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 (6 punts)

Reps una trucada d'un company de l'Oficina Atenció Ciutadana el qual t'indica que no li funciona correctament l'ordinador, ja que tota l'estona es queda bloquejat i no li permet treballar amb normalitat. Està una mica nerviós, ja que hi ha diversos ciutadans que s'esperen que els atenguin.

Com actuaries davant d'aquesta incidència tenint en compte que a primera hora del matí el teu superior t'ha deixat encomandes unes tasques que s'haurien de finalitzar durant el dia d'avui. Descriu tots els passos que faries

Correcció: 1 punt per ítem:

1. Avaluar la urgència: *Després de rebre la trucada, identificaria la gravetat del problema. Si l'ordinador bloquejat impedeix que el company atengui els ciutadans, consideraria la incidència com a urgent, ja que afecta el servei públic directe.*

2. Comunicar amb el meu superior: *Donada la urgència de la situació, contactaria immediatament amb el meu superior per informar-lo de la incidència i confirmar si és possible interrompre momentàniament les tasques assignades. Si no es pot contactar amb el superior, prendria la iniciativa basant-me en la urgència del cas, amb l'objectiu de resoldre el problema ràpidament.*

3. Diagnòstic del problema: *Connectar-me a l'equip de manera remota o bé desplaçar-me per , realitzar un diagnòstic ràpid de l'ordinador:*

- *Comprovar si l'ordinador està realment bloquejat o si és un problema de rendiment (per exemple, per excés de càrrega de treball, aplicacions obertes o falta de memòria).*
- *Si es tracta d'un problema de bloqueig temporal, intentaria fer un reinici ràpid.*
- *Si no es resol amb el reinici o és un problema més complex (per exemple, un error del sistema operatiu o programari malmès), miraria si és possible utilitzar un ordinador de substitució.*

4. Proporcionar una solució temporal: *Si no puc resoldre el problema immediatament, buscaria solucions temporals:*

- *Si l'oficina té més ordinadors disponibles, organitzaria la substitució temporal de l'ordinador afectat perquè el company pugui seguir treballant.*
- *Si no hi ha cap equip disponible en el mateix departament, comprovaria si al magatzem hi ha algun equip que tingui el programari necessari per assignar-li provisionalment fins que es soluciona al problema en el seu equip.*

5. Documentació de la incidència: *És important deixar constància de la incidència al programa de gestió de tiquets per dur un seguiment de les actuacions que es fan en un equip, així com les accions que es fan per resoldre el problema.*

6. Retornar a les tasques assignades: *Un cop la incidència estigui resolta o estabilitzada, tornaria a les tasques encomanades pel meu superior, prioritzant aquelles que s'han de finalitzar durant el dia. Si la incidència ha pres més temps del previst, ho comunicaria al meu superior i gestionaria un ajust del temps o sol·licitant ajuda si fos necessari.*

Supòsit 2 (7 punts)

Es detecta la necessitat d'implantar un sistema de fitxers al núvol que permeti treballar en línia i simultàniament diversos usuaris de la xarxa i fora d'aquesta. De les solucions que hi ha al mercat proposa les dues que consideres més adequades per un ajuntament (una de programari lliure i l'altra subjecta a llicenciament) i detalla les característiques principals que s'han de tenir en compte, compara-les i explica com implantaries aquest servei.

Correcció:
1 .Proposta de solucions (1 punt)
2. Característiques principals (3 punts)
3. Comparativa (1 punts)
4. Procés d'implantació del servei (2 punts)

Solucions lliures: Nextcloud, owncloud, seafile
Solucions amb llicenciament: Google Workspace (Google Drive for Business), Microsoft 365 (OneDrive for Business)

