**SELEZIONE PUBBLICA PER ESAMI PER L'ASSUNZIONE A TEMPO INDETERMINATO DI N. 1 "ISTRUTTORE DIRETTIVO TECNICO" (INFORMATICO SISTEMISTA) – Area dei Funzionari e dell'E.Q da assegnare alla Direzione Generale – U.O. Sistemi Informativi, Territoriali ed Informatici**

## CRITERI DI VALUTAZIONE DELLA PROVA ORALE

In ottemperanza a quanto disposto dall'art. 19 del D. Lgs. del 14/3/2013 n. 33 viene di seguito riportato lo stralcio del verbale della selezione contenente i criteri di valutazione della prova orale sostenuta dai candidati il giorno **3 ottobre 2025**.

La Commissione ha definito i seguenti criteri di valutazione dei quesiti contenuti nella **prova estratta B**, suddividendo i 30 punti a disposizione come segue:

Massimo 27 punti alle domande a contenuto tecnico-professionale e alla prova pratica e precisamente articolati in:

* *due domande di contenuto tecnico-professionale* che saranno diverse nelle tre tracce e relative alle tematiche indicate nel bando di selezione in materia di sistemi informativi, del valore di 9 punti massimo ciascuna;

* *una prova pratico-operativa* del valore anch'essa di massimo 9 punti, che verrà mantenuta uguale nelle tre tracce, tesa a verificare le conoscenze/capacità pratico-operative del candidato in relazione alla configurazione di sistemi e apparati e/o risoluzione di problemi sistemistici per la quale il candidato avrà a disposizione supporti informatici messi a disposizione dal Comune di Ravenna;

Su questa parte la Commissione condivide di esprimere la votazione per la prova pratica e per i quesiti tecnico-professionali utilizzando la scala scolastica da 0 (risposta non data) a 10 (risposta eccellente), riproporzionando quindi in maniera aritmetica le votazioni assegnate in relazione al valore massimo attributo a ciascun quesito/prova pari a 9 punti, secondo i seguenti parametri:

* per i quesiti tecnico-professionali: esposizione sintetica e completa, chiarezza espositiva; capacità di sintesi; correttezza e pertinenza del contenuto rispetto alla domanda; stile linguistico grammaticalmente corretto e adeguato con utilizzo di appropriati termini tecnici;

* per la prova pratico-operativa (uguale in tutte le tracce): correttezza, modalità e tempistica di svolgimento; padronanza/abilità di esecuzione.

E secondo la formula seguente:

$$p = \frac{V \times 9}{10}$$

ove si intende per:

**p:** punteggio riparametrato

**V:** votazione espressa in decimi secondo la scala scolastica

I punteggi di traduzione e ponderazione della sopra riportata scala di valutazione, risultano quindi quelli di cui alla seguente tabella:

| | votazione secondo la scala scolastica punti in /10 | punteggio riparametrato punti in /9 |
|---|---|---|
| Risposta/esecuzione non data | 0 | 0 |
| Risposta/esecuzione gravemente insufficiente | 1 | 0,9 |
| Risposta/esecuzione gravemente insufficiente | 1,5 | 1,35 |
| Risposta/esecuzione gravemente insufficiente | 2 | 1,8 |
| Risposta/esecuzione gravemente insufficiente | 2,5 | 2,25 |
| Risposta/esecuzione gravemente insufficiente | 3 | 2,7 |
| Risposta/esecuzione gravemente insufficiente | 3,5 | 3,15 |

| | votazione secondo la scala scolastica punti in /10 | punteggio riparametrato punti in /9 |
|---|---|---|
| Risposta/esecuzione insufficiente | 4 | 3,6 |
| Risposta/esecuzione insufficiente | 4,5 | 4,05 |
| Risposta/esecuzione insufficiente | 5 | 4,5 |
| Risposta/esecuzione leggermente insufficiente | 5,5 | 4,95 |
| Risposta/esecuzione sufficiente | 6 | 5,4 |
| Risposta/esecuzione più che sufficiente | 6,5 | 5,85 |
| Risposta/esecuzione discreta | 7 | 6,3 |
| Risposta/esecuzione più che discreta | 7,5 | 6,75 |
| Risposta/esecuzione buona | 8 | 7,2 |
| Risposta/esecuzione più che buona | 8,5 | 7,65 |
| Risposta/esecuzione ottima | 9 | 8,1 |
| Risposta/esecuzione più che ottima | 9,5 | 8,55 |
| Risposta/esecuzione eccellente | 10 | 9 |

