

PROVA PRÀCTICA

- Aquest exercici consisteix en respondre, en el **termini màxim de 2 hores**, els següents casos pràctics.
- La qualificació d'aquest exercici serà de 0 a 10 punts.
- Les persones que no aconseguixin un mínim de 5 punts seran eliminades.

CAS PRÀCTIC – 10 preguntes (1 punt cada pregunta)

1. Un usuari informa que no pot accedir a una aplicació corporativa que utilitza cada dia. Diu que ahir funcionava correctament, però avui li mostra un error de connexió. No s'han fet canvis coneguts en el sistema.

Explica quins passos seguiries per diagnosticar i resoldre el problema, indicant com verificaries si l'error és de l'usuari, de la seva estació de treball, de la xarxa o del servidor de l'aplicació. (1 punt)

Per diagnosticar i resoldre el problema d'un usuari que no pot accedir a una aplicació corporativa, seguiria un procediment estructurat per identificar si l'error prové de l'usuari, de l'equip, de la xarxa o del servidor.

1. Verificar si és un problema de l'usuari

Confirmar que l'usuari introdueix correctament les credencials.

Comprovar si el compte està bloquejat o caducat.

Validar si altres usuaris del mateix departament poden accedir-hi.

2. Comprovar l'estació de treball

Revisar la connexió a la xarxa (IP, gateway, DNS).

Fer un ping al servidor de l'aplicació per veure si hi ha connectivitat.

Comprovar si el navegador o client de l'aplicació mostra errors específics.

Revisar si hi ha actualitzacions pendents o canvis recents a l'equip.

3. Validar si és un problema de xarxa

Comprovar si l'usuari pot accedir a altres recursos municipals (intranet, carpetes de xarxa).

Verificar si hi ha talls o incidències a la VLAN o segment on està l'usuari.

Revisar si hi ha problemes amb el DNS que impedeixin resoldre el nom del servidor.

4. Comprovar el servidor de l'aplicació

Validar que el servei està actiu i responent.

Revisar logs del servidor per detectar errors de connexió o autenticació.

Comprovar si hi ha saturació de recursos (CPU, RAM, disc).

Confirmar que no s'han aplicat actualitzacions o canvis que hagin afectat el servei.

5. Resolució i seguiment

Aplicar la solució corresponent segons la causa detectada (desbloqueig de compte, reinici de servei, correcció de configuració, etc.).

Informar l'usuari i verificar que pot accedir-hi amb normalitat.

Registrar la incidència per mantenir traçabilitat i detectar possibles recurrències.

VALORACIÓ

1. Verificació del problema de l'usuari (0–0,2 punts)

0,2 punts — Comprova credencials, bloquejos, caducitats i si altres usuaris tenen el mateix problema. **0,1 punt** — Ho esmenta parcialment (p. ex. només comprovar credencials). **0 punts** — No ho esmenta o és incorrecte.

2. Revisió de l'estació de treball (0–0,2 punts)

0,2 punts — Revisa connectivitat (IP, gateway, DNS), fa ping al servidor, comprova navegador/client i canvis recents. **0,1 punt** — Menciona només algun element. **0 punts** — No ho esmenta.

3. Comprovació de la xarxa (0–0,2 punts)

0,2 punts — Verifica accés a altres recursos municipals, VLAN, incidències de segment, resolució DNS. **0,1 punt** — Ho esmenta de manera superficial. **0 punts** — No ho esmenta.

4. Revisió del servidor de l'aplicació (0–0,2 punts)

0,2 punts — Comprova estat del servei, logs, recursos del servidor i canvis recents. **0,1 punt** — Ho esmenta parcialment. **0 punts** — No ho esmenta.

5. Resolució i seguiment (0–0,2 punts)

0,2 punts — Aplica la solució adequada, valida amb l'usuari i registra la incidència. **0,1 punt** — Només resol o només valida, però no ambdós. **0 punts** — No ho esmenta.

2. Tens les taules següents: (1 punt)

TAULA CITES

id_cita
dni_ciutada
data_cita
servei
estat (pot ser: 'Activa', 'Anul·lada', 'Realitzada')

TAULA CIUTADANS

dni
nom
cognoms
telefon

Escriu una consulta SQL que mostri el nom, cognoms i telèfon dels ciutadans que tenen més d'una cita activa el mateix dia.

