PRUEBAS SELECTIVAS LIBRES PARA EL INGRESO EN EL CUERPO DE TITULADOS MEDIOS (OPCIÓN: INFORMÁTICA), DE LA CÁMARA DE CUENTAS DE ANDALUCÍA OEP 2016

INSTRUCCIONES

1. No abra este cuestionario hasta que se le indique.
2. El presente ejercicio consiste en la resolución de un caso de carácter práctico, a elegir entre **dos propuestas** identificadas como opción A y como opción B. **Debe resolver sólo uno de ellos**, por escrito, en las hojas facilitadas a este efecto. **Indique claramente al principio de sus respuestas qué opción está resolviendo**.
3. Cada caso práctico consta de una parte expositiva denominada ESCENARIO, en la que se describe el entorno en el que se desarrolla el caso, y de cuatro apartados a desarrollar.
4. El cuaderno de examen estará formado por un primer folio con cabecera separable, en la cual debe consignar sus datos de identificación, y por sucesivos folios numerados y sellados, en los que deberá escribir por una sola cara. **No dispondrá de más folios para realizar el examen.**
5. Si se equivoca, tache claramente la parte donde ha cometido el error y continúe el examen. No se retirará ningún folio numerado.
6. Escriba su nombre únicamente en la cabecera separable, cuyo cuerpo hará de primer folio de su examen. **En el resto de folios, no escriba su nombre ni firme ni realice ninguna otra anotación o marca que permita la identificación del aspirante**.
7. **Los exámenes que no cumplan las instrucciones anteriores podrán quedar invalidados**.
8. Redacte las respuestas de forma clara de modo que permitan su corrección por el Tribunal. Puede resolver las cuestiones en el orden que desee. Indique claramente a qué cuestión se refiere cada una de las respuestas.
9. El tiempo de realización de este examen es de 120 minutos.
10. Este cuestionario puede utilizarse como borrador.
11. Solo podrá tener sobre la mesa el cuestionario, las hojas de examen, bolígrafo, DNI y botella de agua. **Todos los efectos personales, incluidos móviles, bolsos, relojes, smartwatch, etc. deberán ser apagados y depositados en el suelo**.
12. Cuando dé por finalizado el examen no se levante de su asiento, avise a un miembro del Tribunal levantando la mano y será éste quien le recoja el examen.
13. Los aspirantes que necesiten justificar su asistencia a este ejercicio podrán solicitar el certificado correspondiente.

Página intencionalmente en blanco

FASE DE OPOSICIÓN. SEGUNDO EJERCICIO

OPCIÓN A.
ESCENARIO: AYUNTAMIENTO

Usted trabaja como responsable de seguridad en un Ayuntamiento, ubicado en la Comunidad Autónoma de Andalucía, y deberá resolver 4 cuestiones relacionadas con:

1. Seguridad
2. Diseño de red
3. Plan de recuperación de desastres
4. Caso de ingeniería de software: PERT

Este ejercicio se calificará de 0 a 20 puntos. Cada cuestión se valorará hasta un máximo de 5 puntos.

Página intencionalmente en blanco

1. Seguridad.

El Ayuntamiento tiene competencias en materia de promoción turística y desea conocer los intereses de los posibles turistas, para lo cual elabora una aplicación móvil para que los usuarios de una red social que estén interesados rellenen un cuestionario. La aplicación puede descargarse desde la web del Ayuntamiento.

En el cuestionario se indagaría sobre los intereses de cada usuario sobre gastronomía, actividades culturales y de entretenimiento en general y, en particular, sobre las oportunidades que en tales aspectos existen en el municipio. El objetivo es adaptar la oferta turística del municipio al resultado del análisis estadístico de las respuestas obtenidas, sin descartar el uso posterior de los datos de contacto de los usuarios para mantenerles informados sobre eventos organizados por el propio Ayuntamiento y también para que algunos establecimientos turísticos de la localidad puedan promocionar su oferta de servicios y ofrecerles descuentos.

Este Ayuntamiento ha recibido fondos europeos y está inmerso en un proceso de innovación tecnológica. Han decidido montar una wifi para dar acceso a Internet corporativo y de invitados.

Adicionalmente y de cara a adecuarse al Esquema Nacional de Seguridad deciden hacer una auditoría para ver su nivel de adecuación al esquema y contratan a un técnico de seguridad que les permita diseñar un plan de modernización con todas las garantías. Últimamente están recibiendo numerosos ataques para entrar en modo edición al portal web.

