|  |  |  |
| --- | --- | --- |
|  | **ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**  **FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICAS**  **DEPARTAMENTO DE MATEMÁTICAS**  TERCERA EVALUACIÓN DE AUDITORIA DE APLICACIONES INFORMÁTICAS  MARZO DE 2015 |  |

MATRICULA: NOMBRE: PARALELO:

|  |  |
| --- | --- |
| **NOTA**: Este examen está diseñado para ser resuelto de manera individual, puede usar un esferográfico.  Solo puede comunicarse con la persona responsable de la recepción del examen; y, cualquier instrumento de comunicación que hubiera traído, deberá apagarlo y ponerlo en la parte anterior del aula, junto con algún otro material que se encuentre acompañándolo. No consultará: libros, notas, algún apunte adicional a las que se entreguen en esta evaluación, ni tampoco utilizará calculadoras o cualquier otro instrumento de cálculo automatizado. Desarrolle los temas de manera ordenada.  ***Firme como constancia de haber leído lo anterior***. | Firma |

Preguntas (70 ptos)

1. Cuál **no** es un propósito del análisis de riesgos?
   1. Soporta decisiones de auditoria basadas en riesgos
   2. Ayuda al auditor a determiner los objetivos de auditoria
   3. garantiza seguridad absoluta durante la auditoria
   4. Ayuda al auditor a identificar los riesgos y amenazas
2. ¿Cuál es la diferencia entre una amenaza y una vulnerabilidad?  
   A. Las amenazas son el camino que puede ser explotada por una vulnerabilidad.  
   B. Las amenazas son los riesgos y se convierten en una vulnerabilidad en caso de que ocurran.  
   C. Las vulnerabilidades son un camino que puede ser tomado por una amenaza, lo que resulta en una pérdida.  
   D. La vulnerabilidad es un evento negativo que causará una pérdida si se produce.
3. 19. ¿Cuáles son los nombres de los cuatro métodos de respuesta al riesgo?  
   A. Evitar, aceptar, transferir y mitigar  
   B. Mitigar, aceptar, transferir y reducir  
   C. No haga caso, aceptar, asignar, y mitigar  
   D. Analizar, mitigar, reducir y asignar
4. Modelo de Madurez COBIT permite el propietario del proceso referencia para:
   1. La medida relativa de las metas de proceso y un conjunto de mejoras
   2. Los controles de los objetivos del proceso actual y establecer las prácticas de control
   3. Las responsabilidades del proceso en curso y los objetivos establecidos para la rendición de cuentas
   4. Medidas del proceso actual y fijar objetivos para los indicadores de meta
5. ¿Qué nivel de madurez en los procesos de TI de COBIT se asocia generalmente con un proceso sometido a vigilancia?
   1. Nivel 1 – Inicial
   2. Nivel 3 – Definido
   3. Nivel 2 – Repetible
   4. Nivel 4 – Gestionado
6. ¿Cuál de los siguientes es un beneficio de la alineación estratégica?
   1. El mantenimiento de los recursos especializados
   2. La creación de software de alta calidad
   3. Cumplimiento de los plazos del proyecto
   4. El uso óptimo de los recursos de TI
7. Los dominios de COBIT proporcionan grupos lógicos para:
   1. Modelos de Madurez
   2. Recursos de TI
   3. Los criterios de información
   4. Procesos de TI
8. ¿Cuál de los siguientes es un requisito de seguridad en la información de COBIT. Criterios?
   1. Entrega
   2. Eficacia
   3. Confidencialidad
   4. Calidad
9. ¿Cuál de dominio COBIT se centra en la estrategia, la táctica y la visión de lo planeado?
   1. Monitorear y evaluar
   2. Planificar y Organizar
   3. Entregar y dar soporte
   4. Adquirir e Implementar
10. ¿Qué nivel de madurez en los procesos de COBIT se asocia con mejores prácticas?
    1. Nivel 3 – Definido
    2. Nivel 4 – Gestionado
    3. Nivel 2 – Repetible
    4. Nivel 5 – Optimizado
11. Considere los siguientes riesgos y determine una medida de respuesta al riesgo para cada uno de ellos indicando que tipo de medida es (Evitar, Aceptación, transferencia o mitigación).
    1. Daños en el servidor causados por interrupción de energía eléctrica
    2. Infección de virus
    3. Acceso no autorizado en aplicaciones
    4. Incumplimiento de proveedor de sistemas
12. Indique la secuencia correcta para el proceso de evaluación de riesgos.

* Determinación de la probabilidad
* Análisis de controles actuales
* análisis de Impacto
* Determinación del riesgo
* Identificación de amenazas
* Identificación de vulnerabilidades
* Recomendaciones de control

1. Identifique a qué principio de seguridad afectan los siguientes incidentes.

a.- Utilizar páginas web falsas para apropiarse de claves privadas.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

b.- Acceso a información de la empresa través de redes inalámbricas sin autorización. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

c.- ataque de correo spam hasta bloquear el servicio. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

d.- Cambios en los datos de transacciones para beneficiarse. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

e.- Suspensión de la energía eléctrica que alimenta a servidores.. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

14 Identifique cuál de los siguientes aspectos no corresponde a la evaluación de la etapa de desarrollo de un sistema. Se auditan:

* + Programas
  + Diseño de programas
  + Lenguaje utilizado
  + Costos
  + Características del hardware utilizado

**Casos (30 ptos):**

1.- El registro siguiente proporciona información sobre tiempos de empleados para la confección de la nómina de una empresa:

|  |  |
| --- | --- |
| **Campo** | **Formato y tamaño del campo** |
| Número de empleado | Numérico, 6 caracteres. |
| Horas normales | Numérico, 2 caracteres. |
| Horas extras | Numérico, 2 caracteres. |
| Gastos / comisiones | Numérico, 6 caracteres. Cuatro enteros y dos decimales. |
| Ausencias por enfermedad | Numérico, 2 caracteres. |
| Vacaciones | Numérico, 2 caracteres. |

¿Qué controles de validación se deben de establecer sobre cada campo? Suponer los valores de los datos que sean necesarios para realizar las pruebas, siempre que sean valores razonables. Todos los campos son de longitud fija.

2.- La empresa Axis especializada en desarrollo de sistemas empresariales, fue contratada para desarrollar un Sistema Integrado en una institución pública en un plazo de 2 años. Luego de haber realizado 2 prórrogas Axis no ha presentado avances del sistema y ha solicitado el pago que corresponde a la fecha, indicando que el sistema ya está terminado. La institución pública solicita realizar pruebas que permitan verificar el avance. Para esto se le consulta a Ud. Cuales son las pruebas requeridas para aprobar el pago. Realice un informe que indique las pruebas y explique en que consisten.