

CRITERI VALUTAZIONE

La Commissione stabilisce i criteri per la valutazione della **prova scritta** che vengono di seguito riportati: la Commissione ha a disposizione 30 punti per la valutazione della prova scritta e pertanto decide di assegnare 1 punto per ogni risposta corretta, 0 punti se errata o non data.

Il superamento della prova scritta è subordinata al raggiungimento di una valutazione di sufficienza, espressa in termini numerici, di almeno 21/30.

La Commissione stabilisce i criteri per la valutazione della **prova pratica** che vengono di seguito riportati: la Commissione ha a disposizione 20 punti per la valutazione della prova pratica, tenendo presente i seguenti criteri:

- precisione del linguaggio e dei termini utilizzati,
- sintesi espositiva,
- conoscenza della materia,
- correttezza e congruenza dei contenuti esposti.

Il superamento della prova pratica è subordinata al raggiungimento di una valutazione di sufficienza, espressa in termini numerici, di almeno 14/20.

La Commissione stabilisce i criteri per la valutazione della **prova orale** che vengono di seguito riportati:

- precisione del linguaggio e dei termini utilizzati,
- sintesi espositiva,
- conoscenza della materia,
- correttezza e congruenza dei contenuti esposti.

Il superamento della prova orale è subordinata al raggiungimento di una valutazione di sufficienza, espressa in termini numerici, di almeno 14/20.

CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI - PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO PROFESSIONALE – INFORMATICO

PROVA SCRITTA N. 1

- 1. Nell'ambito della gestione delle immagini in radiologia, come definirebbe il ruolo del formato DICOM?**
 - (a) È lo standard internazionale per l'archiviazione, la visualizzazione e la trasmissione di immagini e dati diagnostici
 - (b) È un protocollo di rete generico utilizzato esclusivamente per la configurazione dei router ospedalieri
 - (c) È un sistema operativo proprietario sviluppato per il controllo delle macchine radiogene
- 2. Parlando di interoperabilità tra sistemi informativi sanitari, a cosa ci riferiamo quando citiamo lo standard HL7?**
 - (a) A un set di regole per la cifratura dei dati sensibili a riposo nei database
 - (b) Allo standard di riferimento per lo scambio elettronico di informazioni cliniche e amministrative tra sistemi informativi eterogenei
 - (c) A un modello di database dedicato esclusivamente alla gestione dei flussi di magazzino farmaceutico
- 3. Potrebbe spiegare qual è l'utilità principale di una "worklist DICOM" nel flusso di lavoro ospedaliero?**
 - (a) Permette di trasferire automaticamente i dati anagrafici e la lista degli esami prenotati dal RIS ai dispositivi diagnostici, evitando inserimenti manuali
 - (b) Serve a generare un backup crittografato delle immagini immediatamente dopo l'acquisizione
 - (c) È un registro digitale dove i tecnici annotano gli interventi di manutenzione e i fermi macchina
- 4. Quale tra queste descrive meglio la funzione cardine di un sistema PACS all'interno di una struttura sanitaria?**
 - (a) Il monitoraggio dei parametri vitali dei pazienti tramite sensori IoT in tempo reale
 - (b) La gestione centralizzata dell'accettazione e della fatturazione delle prestazioni sanitarie
 - (c) L'archiviazione a lungo termine, la ricerca e la distribuzione rapida di immagini e referti diagnostici
- 5. Quando analizziamo il "rischio clinico" associato all'uso di un software, cosa stiamo valutando nello specifico?**
 - (a) La probabilità che un errore o un malfunzionamento del software provochi un danno diretto o indiretto alla salute del paziente (es. errore diagnostico)
 - (b) Il rischio puramente economico derivante dalla necessità di riparare i server hardware
 - (c) L'eventualità che un ritardo della rete locale impedisca il completamento delle attività amministrative di ufficio
- 6. Qual è l'obiettivo primario perseguito dal Regolamento (UE) 2017/745 (MDR)?**
 - (a) Stabilire standard rigorosi per garantire la sicurezza, l'efficacia e la tracciabilità dei dispositivi medici in tutto il mercato europeo
 - (b) Gestire esclusivamente l'assegnazione degli indirizzi IP all'interno delle infrastrutture IT ospedaliere
 - (c) Fornire le linee guida generali per la protezione dei dati dei cittadini, indipendentemente dal settore d'uso

