
PROCÉS SELECTIU PER COBRIR 41 PLACES DE LA PLANTILLA DE PERSONAL FUNCIONARI I PERSONAL LABORAL, DELS GRUPS A1, A2 I C1 MITJANÇANT CONCURS-OPOSICIÓ VIA D'ACCÉS PER PROMOCIÓ INTERNA.

EXPEDIENT: 2025/000042220

INSTRUCCIONS GENERALS:

- La prova s'ha de respondre amb bolígraf negre o blau (no es pot fer servir retolador ni llapis, ni corrector líquid o en cinta).
- No es podrà fer cap tipus d'anotació al full de resposta, encara que sigui en llapis.
- Les bosses, documentació, etc. hauran d'estar al terra.
- No es podrà consultar material de suport.
- Els mòbils i smartwatch, hauran d'estar apagats o en mode avió durant la realització de les proves.
- Davant una actitud sospitosa, es farà una anotació al full de l'examen i s'informarà de la incidència als membres de l'òrgan de selecció.
- No es podrà començar la prova fins que es doni l'ordre.
- És obligatori mantenir-se en silenci durant la realització de la prova.
- L'òrgan de selecció i l'equip de suport es comunicarà mitjançant grup de WhatsApp, motiu pel qual podreu observar que anem mirant el mòbil.
- Quan acabeu, podreu lliurar la prova i sortir de l'aula. No us podreu quedar amb cap full, ni encara que es tracti d'un esborrany.

Instruccions FULL RESPOSTA:

- A l'apartat *DI*: haureu de fer constar el vostre DNI, sense lletra, a l'espai habilitat al full de respostes. **NO** haureu de fer constar, en cap cas, nom i/o cognoms, **de fer-ho la vostra prova no es corregirà.**
- A l'apartat *Model*: haureu d'indicar 1 o 2, segons s'escaigui.
- Tant el vostre DI (DNI, sense lletra) com el model de la prova, també els haureu d'indicar a la part superior dreta amb X.
- La resposta correcta s'ha de marcar amb una X. No cal remarcar molt la X ni que aquesta ocupi tot el requadre.
- Per anul·lar una resposta cal ombrejar la part central fins que la X no sigui visible.

Referent a la prova teòrica

- **Puntuació màxim 30 punts i mínim 15 per superar-la. Caràcter eliminatori.**
- El full de respostes conté 100 preguntes. **Haureu de respondre des de la 1 a la 22, deixant en blanc des de la 23 a la 100.**
- **Criteris de correcció:**
 - La resposta **CORRECTA** puntua +1,50
 - Les respostes **INCORRECTES**, en **BLANC** o amb **més d'una resposta** ni puntuen, ni descompen.

Es donarà un avís **quan faltin 15 minuts i 5 minuts per acabar**. Un cop acabi el temps, no es podrà escriure res més. Si es segueix escrivint, es farà una anotació al full de la prova i s'informarà de la incidència als membres de l'òrgan de selecció. Quan acabi el temps, s'haurà lliurar la prova. No us podreu quedar amb cap full, encara que es tracti d'un esborrany.

Correcció: Els aspirants rebran un correu electrònic individual, amb la puntuació provisional obtinguda. Els resultats s'elevaran a definitius mitjançant acta de sessió de l'òrgan de selecció, la qual es publicarà i es podrà consultar a la pàgina web, al lloc habitual.



Ajuntament
de Mataró

AJMPI-01 Tècnic/a Superior, subgrup A1, SSIT

MODEL 1

Supòsit pràctic

L'Ajuntament de Mataró ha posat en marxa el **Pla de Transformació municipal**, que en el seu *Objectiu 10* estableix la necessitat d'assegurar una evolució tecnològica contínua per esdevenir resilients en un entorn en canvi permanent. Aquest objectiu incorpora cinc línies d'actuació estratègiques que han de condicionar les decisions tècniques dels propers mesos.

La **línia 1** preveu l'ampliació de les actuacions de ciberseguretat i cibervigilància, incloent-hi la implantació d'un **Centre d'Operacions de Ciberseguretat (SOC)** capaç de monitorar en temps real els sistemes, correlacionar esdeveniments i detectar possibles intrusions. Aquest SOC ha de centralitzar alertes, integracions SIEM, gestió d'incidents i informes de seguretat.

