1. El auditor de sistemas reporta a:
    a. Alta gerencia **[Verdadera]**

2. El proceso de Auditoría comprende:
    1. Planificar
    2. Recolectar evidencia
    3. Evaluar evidencia
    4. Comunicar resultados

3. Objetivos de auditoría
    a. Preservar activos
    b. Eficacia en logro de objetivos
    c. Integridad de datos
    d. Cumplimiento de normativas
    e. Eficiencia en uso de recursos

4. Un auditor de sistemas
    a. Puede ser un profesional de ciencias económicas
    b. Puede no tener formación en sistemas

5. El comité de Auditoría puede estar está conformado por
    a. El auditor externo
    b. El auditor interno
    c. Oficial ejecutivo

6. Al terminar la auditoría comenzamos el análisis de riesgo.
    [Falso]

7. Un auditor de SI debería asegurar que las medidas de rendimiento de la gobernanza de TI:
    a. evalúa las actividades de IT comprometidas

8. ¿Cuál de los siguientes tipos de auditorías asume la ausencia de controles de compensación en el área que se está revisando?
    a. riesgo inherente

9. Al auditar la seguridad lógica, el auditor de SI está más preocupado al observar:
    d. la cuenta de admin del sistema es conocida por todo el mundo

10. Desde el punto de vista de auditoría de sistemas, cuál de los siguientes es el activo más importante en un sistema de información
    b. Personal

11. Si un software propietario es robado, cuál de los objetivos de auditoría se ve afectado
    a. Resguardar los activos

12. En un sistema computarizado las líneas de autoridad y responsabilidad son difíciles de llevar a cabo porque:
    a. Los recursos son compartidos y la propiedad es difícil de asignar
    [Verdadera]

13. En sistema computarizado las pistas de auditoría
    a. A menudo son más extensas que las pistas de auditoría manuales, si están designadas adecuadamente.

14. Comparado con sistemas manuales la supervisión del personal en un sistema computarizado es
    a. Más complejas porque muchas actividades se realizan digitalmente y en forma remota

15. Comparadas con un sistema manual en un sistema computarizado los bienes y datos tienden a estar
    a. Más concentrados en una misma locación

16. En un sistema computarizado se torna dificultoso evaluar el sistema de autorizaciones generales porque están
    a. Embebidas en los programas

17. Comparado con un sistema manual, en un sistema computarizado
    a. Cambian las metodologías para implementar los controles

18. En un sistema computarizado los datos incorrectos causan consecuencias más serias a
    a. Sistemas de control de gestión

19. Un sistema de procesamiento efectivo
    a. Alcanza en forma satisfactoria los objetivos de los usuarios

20. Cual de las siguientes aseveraciones relativas al personal de sistemas es falsa
    a. El personal de sistemas tiene menos poder que el personal que trabaja en sistemas manuales.

21. Los controles generales:
    a. Establecen un marco para los controles de aplicación

22. Comparado con un sistema manual, la consecuencia de errores computacionales a menudo es más seria porque **(revisar, la que no es seguro es la que comienza con los usuarios)**
    a. Los errores en un sistema de computación son generados a gran velocidad y el costo de su corrección puede ser grande.

23. Dado que los sistemas computarizados tienen la capacidad de realizar controles de bienes, ¿cuál de los siguientes puntos es más importante para un auditor?
    D. Contar con controles sobre el desarrollo, mantenimiento y modificación de aplicaciones

24. Una política:
    a. Es de cumplimiento obligatorio
    b. Es reconocida (firmada o aceptada) por las autoridades administrativas

25. Un abuso computacional está mejor definido por
    a. Cualquier incidente asociado con tecnología de computadoras donde una víctima sufre pérdidas y el autor del incidente obtiene ganancias

26. Una guía:
    a. Son acciones a considerar si no se puede aplicar un standard
    b. Son de uso discrecional

27. En una organización que produce manufacturas, la pérdida de cuál de los siguientes archivos tiene consecuencias más graves
    a. Archivo de inventario

28. Relacionado con fraude y malversación, fraude y malversación computarizada parece ser
    a. De tamaño más grande

29. En un sistema de basado en computadoras, la separación de obligaciones
    a. Debe ser implementada de forma diferente a un sistema manual