- 7. Cosa attesta, di fatto, la presenza della marcatura CE su un dispositivo medico?**
- (a) Identifica il Paese di origine del prodotto per fini statistici
 - (b) Attesta che il dispositivo è conforme ai requisiti essenziali previsti dalle direttive o regolamenti comunitari
 - (c) Garantisce che il dispositivo verrà aggiornato gratuitamente dal produttore per almeno dieci anni
- 8. Nel contesto della sicurezza dei dispositivi elettromedicali, quale aspetto viene regolato dalla norma CEI EN 60601-1?**
- (a) I requisiti generali di sicurezza elettrica e le prestazioni essenziali per garantire la protezione di pazienti e operatori
 - (b) Le politiche di gestione delle password per l'accesso ai portali sanitari regionali
 - (c) Gli standard di cablaggio strutturato per la posa di fibra ottica negli ospedali
- 9. Per quale motivo un piano di manutenzione preventiva è considerato fondamentale in ambito clinico?**
- (a) Per agire proattivamente sulle cause di possibile guasto, minimizzando i tempi di fermo macchina e i rischi per il paziente
 - (b) Per permettere l'intervento tecnico solo nel momento in cui l'apparecchio smette di funzionare
 - (c) Per garantire che il sistema operativo riceva sempre l'ultima interfaccia grafica disponibile
- 10. Come definirebbe l'operazione di "taratura" applicata a un dispositivo di misurazione?**
- (a) Un insieme di procedure volte a determinare, e se necessario regolare, lo scostamento tra il valore misurato e un riferimento standard
 - (b) La pulizia approfondita dei sensori e la sanificazione esterna del dispositivo
 - (c) L'installazione della versione più aggiornata del software di gestione (patching)
- 11. Perché è indispensabile garantire la sincronizzazione dell'orario (es. tramite NTP) su tutti i dispositivi clinici?**
- (a) Per ottimizzare il risparmio energetico riducendo la frequenza di aggiornamento dei log di sistema
 - (b) Per accelerare la velocità di trasferimento dei file pesanti tra server differenti
 - (c) Per assicurare la corretta correlazione temporale degli eventi clinici e diagnostici, fondamentale anche ai fini medico-legali
- 12. Potrebbe illustrare la differenza tecnica tra l'isolamento galvanico e la messa a terra di un sistema?**
- (a) L'isolamento galvanico interrompe il percorso di corrente continua tra due circuiti permettendo lo scambio di segnali (es. via trasformatore); la messa a terra disperde cariche indesiderate per sicurezza
 - (b) L'isolamento galvanico serve a disperdere i fulmini, mentre la messa a terra separa elettricamente il paziente dalla rete
 - (c) La messa a terra protegge i dati dalla cancellazione, l'isolamento galvanico impedisce l'accesso non autorizzato ai server
- 13. Quali sono le principali criticità di sicurezza da considerare quando si connette un dispositivo medico in rete?**
- (a) Il rischio di attacchi informatici che potrebbero alterare il funzionamento del dispositivo o esporre dati sensibili del paziente
 - (b) Un miglioramento automatico della stabilità del dispositivo che non richiede più manutenzione fisica
 - (c) Nessuna criticità, poichè i moderni router isolano automaticamente i dispositivi medici dal traffico internet

- 14. In ambito clinico, cosa si intende con il fenomeno della "alarm fatigue"?**
- (a) Il deterioramento dei sensori acustici dovuto all'usura meccanica continua
 - (b) La desensibilizzazione del personale sanitario dovuta all'eccessivo numero di allarmi, che può portare a ignorare segnali critici
 - (c) Un rallentamento della rete che ritarda la notifica visiva degli allarmi sulle console centrali
- 15. In un'architettura IT sanitaria, quale funzione svolge solitamente un gateway?**
- (a) La memorizzazione persistente di tutte le cartelle cliniche elettroniche
 - (b) La funzione di nodo intermedio che media e isola il traffico tra reti o protocolli di comunicazione differenti
 - (c) L'esecuzione dei test di conformità elettrica sui dispositivi connessi
- 16. Quale pilastro della sicurezza informatica viene garantito principalmente attraverso l'uso della cifratura?**
- (a) La disponibilità dei dati in caso di guasto hardware
 - (b) L'integrità fisica dei supporti di memorizzazione
 - (c) La riservatezza delle informazioni, rendendole inintelligibili a chi non possiede la chiave
- 17. Come descriverebbe l'operatività standard di un firewall aziendale?**
- (a) L'ispezione e il filtraggio del traffico dati in transito in base a regole di sicurezza predefinite
 - (b) La creazione automatica di copie di sicurezza di ogni file ricevuto via email
 - (c) La trasformazione di tutti i segnali analogici in digitali per la protezione dai disturbi elettrici
- 18. Cosa si prefigge di ottenere l'applicazione del principio del "minimo privilegio"?**
- (a) Di limitare i costi di licenza software assegnando i permessi a pochi utenti scelti
 - (b) Di concedere a ogni utente solo i permessi strettamente necessari per svolgere le proprie mansioni specifiche
 - (c) Di dare agli amministratori di sistema il diritto di accedere a qualunque dato privato per fini di controllo
- 19. Come si distingue un attacco di phishing da altre minacce informatiche?**
- (a) E' un tentativo di frode basato su tecniche di ingegneria sociale per indurre l'utente a rivelare credenziali o dati sensibili
 - (b) E' un attacco diretto che sfrutta falle fisiche nei server per distruggere i dischi fissi
 - (c) E' una tecnica che rallenta la velocità di connessione internet per saturare la banda larga
- 20. Qual è la differenza fondamentale tra una configurazione RAID e una strategia di backup?**
- (a) Il backup protegge solo dai virus, il RAID serve a velocizzare l'avvio del computer
 - (b) Il RAID garantisce la continuità operativa in caso di guasto ai dischi; il backup protegge dalla perdita definitiva dei dati (es. cancellazione accidentale o cifratura malevola)
 - (c) Il RAID sostituisce completamente la necessità di effettuare backup periodici
- 21. Cosa si intende tecnicamente per "vulnerabilità software"?**
- (a) Una falla o debolezza nel codice di un programma che può essere sfruttata per compromettere la sicurezza del sistema
 - (b) L'assenza di una licenza d'uso valida per il software installato
 - (c) Un errore nella documentazione tecnica che rende difficile l'uso del software da parte dell'utente
- 22. In cosa consiste l'attività di "patch management" all'interno di un'organizzazione?**
- (a) Nella gestione sistematica degli aggiornamenti (patch) per correggere falle di sicurezza e bug del software
 - (b) Nella riparazione fisica dei componenti hardware danneggiati da sbalzi di tensione
 - (c) Nella mappatura dei cavi di rete all'interno dei patch-panel in sala server

