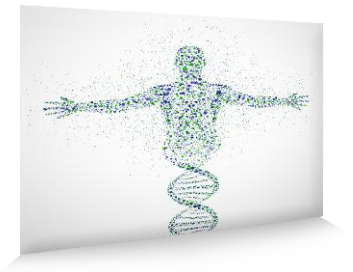
european informatics passport



EIPASS® Sanità Digitale

ver. 3.1

Programma analitico d'esame a cura di:

IMAPPS
Spin Off - Università degli Studi di Napoli Federico II

Disclaimer

Il presente documento è stato redatto da IMAPPS - Spin off dell'Università degli Studi di Napoli Federico II, in base agli standard e ai riferimenti Comunitari ed internazionali vigenti in materia di competenze digitali. IMAPPS non si assume alcuna responsabilità derivante dall'eventuale applicazione del documento in ambito diverso da quello per cui è stato redatto.

Copyright

Il presente documento è di esclusiva proprietà di Certipass che si riserva di aggiornarlo a propria discrezione, in ogni momento e senza darne preavviso, pubblicando le modifiche effettuate. L'Utenza destinataria è tenuta ad acquisire in merito periodiche informazioni, visitando le aree del sito dedicate al Programma.

È vietata qualsiasi riproduzione, anche parziale, del presente documento senza preventiva autorizzazione scritta da parte di Certipass (Unico Ente Erogatore del Programma internazionale di Certificazione Informatica EIPASS).

Il logo EIPASS è di proprietà esclusiva di Certipass. Tutti i diritti riservati.

Premessa

L'innovazione digitale applicata al settore sanitario sta assumendo un impatto significativo sulla qualità e sull'efficienza dei sistemi sanitari locali e delle aziende sanitarie.

I servizi digitali rappresentano una parte integrante della ridefinizione strutturale ed organizzativa del sistema delle reti sanitarie e assistenziali del Paese; la gestione razionale dell'intero processo di cura dei pazienti è oggetto di studio e di applicazione dell' informatica medica. La costante ricerca di adeguamento del settore del welfare, in generale, e di quello sanitario, in particolare, alle nuove tecnologie è motivata dalla considerazione diffusa che la e-health, se pienamente attuata, contribuirà a migliorare la qualità dell'assistenza sanitaria e a ridurne i costi.

Il nuovo scenario tecnologico che si presenta nel panorama sanitario rischia, se non si acquisisce una completa coscienza della rivoluzione culturale che la sanità digitale implica per la gestione della salute, di accentuare il digital divide ed aumentare il costo dell'ignoranza informatica nel settore sanitario.

Tutte le professioni sanitarie dovranno acquisire le competenze informatiche, specifiche dell'ambito medico, necessarie per utilizzare in modo sicuro e cosciente le applicazioni ICT: dal documento digitale unico al sistema sanitario per il supporto alle decisioni mediche (DSS), ogni attività sanitaria è stata o sarà "contaminata" irrevocabilmente da metodologie tecniche e applicazioni digitali.

Ogni operatore sanitario deve possedere, pertanto, un framework culturale teorico, pratico ed esperienziale che gli consenta di utilizzare in modo congruo le tecnologie della comunicazione e dell'informazione, favorendone le scelte e l'utilizzo con sistemi e soluzioni capaci di supportare in modo funzionale la propria attività professionale. In ogni caso, è imprescindibile, per ogni professionista sanitario, la conoscenza degli elementi fondamentali dell'organizzazione sanitaria in Italia e delle problematiche relative alla rappresentazione, alla conservazione e alla trasmissione di informazioni mediche.

Certipass
Comitato Tecnico-Scientifico

Programma analitico d'esame EIPASS Sanità Digitale

Il percorso di certificazione EIPASS Sanità Digitale, partendo dalle conoscenze generiche e di base delle tecnologie informatiche, intende fornire nozioni specifiche relative ai sistemi informativi sanitari.

Lo scopo è far acquisire al professionista sanitario il substrato tecnologico-normativo indispensabile per assolvere pienamente al ruolo di elemento attivo della Pubblica Amministrazione, per costruire, successivamente, le competenze specifiche delle professioni sanitarie.

Saranno ampiamente trattati il ruolo, l'anatomia e la struttura del Sistema Informativo Sanitario (SIS), per trasmettere al fruitore tutte le informazioni necessarie per diventare un operatore efficace, competente e produttivo.

