Ajuntament
d'Olesa de Montserrat

PROVA 2 PRÀCTICA

CONEIXEMENTS PROFESSIONALS

DNI:	
Qualificació:	Data:

Desenvolupar per escrit, en el termini màxim de 120 minuts, el/s següent/s supòsit/s pràctic/s, que tindrà una puntuació màxima de 20 punts. Per superar aquesta prova eliminatòria cal obtenir una puntuació mínima de 10 punts.

Supòsit 1 (5 punts)

Un usuari et truca repetidament perquè no pot accedir a una aplicació implantada en un servidor virtual que gestiona una aplicació critica. Et comuniquen que el problema s'ha produït diverses vegades, però no sabem si és un incident puntual o una fallada més greu.
Quan et connectes al servidor per investigar la incidència, observes que hi ha un nou usuari amb permisos d'administrador que desconeixes, ja que no era part de la configuració inicial de l'entorn.

Detalla la comunicació amb l'usuari en cada una de les fases de la resolució de la incidència.

SOLUCIÓ:

- Confirmar el problema: Un cop s'hagin revisat els logs i realitzat les comprovacions inicials, contacta amb l'usuari per confirmar que estàs al corrent del problema. Pots comunicar-li que estàs investigant la incidència i que estàs a punt de realitzar proves de diagnòstic en el sistema. Comprovar criticitat i priorització.
- Informar sobre els passos següents: Informa a l'usuari que estàs revisant l'accés a l'aplicació i que estàs comprovant els permisos, així com la infraestructura del servidor, per garantir que tot estigui configurat correctament. Si pot ser, comunica a l'usuari un temps estimat de resolució, sempre explicant que la seguretat de les seves dades i el funcionament de l'aplicació són una prioritat.
- Solució temporal: Si la situació es pot solucionar de forma ràpida (per exemple, reiniciar l'aplicació o el servidor), informa a l'usuari que estàs aplicant aquesta solució mentre investigues el problema a fons.
- Informe final a l'usuari: Comunicar les accions realitzades i les millores en la seguretat aplicades.

Ajuntament
d'Olesa de Montserrat

Supòsit 2 (15 punts)

Formes part del departament de Tecnologies de la Informació i la Comunicació (TIC) de l'Ajuntament d'Olesa de Montserrat, el qual té 300 treballadors. Aquest departament, liderat per un responsable tècnic, té com a objectiu supervisar i definir les línies estratègiques tecnològiques de l'organització. Com a tècnic especialista superior TIC, la teva funció és donar suport tècnic i executar accions en col·laboració amb altres membres de l'equip.

Actualment, l'ajuntament afronta un augment de la demanda de serveis tecnològics, fet que ha incrementat el volum de treball relacionat amb incidències, manteniment i la implementació de noves eines. Paral·lelament, s'estan realitzant projectes per millorar serveis com la telefonia IP, el sistema de còpies de seguretat i l'adopció de solucions en el núvol.

<u>Reptes identificats:</u>

1. Gestió d'incidències
   - Increment de problemes de xarxa, errors en aplicacions i equips amb comportaments anòmals (reinicis inesperats)
   - Lentitud i interrupcions entre edificis connectats en xarxa

2. Optimització de xarxes LAN
   - Problemes de rendiment a la xarxa local, que requereixen anàlisi i accions de millora.

3. Manteniment i equips
   - Presència d'equips obsolets amb erros de compatibilitat amb el programari actual.

4. Seguretat TIC
   - S'han detectat contrasenyes febles i configuracions de firewall que necessiten millores.

5. Telefonia IP i comunicacions sense fils
   - Interrupcions freqüents al sistema de telefonia així com a la xarxa WI-FI.

6. Còpies de seguretat:
   - Implementació d'un sistema de còpies de seguretat.

7. Aplicacions al núvol
   - Anàlisi de viabilitat per implementar solucions allotjades al núvol.
   - Avaluació de les diferents opcions disponibles de computació al núvol.

<u>Respon a les qüestions següents:</u>

1. Gestió d'incidències
   1.1. Proposa i descriu els passos tècnics per identificar i resoldre errors de connexió en la xarxa local.
   1.2. Explica com abordaries els problemes amb aplicacions que no responen correctament.