- 23. Qual è lo scopo principale dell'autenticazione a due fattori (MFA)?**
- (a) Permettere a due persone diverse di accedere contemporaneamente allo stesso account
 - (b) Aumentare la sicurezza richiedendo la verifica di due diversi fattori (es. password e codice su smartphone)
 - (c) Dimezzare il tempo di digitazione delle credenziali di accesso
- 24. Per quale finalità tecnica viene solitamente implementata una VLAN?**
- (a) Per migliorare la risoluzione video dei monitor diagnostici connessi alla rete
 - (b) Per segmentare logicamente una rete fisica in più reti separate, migliorando sicurezza e gestione del traffico
 - (c) Per permettere a un computer di funzionare anche in assenza di alimentazione elettrica
- 25. Cosa succede se due dispositivi su una rete locale hanno configurato lo stesso indirizzo IP?**
- (a) Si verifica un conflitto di rete che impedisce a uno o entrambi i dispositivi di comunicare correttamente
 - (b) La velocità della rete raddoppia grazie alla condivisione dell'indirizzo
 - (c) La sicurezza aumenta poichè i dati vengono inviati in duplice copia a entrambi i dispositivi
- 26. In ambito informatico, a cosa ci riferiamo con il termine "log"?**
- (a) A un'interfaccia grafica semplificata per utenti non esperti
 - (b) A un file che registra cronologicamente gli eventi, le operazioni o gli errori avvenuti in un sistema
 - (c) Al processo di spegnimento controllato di un server critico
- 27. Qual è la funzione principale di un sistema SIEM (Security Information and Event Management)?**
- (a) La centralizzazione e l'analisi dei dati di sicurezza (log) per rilevare tempestivamente minacce o anomalie
 - (b) La gestione automatizzata della climatizzazione e dell'energia nel data center
 - (c) La distribuzione del carico di lavoro tra i vari processori di un server (load balancing)
- 28. Qual è la differenza sostanziale nell'uso tipico tra VPN IPsec e VPN SSL?**
- (a) IPsec è generalmente usata per connessioni persistenti "sito-sito"; SSL è spesso usata per l'accesso remoto di singoli utenti via browser o client leggero
 - (b) IPsec funziona solo su reti cablate, mentre SSL è progettata esclusivamente per il Wi-Fi
 - (c) La VPN SSL non utilizza alcuna forma di crittografia, a differenza della IPsec
- 29. Qual è la distinzione fondamentale tra hashing e cifratura?**
- (a) L'hashing è unidirezionale (non invertibile), la cifratura è bidirezionale (invertibile tramite chiave)
 - (b) L'hashing è molto più lento della cifratura e si usa solo per file di grandi dimensioni
 - (c) Entrambi i processi richiedono obbligatoriamente l'invio di una chiave pubblica al destinatario
- 30. In una connessione sicura TLS/HTTPS, come viene garantita l'autenticità del server?**
- (a) Attraverso l'uso di un certificato digitale emesso da una terza parte fidata (Certification Authority)
 - (b) Verificando che il colore della barra degli indirizzi sia sempre verde
 - (c) Grazie al filtraggio preventivo effettuato dai DNS pubblici dell'operatore telefonico

CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI - PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO PROFESSIONALE – INFORMATICO

PROVA SCRITTA N. 2

- 1. Potrebbe descrivere in cosa consiste la procedura di "collaudo di accettazione" di una nuova apparecchiatura?**
 - (a) La verifica formale e tecnica che il dispositivo sia sicuro e conforme ai requisiti prima dell'uso clinico
 - (b) La semplice operazione fisica di sballaggio e posizionamento del dispositivo in reparto
 - (c) Un intervento di manutenzione programmata da eseguire dopo il primo anno di utilizzo
- 2. Quali sono le possibili conseguenze di un'interferenza elettromagnetica (EMC) non controllata in un ambiente ospedaliero?**
 - (a) Il rallentamento della velocità di navigazione internet sulle postazioni amministrative
 - (b) La perdita definitiva delle configurazioni software salvate sui database centrali
 - (c) L'alterazione del corretto funzionamento dei dispositivi medici o la distorsione dei segnali acquisiti
- 3. In fase di acquisizione di una tecnologia, cosa si intende per TCO (Total Cost of Ownership)?**
 - (a) La valutazione di tutti i costi diretti e indiretti lungo l'intero ciclo di vita del dispositivo (acquisto, gestione, smaltimento)
 - (b) Esclusivamente il prezzo di listino concordato con il fornitore al momento dell'ordine
 - (c) Il solo costo relativo ai canoni annui di manutenzione hardware e aggiornamento software
- 4. Cosa determina, solitamente, la dichiarazione di "fine vita" (End of Life) di un dispositivo medico?**
 - (a) Il momento in cui la mancanza di supporto tecnico o ricambi non è più sicuro o sostenibile mantenerlo in funzione
 - (b) La scadenza naturale del periodo di garanzia contrattuale offerto dal produttore
 - (c) La conclusione del turno di utilizzo giornaliero previsto per quella specifica apparecchiatura
- 5. Cosa si intende per interoperabilità effettiva tra un ecografo e il sistema PACS?**
 - (a) La sola capacità dell'ecografo di mostrare a video la lista dei pazienti della giornata
 - (b) La capacità di scambiare immagini e metadati in formato standard DICOM per l'archiviazione e la refertazione
 - (c) La possibilità di controllare i parametri fisici dell'ecografo agendo direttamente dalla console del PACS
- 7. Un dispositivo elettromedicale funziona ma non comunica con il sistema centrale. Qual è il primo controllo tecnico da effettuare?**
 - (a) La verifica della configurazione IP e della connettività fisica (cavi/switch) e logica di rete
 - (b) La riesecuzione della taratura della precisione dei sensori del dispositivo
 - (c) Il controllo della tensione di alimentazione elettrica della presa a muro
- 7. In un flusso RIS-PACS, se le immagini sono associate al paziente sbagliato, dove risiede più probabilmente il problema?**
 - (a) In un errore nel protocollo di trasferimento fisico dei pacchetti dati DICOM
 - (b) In un'errata compilazione della worklist o in un mancato matching degli identificativi (HL7/DICOM)
 - (c) In un guasto hardware dei dischi di archiviazione del server PACS principale