La **línia 2** fixa com a prioritat obtenir la certificació de l'**Esquema Nacional de Seguretat (ENS)**, cosa que obliga a revisar l'arquitectura de sistemes, aplicar mesures de seguretat per a cada categoria, implementar registres d'activitat, reforçar l'autenticació, formalitzar procediments i establir auditories periòdiques.

La **línia 3** estableix l'elaboració d'un **Pla d'evolució tecnològica**, que ha de determinar el full de ruta d'inversions, l'actualització del CPD, la modernització del programari corporatiu, l'adopció d'arquitectures modulars i API-first, la renovació de la virtualització i la racionalització d'aplicacions.

La **línia 4** desplega la **Pataforma de ciutat intel·ligent** basada en FIWARE, orientada a integrar dades heterogènies de mobilitat, medi ambient, espai públic i serveis municipals. Aquest projecte incorpora models d'IA per detectar anomalies i ha de connectar-se directament amb el GIS municipal per representar la informació en capes geoespacionals.

Finalment, la **línia 5** fixa la necessitat d'un **Pla Integral de Resiliència i Continuïtat de serveis**, que inclou estratègies de recuperació, redundància de serveis crítics, alta disponibilitat dels sistemes i plans de comunicació interna en situacions d'incidència.

Aquestes línies afecten directament al Servei de Sistemes d'Informació i Telecomunicacions (SSIT) que haurà de decidir quines actuacions dur a terme per donar compliment a les diferents línies.

Però paral·lelament, el SSIT també està desenvolupant una **nova aplicació per a la gestió de llicències municipals** mitjançant Oracle APEX, amb arquitectura web modular i backend sobre Oracle Database. I durant la revisió del prototip s'han detectat problemes de rendiment i desviacions del calendari del projecte perquè l'equip no ha seguit la metodologia de gestió establerta.

En aquest context, el servei d'atenció a l'usuari del SSIT ha rebut una trucada del departament Recursos Humans informant que l'aplicació de Gestió de Personal no està enviant correctament les dades al gestor d'expedients electrònic. L'usuari indica que, en intentar remetre un expedient, apareix el missatge "**Error 503 – servei d'integració no disponible**". El tècnic valida l'error, comprova que el servei SOAP/REST no responen i detecta que el servidor intermediari presenta un consum de CPU anòmal i els logs mostren errors de connexió amb la base de dades.

1. En el marc de les actuacions de la línia 1, es proposa l'ampliació de les fonts de logs del SIEM, això significa:

- a) Activar més regles de firewall per reduir trànsit.
- b) Duplicar el nombre de servidors de monitoratge.
- c) Incorporar nous sistemes, aplicacions i dispositius perquè enviïn els seus registres al SIEM.
- d) Generar informes mensuals automàtics sense modificar la configuració.

2. En un ajuntament de dimensió mitjana com Mataró, quin model de SOC és el més habitual i viable?

- a) Un SOC 100% intern, amb tot el monitoratge i resposta dins del mateix ajuntament.
- b) Un SOC completament al núvol gestionat només per un únic proveïdor.
- c) Un SOC en modalitat híbrida: monitoratge extern 24/7 i resposta i gestió interna per part del personal municipal.
- d) Un SOC basat en tecnologia blockchain per validar cada paquet de xarxa.

3. Quan es parla de “detecció d’amenaces avançades”, s’està fent referència principalment a:

- a) Sistemes de filtratge antivirus tradicionals basats només en signatures.
- b) Bloquejar manualment adreces IP sospitoses cada vegada que es detecti trànsit anòmal.
- c) Solucions EDR/XDR amb analítica comportamental capaç d’identificar activitats sospitoses, moviments laterals i anomalies en temps real.
- d) Instal·lar sensors de temperatura als racks del CPD per evitar sobreescalfaments.

4. Els sistemes IDS/IPS tenen com a funció principal:

- a) Generar còpies de seguretat automàtiques.
- b) Executar màquines virtuals i gestionar hipervisors.
- c) Detectar activitat anòmla i bloquejar trànsit potencialment maliciós.
- d) Administrar i renovar certificats digitals.

