PRUEBAS SELECTIVAS*

TÉCNICO/A AUXILIAR T.I.C DEL AYUNTAMIENTO DE MADRID

ACCESO LIBRE

EJERCICIO ÚNICO

PARTE PRÁCTICA

27 DE JUNIO DE 2026

*Convocadas por Resolución de 19 de diciembre de 2025 del Director General de Planificación de Recursos Humanos (BOAM nº 10032, de 23 de diciembre de 2025)

SUPUESTO PRÁCTICO

Supuesto práctico: Sistema de Gestión de Incidencias de la Policía Municipal

Eres técnico/a auxiliar TIC del Área de Gobierno de Vicealcaldía, Portavoz, Seguridad y Emergencias del Ayuntamiento de Madrid. La Policía Municipal va a implantar un nuevo sistema integral de gestión de incidencias operativas para coordinar comisarías y unidades desplegadas en vía pública.
El sistema permitirá registrar y consultar avisos, partes de intervención, e incidencias desde puestos corporativos y dispositivos móviles autorizados. La solución deberá integrarse con aplicaciones web internas, bases de datos corporativas, red local de dependencias policiales, comunicaciones móviles y red TETRA para comunicaciones críticas de voz y coordinación operativa. También deberá garantizar seguridad, disponibilidad, trazabilidad, copias de seguridad y cumplimiento de los principios del ENS y del ENI.

PREGUNTAS:

1. Durante el piloto, los puestos fijos de una comisaría acceden correctamente a la aplicación, pero los dispositivos móviles corporativos muestran el mensaje:

"No se puede establecer conexión segura con el servidor".

Otros servicios de Internet funcionan correctamente en esos móviles. ¿Cuál sería la comprobación inicial más adecuada?

a) Comprobar la configuración de proxy y APN en los dispositivos móviles.
b) Validar que el firewall permita el tráfico HTTPS desde la red móvil corporativa.
c) Verificar si los móviles confían en el certificado del servidor o en su autoridad certificadora.

2. Se tiene el siguiente servicio EJB Stateless con transacciones gestionadas por el contenedor:

```
Java@Stateless
public class IncidenciaService {

   @PersistenceContext
   private EntityManager em;

   public void registrarIncidencia(Incidencia incidencia) {
      em.persist(incidencia);

      Auditoria auditoria = new Auditoria();
      auditoria.setAccion("ALTA_INCIDENCIA");
      auditoria.setIdIncidencia(incidencia.getId());

      em.persist(auditoria);
   }
}
```

Al ejecutar registrarIncidencia(), se produce una excepción de tipo RuntimeException durante la inserción de la entrada en la tabla de auditoría. ¿Qué comportamiento es esperable por defecto?

a) Se revierte toda la transacción.
b) Se persiste la incidencia y solo se descarta la auditoría.
c) El contenedor confirma los cambios realizados hasta el momento de la excepción.

3. El panel de la sala de coordinación debe mostrar incidencias no cerradas. Se revisa esta consulta:

```
SELECT id_incidencia, tipo, prioridad, estado, fecha_alta
FROM incidencias
WHERE estado <> 'CERRADA'
  AND fecha_alta > CURRENT_DATE
ORDER BY prioridad DESC, fecha_alta ASC;
```

Algunas incidencias abiertas de días anteriores no aparecen en el panel. ¿Cuál es la causa más probable?

a) La condición fecha_alta > CURRENT_DATE excluye incidencias abiertas anteriores al día actual.
b) ORDER BY elimina automáticamente las incidencias antiguas.
c) El operador <> sólo funciona con campos numéricos.

4. Un agente registra una incidencia desde un dispositivo móvil en una zona con mala cobertura. Al recuperar la conexión, el servidor rechaza la sincronización porque un operador de sala ya había cerrado previamente esa misma incidencia desde la aplicación de escritorio.
¿Qué diseño es más adecuado para tratar este tipo de situaciones?

a) Implementar una estrategia "Last Write Wins" (el último cambio sobrescribe al anterior).
b) Implantar un mecanismo de detección y resolución de conflictos usando versiones, marcas temporales y reglas de negocio específicas.
c) Usar bloqueo pesimista (pessimistic locking) para evitar modificaciones concurrentes en incidencias.