1.3. Detalla el procediment per diagnosticar i solucionar la incidència d'equips que es reinicien inesperadament.
1.4. Explica com registraries i documentaries aquestes incidències al sistema de ticketing.

2. Optimització de xarxes LAN
   2.1. Explica quines accions faries per analitzar el rendiment de la xarxa
   2.2. Proposa solucions tècniques per millorar el rendiment de la xarxa local.

3. Manteniment i gestió d'equips
   3.1. Defineix com solucionaries errors de compatibilitat en els equips antics mentre es planifica la seva renovació.
   3.2. Proposa accions preventives i correctives per garantir el correcte funcionament dels equips informàtics.

4. Seguretat TIC
   4.1. Explica com col·laboraries en l'execució de polítiques de seguretat lògica.

5. Telefonia IP i Comunicacions WiFi
   5.1. Detalla el procediment per verificar la qualitat del servei (QoS) al sistema de telefonia IP.
   5.2. Explica com solucionaries les interrupcions en la xarxa Wi-Fi, incloent-hi accions de per millorar la cobertura.

6. Còpies de seguretat
   6.1. Explica com col·laboraries en la configuració del sistema de còpies de seguretat.
   6.2. Proposa un mètode per garantir la integritat de les dades restaurades.

7. Aplicacions al núvol:
   7.1. Proposa criteris tècnics per avaluar la compatibilitat de les aplicacions allotjades als servidors propis amb un model de computació al núvol.
   7.2. Explica les diferències entre els principals sistemes de computació al núvol (PaaS, Saas, IaaS).

SOLUCIÓ:

1. Gestió d'incidències:

1.1. Passos tècnics per identificar i resoldre errors de connexió en la xarxa local:

- Identificar l'abast del problema (afecta un equip, un grup o tota la xarxa).
- Comprovar el cablejat físic (cables desconnectats o danyats).
- Verificar l'estat dels dispositius de xarxa (switchos, routers) i la seva configuració.
- Realitzar proves de connectivitat amb comandes com *ping, traceroute* o utilitzant eines com *Wireshark* o PRTG Network Monitor per identificar colls d'ampolla.
- Comprovar l'adreçament IP i la configuració del servidor DHCP.
- Solucionar errors identificats (substituir cables, actualitzar configuracions o restablir dispositius).

1.2. Abordar problemes amb aplicacions que no responen correctament:
- Verificar l'estat dels servidors on s'allotgen les aplicacions.
- Comprovar l'estat de l'equip.
- Supervisar el rendiment del servidor on s'executen les aplicacions (ús de CPU, memòria, disc)
- Comprovar les connexions de xarxa i els permisos d'accés.
- Analitzar els registres (*logs*) de l'aplicació per identificar possibles errors.
- Realitzar proves amb versions anteriors de l'aplicació o reinstal·lar-la si cal.
- Revisar les dependències amb altres programari instal·lat amb mateix servidor (revisió de DLL compartides o serveis vinculats)
- Consultar amb el proveïdor de l'aplicació si el problema persisteix.

1.3. Diagnòstic d'equips que es reinicien inesperadament:
- Verificar la temperatura del sistema per identificar possibles problemes de sobreescalfament.
- Revisar les actualitzacions del firmware i dels drivers.
- Comprovar possibles fallades de hardware com la memòria RAM o el disc dur amb eines com *MemTest86+* o *SMART*.
- Analitzar els registres del sistema operatiu (per exemple, *Event Viewer* en Windows).
- Substituir components defectuosos o actualitzar l'equip.

1.4. Registre i documentació de les incidències al sistema de ticketing:
- Assignar un títol descriptiu a la incidència.
- Incloure una descripció completa del problema, els símptomes i l'abast.
- Documentar les proves realitzades i els resultats obtinguts.
- Registrar les accions correctives preses i els resultats finals.
- Adjuntar captures de pantalla, registres i informació addicional, si escau.

2. Optimització de xarxes LAN

2.1. Accions per analitzar el rendiment de la xarxa:
- Monitoritzar el trànsit de xarxa amb eines com *Wireshark*, *SolarWinds* o *PRTG Network Monitor*.
- Identificar colls d'ampolla i dispositius saturats (SolaWinds o Zabbix)
- Comprovar l'ús de l'ample de banda per part dels usuaris i les aplicacions.
- Revisar la configuració dels dispositius de xarxa, com VLANs o prioritats QoS.

