Convocatòria S-20/24-A Tècnic/a superior informàtica ORGT - àmbit d'explotació i sistemes

Qüestionari

I - LINUX

1. **Quina ordre serveix per trobar les línies del fitxer f.txt que contenen la paraula *casa*?**

   a) grep "casa" f.txt.
   b) find f.txt "casa".
   c) cat f.txt | locate "casa".
   d) cat f.txt | find "casa".

2. **Què conté el directori /sbin?**

   a) Fitxers de dispositius presents al sistema.
   b) Fitxers amb binaris per a l'administrador.
   c) Fitxers amb la configuració del sistema.
   d) Fitxers privats de l'usuari sbin.

3. **Quin dels següents formats de disc és nadiu de Linux?**

   a) UDF.
   b) NTFS.
   c) EXT4.
   d) APFS.

II - Bases de dades ORACLE

4. **Quina de les afirmacions següents és certa? El diccionari de dades d'una base de dades...**

   a) Permet que qualsevol usuari de la base de dades hi pugui dur a terme operacions de modificació directa (mitjançant UPDATE).
   b) Emmagatzema la definició de tots els objectes de la BD.
   c) Està emmagatzemat al *tablespace* USERS i hi pot accedir qualsevol usuari de la base de dades.
   d) És opcional; hi pot haver bases de dades sense diccionari de dades.

5. **Amb relació a les transaccions i el seu processament, quina de les afirmacions següents és certa?**

   a) Una transacció és una seqüència d'operacions que s'han d'executar de manera atòmica.
   b) A Oracle, una transacció és una seqüència de sentències SQL, però per mecanismes propis de l'SGBD no és necessari tractar-la com una unitat única.
   c) No hi ha errors de transacció.

d) Quan una transacció acaba amb èxit, les actualitzacions fetes per la transacció es graven amb la sentència ROLLBACK.

6. Quina de les afirmacions següents és certa?

a) Els segments de *rollback* emmagatzemen les últimes sentències fetes sobre la BD.
b) Els fitxers de control emmagatzemen l'estructura lògica de la BD.
c) Un *backup* de la BD és un fitxer d'emmagatzemament de canvis a la BD.
d) Un *backup* lògic no és una còpia de seguretat de la BD.

7. Un error de sistema ha perjudicat el disc on hi ha una BD Oracle i s'hi han produït danys. Es tracta d'una BD en línia en què es fan canvis contínuament. L'únic i darrer *backup* físic que se'n té és de dues hores abans de quan hi ha hagut la fallada. La BD està en mode NO ARCHIVELOG. Quina de les següents afirmacions és certa?

a) Com que tenim el *backup* físic, en podem fer una recuperació completa.
b) Davant d'aquesta situació, s'han perdut totes les dades, i no es pot recuperar res de la BD.
c) Com que tenim el *backup* físic, en podem fer una recuperació però amb pèrdua d'informació.
d) Com que està en mode NO ARCHIVELOG, en podem fer una recuperació completa utilitzant el *backup* i els fitxers REDOLOG.

III - SQL

8. Donades aquestes dues taules:

```
CREATE TABLE usuaris (id number(10) NOT NULL, nom varchar2(50) NOT NULL, nom_ajuntament varchar2(50), espai number NOT NULL );

CREATE TABLE ajuntaments (id number(10) NOT NULL, nom_ajuntament varchar2(50) NOT NULL, comarca varchar2(50) );
```

Quina consulta recupera els noms dels usuaris dels ajuntaments de la comarca del Baix Llobregat?

a) Select nom from usuaris, ajuntaments
   where usuaris.nom_ajuntament = ajuntaments.nom_ajuntament AND comarca = "Baix Llobregat"
b) Select nom from usuaris where nom_ajuntament IN
   (Select nom_ajuntament from ajuntaments where comarca = "Baix Llobregat")
c) Select nom from (SELECT nom, comarca from usuaris, ajuntaments
   where usuaris.nom_ajuntament = ajuntaments.nom_ajuntament)
   where comarca = "Baix Llobregat"
d) Les tres respostes són vàlides.

