SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Convocatoria 04/2017. Dos plazas de técnico de la UASI

Segundo ejercicio

Supuesto 1 Informática y gestión de datos

(10 puntos)

Proyecto de automatización de las tareas de auditoría de una entidad dedicada a la auditoría

Antecedentes:

En una entidad dedicada a la auditoría se está planificando un proyecto de automatización del trabajo de fiscalización.

La situación de partida es la siguiente:

- Hay 60 personas a que realizan tareas de auditoría en la entidad.
- El personal, actualmente utiliza únicamente paquetes ofimáticos.
- Todo el personal auditor de la entidad dispone de un portátil conectado en red con las herramientas básicas de ofimática, Internet y correo electrónico.
- Se dispone de una intranet sencilla de páginas estáticas.
- No existe ningún servidor de base de datos, dado que las bases de datos existentes hasta entonces no son cliente/servidor.
- El departamento de informática está compuesto por un responsable del departamento, 2 técnicos de desarrollo y 3 técnicos de explotación.

Se pide:

1. Enumerar los requerimientos que debería tener una aplicación que automatice el proceso de auditoría.
2. Razonar qué ventajas e inconvenientes tendría escoger entre: a) una o varias aplicaciones estándar, o b) una o más aplicaciones hechas a medida; razonar la elección.
3. Describir de manera resumida con un diagrama de flujo el proceso de auditoría a automatizar.
4. Suponer que el software escogido permite funcionar con una base de datos que no es cliente/servidor y en una que sí que lo es. Dado que es la entidad la que decide qué software de base de datos utiliza, razonar cuál es el escogido, y si sería necesario adquirir hardware para que funcionase aceptablemente.
5. Describir cómo se haría la gestión documental en esta automatización.

Supuesto 2 - Seguridad de los SI y control interno

(12 puntos)

Revisión de los CGTI

Antecedentes:

Un Órgano de Control Externo está realizando una auditoría financiera y de cumplimiento, en términos de seguridad razonable, sobre el gasto de personal de la Administración General de su Comunidad Autónoma, del ejercicio 2017.

Las obligaciones reconocidas totales del capítulo 1 ascienden 1.700 millones de euros, representativa de más de 47.000 empleados públicos.

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: el registro de personal, representativo del historial administrativo de cada empleado, la gestión de las relaciones de puestos de trabajo y las altas y bajas de personal. También realiza las nóminas mensuales, y tiene una interfaz con la aplicación de contabilidad.

A la Unidad de Auditoría de Sistemas de Información (UASI) nos han solicitado la colaboración en ese trabajo. Debemos revisar los sistemas de información y aplicaciones que soportan los procesos de gestión de los recursos humanos, la nómina y contabilidad, incluyendo la eficacia de los controles internos implantados en el sistema de información.

El sistema SGIP fue implantado en el año 2000 tras su desarrollo por la propia Administración con la asistencia técnica de varias empresas especializadas, y está soportado por una base de datos SQL. El servidor de la aplicación y de la base de datos está ubicado en el CPD corporativo.

La crisis económica provocó que en 2011 se paralizara cualquier tipo de actualización del software.

Las competencias para la captura de datos y su grabación en SIGP, gestión de actos administrativos, producción de documentos y generación de incidencias en nómina, corresponde a los 10 servicios territoriales de gestión de personal existentes, que cuentan en total con 150 funcionarios con algún tipo de acceso a los sistemas de gestión de personal.

La competencia para la aprobación de la nómina mensual corresponde a las/los Secretarias/os Administrativas/os de los servicios territoriales de gestión de personal. También corresponde a dichos órganos las comunicaciones con la Tesorería General de la Seguridad Social y con la Agencia Estatal de la Administración Tributaria.

La Intervención General de la Comunidad Autónoma, como órgano superior de control interno, ejerce las funciones de fiscalización y control, entre otras, de las nóminas y los actos administrativos que tengan repercusión en la misma.

