UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Master di II livello

Privacy e protezione dei dati della Pubblica Amministrazione

http://masterprivacy.inginf.units.it

Anno Accademico 2013/14

Presentazione

Il Master in "Gestione della Privacy e della Sicurezza Informatica nella Pubblica Amministrazione" prende spunto dall'esperienza che la Scuola di Studi superiori in Ingegneria Clinica dell'Università di Trieste ha maturato nell'ultimo ventennio, anche grazie alla collaborazione con l'Azienda Ospedaliero - Universitaria "Ospedali Riuniti" di Trieste, inserita in una delle più grandi reti sanitarie pubbliche d'Europa e riconosciuta all'avanguardia a livello nazionale nella gestione delle problematiche relative alla Privacy e alla sicurezza dei sati sanitari in rete, attraverso un lungo percorso di ricerca, progettazione e sperimentazione di soluzioni organizzative e tecnologiche, che hanno dato vita anche ad un laboratorio di ricerca nel settore applicativo della Privacy e Sicurezza Informatica (del. AOUTS 96 d.d. 2/03/2010). Si è deciso pertanto di mettere a disposizione questo bagaglio di conoscenze organizzando il Master in un percorso di Alta formazione multidisciplinare, comprendente sia gli aspetti giuridici, affrontati in collaborazione con la Facoltà di Giurisprudenza, che quelli informatici, tecnico-normativi e gestionali, propri della Facoltà di ingegneria ma anche quelli sociologici e criminologici. Anche questa seconda edizione del Master, che nella sua prima edizione ha riscosso un notevole successo, è rivolto a figure professionali provenienti da diversi percorsi formativi le quali, per interesse personale o per necessità professionali, si trovano a gestire o a dover progettare la sicurezza dell'informazione, in particolare all'interno della Pubblica Amministrazione. La maggior parte di coloro che hanno conseguito il Master nella precedente edizione sta già mettendo a frutto con soddisfazione le competenze acquisite e questo costituisce il miglior indicatore del successo dell'iniziativa.

Chi sarà il "Data Protection Officer"

Il Data Protection Officer (DPO) è una nuovissima figura professionale, la cui presenza sarà resa obbligatoria nelle Pubbliche Amministrazioni e nelle imprese con più di 250 dipendenti dal nuovo Regolamento Europeo sulla data protection (COM 2012-11), in fase di ratifica dopo più di due anni di intenso dibattito, la cui entrata in vigore in tutti gli Stati membri è prevista verso la metà del 2014. In alcune PA più virtuose della realtà italiana era stata già da tempo introdotta la figura del "Privacy e Security Manager"; è questa la funzione che con la nuova normativa Europea sta per divenire obbligatoria. Il DPO rappresenterà il riferimento organizzativo per la Privacy all'interno dell'Ente. In tale veste dovrà curare i rapporti con l'Autorità Garante, coordinare tutte le attività di trattamento dei dati personali e sensibili svolte dalle diverse strutture aziendali e dai punti operativi, sorvegliare il rispetto della normativa di legge, supportare e riscontrare, in particolare per quanto riguarda gli aspetti organizzativi, tutte le funzioni interessate nell'attività di presidio dell'applicazione della legge. Curerà gli adempimenti di carattere generale, coinvolgendo all'occorrenza le diverse strutture aziendali e sarà chiamato a fornire, su richiesta, consulenza interna. Il Data Protection Officer dovrà interagire, ove necessario, con il Titolare ed i Responsabili

del trattamento e formulare proposte nella specifica materia; per quanto concerne i trattamenti di dati informatizzati, collaborerà alla definizione e coordinerà l'applicazione, in accordo con gli Amministratori di Sistema e con la Direzione aziendale, delle regole e dei permessi di accesso ai dati informatizzati ed alla definizione degli strumenti tecnici necessari; predisporrà i regolamenti per la gestione dei profili di accesso ai dati informatici sensibili e per il corretto e legale utilizzo delle risorse informative in senso generale e delle tecnologie della comunicazione in particolare. Sarà chiamato a predisporre i Regolamenti ed i protocolli operativi per le attività che comportano i trattamenti di dati personali e un piano periodico per verificare l'applicazione e l'efficacia delle regole di sicurezza informatica; sarà incaricato di verificare l'efficacia delle misure tecniche di sicurezza adottate per la protezione dei dati informatizzati, gli verrà richiesto di formulare proposte per il piano di formazione in materia per i Responsabili e per gli Incaricati dei trattamenti al fine di renderli edotti dei rischi individuati e delle misure atte alla prevenzione dei danni.

