CONCORSO PUBBLICO per titoli ed esami
per la copertura a tempo indeterminato e tempo pieno di n. 1 posto di
COLLABORATORE TECNICO PROFESSIONALE-INGEGNERE per la SS Ingegneria Clinica
(scaduto in data 18/04/2024 – espletato il 18/09/2024)
assolvimento obbligo aziendale di pubblicazione
ai sensi dell'art. 19 del d.lgs. 33/2013 come modificato dal d.lgs. 97/2016

TRACCE PROVA SCRITTA

PROVA 1

1. La gestione delle vulnerabilità in una rete aziendale prevede:
    A) Solo l'utilizzo di antivirus aggiornati
    B) Analisi periodica con vulnerability assessment e patch management
    C) Criticità gestita esclusivamente tramite firewall
    D) Disabilitazione delle porte USB

2. La sicurezza delle API (Application Programming Interface) si garantisce principalmente mediante:
    A) Pubblicazione della documentazione solo su siti protetti
    B) Implementazione di autenticazione, autorizzazione e rate limiting
    C) Accesso tramite protocolli FTP
    D) Compressione dei dati trasmessi

3. Un attacco di tipo "zero-day" si riferisce a:
    A) Un attacco che sfrutta una vulnerabilità appena scoperta senza patch disponibili
    B) Un attacco lanciato solo da botnet
    C) Un attacco contro sistemi con antivirus scaduto
    D) Una prova di penetrazione programmata

4. Quale tra i seguenti protocolli implementa la forward secrecy per le sessioni cifrate?
    A) TLS con Diffie-Hellman ephemeral (DHE)
    B) HTTP
    C) FTP
    D) POP3

5. In un modello di database relazionale, cosa rappresenta una "chiave primaria"?
    A) Una colonna che può essere nulla
    B) Un identificativo univoco per ogni record in una tabella
    C) Una tabella temporanea
    D) Un campo di testo senza vincoli

6. Se un indirizzo IPv4 è 192.168.1.100/24, qual è il range degli indirizzi IP disponibili nella stessa subnet?
    A) 192.168.1.1 – 192.168.1.254
    B) 192.168.0.1 – 192.168.0.254
    C) 192.168.1.0 – 192.168.1.255
    D) 192.168.1.100 – 192.168.1.200
    E) 192.168.1.1 – 192.168.1.254

7. In base al GDPR, in quale caso si può trattare un dato personale senza consenso esplicito dell'interessato?
    A) Sempre, se si tratta di dati pseudonimizzati
    B) Se esiste un interesse legittimo superiore e documentato
    C) Solo per finalità di marketing
    D) Se i dati sono raccolti tramite cookie tecnici

8. Il DPO può rivestire anche il ruolo di responsabile IT nell'ente pubblico?
    A) No, per evitare conflitti di interesse
    B) Sì, sempre
    C) Solo nelle aziende private
    D) Sì, a condizione che non tratti dati

ù

9. Quale dei seguenti è un esempio di Data Protection Impact Assessment (DPIA) obbligatorio?
    A) Trattamento su larga scala di categorie particolari di dati
    B) Blocco temporaneo di un account utente
    C) Gestione delle ferie del personale
    D) Archiviazione di dati pubblici

10. Se un data breach comporta un rischio elevato per i diritti e le libertà degli interessati:
    A) È sufficiente notificare solo l'autorità competente
    B) Devono essere informati sia l'autorità che gli interessati
    C) Nessuna comunicazione è obbligatoria
    D) Solo la direzione dell'azienda va informata

11. La direttiva NIS2 introduce quale obbligo aggiuntivo rispetto alla NIS1?
    A) Reporting degli incidenti di sicurezza entro 24 ore
    B) Solo formazione facoltativa
    C) Esclusione degli operatori digitali
    D) Nessun obbligo ulteriore

12. Nel contesto NIS2, cosa si intende per “risk management”?
    A) Valutazione, mitigazione e monitoraggio continuo dei rischi di sicurezza
    B) Solo la redazione di policy interne
    C) Gestione esclusiva degli asset hardware
    D) Audit annuale dei bilanci

13. In caso di incidente rilevante, la NIS2 obbliga le organizzazioni a:
    A) Informare esclusivamente le autorità nazionali
    B) Attivare tempestivamente le procedure di risposta e comunicare ad ACN e CSIRT
    C) Non comunicare l’evento

14. Nel ciclo di vita di un documento informatico nella PA, quale processo segue la classificazione e precede la conservazione?
    A) Fascicolazione
    B) Cancellazione
    C) Scansione
    D) Stampa

15. La gestione documentale digitale deve essere conforme a quale normativa, oltre al CAD?
    A) Regolamento eIDAS
    B) Codice Civile
    C) Legge sulla stampa
    D) DPCM 3 dicembre 2013

16. Domanda: Quale tra i seguenti protocolli di rete opera al livello di trasporto del modello OSI ed è responsabile della trasmissione affidabile dei dati tra host?
    A) UDP
    B) TCP
    C) IP
    D) ICMP

17. Quale tra i seguenti livelli del modello OSI è responsabile della segmentazione e riassemblaggio dei dati?

A) Livello di rete
B) Livello di trasporto
C) Livello di presentazione
D) Livello fisico

18. Quale tra le seguenti tipologie di firma elettronica è considerata equivalente, ai fini di legge, alla firma autografa secondo il Codice dell'Amministrazione Digitale?