Elenco moduli d'esame

Modulo 1: Informatica di base

Modulo 2: Digitalizzazione e archiviazione documentale

Modulo 3: Protezione elettronica del dato personale

Modulo 4: Sicurezza digitale

Modulo 5: Sanità digitale

Modulo 1

Informatica di base

Descrizione del modulo

L'innovazione tecnologica è un elemento fondamentale della new-economy; offre potenzialità che possono contribuire ad una vera e propria rivoluzione, anche nel campo dei servizi erogati dalle amministrazioni statali. Affinché ciò accada, è indispensabile che impiegati ed operatori diventino esperti conoscitori degli elementi basilari dell'ITC e di internet. Solo così potranno soddisfare le crescenti aspettative di cittadini ed imprese.

Il **Codice dell'Amministrazione Digitale** (D.Lgs. n. 82/2005) ha tracciato il quadro normativo entro cui deve attuarsi la digitalizzazione della Pubblica Amministrazione; in esso è definito il processo mediante il quale si deve arrivare ad un sistema finalmente moderno, digitale e paperless.

Il presente modulo ha come punto di partenza le conoscenze di base dell'ICT; percorre le metodologie di digitalizzazione dei documenti ed approda alla organizzazione e alla sicurezza dei dati. Lo suo studio è, pertanto, propedeutico all'approfondimento delle procedure di archiviazione documentale, ampiamente trattate nel successivo modulo, e alla piena definizione del ruolo dell'ICT nella Pubblica Amministrazione.

Obiettivo del modulo

Il modulo intende verificare le conoscenze e le abilità che il Candidato possiede in relazione ai contenuti basilari dell'Information Technology.

In particolare, il Candidato dovrà mostrare la propria preparazione in ordine ai seguenti argomenti:

- Introduzione all'ICT
  - Terminologia di base dell'Information Technology;
  - Hardware e software.
- Interfacce Grafiche
  - Componenti di una interfaccia grafica;
  - I menù e loro funzionamento;
  - Le interfacce "touch".
- Internet e il World Wide Web
  - Il funzionamento della rete Internet;
  - Il World Wide Web;
  - Altri servizi disponibili su Internet, posta elettronica e Social Network;
  - Ricercare informazioni sul web;
  - Criteri di ricerca e loro raffinamento;
  - Autorevolezza delle fonti sul Web.
- Digitalizzazione di un documento
  - Trasformare un documento cartaceo in formato digitale;
  - Formato immagine e formato testo;
  - Riconoscimento dei caratteri per la creazione di un file di testo modificabile (OCR/ICR).
- Organizzazione degli archivi digitali
  - L'importanza di una banca dati;
  - Classificazione e fascicolazione di un documento.
- Sicurezza dei dati
  - La cifratura dei dati;
  - La firma digitale;
  - Funzioni hash e Timestamping.

ARGOMENTO	AMBITI DI INTERVENTO		TESTING DI COMPETENZA	
1.0 Introduzione all'ICT	1.0.1	Terminologia di base dell'Information Technology	a.	Comprendere il significato di acronimi e termini propri del mondo ICT.
	1.0.2	Hardware e software	a.	Descrivere la differenza tra hardware e software.
			b.	Riconoscere i principali componenti hardware di un calcolatore.
			c.	Descrivere l'architettura di massima di un calcolatore.
			d.	Distinguere tra sistema operativo ed applicativi utente.
			e.	Conoscere le differenze tra eseguibili, file dati, director.
1.1 Interfacce Grafiche	1.1.1	Componenti di una interfaccia grafica	a.	Identificare le componenti principali di una GUI.
			b.	Descrivere i principi su cui si basa la direttiva 95/46/CE.
	1.1.2	I menù e loro funzionamento	a.	Saper distinguere tra i menù "general purpose" ed i menù "specialistici".
			b.	Comprendere l'utilizzo dei menù general purpose.
			c.	Saper descrivere le operazioni di base del menù general purpose.
			d.	Saper descrivere le operazioni di menù specialistici in applicazioni di ampio utilizzo (word processors, fogli elettronici, database).
			e.	Saper descrivere il concetto di scorciatoia al menù.