- 8. Come definirebbe lo standard DICOM nel contesto della sanità digitale?**
- (a) È lo standard internazionale per la comunicazione e gestione delle immagini e dei dati diagnostici
 - (b) È un protocollo di instradamento dei pacchetti dati specifico per le reti Wi-Fi ospedaliere
 - (c) È un sistema operativo sviluppato per garantire la compatibilità tra diverse macchine radiologiche
- 9. Qual è il ruolo principale dello standard HL7 tra sistemi informativi sanitari?**
- (a) Definire le chiavi di cifratura per la protezione dei dati durante il transito su reti pubbliche
 - (b) Fornire il quadro di regole per lo scambio e l'integrazione di dati clinici e amministrativi tra software diversi
 - (c) Gestire la struttura delle tabelle all'interno di un database SQL dedicato alla cartella clinica
- 10. Qual è il vantaggio operativo derivante dall'utilizzo di una "worklist DICOM"?**
- (a) L'invio automatico dei dati anagrafici dei pazienti ai dispositivi, riducendo errori di inserimento manuale
 - (b) La creazione di una copia di backup delle immagini sulla memoria locale della modalità diagnostica
 - (c) La gestione del calendario delle manutenzioni preventive e straordinarie dei dispositivi
- 11. Qual è la finalità principale di un sistema PACS in una struttura moderna?**
- (a) Il monitoraggio delle performance e del traffico dati di tutta la rete locale
 - (b) La gestione delle anagrafiche e della contabilità amministrativa dei pazienti
 - (c) L'archiviazione sicura, la ricerca e la distribuzione tempestiva delle immagini diagnostiche
- 12. Cosa stabilisce il Regolamento (UE) 2017/745 (MDR) in merito ai dispositivi medici?**
- (a) Definisce i requisiti stringenti per la sicurezza, la progettazione e la commercializzazione dei dispositivi medici in Europa
 - (b) Regola esclusivamente le modalità di accesso alle reti IT degli uffici amministrativi
 - (c) Fornisce le norme generali per il trattamento della privacy, indipendentemente dal tipo di dispositivo
- 13. In cosa differisce la manutenzione preventiva da quella correttiva?**
- (a) La preventiva mira a ridurre la probabilità di guasti futuri tramite controlli programmati
 - (b) La preventiva serve unicamente a riparare un guasto già avvenuto nel minor tempo possibile
 - (c) La preventiva viene eseguita solo se il software segnala un errore di sistema imprevisto
- 14. Qual è la differenza tecnica tra isolamento galvanico e messa a terra?**
- (a) L'isolamento separa elettricamente i circuiti permettendo lo scambio di segnali; la messa a terra scarica dispersioni per sicurezza
 - (b) L'isolamento galvanico disperde i sovraccarichi atmosferici; la messa a terra isola elettricamente i segnali
 - (c) La messa a terra serve a separare logicamente due reti; l'isolamento galvanico protegge dalla perdita di dati
- 15. In ambito software medico, come si definisce il "rischio clinico"?**
- (a) La possibilità che un bug o un errore logico del software influenzi negativamente la diagnosi o la terapia
 - (b) Il rischio legato alla rottura fisica dei monitor o dei componenti hardware del server
 - (c) L'eventualità di un ritardo nella latenza di rete che rallenta l'apertura delle cartelle cliniche

16. Cosa si intende tecnicamente con il termine "Data Breach"?

- (a) Una violazione della sicurezza che comporta la perdita, la modifica o l'accesso non autorizzato a dati personali
- (b) Un errore nel processo di backup che impedisce il salvataggio dei dati giornalieri
- (c) Un guasto improvviso dei dischi fissi che rende i dati temporaneamente indisponibili

17. Qual è l'obiettivo di un'attività di "Penetration Test"?

- (a) Configurare in modo ottimale le regole del firewall aziendale
- (b) Verificare la corretta installazione dell'antivirus su tutti i client
- (c) Simulare attacchi informatici reali per identificare e correggere vulnerabilità nei sistemi

18. Cosa si intende per architettura di sicurezza "Zero Trust"?

- (a) Un modello basato sul presupposto che nessuna entità sia fidata a priori e che ogni accesso vada verificato continuamente
- (b) Una rete priva di misure di sicurezza in cui ogni utente ha accesso libero a tutte le risorse
- (c) Un sistema in cui non è possibile fidarsi dell'integrità dei dati salvati nei backup

19. Qual è la funzione principale del servizio DNS in una rete informatica?

- (a) Cifrare i dati trasmessi tra il client e il server web
- (b) Tradurre i nomi di dominio (es. www.ospedale.it) negli indirizzi IP corrispondenti
- (c) Gestire la programmazione automatica delle copie di sicurezza dei database

20. Perché è considerato rischioso mantenere in produzione un software non aggiornato?

- (a) Perché espone il sistema a vulnerabilità note che potrebbero essere sfruttate per attacchi informatici
- (b) Unicamente perché il software diventa sensibilmente più lento a ogni operazione
- (c) Perché comporta la perdita immediata e irreversibile di tutti i dati storici salvati

21. Cosa indica il concetto di "Business Continuity" in ambito sanitario?

- (a) La sola presenza di un backup automatico dei dati eseguito ogni notte
- (b) La capacità di ripristinare i dati dopo che si è verificato un guasto totale (Disaster Recovery)
- (c) L'insieme delle procedure atte a mantenere operativi i servizi critici anche durante una crisi o un guasto

22. Quale caratteristica del dato viene protetta prioritariamente tramite la cifratura?

- (a) L'integrità, ovvero la certezza che il dato non sia stato modificato
- (b) La disponibilità, ovvero l'accesso al dato in qualsiasi momento
- (c) La riservatezza, ovvero l'accesso al dato solo da parte di chi ne ha diritto

23. Qual è il compito principale di un firewall all'interno di una rete aziendale?

- (a) Monitorare e filtrare il traffico dati in entrata e in uscita secondo criteri di sicurezza prestabiliti
- (b) Cifrare in maniera trasparente tutti i database presenti nella rete interna
- (c) Effettuare la sincronizzazione dei backup tra la sede principale e quella secondaria