A) Firma elettronica semplice
B) Firma elettronica avanzata
C) Firma elettronica qualificata
D) Firma digitale

19. Ai sensi del Codice dell'Amministrazione Digitale, la firma digitale si basa su:

A) Un codice segreto condiviso tra le parti
B) Un sistema di cifratura simmetrica
C) Un sistema di chiavi crittografiche asimmetriche
D) Una password personale

20. Quale tra queste tipologie di dati non deve essere normalmente inclusa nel FSE secondo la normativa italiana vigente?

A) Dati amministrativi di residenza
B) Referti di laboratorio
C) Prescrizioni specialistiche
D) Consensi informati sanitari

21. Secondo il Regolamento UE 2016/679 (GDPR), quale principio deve essere applicato nella gestione del FSE per garantire la privacy del cittadino?

A) Minimizzazione dei dati
B) Detenzione illimitata delle informazioni
C) Accesso libero a tutti i professionisti sanitari
D) Indicizzazione pubblica dei dati

22. Quale standard internazionale viene comunemente adottato per garantire la corretta codifica e lo scambio strutturato di informazioni sanitarie all'interno del FSE?

A) HL7 FHIR
B) PDF/A
C) JPEG
D) ZIP

23. Quale delle seguenti opzioni esprime in modo più accurato una delle innovazioni introdotte dal FSE2.0 rispetto alle versioni precedenti del Fascicolo Sanitario Elettronico?

A) Il FSE2.0 introduce un nuovo sistema di archiviazione esclusivamente per immagini diagnostiche in formato JPEG.

B) Il FSE2.0 consente l'integrazione strutturata e interoperabile dei dati sanitari a livello nazionale, promuovendo la condivisione sicura delle informazioni tra professioniste e professionisti della salute e cittadine e cittadini.

C) Il FSE2.0 limita l'accesso ai dati sanitari soltanto alle strutture di ricovero locale.

D) Il FSE2.0 è progettato specificamente per la conversione di referti clinici in formato ZIP o PDF/A.

24. Il Sistema Pubblico di Identità Digitale (SPID) prevede diversi livelli di sicurezza per l'autenticazione dell'utente. Quale delle seguenti affermazioni descrive correttamente i tre livelli di autenticazione previsti da SPID?

Opzioni di risposta:
A.
Livello 1: accesso con nome utente e password;
Livello 2: accesso con nome utente, password e codice temporaneo (OTP);
Livello 3: accesso con nome utente, password e dispositivo crittografico per la firma digitale o smart card.
B.
Livello 1: autenticazione via email;
Livello 2: autenticazione con OTP;
Livello 3: autenticazione con riconoscimento facciale.
C.
Livello 1: autenticazione tramite CIE;
Livello 2: autenticazione tramite CNS;
Livello 3: autenticazione tramite passaporto elettronico.
D.
Livello 1: accesso con codice fiscale;
Livello 2: accesso con codice fiscale e OTP;
Livello 3: accesso solo da postazione certificata.

25. Nel contesto dei sistemi informativi sanitari, quale tra le seguenti affermazioni descrive correttamente la differenza principale tra il Dossier Sanitario e il Fascicolo Sanitario Elettronico (FSE)?

A) Il Dossier Sanitario raccoglie i dati e i documenti prodotti da diverse strutture sanitarie che hanno preso in carico il paziente, mentre il Fascicolo Sanitario Elettronico contiene solo i dati amministrativi del cittadino.

B) Il Dossier Sanitario è un sistema nazionale obbligatorio per tutti i cittadini, mentre il Fascicolo Sanitario Elettronico è facoltativo e gestito dalle singole strutture sanitarie.

C) Il Dossier Sanitario è gestito e consultabile solo all'interno di una singola Azienda Sanitaria o Ospedaliera per finalità di cura, mentre il Fascicolo Sanitario Elettronico è uno strumento

regionale/nazionale che raccoglie informazioni sanitarie provenienti da più enti e può essere consultato anche a fini di prevenzione, ricerca e governo del sistema sanitario.

D) Il Dossier Sanitario e il Fascicolo Sanitario Elettronico sono sinonimi e indicano lo stesso sistema di archiviazione dei dati clinici del cittadino.

26. In un sistema informativo aziendale ospedaliero integrato, quale tra le seguenti affermazioni descrive correttamente la funzione principale del sistema informativo ospedaliero (SIO) rispetto agli altri moduli applicativi?