Finalità del Master

Lo scopo del Master è quello di formare figure professionali con le necessarie competenze sulla tutela della Privacy e dei dati sensibili, per la progettazione, organizzazione, gestione e coordinamento della sicurezza dell'informazione nella Pubblica Amministrazione e nella Sanità.

Il Master si rivolge ai laureati in discipline tecnico-scientifiche, a coloro che sono già inseriti nel mondo del lavoro, in particolare nell'ambito della pubblica amministrazione centrale e locale e che si trovano nella necessità di acquisire strumenti di conoscenza sulle tematiche della sicurezza dell'ICT in generale, sia sotto l'aspetto della tutela della Privacy che della sicurezza. E' prevista la sponsorizzazione da parte di importanti fornitori di strumenti e servizi. E' prevista la possibilità di svolgere stage presso strutture pubbliche e private convenzionate.

Requisiti di ammissione

Al Master si accede con diploma di laurea quinquennale in Informatica (23/S), Scienze dell'Informazione e della Comunicazione (67/S), Ingegneria (25-38/S), Fisica (20/S), Matematica (45/S), Giurisprudenza (22/S), Scienze Politiche (70/S), Sociologia (89/S) o altri titoli riconosciuti ad essi equipollenti (normativa antecedente il DM 509/99) o Specialistica (secondo il DM 509/99), o Magistrale (secondo il DM 270/04) a carattere ingegneristico, informatico, fisico, matematico, statistico, giuridico, sociologico o altro titolo ritenuto equivalente dal Consiglio del Master, e sarà organizzato secondo quanto previsto dalla delibera CDA dell'8 marzo 2011. Sono ammessi inoltre gli studenti in possesso di diploma di laurea quadriennale secondo il vecchio ordinamento. Ai fini dell'ammissione al Master universitario, la valutazione dei titoli conseguiti all'estero, sia in paesi della CEE che extracomunitari e della loro equivalenza ai soli fini dell'iscrizione al master è decisa dal Consiglio di Master.

Organizzazione generale

Il primo semestre ha lo scopo di fornire le conoscenze di base e gli strumenti necessari nei due ambiti di studio che costituiscono il percorso del Master: quello legale – normativo, che comprende anche gli aspetti gestionali, sociologici e criminologici e quello più strettamente tecnologico e informatico. Il secondo semestre è incentrato sugli aspetti progettuali e gestionali; approfondisce le conoscenze acquisite nel primo semestre e fornisce un bagaglio pratico basato su case study reali relativi alle situazioni più complesse e d'avanguardia a livello nazionale. In particolare è teso a fornire gli strumenti metodologici necessari ad affrontare la progettazione e la gestione della sicurezza all'interno di una grande organizzazione pubblica e comprende anche nozioni di criminalistica informatica, computer forensic e anti forensic.

Alla fine di ogni corso sono previsti vari seminari ai quali vengono invitati docenti e figure professionali di eccellenza a livello nazionale, sia in ambito istituzionale che nel settore privato, che illustreranno nel dettaglio la loro esperienza in materia di tutela dei dati e della sicurezza informatica dei cittadini. Non mancheranno Autorità ed esponenti di altissimo livello delle Forse dell'Ordine e della Magistratura.