9. **Seguim amb les dues taules anteriors. Si considerem que l'espai que ocupa un ajuntament és la suma de l'espai que tenen els seus usuaris, quina és la consulta que recupera els noms dels usuaris dels ajuntaments que n'ocupen més de 1000?**

   a) Select nom from usuaris group by nom having sum(espai) > 1000.
   b) Select nom from usuaris where nom_ajuntament IN (select nom_ajuntament from usuaris group by nom_ajuntament having sum(espai) >1000).
   c) Select nom from usuaris, ajuntaments where usuaris.nom_ajuntament = ajuntaments.nom_ajuntament and sum(espai) > 1000 group by nom.
   d) Select nom from usuaris having nom, sum(espai) > 1000.

IV – TUXEDO

10. **Quina de les característiques següents descriu més bé Oracle Tuxedo?**

    a) Permet l'execució d'aplicacions C, C++, COBOL i Java en entorns distribuïts.
    b) S'utilitza exclusivament per a l'administració de bases de dades Oracle.
    c) Sols funciona en sistemes Windows.
    d) És un *middleware* que no admet transaccions.

11. **Quina de les opcions següents descriu més bé el rol dels servidors a Oracle Tuxedo?**

    a) Són responsables de gestionar sol·licituds de clients i executar la lògica de negoci.
    b) Només emmagatzemen dades i no executen lògica de negoci.
    c) Funcionen exclusivament com a balancejadors de càrrega.
    d) Són opcionals a l'arquitectura de Tuxedo.

V – Estratègies i tècniques de còpies de seguretat i restauració en entorns de fitxers i bases de dades

12. **Quina és la diferència principal entre una còpia de seguretat completa i una d'incremental?**

    a) La còpia completa només desa els fitxers modificats des de l'última còpia.
    b) La còpia incremental només desa els fitxers nous o modificats des de l'última còpia (sigui completa o incremental).
    c) La còpia completa és més ràpida que la incremental.
    d) La còpia incremental es pot restaurar independentment, sense cap altra còpia.

13. **Quina és la millor pràctica per garantir la protecció de les còpies de seguretat contra *ransomware*?**

    a) Mantenir les còpies de seguretat a la mateixa xarxa de producció per accés ràpid.
    a) Utilitzar còpies de seguretat immutable i mantenir-ne almenys una còpia fora de línia.

b) Desar només còpies en un servidor NAS sense xifratge.
c) Fer servir només un sistema RAID per evitar pèrdues de dades.

VI - Seguretat TIC

14. Quina d'aquestes estratègies és més efectiva per garantir la continuïtat del negoci en cas de fallada d'un centre de dades principal?

a) Mantenir *backups* diaris en un centre de dades extern a l'actiu.
b) Implementar un model Active-Active amb rèpliques en temps real en un segon centre de dades.
c) Fer còpies de seguretat manuals només quan es detecta una amenaça potencial.
d) Configurar un sistema RAID al centre de dades principal per evitar la pèrdua de dades.

15. En el marc de la continuïtat del negoci, què mesura l'RTO (*recovery time objective*)?

a) El temps màxim permès per recuperar una operació abans que l'impacte sigui crític.
b) El temps que un sistema pot estar funcionant abans de requerir manteniment preventiu.
c) El temps màxim que un sistema pot romandre inactiu abans que es consideri una fallada permanent.
d) El temps màxim en què es poden perdre dades sense afectar la continuïtat del negoci.

VII - Virtualització

16. Citrix Virtual Apps and Desktops: Com podem fer actualitzacions en un grup de màquines virtuals no persistents aprovisionades amb MCS?

a) Fer canvis a la màquina virtual de referència, crear un *snapshot*, canviar l'*snapshot* de referència al catàleg.
b) Copiar el disc aprovisionat, assignar-lo a una màquina, fer els canvis al disc en mode persistent, canviar el disc a no persistent i assignar-lo a totes les màquines.
c) Clonar la màquina virtual de referència, fer canvis a la màquina clonada, crear un *delivery group* que apunti a la nova màquina clonada.
d) Clonar la màquina virtual de referència, fer canvis a la màquina clonada, crear un catàleg que apunti a la nova màquina clonada.

17. Quin tipus d'adaptador de xarxa és el recomanat a Vsphere ESXi per a una màquina virtual de Windows Server 2022?

a) E1000E.
b) NIC extended.
c) VMXNET 3.
d) E2002.

18. **Tenim un entorn amb diversos servidors hipervisors que allotgen diferents màquines virtuals cadascun. Quins recursos han de compartir aquests servidors hipervisors perquè puguem moure una màquina virtual d'un servidor hipervisor a un altre sense aturar-la?**

    a) L'emmagatzematge dels discos de la màquina virtual i la memòria.
    b) La xarxa on està connectada la màquina virtual.
    c) La memòria dels servidors hipervisors.
    d) Les opcions *a* i *b*.