A) Il SIO si occupa esclusivamente della gestione contabile e amministrativa delle risorse economiche dell'ospedale.

B) Il SIO integra e coordina i diversi sottosistemi clinici, amministrativi e diagnostici dell'ospedale (ad esempio EMR, LIS, RIS/PACS, CUP), garantendo la condivisione e la coerenza dei dati tra le varie aree operative.

C) Il SIO è un modulo specifico dedicato alla gestione del magazzino farmaceutico e dei dispositivi medici.

D) Il SIO è utilizzato unicamente per la trasmissione dei dati al Ministero della Salute e non interagisce con gli altri sistemi aziendali.

27. Nel contesto della gestione della sicurezza e della resilienza dei sistemi informativi aziendali, quale tra le seguenti affermazioni descrive correttamente la differenza tra Business Continuity e Disaster Recovery?

A) La Business Continuity si concentra sul ripristino dei sistemi informatici dopo un guasto, mentre il Disaster Recovery garantisce la continuità dei processi aziendali durante l'emergenza.

B) La Business Continuity comprende le strategie e le misure per assicurare la continuità dei processi aziendali critici, anche in caso di eventi gravi, mentre il Disaster Recovery riguarda in modo più specifico il ripristino dell'infrastruttura IT e dei dati dopo un'interruzione.

C) Il Disaster Recovery è un piano alternativo per la gestione del personale in caso di disastro, mentre la Business Continuity è limitata ai servizi informatici.

D) Non esiste alcuna differenza: Business Continuity e Disaster Recovery sono due termini equivalenti che indicano lo stesso tipo di procedura di emergenza.

28. Nel contesto delle reti informatiche, quale tra le seguenti affermazioni descrive correttamente la differenza principale tra OSPF e Spanning Tree Protocol (STP)?

A) OSPF è un protocollo di routing che opera a livello 3 (rete) e determina il percorso ottimale tra reti IP, mentre lo Spanning Tree Protocol opera a livello 2 (collegamento dati) e previene la formazione di loop nelle topologie Ethernet commutate.

B) Entrambi sono protocolli di routing di livello 3 utilizzati per calcolare i percorsi IP in reti diverse.
C) OSPF viene utilizzato nei dispositivi di rete wireless, mentre lo Spanning Tree Protocol è impiegato esclusivamente nelle reti WAN.
D) OSPF e Spanning Tree Protocol svolgono la stessa funzione, ma sono prodotti da vendor differenti (Cisco e IEEE, rispettivamente).

29. Quale tra le seguenti affermazioni descrive correttamente le caratteristiche distintive dei linguaggi di programmazione strutturati rispetto ad altri paradigmi di programmazione?

A) I linguaggi strutturati si basano sull'uso esclusivo di funzioni ricorsive e sull'eliminazione totale delle variabili globali.
B) I linguaggi strutturati si fondano sul principio di eseguire istruzioni in sequenza e sull'uso controllato di strutture di controllo (sequenza, selezione e iterazione), favorendo la chiarezza e la modularità del codice.
C) I linguaggi strutturati non prevedono alcuna forma di suddivisione in moduli o funzioni e fanno uso esteso di salti condizionali (istruzioni goto).
D) I linguaggi strutturati sono sinonimo di linguaggi orientati agli oggetti e si basano esclusivamente sul concetto di classe ed ereditarietà.

30. Nel campo dell'Intelligenza Artificiale (AI), quale tra le seguenti affermazioni descrive correttamente la differenza tra le principali tipologie di AI: debole, forte e generale?

A) L'AI debole è in grado di replicare completamente l'intelligenza umana, mentre l'AI forte si limita a eseguire compiti specifici senza apprendimento autonomo.
B) L'AI generale è una forma di intelligenza artificiale priva di capacità di apprendimento, mentre l'AI debole e quella forte si basano esclusivamente su reti neurali profonde.
C) L'AI debole (o ristretta) è progettata per svolgere compiti specifici (es. riconoscimento vocale, analisi immagini), l'AI forte mira a replicare il ragionamento e la consapevolezza umana, mentre l'AI generale rappresenta un livello teorico in cui la macchina può apprendere e adattarsi come un essere umano in qualunque dominio.
D) L'AI debole utilizza algoritmi basati su regole fisse, mentre l'AI forte e generale sono esclusivamente forme di intelligenza artificiale quantistica.