Massimo 3 punti saranno assegnati all'accertamento della lingua inglese. La Commissione ha scelto di sottoporre al candidato un brano da leggere e tradurre tratto dal testo in lingua inglese del GDPR (Regolamento Europeo sul trattamento dei dati personali), argomento che coniuga sia la conoscenza della lingua richiesta dal bando di selezione che la conoscenza di una materia specialistica i cui contenuti hanno attinenza coi sistemi informativi.

Il punteggio per l'accertamento della conoscenza della lingua inglese (lettura, traduzione e parlato), sarà attribuito secondo la seguente graduazione con particolare valorizzazione della comprensione del testo:

- ✓ da 0 a 1,5 punti in caso di conoscenza insufficiente,
- ✓ da 1,75 a 2 punti in caso di conoscenza da sufficiente a discreta,
- ✓ da 2,25 a 3 punti in caso di conoscenza da buona a ottima,

in relazione a:
- capacità e fluidità di lettura;
- comprensione del testo;
- corrispondenza della traduzione ed utilizzo di terminologia appropriata;
- padronanza dell'inglese parlato.

In relazione alla prova estratta "**B**", si riportano in maniera sintetica e a titolo esemplificativo i contenuti attesi per le risposte dei tre quesiti tecnico-professionali proposti e per la traduzione del brano in inglese:

**DOMANDA N. 1**

*Nell'ambito della conduzione di un datacenter di un ente pubblico, quali sono i principi e le buone pratiche da adottare per la gestione dei backup tenendo conto degli aspetti tecnici e normativi. In particolare descrivere:*

- *le principali tecnologie e metodi di backup*
- *le politiche di retention*
- *le misure di sicurezza da adottare*
- *l'importanza delle metriche RPO (Recovery Point Objective) e RTO (Recovery Time Objective) nella pianificazione.*

- *Differenza tra backup e replica.*

Sintesi dei possibili contenuti attesi:

La gestione dei backup in un ente pubblico è un'attività critica al fine di garantire continuità operativa, integrità dei dati e conformità normativa.

Principali metodi di backup:

- Backup completo: copia integrale di tutti i dati. È il metodo più sicuro, semplice e veloce da ripristinare, ma richiede molto spazio di archiviazione e tempo per l'esecuzione.
- Backup differenziale: dopo il primo backup completo, copia solo i dati che sono cambiati dall'ultimo backup completo. È più veloce del completo, ma il ripristino richiede il backup completo più l'ultimo differenziale. Rappresenta un compromesso tra velocità e spazio.
- Backup incrementale: copia solo i dati che sono cambiati dall'ultimo backup (incrementale o completo). È il più veloce da eseguire e richiede meno spazio, ma il ripristino è più complesso e lento in quanto richiede l'intero "chain" di backup.
- Snapshot: istantanee dello stato del sistema, utili per VM e database. Molto utilizzato prima di effettuare installazioni/aggiornamenti software su virtual machine.

Le tecnologie di backup si sono evolute, superando i tradizionali sistemi a nastro:

- Backup su Disco (Disk-to-Disk): Offre tempi di backup e ripristino rapidi. I dispositivi di storage (es. NAS, SAN) offrono funzionalità avanzate come la deduplicazione e la compressione.
- Backup su Cloud: Consente di archiviare le copie di sicurezza su un'infrastruttura esterna, garantendo una copia off-site senza la necessità di trasportare fisicamente i supporti. È una soluzione flessibile e scalabile, ma richiede una connessione Internet affidabile.

