



Examen: \_\_\_\_

Lecciones: \_\_\_\_

Deberes: \_\_\_\_

**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**

**Ingeniería en Auditoría y Control de Gestión**

***AUDITORÍA DE APLICACIONES INFORMÁTICOS***

***Pr*imera Evaluación – II Término**

**9/Diciembre/2010**

Nombre: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Paralelo:\_\_\_

**Tema I: Conceptos** (20 puntos, 4 puntos cada una)

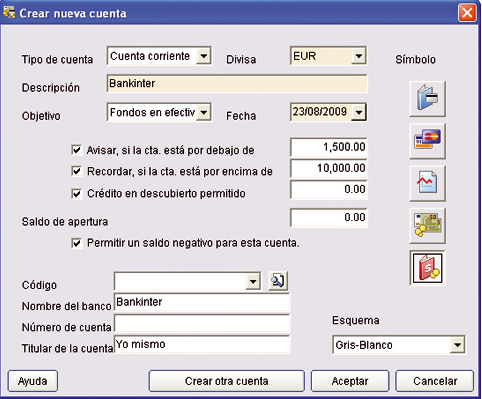
1. *Defina que es riesgo, explique cómo se puede valorizar el riesgo y la importancia de desarrollar esto.*
2. *Defina auditoría informática, explique brevemente la importancia de la misma en una organización.*
3. *Explique los 3 principios de seguridad de información.*
4. *¿Qué es control interno?, mencione los elementos que lo conforman.*
5. *¿Qué es COBIT?, mencione sus Dominios.*

**Tema II: CISA** (10 puntos, 5 puntos cada una)

1. *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:*
   1. *Rehusar la asignación ya que no es la función del auditor de SI*
   2. *Informar a la gerencia de su incapacidad para llevar a cabo futuras auditorías.*
   3. *Realizar la asignación y las futuras auditorías con debido cuidado profesional.*
   4. *Obtener la aprobación de la gerencia usuaria para realizar la implementación y seguimiento.*
2. *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?*
   1. *El personal relacionado de la compañía es notificado sobre el despido/retiro.*
   2. *El usuario y las contraseñas del empleado han sido eliminadas.*
   3. *Los detalles de empleado han sido eliminados de los archivos activos de la nómina.*
   4. *Los bienes de la compañía provistos al empleado han sido devueltos.*

**Tema III. Pruebas** (20 puntos)

*Dada la siguiente interfaz para crear nueva cuenta:*



**Diseñe:**

* *Prueba de caja negra para evaluar del criterío funcionalidad adecuación y exactitud de operación del modulo (enfoque proceso y validación).*
* *Diseñe una cuestionario de 5 preguntas para evaluar la capacidad de operación del criterio Usabilidad.*

**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. No se cumplen ciertas mediadas de seguridad en el manejo de contraseñas permitiendo que las mismas estén formadas de un solo caracterer y no sean cambiadas de forma obligatoria cada cierto periodo.*
* *Servidor de datos ha presentado ciertos problemas debido a que es un equipo deteriorado.*
* *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 respaldos son se generan periódicamente y se encuentra almacenados en las instalaciones del centro de cómputo.*
* *No existe sistema contra incendio, extintores actualizados, ni señales de emergencia.*
* *Inventario de activos se encuentra desactualizado (hace 2 años).*

*Además se identificaron:*

* *El centro cómputo se implemento un sistema que monitorea el volumen de transacciones procesadas.*
* *Un reporte con el inventario de activos de software y hardware.*
* *El DBA genera copias de seguridad del servidor de datos.*
* *Posee extintor contra incendio al inicio del centro de cómputo.*

*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.*