	1.1.3	Le interfacce "touch"	a. Comprendere l'utilizzo delle interfacce touch.
			b. Descrivere gli effetti delle operazioni di tap, slide e pitch.
			c. Saper descrivere i gadget che sostituiscono la tastiera.
1.2 Internet e il World Wide Web	1.2.1	Il funzionamento della rete Internet	a. Saper definire Internet.
			b. Conoscere le funzioni associate a diverse componenti della rete.
			c. Saper descrivere il processo di invio e ricezione delle informazioni.
	1.2.2	Il World Wide Web	a. Definire il World Wide Web.
			b. Comprendere la differenza tra Internet e WWW.
			c. Comprendere le possibili relazioni che intercorrono tra server web diversi.
	1.2.3	Altri servizi disponibili su Internet, posta elettronica e Social Network	a. Comprendere l'esistenza di servizi diversi dal WWW.
			b. Comprendere le differenze tra servizi diversi.
			c. Saper descrivere le funzionalità offerte da servizi web di ampia diffusione (e-mail, Pec, Social Network, motori di ricerca, forum).
	1.2.4	Ricercare informazioni sul web	a. Comprendere la terminologia di base associata ai servizi di ricerca.
			b. Conoscere i principali motori di ricerca.
			c. Saper definire il processo di reperimento delle informazioni.

			d. Comprendere il risultato delle richieste effettuate ai motori di ricerca.
	1.2.5	Criteri di ricerca e loro raffinamento	a. Saper effettuare una ricerca su un motore di ricerca.
			b. Saper descrivere il processo di raffinamento delle query.
			c. Saper identificare le modalità di raffinamento delle query.
	1.2.6	Autorevolezza delle fonti sul Web	a. Saper definire l'autorevolezza di una fonte su Internet.
			b. Saper descrivere i criteri che indicano la non autorevolezza di una fonte.
1.3 Digitalizzazione di un documento	1.3.1	Trasformare un documento cartaceo in formato digitale	a. Saper utilizzare le tecnologie per trasformare un documento cartaceo in uno digitale.
	1.3.2	Formato immagine e formato testo	a. Saper riconoscere i vari formati grafici e testo.
	1.3.3	Riconoscimento dei caratteri per la creazione di un file di testo modificabile (OCR/ICR).	a. Saper utilizzare software (OCR) per la conversione di un documento cartaceo in formato digitale, convertendolo in formato testo modificabile.
1.4 Organizzazione degli archivi digitali	1.4.1	L'importanza di una banca dati e la ricerca delle informazioni	a. Saper utilizzare ed interrogare una banca dati estrapolando informazioni utili e correlate tra loro, confrontando le variazioni tra un periodo e l'altro nella totalità dell'universo dati.
	1.4.2	Classificazione e fascicolazione di un documento	a. Saper svolgere l'attività di classificazione e fascicolazione di tutti i documenti prodotti da un determinato soggetto siano essi protocollati o no.
1.5 Sicurezza dei dati	1.5.1	La cifratura dei dati	a. Conoscere lo scopo degli algoritmi di cifratura.

		b. Saper discutere le differenze tra cifratura simmetrica ed asimmetrica.
		c. Conoscere le condizioni di sicurezza operativa.
1.5.2	La firma digitale	a. Comprendere lo strumento "firma digitale".
		b. Conoscere la definizione e le problematiche inerenti i certificati digitali.
		c. Saper discutere delle problematiche relative alla sicurezza della firma digitale.
1.5.3	Funzioni hash e Timestamping	a. Saper discutere dell'utilità delle funzioni hash e Timestamping.

Modulo 2

Digitalizzazione e archiviazione documentale

Descrizione del modulo

Il processo di archiviazione e conservazione dei flussi documentali in forma digitale è un fattore fondamentale per garantire nel tempo l'integrità, la provenienza, la reperibilità dei documenti. Tale processo favorisce la velocità delle operazioni di ufficio, determinando un abbattimento dei costi per le amministrazioni e le imprese: si tratta, quindi, di qualificante strumento di efficienza.

Negli ultimi anni, diversi interventi normativi hanno promosso il completo passaggio dalla carta al digitale, anche in alcuni ambiti della Pubblica Amministrazione: il documento informatico ha pieno riconoscimento giuridico ed è molto apprezzato dagli operatori per le nuove opportunità di gestione ed archiviazione dei dati che, se ben utilizzato, può assicurare.