PROVA 2

1. Quale tra le seguenti azioni rappresenta una corretta gestione delle vulnerabilità aziendali?
   A. Soltanto l'aggiornamento dei sistemi operativi
   B. Monitoraggio continuo, analisi delle vulnerabilità e applicazione delle patch
   C. Blocco degli accessi VPN
   D. Cambiare periodicamente la password del Wi-Fi

2. Per proteggere efficacemente le API aziendali è necessario:
   A. Affidarsi solo a connessioni HTTP
   B. Utilizzare autenticazione forte e controlli di autorizzazione
   C. Condividere liberamente la documentazione
   D. Limitare il traffico solo a reti pubbliche

3. Un attacco "zero-click" si verifica quando:
   A. L'utente clicca su un link infetto
   B. Una vulnerabilità viene sfruttata senza interazione dell'utente
   C. Un antivirus elimina un virus
   D. Il sistema aggiorna i driver

4. Quale tra i seguenti protocolli garantisce la "perfect forward secrecy"?
   A. SMTP
   B. Telnet
   C. TLS con ECDHE
   D. IMAP

5. In un database relazionale, la chiave esterna serve a:
   A. Garantire l'unicità dei record
   B. Collegare dati tra tabelle diverse
   C. Definire la struttura della tabella
   D. Consentire valori nulli in una colonna

6. Se un indirizzo IPv4 è 10.0.0.50/16, il range di indirizzi disponibili è:
   A. 10.0.0.1 – 10.0.255.254
   B. 10.0.0.1 – 10.0.0.254
   C. 10.0.0.50 – 10.0.1.254
   D. 10.0.0.1 – 10.0.0.100

7. Secondo il GDPR, il trattamento dei dati personali senza consenso è lecito:
    A. Solo con dati anonimi
    B. Per obblighi di legge o contratto
    C. Quando i dati sono pubblici
    D. Mai

8. Il Data Protection Officer (DPO) può:
    A. Svolgere funzioni di marketing
    B. Essere consulente esterno
    C. Gestire direttamente dati dei dipendenti
    D. Redigere i contratti di lavoro

9. Un trattamento che richiede DPIA è:
    A. Invio di newsletter
    B. Monitoraggio video di spazi pubblici
    C. Gestione badge parcheggi
    D. Conservazione dati anonimi

10. In caso di data breach senza rischi per gli interessati:
    A. Notifica solo al garante
    B. Nessuna notifica necessaria
    C. Informare tutti i clienti
    D. Comunicare alla stampa

11. La direttiva NIS2 introduce:
    A. Gestione facoltativa della sicurezza
    B. Solo monitoraggio volontario
    C. Estensione obblighi a nuovi settori
    D. Eliminazione del reporting incidenti

12. Il “risk assessment” nella NIS2 consiste in:
    A. Installare un firewall
    B. Redigere il bilancio
    C. Gestire backup
    D. Valutare regolarmente minacce e rischi

13. In caso di incidente informatico grave le aziende devono:
    A. Limitarsi ad analisi interna
    B. Informare solo i dipendenti
    C. Attivare risposta e segnalare agli organismi
    D. Attendere istruzioni dal cloud

14. Nel ciclo di vita del documento informatico nella PA, tra fascicolazione e conservazione troviamo:
    A. Protocollo
    B. Scansione
    C. Approvazione
    D. Distruzione

15. La gestione digitale dei documenti nella PA deve rispettare:
    A. Solo il DPCM 22/2/2016
    B. Il Regolamento eIDAS e Linee Guida AgID
    C. Il Testo Unico Bancario
    D. ISO 9001

16. Quale protocollo di rete opera al livello applicazione OSI?
    A. TCP
    B. IP
    C. HTTP
    D. ARP

17. Nel contesto delle reti informatiche, quale tra le seguenti affermazioni descrive correttamente la differenza principale tra OSPF e Spanning Tree Protocol (STP)?
    A. OSPF è un protocollo di routing che opera a livello 3 (rete) e determina il percorso ottimale tra reti IP, mentre lo Spanning Tree Protocol opera a livello 2 (collegamento dati) e previene la formazione di loop nelle topologie Ethernet commutate.
    B. Entrambi sono protocolli di routing di livello 3 utilizzati per calcolare i percorsi IP in reti diverse.
    C. OSPF viene utilizzato nei dispositivi di rete wireless, mentre lo Spanning Tree Protocol è impiegato esclusivamente nelle reti WAN.
    D. OSPF e Spanning Tree Protocol svolgono la stessa funzione, ma sono prodotti da vendor differenti (Cisco e IEEE, rispettivamente).

18. La firma elettronica avanzata, per la normativa italiana, è:
    A. Firma che garantisce identificazione e integrità
    B. Scansione della firma autografa
    C. Password temporanea SMS
    D. Codice fiscale digitale

19. La firma digitale, ai sensi del CAD, utilizza:
    A. Chiavi asimmetriche
    B. Crittografia simmetrica
    C. Pin condiviso
    D. QR code

20. Nel Fascicolo Sanitario Elettronico non sono inclusi:
    A. Esami diagnostici
    B. Prescrizioni farmaceutiche
    C. Certificati di vaccinazione
    D. Note personali del medico

21. Secondo il GDPR, la gestione dei dati sanitari nel FSE deve rispettare il principio di:
    A. Rintracciabilità pubblica
    B. Conservazione illimitata
    C. Accessibilità universale
    D. Limitazione della finalità