5. Una comisaría dispone de la red 192.168.20.0/24 y necesita segmentarla según los siguientes requisitos:

Red de Usuarios: 120 dispositivos
Red de Servidores: 25 dispositivos
Red de Impresoras: 12 dispositivos
Red de Videovigilancia: 8 dispositivos

¿Cuál de las siguientes propuestas de segmentación con VLSM es la más eficiente y correcta?

a) /25 (Usuarios) – /27 (Servidores) – /28 (Impresoras) – /28 (Videovigilancia)
b) /24 (Usuarios) – /27 (Servidores) – /28 (Impresoras) – /28 (Videovigilancia)
c) /26 (Usuarios) – /27 (Servidores) – /28 (Impresoras) – /29 (Videovigilancia)

6. La aplicación permite a los agentes adjuntar fotografías como evidencia en las incidencias. Se ha detectado que algunos usuarios intentan subir ficheros ejecutables (.exe) renombrándolos con extensión .jpg. ¿Qué control de seguridad es el más adecuado para mitigar este riesgo?

a) Validar la extensión, el tipo MIME, la firma mágica del archivo, el tamaño máximo y realizar un análisis antimalware antes de almacenarlo.
b) Permitir cualquier tipo de archivo siempre que el usuario esté autenticado y tenga permisos.
c) Comprobar únicamente que la extensión sea .jpg o .png.

7. El panel operativo de la sala de coordinación debe mostrar nuevas incidencias sin refrescar manualmente. Actualmente realiza:

```
setInterval(() => {
  fetch("/api/incidencias/activas")
    .then(r => r.json())
    .then(datos => pintarPanel(datos));
}, 300000);
```

¿Qué problema tiene esta configuración?

a) Actualiza el panel cada 5 minutos, lo cual puede ser insuficiente para una sala de coordinación.
b) Actualiza el panel cada 3 segundos, por lo que podría saturar el sistema.
c) La configuración tiene un error de sintaxis y generaría el mensaje: "Uncaught SyntaxError: missing) after argument list".

8. El sistema de gestión de incidencias de la Policía Municipal trata datos de carácter policial, incluyendo información sensible relacionada con la seguridad ciudadana, la investigación de delitos y la operatividad policial.
Según el ENS, ¿en qué categoría de seguridad debe clasificarse predominantemente este sistema?

a) Categoría BÁSICA
b) Categoría MEDIA
c) Categoría ALTA

9. Los agentes de la Policía Municipal de Madrid utilizan terminales TETRA. Una de las características más relevantes de TETRA para los servicios de emergencias es su modo DMO. ¿Qué significa este modo y cuándo resulta especialmente útil?

a) Digital Monitoring Operation: monitoriza el espectro de frecuencias para detectar interferencias
b) Direct Mode Operation: permite comunicación directa entre terminales sin necesidad de infraestructura de red
c) Data Management Operation: gestiona la transferencia de datos entre la red TETRA y el sistema de información

10. Se ha configurado la siguiente tarea en el cron del servidor para realizar backups:
0 3 * * * /usr/local/bin/backup-diario.sh
¿Qué RPO (Recovery Point Objective) aproximado se está asumiendo con esta configuración?

a) Hasta 24 horas de pérdida máxima de datos.
b) Sin pérdida de datos (RPO = 0).
c) Máximo de tres horas de pérdida de datos.

11. Durante una videoconferencia entre distintas comisarías, se observan pequeños cortes intermitentes en el audio. El sistema no retransmite los paquetes perdidos.
¿Qué principio técnico explica este comportamiento?

a) El uso de TCP como protocolo de transporte es obligatorio en este tipo de aplicaciones.
b) Los protocolos de videoconferencia siempre desactivan la corrección de errores para ahorrar ancho de banda.
c) En comunicaciones en tiempo real se prioriza la baja latencia sobre la fiabilidad total de la entrega.

