Sezione 1 - E-Health: Sicurezza Informatica E Privacy

Dati generali | Caratteristiche | ISTAT Professioni

Durata (in ore)
200

Ore in aula
200

Ore in laboratorio
0

Tipologia laboratorio

Settore
servizi socio sanitari

Ambito
Nuovi settori hi-tech nella Regione Puglia

Descrizione Ambito
Con il termine E-health, di recente ideazione, si fa riferimento all'utilizzo di strumenti informatici, personale specializzato e tecniche di comunicazione medico-paziente nella pratica della salute e, quindi, al complesso delle risorse, soluzioni e tecnologie informatiche di rete applicate alla salute ed alla sanità. Con la crescente diffusione ed applicazione di soluzioni ICT (Information & Communications Technology) nel settore della sanità, si rende necessario salvaguardare la sicurezza informatica e la privacy del cittadino-utente e paziente, sempre più coinvolto nei nuovi processi di profilazione e gestione dei dati personali e sensibili. La sempre maggiore integrazione dei processi amministrativi, organizzativi e clinici tra le diverse strutture sanitarie e l'avvio di reti regionali sanitarie a supporto di modelli organizzativi innovativi, che promuovono la continuità delle cure e la centralità del servizio al cittadino, richiedono tecniche innovative e personalizzate per lo scambio di dati, in modo efficiente, trasparente e sicuro tale da rispondere al bisogno di valide garanzie di sicurezza sia per il paziente, in merito al rispetto della sua dignità e delle sue libertà personali, che per chi è responsabile del trattamento del dato con riferimento alle responsabilità civili e penali che ne conseguono (art.11, 15, 31, 33 e succ. Dlgs 196/03). Nello specifico, lo scopo è: supportare i pazienti per migliorare la qualità della loro vita; garantire la sicurezza sui dati del paziente secondo preferenze di privacy espresse dal paziente stesso e conformi alle normative vigenti; fornire una nuova tecnologia alle organizzazioni sanitarie per affrontare gli attacchi informatici nella gestione dei dati. Da un punto di vista implementativo, è necessario che ogni struttura dotata di Sistemi Informativi automatizzati definisca un Piano di Sicurezza, in grado di fornire servizi secondo standard di riservatezza nell'accesso ai dati (prevedendo per es. meccanismi di autenticazione forte come i dispositivi biometrici, le password dinamiche, i certificati digitali, ecc..), disponibilità (ovvero di fruibilità delle risorse da parte dell'utente autorizzato in presenza di guasti informatici o di eventi catastrofici) continuità, integrità delle informazioni-comunicazioni (in tale contesto l'adozione della firma elettronica, nelle sue declinazioni avanzata, qualificata e digitale, e del processo di conservazione digitale, rafforzano il tema dell'integrità, affermando i principi di autenticità e certezza dell'origine del documento oggetto di firma digitale), autenticità (ovvero certezza sulla provenienza dei dati racchiusi nel messaggio), affidabilità. Di qui l'esigenza di un profilo professionale, sempre più richiesto dagli enti pubblici e privati socio-sanitari, che garantisca sicurezza e privacy nei sistemi informatici: il Security Manager.

Figura di Riferimento
Figura di riferimento scelta da repertorio regionale di riferimento

Descrizione Figura
Il Security manager (esperto della sicurezza) è uno specialista in grado di individuare eventuali intrusioni o tentativi di spionaggio elettronico ai danni dell'impresa per la quale lavora. Contro tali forme di aggressione, egli mette in campo la propria preparazione tecnico-scientifica al fine di garantire e proteggere i dati su Internet, intranet e reti. Il Security manager, oltre a progettare antivirus e a mettere in atto - in caso di necessità - l'antispionaggio industriale, deve anche intervenire direttamente sul software dell'azienda, rendendolo impenetrabile dall'esterno con appositi filtri, qualora i tradizionali antivirus falliscano il proprio compito. Egli ha, inoltre, il dovere di mantenersi costantemente aggiornato in tema di sicurezza (tutela della privacy, legislazione relativa ai crimini informatici), e su tutti i nuovi tipi di virus. Dovrà, quindi, effettuare con regolarità test di penetrazione e auditing (ricerca delle imperfezioni nella sicurezza di un sistema) del software; creare antivirus idonei, utilizzare specifici software per la crittografia, fornire ai membri dell'azienda una serie di procedure da seguire e controllare che vengano realmente applicate, nonché individuare eventuali imperfezioni nelle diverse applicazioni, in particolare quelle web, che costituiscono un rischio per eventuali infiltrazioni di intrusi. Il Security manager deve, altresì, essere in grado di elaborare e di adoperare tecniche di analisi dei rischi, in modo da prevedere le situazioni di pericolo e da ridurne gli eventuali danni. La valutazione del rapporto costi/benefici per gli interventi di tutela aziendale è, infine, un'altra mansione di sua competenza. Per svolgere al meglio la sua professione il Security manager deve possedere: ' competenze giuridico-legali e di criminologia, con riferimento specifico ai crimini informatici e alla tutela delle informazioni; ' nozioni sul rischio, sulla protezione aziendale e sulla tutela di marchi e brevetti; ' competenze relative ad Internet e a tutte le problematiche inerenti a server, reti e periferiche; ' familiarità con le piattaforme hardware e software e con le modalità del commercio elettronico, oltre che con i più diffusi protocolli di comunicazione e con i linguaggi come Java e HTML; ' padronanza della lingua inglese. La capacità di lavorare in team e la disponibilità ad orari flessibili, oltre all'autorevolezza necessaria per far comprendere al cliente l'importanza di adottare determinati provvedimenti che si ritengono indispensabili per la sicurezza, sono altre doti fondamentali per questa figura professionale.