La consulta ha d'ordenar el resultat per data_cita i per nom.

RESPOSTA:

```
SELECT c.nom, c.cognoms, c.telefon, ci.data_cita
FROM CITES ci
JOIN CIUTADANS c
  ON ci.dni_ciutada = c.dni
WHERE ci.estat = 'Activa'
GROUP BY c.nom, c.cognoms, c.telefon, ci.data_cita
HAVING COUNT(ci.id_cita) > 1
ORDER BY ci.data_cita, c.nom;
```

JOIN per relacionar ciutadans amb les seves cites.

WHERE per filtrar només les cites actives.

GROUP BY per agrupar per ciutadà i dia.

HAVING COUNT > 1 per detectar ciutadans amb més d'una cita activa el mateix dia.

ORDER BY per ordenar el resultat de manera coherent.

VALORACIÓ

Definició correcta de VLAN (0–0,4 punts)

0,4 punts — Defineix VLAN com una *xarxa local virtual* que segmenta l'estructura física en xarxes lògiques independents. Explica que separa trànsit, crea dominis de broadcast i millora l'organització. **0,2–0,3 punts** — Defineix VLAN de manera parcial però correcta (p. ex. “segmentació de xarxa”). **0,1 punt** — Menciona algun concepte relacionat però incomplet o poc precís. **0 punts** — Definició incorrecta o absent.

2. Utilitat en una xarxa municipal (0–0,4 punts)

0,4 punts — Explica clarament almenys *tres* usos rellevants en entorns municipals, com:

- Aïllar departaments (Policia, Serveis Socials, OAC, etc.)
- Millorar la seguretat i confidencialitat
- Reduir trànsit broadcast i millorar rendiment
- Aplicar polítiques de xarxa diferenciades
- Separar serveis (telefonía IP, videovigilància, servidors)

0,2–0,3 punts — Menciona usos correctes però de manera parcial o poc detallada. **1 punt** — Només indica un ús o ho fa de manera molt superficial. **0 punts** — No explica cap utilitat o és incorrecte.

3. Claredat i estructura de la resposta (0–0,2 punts)

0,2 punts — Resposta clara, ordenada i coherent. **0,1 punt** — Resposta entenedora però amb desordre o manca de precisió. **0 punts** — Resposta confusa o difícil d'interpretar.

3. Un usuari ens alerta que ha accedit a un link rebut per correu electrònic i que l'equip ha començat a comportar-se de manera estranya. Quines actuacions duries a terme ? (1 punt)

Davant d'una alerta d'infecció per accés a un enllaç maliciós, seguiria aquestes actuacions:

1. Contenció immediata

- Aïllar l'equip afectat de la xarxa (desconnectar cable o WiFi)
- Evitar la propagació a altres equips

2. Anàlisi de la incidència

- Revisar l'alerta de l'antivirus (tipus d'amenaça)
- Identificar l'origen (correu, URL, fitxer descarregat)
- Comprovar si hi ha altres equips afectats

3. Eliminació i neteja

- Executar un escaneig complet amb l'antivirus/antimalware
- Eliminar o posar en quarantena els fitxers maliciosos
- Revisar processos actius i programes instal·lats recentment

4. Mesures de seguretat

- Canviar credencials de l'usuari afectat
- Comprovar possibles accessos no autoritzats

- Revisar logs i sistemes de seguretat

5. Gestió del correu

- Analitzar el correu (phishing)
- Bloquejar el remitent o domini
- Avisar la resta d'usuaris per prevenir incidents similars

6. Recuperació

- Restaurar el sistema si cal (còpia de seguretat)
- Verificar que l'equip torna a funcionar correctament

7. Prevenció i millora

- Informar i formar l'usuari (bones pràctiques)
- Actualitzar antivirus i sistemes
- Documentar la incidència

8. Comunicació

- Comunicar l'incident de seguretat al comitè de seguretat
- Comunicar l'incident a l'Agència de Ciberseguretat de Catalunya i Autoritat de Protecció de dades si procedeix.

En resum: aïllar, analitzar, eliminar, recuperar i prevenir, seguint un procediment ordenat de gestió d'incidents.