12. Un usuario autenticado con rol de agente, perteneciente a la Comisaría 08, realiza la siguiente petición:

GET /api/incidencias/4812
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5c6IkpXVCJ9...

La incidencia solicitada (ID 4812) pertenece a la Comisaría 12. Sin embargo, la API responde correctamente con todos los datos detallados de la incidencia.
¿Qué vulnerabilidad de seguridad presenta este comportamiento?

a) Falta de validación de autorización a nivel de recurso u objeto (Object Level Authorization).
b) Ausencia de controles de rate limiting en los endpoints de consulta.
c) Uso inadecuado del método HTTP GET para recuperar información sensible.

13. El equipo TIC del Ayuntamiento utiliza una herramienta de gestión de proyectos basada en metodología ágil, con tableros visuales que muestran tareas en columnas como 'Pendiente', 'En progreso' y 'Completado'. ¿Qué metodología y herramienta de visualización describe esta práctica?

a) Metodología en cascada (Waterfall) con diagrama de Gantt
b) Metodología Kanban con tablero Kanban
c) Metodología PRINCE2 con registro de riesgos

14. Cuando un agente envía una incidencia desde su dispositivo móvil al servidor central, los datos se encapsulan en distintas capas antes de transmitirse. ¿En qué capa del modelo OSI se realiza el enrutamiento de paquetes entre redes diferentes?

a) Capa 2 — Enlace de datos
b) Capa 3 — Red
c) Capa 4 — Transporte

15. La sala de coordinación de la Policía Municipal necesita garantizar comunicaciones de voz entre agentes incluso si la red de datos falla. ¿Qué sistema de comunicaciones está diseñado específicamente para cubrir esta necesidad en servicios de emergencias y seguridad pública?

a) Red WiFi 802.11ac
b) Red 4G/LTE comercial
c) Sistema TETRA

16. Observa el siguiente pseudocódigo que busca un parte en una lista ordenada de partes policiales por número de expediente:

```
inicio = 0; fin = N-1
mientras inicio <= fin:
   medio = (inicio + fin) / 2
   si lista[medio] == objetivo: devolver medio
   si lista[medio] < objetivo: inicio = medio + 1
   sino: fin = medio - 1
devolver -1
```

¿Qué algoritmo de búsqueda implementa este código?

a) Búsqueda lineal (secuencial)
b) Búsqueda binaria (dicotómica)
c) Búsqueda en profundidad (DFS)

17. Un desarrollador ejecuta por error el comando: git push origin main --force
en el repositorio compartido, sobrescribiendo el historial remoto. Otros tres desarrolladores tienen cambios locales sin subir. ¿Cuál es el impacto de este comando y cómo se debe proceder para recuperar el historial?

a) El historial se pierde de forma definitiva y todos los desarrolladores deben volver a clonar el repositorio.
b) El historial remoto queda sobrescrito, pero los commits eliminados pueden recuperarse usando git reflog.
c) El comando no afecta a los repositorios locales. Los desarrolladores recibirán una notificación y podrán sincronizar automáticamente.

18. Se ha detectado que un equipo de la red interna está enviando peticiones DNS a un dominio externo desconocido cada 60 segundos. Los nombres consultados contienen cadenas aleatorias largas (ej: a3f92bc1d72e.maldominio.com). ¿Qué técnica de ataque representa este comportamiento?

a) Amplificación DNS
b) DNS Tunneling
c) DNS Cache Poisoning

19. Se detecta en los logs del servidor web del sistema de incidencias la siguiente entrada repetida:
GET /buscar?expediente=1+OR+1=1-- HTTP/1.1. ¿Qué tipo de ataque indica esta entrada en el log?

a) Es un ataque de Cross-Site Scripting (XSS) reflejado.
b) Es un intento de inyección SQL (SQL injection).
c) Es un ataque de fuerza bruta contra el campo de búsqueda.