VIII – Comunicacions LAN, SAN i WAN. Tecnologies i dispositius associats

19. **Quina tecnologia és més habitual per a la connexió i transport de dades en una SAN corporativa?**

    a) FTP (File Transfer Protocol).
    b) Fibre Channel.
    c) HTTP (Hypertext Transfer Protocol).
    d) VLAN (Virtual Local Area Network) Trunking Protocol.

20. **Quin dispositiu s'utilitza per segmentar l'espai de *broadcast* d'una LAN mitjançant VLANs?**

    a) *Hub*.
    b) *Switch* de capa 2 o superior.
    c) Modem ADSL (Asymmetric Digital Subscriber Line).
    d) Repetidor.

21. **En quin escenari s'usa normalment el protocol MPLS (Multiprotocol Label Switching)?**

    a) Per transmetre arxius entre clients i servidors d'emmagatzematge local.
    b) En enllaços sense fils de curt abast en entorns LAN (Local Area Network).
    c) Per interconnectar xarxes WAN (Wide Area Network) amb trànsit a gran escala i qualitat de servei.
    d) Per a sessions d'SSH (Secure Shell) en entorns de gestió remota.

22. **Quin protocol s'utilitza habitualment per establir una VPN *site-to-site* segura sobre una WAN, encapsulant i xifrant el trànsit IP?**

    a) DHCP (Dynamic Host Configuration Protocol).
    b) PPTP (Point-to-Point Tunneling Protocol).
    c) IPsec (Internet Protocol Security).
    d) ARP (Address Resolution Protocol).

IX - Elements de seguretat: antivirus, *antispyware*. Seguretat perimetral: *antispam*, tallafocs, detecció d'intrusions, WAF, EDR, SIEM

23. **Quina diferència clau hi ha entre un sistema IDS (*intrusion detection system*) i un IPS (*intrusion prevention system*)?**

a) L'IDS pot bloquejar atacs en temps real, mentre que l'IPS només els monitoritza.
b) L'IDS monitoritza i alerta; l'IPS pot actuar bloquejant el trànsit sospitós.
c) L'IDS funciona només en entorns virtuals; l'IPS, en entorns físics.
d) L'IDS serveix per a correu electrònic i l'IPS per a trànsit web.

24. Quin tipus de solució unifica i correla *logs* de múltiples fonts en temps real per detectar amenaces avançades?

a) *Firewall* d'aplicació (WAF).
b) SIEM (Security Information and Event Management).
c) EDR (Endpoint Detection and Response).
d) Antispam Gateway.

25. Quina tecnologia permet a un tallafocs inspeccionar i analitzar el trànsit xifrat HTTPS?

a) *Sandboxing* de *malware*.
b) NAT (Network Address Translation) estàtic.
c) SSL/TLS (Secure Socket Layer / Transport Layer Security) Inspection.
d) *Hashing* unidireccional.

26. Quina característica diferencia una solució EDR (Endpoint Detection Response) d'un antivirus tradicional?

a) Funciona exclusivament en local, sense actualitzacions al núvol.
b) Només detecta *malware* basant-se en signatures.
c) Ofereix detecció i resposta en temps real basades en anàlisi de comportament.
d) Permet l'anàlisi forense i la contenció remota de l'*endpoint*.

X - Esquema Nacional de Seguretat

27. Segons l'article 12 del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), el conjunt de directrius que regeixen la forma en què una organització gestiona i protegeix la informació que tracta i els serveis que presta s'anomena:

a) Vigilància contínua.
b) Política de seguretat de la informació.
c) Qualitat.
d) Glossari.

28. Segons l'article 13 del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), és missió específica del responsable de seguretat:

a) Determinar els requisits de la informació tractada.
b) Designar un POC (punt o persona de contacte).
c) Determinar les decisions per satisfer els requisits de seguretat de la informació i dels serveis.
d) Totes les anteriors.