La gestione informatica dei documenti, intesa come "insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla dematerializzazione, alla classificazione, organizzazione, assegnazione, reperimento e conservazione amministrativo-giuridica dei documenti informatici acquisiti dalle amministrazioni", si colloca come uno dei processi più importanti degli ultimi anni nell'evoluzione dei servizi erogati dalla Pubblica Amministrazione e dalle imprese.

In questo quadro, il Programma di certificazione informatica EIPASS Pubblica Amministrazione intende diffondere la cultura della dematerializzazione, affinché il personale addetto conosca i processi di:

- Razionalizzazione e unificazione dei flussi documentali e del protocollo informatico;
- Ammodernamento della Pubblica Amministrazione in termini di
  - miglioramento dei servizi resi a terzi,
  - trasparenza dell'azione amministrativa,
  - contenimento dei costi secondo criteri di economicità, efficacia e pubblicità dell'azione amministrativa.

Obiettivo del modulo

Il modulo intende accertare le competenze del Candidato sulle tecniche della digitalizzazione e dell'archiviazione documentale, trattate mediante il supporto delle nuove tecnologie del mondo ICT.

In particolare, il Candidato dovrà mostrare la propria preparazione in ordine ai seguenti argomenti:

- Il documento analogico ed informatico
  - Copie analogiche di documenti informatici;
  - Copie informatiche di documenti analogici;
  - Duplicati e copie informatiche di documenti informatici;
  - Procedimento e fascicolo informatico.
- Il codice dell'amministrazione digitale
  - Allineamento dei dati;
  - Autenticazione del documento informatico;
  - Carta d'identità elettronica;
  - Certificato qualificato.
- La dematerializzazione e conservazione sostitutiva
  - Dematerializzazione della documentazione amministrativa;
  - La conservazione sostitutiva dei documenti analogici ed informatici;
  - Il processo di conservazione sostitutiva;
  - La distruzione del documento passato in conservazione sostitutiva;
  - Il responsabile della conservazione.
- La firma elettronica
  - La firma elettronica avanzata;
  - La firma elettronica qualificata;
  - Dispositivi per la firma digitale.
- Il Timestamping
  - Uso della Marca temporale.
- La PEC
  - Principi di funzionamento dei meccanismi di crittografia a chiave pubblica;
  - Uso e gestione della posta certifica.

ARGOMENTO	AMBITI DI INTERVENTO		TESTING DI COMPETENZA
2.0 Il documento analogico ed informatico	2.0.1	Copie analogiche di documenti informatici	a. Conoscere gli obiettivi dell'Agenda Digitale.
			b. Conoscere la procedura per la realizzazione e la validazione di una copia analogica di un documento informatico.
	2.0.2	Copie informatiche di documenti analogici	a. Conoscere la procedura per realizzare documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti ed i documenti amministrativi, formati in origine su supporto analogico.
	2.0.3	Duplicati e copie informatiche di documenti informatici	a. Conoscere le vigenti regole tecniche e le procedure per realizzare copie informatiche di documenti informatici.
	2.0.4	Procedimento e fascicolo informatico	a. Conoscere le regole per la costituzione, l'identificazione e l'utilizzo del fascicolo informatico.
2.1 Il codice dell'amministrazione digitale	2.1.1	Allineamento dei dati	a. Saper definire il processo di allineamento dei dati.
	2.1.2	Autenticazione del documento informatico	a. Saper validare un documento digitale.
	2.1.3	Carta d'identità elettronica	a. Saper descrive l'utilizzo della carta nazionale dei servizi.
	2.1.4	Certificato qualificato	a. Conoscere la specificità dei certificati elettronici.
2.2 La Dematerializzazione e conservazione sostitutiva	2.2.1	Dematerializzazione della documentazione amministrativa	a. Saper individuare i processi qualificati per la trasposizione e il riversamento dei documenti dal formato cartaceo a quello digitale.