VALORACIÓ

- **Contenció: 0-0,2 punts**
- **Anàlisi: 0-0,2 punts**
- **Recuperació: 0-0,2 punts**
- **Prevenció: 0-0,2 punts**
- **Comunicació: 0-0,2 punts**

4. Explica la diferència entre idCAT Certificat, idCAT Mòbil i Cl@ve. (1 punt)

idCAT Certificat

És un certificat digital instal·lat a l'ordinador (o en un dispositiu segur) que identifica l'usuari de manera robusta.

Permet signar documents electrònicament, fer tràmits complets i accedir a serveis que requereixen un nivell de seguretat alt.

És emès pel Consorci AOC i s'utilitza molt en administracions catalanes.

idCAT Mòbil

És un sistema d'identificació sense certificat, basat en el telèfon mòbil.

Funciona amb codi d'un sol ús (OTP) enviat per SMS o notificació.

És més senzill d'utilitzar i no requereix instal·lació, però no permet signatura digital avançada, només autenticació i validació d'identitat.

Cl@ve

És el sistema d'identificació electrònica de l'Administració General de l'Estat.

Inclou diferents nivells:

Cl@ve PIN (codi temporal, similar a idCAT Mòbil)

Cl@ve Permanent (usuari + contrasenya)

Certificat o DNle (nivell alt)

En resum

idCAT Certificat → Certificat digital instal·lat; màxima seguretat; permet signar; de l'AOC
idCAT Mòbil → Identificació via mòbil; fàcil; no permet signatura avançada; de l'Administració General de l'Estat; de l'AOC
Cl@ve → Sistema estatal; diversos nivells; de l'Administració General de l'Estat.

VALORACIÓ

1. Explicació correcta d'idCAT Certificat (0–0,3 punts)

0,3 punts — Explica que és un *certificat digital instal·lat*, d'alt nivell de seguretat, que permet *signatura electrònica avançada* i autenticació robusta. **0,2 punts** — Explicació parcial però correcta (p. ex. “certificat digital per fer tràmits”). **0,1 punt** — Menciona algun element però de manera superficial o incompleta. **0 punts** — No ho esmenta o és incorrecte.

2. Explicació correcta d'idCAT Mòbil (0–0,3 punts)

0,3 punts — Indica que és un sistema d'identificació *sense certificat*, basat en *codi d'un sol ús* enviat al mòbil, fàcil d'usar i que *no permet signatura avançada*. **0,2 punts** — Explicació parcial però correcta. **0,1 punt** — Menciona només que funciona amb el mòbil o amb SMS. **0 punts** — No ho esmenta o és incorrecte.

3. Explicació correcta de Cl@ve (0–0,3 punts)

0,3 punts — Explica que és el sistema d'identificació de l'*Administració General de l'Estat*, amb diferents nivells (Cl@ve PIN, Permanent, Certificat/DNle) i necessari per a tràmits estatals. **0,2 punts** — Explicació parcial però correcta. **0,1 punt** — Només diu que és un sistema estatal. **0 punts** — No ho esmenta o és incorrecte.

4. Claredat i estructura de la resposta (0–0,1 punt)

0,1 punt — Resposta clara, ordenada i fàcil d'entendre. **0 punts** — Resposta confusa, desordenada o difícil de seguir.

5. Un usuari diu que “Internet no funciona”. Escriu l'arbre de comprovacions que faries. (1 punt)

1. Comprovacions bàsiques amb l'usuari

- L'usuari té **cable connectat** o **Wi-Fi activat**.
- Hi ha altres equips al mateix espai que **sí tenen Internet**.
- Ha provat de reiniciar el navegador o l'equip.

2. Comprovar la connectivitat local

- Comprovar si l'equip té **adreça IP**, **gateway** i **DNS** correctes.
- Fer **ping al gateway**.
 - Si no respon → problema local o de xarxa interna.
- Fer **ping a una IP externa** (ex. 8.8.8.8).
 - Si respon → el problema és DNS.
 - Si no respon → problema de sortida a Internet.

3. Comprovar la resolució DNS

- Fer **ping a un domini** (ex. google.com).
 - Si IP respon però domini no → problema de DNS.

- Revisar configuració DNS (manual/automàtica).
- Provar amb un DNS alternatiu.