22. Quale standard internazionale agevola lo scambio di dati sanitari strutturati?
    A. HL7 CDA
    B. GIF
    C. PDF
    D. RAR

23. Il FSE2.0 introduce:
    A. Integrazione/condivisione dati sanitari a livello nazionale
    B. Solo visualizzazione immagini diagnostiche
    C. Accesso limitato alle regioni
    D. Solo referti PDF/A

24. SPID: quale affermazione descrive correttamente i livelli di autenticazione?

A. Livello 1: credenziali base; Livello 2: base + OTP; Livello 3: dispositivo fisico
B. Livello 1: CIE; Livello 2: firma elettronica; Livello 3: CNS
C. Livello 1: e-mail; Livello 2: telefono; Livello 3: riconoscimento vocale
D. Livello 1: codice fiscale; Livello 2: codice fiscale + OTP; Livello 3: terminale certificato

25. Il Dossier Sanitario rispetto al FSE:
    A. Raccoglie dati di più reparti di una struttura, non consultabile a livello nazionale
    B. Include solo dati amministrativi
    C. È obbligatorio per tutti
    D. Non differisce dal FSE

26. Il Sistema Informativo Ospedaliero (SIO):
    A. Coordina i sottosistemi clinici e amministrativi
    B. Gestisce solo magazzino
    C. Si occupa solo della contabilità
    D. Non interagisce con altri sistemi

27. Differenza tra Business Continuity e Disaster Recovery:
    A. La prima mantiene i processi attivi durante emergenze, la seconda recupera IT e dati dopo un blocco
    B. Nessuna differenza
    C. Business Continuity: sicurezza fisica
    D. Disaster Recovery: solo gestione personale

28. Quali sono i principali modelli di servizio offerti dal paradigma cloud e quali sono le differenze fondamentali tra di essi in termini di responsabilità, gestione e applicazioni pratiche?
    A. IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service)
    B. PaaS (Platform as a Service), CaaS (Container as a Service), TaaS (Testing as a Service)
    C. SaaS (Software as a Service), DaaS (Data as a Service), FaaS (Function as a Service)
    D. IaaS (Infrastructure as a Service), NaaS (Network as a Service), PaaS (Platform as a Service)

29. Nel contesto delle reti IP, il Domain Name System (DNS) è essenziale per la risoluzione dei nomi di dominio. Quale delle seguenti affermazioni descrive correttamente il funzionamento completo del DNS, incluse le differenze tra server ricorsivi e autorevoli, nonché i principali record utilizzati?
    A. I server DNS ricorsivi memorizzano permanentemente tutti i record di dominio e rispondono direttamente senza consultare altri server, mentre i server autorevoli contengono solo record temporanei e delegati; i record principali sono A, B e CNAME.
    B. I server DNS ricorsivi ricevono la richiesta di un client e, se non conoscono la risposta, interrogano altri server DNS fino a ottenere il risultato finale; i server autorevoli contengono i record ufficiali di un dominio e rispondono con informazioni definitive. I principali record includono A (IPv4), AAAA (IPv6), MX (posta), CNAME (alias) e NS (name server).
    C. Il DNS funziona esclusivamente in modalità Client-Server senza differenze tra tipologie di server; tutti i record vengono memorizzati localmente sul client.
    D. I server DNS autorevoli risolvono solo richieste interne alla rete locale, mentre i server ricorsivi sono responsabili di generare nuovi indirizzi IP dinamicamente; i record principali sono DHCP, NAT e PTR

30. La Posta Elettronica Certificata (PEC) è uno strumento utilizzato in ambito pubblico e privato per garantire valore legale alle comunicazioni elettroniche. Quale delle seguenti affermazioni descrive correttamente il funzionamento avanzato della PEC, includendo protocolli, firme digitali e interoperabilità tra gestori certificati?

A. La PEC utilizza protocolli standard SMTP e POP3 senza alcuna modifica, non richiede firme digitali e non prevede controlli tra gestori; quindi, non garantisce né integrità né valore legale dei messaggi.
B. La PEC garantisce valore legale tramite ricevute di accettazione e consegna, protocolli SMTP con estensioni PEC, crittografia dei messaggi, firma digitale dei gestori certificati AgID e interoperabilità tra gestori PEC, assicurando tracciabilità e integrità del contenuto.
C. La PEC è una semplice casella e-mail protetta da password, che non utilizza protocolli standardizzati, e le ricevute sono opzionali e non certificate legalmente.
D. La PEC funziona solo tramite webmail fornita dai gestori e non è compatibile con client di posta standard; il valore legale è garantito solo se il mittente invia una copia cartacea.