Conteste las siguientes cuestiones (razone todas las respuestas):

1.1. ¿Debería el Ayuntamiento comunicar a alguien que está recibiendo ataques? En caso afirmativo, ¿a quién? ¿Y si en el ataque acceden a datos de carácter personal? ¿Se podría sancionar económicamente al Ayuntamiento por la pérdida de los datos?

1.2. El Ayuntamiento quiere realizar una declaración de aplicabilidad en el Esquema Nacional de Seguridad para la aplicación móvil construida. ¿En qué consiste esta declaración? ¿Por quién deberá ser aprobada formalmente?

1.3. Describa brevemente el procedimiento a seguir para realizar la mencionada declaración de aplicabilidad.

1.4. Suponiendo que fuera el técnico de seguridad, ¿qué recomendaciones de seguridad daría para el montaje de la wifi? Realice una enumeración y una breve descripción de cada una de la recomendaciones.

1.5. ¿Qué recomendaciones de seguridad daría para evitar un ataque del tipo ransomware? Realice una enumeración y una breve descripción de cada una de la recomendaciones.

2. Diseño de red.

Este apartado consiste en realizar un documento de requisitos técnicos para el suministro, instalación, configuración y puesta en marcha de la solución necesaria para la infraestructura de red, de seguridad y acceso a Internet para el Ayuntamiento y sus Organismos Autónomos.

Debe considerar que:

- Existen servidores de tipo: A, B, C.
- Dos centros de cableado principales con cableado vertical, equipos de distribución y que además actúan como CPD principal y redundante. Ocho centros de cableado secundarios con cableado horizontal.
- Existen cinco grupos de trabajo de auditoría y administración.
- Impresoras.
- Cámaras IP.
- Puntos de acceso wifi.

El contrato tiene por objeto la:

- Red Corporativa Multiservicio del Ayuntamiento.
- Infraestructura de Red.
- Infraestructura de Seguridad.
- Servicio de acceso a Internet.

Para la realización del documento de requisitos técnicos proponga:

2.1. La arquitectura lógica y física.

2.2. El plan de direccionamiento IP, justificando los criterios utilizados.

2.3. Soluciones de seguridad, para evitar la generación de bucles y para limitar la visibilidad entre subredes, grupos o conjuntos de elementos de la red.

3. Plan de recuperación de desastres.

El responsable de seguridad del Ayuntamiento, de acuerdo con lo acordado por el Comité de Seguridad de la Información, debe elaborar un Plan de Recuperación de Desastres. Dicha acción se ha establecido con objeto de dar respuesta a la medida "[op.cont.2] Plan de continuidad" del Esquema Nacional de Seguridad, dado que la entidad ha sido clasificada como de nivel alto.

El Plan de Recuperación de Desastres es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

El responsable de seguridad debe tener en cuenta la situación particular del Ayuntamiento para la elaboración del plan y ha identificado específicamente los siguientes hechos:

- El municipio se encuentra en una zona con lluvias poco frecuentes, pero cíclicamente torrenciales.
- Los centros de cableado no se pensaron para ello. El CPD principal es un bajo. Los centros de cableado tienen tuberías.
- Se sufren episodios de caída eléctrica en determinados locales.
- Se dispone de dos ubicaciones, centros de cableado desde los que se instalan conexiones físicas a otros centros del Ayuntamiento.
- Existen determinados locales del Ayuntamiento, que por el servicio que proporcionan, son particularmente sensibles a la disponibilidad, dado que no admiten desconexiones del sistema de información central.
- Existen determinados activos de información ubicados en el CPD que son particularmente sensibles en cuanto a pérdidas de datos y a modificaciones en su integridad.

Detalle los siguientes puntos:

3.1. Los aspectos fundamentales que debe tener en cuenta el responsable de seguridad para la elaboración del Plan.

3.2. Las acciones que debe acometer durante el proceso de elaboración del Plan y a lo largo de la vigencia del mismo.

3.3. El índice del documento y una breve explicación del contenido de cada apartado, incluyendo alguna propuesta o medida que permita prevenir o mitigar los dos riesgos más importantes identificados.

4. Caso de ingeniería de software: PERT.

Partiendo de la siguiente tabla de actividades, precedencias y duraciones de un proyecto, cree el diagrama de PERT correspondiente, y determine los posibles caminos críticos del mismo, detallando aquellas actividades cuya holguras totales son superiores a cero y determinando cuantitativamente las mismas.

