AUDITORIA DE SISTEMAS

Trabajo Práctico Nº 3

1. ¿Cuáles son las tareas que debe realizar un gerente y que un auditor puede evaluar?
2. Brevemente describa cada uno de los dos planes que deben realizarse para la función de sistemas de información.
3. ¿Qué criterio utiliza McFarlan para clasificar los tipos de organizaciones con respecto a los sistemas de información? ¿Cómo es la clasificación? Elegir dos de las clasificaciones y ejemplificar situaciones que estén comprendidas en las mismas.
4. Qué criterio utiliza Sullivan para clasificar los tipos de organizaciones con respecto a los sistemas de información? ¿Cómo es la clasificación? Elegir dos de las clasificaciones y ejemplificar situaciones que estén comprendidas en las mismas.
5. ¿Por qué es importante que el auditor tenga en cuenta estas clasificaciones?
6. ¿Qué entiende por frameworks para e-gobernance? ¿Conoce alguno? ¿Qué debe hacer el auditor para estos casos?
7. ¿Qué es "information Secure Governance"? ¿De qué se ocupa? Desde el punto de vista de Auditoría, ¿nos asegura algo?
8. Defina Política y Procedimientos
9. Dada su PC de escritorio, establezca políticas y procedimientos de:
    - Seguridad de acceso
    - Seguridad física
    - Resguardos de datos

10. Desarrolle un programa de Manejo de Riesgo para: "Protección de su PC de desarrollo"
11. Para cada una de las siguientes funciones, identifique controles que la alta gerencia debería efectuar.
    i) Incorporación de personal
    ii) Finalización de servicios
12. ¿Por qué los auditores deben evaluar si existen planes de capacitación del personal?
13. Para la gerencia de SI ¿Cuáles son los principales factores a tener en cuenta para realizar un liderazgo eficiente?
12. Suponga que es el de Administrador de SI del DCIC ¿Qué aspectos tendría en cuenta al momento de invertir en el área de sistemas?
13. (cont.) Se le ha comunicado que viene el auditor interno de la UNS, ¿qué solicitará?

Caso de Estudio

14. Una organización ha implementado una aplicación para soportar sus procesos de negocios. Llegó a un entendimiento con el vendedor de la aplicación para mantenimiento y soporte para usuarios y administradores del sistema. Este soporte es provisto en forma remota utilizando un acceso irrestricto tanto de lectura como de escritura a todos los archivos existentes en el server donde está operativa la aplicación. El acceso se logra mediante la utilización de un usuario especial (super user). Se mantiene un log de actividades por 90 días.

    i. ¿En cuál de los siguientes aspectos deberíamos tener mayor atención?
        A. Los logs de actividades se mantengan por 90 días.
        B. El acceso al usuario especial es remoto
        C. El usuario especial puede alterar el log de actividades
        D. El vendedor de sistemas puede testear e implementar paquetes de software en nuestros servers.

¿Por qué?

    ii. ¿Cuál de las siguientes acciones sería más efectiva para reducir el riesgo respecto de la utilización de la cuenta de usuario especial?
        A. La cuenta especial se encuentra deshabilitada excepto cuando se requiera mantenimiento.
        B. Todo uso de esa cuenta deberá ser mantenido en un log.
        C. Se debe modificar el acuerdo de tal forma que todo mantenimiento sea realizado in-situ
        D. Todos los paquetes de actualización deberían ser aprobados previos a su implementación.

¿Por qué?