20. El CAU (Centro de Atención a Usuarios) recibe una incidencia: el ordenador de un agente en la Comisaría Integral de Distrito de Salamanca muestra una pantalla azul (BSOD) de forma recurrente al abrir el sistema de incidencias. El técnico conecta de forma remota mediante RDP pero el equipo vuelve a mostrar BSOD durante la sesión remota. ¿Cuál es el siguiente paso técnico correcto?

a) Cerrar la sesión RDP y llamar por teléfono al agente para que lea en voz alta el código de error del BSOD, ya que no es posible capturar información de un BSOD mediante herramientas remotas.
b) Antes de que vuelva a producirse el BSOD, revisar remotamente el Visor de eventos de Windows (Event Viewer) en los registros de Sistema y Aplicación para identificar errores críticos previos al fallo, así como analizar el fichero de volcado de memoria.
c) Reinstalar el sistema operativo de forma remota mediante WDS (Windows Deployment Services).

21. En el portal web del sistema de incidencias, un campo de búsqueda usa únicamente el atributo placeholder como referencia textual, sin etiqueta <label> asociada. ¿Qué problema de accesibilidad presenta este diseño?

a) El placeholder desaparece al escribir, dificultando la experiencia de usuarios con problemas cognitivos, y los lectores de pantalla no siempre lo anuncian como etiqueta del campo. Incumple los criterios 1.3.1 y 3.3.2 de las WCAG 2.1.
b) No existe problema relevante: los principales lectores de pantalla como NVDA o JAWS leen el placeholder al enfocar el campo, por lo que es suficiente como referencia textual.
c) El problema es de contraste: el placeholder suele tener color gris claro sobre fondo blanco, incumpliendo el criterio 1.4.3 (Contraste mínimo) de las WCAG 2.1.

22. Al arrancar el servidor de aplicaciones del sistema de gestión de incidencias, el técnico observa que el proceso Java consume el 95% de la CPU durante varios minutos antes de estabilizarse. Revisando la configuración, comprueba que la JVM se ha iniciado con los parámetros -Xms64m -Xmx64m. ¿Cuál es la causa más probable de ese comportamiento y qué parámetro debería modificarse primero?

a) El parámetro -Xmx64m limita el heap máximo a 64 MB, un valor insuficiente para una aplicación Spring Boot con alta carga. La JVM ejecuta el garbage collector de forma continua intentando liberar memoria, lo que dispara el consumo de CPU. Debería aumentarse -Xmx al menos a 512m.
b) El problema es que -Xms y -Xmx tienen el mismo valor, lo que impide al planificador de la JVM asignar más hilos al proceso. La solución es establecer -Xms a la mitad de -Xmx para dejar margen de crecimiento.
c) El parámetro -Xms64m fuerza a la JVM a reservar 64 MB de CPU al arranque. Para reducir el consumo inicial se debe eliminar -Xms del comando de arranque y dejar que la JVM gestione la CPU de forma dinámica.

23. El sistema de incidencias debe asignar cada aviso a la patrulla disponible más cercana, recalculando la distancia según la posición GPS de los vehículos y manteniendo una consulta eficiente cuando hay muchas unidades desplegadas.
¿Qué estructura o enfoque sería más adecuado?

a) Una pila LIFO, de forma que se asigne siempre la última patrulla que haya comunicado disponibilidad, ya que la operación de extracción es O(1).
b) Una estructura espacial como un árbol k-d o índice geoespacial, que permite organizar puntos por coordenadas y realizar búsquedas de vecinos más cercanos de forma más eficiente que recorrer todas las patrullas.
c) Una lista simple no ordenada, recorriéndola completa en cada aviso para calcular la distancia a todas las patrullas y seleccionar la menor, con coste O(n) por consulta.

24. La base de datos PostgreSQL del sistema de incidencias tiene activado el modo autocommit. Un técnico ejecuta por error el siguiente bloque:

```
UPDATE incidencias
SET estado='ARCHIVADA'
WHERE id_incidencia > 0;
```

y a continuación intenta revertirlo con ROLLBACK. ¿Cuál es el resultado?

a) El ROLLBACK revierte correctamente la operación porque PostgreSQL mantiene el registro de transacciones (WAL) y siempre permite deshacer cambios, independientemente del modo autocommit.
b) El ROLLBACK no tiene efecto. Con autocommit activado, cada sentencia SQL se confirma automáticamente como una transacción independiente en cuanto se ejecuta. Para que ROLLBACK funcione, el técnico debería haber iniciado explícitamente una transacción con BEGIN antes del UPDATE.
c) El ROLLBACK revierte el UPDATE solo si se ejecuta en los 30 segundos siguientes, que es el tiempo de retención por defecto del buffer de transacciones de PostgreSQL antes de hacer flush al disco.