30. Cuando hablamos de evaluación del Riesgo ¿Cuál es su orden de proceso?
    a. Paso 1 Identificar los objetivos de negocio
    b. Paso 2 Identificar los bienes
    c. Paso 3 Realizar la evaluación del Riesgo
    d. Paso 4 Realizar el tratamiento del Riesgo
    e. Paso 5 Realizar evaluaciones periódicas del Riesgo

31. Los riesgos de IT deben manejarse diferente que otros riesgos en la organización
    [Falso]

32. En el mantenimiento adaptativo se realizan modificaciones para mejorar la eficiencia del procesamiento.
    [Falso]

33. Para controlar en forma más efectiva el acceso a los sistemas por personas no autorizadas (hackers). ¿Qué control es más efectivo?
    b. passwords robustas

34. De los siguientes objetivos cuál parece ser más un objetivo en el diseño de un procedimiento
    a. Contar con la mayor documentación posible **mmm dijo la muda**
    b. Especificaciones mínimas posibles
    c. Documentación lo menos formal posible **creo q es esta en vez de la A**
    d. Diferenciarse de los otros procedimientos

35. La responsabilidad más importante de un oficial de seguridad de datos es:
    d. recomendar y monitorear las políticas de seguridad de datos

36. Los controles deberían **[prevenir o reducir]** la probabilidad de que el evento de riesgo ocurra, **[detectar]** la ocurrencia, **[minimizar]** el impacto o **[transferir]** el riesgo

37. Los riesgos IT son dinámicos:
[Verdadero]

38. El plan de continuidad de negocios no es es responsabilidad directa de la gerencia de sistemas. **VERDADERO.**

39. En cuanto a la instalación de sistemas:
Discontinuación abrupta **[**No hay vuelta atrás, **(3) reduce costos de conversión]**
Instalación por etapas **[(1) Transición es ordenada,** dificultad para usuarios + las 2 de arriba**]**
Instalación en paralelo **[** Corren en paralelo, **(2) menor riesgo,** más dificultad, más costos**]**

40. De las siguientes tipos de backups, ¿Cual es el que necesita mas uso de hardware?
Hot site.

41. Si una entidad ***UTILIZA UN PROVEEDOR*** de servicios de sistemas, ¿Como debe evaluar el auditor de IS el backup y el procesamiento por lotes dentro de las operaciones informáticas?
d. confiar en el informe del auditor de servicios
(chequear bien que diga proveedor de servicios, si no es otra respuesta)

42. El principal objetivo de los testeos sobre controles es:
a. determinar si existen errores en esas clases de transacciones.
b. Determinar si un control está en su lugar.
c. Identificar patrones de error e irregularidades que pueden existir en los balances finales
d. Determinar si los controles están operando efectivamente.

43. Una organización realiza backups diariamente para los archivos con datos y software críticos resguardando una copia en otra locación. Estos backups se guardan para restaurar los sistemas en casos de fallas. Esto es un:
d. **control correctivo**

44. Para evaluar la función de dirección, es más relevante
b. **basarse en variables tales como la rotación de personal, nivel de ausentismo, frecuencia de faltas de los proyectos en cuanto a tiempos de implementación**

45. Básicamente el foco de mantenimiento correctivo es:
Remover los errores lógicos del sistema

46. En el mantenimiento correctivo se modifican cambios en el sistema para adaptarlos al entorno . **FALSO**

47. De los siguientes cual parece ser un control preventivo
Estándares de métodos.

48. ¿A qué se corresponden cada uno de estos ítems?:

Se definen los procedimientos para restaurar las capacidades completas de los

SI. =>
Plan de Recuperación.

Se deben ejecutar periódicamente, esto es simular los desastres y requerir al personal que cumpla con los procedimientos estipulados en los planes. =>
Plan de Testeo.

Inventario de insumos críticos almacenados de manera segura en el sitio y fuera del sitio, con listas de vendedores que provean los insumos. =>
Plan de Backup.

49. La evolución de la tecnología necesita ser controlada porque :
Debido a que la tecnología es neutral, su uso puede producir problemas sociales.

Preguntas de diapo:

¿Cuál es la mejor definición del concepto de diligencia debida?

A. Proporcional al nivel de riesgo o pérdida que podría producirse

¿Cuál de las siguientes opciones describe la relación entre las pruebas de cumplimiento y las pruebas sustantivas / testing sustantivo?

