

**CONCORSO PER L'ASSUNZIONE DI 4 LAUREATI NELLE DISCIPLINE DELL'ICT
(INFORMATION AND COMMUNICATION TECHNOLOGY) CON CONOSCENZE NELLA
SICUREZZA INFORMATICA O NELLE TECNOLOGIE DEI SISTEMI INFORMATICI
DISTRIBUITI E A REGISTRO DISTRIBUITO E DELL'INTELLIGENZA ARTIFICIALE**

(Bando pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana – 4ª serie speciale “Concorsi ed Esami”
n. 86 del 28 ottobre 2022)

PROVA SCRITTA DEL 27 APRILE 2023

TESTO N. 1

Il candidato scelga una coppia di materie (A e B oppure C e D) e svolga due quesiti, uno per ciascuna materia della coppia prescelta. La traccia di lingua inglese è invece unica.

A. ARCHITETTURE DEI SISTEMI DISTRIBUITI (un quesito a scelta)

Quesito A.1

Un *pattern* architetturale fornisce una descrizione strutturata volta a supportare la progettazione dell'architettura di un sistema *software*. Nel caso specifico dei sistemi distribuiti, l'architettura del sistema viene spesso suddivisa in *layer*. La candidata/il candidato, considerando il *pattern* architetturale *client-server* per l'erogazione di servizi *web*:

- illustri una possibile strutturazione in *layer* delle componenti *server*, descrivendo le funzionalità dei vari livelli, con particolare riferimento alle caratteristiche dello strato *middleware*;
- descriva le soluzioni tecnologiche volte a garantire la tolleranza ai guasti che possono essere adottate nei *layer* descritti al punto precedente.

Si consideri il caso particolare di un servizio di *e-commerce* realizzato mediante un'applicazione *web* che fa uso di un *database* distribuito a livello geografico. La candidata/il candidato:

- descriva sinteticamente le caratteristiche dei *database* distribuiti, illustrando in particolare, con riferimento all'applicazione di *e-commerce* in esame, le problematiche e i vincoli connessi alla disponibilità del servizio e alla consistenza dei dati, anche nei casi di partizionamento del sistema.

Quesito A.2

Nelle moderne organizzazioni si sono affermate, nell'ambito del processo di sviluppo *software*, soluzioni tecnologiche e organizzative per la gestione del ciclo di vita delle applicazioni. La candidata/il candidato:

- descriva il modello organizzativo *DevOps* e i processi di gestione del ciclo di vita di una applicazione che lo rendono possibile; discuta inoltre le problematiche di sicurezza da tenere in considerazione nell'adottare tale modello e le misure da adottare per mitigare i relativi rischi;
- descriva le caratteristiche delle architetture applicative basate su microservizi, illustrandone vantaggi e svantaggi rispetto ad un classico approccio *service-oriented*.

Si consideri il caso di un'applicazione di *e-commerce* per la gestione di spettacoli. L'applicazione fa uso di *web services* per esporre diverse funzionalità (ad es. la ricerca degli eventi, la prenotazione dei posti disponibili, l'acquisto dei biglietti, la gestione del profilo utente). In occasione di particolari eventi, l'applicazione mostra *performance* non adeguate a causa dell'elevato carico di richieste contemporanee. A seguito di un'analisi dell'applicazione, i problemi prestazionali sono stati ricondotti ad alcuni *web*

services che incapsulano blocchi di codice complessi, costruiti per fornire più funzionalità. E' emerso altresì che l'applicazione non è scalabile. La candidata/il candidato:

- descriva possibili approcci per ristrutturare l'applicazione in una logica a microservizi, al fine di migliorare le *performance* e la scalabilità dell'applicazione, evidenziando gli aspetti a cui prestare particolare attenzione durante la reingegnerizzazione del codice.