Durante la fiscalización hemos observado lo siguiente:

1. Los controles respecto a la gestión y revisión de usuarios: altas, bajas, perfiles, privilegios, la normalización de la identificación, etc, son mejorables. No se ha elaborado y aprobado un procedimiento general por escrito que regule todos los aspectos de la gestión de usuarios y las revisiones periódicas de usuarios y sus privilegios.
2. Ciertos conceptos retributivos como el complemento de productividad, los devengos por incapacidad laboral o la carrera profesional los calcula el administrativo de recursos humanos en una hoja de cálculo que imprime y se la pasa al administrativo de nóminas que introduce los datos en SIGP el día anterior a la ejecución de la nómina mensual. Los controles posteriores no han detectado errores materiales. Las incidencias por bajas siguen el mismo procedimiento.
3. No se dispone de un plan de recuperación de la actividad debidamente aprobado, que garantice la recuperación en plazos preestablecidos de los elementos críticos del SIGP ante potenciales eventos adversos, accidentales o intencionados, que afecten gravemente a los activos (instalaciones, programas y datos) de este sistema.
4. No han realizado la auditoría bianual que exige la normativa sobre protección de datos. Tampoco se ha realizado el plan de adecuación al Esquema Nacional de Interoperabilidad ni al Esquema Nacional de Seguridad.
5. Los centros gestores no tienen una política de seguridad aprobada.
6. El departamento de sistemas no tiene un plan estratégico ni un presupuesto específico.
7. No hay un plan de concienciación sobre seguridad de la información en los centros gestores.
8. No existe un análisis de riesgos reciente (el último data de 2012).
9. Hemos verificado que existen un total de 300 usuarios activos con acceso a SIGP.
10. De estos hay 50 usuarios que han sido baja o se han trasladado a otros departamentos.
11. 40 usuarios no acceden a SIGP hace más de seis meses.
12. Hay una instrucción para que las contraseñas se cambien una vez al año.
13. Se ha comprobado que hay dos líneas de gestión de incidencias, una a través de una aplicación externa al SIGP y otra a través de la propia aplicación SIGP. En esta última se suelen corregir incidentes de tipo económico sin indicar el detalle del cálculo de las cuantías.
14. Hay 20 personas distintas, asignados al mismo usuario genérico. La mayoría es personal externo.
15. Existen personas físicas con hasta 6 usuarios asociados.
16. Aunque no existe un procedimiento de copias de seguridad debidamente aprobado, se hacen copias de seguridad de los datos cada tres meses, y las copias se custodian en un armario blindado en el CPD.
17. Nos han informado que el CPD cuenta con todas las medidas de seguridad, incluyendo aspersores de agua antiincendios.
18. En cada servicio territorial de gestión de personal el secretario administrativo es administrador de la base de datos, de forma que pueda modificar los datos con agilidad y corregir posibles errores que se dan con relativa frecuencia, de forma que no se retrasen las nóminas mensuales. Con la misma finalidad en el departamento de sistemas hay un usuario genérico administrador para que cualquiera de los informáticos pueda subsanar errores, pero únicamente en caso de urgente necesidad.
19. El Antivirus no se actualiza hace tres años.

Se pide:

1. Preparar un programa de auditoría para el equipo de la UASI para revisar los CGTI.
2. Diseñar un cuestionario de controles generales de tecnologías de la información, detallando las áreas y proponiendo, al menos, DIEZ preguntas o cuestiones, dos por cada una de las cinco áreas establecidas en MFSC-2850.
3. A partir de toda la información disponible preparar un detalle de los hallazgos de auditoría relativos a los CGTI con la siguiente estructura:

   Poner un máximo de DIEZ hallazgos, los más relevantes.

#	Situación observadas	Criterio de auditoría	Riesgo	Tipo de deficiencia	Recomendación
1			*Se describirá sucintamente el riesgo identificado, sus consecuencias potenciales y se valorará como:* *Alto/Medio/Bajo*	*Se calificarán según su importancia según metodología MFSC-2850*	
2					

Para responder este apartado se puede utilizar las hojas adjuntas preformateadas.

4. Determinar si alguna de las deficiencias anteriores afectarían a la auditoría financiera y fundamentarlo.
5. Cuál sería nuestra conclusión-opinión de auditoría sobre los CGTI.

Supuesto 3 Auditoría

(9 puntos)

Planificación de la auditoría. Identificación de riesgos. recomendaciones

Antecedentes:

Somos un auditor al que han encomendado planificar y ejecutar la auditoria de las cuentas anuales de 2017 de la Entidad X, prestadora de servicios al ciudadano.