29. **Segons l'article 20 del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), els sistemes d'informació s'han de dissenyar i configurar atorgant els mínims privilegis necessaris per al seu correcte funcionament, cosa que implica incorporar els aspectes següents:**

    a) S'apliquen guies de configuració de seguretat per a les diferents tecnologies, adaptades a la categorització del sistema.
    b) S'eliminen o desactiven, mitjançant el control de la configuració, les funcions que siguin innecessàries o inadequades a la finalitat que es persegueix.
    c) El sistema proporciona la funcionalitat imprescindible perquè l'organització assoleixi els seus objectius competencials o contractuals.
    d) Totes les anteriors.

30. **Segons l'article 31 del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), els sistemes d'informació compresos en l'àmbit d'aplicació d'aquest reial decret han de ser objecte d'una auditoria regular ordinària almenys:**

    a) Anualment.
    b) Cada dos anys.
    c) Segons la potestat de la direcció.
    d) El Reial decret no regula aquest extrem.

XI – Internet

31. **Si hem d'evitar comunicacions no xifrades o amb protocols declarats insegurs, quin és el protocol que s'ha d'utilitzar en una comunicació segura amb un servidor web?**

    a) HTTP.
    b) SSL versió 3.
    c) TLS versió 1.2.
    d) SSL versió 4.

32. **Quin dels següents és un protocol relacionat amb el correu electrònic (*e-mail*)?**

    a) IMAP.
    b) EGP.
    c) SSH.
    d) ARP.

33. **Quin paràmetre de DHCP determina quant de temps un equip pot fer servir una IP abans de renovar-la?**

    a) Subnet Mask.
    b) Default Gateway.
    c) Lease Time.
    d) DNS Server.

34. Quina característica clau defineix el protocol DHCP en comparació amb la configuració estàtica d'IP?

a) Permetre resoldre noms de domini sense un servidor DNS.
b) Assignar adreces IP sense necessitat d'un servidor central.
c) Assignar automàticament l'adreça IP i altres paràmetres de xarxa.
d) Garantir velocitats de transferència més altes en entorns LAN.

XII - Directori actiu

35. Digues quina frase és certa pel que fa al directori actiu:

a) Es pot augmentar el nivell funcional del domini a 2016 amb controladors al mateix domini en versions de Windows Server 2012 R2.
b) Es pot augmentar el nivell funcional del bosc a 2019 si tots els dominis que hi pertanyen estan en nivell funcional 2019.
c) El nivell funcional del domini es pot reduir després d'haver estat augmentat.
d) Els controladors de domini han de tenir versions iguals o superiors al nivell funcional establert.

36. En un entorn híbrid amb l'Azure AD Connect, quina és la manera més recomanada d'habilitar MFA per als usuaris autenticats amb Single Sign-On (SSO)?

a) Configurar MFA directament a l'Azure AD Conditional Access.
b) Activar MFA a l'Active Directory Users and Computers (ADUC).
c) Instal·lar un servidor físic per gestionar MFA localment.
d) Configurar MFA mitjançant *group policies* (GPO) a l'Active Directory.

XIII – Powershell

37. Quina és l'ordre Powershell necessària per executar *scripts* sense signar?

a) Set-AllowedScript All.
b) Set-ExecutionPolicy Unrestricted.
c) Set-LockedScript Unrestricted.
d) Set-UnlockedScript All.

38. Què fa el següent *script*: Get-ChildItem | Get-Member?

a) Retorna la llista de fitxers del directori actual.
b) Retorna el contingut dels fitxers del directori actual.
c) Retorna els atributs dels fitxers del directori actual.
d) Retorna la llista de propietats i mètodes de fitxers i directoris.

39. Què fa el següent *script*: import-module ActiveDirectory
Get-ADComputer -Filter 'Name -like "v*"' | Select Name?

a) No fa res. Dona un error.

b) Obté els objectes dels ordinadors que comencin amb la lletra *v* que tenim donats d'alta a l'Active Directory.
c) Obté els noms dels ordinadors que comencin amb la lletra *v* que tenim donats d'alta a l'Active Directory.
d) Obté els noms dels servidors que comencin amb la lletra *v* que tenim donats d'alta a l'Active Directory.

XIV - Criptografia: definició i descripció. Certificats digitals i entitats certificadores. Connexions segures. Signatura electrònica

40. Quin element garanteix la validesa i la confiança en un certificat digital?

a) El període de validesa indicat al certificat.
b) La signatura de l'entitat certificadora (CA).
c) La presència del nom de domini al camp Subject del certificat.
d) La presència d'una autoritat *root* autosignada al magatzem de claus del sistema.

