporto di lavoro nella sanità pubblica e privata: adempimenti sulla trasparenza della protezione dei dati e controllo a distanza dei lavoratori anche in relazione alle nuove soluzioni tecnologiche e all'innovazione digitale
 - La videosorveglianza nell'ambito sanitario: analisi degli aspetti legali e di GDPR
 - Il GDPR nella Sanità pubblica: analisi del quadro normativo complessivo, la gestione del registro delle attività e degli adempimenti Gdpr nella sanità pubblica
 - Trasferimenti dei dati all'estero: analisi del contesto normativo generale
 - Analisi delle decisioni di adeguatezza normativa
 - Analisi delle garanzie per il trasferimento dei dati all'estero
 - Analisi delle clausole contrattuali tipo
 - Analisi della pronuncia Schrems II e della conseguenza sugli accordi internazionali
-



9 CFU
ING- INF/05
IUS/10

CYBERSECURITY IN AMBITO SANITARIO

- Definire l'ambito connesso all'innovazione digitale in sanità
- Casi di studio e simulazioni
- Unione Europea: normativa generale ed interventi nell'area UE: la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 (c.d. Direttiva NIS), Reg. UE 2016/679, Direttiva UE 2016/680 e Direttiva UE 2016/681
- Analisi dei criteri, principi e adempimenti previsti dalle normative europee sopra richiamate
- Il diritto italiano: analisi delle normative di recepimento nazionale, analisi di disposizioni rilevanti del codice penale, di procedura penale e della normativa speciale di settore.
- Perimetro Sicurezza Il decreto-legge 21 settembre 2019, n. 105,
- Analisi delle normative di attuazione del perimetro di cybersecurity nazionale
- La Agenzia di Cybersecurity Nazionale (ACN): analisi del ruolo nel quadro normativo e confronto con il ruolo del DIS
- Il ruolo di ACN nella gestione del CSIRT Italia e i CERT: l'importanza dell'interoperabilità tra Stato Regioni e aziende nella gestione degli alert di sicurezza
- Il Comitato di Valutazione e Certificazione Nazionale: sistema di verifica, i laboratori di test per i beni e servizi ICT, il nuovo sistema di accreditamento
- L'uso delle tecnologie IoT nel settore sanitario
- Aspetti di cybersecurity riferiti ai sistemi IoT ed ICT e la gestione del rischio in ambito sanitario
- L'intelligenza Artificiale e le prospettive future in ambito sanitario
- La proposta di regolamento sull'Intelligenza Artificiale, gestione della tecnologia e dei dati sanitari
- Analisi dei casi di incidente informatico in ambito sanitario: differenze tra notificazione in base alla NIS e in base al GDPR
- Cybersecurity in ambito sanitario pubblico e privato: laboratori, strategie e tattiche relative agli incident handling



8 CFU
ING-INF/05
IUS/01

SISTEMI DI GESTIONE E LE CERTIFICAZIONI: INFORMATION SECURITY E IL MODELLO DI GESTIONE E CONTROLLO

- Introduzione ai concetti di certificazione e accreditamento
 - Famiglia ISO 27000, terminologia
 - Introduzione ai sistemi di gestione (PDCA, HLS)
 - Il sistema di gestione per la sicurezza delle informazioni
 - La ISO/IEC 27001 (vecchia e nuova versione)
 - I controlli (vecchi e nuovi)
 - Le estensioni della ISO/IEC 27001 e la ISO/IEC 27999
 - Il processo di certificazione del SGSI
 - Auditor e audit interni
 - Certificazione delle competenze
 - Modelli di gestione e controllo 231 in ambito sanitario
 - Sistemi di certificazione e di gestione per le apparecchiature elettromedicali
-

3 CFU Tesi finale

Nell'insieme l'attività formativa prevede 40 CFU crediti complessivi.



