PRUEBAS SELECTIVAS LIBRES PARA EL INGRESO EN EL CUERPO DE TITULADOS SUPERIORES (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.** Si se equivoca, tache claramente la parte donde ha cometido el error y continúe el examen. No se retirará ningún folio numerado.
5. 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**.
6. **Los exámenes que no cumplan las instrucciones anteriores podrán quedar invalidados**.
7. 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.
8. El tiempo de realización de este examen es de 120 minutos.
9. Este cuestionario puede utilizarse como borrador.
10. 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**.
11. 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.
12. 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. Protección de datos
2. Plan de continuidad de negocio
3. Esquema Nacional de Seguridad: Elaboración de políticas, normativas y procedimientos.
4. Caso de ingeniería de software: Diagrama de casos de uso.

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

Página intencionalmente en blanco

1. Protección de datos.

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. Tiene un centro de proceso de datos que se está quedando obsoleto y se está valorando la externalización de éste a un proveedor de servicios, pero se les plantea la duda acerca de la ubicación física de los datos ya que algunos de los proveedores que pueden licitar a estos proyectos tienen sus centros de proceso de datos en terceros países no pertenecientes a la Unión Europea.

Conteste las siguientes cuestiones (razone todas las respuestas):

1.1. ¿Qué información debería facilitar el Ayuntamiento a los usuarios en el momento de conectar su perfil de la red social con la aplicación móvil?

1.2. ¿Es preciso recabar el consentimiento de los usuarios para el tratamiento de sus datos identificativos y de intereses?

1.3. Al margen de las respuestas facilitadas por los usuarios al rellenar el cuestionario, ¿el Ayuntamiento podría legítimamente, para adaptar la oferta turística del municipio, indagar en los intereses que los usuarios exponen a través del muro de la red social? ¿Y en los intereses de los contactos de los usuarios participantes?

1.4. Teniendo en cuenta que la persona designada para desempeñar las funciones de Delegado de Protección de Datos puede realizar otras funciones en la organización, ¿qué funciones considera que podrían representar, en un principio, un conflicto de intereses y qué mecanismos o procedimientos se podrían habilitar para, en caso necesario, mitigar esos conflictos?

1.5. En caso de que llegaran a externalizar el servicio, desde el punto de vista de la normativa de protección de datos, ¿qué papel ejercería el proveedor de servicios con respecto a los tratamientos de datos? ¿Qué cláusula habría que poner en un pliego de prescripciones técnicas para garantizar la protección de los datos con las mismas garantías que si su ubicación estuviera en España o cualquier otro país de la Unión Europea?

2. Plan de continuidad de negocio.

El responsable de seguridad del Ayuntamiento, de acuerdo con lo acordado por el Comité de Seguridad de la Información, debe elaborar un Plan de Continuidad de Negocio. Dicha acción se ha establecido con objeto de dar respuesta a las medidas "[op.cont.2] Plan de continuidad" y "Análisis de impacto [op.cont.1]" del Esquema Nacional de Seguridad, dado que la entidad ha sido clasificada como de nivel alto.

El Plan de Continuidad de Negocio es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

El responsable de seguridad debe tener en cuenta la situación particular del Ayuntamiento para la elaboración del plan y ha identificado específicamente los servicios al ciudadano que se han incluido en la sede electrónica:

- Carpeta Ciudadana:
  - Consulta de tributos municipales
  - Consulta de datos de empadronamiento
- Hacienda:
  - Inspección Tributaria: contestación requerimientos, presentación alegaciones y/o aportación documentos.
  - Inspección Tributaria: presentación de recurso de reposición y/o reclamación económico-administrativa
  - Tribunal Económico Administrativo Municipal: Contestación requerimientos, presentación alegaciones, aportación documentos y/o interposición de recursos
- Recursos Humanos:
  - Convocatoria de oposiciones y de bolsas de empleo temporal
- Sanidad:
  - Denuncias Sanitarias
- Tributos, multas, sanciones y demás ingresos municipales de derecho público o privado:
  - Pago on-line de tributos, multas, sanciones y demás ingresos municipales
  - Solicitud de certificaciones de deudas tributarias para los procedimientos de licitación
  - Solicitud aplazamiento/fraccionamiento de deudas
- Población:
  - Certificado de empadronamiento (se enviará por correo electrónico). Es necesaria firma electrónica

