

DNI.:

**PROCÉS SELECTIU D'UN/A TÈCNIC/A ESPECIALISTA EN INFORMÀTICA, EN RÈGIM FUNCIONARI DE CARRERA EN LA PLANTILLA DE L'AJUNTAMENT DE MONTORNÈS DEL VALLÈS I LA CREACIÓ D'UNA BORSA DE TREBALL PER COBRIR POSSIBLES VACANTS I SUBSTITUCIONS.**

**Segona prova. Prova teòric pràctica.**

Aquesta prova serà de caràcter obligatori i eliminatori i consistirà en el desenvolupament de tres supòsits pràctics relacionats amb les funcions a desenvolupar i basades en el temari que consta a les bases.

Aquesta prova serà qualificada amb 45 punts, i quedaran eliminades les persones que no tinguin una puntuació igual o superior a 22,5 punts.

El temps per realitzar aquesta prova és de 2 hores i 30 minuts.

**SUPÒSITS TEÒRIC PRACTIQUES (45 punts):**

- 1. L'Ajuntament de Montornès del Vallès, no disposa d'un pla de còpies de seguretat i vol implementar un pla de backups nou. La infraestructura que es disposa, de forma resumida, és de 3 servidors físics (2 ubicats al CPD principal i 1 a un CPD ubicat en una altre dependència municipal) i sobre aquests existeixen diferents servidors virtuals que contenen les aplicacions municipals.**

**Explica com dissenyaries i implementaries un pla de còpies de seguretat per l'Ajuntament de Montornès del Vallès. Es valorarà el detall i coherència de la solució proposada. (15 punts).**

*Guia de valoració.*

- *Implementació d'estratègia de backup 3-2-1-1-0 (tope puntuació) o 3-2-1.*
- *Mantenir al menys 3 còpies de seguretat de les dades.*
- *Emmagatzemar les còpies en 2 suports diferents (per exemple: disc i cintes).*
- *Tenir al menys 1 còpia fora de les instal·lacions (off-site).*
- *Còpia d'últim recurs al núvol.*
- *Tenir al menys 1 còpia off-line (o immutable).*
- *Disposar empresa que emmagatzema còpies externes.*
- *Assegurar que hi ha 0 errors en les còpies de seguretat (fent restauracions de prova).*
- *Documentar les proves que es fan i les restauracions de proves dins un pla procedimentat.*
- *Redacció d'un pla de contingència.*



DNI.:

**2. L'Ajuntament de Montornès del Vallès vol substituir el sistema de telefonia actual, atès que és obsolet, per un altre basat en Telefonia IP.**

**Com realitzaries la implementació del sistema esmentat, el principal requeriment és que el sistema ha de ser "on premise" (no al núvol). Es valorarà el detall i coherència de la implementació proposada (15 punts).**

*Guia de valoració.*

- *Implementació de servidor telefonia IP i backup del mateix.*
- *Configuració de una vlan per "telefonia IP" separada per cada switch.*
- *Si es planteja FreePBX i ho justifiquen amb l'estalvi de costos.*
- *Canvi de terminals per terminal IP o softphones.*
- *Si comenta el tema d'aprofitar un punt de xarxa i connectar el pc al telèfon.*
- *Implementació de sistema per parlar amb castos des de el PC*
- *Integració amb directori actiu AD.*
- *Càrrega agenda telefònica centralitzada.*
- *Configuració de rutes de salt als diferents departaments.*
- *Configuració dels diferents DDI (punts d'entrada 935721110 o 935721170) i que cadascú tingui un grup de salt i un missatge de benvinguda segons horari.*
- *Integració amb eines externes de videoconferències com ara Teams.*
- *Proves de rendiment del sistema.*
- *Formació del sistema als usuaris.*
- *Contractació d'un primari o SIP al 10 sortides mínim amb operadors.*
- *Configuració de gravació de trucades (especialment per Policia Local).*
- *Modificar regles del Firewall per permetre tràfic de telefonia IP cap al sistema de l'operador.*
- *Tot ha de quedar configurat per tenir una sortida a Internet principal i de backup, així com sistema d'últim recurs com una sortida mòbil, satel.lital o similar.*
- *Dotar d'extensions curtes a cada telèfon.*
- *Integració amb telefonia mòbil i que els mòbils també tinguin numeració curta.*
- *Crear una plantilla de configuració per els diferents models de telèfons.*

**3. Arribes a treballar a l'Ajuntament, la resta del departament TIC està de vacances i trobes que els usuaris t'avisen que no poden accedir a les seves carpetes al servidor, tampoc a aplicacions municipals ni correu electrònic, i et trobes que cap fitxer del servidor es pot obrir i únicament pots obrir un fitxer txt on llegeixen que tots els fitxers s'han encriptat i es demana el pagament de 30 bitcoins per part de l'Ajuntament a un tercer, però sembla que les Bases de dades municipals no estan afectades. (15 punts).**