B. SICUREZZA INFORMATICA (un quesito a scelta)

Quesito B.1

Aziende e Istituzioni sono sempre più spesso oggetto di attacchi *cyber*, che mirano a compromettere la confidenzialità, l'integrità e la disponibilità dei dati e la continuità dei servizi ICT. La candidata/il candidato:

- descriva le fasi tipiche di un attacco *cyber* riferendosi ad almeno un modello di *cyber kill chain*, e indichi utilità e limiti di modelli di questo tipo;
- illustri le caratteristiche di un attacco di tipo *denial of service* (DoS) e ne descriva le possibili tipologie, indicando quali misure tecniche e organizzative possono essere adottate per mitigare il rischio associato ad attacchi di questo genere.

Si consideri un'azienda che vende prodotti esclusivamente *on-line* tramite il suo portale di *e-commerce* e che consente ai dipendenti di lavorare saltuariamente da remoto collegandosi ai sistemi informatici aziendali tramite un servizio di VPN. L'azienda ha ricevuto minacce, da parte di un noto gruppo di cybercriminali, di attacchi di tipo *distributed denial of service* (DDoS) diretti contro i suoi servizi esposti in caso del mancato pagamento di una rilevante somma di denaro. La candidata/il candidato:

- valuti qualitativamente il rischio associato all'attacco sopradescritto, eventualmente riferendosi a una metodologia esistente, e proponga una strategia per la sua gestione. Se necessario, si formulino assunzioni sulle informazioni mancanti.

Quesito B.2

Una delle misure più efficaci per ridurre la superficie di attacco e mitigare il rischio *cyber* consiste nell'esecuzione di *security assessment*, finalizzati a verificare sia l'assetto di sicurezza delle componenti infrastrutturali e applicative, sia l'efficacia dei presidi di sicurezza tecnici e organizzativi. La candidata/il candidato:

- descriva, facendo riferimento ad almeno un *framework* esistente, le finalità e le fasi di un *red team test*, illustrandone le principali differenze rispetto alle attività di *vulnerability assessment* e *penetration testing*;
- discuta l'utilità di affiancare alle attività di *security assessment* un processo di gestione delle vulnerabilità *software* note pubblicamente, descrivendone le principali fasi e illustrandone gli aspetti tecnici e organizzativi;
- indichi, eventualmente facendo riferimento a uno standard esistente, i criteri da utilizzare per quantificare la gravità delle vulnerabilità *software*; illustri, inoltre, come sia possibile mitigare il rischio associato a vulnerabilità gravi prima dell'applicazione delle relative correzioni.

C. PROGRAMMAZIONE, ALGORITMI, STRUTTURE E MODELLI DATI (un quesito a scelta)

Quesito C.1

Per superare le difficoltà di progettazione di una base di dati, ci si avvale di una metodologia che articola il processo in fasi. In una prima fase, detta progettazione concettuale, i dati sono descritti attraverso uno schema concettuale, espresso con un modello dei dati indipendente dal sistema di gestione della base di dati (DBMS) utilizzato nell'implementazione. Segue una fase di progettazione logica, in cui lo schema concettuale viene tradotto in uno schema logico espresso dal modello logico adottato dal DBMS scelto per l'implementazione. La candidata/il candidato:

- descriva un modello concettuale dei dati per la progettazione di una base di dati, illustrandone sia i costrutti che la notazione grafica;
- utilizzando il modello descritto nel punto precedente, produca uno schema concettuale della base di dati per la gestione dei corsi professionali offerti da un ente di formazione, secondo le seguenti specifiche:
 1. di ogni corso interessa il codice identificativo, il nome, il numero di lezioni, gli eventuali corsi propedeutici;
 2. per ogni corso si tengono più edizioni. Ogni edizione ha un numero che la identifica tra le edizioni dello stesso corso, una data di inizio e una data di fine, un docente;
 3. i docenti hanno codice fiscale, nome, cognome, *email*, data e comune di nascita;
 4. ogni edizione si articola in più lezioni; ogni lezione ha una data che la identifica nell'ambito delle lezioni dell'edizione, un'ora di inizio, una durata e una descrizione;
 5. le edizioni di un corso si possono tenere *online* oppure in presenza. Per le edizioni *online* interessa la piattaforma di *e-learning* utilizzata; per le edizioni in presenza interessa il numero massimo di allievi ammessi, l'indirizzo e il nome dell'aula in cui si tiene la lezione.
- supponendo che si sia scelto di utilizzare un DBMS relazionale, a partire dallo schema concettuale sviluppato nel punto precedente, produca uno schema logico (relazionale), avendo cura di specificare anche i vincoli volti a garantire l'integrità dei dati.