25. La Jefatura de la Policía Municipal necesita un formulario web para que los agentes reporten incidencias menores sin pasar por el sistema principal. El técnico TIC dispone de poco tiempo y usa una plataforma low-code del catálogo de herramientas municipales para construirlo. ¿Cuál es el riesgo técnico más relevante que debe valorar antes de desplegarlo en producción?

a) Las plataformas low-code generan código HTML estático por lo que el formulario no podría enviar los datos al sistema de incidencias bajo ningún concepto.
b) La plataforma low-code puede introducir dependencia de proveedor (vendor lock-in). Además, debe verificarse que cumple con el ENS y el RGPD antes de procesar datos policiales.
c) Las plataformas low-code solo admiten conexiones con APIs REST modernas. Si el sistema de incidencias expone servicios SOAP o acceso directo a base de datos, la integración sería técnicamente inviable y el formulario no podría trasladar los datos al sistema principal.

26. Al revisar el diseño de la tabla de incidencias, el técnico detecta que el campo nombre_agente se repite en cada fila junto al id_agente, causando redundancia. ¿En qué forma normal se resuelve esta anomalía?

a) Primera Forma Normal (1FN)
b) Segunda Forma Normal (2FN)
c) Tercera Forma Normal (3FN)

27. El analista de datos diseña el modelo conceptual del sistema y define la siguiente relación: un AGENTE puede gestionar muchas INCIDENCIAS, pero cada INCIDENCIA es gestionada por exactamente un AGENTE. Adicionalmente, una INCIDENCIA puede involucrar a varios VEHÍCULOS, y un VEHÍCULO puede aparecer en varias INCIDENCIAS. ¿Cómo se representan correctamente estas cardinalidades en el modelo Entidad-Relación?

a)
AGENTE — (1, N) — INCIDENCIA con relación 'gestiona';
INCIDENCIA — (N, M) — VEHÍCULO con relación 'involucra'.
b)
AGENTE — (1, 1) — INCIDENCIA con relación 'gestiona'
INCIDENCIA — (1, N) — VEHÍCULO con relación 'involucra'.

c) Todas las relaciones son (N,M) por defecto en el modelo E/R conceptual. Las cardinalidades exactas se definen únicamente en la fase de diseño lógico al transformar el modelo al relacional.

28. El servidor Linux del sistema de incidencias muestra un uso de CPU al 100% de forma sostenida. El técnico ejecuta el comando 'top' y detecta que un proceso acumula el 98% de CPU con PID 4821. Necesita terminar el proceso de forma ordenada para que libere recursos antes de morir. ¿Qué comando utiliza?

a) kill -1 4821
b) kill -9 4821
c) kill -15 4821

29. En el código del sistema, la clase Atestado hereda de la clase Documento, que a su vez define el método firmar(). Al llamar a miAtestado.firmar(), se ejecuta la versión sobreescrita en Atestado. ¿Qué concepto de la POO describe este comportamiento?

a) Encapsulación
b) Polimorfismo
c) Abstracción

30. El Ayuntamiento implanta una aplicación cloud para la gestión de partes de incidencias. La aplicación debe almacenar fotografías, vídeos y documentos adjuntos asociados a cada parte, con posibilidad de acceder a ellos desde distintas instancias de la aplicación y sin depender del disco local de un servidor concreto. ¿Cuál de los siguientes servicios de almacenamiento cloud sería más adecuado?

a) Amazon EBS, Azure Managed Disks o Google Persistent Disk
b) Amazon S3, Azure Blob Storage o Google Cloud Storage
c) Amazon ElastiCache, Azure Cache for Redis o Google Cloud Memorystore.