En estos momentos estamos en una fase inicial del trabajo y solo disponemos de la información que se señala a continuación, pero debemos hacer una planificación preliminar de la auditoria con la información disponible.

Cuentas anuales de 2017 (cifras en miles de euros):

Balance

Activo		Pasivo	
85.000	Inmovilizado	Fondos propios	-30.000
15.000	Deudores	Préstamos a L.P.	100.000
20.000	Tesorería	Proveedores	40.000
110.000			**110.000**

Liquidación del presupuesto

Derechos reconocidos		Obligaciones reconocidas	
550.000	4. Transferencias	1. Gastos personal	270.000
35.000	9. Pasivos financieros	2. Compras de bienes y servicios	250.000
		3. Gastos financieros	10.000
		6. Inversiones	55.000
585.000	**Total**	**Total**	**585.000**

La entidad tiene 5.500 empleados

Las transferencias las recibe del Estado por dozavas partes.

Nos han informado que las principales aplicaciones informáticas utilizadas son:

Proceso	Aplicación	B.D.	S.O. Servidor
Contabilidad	CONTAMAX	Oracle	Linux
RR.HH. y nóminas	HUMAN+	Oracle	Linux
Compras	SAP	Oracle	Linux
Correo electrónico	Outlook	-	WS
Tesorería	SAP	Oracle	Linux

Durante las pruebas preliminares se ha observado lo siguiente:

En una primera revisión, hemos observado los siguientes privilegios en las aplicaciones:

ID Usuario	Personal HUMAN+	Contabilidad CONTAMAX	Compras SAP	Tesorería SAP
SECADM001	Actualizar Fichero Maestro. Autorizar nóminas. Autorizar contrataciones.	Autorizar documentos "O"	SAP_ALL	SAP_ALL
SECADM002		Contabilizar nómina	SAP_ALL	SAP_ALL
SECADM003			SAP_ALL	SAP_ALL
SECADM004			SAP_ALL	SAP_ALL
SECADM005	Aprobar variaciones de nómina.		SAP_ALL	SAP_ALL
SECADM006			SAP_ALL	SAP_ALL
SECADM007			SAP_ALL	SAP_ALL
UDINF008			SAP_ALL	SAP_ALL
UDINF009			SAP_ALL	SAP_ALL
UDINF010			SAP_ALL	SAP_ALL
UDINF011			SAP_ALL	SAP_ALL
UDINF012			SAP_ALL	SAP_ALL
USER0013	Actualizar Fichero Maestro			
USER014			Actualización Fichero Maestro de proveedores. Autorización compras.	Autorización pagos.
USER015	Introducir variaciones de nómina.	Actualización Fichero Maestro		
USER0016			Autorización compras.	Autorización pagos.
USER017				Autorizar pagos. Aprueba conciliaciones bancarias.
USER0018	Ordenar el pago de la nómina.	Contabilizar nómina. Conciliar transferencias de nómina con el resumen de la nómina.		

El secretario administrativo de la entidad y seis funcionarios más de su unidad, y cinco funcionarios del departamento de informática tienen privilegios SAP_ALL y son administradores de la BD Oracle de CONTAMAX.

Se pide:

1º Calcular y razonar, de acuerdo con la GPF-OCEX 1320:

- El nivel de importancia relativa.
- El nivel de importancia relativa para la ejecución del trabajo.
- El umbral de las incorrecciones claramente insignificantes.

2º Señale:

- En qué áreas focalizará la auditoria.
- Qué tipos de transacciones se podrán considerar significativas.
- Qué procesos de gestión serán significativos.
- Qué aplicaciones serán significativas.
- ¿Se percibe algún riesgo significativo?

3º Determine y razone qué estrategia preliminar de auditoría adoptaremos: Mezcla de pruebas de controles y sustantivas, uso de especialistas TI, en qué áreas, uso de CAAT, etc.

4º Señale los conflictos de segregación de funciones existentes (SdF), cualquier deficiencia con impacto en una adecuada SdF, y el efecto general sobre el control interno.

5º Efectúe las recomendaciones que estime oportuno.