Característiques principals:
- *Control total de les dades: Com que es pot instal·lar en servidors interns, l'ajuntament té el control absolut sobre on s'emmagatzemen les dades, complint amb les normatives de protecció de dades com el RGPD.*
- *Col·laboració en temps real: Permetre la creació i edició de documents de forma simultània entre diversos usuaris.*
- *Seguretat avançada: Ofereix funcions com l'autenticació de dos factors (2FA), encriptació de dades en trànsit i en repòs, gestió de permisos d'accés granular i integració amb sistemes LDAP o Active Directory. Xifrat de fitxers. Gestió d'usuaris i permisos*

- *Integració amb altres eines: Permetre la integració amb altres aplicacions com calendaris, correu electrònic i gestió de tasques, millorant l'eficiència del treball.*
- *Escalabilitat i personalització: Com a programari de codi obert, es pot personalitzar segons les necessitats específiques de l'ajuntament i escalar amb el creixement de l'organització.*
- *Sincronització ràpid i eficient: Permet la sincronització de fitxers grans de manera més ràpida*
- *Històric i recuperació de fitxers: Es poden recuperar versions anteriors dels fitxers durant un període de temps determinat, útil en cas d'errors o pèrdua d'informació.*
- *Administració centralitzada: Un panell d'administració facilita la gestió dels usuaris, dispositius i permisos d'accés.*

En cas de llicenciament:

- *Emmagatzematge escalable: Disposa de diferents plans que permeten augmentar la capacitat d'emmagatzematge segons les necessitats de l'ajuntament.*

Comparativa:

Característica	Nextcloud (Programari lliure)	Microsoft 365 (OneDrive for Business)
Cost	Sense cost de llicència, però cal inversió en infraestructures i manteniment tècnic.	Subscripció per usuari, amb suport tècnic i manteniment inclosos.
Control de dades	Control complet sobre les dades, ja que es poden allotjar en servidors propis.	Les dades es guarden en els servidors de Microsoft (amb opcions de núvol privat).
Facilitat d'ús	Pot requerir formació tècnica inicial.	Integració fluida amb les eines d'Office, fàcil d'utilitzar per a la majoria dels usuaris.
Seguretat	Gestió pròpia de la seguretat amb funcions avançades com encriptació i 2FA.	Seguretat gestionada per Microsoft amb opcions avançades com MFA i DLP.
Col·laboració en temps real	Integració amb OnlyOffice o Collabora per a la col·laboració.	Col·laboració nativa amb Office, permet treballar fàcilment en documents d'Office en temps real.
Escalabilitat	Altament escalable, però depèn de la infraestructura pròpia.	Escalabilitat fàcilment gestionada a través de subscripcions de Microsoft 365.
Compliment normatiu	Totalment adaptable a les normatives locals de protecció de dades.	Compliment automàtic del RGPD i altres normatives amb Microsoft.

Comparativa entre les opcions:

Característica	Seafile (Lliure)	Pydio Cells (Lliure)	Google Workspace (Llicència)	Dropbox Business (Llicència)
Cost	Sense cost de llicència, però cal infraestructures pròpies.	Sense cost de llicència, requereix infraestructura pròpia.	Subscripció mensual per usuari.	Subscripció mensual per usuari.
Control de dades	Control total amb allotjament local.	Control total amb allotjament local.	Dades allotjades en servidors de Google.	Dades allotjades en servidors de Dropbox.
Seguretat	Xifrat avançat i gestió pròpia.	Xifrat avançat i control granular.	Xifrat avançat i autenticació multifactor.	Xifrat i autenticació multifactor.
Facilitat d'ús	Pot requerir formació tècnica inicial.	Requereix una corba d'aprenentatge inicial.	Molt fàcil d'utilitzar, especialment amb aplicacions de Google.	Interfície intuïtiva i fàcil d'utilitzar.
Col·laboració en temps real	Possible amb integració de LibreOffice/Collabora.	Possible amb Collabora.	Nativa amb Google Docs, Sheets, etc.	Integra amb Office 365 i Google Workspace.
Escalabilitat	Altament escalable però depèn de la infraestructura pròpia.	Altament escalable, però requereix manteniment tècnic.	Altament escalable amb plans flexibles.	Altament escalable amb subscripció per usuari.