4. Comprovar la xarxa del departament / VLAN

- Validar que l'equip està a la **VLAN correcta**.
- Comprovar si hi ha incidències al **switch** o al segment.
- Revisar si altres usuaris de la mateixa VLAN tenen el mateix problema.

5. Comprovar el tallafoc o proxy municipal

- Validar si el **firewall** està bloquejant trànsit.
- Comprovar si el **proxy** està configurat i operatiu.
- Revisar si hi ha restriccions aplicades a l'usuari.

6. Comprovar la sortida general a Internet

- Verificar si la **connexió WAN** de l'Ajuntament està operativa.
- Revisar si hi ha incidències amb el **proveïdor d'Internet**.
- Comprovar logs del tallafoc per detectar talls o saturació.

7. Accions finals

- Aplicar la solució segons la causa detectada.
- Validar amb l'usuari que Internet funciona.
- Registrar la incidència per traçabilitat.

VALORACIÓ

- **0,20 punts** si inclou comprovacions bàsiques amb l'usuari (connexió física o Wi-Fi, altres equips, reinici bàsic).
- **0,20 punts** si revisa la connectivitat local (adreça IP, gateway, DNS, ping al gateway).
- **0,20 punts** si comprova la connectivitat externa (ping a una IP pública i interpretació del resultat).
- **0,20 punts** si comprova la resolució DNS (ping a dominis i identificació d'error DNS).
- **0,20 punts** si revisa aspectes de xarxa més amplis: VLAN, incidències de segment, proxy, firewall o sortida WAN.

6. S' ha de crear una pàgina web molt simple per mostrar informació bàsica d'un servei municipal. La pàgina ha d'incloure un títol, un subtítol, un paràgraf i un enllaç que porti a la web de l'Ajuntament. (1 punt)

Escriu un fragment d'HTML que contingui:

1. Un títol principal (nivell <h1>).
2. Un subtítol (nivell <h2>).
3. Un paràgraf amb text descriptiu.
4. Un enllaç (<a>) que apunti a <https://www.blanes.cat>.

RESPOSTA:

```
<!DOCTYPE html>
<html>
<head>
  <title>Servei Municipal</title>
```

```
</head>
<body>

  <h1>Informació del Servei Municipal</h1>
  <h2>Atenció Ciutadana</h2>

  <p>
    Aquest servei ofereix informació i suport als ciutadans en tots els tràmits municipals, incloent
    consultes, gestions i sol·licituds.
  </p>

  <a href="https://www.massanetdelaselva.cat" target="_blank">
    Visita la web de l'Ajuntament de Maçanet de la Selva
  </a>

</body>
</html>
```

VALORACIÓ

```
<!DOCTYPE html>
<html>
<head>
  <title>Servei Municipal</title>
</head>
<body>

  <h1>Informació del Servei Municipal</h1>
  <h2>Atenció Ciutadana</h2>

  <p>
    Aquest servei ofereix informació i suport als ciutadans en tots els tràmits municipals, incloent
    consultes, gestions i sol·licituds.
  </p>

  <a href="https://www.massanetdelaselva.cat" target="_blank">
    Visita la web de l'Ajuntament de Maçanet de la Selva
  </a>

</body>
</html>
```

- **0,2 punts**

```
<head>
  <title>Servei Municipal</title>
</head>
```

- **0,2 punts**

```
<body>
```

- **0,2 punts**

```
<h1>
```

```
<h2>
```

- **0,2 punts**

```
<p>
```

- **0,2 punts**

```
<a href....> </a>
```

7. Explica la diferència entre xifratge simètric i asimètric. (1 punt)

Xifratge simètric

- Utilitza **una única clau** per xifrar i desxifrar.
- És **molt ràpid** i eficient, adequat per grans volums de dades.
- El problema principal és la **distribució segura de la clau**: si algú l'intercepta, pot desxifrar tota la informació.
- Exemples: **AES, DES, 3DES**.

Xifratge asimètric

- Utilitza **dues claus diferents**:
 - **Clau pública** per xifrar
 - **Clau privada** per desxifrar
- És més **segur per compartir claus**, perquè la clau privada no es transmet mai.
- És **més lent** que el simètric, per això sovint s'utilitza només per establir connexions segures o intercanviar claus.
- Exemples: **RSA, ECC**.

