SELEZIONE PUBBLICA PER ESAMI PER L'ASSUNZIONE A TEMPO INDETERMINATO E PIENO DI N. 1 "ISTRUTTORE DIRETTIVO TECNICO" (INFORMATICO-SISTEMISTA) – AREA FUNZIONARI E DELL'E.Q.

CRITERI DI VALUTAZIONE DELLA PROVA SCRITTA

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 scritta sostenuta dai candidati il giorno **19 SETTEMBRE 2025**.

La Commissione ha definito i seguenti criteri di valutazione dei 6 quesiti a risposta sintetica contenuti nella **prova estratta - C**, ad ognuno dei quali è assegnato un valore compreso tra 0 e 5 punti per un punteggio massimo complessivo di 30 assegnati in base ai seguenti elementi della risposta:

- Completezza e correttezza in riferimento alla tematica proposta;
- Pertinenza tecnica rispetto alla domanda;
- Chiarezza espositiva, capacità di sintesi e logicità della risposta;
- Stile linguistico grammaticalmente corretto ed adeguato, anche in relazione all'utilizzo di terminologia tecnico-specialistica appropriata per le diverse tematiche.

Considerato che ai sensi dell'art. 18 comma 7 del Regolamento delle Selezioni del Comune di Ravenna il punteggio minimo richiesto per il superamento di una prova è di 21/30, corrispondente al giudizio di discreto, la Commissione ha espresso la votazione, per ogni quesito, 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 pari a 5 punti, secondo la seguente formula:

$$p = \frac{V \times 5}{10}$$

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 scala scolastica punti in /10	punteggio riparametrato punti in /5
Risposta non data	0	0
Risposta gravemente insufficiente	1	0,5
Risposta gravemente insufficiente	1,5	0,75
Risposta gravemente insufficiente	2	1
Risposta gravemente insufficiente	2,5	1,25
Risposta gravemente insufficiente	3	1,5
Risposta gravemente insufficiente	3,5	1,75
Risposta insufficiente	4	2
Risposta insufficiente	4,5	2,25
Risposta insufficiente	5	2,5
Risposta lievemente insufficiente	5,5	2,75
Risposta sufficiente	6	3
Risposta più che sufficiente	6,5	3,25
Risposta discreta	7	3,5
Risposta più che discreta	7,5	3,75
Risposta buona	8	4

	votazione scala scolastica punti in /10	punteggio riparametrato punti in /5
Risposta più che buona	8,5	4,25
Risposta ottima	9	4,5
Risposta più che ottima	9,5	4,75
Risposta eccellente	10	5

Si riportano di seguito i contenuti della risposta attesa per ogni quesito definiti dalla Commissione in modo schematico ed a titolo esemplificativo:

QUESITO 1

Descrivere il sistema Active Directory e il suo utilizzo nella gestione di una rete basata su Microsoft Windows Server, tracciandone un esempio di utilizzo in una rete comunale di circa 1000 PC, 100 server e 1200 utenti.

Active directory è il servizio di directory derivato da LDAP di Windows Server che permette di centralizzare la gestione di utenti, computer, gruppi, risorse di rete, etc: con il suo utilizzo autenticazione, autorizzazione e applicazione di policy (oltre a tanti altri servizi) possono essere gestiti in modo centralizzato, garantendo maggiore sicurezza, riduzione dei costi operativi e alta affidabilità. Nella rete comunale descritta sarà configurata una foresta AD e uno o più domini, declinati in diverse OU. I controller di dominio, almeno 2 per garantire ridondanza e bilanciamento di carico, saranno configurati per gestire i 5 ruoli FSMO (Schema Master, Domain Naming Master, RID Master, PDC Emulator, Infrastructure Master). I server e i PC saranno tutti uniti al dominio. Gli utenti, configurati come utenti di dominio, potranno essere distribuiti nelle OU configurate (eventualmente corrispondenti a servizi/uffici del Comune). Gli utenti e i PC saranno inclusi in appositi gruppi di AD in modo da gestire semplicemente i permessi di accesso a tutte le risorse di rete (PC, server, applicazioni, cartelle condivise, stampanti, navigazione Internet, ecc). Ogni utente potrà potenzialmente accedere, con le proprie credenziali di dominio, a qualsiasi PC appartenente al dominio stesso.