	2.2.2	La conservazione sostitutiva dei documenti analogici ed informatici	a. Saper valutare i benefici della conservazione sostitutiva per un'azienda e quali tipi di documenti possono essere conservati in modalità sostitutiva.
			b. Perché conservare in modo sostitutivo i messaggi PEC.
	2.2.3	Il processo di conservazione sostitutiva	a. Conoscere le operazioni basilari che vanno eseguite in una conservazione sostitutiva.
	2.2.4	La distruzione del documento passato in conservazione sostitutiva	a. Conoscere le procedure da rispettare per distruzione dei documenti cartacei.
	2.2.5	Il responsabile della conservazione	a. Conoscere il ruolo e le funzioni.
2.3 La firma elettronica	2.3.1	La firma elettronica avanzata	a. Conoscere la struttura della firma elettronica avanzata intesa come insieme di dati digitali allegati o connessi a un documento informatico che consentono l'identificazione univoca del firmatario del documento.
	2.3.2	La firma elettronica qualificata	a. Conoscere le specifiche della firma elettronica avanzata basata su un certificato qualificato.
	2.3.3	Dispositivi per la firma digitale	a. Saper utilizzare un dispositivo elettronico per la verifica della firma digitale.
2.4 Il Timestamping	2.4.1	Uso della Marca temporale	a. Conoscere il significato e l'utilizzo della Marca temporale, nonché l'importanza di un oggetto contenente l'Hash (riferimento univoco) del documento digitale.
2.5 La PEC	2.5.1	Principi di funzionamento dei meccanismi di crittografia a chiave pubblica	a. Saper definire il significato del termine crittografia ed indicare il suo ruolo in un sistema informatico.

		b. Saper descrive i meccanismi alla base della crittografia a chiave pubblica.
2.5.2	Uso e gestione della posta certifica	a. Conoscere la procedura di "invio e ricezione" della posta certificata.
		b. Saper individuare la ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata.
		c. Saper attivare la procedura di recupero della ricevuta di posta inviata nel caso di uno smarrimento.

Modulo 3

Protezione elettronica del dato personale

Descrizione del modulo

Il termine privacy sta ad indicare il diritto alla riservatezza delle informazioni personali e della propria vita privata: è uno strumento posto a salvaguardia e a tutela della sfera privata del singolo individuo.

Il diritto alla privacy ha, dunque, lo scopo di impedire che le informazioni riguardanti tale sfera personale siano divulgate in assenza dell'autorizzazione dell'interessato; tutela, inoltre, il diritto alla non intromissione nella sfera privata da parte di terzi. Ciò assicura che i dati riguardanti la vita privata di ogni singolo individuo vengono protetti, tutelati e al contempo diffuse secondo regole chiare che infondono fiducia nell'individuo stesso.

Le regole, cui si faceva cenno in precedenza, devono essere indipendenti dalle modalità tecniche utilizzate: devono, cioè, essere applicabili in qualsiasi contesto, sia se i dati personali vengano divulgati tramite pubblicazione cartacea sia se immessi in rete tramite pubblicazione sul web.

I motivi della riforma (IP/12/46) sono chiari: l'economia digitale ha bisogno della fiducia dei consumatori per svilupparsi. Norme rigorose ed affidabili devono essere applicate uniformemente in modo da rendere il trattamento dei dati più sicuro e meno costoso, nell'interesse di tutti.

Obiettivo del modulo

Il Modulo intende approfondire i contenuti delle **Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali - Consultazione pubblica (26 luglio 2012)**, il cui scopo è quello di definire in modo unitario le misure e gli accorgimenti che i soggetti pubblici sono tenuti a rispettare ed applicare in attuazione alle disposizioni normative vigenti sulla privacy, in fatto di trasparenza, pubblicità dell'azione amministrativa e consultazione di atti pubblici.

- Trattamento dei dati personali
  - Protezione dei dati personali e legge sulla privacy;
  - Il Garante per la protezione dei dati personali;
  - Informativa sul trattamento all'interessato.
- La raccolta dei consensi
  - Trattamento dei dati da parte del datore di lavoro;
  - Trattamento dei dati relativi a studenti;
  - Trattamento dei dati da parte di soggetti privati;
  - La lettera di informatica e consenso.
- Misure di sicurezza
  - Misure minime;
  - Le autorizzazioni;
  - Trattamenti con o senza l'ausilio di strumenti elettronici.