Consiglio didattico e scientifico

COORDINAZIONE SCIENTIFICA

Avv. Di Resta

CORPO DOCENTE

Dott. Mauro Alovisio, avvocato. È il coordinatore del corso di perfezionamento in materia di GDPR dell'Università degli Studi di Torino, professore a contratto presso Università Statale di Milano, già componente del Comitato Etico interaziendale Città della Salute e della Scienza, Ospedale Mauriziano e Asl Città di Torino, autore di pubblicazioni e articoli in materia di informatica giuridica, GDPR e videosorveglianza e formatore

Dott. Fabio Miraglia, imprenditore e docente di economia e innovazione sanitaria presso Università La Sapienza di Roma. Fondatore e Presidente di C.H.I.CO Cluster of Health Innovation and Community, Cluster della Salute della Regione Lazio, Roma. Fondatore e CEO di LifeSeeder spa. Presidente GIOMI RSA (Italia), Giomi Deutschland (Germania) e Tong Ren Tang Giomi Srl (Cina). Past President Consorzio Tecnopolo di Castel Romano, Past President Unindustria Latina e Vice Presidente di Unindustria – Unione degli industriali e delle imprese Roma Frosinone Latina Rieti Viterbo fino al settembre 2016, Past President della Commissione E-Health UEPH (European Association private hospital).

Avv. Riccardo Abeti, laureato in giurisprudenza nel 1999 e avvocato dal 2002, si occupa di diritto dell'informatica. Sin dagli esordi ha coniugato le conoscenze giuridiche con le nozioni gestionali/organizzative, offrendo un nuovo tipo di approccio alle materie della protezione dei dati, della cybersecurity e della responsabilità amministrativa delle società (c.d. 231). Nel corso dell'esperienza ultraventennale ha affrontato e condotto a compimento centinaia di progetti. L'esperienza maturata spazia su ambiti differenti ma dal 2006 ha assunto una peculiarità nell'applicazione della normativa in materia di protezione dei dati nell'ambito sanitario. Docente da circa un decennio per università pubbliche e private ma anche per enti di formazione. Dal 2008 è Presidente della Commissione "New Technology, Personal Data and Communication



Law” dell’Unione Avvocati Europei, con la quale ha organizzato importanti eventi di respiro nazionale e internazionale. È attualmente Responsabile della Protezione dei Dati (aka Data Protection Officer) di importanti realtà in ambito e-health, system integration e petrolifero nonché consulente per alcune multinazionali.

Dott. Fabrizio Cirilli, dal 1983 svolge attività di consulenza, audit, assessment e formazione nelle tematiche di: IT service management, information security, risk management, incident handling, business continuity, disaster recovery, security supply chain, IT/OT cybersecurity, security awareness. È certificato come lead auditor professionista in registri nazionali ed internazionali. Opera con organismi di certificazione a livello nazionale ed internazionale in qualità di lead auditor nel settore ICT sin dal 1995. È progettista e docente dei corsi registrati di qualifica per erogati anche per università pubbliche e private. Dal 2004 è membro del Comitato ISO e UNINFO per gli standard della sicurezza delle informazioni.

Dott.ssa Pinuccia Carena, laureata in matematica nel 1989, è analista dirigente in sanità dal 1992. Si è occupata, sia nella propria Azienda sia in diverse consulenze, oltre che di informatica, anche di Controllo di Gestione (per cui è stata Responsabile della Struttura Complessa Aziendale) e di Valutazione dei Dirigenti (è componente di Organismi Indipendenti di Valutazione ed è iscritta all’albo nazionale). Negli ultimi anni è stata anche Data Protection Officer in diverse Aziende sanitarie. Da circa 20 anni è docente a contratto sia dell’Università di Torino sia dell’Università del Piemonte Orientale in corsi di informatica, sistemi informativi e management sanitario; sulle medesime materie ha anche svolto docenza in diversi corsi professionali e Master di specializzazione. È attualmente Responsabile della Struttura Complessa Innovazione e Sicurezza Informatica e Ciclo della Performance in ASLCN1.