A. Las pruebas de cumplimiento comprueban la presencia de controles; las pruebas sustantivas comprueban la integridad de los contenidos internos.

Preguntas traducidas

1-1
¿Cuál de los siguientes puntos describe la autoridad general para realizar una auditoría de SI?
A. El alcance de la auditoría con metas y objetivos
B. Una solicitud de la dirección para realizar una auditoría
C. La carta de auditoría aprobada
D. El programa de auditoría aprobado

1-2
En la realización de una auditoría basada en el riesgo, ¿qué evaluación de riesgos completa PRIMERO un auditor de SI?
A. La evaluación del riesgo de detección
B. Evaluación del riesgo de control
C. Evaluación del riesgo inherente
D. Evaluación del riesgo de fraude

1-3
¿En cuál de los siguientes aspectos es más probable que se centre un auditor de SI al desarrollar un programa de auditoría basado en el riesgo?
A. Procesos de negocio
B. Controles administrativos
C. Controles ambientales
D. Estrategias empresariales

1-4
¿Cuál de los siguientes tipos de riesgo de auditoría supone la ausencia de controles compensatorios en el área
que se está revisando?
A. Riesgo de control
B. Riesgo de detección
C. Riesgo inherente
D. Riesgo de muestreo

1-5
Un auditor de SI que realiza una revisión de los controles de una aplicación encuentra una debilidad en el software del sistema que podría afectar materialmente a la aplicación. En esta situación, un auditor de SI debería:
A. Ignorar estas debilidades de control porque una revisión del software del sistema está más allá del alcance de esta revisión.
B. Llevar a cabo una revisión detallada del software del sistema e informar sobre las debilidades de control.
C. Incluir en el informe una declaración de que la auditoría se limitó a una revisión de los controles de la aplicación.

D. Revisar los controles del software del sistema según corresponda y recomendar una revisión detallada del software del sistema.

1-6
¿Cuál de las siguientes es la razón MÁS importante por la que un proceso de planificación de auditoría debería revisarse a intervalos periódicos?
A. Para planificar el despliegue de los recursos de auditoría disponibles
B. Para considerar los cambios en el entorno de riesgo
C. Proporcionar información para la documentación de la carta de auditoría
D. Identificar las normas de auditoría de SI aplicables

1-7
¿Cuál de las siguientes opciones es la MÁS eficaz para llevar a cabo una autoevaluación del control en las pequeñas empresas?
A. Revisiones informales entre pares
B. Talleres facilitados
C. Narrativas del flujo del proceso
D. Diagramas de flujo de datos

1-8
¿Cuál de las siguientes acciones realizaría un auditor de SI PRIMERO al planear una auditoría de SI?
A. Definir los resultados de la auditoría.
B. Finalizar el alcance y los objetivos de la auditoría.
C. Comprender los objetivos y la finalidad de la empresa.
D. Desarrollar el enfoque o la estrategia de auditoría.

1-9
El enfoque que un auditor de SI debe utilizar para planificar la cobertura de la auditoría de SI debe basarse en:
A. el riesgo.
B. la materialidad.
C. el control del fraude.
D. la suficiencia de las pruebas de auditoría.

1-10
Una organización realiza una copia de seguridad diaria de los datos y archivos de software críticos y almacena las
cintas de respaldo en una ubicación externa. Las cintas de respaldo se utilizan para restaurar los archivos en caso de una interrupción. Este es un ejemplo de un:
A. control preventivo.
B. control de gestión.
C. control correctivo.
D. control detectivesco.

CASO DE ESTUDIO CAP 1

1.

¿Qué debe hacer el auditor del SI PRIMERO?

A. Realizar una auditoría de estudio de los controles de acceso lógico.

B. Revisar el plan de auditoría para centrarse en la auditoría basada en el riesgo.

C. Realizar una evaluación de riesgos de TI.

D. Comenzar a probar los controles que el auditor de SI considera más críticos.

2.

Al auditar la seguridad lógica, el auditor de SI está MÁS preocupado cuando observa:

A. La cuenta del administrador del sistema es conocida por todos.

B. Las contraseñas no están obligadas a cambiar con frecuencia.

C. El administrador de la red tiene permisos excesivos.

D. El departamento de IT no tiene una política escrita sobre la gestión de privilegios privilegios.

3.

Al probar la gestión de cambios del programa en este caso, ¿cómo debe seleccionarse la muestra?