ARGOMENTO	AMBITI DI INTERVENTO		TESTING DI COMPETENZA
3.0 Trattamento dei dati personali	3.0.1	Protezione dei dati personali e legge sulla privacy	a. Conoscere le normative che regolano il trattamento dei dati personali concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la selezione, l'estrazione, la comunicazione, la diffusione e la cancellazione, anche se non registrati in una banca dati.
	3.0.2	Il Garante per la protezione dei dati personali	a. Conoscere gli adempimenti del Garante in fatto di protezione dei dati personali.
	3.0.3	Informativa sul trattamento all'interessato	a. Conoscere gli adempimenti a cui il "Titolare" deve ottemperare per il corretto trattamento dei dati e la regolare comunicazione dovuta all'interessato.
3.1 La raccolta dei consensi	3.1.1	Trattamento dei dati da parte del datore di lavoro	a. Sapere quando e come il datore deve chiedere il consenso del dipendente, per utilizzarne correttamente i dati sensibili.
	3.1.2	Trattamento dei dati relativi a studenti	a. Sapere quando e come si può chiedere allo studente l'utilizzo dei suoi dati sensibili.
	3.1.3	Trattamento dei dati da parte di soggetti privati	a. Conoscere le norme che regolano il trattamento dei dati di soggetti privati.
	3.1.4	La lettera di informatica e consenso	a. Conoscere la procedura corretta affinché l'ottenimento del consenso da parte dell'interessato sia valido.
3.2 Misure di sicurezza	3.2.1	Misure minime	a. Conoscere le misure minime di sicurezza obbligatorie volte ad assicurare la protezione dei dati personali.
	3.2.2	Le autorizzazioni	a. Conoscere i vari tipi di autorizzazioni che il Garante può concedere per operazioni specifiche sul trattamento dei dati sensibili.

3.2.3	Trattamenti con o senza l'ausilio di strumenti elettronici	a. Conoscere le misure minime da adottare per il trattamento dei dati sensibili nei seguenti due casi: › Trattamento con strumenti elettronici. › Trattamento senza l'ausilio di strumenti elettronici.

Modulo 4

Sicurezza digitale

Descrizione del modulo

Uno degli aspetti più importanti nell'evoluzione del mondo digitale emerso negli ultimi anni è quello concernente la protezione e la salvaguardia dei dati digitali dagli attacchi dei cybercriminali.

La sicurezza digitale è ormai parte integrante di qualsiasi sistema informatico ed ha come obiettivo la tutela dell'integrità fisica (hardware) e logico-funzionale (software) del suddetto sistema e dei dati in esso contenuti o scambiati in una comunicazione con un utente.

Tale protezione è ottenuta attraverso misure di carattere tecnico-organizzativo e funzionali tese ad assicurarne:

- L'accesso fisico e/o logico solo ad utenti autorizzati (autenticazione);
- La fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (disponibilità);
- La correttezza dei dati (integrità);
- L'oscuramento dei dati (cifratura);
- La protezione del sistema da attacchi di software malevoli.

Obiettivo del modulo

Il continuo aggiornamento professionale, lo scambio di informazioni, la consapevolezza dell'importanza della norma sono gli strumenti più efficaci per far fronte ai problemi della sicurezza informatica. Il Modulo approfondisce i contenuti più importanti del tema e verifica che il Candidato ne abbia compreso la centralità e abbia acquisito le competenze necessarie per operare efficacemente anche in questo contesto.

- Sicurezza dei dati
  - Sicurezza dei dati, dei sistemi e delle infrastrutture delle PA;
  - Procedure di gestione del trattamento dati, adozioni delle misure minime;
  - Memorizzazione non volatile dei dati.
- Normativa sulla sicurezza dei dati
  - Il Codice in materia di protezione dei dati personali;
  - Il quadro normativo in materia di protezione dei dati personali;
  - Documento Programmatico per la Sicurezza e documento di conformità delle misure di sicurezza.
- Tecniche di sicurezza
  - Sicurezza passiva;
  - Sicurezza attiva;
- Principali tecniche di difesa
  - Difesa hardware e software;
  - Sicurezza della rete internet;
- Sicurezza sanitaria
  - I concetti di data storage e backup;
  - Principi fondamentali di sicurezza di un SIS.