Avv. Antonio Mauro, avvocato, lavora presso Università, è il coordinatore del corso di perfezionamento in materia di GDPR dell’Università degli Studi di Torino, professore a contratto presso l’Università Statale di Milano, già componente del Comitato Etico interaziendale Città della Salute e della Scienza, Ospedale Mauriziano e Asl Città di Torino, autore di pubblicazioni e articoli in materia di informatica giuridica, GDPR e videosorveglianza e formatore.

Dott. Gianluca Savino, avvocato, in servizio come Funzionario, Area Direttiva, presso il



Garante per la protezione dei dati personali. Cultore della materia nell'insegnamento di Cybersecurity e protezione dei dati personali presso la facoltà di Giurisprudenza dell'Università degli studi di Roma Niccolò Cusano. Docente di Master universitari presso il dipartimento di Giurisprudenza dell'Università Niccolò Cusano di Roma. Autore di pubblicazioni scientifiche in materia di protezione dati e relatore in corsi di formazione e seminari di approfondimento sui temi del diritto della privacy, diritto civile, commerciale e del lavoro, per importanti enti pubblici e privati. Componente consiglio direttivo di importanti associazioni professionali.

Dott. Maurizio Pastore, ingegnere elettronico ed esperto di sicurezza informatica e privacy, possiede una consolidata esperienza in materia di protezione dei dati personali per conto di Organismi Sanitari pubblici (Aziende Sanitarie / Ospedaliere), Pubbliche Amministrazioni Locali (Regioni, Province, Città Metropolitane, Unione di Comuni, Comuni), Enti del terzo settore, Aziende. È il coordinatore del Centro di Competenza sul GDPR di Liguria Digitale e in tale veste segue tutte le attività Privacy per i clienti e per Liguria Digitale stessa.

Segue attualmente per conto di Alisa (coordinatrice delle ASL/AO Liguri) le problematiche NIS e Privacy seguendo anche attività di Titolarità di 5 ASL, IRCCS S.Martino, IRCCS Gaslini, AO Galliera, Ospedale Evangelico Internazionale. Ha coordinato le attività di valutazione del rischio cyber dei sistemi esterni per l'Ospedale Evangelico Internazionale; ASL 3 Genovese; ARPAL, AOU S.Martino di Genova. Dal 2016 ha seguito l'adeguamento al GDPR di Liguria Digitale, Regione Liguria, Filse e sue partecipate, Azienda In Liguria, le 4 ARTE della Liguria, la Città metropolitana di Genova, di alcune partecipate del comune di Genova (Genova Parcheggi, Fulgis). Dal 2017 Product Manager Applicazione Privacy Web e servizi GDPR.

Avv. Silvano Sacchi, dopo il conseguimento del titolo di avvocato, ottiene la laurea in Economia e Commercio presso l'università di Bergamo ed in seguito il diploma di master universitario di secondo livello in ambito privacy presso l'Università Niccolò Cusano di Roma. Svolge attività di consulenza alle imprese in ambito di compliance, attuazione di modelli ex D. Lgs. 231/01, data protection e privacy. Collabora, a decorrere dal 2018, con lo studio Di Resta Lawyers e ricopre attualmente la posizione di Responsabile della protezione dei dati personali (Data Protection Officer) in entità impegnate nella gestione di software per la gestione aziendale. È docente universitario a contratto nei Corso di Perfezionamento e Aggiornamento Professionale in "I nuovi



professionisti privacy; il responsabile della protezione dei dati personali e i privacy specialist” e “Specialista in cybersecurity, digital forensics e data protection” presso l’Università Niccolò Cusano di Roma dal 2022. È autore di diverse pubblicazioni in ambito privacy e data protection e, dal 2022, cultore della materia in cybersecurity e protezione dei dati presso la facoltà di giurisprudenza dell’Università Niccolò Cusano di Roma.