PROVA 3

1. Quale tra le seguenti azioni rappresenta una corretta gestione delle vulnerabilità aziendali?
    a) Soltanto l'aggiornamento dei sistemi operativi
    b) Monitoraggio continuo, analisi delle vulnerabilità e applicazione delle patch
    c) Blocco degli accessi VPN

d) Cambiare periodicamente la password del Wi-Fi

2. La sicurezza delle API (Application Programming Interface) si garantisce principalmente mediante:
    a) Pubblicazione della documentazione solo su siti protetti
    b) Implementazione di autenticazione, autorizzazione e rate limiting
    c) Accesso tramite protocolli FTP
    d) Compressione dei dati trasmessi

3. Un attacco “zero-click” si verifica quando:
    a) L’utente clicca su un link infetto
    b) Una vulnerabilità viene sfruttata senza interazione dell’utente
    c) Un antivirus elimina un virus
    d) Il sistema aggiorna i driver

4. Quale tra i seguenti protocolli implementa la forward secrecy per le sessioni cifrate?
    a) TLS con Diffie-Hellman ephemeral (DHE)
    b) HTTP
    c) FTP
    d) POP3

5. In un database relazionale, la chiave esterna serve a:
    a) Garantire l’unicità dei record
    b) Collegare dati tra tabelle diverse
    c) Definire la struttura della tabella
    d) Consentire valori nulli in una colonna

6. In base al GDPR, in quale caso si può trattare un dato personale senza consenso esplicito dell’interessato?
    a) Sempre, se si tratta di dati pseudonimizzati
    b) Se esiste un interesse legittimo superiore e documentato
    c) Solo per finalità di marketing
    d) Se i dati sono raccolti tramite cookie tecnici

7. Il Data Protection Officer (DPO) può:
    a) Svolgere funzioni di marketing

b) Essere consulente esterno
c) Gestire direttamente dati dei dipendenti
d) Redigere i contratti di lavoro

8. Quale dei seguenti è un esempio di Data Protection Impact Assessment (DPIA) obbligatorio?
    a) Trattamento su larga scala di categorie particolari di dati
    b) Blocco temporaneo di un account utente
    c) Gestione delle ferie del personale
    d) Archiviazione di dati pubblici

9. La direttiva NIS2 introduce:
    a) Gestione facoltativa della sicurezza
    b) Solo monitoraggio volontario
    c) Estensione obblighi a nuovi settori
    d) Eliminazione del reporting incidenti

10. Nel contesto NIS2, cosa si intende per “risk management”?
    a) Valutazione, mitigazione e monitoraggio continuo dei rischi di sicurezza
    b) Solo la redazione di policy interne
    c) Gestione esclusiva degli asset hardware
    d) Audit annuale dei bilanci

11. Nel ciclo di vita del documento informatico nella PA, tra fascicolazione e conservazione troviamo:
    a) Protocollo
    b) Scansione
    c) Approvazione
    d) Distruzione

12. La gestione documentale digitale deve essere conforme a quale normativa, oltre al CAD?
    a) Regolamento eIDAS
    b) Codice Civile
    c) Legge sulla stampa
    d) DPCM 3 dicembre 2013

13. Quale tra i seguenti protocolli di rete opera al livello applicazione OSI?
    a) TCP
    b) IP

c) HTTP

d) ARP

14. Quale tra le seguenti tipologie di firma elettronica è considerata equivalente, ai fini di legge, alla firma autografa secondo il Codice dell'Amministrazione Digitale?
    a) Firma elettronica semplice
    b) Firma elettronica avanzata
    c) Firma elettronica qualificata
    d) Firma digitale

15. Nel Fascicolo Sanitario Elettronico non sono inclusi:
    a) Esami diagnostici
    b) Prescrizioni farmaceutiche
    c) Certificati di vaccinazione
    d) Note personali del medico

16. Quale standard internazionale viene comunemente adottato per garantire la corretta codifica e lo scambio strutturato di informazioni sanitarie all'interno del FSE?
    a) HL7 FHIR
    b) PDF/A
    c) JPEG
    d) ZIP

17. Il FSE2.0 introduce:
    a) Integrazione/condivisione dati sanitari a livello nazionale
    b) Solo visualizzazione immagini diagnostiche
    c) Accesso limitato alle regioni
    d) Solo referti PDF/A

18. Il Sistema Informativo Ospedaliero (SIO):
    a) Coordina i sottosistemi clinici e amministrativi
    b) Gestisce solo magazzino
    c) Si occupa solo della contabilità
    d) Non interagisce con altri sistemi

19. Nel contesto della gestione della sicurezza e della resilienza dei sistemi informativi aziendali, quale tra le seguenti affermazioni descrive correttamente la differenza tra Business Continuity e Disaster Recovery?

a) La Business Continuity si concentra sul ripristino dei sistemi informatici dopo un guasto, mentre il Disaster Recovery garantisce la continuità dei processi aziendali durante l'emergenza.
b) La Business Continuity comprende le strategie e le misure per assicurare la continuità dei processi aziendali critici, anche in caso di eventi gravi, mentre il Disaster Recovery riguarda in modo più specifico il ripristino dell'infrastruttura IT e dei dati dopo un'interruzione.
c) Il Disaster Recovery è un piano alternativo per la gestione del personale in caso di disastro, mentre la Business Continuity è limitata ai servizi informatici.
d) Non esiste alcuna differenza: Business Continuity e Disaster Recovery sono due termini equivalenti che indicano lo stesso tipo di procedura di emergenza.