ARGOMENTO	AMBITI DI INTERVENTO		TESTING DI COMPETENZA
4.0 Sicurezza dei dati	4.0.1	Sicurezza dei dati, dei sistemi e delle infrastrutture delle PA	a. Conoscere le regole tecniche stabilite nella normativa vigente che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture.
	4.0.2	Procedure di gestione del trattamento dati, adozioni delle misure minime.	a. Conoscere le misure previste per la protezione dei dati.
			b. Definire le attività da svolgere in caso di violazione della sicurezza dei dati personali.
	4.0.3	Memorizzazione non volatile dei dati	a. Conoscere i dispositivi hardware, le infrastrutture ed i software dedicati alla memorizzazione non volatile di informazioni in formato elettronico.
			b. Conoscere la differenza tra storage e backup.
4.1 Normativa sulla sicurezza dei dati	4.1.1	Il Codice in materia di protezione dei dati personali	a. Conoscenza del Codice che garantisce il trattamento dei dati personali con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
	4.1.2	Il quadro normativo in materia di protezione dei dati personali	a. Conoscere le norme fondamentali destinate a garantire la fiducia degli utilizzatori nei servizi e nelle tecnologie delle comunicazioni elettroniche.
	4.1.3	Documento Programmatico per la Sicurezza e documento di conformità delle misure di sicurezza	a. Conoscere lo stato normativo del Documento Programmatico per la Sicurezza e l'evoluzione verso il documento di conformità (Decreto Monti su Privacy e documento programmatico)

4.2 Tecniche di sicurezza	4.2.1	Sicurezza passiva	a. Conoscere le tecniche e gli strumenti di tipo difensivo ossia quel complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata (sicurezza passiva).
	4.2.2	Sicurezza attiva	a. Conoscere tutte quelle tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (confidenzialità), sia dalla possibilità che un utente non autorizzato possa modificarli (integrità). (sicurezza attiva).
4.3 Principali tecniche di difesa	4.3.1	Difese hardware e software	a. Conoscere le principali tecniche di difesa sia hardware che software.
	4.3.2	Sicurezza della rete internet	a. Conoscere il programma di protezione "Safer Internet" e i vari apparati di sicurezza di rete come: Firewall, Intrusion detection system (IDS), Intrusion prevention system(IPS).
5.4 Sicurezza sanitaria	4.4.1	I concetti di data storage e backup	a. Conoscere i dispositivi hardware, le infrastrutture ed i software dedicati alla memorizzazione non volatile di informazioni in formato elettronico.
			b. Definire la differenza tra storage e backup.
	4.4.2	Principi fondamentali di sicurezza di un SIS	a. Saper individuare le vulnerabilità dei sistemi informativi.
			b. Individuare possibili minacce alla sicurezza di un SIS.

Modulo 5

Descrizione del modulo

Il modulo presenta l'e-Health, ovvero lo studio di servizi innovativi basati sulle TIC, che supportano la gestione di dati, informazioni e conoscenze in campo sanitario. I modelli, le tecnologie e i servizi presentati avranno come riferimento il sistema sanitario italiano e il quadro normativo nazionale ed europeo. Il modulo descriverà il contributo fornito dall'ICT nei seguenti tre aspetti:

- Supporto dei processi sanitari e amministrativi delle aziende sanitarie;
- Gestione delle relazioni tra strutture e pazienti;
- Governo dei sistemi sanitari regionali e nazionali.

Il background comune a tutti i capitoli del presente modulo avrà come paradigma innovativo la centralità della condivisione dell'informazione clinica e della sua gestione digitale sicura, trasparente e rispettosa delle norme; il risultato finale sarà il disegno di un sistema sanitario che rapidamente si avvia a diventare paperless e filmles.

Obiettivo del modulo

Il Modulo intende far acquisire al discente tutte le nozioni utili per comprendere e partecipare attivamente all'organizzazione, alla struttura e agli aspetti chiave di un Sistema Informativo Sanitario.

Il professionista sanitario sarà in grado di definire ed attivare i processi di produzione, archiviazione e trasmissione sicura dei dati sanitari.

Le tecnologie Medical imaging occuperanno una parte rilevante del modulo; il percorso previsto parte dalla definizioni di base e arriva allo studio del RIS - sistema informatico radiologico -, descrivendone le caratteristiche, il ruolo e i motivi, anche storici, per cui tale sistema è centrale in un'organizzazione sanitaria.

Centrale è il capitolo relativo ai Documenti Digitali; il discente sarà in grado di individuare le specificità e il ruolo dei vari documenti all'interno del Fascicolo Sanitario Elettronico (libretto sanitario digitale).

