ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
INGENIERÍA EN AUDITORÍA Y CONTROL DE GESTIÓN
AUDITORÍA DE APLICACIONES INFORMÁTICOS
***P*rimera Evaluación – I Término**
08/Julio/2009

Nombre: _____ Paralelo:___

Examen: _____
Lecciones: _____
Deberes: _____

Tema I: Conceptos (20 puntos, 5 puntos cada una)

1. *Defina que es riesgo, explique cómo se puede valorizar el risgo y la importancia de desarrollar esto.*
2. *Defina auditoría informática, explique brevemente la importancia de la misma en una organización.*
3. *Qué es el control interno informático?, Mencione los objetivos del control interno.*
4. *¿Qué es COBIT?, mencione los elementos que lo conforman.*

Tema II: CISA (15 puntos, 5 puntos cada una)

5. *La alta gerencia ha solicitado que un auditor de TI asista a la gerencia departamental en la implementación de los controles necesarios. El auditor de SI debería:*
   a. *Rehusar la asignación ya que no es la función del auditor de SI*
   b. *Informar a la gerencia de su incapacidad para llevar a cabo futuras auditorías.*
   c. *Realizar la asignación y las futuras auditorías con debido cuidado profesional.*
   d. *Obtener la aprobación de la gerencia usuaria para realizar la implementación y seguimiento.*
6. *Durante una auditoría de aplicaciones, el auditor de SI encuentra varios problemas relacionados con datos corruptos en la base de datos. ¿Cuál de los siguientes es un control correctivo que debe ser recomendado por el auditor de SI?*
   a. *Implementar procedimientos de copias de respaldo de datos y de recuperación*
   b. *Definir estándares y monitorear de cerca el cumplimiento.*
   c. *Asegurar que sólo el personal autorizado pueda actualizar la base de datos.*
   d. *Establecer controles para manejar los problemas concurrentes de acceso.*
7. *Un auditor de SI está auditando los controles relativos al despido/retiro de empleados. ¿Cuál de los siguientes aspectos es el más importante que debe ser revisado?*
   a. *El personal relacionado de la compañía es notificado sobre el despido/retiro.*
   b. *El usuario y las contraseñas del empleado han sido eliminadas.*
   c. *Los detalles de empleado han sido eliminados de los archivos activos de la nómina.*
   d. *Los bienes de la compañía provistos al empleado han sido devueltos.*

Tema III. Seguridad Física (20 puntos)

Realice una revisión para el área de control: Seguridad de la información considerando el objetivo de control Restricciones de acceso físico son puestas en práctica y administradas para asegurar que los individuos sólo autorizados tienen la capacidad de tener acceso y uso de los recursos de la información.
Las actividades de control son:

- *Mecanismo de control de acceso físico se está utilizando para registrar y restringir el acceso a áreas protegidas y la autoridad para cambiar mecanismos de control de acceso físicos es limitada para asignar el personal.*
- *El acceso físico al edificio es supervisado y restringido.*

Determinar:

a. *4 riesgos asociados al acceso físico para la seguridad de la información.*
b. *Para cada actividad de control realice una prueba de cumplimiento y prueba demostrativas(evaluación).*
c. *Defina 3 políticas de seguridad de la información relacionada al acceso físico.*

Tema IV. Análisis de Riesgo (45 puntos)

En una revisión a un centro de cómputo se pudo observar lo siguiente:

- *No existen políticas formalmente documentadas de seguridad de información.*
- *El sistema transacciones donde se maneja el Core Business del negocio, el cual se requiere que opere de 8:00 a 17:00 horas ininterrumpida, depende totalmente de un servidor ubicado en la oficina matriz.*
- *Los respaldo Backup no tiene una periodicidad de generación.*
- *No existe sistema contra incendio, extintores, ni señales de emergencia.*
- *Inventario de activos desactualizado (hace 2 años).*

Además se identificaron:

- *El centro cómputo se implemento un sistema que monitorea el volumen de transacciones procesadas.*
- *Poseen licencias de Antivirus actualizadas*
- *Un reporte con el inventario de activos de software y hardware.*
- *Se generan copias de seguridad del servidor de datos.*

Realice un análisis de riesgo cualitativo considerando:

- *Identificación de riesgos presentes en la situación anterior.*
- *Análisis de evaluación del riesgo de forma cualitativa, determinando ocurrencia, nivel de impacto, severidad, efectividad de controles y valor residual para cada riesgo. Justificar valor de efectividad del control.*
- *Realice un diagrama causa efecto para el riesgo de mayor severidad.*
- *Para los dos riesgos más severos, establezca dos controles para cada uno.*

Bono (3 puntos)

¿Explique los principios de seguridad de la información?