Actividad	Precedente	Duración
A	-	4
B	A	4
C	A	8
D	A	1
E	B,C,D	3
F	E	5
G	F	6
H	F	2
I	G	10

Página intencionalmente en blanco

FASE DE OPOSICIÓN. SEGUNDO EJERCICIO

OPCIÓN B
ESCENARIO: HOSPITAL

Usted trabaja como responsable TIC en un hospital público de pequeño tamaño (menos de 50 trabajadores), ubicado en la Comunidad Autónoma de Andalucía, deberá resolver 4 cuestiones relacionadas con:

1. Auditoría del Esquema Nacional de Seguridad: Cuestionarios y hallazgos
2. Backup: Documento de requisitos técnicos
3. Conexionado de redes
4. Diseño de base de datos: Reducción a modelo relacional

Este ejercicio se calificará de 0 a 20 puntos. Cada cuestión se valorará hasta un máximo de 5 puntos.

Página intencionalmente en blanco

1. Auditoría del Esquema Nacional de Seguridad: Cuestionarios y hallazgos.

Un OCEX está realizando una auditoría financiera y de cumplimiento sobre el gasto de personal del hospital, del ejercicio 2018.

Se ha incluido en el alcance la revisión del sistema de información que soporta los procesos de gestión del personal. Este sistema, denominado SIGP, integra todos los procesos de gestión de personal. Dicho sistema ha sido categorizado como de nivel ALTO, en relación al cumplimiento de los requisitos del Esquema Nacional de Seguridad.

Durante la fiscalización y como resultado proceso de conocimiento del control interno de la entidad, hemos observado lo siguiente:

- Nos han informado que el CPD cuenta con todas las medidas de seguridad, incluyendo aspersores de agua como medida antiincendios.
- El CPD se encuentra protegido mediante llave, de la que únicamente disponen 4 personas.
- Se registran las entradas y salidas al CPD únicamente de los trabajadores externos a la entidad, dado que los trabajadores internos son compañeros de los administradores, que disponen de llave.
- El CPD es suficientemente grande como para instalar equipamiento adicional en caso de desastre natural, en una sala contigua parcialmente equipada, con lo que no se ha considerado el uso de instalaciones alternativas.
- El CPD dispone de SAI, pero por su capacidad únicamente puede proporcionar servicio a algunos de los sistemas. No obstante, no se considera necesaria su ampliación dado que se dispone de dos proveedores distintos de suministro eléctrico.
- Por el local del CPD discurren tuberías de presión para el suministro de agua del edificio, pero el local no se encuentra en planta baja, con lo que nos indican que el riesgo de inundación es bajo y no son necesarias medidas adicionales.
- No se ha elaborado y aprobado un procedimiento general por escrito que regule todos los aspectos de la gestión de usuarios (altas, bajas, perfiles, privilegios) y las revisiones periódicas de usuarios y sus privilegios.
- La gestión de usuarios se realiza mediante las herramientas del Directorio Activo, dado que todos los sistemas de la entidad disponen de SSO o autenticación en el mismo mediante radius server.
- Para la autenticación mediante contraseña no se ha habilitado la complejidad ni la caducidad de las mismas, dado que dichas medidas provocaban numerosas quejas del personal del hospital y bloqueos de usuarios, que impedían el normal funcionamiento de los servicios de éste.
- Los administradores del hospital disponen de 3 identificadores de usuario cada uno: un identificador como trabajador del organismo con permisos mínimos, un

identificador como administrador de equipos de usuario y un tercer identificador como administrador de dominio, servidores y sistemas.

- Hemos verificado que existen un total de 300 usuarios activos con acceso a SIGP:
  - De éstos hay 50 usuarios que se han trasladado a otros departamentos, pero nos indican que se han mantenido activos porque de esta manera se agilizan los trámites en caso de reincorporación de alguno de ellos.
  - Todo el personal externo de la empresa encargada del mantenimiento utiliza el mismo identificador genérico y se nos indica que de esta manera es más ágil la gestión de privilegios de personal externo, dado que hay frecuentes cambios en el equipo de trabajo.
  - Se identifica que 40 de los usuarios activos no acceden a SIGP hace más de seis meses.

Como resultado de la valoración de riesgos preliminar en el trabajo de auditoría se ha detectado, en base a las situaciones observadas en la entidad, que existen dos controles de TI particularmente relevantes para el trabajo de fiscalización, considerando como marco metodológico el conjunto de medidas de seguridad descritas en el ENS.

Estos controles son los siguientes:

- Control de acceso [op.acc]
- Protección de las instalaciones e infraestructuras [mp.if]

1.1. Diseñe un cuestionario de controles generales de tecnologías de la información que incluya al menos 6 preguntas o cuestiones, donde se pongan de manifiesto los requisitos a validar con respecto los dos controles de TI más relevantes identificados. Se valorará la adecuación de la respuesta con lo establecido en las guías de auditoría del Esquema Nacional de Seguridad.