Implantació:

Un cop configurat el servei ja que sigui en servidors propis o no, ***informar als usuaris*** *d'aquest nou servei.* ***Planificar una reunió per concretar les necessitats especifiques*** *i sobretot fer* ***guies explicatives i/o sessions informatives*** *explicant com s'utilitzà i quines funcionalitats permet per treure el màxim profit possible. S'ha d'intentar prioritzar l'experiència de l'usuari per garantir el bon ús del programari. Fer* ***proves*** *abans de donar per finalitzada la implantació.*

Ajuntament
d'Olesa de Montserrat

Supòsit 3 (7 punts)

L'Ajuntament ha patit un atac de ransomware i ha encriptat part de la informació del sistema. Els usuaris comencen a trucar que no poden treballar, ja que no poden accedir als diversos sistemes informació (expedients, programa de nòmina, fitxers de xarxa...). La telefonia IP tampoc funciona correctament.

Davant d'aquesta situació quines accions prioritzaries i justifica-les.

Un cop resolt el problema i estabilitzada la situació, que s'hauria de tenir en compte perquè no es tornés a repetir aquesta incidència.

Accions (3.5 punts)
Prevenció d'atacs (3.5 punts)

*Davant d'un atac de ransomware que afecta un ajuntament, és fonamental seguir **el pla de contigència** o bé un pla d'actuació ràpid i estructurat per minimitzar els danys, restaurar els sistemes crítics i assegurar-se que l'incident no es repeteixi en el futur. Les accions a prioritzar són les següents:*

1. Aïllament immediat dels sistemes afectats

- *Desconnectar la xarxa: El primer pas és aïllar immediatament els sistemes afectats desconnectant-los de la xarxa (interna i externa) per evitar que el ransomware es propagui a altres dispositius i sistemes. Això inclou desconnectar equips, servidors i sistemes crítics que estiguin potencialment exposats.*
- *Suspensió temporal de la telefonia IP: Atès que la telefonia IP es basa en la xarxa de dades, també es podria veure afectada. És necessari aïllar aquests sistemes per evitar que el ransomware es propagui per altres serveis. Habilitar els desviaments necessàries per tal de poder atendre a la ciutadania en cas d'urgència.*

Justificació: L'aïllament limita la propagació de l'atac i evita que més dades siguin xifrades o que altres sistemes quedin inutilitzables. El ransomware sol expandir-se ràpidament per les xarxes interconnectades, per la qual cosa és vital tallar qualsevol possibilitat d'expansió.

2. Notificar l'incident als equips clau i responsables de ciberseguretat

- *Informar l'equip de TI i ciberseguretat: Cal informar immediatament l'equip tècnic intern i, si escau, contactar amb experts externs en ciberseguretat per començar a gestionar la situació. Agencia de Ciberseguretat de Catalunya. com el Centre Criptològic Nacional a Espanya*
- *Avisar la direcció de l'ajuntament: Informar els responsables de l'ajuntament de l'incident per coordinar l'estratègia de resposta i la comunicació interna i externa.*

Justificació: La resposta coordinada per part d'experts és clau per prendre les mesures adequades, establir la prioritat d'actuació i minimitzar l'impacte sobre els serveis públics.

3. Avaluar l'abast de l'atac

- *Determinar quins sistemes han estat afectats: Avaluar quins fitxers, servidors i sistemes han estat xifrats o inutilitzats pel ransomware. Prioritzar l'anàlisi dels sistemes més crítics per a l'ajuntament, com ara la gestió d'expedients, nòmines i fitxers de xarxa.*
- *Comprovar les còpies de seguretat: Revisar l'estat de les còpies de seguretat per assegurar-se que hi hagi versions no compromeses dels fitxers crítics.*

Justificació: És essencial identificar amb precisió què ha estat afectat per a poder planificar la restauració i reparació dels sistemes d'una manera ordenada i eficient.