Politiche di retention: le politiche di retention definiscono per quanto tempo e quante copie di backup devono essere conservate.

- Un principio largamente adottato è la regola del 3-2-1: 3 copie dei dati, 2 supporti di archiviazione diversi (es. disco e nastro), 1 copia off-site (in un luogo geograficamente separato). Questa politica riduce drasticamente il rischio di perdita dei dati.
- Per la retention, si possono adottare approcci come la "Grandfather-Father-Son" (GFS), che prevede backup completi mensili (Grandfather), settimanali (Father) e giornalieri (Son), garantendo una copertura a lungo termine.
- Principio GDPR: i dati devono essere conservati solo per il tempo necessario alle finalità del trattamento.
- Linee Guida AgID: definire tempi di conservazione coerenti con obblighi legali e piani di continuità operativa.
- Best practice: retention differenziata per tipologia di dato e nei limiti di legge.
- Documentazione: indicare i tempi nel Registro dei trattamenti e nel Piano di Continuità Operativa.

Misure di sicurezza:

- Crittografia: dati cifrati a riposo e in transito.
- Isolamento dalla Rete: mantenere le copie di backup "offline" o in un ambiente isolato
- Controllo accessi: autenticazione forte, segregazione dei ruoli.
- Backup immutabili (WORM): protezione da ransomware utilizzando soluzioni che rendono i backup non modificabili per un periodo di tempo, prevenendo la loro manomissione o cancellazione.
- Test periodici di restore: obbligatori per garantire efficacia.
- Logging e monitoraggio: per rilevare anomalie e incidenti

Importanza di RPO e RTO:

- RPO (Recovery Point Objective): rappresenta la quantità massima di dati (misurata in tempo) che si è disposti a perdere in caso di disastro. Un RPO di 24 ore significa che si accetta di perdere un giorno di dati. Per i servizi critici, l'RPO deve essere il più vicino possibile allo zero.
- RTO (Recovery Time Objective): rappresenta il tempo massimo entro cui un servizio deve essere ripristinato e tornare operativo dopo un disastro. Per i servizi essenziali, l'RTO deve essere estremamente basso (es. poche ore).

La definizione di RPO e RTO è il primo passo per progettare una strategia di backup e ripristino, poiché stabilisce i requisiti di performance e costo delle soluzioni da adottare.

Differenza tra backup e replica

- Backup: copia dei dati in un determinato istante di tempo per ripristino in caso di perdita; orientato alla protezione storica. È la soluzione ideale per il recupero di dati corrotti o cancellati accidentalmente. I backup sono storici e possono essere conservati per lunghi periodi.
- Replica: duplicazione in tempo reale o quasi (fino a poche ore), per garantire continuità (es. cluster geografico).
- Uso combinato: replica per alta disponibilità, backup per protezione da corruzione o ransomware.

**DOMANDA N. 2**

*Argomento: VPN*

1. *Cosa significa l'acronimo VPN?*
2. *Qual è lo scopo principale di una VPN?*
3. *Quali sono due tipi principali di VPN (in base alla tecnologia usata)?*
4. *Che differenza c'è tra VPN site-to-site e VPN remote access? Quali tecnologie si usano tipicamente nei due casi?*

Sintesi dei possibili contenuti attesi:

1. Virtual Private Network.
2. Creare un canale sicuro e privato su una rete pubblica (es. Internet).
3. VPN basata su IPsec e VPN basata su SSL/TLS.
4. Site-to-site collega reti aziendali; remote access collega singoli utenti remoti a una rete. Site to site: IPSEC (tunnel mode); remote access: SSL/TLS VPN, OpenVPN, Wireguard.