Avv. Giovanni Grassucci, Avvocato, laureatosi nel 2008 presso la “LUISS Guido Carli - Libera Università degli Studi Sociali di Roma”, discutendo una tesi specialistica sulla Tutela Penale del Domicilio Informatico, si specializza nel 2010 nella Professione Legale presso la Scuola di Specializzazione de “La Sapienza di Roma”. Dal 2018 collabora con lo Studio Di Resta Lawyers nella tutela anche giudiziale in ambito protezione dei dati nei diversi settori, redazione e gestione dei Modelli 231.

Dott.ssa Alessandra Gaetano, consulente e formatore aziendale in ambito di sistemi di gestione per la protezione dei dati personali. Da oltre 20 anni, ha maturato esperienza professionale in società di servizi, che offrono consulenza e formazione nel settore della privacy, della sicurezza nei luoghi di lavoro, dei sistemi di gestione retti da normative volontarie. In tali realtà ha ricoperto altresì la carica di amministratore unico, responsabile del personale e di progetto, con funzione di coordinamento risorse umane e monitoraggio qualità, per le commesse sviluppate a favore di enti pubblici articolati. Ricopre l’incarico di RPD/DPO in diversi contesti organizzativi, distribuiti su tutto il territorio nazionale, con particolare riguardo al settore sanitario, presso aziende pubbliche complesse (quali ASL, aziende ospedaliere, aziende ospedaliere universitarie) e il settore degli Enti locali, con riferimento ai comuni. È stato componente del Tavolo di Coordinamento dei DPO/RPD della Sanità Piemontese. E’, inoltre, componente del Tavolo di Supporto Regionale Piemontese per le attività di organizzazione per la ricerca sanitaria e biomedica nelle ASR Programma di miglioramento e coordinamento regionale per la gestione amministrativa delle sperimentazioni cliniche e attività di ricerca. È in possesso della certificazione in base alla norma UNI 11697:2017 per il profilo professionale di responsabile della protezione dati. È autrice del “Caso studio in ambito sanitario: organizzazione complessa relativa ad Azienda Sanitaria Locale” per il Manuale “Privacy, Data Protection e Cybersecurity” - autore Fabio Di Resta, con prefazione di Franco Pizzetti, già Presidente del Garante per la Protezione dei Dati Personali, ottobre 2021, DUEPUNTOZERO editore.



Dott.ssa Chiara Bellosono, responsabile della protezione dei dati e consulente legale per imprese e Pubbliche Amministrazioni, con rilevante esperienza in ambito di Sviluppo software, Sanità, Telecomunicazioni.

Docente a contratto in diritto alla protezione dei dati personali e cybersecurity per aziende e Università. Coordinatrice del Comitato scientifico del Centro Studi di



Costi e agevolazioni

Il costo annuo del Corso è di **€ 1.800,00** (milleottocento/00), oltre marca da bollo da 16 euro.

Il pagamento verrà corrisposto in quattro rate mensili e consecutive di pari importo di cui la prima all'atto dell'iscrizione, ciascuna pari ad **€ 450,00** (quattrocentocinquanta/00).

È prevista una quota d'iscrizione ridotta, pari a **€ 1600,00** (milleseicento/00) per le seguenti categorie:

- Iscritti ai Corsi di laurea Unicusano
- Laureati Unicusano
- Avvocati iscritti all'Ordine
- Dipendenti della Pubblica Amministrazione
- Ingegneri iscritti all'Ordine

Contatti

Ufficio consulenza orientamento didattico Master e Corsi di Perfezionamento (pre-iscrizione):

Telefono: 06 45678363

dal Lunedì al Venerdì dalle 9:00 alle 18:00

Mail: infomaster@unicusano.it

Ufficio Assistenza Didattica (post-iscrizione):

Telefono: 06 89320000

dal Lunedì al Venerdì dalle 9:00 alle 22:00

Mail: master@unicusano.it

unicusano.it/master-universitari-online



**UNIVERSITÀ
CUSANO**