Detalle como respuesta a esta cuestión los siguientes puntos:

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

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

2.3. El índice del documento y una breve explicación del contenido de cada apartado, incluyendo alguna propuesta o medida que permita prevenir o mitigar los riesgos que se estimen para dos de los servicios de entre los ofrecidos por el Ayuntamiento en la sede electrónica.

3. Esquema Nacional de Seguridad: Elaboración de políticas, normativas y procedimientos.

El responsable de seguridad, de acuerdo con lo acordado por el Comité de Seguridad de la Información y con objeto de dar respuesta a las medidas del Esquema Nacional de Seguridad sobre el marco organizativo, debe elaborar los siguientes documentos:

- Política de Seguridad, como respuesta a la medida "Política de seguridad [org.1]" del ENS.
- Normativa de Seguridad, como respuesta a la medida "Normativa de seguridad [org.2]" del ENS.
- Procedimientos de Seguridad, como respuesta a la medida "Procedimientos de seguridad [org.3]" del ENS.

3.1. Para cada uno de los dos primeros documentos (Política y Normativa) detalle:

- Responsabilidad en la elaboración y aprobación.
- Índice del documento y una breve explicación del contenido de cada apartado.

3.2. Elabore, sobre un hipotético procedimiento de gestión de usuarios de TI de los servicios administrativos del Ayuntamiento, un índice y una breve explicación del contenido de cada apartado.

4. Caso de ingeniería de software: Diagrama de casos de uso.

Cree un diagrama de casos de uso de una extensión de la aplicación de gestión de intereses turísticos descrita anteriormente. Esta extensión permitirá hacer llegar a los turistas del municipio distintas actividades de ocio, así como mostrar la diversidad de la oferta gastronómica del mismo.

La aplicación permitirá a los usuarios acceder a los listados de actividades de ocio y oferta gastronómica, permitiendo dentro de dichos listados realizar un filtrado de la información mostrada en función del criterio establecido por el usuario. Los usuarios identificados, además de las anteriores funciones, podrán realizar reservas de plazas en las actividades de ocio, o enviar solicitudes de reserva a los locales gastronómicos registrados en la aplicación.

Un usuario sin identificar podrá crear una cuenta. Si éste dispone de ella, el sistema permitirá su identificación mediante la introducción de clave y contraseña, o mediante un certificado digital, a elección del usuario.

En lo que se refiere a la reserva de plazas en actividades de ocio, al cursar la misma, el sistema comprobará que aún existen plazas disponibles. En el caso de que existan, se procederá al pago del importe, para lo que se hará uso de una pasarela de pago externa al sistema. Si no existiesen plazas se avisará al usuario y se procederá a inscribirlo en una lista de espera si así lo desea.

De la misma forma, al cursar una petición de reserva para un establecimiento gastronómico, se procederá al pago de un importe, que se corresponderá con una cantidad de 10 euros por cada comensal reservado. En este caso, no se harán comprobaciones sobre la disponibilidad del establecimiento, simplemente se enviará un correo electrónico al mismo.

El sistema permitirá a los comerciantes la publicación de actividades de ocio y la creación de nuevas entradas para establecimientos gastronómicos. Para ello, este tipo de usuarios se identificarán en el sistema de la misma forma que el resto de usuarios, pero su cuenta estará marcada como cuenta de comerciante, dándole acceso, además de a las funcionalidades del resto de usuarios, a aquellas que les son propias. Finalmente, para el caso de reservas en establecimientos gastronómicos, el comerciante tendrá la posibilidad de anular las mismas (en el caso de que no pueda atenderlas), procediendo el sistema a realizar el reembolso de la cantidad reservada mediante la pasarela de pago externa.