24. Cosa prevede l'applicazione rigorosa del principio del "minimo privilegio"?

- (a) L'assegnazione temporanea di pieni poteri a tutti gli utenti del sistema
- (b) La concessione agli amministratori di sistema di credenziali universali sempre attive
- (c) L'attribuzione all'utente dei soli permessi indispensabili per svolgere le proprie mansioni

25. Qual è la caratteristica distintiva di un attacco di tipo phishing?

- (a) L'uso di tecniche di manipolazione (ingegneria sociale) per sottrarre informazioni tramite messaggi ingannevoli
- (b) Un attacco di tipo brute-force mirato a indovinare la password del database
- (c) L'inserimento di codice malevolo all'interno di un form di una pagina web (SQL Injection)

- 26. Qual è la differenza sostanziale tra una configurazione RAID e una procedura di backup?**
- (a) Il backup protegge solo dai guasti fisici, mentre il RAID serve a comprimere i dati
 - (b) Il RAID può essere considerato a tutti gli effetti un sostituto della strategia di backup
 - (c) Il RAID garantisce la tolleranza ai guasti hardware, il backup protegge dalla perdita logica o accidentale dei dati
- 27. Come definirebbe una "vulnerabilità software" in termini di cybersecurity?**
- (a) Una debolezza o falla nel sistema che può essere sfruttata per violarne la sicurezza
 - (b) Una configurazione hardware errata che impedisce l'accensione del server
 - (c) La presenza di un aggiornamento software che non è ancora stato installato dall'utente
- 28. In cosa consiste l'attività di "patch management"?**
- (a) Nella gestione e installazione sistematica degli aggiornamenti per correggere bug e falle di sicurezza
 - (b) Nella configurazione fisica dei collegamenti tra i server e gli switch di rete
 - (c) Nel monitoraggio continuo del carico di lavoro dei processori e della memoria RAM
- 29. Qual è il vantaggio principale dell'autenticazione basata su chiavi (es. SSH keys) rispetto alle password?**
- (a) Un aumento significativo della velocità di trasmissione dei dati sulla rete
 - (b) Una drastica riduzione dei rischi legati ad attacchi di forza bruta e phishing sulle credenziali
 - (c) L'eliminazione totale della necessità di tenere dei log di accesso al sistema
- 30. In caso di attacco ransomware, quale misura si rivela più efficace per ridurre l'impatto operativo?**
- (a) Disporre di un antivirus costantemente aggiornato su tutte le postazioni
 - (b) Avere un backup offline (isolato dalla rete) e testato periodicamente per il ripristino
 - (c) Utilizzare un firewall perimetrale di ultima generazione con ispezione dei pacchetti

CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI - PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO PROFESSIONALE – INFORMATICO

PROVA SCRITTA N. 3

- 1. Cosa attesta formalmente la presenza della marcatura CE su un dispositivo medico?**
 - (a) L'identità e la sede legale del produttore del dispositivo
 - (b) La conformità del prodotto ai requisiti essenziali di sicurezza e prestazione previsti dalle norme UE
 - (c) La garanzia di un servizio di assistenza tecnica post-vendita illimitato nel tempo
- 2. Quale ambito della tecnologia sanitaria viene regolato dalla norma CEI EN 60601-1?**
 - (a) I requisiti generali per la sicurezza elettrica e le prestazioni essenziali dei dispositivi elettromedicali
 - (b) Le procedure amministrative per la gestione della privacy dei pazienti
 - (c) Gli standard di comunicazione e cablaggio per le reti LAN ospedaliere
- 3. In cosa consiste l'operazione di "taratura" applicata a un dispositivo di misurazione clinica?**
 - (a) Nella verifica e regolazione della precisione del dispositivo rispetto a uno standard di riferimento
 - (b) Nella pulizia approfondita dei componenti ottici e meccanici dell'apparecchiatura
 - (c) Nell'installazione dell'ultima versione disponibile del firmware di gestione
- 4. Perché è considerato fondamentale sincronizzare l'orario (es. tramite protocollo NTP) di tutti i dispositivi in rete?**
 - (a) Per ridurre il carico di messaggi sulla rete e ottimizzare il risparmio energetico
 - (b) Per aumentare la velocità di elaborazione dei server durante i picchi di traffico
 - (c) Per poter correlare temporalmente in modo univoco tutti gli eventi clinici e diagnostici (valore medico-legale)
- 5. Quali sono le principali criticità nel collegare un dispositivo medico alla rete informatica aziendale?**
 - (a) L'esposizione a potenziali minacce cyber che potrebbero compromettere l'integrità del dispositivo e dei dati
 - (b) Un miglioramento automatico della sicurezza clinica senza necessità di ulteriori controlli
 - (c) Non vi sono rischi aggiuntivi, in quanto i vantaggi della connettività eliminano ogni pericolo
- 8. In un reparto ad alta intensità tecnologica, cosa si intende per "alarm fatigue"?**
 - (a) Un progressivo degradamento fisico dei sistemi di notifica acustica
 - (b) La riduzione dell'attenzione del personale dovuta all'eccessivo numero di allarmi, con rischio di ignorare segnali critici
 - (c) Un ritardo sistematico nella trasmissione dei segnali di allerta verso le centraline di monitoraggio
- 7. Qual è la funzione cardine di un gateway all'interno di un'infrastruttura clinica complessa?**
 - (a) L'archiviazione definitiva di tutti i dati clinici acquisiti dai reparti
 - (b) La mediazione, l'isolamento e la traduzione delle comunicazioni tra reti o protocolli differenti
 - (c) L'esecuzione automatica dei backup per i database delle cartelle cliniche