QUESITO 2

Un servizio comunale, configurato all'interno di un dominio Active Directory del Comune, ha 10 utenti e una rete di 10 PC, e utilizza un server Windows come file server. Come configureresti una cartella condivisa da far utilizzare ai 10 utenti? Se alla fine delle operazioni uno dei 10 utenti non riesce comunque ad accedere alla cartella, cosa può essere successo e come agisci?

La cartella sul file server va condivisa con due accorgimenti: permessi di accesso a livello di condivisione e permessi di accesso a livello di file system (tipicamente NTFS). In entrambi i casi è buona norma creare uno o più gruppi di dominio per la risorsa e popolarlo con utenti e/o gruppi di utenti (come best practice, usando solo gruppi) che devono aver accesso alla risorsa stessa. In tal modo la gestione dell'accesso alla cartella risulta semplificata riducendo costo operativo e possibilità di errori. Ad esempio: la cartella "D:\shared" viene condivisa con permessi lettura/scrittura al gruppo "shared_ServizioComunale_users_rw", e vengono assegnati permessi NTFS lettura/scrittura al gruppo stesso o, preferibilmente, ad un gruppo dedicato (es. "FS_shared_ServizioComunale_users_rw). In questo modo ogni utente del servizio per accedere alla cartella dovrà essere nel primo gruppo per avere accesso in lettura/scrittura alla condivisione e nel secondo gruppo per aver accesso in lettura/scrittura al filesystem (che tipicamente è un sottoinsieme della condivisione).
Se alla fine delle operazioni uno degli utenti non accede alla cartella può significare che: non è stato inserito in uno o entrambi i gruppi definiti, oppure sull'utente, o sulla risorsa, sono attive restrizioni di altro tipo, ad esempio una regola DENY specifica sulla cartella stessa che ha priorità sulla regola di accesso definita dall'appartenenza al gruppo.

QUESITO 3

Descrivere brevemente la differenza tra switch, router e firewall e delinearne una loro implementazione per una rete Windows di 5 PC, 1 server che eroga servizi web su Internet e 1 file server a servizio degli utenti interni, considerando la componente router integrata nella componente firewall.

Uno switch è un dispositivo di livello 2 che interconnette tra loro più host a livello locale e instrada i messaggi (frame) tra questi basandosi sull'indirizzo fisico delle schede di rete (c.d. MAC address).
Un router è un dispositivo di livello 3 che collega tra loro reti diverse (segmentando i diversi rami di livello 2 sulle sue singole interfacce fisiche o virtuali) e instradando i messaggi (pacchetti) in base agli indirizzi IP assegnati all'interfaccia di rete degli host.

Un firewall è un dispositivo che controlla e filtra il traffico in ingresso/uscita dalle sue interfacce di rete secondo regole basate su diversi parametri (indirizzo sorgente/destinazione, protocollo, porta sorgente/destinazione, ecc), permettendo solo il traffico ritenuto "lecito" e bloccando il traffico ritenuto "illecito" o comunque non consentito.
I 5 PC e il file server (qualora non sia necessaria una sua ulteriore protezione inserendolo in LAN dedicata) sono configurati con indirizzi IP appartenenti alla stessa rete privata, con default gateway corrispondente all'interfaccia interna (LAN) del router/firewall, sempre appartenente alla stessa subnet IP, e connessi fisicamente alle porte dello switch. Un'altra porta dello switch è a sua volta connessa all'interfaccia interna (LAN) del router/firewall. Una seconda interfaccia del router/firewall (DMZ) è collegata al server web (direttamente oppure, se possibile, sfruttando le funzionalità VLAN dello switch esistente o con un secondo switch se ci sono altri server in DMZ); il server web è configurato in una subnet privata diversa da quella in uso nella LAN e con default gateway configurato come l'IP assegnato all'interfaccia DMZ del router/firewall. L'interfaccia esterna del router/firewall (WAN o Internet) è connessa al provider Internet e, se non lo fa il provider, è configurata per eseguire il NAT almeno in uscita (Overload) per la navigazione Internet. Opportune regole del firewall permetteranno la navigazione Internet, l'accesso dalla LAN al server in DMZ (e viceversa) e l'accesso da Internet al server web in DMZ (tipicamente con un NAT 1-1 tra un IP pubblico dedicato, e diverso da quello di navigazione, e l'IP privato del server web o un PAT tra la porta 443 di un IP pubblico qualsiasi e la porta 443 dell'IP privato del server web).