5. Una bona pràctica per reforçar la seguretat en un entorn de virtualització és:

- a) Configurar tots els hosts i màquines virtuals dins d’un sol segment de xarxa per simplificar la gestió.
- b) Deixar habilitats ports d’administració com el 443 sense control d’accés.
- c) Implementar microsegmentació per limitar moviments laterals dins del CPD.
- d) Donar accés d’administrador global a tots els tècnics del servei per agilitzar incidències.

6. En la publicació de serveis públics a Internet, quina és la pràctica adequada per protegir un servidor web municipal?

- a) Traslladar-lo a la xarxa interna per facilitar-ne la gestió.
- b) Evitar la segmentació per reduir complexitat.
- c) Ubicar-lo en una DMZ amb accés estrictament filtrat.
- d) Obrir tots els ports del firewall per evitar bloquejos.

7. En la certificació de l’ENS, el nivell MIG s’aplica quan:

- a) L’Ajuntament ha desplegat el SOC i supera els 50 treballadors.
- b) Els sistemes no gestionen dades personals.
- c) El risc potencial és moderat en impacte i probabilitat segons l’anàlisi de riscos.
- d) Els servidors principals del CPD estan allotjats íntegrament al núvol.

8. Una mesura reforçada pròpia del nivell MIG de l’ENS és:

- a) Reduir el volum de logs per simplificar l’auditoria.
- b) Permetre configuracions com TLS 1.0.
- c) Realitzar proves de pentesting i tests de vulnerabilitat de manera periòdica.
- d) Prescindir d’eines de monitoratge com el SIEM.

9. Una actuació habitual per augmentar la disponibilitat del CPD és:

- a) Eliminar un dels SAI per reduir costos i simplificar el manteniment.
- b) Agrupar tots els servidors i sistemes en una única VLAN per facilitar la gestió.
- c) Implementar redundància en climatització, energia i cabines d’emmagatzematge, garantint continuïtat davant fallades.
- d) Substituir servidors físics per ordinadors d’escriptori per estalviar consum energètic.

10. Quina actuació és coherent amb una modernització del CPD i els serveis TIC?

- a) Reduir la capacitat d’emmagatzematge per disminuir el consum energètic.
- b) Automatitzar desplegaments, còpies de seguretat i monitoratge per millorar l’eficiència i reduir errors humans.
- c) Rebutjar l’ús de virtualització i tornar a servidors físics dedicats.
- d) Limitar l’ús d’eines cloud per simplificar la gestió interna.

11. Una actuació del Pla d'evolució tecnològica en un entorn de virtualització municipal és:

- a) Afegir memòria RAM de models heterogenis sense validar compatibilitat.
- b) Consolidar els hosts, actualitzar-los a versions recents i aplicar pegats de seguretat de forma controlada.
- c) Operar l'entorn virtual sense infraestructura DNS corporativa.
- d) Desactivar els serveis de gestió remota per reduir trànsit.

12. En el desplegament d'una plataforma de Ciutat Intel·ligent, LoRaWAN és especialment adequada per a:

- a) Transmetre vídeo en alta definició des de càmeres urbanes.
- b) Gestionar transaccions bancàries crítiques en temps real.
- c) Connectar sensors de ciutat de llarg abast i consum ultra-baix.
- d) Donar servei troncal a la xarxa de fibra òptica municipal.

13. En el desplegament d'una infraestructura IoT municipal, quina és una mesura de seguretat imprescindible per protegir les comunicacions entre sensors i la plataforma?

- a) Desactivar el registre de logs per reduir consum.
- b) Implantar certificats TLS, autenticació robusta i xifrat als IoT Agents.
- c) Permetre accés root als dispositius IoT per facilitar el manteniment.
- d) Mantenir les contrasenyes per defecte dels fabricants per garantir compatibilitat.

14. En el projecte d'IA en temps real integrat amb la plataforma de Ciutat Intel·ligent i el GIS municipal, quin factor és especialment crític i pot provocar problemes greus de rendiment en el model d'IA?