A. Los documentos de gestión de cambios deben seleccionarse al azar y examinados para ver si son apropiados.

B. Los cambios en el código de producción deben ser muestreados y rastreados hasta la documentación de autorización apropiada.

C. Los documentos de gestión de cambios deben seleccionarse en función de la criticidad del sistema y examinarlos para ver si son apropiados.

D. Los cambios en el código de producción deben ser muestreados y rastreados hasta los registros producidos por el sistema indicando la fecha y hora del cambio.

4.

Enumere tres controles generales de TI que el auditor de SI utilizaría para las pruebas sustantivas en este caso.

Una vez finalizado el trabajo preliminar, Betatronics decide planificar las auditorías para los dos años siguientes.

años. Tras aceptar el nombramiento, el auditor de SI observa que:

- La entidad tiene una carta de auditoría que detalla el alcance y las responsabilidades de la función de auditoría de SI y especifica que el comité de auditoría es el órgano que supervisa la actividad de auditoría.
- La entidad está sujeta a requisitos de cumplimiento normativo que exigen que su dirección certifique la eficacia del sistema de control interno en relación con la información financiera.
- La entidad ha registrado un crecimiento constante en los dos últimos años, al doble de la media del sector.
- La entidad también ha visto aumentar la rotación de empleados.

Algunas respuestas posibles son:

- El auditor de SI puede comprobar qué cuenta se utilizó para ejecutar una determinada tarea de administrador del sistema administrador del sistema.
- El auditor de SI puede comprobar si hubo un registro de cambios para cualquier cambios del sistema seleccionados (por ejemplo, reinicio del servidor y aplicación de parches).
- El auditor IS puede revisar las transacciones para ver si separaron las tareas incompatibles.

5.
La PRIMERA prioridad del auditor de SI en el primer año debe ser estudiar los:
A. los informes de auditoría de SI anteriores y planificar el calendario de la auditoría.
B. los estatutos de la auditoría y planificar el calendario de la misma.
C. el impacto del aumento de la rotación de personal.
D. El impacto de la implementación de un nuevo ERP en el entorno de TI.

6.
¿Cómo debe evaluar el auditor de SI las copias de seguridad (backup) y el procesamiento por lotes dentro de las operaciones informáticas?
A. Basarse en el informe del auditor de servicios del proveedor de servicios.
B. Estudiar el contrato entre la entidad y el proveedor de servicios.
C. Comparar el informe de prestación del servicio con el acuerdo de nivel de servicio.
D. Planificar y realizar una revisión independiente de las operaciones informáticas.

7.
Durante el trabajo diario, el auditor de SI advierte que existe el riesgo de que la revisión de los registros no dé lugar a detección oportuna de errores. Este es un ejemplo de cuál de los siguientes:
A. riesgo inherente
B. riesgo residual
C. riesgo de control
D. riesgo material

8.
El auditor de SI aconsejó al CIO y a su equipo que mejoraran el entorno general de control de TI. Se propuso la adaptación de COBIT. ¿Qué recomendaciones haría el auditor de SI al considerar este marco?

Posible respuesta:
El marco COBIT puede aprovecharse y adaptarse.
Cada proceso puede clasificarse como totalmente abordado, parcialmente abordado y no aplicable mediante comparando el marco COBIT estándar con la realidad de la organización. Otros marcos, normas y prácticas pueden incluirse en cada proceso respectivo, como sugiere la guía COBIT.

2-1
Para que la dirección pueda supervisar eficazmente el cumplimiento de los procesos y las aplicaciones, ¿cuál de las siguientes opciones sería la MÁS idónea?
A. Un repositorio central de documentos
B. Un sistema de gestión del conocimiento
C. Un panel de control
D. Un benchmarking

2-2
¿Cuál de los siguientes elementos se incluiría en un plan estratégico de SI?
A. Especificaciones para las compras de hardware planificadas
B. Análisis de los futuros objetivos empresariales
C. Fechas previstas para los proyectos de desarrollo
D. Objetivos presupuestarios anuales para el departamento de TI

2-3
¿Cuál de las siguientes opciones describe mejor el proceso de planificación estratégica de un departamento de TI?
A. El departamento de TI tendrá planes a corto o largo plazo dependiendo de los planes y objetivos más amplios de la organización.
B. El plan estratégico del departamento de TI debe estar orientado al tiempo y a los proyectos, pero no tan detallado como para abordar y ayudar a determinar las prioridades para satisfacer las necesidades del negocio.
C. La planificación a largo plazo del departamento de TI debe reconocer los objetivos de la organización, los avances tecnológicos y los requisitos normativos.
D. La planificación a corto plazo del departamento de TI no necesita integrarse en los planes a corto plazo de la organización, ya que los avances tecnológicos impulsarán los planes del departamento de TI mucho más rápido que los planes de la organización.

