



CORSO DI PERFEZIONAMENTO E AGGIORNAMENTO PROFESSIONALE IN MATERIA DI PRIVACY E SICUREZZA INFORMATICA NEL SETTORE SANITARIO

COMITATO SCIENTIFICO

Prof. Avv. Alessandro Benedetti (coordinatore)
Prof. Avv. Valeria Falce
Prof. Avv. Giusella Finocchiaro
Prof. Avv. Alberto Gambino
Prof. Avv. Salvatore Sica
Prof. Avv. Andrea Stazi

COORDINATORE DIDATTICO

Avv. Davide Mula

DURATA

3 mesi (60 ore complessive)
1° ed.: 2 marzo 2018 – 25 maggio 2018

FREQUENZA

1 venerdì a settimana, dalle ore 9:00 alle ore 14:00 (5 ore giornaliere)

SEDE SVOLGIMENTO LEZIONI

I.N.M.I. "Lazzaro Spallanzani", Via Portuense n. 292, 00149 Roma

PERSONALE DOCENTE

Professori e collaboratori dell'Università Europea di Roma

DESTINATARI

Personale I.N.M.I. ed eventuale personale sanitario di altre ASL/AO

ATTESTAZIONE FINALE

Per coloro che avranno frequentato l'intero corso, verrà rilasciato un attestato di frequenza del corso di perfezionamento e aggiornamento professionale in materia di *privacy* e sicurezza informatica nel settore sanitario.



DESCRIZIONE DEL CORSO

Il corso di perfezionamento e aggiornamento professionale in materia di privacy e sicurezza informatica nel settore sanitario ha una durata trimestrale ed si propone di fornire una piena conoscenza dal punto di vista sostanziale e procedurale delle informazioni e dei contenuti proteggibili, delle procedure informatiche e giuridiche conformi alle normative nazionali e, in prospettiva, al nuovo Regolamento europeo n. 679/2016 in materia di privacy, nonché di evidenziare le *best practises* internazionali in materia di sicurezza informatica nella gestione di strutture sanitarie pubbliche e private.

L'*iter* formativo prevede l'acquisizione di competenze trasversali sanitarie, giuridiche ed informatiche, alla luce delle esigenze dei maggiori operatori del settore che necessitano di figure specializzate sulle tematiche indicate, in grado di poter affrontare le criticità e pianificare le attività in una prospettiva multidisciplinare.

FINALITÀ FORMATIVE

Il Corso si rivolge a coloro i quali già operano all'interno delle strutture del Sistema Sanitario Regionale e necessitano di una formazione avanzata in materia di privacy e sicurezza informatica nel settore sanitario.

È indirizzato a persone che intendono accrescere la loro professionalità riguardo le problematiche relative alla sicurezza informatica dei sistemi informativi e delle reti informatiche, dal punto di vista manageriale, organizzativo, normativo e tecnologico

STRATEGIA DELL'APPRENDIMENTO E DELL'INSEGNAMENTO

La strategia di apprendimento e di insegnamento si fonda sulla ricerca attuale oltre che sui requisiti della pratica professionale e riflette i risultati educativi del programma.

Il metodo applicato è legato ai requisiti specifici di valutazione. I discenti, quindi, saranno esposti a un programma accademico e professionale interdisciplinare guidato da leader accademici e professionisti internazionali in un ambiente di apprendimento che ingloba una varietà di metodi di insegnamento e di apprendimento.

Accanto alla disseminazione delle informazioni e promozione dell'apprendimento tramite lezioni, i discenti saranno coinvolti in dibattiti e discussioni anche attraverso la previsione di seminari e workshop. I casi di studio saranno analizzati da accademici e sintetizzati al fine di illustrare ai discenti eventuali ripercussioni sulla gestione delle strutture sanitarie.



CARATTERISTICHE DEL CORSO

Il corso soddisfa il forte fabbisogno di accrescimento formativo che proviene da aree professionali emergenti legate al concetto trasversale della sicurezza informatica: di chi risponde della sicurezza dei propri sistemi informativi nei confronti dei propri clienti, di chi ha la necessità di impostare o rafforzare gli schemi e le politiche di sicurezza.