20. Un trattamento che richiede DPIA è:
a) Invio di newsletter
b) Monitoraggio video di spazi pubblici
c) Gestione badge parcheggi
d) Conservazione dati anonimi

21. La gestione digitale dei documenti nella PA deve rispettare:
a) Solo il DPCM 22/2/2016
b) Il Regolamento eIDAS e Linee Guida AgID
c) Il Testo Unico Bancario
d) ISO 9001

22. Nel contesto dei sistemi informativi sanitari, quale tra le seguenti affermazioni descrive correttamente la differenza principale tra il Dossier Sanitario e il Fascicolo Sanitario Elettronico (FSE)?
a) Il Dossier Sanitario raccoglie i dati e i documenti prodotti da diverse strutture sanitarie che hanno preso in carico il paziente, mentre il Fascicolo Sanitario Elettronico contiene solo i dati amministrativi del cittadino.
b) Il Dossier Sanitario è un sistema nazionale obbligatorio per tutti i cittadini, mentre il Fascicolo Sanitario Elettronico è facoltativo e gestito dalle singole strutture sanitarie.
c) Il Dossier Sanitario è gestito e consultabile solo all'interno di una singola Azienda Sanitaria o Ospedaliera per finalità di cura, mentre il Fascicolo Sanitario Elettronico è uno strumento regionale/nazionale che raccoglie informazioni sanitarie provenienti da più enti e può essere consultato anche a fini di prevenzione, ricerca e governo del sistema sanitario.
d) Il Dossier Sanitario e il Fascicolo Sanitario Elettronico sono sinonimi e indicano lo stesso sistema di archiviazione dei dati clinici del cittadino.

23. Quale standard internazionale viene comunemente adottato per garantire la corretta codifica e lo scambio strutturato di informazioni sanitarie all'interno del FSE?
    a) HL7 FHIR
    b) PDF/A
    c) JPEG
    d) ZIP

24. Quali sono i principali modelli di servizio offerti dal paradigma cloud e quali sono le differenze fondamentali tra di essi in termini di responsabilità, gestione e applicazioni pratiche?
    a) IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service)
    b) PaaS (Platform as a Service), CaaS (Container as a Service), TaaS (Testing as a Service)
    c) SaaS (Software as a Service), DaaS (Data as a Service), FaaS (Function as a Service)
    d) IaaS (Infrastructure as a Service), NaaS (Network as a Service), PaaS (Platform as a Service)

25. La Posta Elettronica Certificata (PEC) è uno strumento utilizzato in ambito pubblico e privato per garantire valore legale alle comunicazioni elettroniche. Quale delle seguenti affermazioni descrive correttamente il funzionamento avanzato della PEC, includendo protocolli, firme digitali e interoperabilità tra gestori certificati?
    a) La PEC utilizza protocolli standard SMTP e POP3 senza alcuna modifica, non richiede firme digitali e non prevede controlli tra gestori, quindi non garantisce né integrità né valore legale dei messaggi.
    b) La PEC garantisce valore legale tramite ricevute di accettazione e consegna, protocolli SMTP con estensioni PEC, crittografia dei messaggi, firma digitale dei gestori certificati AgID e interoperabilità tra gestori PEC, assicurando tracciabilità e integrità del contenuto.
    c) La PEC è una semplice casella email protetta da password, che non utilizza protocolli standardizzati, e le ricevute sono opzionali e non certificate legalmente.
    d) La PEC funziona solo tramite webmail fornita dai gestori e non è compatibile con client di posta standard; il valore legale è garantito solo se il mittente invia una copia cartacea.

26. Nel contesto delle reti informatiche, quale tra le seguenti affermazioni descrive correttamente la differenza principale tra OSPF e Spanning Tree Protocol (STP)?

    a) OSPF è un protocollo di routing che opera a livello 3 (rete) e determina il percorso ottimale tra reti IP, mentre lo Spanning Tree Protocol opera a livello 2 (collegamento dati) e previene la formazione di loop nelle topologie Ethernet commutate.
    b) Entrambi sono protocolli di routing di livello 3 utilizzati per calcolare i percorsi IP in reti diverse.

c) OSPF viene utilizzato nei dispositivi di rete wireless, mentre lo Spanning Tree Protocol è impiegato esclusivamente nelle reti WAN.
d) OSPF e Spanning Tree Protocol svolgono la stessa funzione, ma sono prodotti da vendor differenti (Cisco e IEEE, rispettivamente).