2-4
La responsabilidad MÁS importante de un responsable de seguridad de datos en una organización es:
A. recomendar y supervisar las políticas de seguridad de datos.
B. promover la concienciación sobre la seguridad dentro de la organización.
C. establecer procedimientos para las políticas de seguridad informática.
D. administrar los controles de acceso físico y lógico.

2-5
¿Qué se considera el elemento MÁS crítico para la implementación exitosa de un programa de seguridad de la información?
A. Un marco eficaz de gestión de riesgos empresariales
B. El compromiso de la alta dirección
C. Un proceso presupuestario adecuado
D. Una planificación meticulosa del programa

2-6
Un auditor de SI debe asegurarse de que las medidas de rendimiento del gobierno / governanza de TI:
A. evalúen las actividades de los comités de supervisión de TI.
B. proporcionen impulsores estratégicos de TI.
C. se adhieran a las normas y definiciones de los informes reglamentarios.
D. evaluar el departamento de TI.

2-7
¿Cuál de las siguientes tareas puede ser realizada por la misma persona en un centro informático de procesamiento de información bien controlado?
A. Administración de seguridad y gestión de cambios
B. Operaciones informáticas y desarrollo de sistemas
C. Desarrollo de sistemas y gestión de cambios
D. Desarrollo de sistemas y mantenimiento de sistemas

2-8
¿Cuál de los siguientes es el control MÁS crítico de la administración de bases de datos (DBA)?
A. Aprobación de las actividades de DBA
B. Segregación de funciones en cuanto a la concesión/revocación de derechos de acceso
C. Revisión de los registros y actividades de acceso
D. Revisión del uso de las herramientas de la base de datos

2-9
Cuando no se puede lograr una completa segregación de funciones en un entorno de sistema en línea, ¿cuál de las siguientes funciones debe separarse de las demás?
A. Originación
B. Autorización
C. Grabación
D. Corrección

2-10
En una pequeña organización en la que la segregación de funciones (SoD) no es práctica, un empleado desempeña la función de operador informático y programador de aplicaciones. ¿Cuál de los siguientes controles debería recomendar el auditor de SI?
A. Registro automatizado de los cambios en las bibliotecas de desarrollo
B. Personal adicional para proporcionar SoD
C. Procedimientos que verifiquen que sólo se aplican los cambios de programa aprobados
D. Controles de acceso para evitar que el operador realice
modificaciones del programa

CASO DE ESTUDIO CAP 2

1.

¿Cuál de los siguientes aspectos debería preocupar más al auditor de TI relacionados con la estrategia empresarial de TI de Accenco?

A. Los documentos de estrategia son informales e incompletos.

B. El comité de gestión de riesgos rara vez se reúne y no lleva actas.

C. Los presupuestos no parecen adecuados para respaldar futuras inversiones en TI.

D. No hay un CIO a tiempo completo.

2.

¿Cuál de los siguientes sería el asunto MÁS importante a tratar en relación con la estrategia empresarial de TI de Accenco? de TI de Accenco?

A. El comportamiento relacionado con el código de acceso y migración de los programadores de aplicaciones

B. La falta de políticas y procedimientos de TI

C. Las prácticas de gestión de riesgos en comparación con otras organizaciones similares D. La estructura de informes para TI

3.

Teniendo en cuenta las circunstancias descritas, ¿qué es lo que más preocupa preocupación desde la perspectiva del gobierno de TI?

A. La organización no tiene un CIO a tiempo completo.

B. La organización no tiene un comité de dirección de TI. C. El consejo de administración desempeña un papel importante en el seguimiento de las iniciativas de TI.

D. El director de sistemas de información depende del director financiero.

4.

Teniendo en cuenta las circunstancias descritas, ¿qué es lo que más preocupa preocupación desde la perspectiva de la DSI?