4. Restaurar sistemes a partir de còpies de seguretat

- *Prioritzar els sistemes crítics: Restaurar els sistemes més essencials per al funcionament de l'ajuntament, començant pels servidors de dades, el sistema d'expedients i els sistemes de nòmines, si és possible, a partir de còpies de seguretat no compromeses.*
- *Verificar l'estat dels sistemes restaurats: És important revisar que els sistemes restaurats funcionin correctament i no estiguin infectats abans de tornar-los a posar en funcionament.*

Justificació: La restauració ràpida de còpies de seguretat permetrà reprendre les operacions crítiques, garantint que els serveis bàsics de l'ajuntament continuïn operatius.

5. Màxima comunicació en tot moment:

- *Informar als treballadors: Cal establir una comunicació clara amb els usuaris afectats per informar-los de la situació i els passos que s'estan prenent per solucionar-la.*

Mesures per evitar futurs atacs de ransomware:

Un cop l'incident s'ha resolt i els sistemes han estat restaurats, cal prendre una sèrie de mesures per assegurar-se que aquesta situació no es repeteixi:

1. Millorar la seguretat de les còpies de seguretat

- *Còpies de seguretat regulars i segregades: Assegurar que hi hagi còpies de seguretat regulars, que estiguin completament aïllades de la xarxa principal (per exemple, en un sistema de núvol segur o un sistema de còpia de seguretat físicament separat). Això impedirà que aquestes còpies també es vegin afectades per un atac.*
- *Provar les restauracions: Realitzar proves periòdiques per assegurar que les còpies de seguretat es poden restaurar ràpidament en cas de necessitat.*

Justificació: Tenir còpies de seguretat actualitzades i no afectades per l'atac és essencial per a la continuïtat del servei i la recuperació ràpida.

2. Formació dels treballadors

- *Formació en ciberseguretat: Realitzar sessions de formació regulars per al personal sobre bones pràctiques de seguretat, com ara evitar obrir correus electrònics sospitosos, enllaços o adjunts, i reconèixer possibles senyals d'atacs.*
- *Simulacions d'atacs: Executar exercicis de simulació d'atacs per preparar els empleats per a futures incidències i reduir la probabilitat de caure en trampes de phishing.*

Justificació: Els atacs de ransomware sovint comencen amb la manipulació dels usuaris (phishing), per la qual cosa és essencial que el personal estigui ben preparat per reconèixer aquests atacs.

3. Implementació de mesures de seguretat tècnica

- *Autenticació multifactor (MFA): Implementar autenticació multifactor per a tots els usuaris, especialment per a aquells amb accés a sistemes crítics o dades sensibles.*
- *Seguretat perimetral: Millorar els tallafocs, sistemes de detecció d'intrusos (IDS) i altres eines de seguretat per detectar i bloquejar atacs en temps real.*
- *Parches i actualitzacions de programari: Mantenir tots els sistemes i programari actualitzats per evitar vulnerabilitats que puguin ser explotades pels atacants.*
- *Segmentació de la xarxa: Dividir la xarxa en segments per tal que, en cas d'un atac, no es propagui fàcilment a altres parts de la infraestructura.*

Justificació: Aquestes mesures reforcen la seguretat dels sistemes i limiten la capacitat dels atacants de penetrar o propagar-se en la xarxa.

4. Monitoratge i resposta proactiva

- *Monitoratge constant: Implementar sistemes de monitoratge 24/7 que detectin comportaments sospitosos o accessos no autoritzats en temps real.*
- *Programes antivirus i antimalware avançats: Utilitzar programes de detecció i eliminació de ransomware, combinats amb eines d'anàlisi de comportament que detectin activitats anòmales.*

Justificació: La detecció proactiva permet identificar possibles amenaces abans que esdevinguin atacs reals, donant temps per actuar preventivament.