27. Nel campo dell'Intelligenza Artificiale (AI), quale tra le seguenti affermazioni descrive correttamente la differenza tra le principali tipologie di AI: debole, forte e generale?

a) L'AI debole è in grado di replicare completamente l'intelligenza umana, mentre l'AI forte si limita a eseguire compiti specifici senza apprendimento autonomo.
b) L'AI generale è una forma di intelligenza artificiale priva di capacità di apprendimento, mentre l'AI debole e quella forte si basano esclusivamente su reti neurali profonde.
c) L'AI debole (o ristretta) è progettata per svolgere compiti specifici (es. riconoscimento vocale, analisi immagini), l'AI forte mira a replicare il ragionamento e la consapevolezza umana, mentre l'AI generale rappresenta un livello teorico in cui la macchina può apprendere e adattarsi come un essere umano in qualunque dominio.
d) L'AI debole utilizza algoritmi basati su regole fisse, mentre l'AI forte e generale sono esclusivamente forme di intelligenza artificiale quantistica.

28. Quale tra le seguenti affermazioni descrive correttamente le caratteristiche distintive dei linguaggi di programmazione strutturati rispetto ad altri paradigmi di programmazione?

a) I linguaggi strutturati si basano sull'uso esclusivo di funzioni ricorsive e sull'eliminazione totale delle variabili globali.
b) I linguaggi strutturati si fondano sul principio di eseguire istruzioni in sequenza e sull'uso controllato di strutture di controllo (sequenza, selezione e iterazione), favorendo la chiarezza e la modularità del codice.
c) I linguaggi strutturati non prevedono alcuna forma di suddivisione in moduli o funzioni e fanno uso esteso di salti condizionali (istruzioni goto).
d) I linguaggi strutturati sono sinonimo di linguaggi orientati agli oggetti e si basano esclusivamente sul concetto di classe ed ereditarietà.

29. Quale tra le seguenti affermazioni rappresenta in modo più preciso una caratteristica distintiva del modello Infrastructure as a Service (IaaS) nel cloud computing?

a) L'utente può gestire direttamente macchine virtuali, storage e reti, senza occuparsi della gestione fisica dell'hardware sottostante.
b) L'utente può installare e configurare solo applicazioni software senza alcun controllo sull'infrastruttura sottostante.

c) L'accesso alle risorse cloud è limitato esclusivamente al provider di servizi, che ne controlla ogni aspetto gestionale e operativo.
d) Il modello IaaS consente esclusivamente la condivisione di documenti tra dispositivi locali, senza possibilità di espansione dinamica delle risorse.

30. Quale delle seguenti affermazioni rappresenta in modo più accurato la funzione principale di una VLAN in un contesto di rete aziendale complesso?
a) Una VLAN separa il traffico di rete in base ai protocolli utilizzati dai dispositivi, riducendo così la latenza tra segmenti di rete geograficamente distanti.
b) Una VLAN consente la suddivisione logica di una rete fisica in più domini di broadcast indipendenti, migliorando la gestione delle risorse, la sicurezza e l'efficienza della rete.
c) Una VLAN agisce come firewall hardware, impedendo automaticamente qualsiasi comunicazione tra dispositivi con indirizzi IP diversi all'interno della stessa infrastruttura di rete.
d) Una VLAN è un sistema di distribuzione che ottimizza la ripartizione della banda tra dispositivi wireless e cablati in una rete locale.

TRACCE PROVA PRATICA

Tema n° 1

Il candidato definisca gli elementi principali di un capitolato di gara per l'acquisizione di una soluzione per il Tele monitoraggio di pazienti presso il loro domicilio.

Tema n° 2

Il candidato descriva le differenze e le architetture che sovraintendono a soluzioni tipo SaaS, IaaS e PaaS cercando di identificare quali sono i punti di forza/debolezza di ciascuna di esse.

Tema n° 3

Il candidato descriva un modello di architettura software, organizzata per aree applicative per una sanità digitale; per ogni area si proceda a dare una descrizione delle funzioni necessarie per la gestione dei processi amministrativi e sanitari di un ospedale.

TRACCIA PROVA ORALE

1. Cos'è un DNS e un DNS autoritativo?
2. Cosa significa SPID e quali sono i livelli?
3. Firma digitale: cos'è e come funziona

4. Regolamento EU679/2016, GDPR: Data Breach, cos'è, come va gestito, quali sono gli obblighi normativi.
5. Cos'è una VLAN
6. Business Continuity & Disaster recovery: cosa sono e a cosa servono.
7. Differenza tra spamming e phising
8. Descrivere brevemente quali sono gli aspetti di sicurezza applicativa ed architetturale per una applicazione esposta sul web;

CRITERI DI VALUTAZIONE DELLA COMMISSIONE: Artt. 11,14,20,21,22,23,27 D.P.R. 483/97