A. Los programadores de aplicaciones deben obtener la aprobación del DBA para el acceso de escritura directa a los datos. acceso directo a los datos.

B. Los programadores de aplicaciones deben entregar el código del programa desarrollado al bibliotecario para la migración a la producción.

C. El departamento de auditoría interna depende del director financiero.

D. Las revisiones del rendimiento de la empresa deben ser firmadas únicamente por los directores de la empresa.

5.

¿Cuál de las siguientes opciones sería la MEJOR para abordar la integridad de los datos desde el punto de vista del control de mitigación?

A. Los programadores de aplicaciones deben obtener la aprobación del DBA para el acceso directo a los datos.

B. Se requiere que los programadores de aplicaciones entreguen los códigos de programa desarrollados al bibliotecario de programas para que los transfiera a producción.

C. El departamento de auditoría interna depende del director financiero.
D. Los resultados del rendimiento empresarial deben ser revisados y firmados por los directores de negocio.

6, 7 y 8 son para desarrollar

3-1
Para ayudar a probar un sistema bancario esencial que se está adquiriendo, una organización ha proporcionado al proveedor datos sensibles de su sistema de producción existente. La preocupación PRIMARIA de un auditor de SI es que los datos deben ser:
A. sanitizados
B. completos.
C. representativos.
D. actualizados.

3-2
¿Cuál de los siguientes es el propósito PRIMARIO para llevar a cabo pruebas en paralelo?
A. Determinar si el sistema es rentable
B. Permitir la realización de pruebas integrales de unidades y sistemas
C. Para resaltar los errores en las interfaces del programa con los archivos
D. Para asegurar que el nuevo sistema cumple con los requisitos del usuario

3-3
Al realizar una revisión de la reingeniería de procesos de negocio, un auditor de SI encontró que se había eliminado un importante control preventivo. En este caso, el auditor de SI debería:
A. informar a la dirección del hallazgo y determinar si la dirección está dispuesta a aceptar el riesgo material potencial de no tener ese control preventivo.
B. determinar si un control de detección ha sustituido al control preventivo durante el proceso, y si no lo ha hecho, informar de la supresión del control preventivo.
C. recomendar que éste y todos los procedimientos de control que existían antes de la reingeniería del proceso se incluyan en el nuevo proceso.
D. Desarrollar un enfoque de auditoría continua para supervisar los efectos de la eliminación del control preventivo.

3-4
¿Cuál de las siguientes ediciones de validación de datos es eficaz para detectar errores de transposición y transcripción?
A. Comprobación de rangos
B. Comprobación de dígitos
C. Comprobación de validez
D. Comprobación de duplicados

3-5
¿Cuál de los siguientes puntos débiles se consideraría el MÁS grave en el software de planificación de recursos empresariales utilizado por una organización financiera?
A. No se han revisado los controles de acceso.
B. La documentación disponible es limitada.
C. No se han sustituido las cintas de seguridad de hace dos años.
D. Las copias de seguridad de la base de datos se realizan una vez al día.

3-6
Al auditar la fase de requisitos de una adquisición de software, un auditor de SI debería:
A. evaluar la razonabilidad del calendario del proyecto.
B. evaluar los procesos de calidad propuestos por el proveedor.
C. asegurarse de que se adquiere el mejor paquete de software.
D. revisar la integridad de las especificaciones.

3-7
Una organización decide comprar un paquete de software en lugar de desarrollarlo. En este caso, las fases de diseño y desarrollo de un ciclo de vida de desarrollo de sistemas tradicional se sustituirían por:
A. fases de selección y configuración
B. fases de viabilidad y requisitos
C. fases de implementación y prueba
D. nada, ya que la sustitución no es necesaria.

3-8
Las especificaciones del usuario para un proyecto de desarrollo de software que utiliza la metodología tradicional (cascada) del ciclo de vida de desarrollo del sistema no se han cumplido. Un auditor de SI que busque una causa debería buscar en cuál de las siguientes áreas?
A. Aseguramiento de la calidad
B. Requisitos
C. Desarrollo
D. Formación de los usuarios

3-9
Al introducir la arquitectura de cliente ligero, ¿cuál de los siguientes tipos de riesgo en relación con los servidores aumenta significativamente?
A. Integridad
B. Concurrencia
C. Confidencialidad
D. Disponibilidad

3-10
¿Cuál de los siguientes procedimientos debe implementarse para ayudar a garantizar la integridad de las transacciones entrantes a través del intercambio electrónico de datos (EDI)? Intercambio de datos electrónicos (EDI)?