QUESITO 4

Un servizio di un Comune ha una rete con indirizzamento IP 192.168.0.0/24 e un server proxy con indirizzo 192.168.0.200. Descrivere brevemente come configurare i PC della rete e le regole del firewall per la navigazione Internet senza forzare l'utilizzo del proxy server, completando di conseguenza la tabella seguente.

Source interface	*Source network*	*Destination interface*	*Destination network*	*Services*	*NAT*	*Action*
LAN	*192.168.0.0/24*	*WAN*				

Qualora il Comune decidesse di utilizzare il proxy forzandone l'utilizzo anche a livello di firewall, come cambierebbe la configurazione? Completare la tabella seguente di conseguenza.

Source interface	*Source network*	*Destination interface*	*Destination network*	*Services*	*NAT*	*Action*
LAN	*192.168.0.0/24*	*WAN*				
LAN	*192.168.0.200/32*	*WAN*				

In riferimento alla correzione del presente quesito la Commissione, nella condivisione dei contenuti attesi, oltre a tenere conto del refuso già segnalato da un candidato in sede di prova scritta sulla prima tabella (ossia che l'indicazione corretta non è ... 0/0 bensì .... 0/24), si rende conto che alcune ambiguità nella formulazione anche della seconda tabella potrebbero aver determinato difficoltà interpretative da parte dei candidati e/o aver indotto i candidati a non compilare la tabella medesima: tenuto conto che l'esercizio può essere suddiviso in due parti, ossia uno sviluppo teorico e la relativa soluzione pratico-operativa sintetizzata nella compilazione delle tabelle, la Commissione procede a suddividere i 5 punti a disposizione attribuendone metà (massimo 2,5 punti) all'esposizione dei contenuti teorici del quesito e metà (massimo 2,5 punti) allo sviluppo pratico-operativo di compilazione delle tabelle e di assegnare, in relazione ai dubbi interpretativi che la compilazione della seconda tabella pone, i relativi 2,5 punti per intero a tutti i candidati graduando invece nel modo seguente i 2,5 punti massimi attribuibili alla parte di sviluppo teorico del quesito secondo la seguente tabella di parametrazione e i seguenti contenuti attesi:

	votazione scala scolastica punti in /10	punteggio riparametrato punti in /2,5
Risposta non data	0	0
Risposta gravemente insufficiente	1	0,25
Risposta gravemente insufficiente	1,5	0,375
Risposta gravemente insufficiente	2	0,5
Risposta gravemente insufficiente	2,5	0,625
Risposta gravemente insufficiente	3	0,75
Risposta gravemente insufficiente	3,5	0,875

	votazione scala scolastica punti in /10	punteggio riparametrato punti in /2,5
Risposta insufficiente	4	1
Risposta insufficiente	4,5	1,125
Risposta insufficiente	5	1,25
Risposta lievemente insufficiente	5,5	1,375
Risposta sufficiente	6	1,5
Risposta più che sufficiente	6,5	1,625
Risposta discreta	7	1,75
Risposta più che discreta	7,5	1,875
Risposta buona	8	2
Risposta più che buona	8,5	2,125
Risposta ottima	9	2,25
Risposta più che ottima	9,5	2,375
Risposta eccellente	10	2,5

I PC della rete devono essere configurati con IP appartenenti alla subnet 192.168.0.0/24 e con default gateway l'indirizzo IP del firewall sull'interfaccia LAN (es. 192.168.0.254 oppure 192.168.0.200 se il proxy è integrato nel firewall). Il firewall accetta tutto il traffico proveniente dalla rete 192.168.0.0/24 e destinato, su qualsiasi servizio (TCP/UDP/ICMP, ecc) verso qualsiasi rete (0.0.0.0/0) effettuando il NAT con l'IP pubblico dell'interfaccia esterna. In questo modo i PC possono navigare senza proxy, ma anche con il proxy se configurato sul client.