- 8. Potrebbe spiegare l'obiettivo principale del "collaudo di accettazione" di un nuovo dispositivo?**
- (a) Verificare che l'apparecchiatura sia conforme ai requisiti di sicurezza e operativi prima di metterla in uso
 - (b) Effettuare la sola installazione fisica del dispositivo nella sua collocazione definitiva
 - (c) Eseguire la prima operazione di manutenzione ordinaria prevista dal contratto
- 9. In che modo un'interferenza elettromagnetica (EMC) può impattare sull'attività sanitaria?**
- (a) Causando un'interruzione temporanea della navigazione internet negli uffici amministrativi
 - (b) Provocando la perdita dei dati anagrafici salvati sui server centrali
 - (c) Alterando il corretto funzionamento dei dispositivi medici o la qualità dei segnali diagnostici acquisiti
- 10. Come definirebbe il TCO (Total Cost of Ownership) nell'ambito della gestione delle tecnologie sanitarie?**
- (a) La somma di tutti i costi diretti e indiretti generati dal dispositivo lungo tutto il suo ciclo di vita
 - (b) Il solo prezzo di acquisto del bene al momento della chiusura della gara d'appalto
 - (c) La spesa annuale dedicata esclusivamente ai ricambi e agli aggiornamenti software
- 11. Cosa indica tecnicamente la "fine vita" (End of Life) di un dispositivo medico?**
- (a) Il momento in cui non è più considerato sicuro o economicamente sostenibile mantenere l'apparecchio operativo
 - (b) La naturale scadenza del periodo di garanzia offerto dal produttore (solitamente 12-24 mesi)
 - (c) La fine del normale utilizzo del dispositivo al termine di una sessione di lavoro giornaliera
- 12. Cosa si intende per interoperabilità tra un ecografo e un sistema PACS?**
- (a) La sola capacità del dispositivo di ricevere la lista dei pazienti (worklist) dal sistema centrale
 - (b) La capacità di scambiare immagini e dati clinici in formato standard DICOM tra i due sistemi
 - (c) La possibilità di pilotare le funzioni dell'ecografo utilizzando esclusivamente l'interfaccia del PACS
- 13. In presenza di un dispositivo che non comunica con il sistema centrale, quale controllo suggerirebbe come prioritario?**
- (a) La verifica della configurazione IP e della connettività fisica e logica della rete
 - (b) La ripetizione della procedura di taratura della precisione del dispositivo
 - (c) Il controllo dell'interruttore generale dell'alimentazione elettrica
- 14. In un sistema RIS-PACS, qual è la causa più probabile di un'errata associazione tra immagini e paziente?**
- (a) Un errore tecnico nel protocollo di trasferimento fisico dei dati DICOM
 - (b) Un errore nel matching degli identificativi del paziente tra i messaggi HL7 e lo standard DICOM
 - (c) Un problema hardware relativo ai dischi di archiviazione del server PACS
- 15. Qual è la finalità principale di un sistema PACS in un'azienda sanitaria?**
- (a) Il monitoraggio costante dell'integrità e del traffico dei pacchetti di rete
 - (b) La gestione centralizzata dell'accettazione e della fatturazione delle prestazioni
 - (c) L'archiviazione e la distribuzione efficiente delle immagini diagnostiche agli operatori autorizzati

- 16. Qual è lo scopo principale dell'implementazione di un'autenticazione a due fattori (MFA)?**
- (a) Velocizzare le operazioni di login per il personale sanitario
 - (b) Aumentare la sicurezza richiedendo due diversi elementi di verifica dell'identità dell'utente
 - (c) Eliminare definitivamente l'utilizzo delle password alfanumeriche
- 17. Per quale esigenza tecnica si decide di configurare una VLAN?**
- (a) Per sostituire integralmente le funzioni di un firewall perimetrale
 - (b) Per incrementare le prestazioni di calcolo dei processori dei server
 - (c) Per segmentare logicamente una rete fisica in più sottoreti isolate e sicure
- 18. Cosa accade se a due dispositivi in rete viene assegnato accidentalmente lo stesso indirizzo IP?**
- (a) Si genera un conflitto di rete che impedisce a uno o entrambi i dispositivi di comunicare correttamente
 - (b) Si ottiene un miglioramento della ridondanza della connessione internet
 - (c) La sicurezza dei dati aumenta grazie alla creazione automatica di copie ridondate dei pacchetti
- 19. Cosa si intende con il termine "log" in ambito di amministrazione di sistema?**
- (a) Una copia di sicurezza completa di tutti i file dell'utente
 - (b) Un registro cronologico che riporta le attività e gli eventi significativi avvenuti nel sistema
 - (c) La configurazione specifica delle risorse hardware del server
- 20. Qual è la funzione cardine di una piattaforma SIEM?**
- (a) La raccolta e l'analisi centralizzata dei log di sicurezza per il rilevamento di anomalie
 - (b) La gestione automatizzata della rotazione dei backup sui nastri magnetici
 - (c) Il monitoraggio puramente visivo dello stato dei cavi nelle sale server
- 21. Potrebbe illustrare la differenza d'uso tipica tra una VPN IPsec e una VPN SSL?**
- (a) La VPN SSL è intrinsecamente più sicura della IPsec per qualsiasi tipo di utilizzo
 - (b) La IPsec è ideale per collegamenti permanenti tra sedi; la SSL per l'accesso remoto di singoli utenti
 - (c) La tecnologia IPsec è utilizzabile esclusivamente tramite un comune browser web
- 22. Cosa definisce tecnicamente una situazione di "Data Breach"?**
- (a) Una violazione della sicurezza che compromette la riservatezza, l'integrità o la disponibilità di dati personali
 - (b) Il fallimento del processo di backup notturno programmato sul database
 - (c) Un guasto hardware che richiede la sostituzione fisica di un server di rete
- 23. Qual è l'obiettivo finale di un "Penetration Test"?**
- (a) Definire la configurazione ottimale delle regole di un firewall
 - (b) Procedere all'installazione dell'antivirus su tutte le postazioni di lavoro
 - (c) Simulare scenari di attacco reale per individuare e sanare le vulnerabilità del sistema
- 24. Cosa si intende per modello di sicurezza "Zero Trust"?**
- (a) Un approccio che prevede la verifica continua dell'identità e dell'accesso per ogni singola transazione
 - (b) Una rete priva di qualunque sistema di difesa dove ogni utente ha accesso illimitato
 - (c) Un sistema in cui non è possibile fare affidamento sull'integrità dei dati salvati nei backup
- 25. Qual è la funzione del servizio DNS (Domain Name System)?**
- (a) Cifrare il traffico dati tra il client e il server remoto
 - (b) Risolvere i nomi di dominio (es. sanita.it) negli indirizzi IP numerici corrispondenti
 - (c) Gestire la pianificazione delle copie di sicurezza dei sistemi critici