In estrema sintesi, l'obiettivo del corso di perfezionamento e aggiornamento professionale in materia di privacy e sicurezza informatica nel settore sanitario è quello di **formare figure professionali nell'area della sicurezza informatica in grado di gestire la sicurezza del patrimonio informativo e di fronteggiare le eventuali minacce causate da una cattiva implementazione delle tecnologie informatiche.**

Il corso fornisce ai discenti la capacità di gestire:

- l'impatto delle nuove tecnologie e dei media digitali sul settore dell'*healthcare*;
- le problematiche relative alla tutela on line e alla sicurezza informatica;
- i profili della normativa nazionale ed europea per la protezione dei dati personali e delle informazioni commerciali sensibili nel sistema sanitario (incluse le prescrizioni del Codice in materia di protezione dei dati personali, la figura dell'Autorità Garante e il Gruppo dei Garanti europei; recenti innovazioni apportate dal Regolamento europeo);
- i profili inerenti la tutela dei diritti nell'ambito delle sperimentazioni cliniche, il trattamento e la tutela dei dati genetici;
- il trattamento dei dati con strumenti informatici e gli strumenti di refertazione online (cartelle cliniche elettroniche, Dossier sanitario elettronico e Fascicolo sanitario elettronico) e sistemi di dematerializzazione documentale che permettono di gestire i dati dei pazienti con facilità e sicurezza e di scambiarli agevolmente tra le diverse figure professionali interessate (medici di medicina generale, specialisti, care-team, farmacie);
- servizi di telemedicina (Mobile Health; IoT e device per l'homecare; App e dispositivi mobili) che permettono ai pazienti di confrontarsi con il personale sanitario e parasanitario, evitando di doversi recare nelle strutture sanitarie e senza costringere i medici ad effettuare visite a domicilio;
- le infrastrutture informatiche aziendali e gli strumenti di comprensione dei principali sviluppi nel settore dell'ICT Security, nonché gli strumenti per esaminare il rapporto tra la costante evoluzione tecnologica e la vulnerabilità dei sistemi, l'integrazione delle fonti informative e l'interoperabilità dei processi fra piattaforme differenti.



PROGRAMMA DEL CORSO

Il Corso si compone di 12 lezioni da 5 ore ciascuna ed è articolato in due parti: la prima dedicata allo studio della disciplina recata dal Regolamento Generale sulla Protezione dei Dati Personali e la seconda dedicata allo studio della sicurezza delle reti e degli strumenti impiegati nel trattamento dei dati personali.

GIORNO	OGGETTO	ORE
Parte I - Il Regolamento Generale sulla Protezione dei Dati personali (45 ore)		
02.03	Evoluzione normativa in materia di trattamento di dati personali	2
	Ambito di applicazione del Regolamento e ruolo del Garante	3
09.03	I principi generali del Regolamento	2
	Le tipologie di dati personali	3
16.03	Le finalità del trattamento dei dati nelle strutture sanitarie	5
23.03	L'Informativa sul trattamento dei dati	3
	Il consenso al trattamento dei dati	2
06.04	Accountability e privacy by design nelle organizzazioni sanitarie	5
13.04	Le figure del trattamento	3
	Il Data Protection Officer	2
20.04	I diritti dell'interessato: la portabilità dei dati sanitari e il F.S.E.	3
	Il registro del trattamento dei dati sanitari	2
27.04	I rapporti con i fornitori di servizi esterni	2
	I trasferimenti di dati all'estero	3
04.05	Risvolti penali del trattamento dei dati personali	5
Parte II - Sicurezza informatica e disciplina in materia dei dati personali nell'ambito sanitario (15 ore)		
11.05	Introduzione alla sicurezza delle reti e dei sistemi	2
	Organizzazione e gestione della sicurezza informatica	3
18.05	Rilevazione e classificazione dei livelli di criticità dei sistemi informatici	3
	Valutazione e gestione del rischio	2
25.05	Tecniche di crittografia dei dati	3
	Business continuity e crisis management	2

Tutor d'aula: Veronica Gallo