En resum:

- **Simètric** → una clau, ràpid, problema de distribució de la clau.
- **Asimètric** → dues claus, més segur per intercanvi, però més lent.

VALORACIÓ

- **0,40 punts** si explica correctament que el **xifratge simètric utilitza una única clau** per xifrar i desxifrar, és ràpid i té el problema de la distribució segura de la clau.
- **0,40 punts** si explica correctament que el **xifratge asimètric utilitza dues claus diferents** (pública i privada), és més segur per intercanviar claus però més lent.
- **0,20 punts** si inclou un **resum comparatiu clar** (per exemple: "simètric = una clau; asimètric = dues claus") o aporta exemples correctes (AES, RSA, etc.).

8. Què és el doble factor d'autenticació i per què és important. (1 punt)

El **doble factor d'autenticació (2FA)** és un mecanisme de seguretat que requereix **dos elements diferents** per verificar la identitat d'un usuari quan accedeix a un sistema, aplicació o servei. Normalment combina **alguna cosa que saps**, **alguna cosa que tens** o **alguna cosa que ets**.

El 2FA obliga l'usuari a validar-se amb **dos factors independents**, per exemple:

- **Alguna cosa que saps** → una contrasenya o PIN
- **Alguna cosa que tens** → un mòbil amb SMS, una app d'autenticació, una targeta criptogràfica, un token
- **Alguna cosa que ets** → empremta digital, reconeixement facial

Això vol dir que, encara que un atacant obtingui la contrasenya, **no podrà accedir** sense el segon factor.

El 2FA és essencial perquè:

- **Redueix dràsticament el risc de robatori de comptes**, fins i tot si la contrasenya ha estat compromesa.
- **Evita accessos no autoritzats** en entorns sensibles com l'administració pública.
- **Protegeix dades personals i informació municipal crítica**.

- **És un requisit recomanat per l'ENS** en processos d'autenticació d'alts privilegis o accés a dades sensibles.
- **Bloqueja atacs habituals** com phishing, força bruta o reutilització de contrasenyes filtrades.

En resum

El doble factor d'autenticació afegeix una capa extra de protecció i és una mesura clau per garantir la seguretat dels sistemes municipals i de les dades dels ciutadans.

VALORACIÓ

- **0,40 punts** si explica correctament què és el **doble factor d'autenticació (2FA)**: un sistema que requereix dos factors independents (alguna cosa que saps, que tens o que ets).
- **0,40 punts** si descriu **per què és important**: augmenta la seguretat, evita accessos no autoritzats, protegeix dades sensibles, redueix riscos en cas de contrasenya compromesa, és recomanat per l'ENS, etc.
- **0,20 punts** si aporta un **exemple clar** (SMS, app d'autenticació, token, biometria) o un resum comparatiu que demostrï compre

9. Un equip obté IP del DHCP però no té accés a cap recurs de xarxa. Explica tres possibles causes i com les verificaries. (1 punt)

Quan un equip rep una IP del DHCP però no pot accedir a cap recurs de xarxa, vol dir que **la configuració bàsica funciona**, però hi ha un problema en algun punt del camí cap als recursos municipals. Tres causes habituals són:

1. Gateway incorrecte o inoperatiu

Causa: El DHCP pot haver assignat un gateway erroni, o el gateway de la VLAN pot estar caigut.

Com verificar-ho:

- Comprovar la configuració IP amb ipconfig o equivalent.
- Fer **ping al gateway**.
 - Si no respon → problema de gateway o de xarxa interna.
- Comprovar si altres equips de la mateixa VLAN tenen el mateix problema.

2. Problema de VLAN o configuració del port del switch

Causa: L'equip pot estar en una **VLAN equivocada**, o el port del switch pot estar mal configurat (canvi de VLAN, port en err-disabled, etc.).

Com verificar-ho:

- Validar amb l'equip de xarxes la **VLAN assignada al port**.
- Comparar amb un altre equip que funcioni correctament.
- Comprovar si l'equip obté una IP coherent amb la VLAN esperada.
 - Si la IP és correcta però no hi ha trànsit → possible bloqueig o error al switch.