26. Qual è il rischio principale derivante dall'utilizzo di un software non aggiornato?

- (a) L'esposizione a vulnerabilità di sicurezza note che potrebbero facilitare intrusioni esterne
- (b) Una riduzione generale della velocità di esecuzione delle operazioni amministrative
- (c) La perdita immediata dei dati nel momento in cui il software viene chiuso

27. Cosa si prefigge di garantire una strategia di "Business Continuity"?

- (a) L'esecuzione automatica del backup dei file ogni volta che vengono salvati
- (b) Il ripristino delle informazioni esclusivamente dopo che un guasto grave si è concluso
- (c) La capacità di mantenere operativi i servizi critici anche durante situazioni di emergenza o crisi

28. Cosa distingue un Vulnerability Assessment da un Penetration Test?

- (a) Sono due termini che indicano esattamente la stessa attività tecnica
- (b) Il Penetration Test è un processo automatico, mentre il Vulnerability Assessment è manuale
- (c) Il primo identifica le falle teoriche; il secondo ne verifica l'effettiva sfruttabilità

29. Quale di questi principi appartiene a un'architettura di tipo Zero Trust?

- (a) La verifica continua e costante dell'identità e del contesto per ogni richiesta di accesso
- (b) L'accesso libero e non controllato a tutte le risorse della rete interna aziendale
- (c) La fiducia implicita garantita a ogni dispositivo che sia di proprietà dell'azienda

30. Qual è il rischio più critico legato all'utilizzo di credenziali di accesso condivise?

- (a) L'impossibilità di attribuire responsabilità individuali e l'aumento dei rischi di uso improprio
- (b) L'impossibilità tecnica di garantire un corretto piano di Disaster Recovery
- (c) Un aumento significativo della latenza di risposta del server durante l'accesso

CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI - PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO PROFESSIONALE – INFORMATICO

PROVA PRATICA N. 1

Il candidato scelga e svolga uno dei quesiti tra quelli indicati, predisponendo un elaborato completo, chiaro e coerente con le richieste della traccia.

Quesito 1

Si rende necessario installare una centrale di monitoraggio per i parametri vitali dei pazienti in una Stroke Unit.

Il candidato descriva:

- le modalità di integrazione con i sistemi informativi tipici di un ospedale (es. ADT, CCE, repository clinico, sistemi di allarme);
- gli standard di interoperabilità eventualmente utilizzati;
- le principali considerazioni relative alla sicurezza dei dati e alla continuità operativa.

Si descrivano inoltre i test minimi essenziali da effettuare prima della messa in esercizio su pazienti.

Quesito 2

In seguito a un attacco ransomware che ha colpito sistemi clinici, il candidato definisca:

- piano di risposta all'incidente
- strategie di continuità operativa
- gestione dei backup (strategie, test, segregazione)
- comunicazione interna ed esterna
- misure preventive future

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA PRATICA N. 2

**Il candidato scelga e svolga uno dei quesiti tra quelli indicati,
predisponendo un elaborato completo, chiaro e coerente con le richieste della traccia.**

Quesito 1

Un'Azienda Ospedaliera ha pianificato l'evoluzione tecnologica dei propri sistemi dedicati all'area dell'Emergenza-Urgenza attraverso l'implementazione di una nuova soluzione digitale.

Il candidato in relazione a

Analisi Funzionale: illustri i requisiti funzionali e i processi clinico-organizzativi che la soluzione deve supportare per gestire correttamente il flusso del paziente in emergenza (dall'accoglienza alla dimissione/trasferimento);

Interoperabilità: descriva il modello di integrazione con l'ecosistema digitale esistente (composto da sistemi di anagrafica centralizzata, repository clinici e strumenti di prescrizione/ordine), specificando i flussi informativi e gli standard di comunicazione necessari a garantire la coerenza del dato;

Project Management: definisca un piano operativo per la transizione alla nuova soluzione, strutturato per fasi (es. analisi, configurazione, test, formazione, go-live);

Risk Management: identifichi le principali criticità attese, definendo le strategie per garantire la continuità operativa durante lo switch-over, la qualità delle informazioni migrate e la sicurezza dei dati sensibili."

Quesito 2

Nel reparto di cardiologia è presente un sistema elettromedicale gestito da un PC con sistema operativo Windows 8.

Il primario richiede l'integrazione in rete per l'invio delle immagini al PACS aziendale.

Il candidato descriva:

- le principali criticità tecniche e di sicurezza;
- le valutazioni preliminari da effettuare (es. analisi del rischio, verifica conformità, assessment vulnerabilità);
- le possibili opzioni operative.

Si richiede di motivare le scelte.

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA PRATICA N. 3

**Il candidato scelga e svolga uno dei quesiti tra quelli indicati,
predisponendo un elaborato completo, chiaro e coerente con le richieste della traccia.**

Quesito 1

Nell'ambulatorio di oculistica della Casa di Comunità di Darfo Boario Terme è emersa la necessità di acquisire un retinografo.