**¿Que pot estar passant?**

**¿Davant aquesta actuació com actuaries?**

**¿Quines mesures implementaries a futur, per evitar que no torni a passar?**

*Guia de valoració*



DNI.:

1. *L'Ajuntament patit un ciberincident de Ransomware, és un incident de ciberseguretat greu (1 punt).*
2. *Com actuar:*
  - 2.1. *Primer de tot Identificar l'amenaça i l'abast de l'incident, fer una primera avaluació.*
    - 2.1.1. *Guardar fitxer de text amb nota de rescat.*
    - 2.1.2. *Mostra de fitxers afectats.*
    - 2.1.3. *Mostra del ransomware, del correu de phishing, arxiu ofimàtic o de qualsevol evidència que permeti analitzar el codi nociu.*
    - 2.1.4. *Evidències de xarxes i inventari (diagrama de xarxa, llistat de servidors i actius principals, adreçaments ip, logs de xarxa, antivirus, EDR, antispam, accessos VPN, etc...)*
  - 2.2. *Contenir: L'objectiu es evitar que el mal s'expandeixi a tota la xarxa de l'Ajuntament.*
    - 2.2.1. *No apagar ni reiniciar els equips. No encendre equips apagats. Exclusivament en cas de ransomware, aïllar els equips d'Internet i de la xarxa corporativa.*
    - 2.2.2. *Aïllar els servidors de fitxers i les bases de dades corporatives, i si cal tirar del cable.*
    - 2.2.3. *Desactivar connexions remotes VPN, RDP o SSH.*
    - 2.2.4. *Aïllar sistema de back-up i sobretot el servidor de les BBDD.*
    - 2.2.5. *Intentar no donar pistes als atacants.*
    - 2.2.6. *Capturar proves volàtils*
    - 2.2.7. *Mai pagar i si cal que siguin els CCSS els que contactin amb els ciberdelinqüents o seguint les seves indicacions.*
  - 2.3. *Informar i notificar*
    - 2.3.1. *Informar-ne el Responsable de Seguretat de l'entitat*
    - 2.3.2. *Trucar al CATALONIA CERT (ciberseguretat de Catalunya) o CCN CERT i aplicar accions immediates que ens indiquin.*
    - 2.3.3. *Anàlisi inicial de l'incident i identificació conjunta de les figures a implicar en els equips de treball.*
    - 2.3.4. *El responsable de Seguretat convocarà al Comitè de Crisi de l'Entitat i es formaran els equips de treball.*
    - 2.3.5. *En cas d'afectar dades personals, informar-ne el DPD que avaluarà si cal comunicar-ho a APDCAT.*
    - 2.3.6. *Que Premsa de l'Ajuntament informi a la ciutadania, però que deixin treballar als tècnics.*
  - 2.4. *Mitigar i recuperar el sistema*
    - 2.4.1. *Sempre en un entorn aïllat i restablint serveis poc a poc*
    - 2.4.2. *Recuperar de la última còpia de seguretat bona.*
    - 2.4.3. *Recuperar AD primer.*
    - 2.4.4. *Canvis total de credencials total.*
    - 2.4.5. *Evitar eliminar proves per fer després investigació de l'incident.*
    - 2.4.6. *Seguir les pautes de ciberseguretat de Catalunya*



DNI.:

- 2.4.7. *Inventariat d'actius i fitxers afectats.*
- 2.4.8. *Actualització o parxeig d'equips.*
- 2.4.9. *Actualització de regles a antispam i firewalls, segons estudi de tràfic de xarxa del ransomware.*
- 2.4.10. *Actualitzar regles de EDR per bloquejar processos de sistema maliciosos.*

3. *Accions a futur:*

- 3.1. *Implementació de mesures del ENS*
- 3.2. *Segmentació de la xarxa informàtica*
- 3.3. *Implementació microclaudia , EDR i SIEM.*
- 3.4. *Revisió implementació Firewall.*
- 3.5. *Afegir-nos al SOC de la Generalitat (o contractar-ne un).*
- 3.6. *Establir un pla de contingència.*
- 3.7. *Ajustar les mesures de backups, si cal.*
- 3.8. *Creació d'un playbook.*
- 3.9. *Implementació de polítiques de seguretat de domini.*
- 3.10. *Lliçons apreses post incident, no acaba el incident un cop està tot en producció.*
- 3.11. *Implementació de HoneyPot.*

[https://www.localret.cat/wp-content/uploads/2025/10/Protocol-breu-davant-un-incident-de-seguretat\\_revisatACC-correct-1.pdf](https://www.localret.cat/wp-content/uploads/2025/10/Protocol-breu-davant-un-incident-de-seguretat_revisatACC-correct-1.pdf)

<https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/5867-ccn-cert-bp-21-gestion-de-incidentes-de-ransomware-1/file?format=html>