2.2. Solucions tècniques per millorar el rendiment de la xarxa local:
- Configurar VLANs per segmentar el trànsit i reduir la congestió.
- Optimitzar la configuració QoS per prioritzar trànsit crític.
- Actualitzar switchos o routers obsolets amb models més potents.
- Implementar connexions redundants per millorar la disponibilitat.

3. Manteniment i gestió d'equips

3.1. Solució d'errors de compatibilitat en equips antics:
- Utilitzar entorns virtualitzats per executar software incompatible.
- Cercar actualitzacions de divers o controladors o adaptacions del software

- Substituir aplicacions incompatible per alternatives més lleugeres sempre que sigui possible.

3.2. Accions preventives i correctives per garantir el correcte funcionament:
- Implementar manteniment preventiu (actualitzacions periòdiques, neteja física d'equips).
- Configurar polítiques d'actualització automàtica per mantenir el programari actualitzar.
- Realitzar inventaris periòdics per identificar equips en risc de fallar.
- Garantir còpies de seguretat periòdiques de les dades dels equips.

4. Seguretat TIC

4.1. Execució de polítiques de seguretat lògica:
- Implementar polítiques de contrasenyes fortes (longitud mínima, complexitat i caducitat).
- Configurar firewalls per bloquejar trànsit no autoritzat i limitar l'accés a serveis essencials. Vlan's.
- Activar l'autenticació multifactor (2FA) per als accessos crítics.
- Monitoritzar la xarxa amb sistemes IDS/IPS (per exemple, *Snort* o *Suricata*).
- Realitzar simulacions d'atacs (test de penetració) per detectar vulnerabilitats.

5. Telefonia IP i Comunicacions Wi-Fi

5.1. Verificació de la qualitat del servei (QoS) en telefonia IP:
- Configurar regles de QoS als routers i switchos per prioritzar el trànsit de veu.
- Utilitzar eines com VoIPMonitor, SolarWinds VoIP & Network Quality Manager per monitoritzar latència i pèrdua de paquets.
- Realitzar proves amb eines com *MOS score* per garantir la qualitat de l'àudio.

5.2. Solucions per a interrupcions de la xarxa Wi-Fi:
- Optimitzar la ubicació dels punts d'accés per evitar zones amb cobertura insuficient.
- Configurar canals Wi-Fi per evitar interferències amb altres xarxes.
- Implementar sistemes Wi-Fi Mesh per ampliar la cobertura.

6. Còpies de seguretat

6.1. Configuració del sistema de còpies de seguretat:
- Planificar còpies diàries automàtiques, diferenciant còpies completes i incrementals.
- Configurar còpies externes i fora de línia per protegir contra ransomware.
- Monitoritzar el sistema per garantir la finalització correcta de cada còpia.

6.2. Garantir la integritat de les dades restaurades:
- Realitzar proves periòdiques de restauració en entorns de proves.
- Verificar la integritat de les dades amb sumes de verificació (*checksums*).

7. Aplicacions al núvol

7.1. Criteris tècnics per avaluar la compatibilitat amb el núvol:

- Analitzar els requisits de les aplicacions (CPU, RAM, espai d'emmagatzematge).
- Identificar les aplicacions actuals que es poden migrar al núvol sense afectar la seva funcionalitat.
- Verificar que les aplicacions compleixen amb els estàndards de seguretat del núvol. Compliment del RGPD
- Avaluar els costos de migració i manteniment en comparació amb l'entorn actual.

7.2. Diferències entre PaaS, SaaS i IaaS:

- IaaS (Infraestructura com a Servei): Proporciona recursos d'infraestructura bàsics com servidors i emmagatzematge. És útil per a projectes personalitzats.
- PaaS (Plataforma com a Servei): Ofereix entorns per desenvolupar i desplegar aplicacions, reduint la necessitat de gestionar la infraestructura.
- SaaS (Software com a Servei): Ofereix aplicacions preparades per al seu ús immediat (correu electrònic, gestió de dades, etc.). Ideal per a eines corporatives.