A. Recuentos de segmentos incorporados en el tráiler del conjunto de transacciones
B. Un registro del número de mensajes recibidos, verificado periódicamente con el originador de la transacción
C. Una pista de auditoría electrónica para la rendición de cuentas y el seguimiento
D. Cotejar las transacciones de acuse de recibo recibidas con el registro de mensajes EDI enviados

CASO DE ESTUDIO CAP 3
1.
¿Cuál de las siguientes opciones presentaría el MAYOR riesgo para el minorista?
A. Los parches de la base de datos están muy desactualizados.
B. Las cajas registradoras inalámbricas de los puntos de venta utilizan el cifrado WEP.
C. La información del titular de la tarjeta de crédito se envía por Internet.
D. Los datos de ventas agregados se envían a un tercero.

2.
Basándose en el estudio del caso, ¿cuál de los siguientes controles sería el más importante a implementar?
A. Los registros de los puntos de venta deben utilizar una autenticación de dos factores, con contraseñas complejas reforzadas.
B. Los puntos de acceso inalámbricos deben utilizar el filtrado de direcciones MAC.
C. El sistema ERP actual debe ser parcheado para cumplir con el GDPR.
D. Los datos de ventas agregados deben ser anónimos y encriptados antes de su distribución.

3.
En el informe preliminar a la dirección, en relación con el estado de la actualización de la base de datos, ¿cuál de los siguientes puntos es el MÁS importante que debe incluir el auditor de SI?
A. La auditoría interna debe incluirse entre las aprobaciones del comité de dirección.
B. Existe la posibilidad de que la nueva base de datos no sea compatible con la solución ERP existente.
C. Se requiere una actualización y/o un parche del ERP para garantizar la compatibilidad de la base de datos actualizada.
D. La auditoría interna debe poder revisar la base de datos actualizada para garantizar el cumplimiento de la norma de seguridad de datos del sector de las tarjetas de pago (PCI-DSS).

4.
Con el fin de contribuir más directamente a ayudar a resolver los problemas en torno a la actualización de la base de datos, el auditor de SI debería:
A. Revisar la validez de las especificaciones funcionales del proyecto como base para una mejor definición de la base de datos del software.

B. Proponer su inclusión en el equipo del proyecto como consultor para el control de calidad de los resultados.
C. Investigar más a fondo los problemas para identificar las causas fundamentales y definir las contramedidas adecuadas.
D. Ponerse en contacto con el jefe de proyecto y discutir los planes del proyecto y recomendar la redefinición del calendario de entrega utilizando la metodología PERT.

4-1
¿Cuál de las siguientes opciones proporciona el MEJOR método para determinar el nivel de rendimiento que proporcionan entornos de instalaciones de procesamiento de información similares?
A. La satisfacción del usuario
B. Cumplimiento de objetivos
C. Evaluación comparativa
D. Planificación de la capacidad y el crecimiento

4-2
Para los sistemas de misión crítica con una baja tolerancia a la interrupción y un alto costo de recuperación, el auditor de SI, en principio, recomienda el uso de cuál de las siguientes opciones de recuperación?
A. Sitio móvil
B. Sitio caliente
C. Sitio frío
D. Sitio caliente hot site

4-3
¿Cuál de los siguientes es el método MÁS eficaz que puede utilizar un auditor de SI para probar el proceso de gestión de cambios del programa?
A. Rastrear desde la información generada por el sistema hasta la documentación de gestión de cambios
B. Examinar la documentación de gestión de cambios para obtener pruebas de exactitud
C. Rastrear desde la documentación de gestión de cambios hasta una pista de auditoría generada por el sistema
de auditoría generada por el sistema
D. Examinar la documentación de gestión de cambios para comprobar que está integridad

4-4
¿Cuál de las siguientes opciones permitiría a una empresa extender su intranet a través de Internet a sus socios comerciales?
A. Red privada virtual VPN
B. Cliente-servidor
C. Acceso telefónico
D. Proveedor de servicios de red

4-5
La clasificación basada en la criticidad de una aplicación de software como parte de un plan de continuidad del negocio de SI se determina por la:
A. la naturaleza del negocio y el valor de la aplicación para el negocio.
B. el coste de sustitución de la aplicación.
C. el soporte del proveedor disponible para la aplicación.
D. las amenazas y vulnerabilidades asociadas a la aplicación.