3. DNS incorrecte o no funcional

Causa: L'equip pot tenir DNS assignats però aquests no resolen noms, cosa que impedeix accedir a recursos municipals (servidors, aplicatius, portals interns).

Com verificar-ho:

- Fer **ping a una IP interna** (per exemple, un servidor).
 - Si respon → la xarxa funciona, però el DNS falla.
- Fer **ping a un nom de domini intern**.
 - Si no resol → problema de DNS.
- Comprovar quins DNS assigna el DHCP i si són els correctes.

Altres causes possibles

- Tallafof local bloquejant trànsit.
- Polítiques NAC / 802.1X que posen l'equip en VLAN de convidats.
- Rutes estàtiques incorrectes.
- Problemes al servidor DHCP (assignació d'opcions incompletes).

VALORACIÓ

- **0,35 punts** si identifica i explica correctament una **primera causa plausible** (per exemple: gateway incorrecte, gateway caigut, problema de routing) i descriu **com la verificaria** (ping al gateway, comprovació de configuració IP, comparació amb altres equips).
- **0,35 punts** si identifica i explica una **segona causa plausible** (per exemple: VLAN incorrecta, port del switch mal configurat, err-disabled) i indica **com ho comprovava** (validació de VLAN, revisió del port, coherència de la IP assignada).
- **0,30 punts** si identifica i explica una **tercera causa plausible** (per exemple: DNS incorrecte, DNS caigut, firewall local bloquejant trànsit) i descriu **com ho verificaria** (ping a IP interna, ping a nom, revisió de DNS assignats, desactivació temporal del firewall).

10. Un usuari informa que perd la connexió a la xarxa LAN de manera intermitent. Indica tres possibles causes relacionades i com les diagnosticaries. (1 punt).

Quan la desconexió és **intermitent**, gairebé sempre hi ha un problema físic o de negociació entre l'equip i el switch.

Tres causes habituals són:

1. Cablejat defectuós o mal grimpat

Causa: Un cable de xarxa deteriorat, amb el connector mal grimpat pot provocar talls puntuals, errors CRC i renegociacions de velocitat.

Com verificar-ho:

- Substituir temporalment el cable per un de nou i homologat (Cat5e/Cat6).
- Revisar el port del patch panel i el cablejat estructurat.
- Comprovar al switch si hi ha **errors CRC**, **late collisions** o **flapping** del port.

2. Port del switch defectuós o mal configurat

Causa: El port pot tenir problemes físics, estar saturat, tenir una configuració incorrecta (velocitat/duplex) o estar patint microtalls.

Com verificar-ho:

- Moure el cable a **un altre port del switch** i observar si el problema desapareix.
- Revisar els logs del switch per detectar **link up/down** freqüents.
- Comprovar la configuració de **velocitat i duplex** (ha de ser "auto" en la majoria d'entorns).

3. Targeta de xarxa (NIC) de l'equip amb fallades

Causa: La NIC pot tenir un driver obsolet, problemes de maquinari o estar forçant una velocitat/duplex incompatible.

Com verificar-ho:

- Actualitzar drivers de la NIC.
- Revisar l'**Event Viewer** de Windows per errors de xarxa.
- Forçar la NIC a **auto-negociació** i comprovar si el port del switch negocia correctament.
- Provar amb un adaptador USB-Ethernet per descartar problema físic.

Altres causes que es poden mencionar

- Interferències elèctriques en el cablejat.
- Configuració d'energia de Windows que desactiva la NIC.
- Bucle de xarxa en un altre punt de la LAN.

VALORACIÓ

- **0,35 punts** si identifica i explica correctament una **primera causa plausible** relacionada amb **cablejat** (cable defectuós, mal crimpat, interferències) i descriu **com la verificaria** (substitució del cable, revisió de CRC al switch, proves físiques).
- **0,35 punts** si identifica i explica una **segona causa plausible** relacionada amb el **port del switch** (port defectuós, configuració incorrecta, flapping) i indica **com ho comprovava** (moure a un altre port, revisar logs, validar negociació).
- **0,30 punts** si identifica i explica una **tercera causa plausible** relacionada amb la **NIC de l'equip** (drivers, maquinari, negociació incorrecta) i descriu **com ho verificaria** (actualitzar drivers, revisar Event Viewer, provar adaptador alternatiu).