Iscritti

Il numero massimo degli ammessi al corso di Master è fissato a 50, il numero minimo a 10. La modalità di selezione dei partecipanti prevede le seguenti due fasi consecutive: a) valutazione positiva dell'idoneità all'ammissione al master fino al raggiungimento delle prime 30 idoneità b) valutazione congiunta dell'idoneità all'ammissione al master e di una graduatoria per titoli stabilita in base ad un punteggio espresso in centesimi per le eventuali idoneità eccedenti le prime 30. Tutti i candidati saranno sottoposti, sulla base dei titoli posseduti, all'esame della loro idoneità all'iscrizione al master PSIS. I primi 40 candidati valutati positivamente per loro idoneità all'iscrizione saranno selezionati per l'iscrizione al Master, indipendentemente dall'entità dei titoli posseduti. Per l'eventuale attribuzione dei posti dal 41 al 50 la commissione valuterà i titoli posseduti dai candidati valutati positivamente per loro idoneità all'iscrizione al Master secondo i seguenti criteri: la tesi di Laurea (fino ad un max di 20 punti) il voto di Laurea (fino ad un max di 25 punti) il voto riportato negli esami di profitto dei Corsi di Laurea in discipline attinenti al Master (di ingegneria clinica, biomedica, elettronica, informatica, gestionale e industriale, di cultura generale in biologia, medicina, impiantistica e gestione del rischio, giurisprudenza, economia, scienze politiche, sociologia) (fino ad un max di 25 punti) pubblicazioni scientifiche ed eventuali altre tesi, in materia attinente al Master (fino ad un max di 10 punti). Per i lavori pubblicati all'estero deve risultare la data ed il luogo di pubblicazione. Non saranno valutati lavori originali non pubblicati od in corso di stampa. In caso di presentazione di estratti anche in copia conforme, dovrà essere possibile rilevare l'editore. altri titoli di studio e professionali, atti di frequenza a corsi professionali e di aggiornamento, e attestati di attività professionali in campi attinenti al Master (fino ad un massimo di 10 punti). titoli di conoscenza della lingua inglese (fino ad un max di 10 punti; le prove di accertamento della lingua inglese superate come esame di un corso di laurea valgono tanti punti quanto sono i crediti attribuiti moltiplicati per due, fino a saturazione a 10). Saranno selezionati per l'iscrizione al Master i primi dieci candidati secondo la graduatoria formata dalla valutazione dei titoli. Ai fini della valutazione dei titoli il candidato dovrà inviare, tramite raccomandata R.R., alla Direzione del Corso entro e non oltre il 08/11/2011 (presso il Dipartimento di Elettrotecnica, Elettronica ed Informatica, Università degli Studi di Trieste, Piazzale Europa 1, 34127 TRIESTE tel: 040 558 7124) tutta la documentazione necessaria corredata dalla modulistica (modulo B – distinta titoli - vedi modulistica) indicando sulla busta: "Domanda di ammissione al Master in "Gestione della Privacy e della Sicurezza Informatica in Sanità".

Conseguimento del titolo di Master in Gestione della Privacy e della Sicurezza Informatica nella pubblica Amministrazione.

Il Master prevede un ciclo didattico seguito da uno stage. Hanno diritto al titolo coloro che avranno frequentato almeno il 70% delle ore di lezione e che avranno superato le prove di verifica di ciascuna delle materie. Al termine dello stage lo studente è tenuto a presentare una tesi scritta su tematiche da concordare con i docenti e da sottoporre all'approvazione del direttore del Master. Il ciclo didattico darà diritto a 60 crediti formativi e lo stage, che si concluderà con la redazione di un elaborato consistente in un Documento Programmatico sulla Sicurezza secondo quanto previsto dal DLgs 96/03 "Codice in materia di protezione dei dati personali", Art. 34, comma g) e che darà diritto a 6 crediti formativi.