- a) Que l'ordinador del tècnic que visualitza el dashboard sigui massa antic.
- b) Que al GIS hi hagi activades diverses capes d'informació simultàniament.
- c) Que la velocitat i volum de dades IoT entrants superin la capacitat de processament del motor d'IA.
- d) Que el navegador no disposi de memòria cau suficient.

15. En un sistema de Ciutat Intel·ligent basat en FIWARE amb un model d'IA integrat, la historització de dades és essencial perquè:

- a) Serveix només per generar còpies de seguretat automàtiques.
- b) És un requisit obligatori per poder mostrar capes GIS bàsiques.
- c) Permet entrenar models d'IA, validar prediccions i analitzar l'evolució temporal de patrons.
- d) Redueix considerablement el consum de trànsit entre IoT Agents i la plataforma FIWARE.

16. En el projecte de l'aplicació de gestió de llicències municipals, gestionat amb metodologia àgil, quin enfocament és el correcte segons les pràctiques Scrum?

- a) Definir tota la solució al detall al principi i evitar canvis fins al lliurament final.
- b) Bloquejar iteracions per reduir la participació dels usuaris i així accelerar el desenvolupament.
- c) Treballar en iteracions curtes (sprints), incorporant feedback continu dels usuaris i adaptant el producte progressivament.
- d) Evitar documentar el projecte perquè la metodologia no requereix cap documentació formal.

17. En aquest projecte, quina és la millor pràctica per implementar la lògica de negoci?

- a) Delegar tota la lògica en processos JavaScript al navegador per reduir càrrega del servidor.
- b) Distribuir la lògica en triggers i funcions aïllades en diferents taules per agilitzar la resposta del sistema.
- c) Centralitzar la lògica en PL/SQL (packages, procedures i funcions) com a capa de negoci integrada amb APEX.
- d) Programar totes les regles de negoci en fulls de càlcul externs i importar-ne els resultats a APEX.

18. Per millorar el rendiment de les consultes a Oracle és recomanable:

- a) Limitar-se a fer SELECT * per evitar problemes amb canvis d'esquema.
- b) Combinar totes les dades en una única taula gran per reduir el nombre de JOIN.
- c) Dissenyar i mantenir índexs adequats, revisar plans d'execució i optimitzar SQL/PL/SQL.
- d) Desactivar les claus primàries per agilitzar insercions.

19. Quan el servei d'atenció a l'usuari detecta un error en la integració entre l'aplicació de Gestió de Personal i el sistema d'expedients, quin és el primer pas procedimental correcte segons el protocol d'atenció?

- a) Reiniciar tots els serveis del CPD sense anàlisi prèvia.
- b) Donar per fet que és un problema del servidor i avisar directament sistemes.
- c) Reproduir la incidència, validar que no és un error d'usuari i confirmar l'abast del problema.
- d) Escalar automàticament la incidència al nivell 3 sense comprovacions.

20. Un error "503 – servei no disponible" indica habitualment:

- a) Un error de credencials o contrasenya de l'usuari.
- b) Una fallada del servidor DNS que impedeix resoldre noms.
- c) Que el servei d'integració està caigut o no està responant correctament.
- d) Que la base de dades s'ha quedat sense espai.

PREGUNTES DE RESERVA

21. RESERVA 1. Quina és una actuació recomanable per reforçar la seguretat de l'accés VPN corporatiu?

- a) Implementar MFA, limitar l'accés per segments de xarxa i aplicar polítiques de control d'endpoint.
- b) Permetre connexions VPN només amb túnels sense certificats per reduir latència.
- c) Oferir accés VPN sense restriccions per facilitar el teletreball.
- d) Permetre que qualsevol dispositiu personal s'hi connecti si té antivirus actiu.

22. RESERVA 2. Que ha d'incloure l'arquitectura de la plataforma de Ciutat Intel·ligent per ser funcionalment completa:

- a) Només sensors de trànsit, ja que la resta de dades es poden importar manualment.
- b) Una xarxa Wi-Fi pública per garantir la connectivitat de tots els dispositius intel·ligents.
- c) Únicament una base de dades SQL central per emmagatzemar totes les lectures IoT.
- d) Sensors IoT, brokers de context, mòduls d'històrics i integració amb dashboards i GIS.