Volendo forzare l'utilizzo del proxy a livello di firewall, occorre abilitare il traffico proveniente dal solo proxy server verso Internet, in questo caso limitando eventualmente il traffico verso le porte standard di navigazione Internet (80/tcp, 443/tcp) e impostando il NAT, e contemporaneamente bloccare il traffico proveniente dai PC e diretto verso Internet.

Si considerano adeguate anche soluzioni alternative proposte dai candidati, purchè compatibili con gli elementi dati.

QUESITO 5

Data la seguente query SQL relativa ad un DB SqlServer, indicare come è composto il DB (tabelle, chiavi) e che effetto produce la query:

```
UPDATE articoli
SET articoli.sconto = 10
FROM articoli
JOIN generi ON generi.id_genere = articoli.id_genere
JOIN produttori ON produttori.id_produttore = articoli.id_produttore
WHERE generi.genere = 'giardinaggio' AND produttori.nazione = 'Italia'
AND articoli.prezzo > 100;
```

Il DB si compone di tre tabelle: la tabella degli articoli con chiave primaria non desumibile dalla query, e i campi sconto e prezzo; la tabella generi con primary key id_generi e campo genere; la tabella produttori con primary key id_produttore e campo nazione. Nella tabella articoli ci sono due foreign key: id_genere in relazione con la tabella generi, id_produttore con tabella produttori.

La query è una update e quindi aggiorna dei record della tabella articoli; in particolare viene aggiornato il campo sconto ponendone il valore uguale a 10 per tutti quei record tali che fanno riferimento ad articoli aventi il prezzo maggiore di 100 e che sono in relazione con i record della tabella generi aventi il campo genere uguale a giardinaggio e contemporaneamente sono in relazione con i record della tabella produttori che hanno il campo nazione uguale a Italia; in sintesi viene aggiornato a 10 lo sconto per tutti gli articoli di giardinaggio di produttore italiano che hanno prezzo maggiore di 100.

QUESITO 6

Definire cosa si intende per web server e descrivere il suo ruolo nel funzionamento di un sito web. Illustrare i principali componenti e protocolli coinvolti e spiega come avviene la gestione delle richieste da parte del server. Indicare misure di sicurezza che possono essere adottate per proteggere un web server da attacchi comuni.

Un web server è un software (o il dispositivo che lo ospita) che gestisce le richieste provenienti da client (tipicamente browser) in genere di protocolli http/https e restituisce le risposte appropriate che possono essere pagine html, file, immagini, dati. Tipicamente, ma non esclusivamente, il server web riceve le richieste sulla porta TCP 80 (protocollo http) o 443 (protocollo https). Quando un utente digita un indirizzo web (URL) sul proprio browser, esso invia la richiesta all'apposito server web (l'indirizzo IP del server web viene dedotto tramite il servizio DNS). Si crea una connessione con il server web. Il server web elabora la richiesta che potrebbe riguardare una pagina statica o una pagina dinamica (un apposito motore server-side esegue il codice per determinare il contenuto).

Per proteggere un server web è fondamentale utilizzare un firewall con regole che limitano la superficie di attacco secondo il principio del minimo privilegio necessario; occorre bloccare il traffico inutile consentendo l'accesso solo alle porte e indirizzi IP necessari. E' fondamentale usare il protocollo https al posto di http. Occorre tenere il server costantemente aggiornato e disabilitare i servizi non necessari. Implementare politiche per prevenire attacchi di tipo denial of service limitando il numero e la frequenza delle richieste gestite. Appositi firewall di ultima generazione, c.d. WAF, possono proteggere il traffico fino al layer7 ISO/OSI.

Ravenna, 24 settembre 2025

LA PRESIDENTE	dott.ssa Maria Brandi
L'ESPERTO INTERNO	Ing. Alessandro Bucci
L'ESPERTO ESTERNO	Ing. Luca Farabegoli
LA SEGRETARIA	dott.ssa Silvia Fiammenghi