La parte finale è riservata alle tecniche di digitalizzazione e validazione dei documenti.

- Sistema Informativo
  - Sistema informativo sanitario;
  - Struttura di un Sistema Informativo Sanitario;
  - La Banca Dati e il Repository aziendale;
  - Sistema informatico per il supporto alle decisioni mediche (dss).
- Medical Imaging Technology
  - Basi di Medical Imaging;
  - Elaborazione delle immagini;
  - ACS - Sistema di archiviazione e trasmissione di immagini;
  - RIS - Sistema informatico radiologico.
- Documenti digitali
  - Documento Digitale Unificato;
  - Fascicolo Sanitario Elettronico;
  - Le Cartelle Cliniche personali (Personal Health Record, PHR);
  - Le Cartelle Cliniche informatizzate (EHR);
  - La digitalizzazione dei documenti sanitari.

ARGOMENTO	AMBITI DI INTERVENTO		TESTING DI COMPETENZA	
5.0 Sistema Informativo	5.0.1	Sistema informativo sanitario	a.	Descrivere il ruolo di un Sistema Informativo Sanitario ed indicare il tipo di operazione gestiste in questo ambito.
	5.0.2	Struttura di un Sistema Informativo Sanitario	a.	Definire la struttura e le funzioni di un SIS, identificando e riconoscendone funzioni e strumenti.
	5.0.3	La Banca Dati e il Repository aziendale	a.	Definire cos'è una base dati, classificarle in base alle proprietà, descriverne struttura e organizzazione.
			b.	Definire cos'è un repository clinico-sanitario aziendale, da cosa si differenzia da una base di dati, classificarlo e descriverne struttura e organizzazione.
	5.0.4	Sistema informatico per il supporto alle decisioni mediche (dss)	a.	Descrivere le caratteristiche di un DSS.
			b.	Individuare il ruolo di un DSS e le situazioni cliniche in cui sono utilizzati.
			c.	Indicare i dati e le informazioni che utilizzano per la produzione dei risultati.
5.1 Medical Imaging Technology	5.1.1	Basi di Medical Imaging	a.	Descrivere le tecniche e le metodologie per il Medical Imaging.
	5.1.2	Elaborazione delle immagini	a.	Descrivere le metodiche di acquisizione e di elaborazione delle immagini.
	5.1.3	ACS - Sistema di archiviazione e trasmissione di immagini	a.	Descrivere il sistema hardware e software dedicato all'archiviazione, trasmissione, visualizzazione e stampa delle immagini diagnostiche digitali.
			b.	Definire le procedure con cui vengono ricevute e trasmesse le immagini.

	5.1.4	RIS - Sistema informatico radiologico	a. Descrivere le funzionalità del RIS ed indicare il rapporto tra il RIS e il sistema di integrazione informatica di una radiologia.
5.2 Documenti digitali	5.2.1	Documento Digitale Unificato (art. 1 Decreto 179/2012 "Ulteriori misure urgenti per la crescita del Paese")	a. Descrivere le caratteristiche del nuovo documento digitale, indicandone le funzioni svolte e i servizi telematici accessibili.
	5.2.2	Fascicolo Sanitario Elettronico (art. 12 Decreto 179/2012 "Ulteriori misure urgenti per la crescita del Paese")	a. Descrivere l'insieme dei documenti appartenenti al FSE e la loro strutturazione, i dati contenuti e la codifica degli stessi.
			b. Definire ruoli, profili e modalità di accesso al FSE.
	5.2.3	Le Cartelle Cliniche personali (Personal Health Record, PHR)	a. Descrivere la struttura, l'organizzazione e gli obiettivi di una cartella clinica personale. Individuare le differenze con una EHR. Definire il meccanismo di aggiornamento, controllo e accesso ad una PHR.
	5.2.4	Le Cartelle Cliniche informatizzate (EHR)	a. Descrivere la struttura, l'organizzazione e gli obiettivi di una cartella clinica informatizzata.
			b. Definire i meccanismi di condivisione e il sistema di accesso a una EHR.
	5.2.5	La digitalizzazione dei documenti sanitari	a. Descriverei principi fondamentali per la digitalizzazione dei documenti sanitari.
			b. Conoscere i sistemi di validazione di un documento, la marca temporale e il riferimento temporale.