Insegnamenti

Area Informatico-ingegneristica-gestionale

- Fondamenti di sicurezza informatica (ING-INF/05) - 3 crediti formativi - 24 ore di lezione
- Reti di calcolatori (ING-INF/05) - 2 crediti formativi - 16 ore di lezione
- Modelli organizzativi per la sicurezza informatica nella pubblica amministrazione (ING-INF-05) - 2 crediti formativi - 16 ore di lezione
- Infrastrutture tecnologiche per la sicurezza informatica nella pubblica amministrazione (ING-INF05) - 2 crediti formativi - 16 ore di lezione
- La sicurezza informatica in un progetto di ICT (ING-INF05) - 2 crediti formativi - 16 ore di lezione
- Tecniche di protezione e crittografia dei dati (ING-INF05) - 1 crediti formativi - 8 ore di lezione
- Tecniche di protezione e sicurezza dei documenti digitali (ING-INF05) - 2 crediti formativi - 16 ore di lezione
- Sicurezza e privacy nel trattamento informatico dei dati sensibili (ING-INF05) - 3 crediti formativi - 24 ore di lezione
- Organizzazione della Sicurezza e della Privacy su Internet (ING-INF05) - 3 crediti formativi - 24 ore di lezione
- Sicurezza delle reti di telecomunicazioni (ING-INF05) - 2 crediti formativi - 16 ore di lezione
- Privacy e Sicurezza ICT nella Pubblica Amministrazione (ING-INF05) - 2 crediti formativi – 16 ore di lezione
- Valutazione e Gestione del rischio informatico (ING-INF05) - 3 crediti formativi - 24 ore di lezione
- Redazione, valutazione e monitoraggio dell'attuazione di un Piano di sicurezza informatica (ING-INF05) - 3 crediti formativi - 24 ore di lezione
- Redazione di un Documento Programmatico della Sicurezza (ING-INF05) – 3 crediti formativi – 24 ore di lezione

Area Giuridico – sociale - criminologica

- Diritto dell'Informatica (EC089) – 4 crediti formativi 32 ore di lezione
- Economia delle Aziende Pubbliche e no profit (SECS-P02) – 3 crediti formativi 16 ore di lezione
- Inquadramento normativo e giuridico delle Privacy (IUS04) - 3 crediti formativi - 24 ore di lezione
- Firma digitale e documento informatico (IUS04) - 2 crediti formativi - 16 ore di lezione
- Analisi del rapporto costi/benefici nel trattamento del rischio (IUS04) - 1 crediti formativi – 8 ore di lezione
- Modalità di redazione e di analisi di Capitolati di gara relativamente agli aspetti di sicurezza informatica e tutela della privacy (IUS04) - 2 crediti formativi - 16 ore di lezione
- Norme e standard nazionali ed internazionali di sicurezza informatica (IUS04) - 2 crediti formativi - 16 ore di lezione
- e-health –sanità e salute al tempo di internet (89S) – 2 crediti formativi – 16 ore di lezione
- Informatica Forense (IUS04) – 2 crediti formativi – 16 ore di lezione
- Stage - 6 crediti formativi

Informazioni

Le informazioni sono disponibili sul sito dell'Università di Trieste:

http://esse3web.units.it/esse3/Guide/PaginaCorso.do;jsessionid=BE5314EAE5CED3B97E4573378D356455?corso_id=10345

Qui la documentazione e la modulistica per l'iscrizione:

http://apps.units.it/Sitedirectory/InformazioniSpecificheCdS/Default.aspx?cdsid=10345&ordinamento=2011&sede=1&int=web&lingua=15

Il Master è stato ritenuto di rilevante interesse dall'INPS, che ha attivato un bando per 20 borse di studio a copertura dell'intero importo di iscrizione, destinate a disoccupati/inoccupati figli o nipoti di Pubblici Dipendenti in servizio o pensionati. Di seguito il collegamento al Bando:

http://www.inps.it/portale/default.aspx?sID=%3b0%3b9154%3b9155%3b&lastMenu=9155&iMenu=1&itemDir=9329

Sono stati richiesti contributi per Borse di Studio riservate in particolare a dipendenti pubblici a Sponsor. Ogni informazione è reperibile sul sito del Master:

http://masterprivacy.inginf.units.it/

Tutti i corsi saranno disponibili sulla piattaforma didattica Moodle d'Ateneo. Di seguito la pagina relativa alla precedente edizione:

http://privacy.di3.units.it/moodle/

Per qualsiasi informazione e per preiscrizioni, scrivere a:

accardo@units.it

depetris@ssic.units.it