Obiettivi di apprendimento (Competenze in uscita)
Il percorso si prefigge di fornire gli strumenti per conoscere, valutare e saper utilizzare i sistemi E-Health e gli aspetti giuridici e sociologici inerenti il loro uso, nonché i sistemi e le tecnologie di reti Internet per la sanità.
In particolare, gli obiettivi di apprendimento sono:
- acquisire le modalità di comprensione e valutazione della complessità delle problematiche di sicurezza che impattano sull'ICT aziendale, anticipandole con un approccio proattivo;
- saper stimare i costi e i benefici delle diverse soluzioni, valutare il ritorno degli investimenti in sicurezza e comprendere i risvolti organizzativi dell'information security;
- trattare gli aspetti legali e relativi alla normativa sulla privacy, sulla sicurezza e sulla protezione dei dati personali;
- saper progettare, valutare, implementare e gestire un Information Security Management System integrato con il core business aziendale, in accordo ai principali standard di riferimento, favorendo quindi un'efficace gestione dei rischi noti o prevedibili ed anticipando l'insorgenza dei nuovi.

Struttura del Percorso e Contenuti Formativi
Mod 1 ' E-Health: aspetti etici e giuridici (20 ore)
Mod 2 - ICT sul territorio e le reti Internet della sanità e dei servizi sociali (20 ore)
Mod 3 - Il Centro unificato di prenotazione (CUP) ed il nuovo modello di farmacia dei servizi (20 ore)
Mod 4 - I Certificati di malattia on-line (20 ore)
Mod 5 - La ricetta "dematerializzata" ai blocchi di partenza (20 ore)
Mod 6 - Il referto on-line (20 ore)
Mod 7 - La Cartella clinica elettronica (30 ore)
Mod 8 - Il fascicolo sanitario elettronico (FSE) e l'attuale scenario normativo (30 ore)
Mod 9 ' Management e organizzazione nell'area dell' E_Health (20 ore)

Attestazione finale
Attestato di Frequenza con profitto

Modalità Valutazione Finale degli Apprendimenti
Per verificare l'apprendimento, durante il percorso didattico saranno svolte delle verifiche in itinere con valutazione espressa in dieci decimi, mentre, a conclusione dell'intero percorso, è prevista una verifica finale, valutata in trentesimi, consistente in un test scritto sugli argomenti oggetto del corso.

Fabbisogno Occupazionale
Il continuo ingresso di aziende nel web ha reso il problema della sicurezza delle informazioni una questione centrale, non ulteriormente trascurabile: qualsiasi azienda che decida di affacciarsi in rete non può evitare di fare i conti con il problema della sicurezza. La sicurezza è oggi più che mai prevenzione, ma questo significa soprattutto rendere consapevoli i vari soggetti che vivono in azienda che la sicurezza gioca un ruolo importante, se non addirittura fondamentale, per lo sviluppo del business. È questo il tassello iniziale da cui bisogna partire per costruire una strategia di sicurezza coerente in azienda. Attualmente si rileva il crescente bisogno di sinergie fra le diverse aziende che sempre più devono fare sistema. Da qui nasce la necessità di individuare figure in grado di operare come interfacce fra le aziende e le altre realtà pubbliche e private. E' ormai evidente, infatti, che la crescente complessità aziendale e sociale richieda un maggiore scambio di informazioni, soprattutto in fase emergenziale. Operazione che non può che estrinsecarsi nell'individuazione, di norma all'interno del dipartimento stesso della security, di figure professionali con le opportune competenze e altamente specializzate per perseguire questo tipo di obiettivi. Il mercato e le best practices, anche internazionali, definiscono la security come un processo che si articola su tre componenti principali di sicurezza organizzativa, logica e fisica. Quest'ultima è stata rivalutata soprattutto nell'ultimo periodo (dopo che in alcuni anni aveva perso un po' di smalto a causa del proliferare di tecnologie informatiche), perché continua a costituire un pilastro importante per la protezione e la salvaguardia del patrimonio aziendale, soprattutto in realtà industriali che ricercano, ad esempio, certificazioni di settore, che richiedono standard in materia di sicurezza perimetrale, di controllo degli accessi e di sistemi di videosorveglianza. In tale quadro, proprio al fine di proteggere uno dei beni più importanti che le aziende hanno, ossia i dati dei propri clienti, diventa utile impiegare i security manager, le cui previsioni occupazionali sembrano, dunque, positive.

Note