1.2. A partir de la información disponible como resultado del proceso de conocimiento del control interno de la entidad y considerando como base las guías, preparare un detalle de los 6 hallazgos de auditoría más relevantes relativos a los dos controles de TI identificados para el trabajo de fiscalización, con la siguiente estructura:

#	Situación observada	Objetivo de Control	Riesgo	Recomendación
1	*En base al conocimiento del control interno de la entidad*	*Criterio de auditoría para valorar la existencia de una deficiencia de un control de TI*	*Descripción del riesgo identificado, sus consecuencias potenciales y su valoración como: Alto/Medio/Bajo*	*Con objeto de solventar las deficiencias de control detectadas.*

2. Backup: Documento de requisitos técnicos.

El Hospital dispone de varios sistemas de backup que realizan las copias de seguridad de los sistemas de información. Dispone de un servidor de la actual solución de backup conectado mediante una red SAN de dos switches a una cabina de almacenamiento y una librería LTO. Sus características son las siguientes:

- Servidor de Backup con 2 procesadores, 32 GB de memoria, 3 discos duros de 300 GB de capacidad y tiene asignados 3 Tb de la cabina de discos.

- Librería de cintas LTO con 2 Drives FC Ultrium 4 y 45 slots.

- Switches de FO: 2 equipos a 8 Gbps. De las 16 interfaces licenciadas, hay una interfaz libre en un switch y 3 interfaces libres en el otro switch (una de las 3 interfaces no tiene transceiver). Quedan 8 interfaces libres sin licenciar y sin transceiver por cada switch.

- Almacenamiento: Cabina con doble controladora: 12 TB capacidad neta, discos SAS de 15Krpm, y 20TB capacidad neta, discos SATA de 7,2Krpm, 8 puertos FC a 8Gbps y 2 puertos Ethernet 10GbE (FCoE, iSCSI).

La cabina de almacenamiento, además de proporcionar espacio en disco a los diferentes servidores, se utiliza también como recurso de red compartido (servidor de ficheros) en el que diferentes equipos Windows consolidan copias manuales (en modo fichero). Estos ficheros son posteriormente movidos a cinta por un cliente de backup. Hay unos 11 TB.

Adicionalmente conectados a la SAN hay 3 servidores ESX para virtualización, algunas de las MVs tienen el cliente de backup instalado.

- Entorno virtualizado Nº 1:
    - 3 Equipos con 2 CPUs Intel Xeon 8 Cores Model E5-2670 a 2.6GHz.
    - 256 GB RAM, en módulos de 8GB ECC DDR3 1600MHz.
    - 2 HBAs QLogic 8Gb FC Dual-port + Doce puertos de red.
    - VMWare versión 6.0.
    - Aprox. 64 máquinas virtuales.

- Entorno Virtualizado Nº 2:
    - 3 Equipos con 2 procesadores E5-2660 v4, 14 núcleos, 2 GHz.
    - 256 GB RAM, en módulos de 8GB ECC DDR3 1600MHz.
    - VMWare versión 6.0.
    - Aprox. 15 máquinas virtuales.

- Entorno Virtualizado Nº 3:
    - 3 Equipos con 2 procesadores Intel Xeon E5-2650v4 12C/24T 2.20 GHz.
    - 256 GB RAM, en módulos de 8GB ECC DDR3 1600MHz.
    - VMWare Versión 6.5.
    - Aprox. 12 máquinas virtuales.

Estos dos últimos entornos virtualizados (nº2 y nº3) actualmente no utilizan una solución de backup específica.

Elabore un documento de requisitos técnicos para el suministro, instalación, configuración y puesta en marcha de la solución necesaria para la centralización de dichos sistemas de backup, para que sirva de base en una licitación de un contrato llave en mano a riesgo del contratista.

Los puntos principales a desarrollar son:

2.1. Describa cómo actualizar y ampliar la solución de backup actual, extendiéndola al resto de equipos en un proceso de consolidación de todos los entornos de virtualización.

2.2. Describa una nueva solución basada en dispositivos diseñados específicamente para realizar copias de seguridad y eliminación de datos duplicados.

2.3. El troyano Emotet infecta a un equipo conectado al servidor de ficheros. Indique las actuaciones y tareas que realizaría para recuperar el sistema minimizando los daños.