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. Protección de datos
4. Modelado de datos: Modelo Entidad/Relación

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 del proceso de conocimiento del control interno de la entidad, hemos observado lo siguiente:

- El mantenimiento del sistema SIGP lo realiza una empresa externa tras licitación de dicho mantenimiento.
- El pliego del mantenimiento no recoge las particularidades de la prestación del servicio ni todas las obligaciones del adjudicatario, pero el anterior contrato de mantenimiento fue adjudicado a la misma empresa, con lo que ésta conoce perfectamente cuáles son sus obligaciones y funciones.
- El responsable del sistema SIGP, que es a su vez el gestor del contrato de mantenimiento, no ha necesitado incluir en los pliegos el uso de indicadores ni mecanismos para medir el cumplimiento de las obligaciones, dado que es responsable del sistema desde que se implantó y conoce todas las gestiones necesarias con la empresa para asegurar que el servicio es adecuado según su criterio.
- Tanto el servidor de aplicación de SIGP como su base de datos únicamente residen en el CPD principal de la entidad.
- No existe un procedimiento de copias de seguridad debidamente aprobado. No obstante, se hacen copias de seguridad de los datos cada tres meses de acuerdo con el criterio de los administradores de los sistemas. Dichas copias se custodian en un armario en el propio CPD.
- No se dispone de un plan de continuidad de la actividad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. No obstante, se ha habilitado una sala de crisis en las inmediaciones del CPD que permitirá, en caso de producirse un evento, que los administradores del sistema tomen las decisiones necesarias para restaurar los servicios.
- No se ha analizado de manera metodológica el impacto de las amenazas sobre los sistemas y su afección sobre los servicios. Pero en base a experiencias anteriores, el responsable del sistema SIGP conoce el impacto que tiene una interrupción en el servicio durante diferentes periodos de tiempo.
- Dado que existen frecuentes eventos e interrupciones de los servicios que nunca han supuesto un impacto significativo, se ha estimado que no es necesario realizar pruebas periódicas que simulen la caída de los servicios.

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:

- Continuidad del servicio [op.cont]
- Servicios externos [op.ext]

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, prepare 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 un entorno de virtualización consistente en 9 equipos, cada equipo con:

- 2 procesadores E5-2660 v4, 14 núcleos, 2 GHz.
- 256 GB RAM, en módulos de 8GB ECC DDR3 1600MHz.
- VMWare versión 6.0.

que soportan conjuntamente un total de 95 máquinas virtuales.

Para hacer el backup, cuentan con:

- 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 8Gbps. Con interfaces suficientes de interconexión.
- Almacenamiento: Cabina con doble controladora con 50TB de capacidad neta con discos SAS de 15 Krpm, 120 TB de capacidad neta con discos SATA de 7,2Krpm, 8 puertos FC a 8Gbps y 2 puertos Ethernet 10GbE (FCoE, iSCSI).

El servicio de radiología ha introducido unos nuevos equipos de imágenes médicas. Dichos equipos permiten almacenar las imágenes en formato jpg, así como vídeos en H.264, junto con sus correspondientes informes. La información debe ser consultada por la aplicación Salud1clic de la Consejería de Sanidad, como parte del historial del paciente. El espacio máximo asignado son 50TB.

Elabore un documento de requisitos técnicos para poder realizar este backup en la nube, para que sirva de base para una licitación de un contrato llave en mano a riesgo del contratista.

Los puntos principales a desarrollar en este documento son:

2.1. Describa una política de backup adecuada que permita contar con un entorno de copia de seguridad en la nube a un coste económicamente asumible y ajustado al uso que se haga del servicio de imágenes médicas.

2.2. Describa los requisitos sobre los tipos de elementos que considere necesarios en el Hospital, tanto hardware, software, licencias, comunicaciones, etc. para optimizar la solución.