**READ AND TRANSLATE**

*TOPIC FROM GDPR*

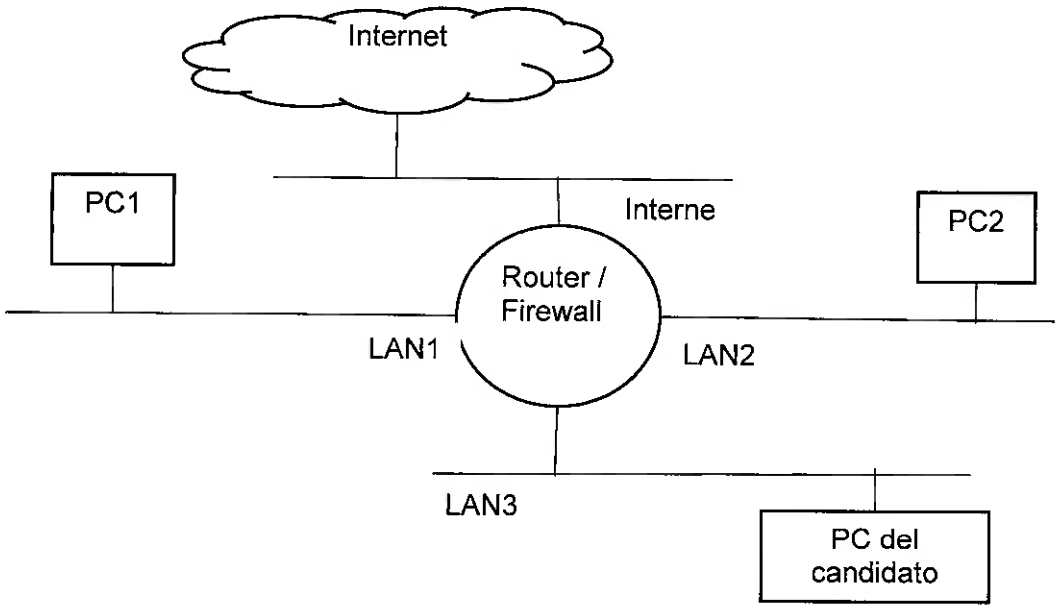
*Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.*

Traduzione:

Il testo riproduce la Premessa n. 6 agli articoli del GDPR. La seguente traduzione è tratta dalla versione italiana del GDPR pubblicata sul portale EUR-Lex dell'Unione Europea:

La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

**PROVA PRATICA – da risolvere secondo le seguenti istruzioni:**




Un sistemista distratto ha configurato il PC1, il PC2 e il firewall per permettere ai due PC la navigazione in Internet, ma ha commesso alcuni errori. Nel sistema sono presenti un DHCP server (integrato nel router/firewall e configurato sulle sole interfacce LAN2 e LAN3 del PC del candidato) e alcune regole di firewalling. Sapendo che le policy di firewalling (menu "Policy & Objects" -> "IPv4 Policy" nella console di configurazione del firewall) hanno **al più** 1 (un) errore ciascuno, e che ci sono altri errori di configurazione di rete su PC1 e PC2, trovare gli errori e correggerli in modo da far sì che:

- PC1 e PC2 siano configurati correttamente in rete (verifica tramite ping al rispettivo default gateway);
- PC1 sia raggiungibile in rete da PC2 (verifica tramite ping o altro tool);
- PC1 e PC2 possano navigare in Internet (verifica su entrambi i PC mediante accesso a un sito web qualunque).

Configurazione dei dispositivi:

| PC/Dispositivo | Networking | Credenziali |
|---|---|---|
| PC1<br>(Windows 10) | Rete: LAN1<br>IP: 192.168.1.100<br>SM: 255.255.255.0<br>GW: 192.168.1.254<br>DNS: 8.8.8.8, 8.8.4.4 | Username: Utente1<br>Password: Password1 |
| PC2<br>(Windows 10) | Rete: LAN2<br>IP: DHCP client (rete 192.168.2.0/24) | Username: Utente1<br>Password: Password1 |
| PC del candidato<br>(Windows 11) | Rete: LAN3<br>IP: DHCP client (rete 192.168.3.0/24) | Username: Utente1<br>Password: Password1 |
| Router/Firewall<br>(Fortigate) | LAN1 IP: 192.168.1.254/24<br>LAN2 IP: 192.168.2.254/24 + DHCP server<br>LAN3 IP: 192.168.3.254/24+ DHCP server<br>Internet IP: DHCP client | Username: admin<br>Password: Password1 |