3. Conexionado de redes.

Las oficinas del hospital están en un edificio anexo de dos plantas. Está ocupado por tres servicios: investigación clínica, informática y farmacia. Por razones de gestión y seguridad, se desea crear tres subredes distintas (tres dominios de broadcast distintos), una para cada servicio. En la planta baja se encuentran los empleados de cada servicio (3 de investigación clínica, 5 de informática y 7 de farmacia). En la primera planta están los despachos de los jefes de servicio de cada área y el router que conecta el edificio con el exterior. El administrador de sistemas decide crear diferentes VLANs.

3.1. ¿Cuántos switches se necesitan, como mínimo, para implementar las VLANs, si queremos que exista conectividad entre los distintos dominios de broadcast? ¿Cuántas bocas debe tener cada switch, como mínimo?

3.2. Dibuje el conexionado necesario.

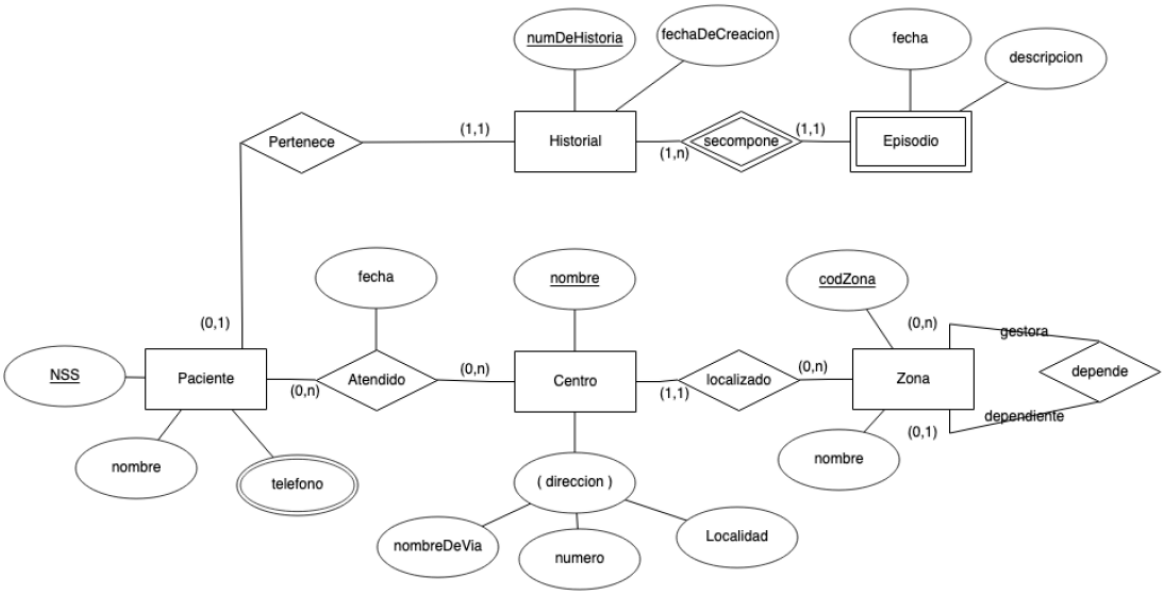
3.3. Un empleado del servicio de investigación clínica envía paquetes de datos a otro compañero del mismo servicio. ¿Cuáles son las direcciones MAC origen y destino de las tramas enviadas?

3.4. ¿Y en el caso de que un empleado del servicio de farmacia envíe paquetes de datos a su jefe?

3.5. ¿Y si un empleado del servicio de farmacia envía paquetes de datos a un empleado del servicio de investigación?

4. Diseño de base de datos: Reducción a modelo relacional.

En el hospital se gestiona la siguiente información representada mediante un modelo entidad/relación:



Realice una reducción a un modelo relacional del modelo entidad/relación suministrado, empleando el menor número de relaciones posible. Tenga en cuenta que en dicho modelo las cardinalidades de participación de cada entidad en una relación se indican junto a ésta (no en el otro lado).

Adicionalmente, indique las restricciones físicas necesarias (NOTNULL, UNIQUE) que permitan mantener las restricciones de cardinalidad.

Emplee para ello la siguiente notación:

A(a1,a2,a3)
PK: a1,a2
FK1: a3 → B.b1
B(b1,b2)
PK: b1
Restricciones:
b2 NOTNULL

donde A y B son relaciones compuestas por los atributos a1, a2 y a3, para el caso de A, y b1 y b2 para el caso de B. PK indica la lista de atributos que forman la clave primaria de la misma, FKx son las claves externas que se definen y “Restricciones” indica la lista de restricciones físicas aplicables.

Página intencionalmente en blanco