2.3. La solución debe contemplar todos aquellos requisitos y buenas prácticas que la legislación vigente y las autoridades establecen sobre este tipo de sistemas y datos. Describa todos aquellos acuerdos y condiciones a requerir a los prestadores del servicio.

2.4. Adaptación del Hospital a los requerimientos establecidos por el Esquema Nacional de Seguridad en lo relativo a la recuperación ante desastres, delimitado al nuevo sistema de imágenes médicas.

3. Protección de datos.

En el hospital se gestiona la siguiente información:

- Pacientes
- Lista de espera
- Urgencias
- Quirófanos
- Personal
- Investigación clínica

El hospital cuenta con un responsable de seguridad, que iba a ser designado por la Dirección de este centro de salud como Delegado de Protección de Datos.

No obstante, con motivo de la entrada en vigor de la nueva normativa en materia de protección de datos recibe la visita de un profesional de la privacidad que oferta sus servicios como delegado de protección de datos para:

- Adaptar los ficheros que actualmente posee el hospital al contenido del RGPD.
- Que le nombren como delegado de protección de datos.

Los servicios que le oferta esta persona son los siguientes:

- Asesorar al responsable del hospital sobre el contenido del RGPD.
- Actualizar la información gestionada al nuevo registro de ficheros que está preparando la AEPD para que los citados ficheros se adecuen al RGPD.
- Asignar responsabilidades al personal del hospital.
- Formar al personal.
- Implementar el nuevo nivel de seguridad, denominado “muy alto”, que regula el RGPD respecto a los datos de salud.
- Tramitar las denuncias de protección de datos ante la autoridad de control.
- Gestionar las tutelas de derechos.
- Elaborar las evaluaciones de impacto.
- Diseñar e implantar las políticas de protección de datos.

Conteste las siguientes cuestiones (razone todas las respuestas):

3.1. ¿Debe este hospital realmente nombrar un delegado de protección de datos?

3.2. Si nombrase un delegado de protección de datos, ¿podría ser externo o debe ser personal del hospital?

3.3. ¿Podría el hospital nombrar como delegado de protección de datos al responsable de seguridad?

3.4. ¿Debería elegir ese hospital a ese profesional como delegado de protección de datos atendiendo a los servicios que presta?

3.5. Con motivo de una mudanza de los archivos del hospital se produce una brecha de seguridad y se pierden los expedientes de algunos pacientes. ¿Cómo lo gestionaría? ¿A quiénes habría que comunicarlo? ¿En qué plazos?

4. Modelado de datos: Modelo Entidad/Relación.

Diseñe una base de datos para la gestión de las atenciones médicas del hospital siguiendo las especificaciones suministradas a continuación. Para ello, cree un diagrama entidad relación y una explicación razonada de su contenido. Si considera necesario hacer algunas asunciones o ampliaciones de la información suministrada, describa las mismas y justifíquelas.

La base de datos de los pacientes mantendrá sus datos personales (nombre, apellidos, teléfonos de contacto y número de la seguridad social – siendo éste único –), así como información acerca de los actos médicos que han recibido en el hospital (fecha, hora, motivo del acto e informe del mismo).

Cada acto médico estará identificado por un código numérico incremental denominado *actoId*.

Estos actos pueden ser consultas en urgencias o intervenciones quirúrgicas.

Para el caso de las consultas de urgencias, éstas llevan anexa información de triaje (informe de triaje y valoración de gravedad). En el caso de las intervenciones quirúrgicas se indica la duración de la intervención y el quirófano en que se han realizado.

Asimismo, el sistema contendrá información sobre el personal médico del hospital (nombre, apellidos, DNI – que será único – y especialidad), registrando por cada acto médico el miembro de la plantilla que ha estado a su cargo. Se ha de tener en cuenta que el personal médico se organiza de forma jerárquica y será necesario indicar quién es el supervisor/a de cada uno de ellos, en el caso de que lo tuviese.