SOLUZIONE:

La piccola rete rappresentata nello schema precedente è formata da:

- PC del candidato, all'interno del quale è installato un software di virtualizzazione;
- due macchine virtuali Windows 10, PC1 e PC2, installate nel sistema di virtualizzazione;
- un firewall Fortigate 60E;
- un router 4G con porta LAN (coincidente in figura con la nuvoletta "Internet") che garantisce l'accesso a Internet.

Il PC del candidato dispone di 3 schede di rete: una dedicata al PC del candidato stesso per l'accesso a LAN3, le altre due dedicate a PC1 e PC2 per l'accesso a LAN1 e LAN2 rispettivamente. Le schede di rete sono collegate fisicamente mediante cavo UTP cat.6 alle interfacce internal1 (PC1), internal2 (PC2), internal3 (PC del candidato) del firewall. L'interfaccia LAN del router 4G è collegata all'interfaccia wan1 del firewall.

Il candidato ha a disposizione il PC del candidato e gli strumenti standard presenti a bordo di Windows (browser Internet, cmd, ecc) per risolvere la prova pratica.

Nell'esercizio proposto sono presenti i seguenti errori:
1. Il PC1 è configurato in DHCP invece che con IP statico;
2. Il PC2 è configurato con IP statico e con valori non corrispondenti alla rete in cui è inserito;
3. La regola che permette la navigazione di PC1 (LAN1) ha il NAT disabilitato;
4. La regola che permette la raggiungibilità da PC1 (LAN1) a PC2 (LAN2) è disabilitata;
5. La regola che permette la navigazione di PC2 (LAN2) ha "NONE" come destinazione;
6. La regola che permette la raggiungibilità da PC2 (LAN2) a PC1 (LAN1) ha come Action "DENY".

| ID | Name | Source | Destination | Schedule | Service | Action | NAT |
|---|---|---|---|---|---|---|---|
| LAN1 - PC1 (internal1) → Internet (wan1) | | | | | | | |
| 2 | Navigazione LAN1 | all | all | always | ALL | ACCEPT | Disabled |
| LAN1 - PC1 (internal1) → LAN2 - PC2 (internal2) | | | | | | | |
| 4 | LAN1 -> LAN2 | all | all | always | ALL | ACCEPT | Disabled |
| LAN2 - PC2 (internal2) → Internet (wan1) | | | | | | | |
| 3 | Navigazione LAN2 | all | none | always | ALL | ACCEPT | Enabled |
| LAN2 - PC2 (internal2) → LAN1 - PC1 (internal1) | | | | | | | |
| 5 | LAN2 -> LAN1 | all | all | always | ALL | DENY | |
| LAN3 - PC Candidato (internal3) → Internet (wan1) | | | | | | | |
| 1 | Navigazione LAN3 | all | all | always | ALL | ACCEPT | Enabled |
| Implicit | | | | | | | |
| 0 | Implicit Deny | all | all | always | ALL | DENY | |

E le soluzioni sono le seguenti:
1. Configurare il PC1 con IP statico immettendo i valori inseriti nella tabella di configurazione;
2. Configurare il PC2 con IP dinamico;
3. Abilitare il NAT sulla regola;
4. Abilitare la regola;
5. Immettere "ALL" invece di "NONE" nella regola di navigazione di PC2;
6. Immettere "ACCEPT" come Action nella regola.

Ravenna, 3/10/2025

IL PRESIDENTE dott.ssa Maria Brandi

LA SEGRETARIA dott.ssa Silvia Fiammenghi