AUDITORIA DE SISTEMAS

Trabajo Práctico Nº 4

1. ¿Qué debe contener el plan estratégico de una organización? ¿Y el plan operacional? De la siguiente lista de elementos, elija cuales deben ser incluidos en el plan estratégico, cuales en el plan operacional y cuales en ninguno de los dos, justificando la respuesta en cada caso:
    - Análisis de objetivos de negocio futuros
    - Fechas de entrega estimadas para proyectos
    - Presupuestos ideales para el departamento de SI en los próximos años
    - Especificaciones detalladas del HW a adquirir
    - Plan de backup de los servidores
2. Suponga un área de sistemas para el DCIC conformada por un analista programador, dos programadores junior un administrador de base de datos.
    a. ¿Es suficiente?
    b. Indique cómo evaluaría las funciones de cada rol desde su posición de auditor de SI.
3. Ejemplifique riesgos que se pueden mencionar debido a una incorrecta separación de obligaciones para un sistema comercial.
4. ¿Cuál de las siguientes es la principal responsabilidad de un data security officer? Justifique.
    - Recomendar y monitorear políticas para la seguridad de los datos
    - Gestionar controles de acceso físicos y lógicos
5. ¿Qué medidas se pueden tomar para intentar asegurar la separación de funciones?
6. Suponga que la organización es mediana y debido al escaso personal no pueden separarse las funciones adecuadamente, ¿qué actitud debemos tomar?
7. Cuales de las siguientes funciones pueden ser realizadas por la misma persona sin que estos sea un problema desde el punto de vista de la separación de obligaciones?
    - Administración de la seguridad y gestión de los cambios
    - Desarrollo de sistemas y operación de sistemas
    - Desarrollo de sistemas y mantenimiento de sistemas

Justifique en cada caso su respuesta, sea esta negativa o positiva.

8. ¿Qué frameworks de IT governance conoce?
9. ¿Dónde debería ubicarse la función de TI dentro del organigrama de una organización? ¿Por qué?
10. ¿Qué ítems tiene en cuenta el auditor para evaluar la Función de Control de la Gerencia?

11. ¿Cuál es la función de las políticas de una organización?¿Y de los procedimientos?¿Cuál es la diferencia?
12. ¿Qué debe tener en cuenta un auditor al evaluar las políticas y los procedimientos de una organización dada?¿Qué sucede en el caso que no existan políticas o procedimientos?
13. Dada la siguiente situación plantee un análisis de riesgo: "… Durante el último fin de semana hubo un corte de luz que afectó las comunicaciones de la empresa impidiendo las ventas on-line …"
14. ¿Cuál es el objetivo de RiskIT?¿Cuáles son sus dominios y como interactúan entre sí?
15. ¿Qué controles debe verificar el auditor en el contexto del manejo de RRHH?
16. Suponga que se ha decidido tercerizar el servicio de hosting de la página web de una organización que tiene un servicio de venta online de sus productos (autopartes de vehículos). Esta organización tiene un volumen considerable de ventas dentro del país. ¿Qué riesgos debe tener en cuenta el auditor? ¿Qué debe revisar el auditor para evaluar si se ha realizado correctamente el contrato?
17. ¿Cómo se puede auditar un Plan de Continuidad de Negocios?
18. Enumere las fases que debería contemplar un Plan de Recuperación de Desastres.
19. ¿Qué es un Plan de Backup? ¿Qué consideraciones se deben tener en cuenta? ¿Qué alternativas existen con respecto a la elección del sitio de backup? Justifique que alternativa elegiría en cada caso:
    - Plan de backup para una agencia clave de seguridad nacional.
    - Plan de backup para una cadena de venta de materiales de contrucción con cinco sucursales distribuídas en todo el país.
20. ¿Se pueden establecer controles sobre los planes de backup? ¿Cuáles?
21. Desarrolle un plan de Recuperación de Desastres para su PC de uso cotidiano en la que realiza sus tareas diarias
22. ¿Cual de las siguientes tareas es una responsabilidad primaria del departamento de SI y por qué?:
    - Desarrollar el plan de continuidad del negocio
    - Restaurar los datos y los sistemas de IT luego de ocurrido un desastre