41. Quina és la funció principal d'una CA (*certificate authority*)?

a) Encriptar correus electrònics.
b) Emetre i revocar certificats digitals.
c) Generar claus simètriques per als usuaris.
d) Emmagatzemar de manera segura les claus privades dels usuaris.

42. Què assegura que una signatura electrònica sigui considerada vàlida i no repudiable?

a) Enviar el document signat mitjançant un servei de correu electrònic xifrat (per exemple, S/MIME).
b) Fer servir únicament un xifratge simètric compartit entre emissor i receptor.
c) Comptar amb un certificat emès per una CA (*certificate authority*) reconeguda i utilitzar signatura asimètrica.
d) Incorporar un segell de temps (*timestamp*) digital al document signat.

XV - Emmagatzematge (SAN, NAS). Redundància i sincronització de dades entre CPDs. Tipus de discos i configuracions RAID

43. Quina és una característica distintiva de la configuració RAID 5?

a) Combina *striping* i *mirroring* per millorar el rendiment i la redundància.
b) Ofereix la màxima redundància en duplicar totes les dades a dos conjunts de discos.
c) Utilitza paritat distribuïda per oferir redundància i millorar la capacitat d'emmagatzematge.
d) Se centra exclusivament en la millora del rendiment mitjançant la distribució de dades entre diversos discos.

44. Quina és la principal diferència entre SAN i NAS?

a) SAN utilitza connexions basades en xarxa, mentre que NAS no.
b) NAS proporciona accés a arxius a través de protocols de xarxa, mentre que SAN proporciona accés a blocs de dades.
c) SAN només s'usa per a emmagatzematge al núvol, mentre que NAS s'usa localment.
d) NAS és més costós que SAN.

45. Quin desavantatge té la replicació síncrona entre dos CPDs?

a) Més latència a causa de la necessitat de confirmar cada escriptura als dos llocs abans de completar-se.
b) Més risc de pèrdua de dades en cas de fallada del sistema.
c) No permet una recuperació ràpida en cas de fallada.
d) Només funciona amb connexions de baixa velocitat.

PREGUNTES DE RESERVA

1. **Quin mètode de còpia de seguretat és més adequat per garantir la mínima pèrdua de dades en bases de dades crítiques?**

   a) Fer només còpies completes diàries.
   b) Desactivar la replicació de la base de dades per evitar corrupcions durant la còpia.
   c) Configurar còpies completes en un servidor extern i restaurar manualment quan sigui necessari.
   d) Utilitzar una combinació de còpies completes, diferencials i registres de transaccions.

2. **En quina capa del model OSI se situa normalment el protocol DNS?**

   a) Sessió (capa 5).
   b) Xarxa (capa 3).
   c) Aplicació (capa 7).
   d) Presentació (capa 6).

3. **En un *handshake* TLS quin element s'utilitza per a l'autenticació del servidor en una connexió HTTPS?**

   a) L'arxiu robots.txt.
   b) El certificat digital X.509.
   c) El manifest JSON.
   d) Les polítiques de DNSSEC.

4. **Quina norma internacional és àmpliament utilitzada per a la gestió de la continuïtat de negoci?**

   a) ISO 27001.
   b) ISO 22301.
   c) ISO 9001.
   d) NIST 800-53.

Àrea de Serveis Generals i Transició Digital

Direcció dels Serveis de Recursos Humans

c/ Minerva, 4. 08006 Barcelona
Tel. 934 725 221
dsrh.reclutament@diba.cat - www.diba.cat

Convocatòria S-20/24-A Tècnic/a superior informàtica ORGT - àmbit d'explotació i sistemes

Plantilla qüestionari

Pregunta	Resposta
1	a
2	b
3	c
4	b
5	a
6	a
7	c
8	d
9	b
10	a
11	a
12	b
13	b
14	b
15	a
16	a
17	c
18	d
19	b
20	b
21	c
22	c
23	b
24	b
25	c
26	c
27	b
28	c
29	d
30	b
31	c
32	a
33	c

Àrea de Serveis Generals i Transició Digital

Direcció dels Serveis de Recursos Humans

Minerva, 4. 08006 Barcelona
Tel. 934 725 221 · Fax 934 022 279
ds.recursosh@diba.cat - www.diba.cat

34	c
35	d
36	a
37	b
38	d
39	c
40	b
41	b
42	c
43	c
44	b
45	a

Preguntes de reserva:

Pregunta	Resposta
1	d
2	c
3	b
4	b