Quesito C.2

Per la progettazione della componente server di una applicazione *web* solitamente viene adottato il *pattern Model View Controller (MVC)*; l'implementazione si presta facilmente ad essere realizzata con linguaggi di programmazione orientata agli oggetti (ad esempio, Java o C#), mentre la persistenza dei dati è spesso affidata ad un DBMS relazionale. La candidata/il candidato:

- descriva i componenti del *pattern MVC* e le loro interazioni, facendo anche riferimento a tecnologie e *framework* comunemente utilizzati nella pratica nel contesto delle applicazioni *web*.

Il modello relazionale non è adatto a memorizzare direttamente gli oggetti; ciò dà origine ad un problema noto come disaccoppiamento di impedenza oggetti-relazioni (*object-relational impedance mismatch*). La candidata/il candidato:

- discuta le principali difficoltà concettuali e tecnologiche che danno origine al problema, e descriva le soluzioni tecnologiche generalmente adottate per risolverlo.

Un'applicazione *web* è naturalmente esposta ad attacchi cyber. La candidata/il candidato:

- descriva, anche attraverso esempi concreti, la vulnerabilità XSS (*Cross-Site Scripting*) e illustri le contromisure da adottare in fase di progettazione e sviluppo del codice.

D. DISTRIBUTED LEDGER TECHNOLOGY E INTELLIGENZA ARTIFICIALE (un quesito a scelta)

Quesito D.1

Nelle *Distributed Ledger Technologies* (DLT), dove molteplici partecipanti (o nodi) mantengono una replica locale del *ledger*, i nodi validatori svolgono un ruolo importante per mantenere una visione consistente del *ledger* condiviso. La *blockchain* è una particolare DLT nella quale i dati sono organizzati in blocchi concatenati in maniera crittograficamente sicura. Considerate le DLT di tipo *blockchain*, la candidata/il candidato:

- definisca in cosa consiste il ruolo di validatore della rete e descriva i processi di validazione di una transazione e di un blocco;
- illustri almeno due meccanismi di consenso utilizzati nelle reti *blockchain*, descrivendone le caratteristiche principali; in tale contesto si analizzi il rischio del *double spending* descrivendo le possibili misure di mitigazione;
- discuta l'applicazione dei meccanismi di consenso sulla base della tipologia della rete *blockchain* facendo riferimento al concetto di natura probabilistica o deterministica di tali meccanismi; si descriva inoltre la differenza tra un *fork* temporaneo (o accidentale), un *soft fork* e un *hard fork* eventualmente facendo riferimento a casi reali.

Quesito D.2

Con *machine learning* si intende un'area dell'intelligenza artificiale costituita da algoritmi che apprendono sulla base dell'osservazione empirica dei dati mediante un processo di generalizzazione. Facendo riferimento ai processi di apprendimento, si distinguono approcci supervisionati, non supervisionati e di rinforzo (*reinforcement learning*). La candidata/il candidato:

- descriva le tecniche di apprendimento supervisionato e, in tale ambito, illustri cosa si intende per problemi di regressione e classificazione;
- considerando un problema di classificazione binaria, fornisca una definizione di modello basato su reti neurali;
- per il modello basato su reti neurali, definisca cosa si intende per funzione di attivazione e livelli (o *layer*) di una rete neurale distinguendo tra reti neurali *single-layer* e *multi-layer*; per tali reti si illustrino gli ambiti di applicazione, le caratteristiche e i limiti, il processo di addestramento; fornisca la descrizione di due metriche di qualità per i modelli basati su reti neurali;
- descriva il rischio di *bias* per un modello di classificazione, esemplificando i potenziali impatti; fornisca quindi almeno un esempio delle possibili misure di mitigazione.

TRACCIA DI LINGUA INGLESE

As result of the pandemic, many companies have adopted forms of hybrid working (mixing remote working and working in the office). Discuss the advantages and disadvantages of this type of work.