Il candidato descriva:

1. Le informazioni minime da raccogliere dai clinici per garantire la corretta integrazione del sistema.
2. I requisiti tecnici e funzionali minimi dell'apparecchiatura
3. Le condizioni necessarie per l'integrazione con il Fascicolo Sanitario Elettronico

Quesito 2

In un moderno contesto sanitario digitale, la resilienza delle infrastrutture è condizione essenziale per la sicurezza delle cure. Il candidato tratti i paradigmi della Business Continuity (BC) e del Disaster Recovery (DR), approfondendo i seguenti punti:

Quadro Concettuale: definisca i due concetti evidenziandone le interdipendenze, le specificità operative e le principali differenze (es. obiettivi di ripristino RTO e RPO);

Pianificazione Strategica: illustri i contenuti portanti di un Business Continuity Plan (BCP) e di un Disaster Recovery Plan (DRP), con un focus specifico sulla protezione dei sistemi critici ad alta intensità assistenziale (es. Pronto Soccorso, Terapie Intensive, Sale Operatorie);

Analisi d'Impatto: descriva il ruolo della Business Impact Analysis (BIA) come strumento per prioritizzare il ripristino dei servizi in relazione agli aspetti tecnologici, organizzativi e di sicurezza dei dati;

Contestualizzazione e Sfide: identifichi le criticità tipiche nell'implementazione di tali piani all'interno di un'Azienda Sanitaria (es. obsolescenza tecnologica, sistemi legacy, formazione del personale) e indichi gli elementi chiave per garantirne l'efficacia e l'aggiornamento continuo.

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 1

I nuovi frigoriferi acquistati per le case di comunità non hanno un disco grafico per la registrazione delle temperature che devono essere visionate al PC. L'operatore deve scaricare il grafico settimanalmente utilizzando una memoria USB. Quali considerazioni può fare su questo sistema?

What are the main components of a computer system, and what is the function of each one?

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 2

Cosa si intende per telemedicina? Quali sono gli ambiti di applicazione, le finalità e quali sono le principali categorie dei servizi di telemedicina?

What is an operating system, and why is it essential for a computer to work properly?

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 3

Differenza principale tra Televisita, Telemonitoraggio e Telerefertazione.

Nel caso si intendano monitorare i parametri di un paziente a domicilio (glicemia, peso, saturazione, etc...). Quali sono gli strumenti e le infrastrutture che ritengono necessarie?

What is malware, and what are the most common types that can affect a computer system?

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 4

Qual è il rischio della conservazione di tutti i dati di uno strumento elettromedicale in locale sul dispositivo? Quali possono essere le alternative?

What is data privacy, and why is it especially important in the healthcare sector?

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 5

Qual è il rischio principale derivante dalla mancata integrazione della strumentazione elettromedicale con i sistemi informatici ospedalieri?

The candidate shall explain what is meant in the General Data Protection Regulation (GDPR) by “privacy by default” and “privacy by design”.

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 6

Cosa si intende per firma elettronica e quali sono le principali finalità, ci sono differenze con la firma digitale? Quali altre tipologie di firme elettroniche conosce?

What is the difference between the Internet and a local network (LAN)?

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 7

L'infermiera della casa di Comunità di Ponte di Legno esegue l'elettrocardiogramma ai pazienti mentre il medico compila il referto dal proprio reparto di Cardiologia dell'ospedale di Esine. Si descrivano le caratteristiche necessarie dell'apparecchiatura e le infrastrutture necessarie per poter svolgere quest'attività di telerefertazione.

Can you explain what an IP address is and the difference between IPv4 and IPv6?

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 8

In Blocco Operatorio si rende necessario l'acquisto di una colonna artroscopica per la sala di ortopedia così da permettere la registrazione di video in alta risoluzione e la loro conservazione a PACS. Considerando che l'apparecchiatura non viene sempre utilizzata nella stessa sala, si valuti la connessione LAN o WIFI e si illustrino i sistemi possibili per la conservazione dei video.

What is virtualization, and what are its main advantages in an IT environment?

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 9

Che differenze fondamentali può individuare in un sistema informativo ospedaliero rispetto ad un sistema informativo di un'azienda non sanitaria?

What is a firewall, and how does it help protect a network?

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 10

Si riceve una segnalazione dal reparto di cardiologia poiché un medico non riesce a inviare le immagini dell'ecografo al PACS aziendale. Quali sono i controlli che farebbe per un'analisi iniziale?

What is encryption, and why is it important for data security?

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 11

In Azienda, si deve informatizzare un Servizio Ospedaliero (es. Cardiologia). E' quindi necessario prevedere tutte le necessarie integrazioni con il Sistema Informativo Esistente (Anagrafica Pazienti centralizzata, Sistemi di Prenotazione delle prestazioni, PACS, Cartella Clinica etc.)

Il candidato proponga diverse modalità/tecnologie per la realizzazione di tali integrazioni e ne analizzi i relativi pro e contro.

What is system redundancy, and why is it important for ensuring service availability?

**CONCORSO PUBBLICO, PER TITOLI ED ESAMI, PER LA COPERTURA DI N.1 POSTO DI
PERSONALE DELL'AREA DEI PROFESSIONISTI DELLA SALUTE E DEI FUNZIONARI -
PROFILO PROFESSIONALE DEL RUOLO TECNICO - COLLABORATORE TECNICO
PROFESSIONALE – INFORMATICO**

PROVA ORALE N. 12

I sistemi informativi aziendali ricevono una comunicazione via email da un mittente sconosciuto indicante semplicemente “Siamo riusciti a penetrare nei vostri sistemi informatici, in allegato un referto recuperato dai vostri sistemi, contattateci immediatamente alla mail 1234_6543@gmail.com per avere informazioni su come impedire la diffusione di 3.2 Terabyte di informazioni che abbiamo esfoliato dai vostri sistemi”. Verificato che il referto è reale ed effettivamente emesso dalla ASST di cui è dipendente, come procede?

What is the difference between structured and unstructured data? Can you give examples?