4-6
Cuando se lleva a cabo una auditoría de la seguridad de las bases de datos cliente-servidor, el auditor de SI debería estar MÁS preocupado por la disponibilidad de:
A. las utilidades del sistema.
B. los generadores de programas de aplicación.
C. la documentación de seguridad de los sistemas.
D. el acceso a los procedimientos almacenados.

4-7
Al revisar una red utilizada para las comunicaciones por Internet, un auditor de SI examinará PRIMERO la:
A. la validez de las ocurrencias de cambio de contraseña.
B. la arquitectura de la aplicación cliente-servidor.
C. la arquitectura y el diseño de la red.
D. la protección del firewall y los servidores proxy.

4-8
Un auditor de SI debe participar en:
A. observar las pruebas del plan de recuperación de desastres
B. Desarrollar el plan de recuperación de desastres.
C. mantener el plan de recuperación de desastres.
D. revisar los requisitos de recuperación de desastres de los contratos de los proveedores.

4-9
La réplica de datos debe ser implementada como una estrategia de recuperación cuando:
A. El objetivo de punto de recuperación (RPO) es bajo.
B. El objetivo de punto de recuperación (RPO) es alto.
C. el objetivo de tiempo de recuperación (RTO) es alto.
D. la tolerancia al desastre es alta.

4-10
¿Cuál de los siguientes componentes de un plan de continuidad del negocio es PRIMARIAMENTE la responsabilidad del departamento de IS de una organización?
A. Desarrollar el plan de continuidad del negocio
B. Seleccionar y aprobar las estrategias de recuperación utilizadas en el plan de continuidad del negocio

C. Declarar una catástrofe
D. Restauración de los sistemas informáticos y de los datos después de una catástrofe

CASO DE ESTUDIO CAP 4
1.
Al revisar la información para este proyecto, ¿cuál sería la preocupación más importante en relación con el uso de los sistemas de radiocomunicación por microondas según el escenario anterior?
A. Susceptibilidad de interceptación de los datos transmitidos.
B. Falta de soluciones de encriptación de la transmisión de datos disponibles
C. Probabilidad de interrupción del servicio
D. Sobrecostes en la implantación

2.
¿Cuál de las siguientes opciones reduciría mejor la probabilidad de que los sistemas empresariales sean atacados con éxito desde la Internet pública a través de la red inalámbrica?
A. Escanear todos los dispositivos conectados en busca de malware
B. Segmentar la red interna y el acceso a la Internet pública a través de una subred con firewall.
C. Registro de todos los accesos y emisión de alertas por intentos fallidos de inicio de sesión
D. Limitar todos los accesos a la red a las horas normales de trabajo y a los protocolos estándar

3.
Al negociar nuevos contratos con el proveedor, ¿cuál de los siguientes puntos debería recomendar el auditor de SI a la dirección en relación con el hot site en esta situación?
A. Los ordenadores de sobremesa en el hot site deberían aumentarse a 750.
B. Que se añadan 35 servidores adicionales al contrato del hot site.
C. Todos los medios de copia de seguridad deben almacenarse en el sitio caliente para acortar el RTO.
D. Las necesidades de equipos de escritorio y servidores deberían revisarse trimestralmente. (esto)

4.
Al negociar nuevos contratos con el proveedor, ¿cuál de los siguientes puntos debería recomendar el auditor de SI a la dirección en relación con la recuperación de la sucursal?
A. Añadir cada una de las sucursales al contrato de sitio caliente existente.
B. Asegurarse de que las sucursales tienen suficiente capacidad para respaldarse mutuamente.

C. Reubicar todos los servidores de correo y archivos/impresión de las sucursales en el centro de datos.
D. Añadir capacidad adicional al contrato de hot site igual a la sucursal más grande.

5-1
Un auditor de SI que revisa la configuración de un sistema de detección de intrusos basado en firmas estaría MÁS preocupado si se descubre cuál de las siguientes cosas?
A. La actualización automática está desactivada.
B. El escaneo de vulnerabilidades de aplicaciones está deshabilitado.
C. El análisis de paquetes de datos encriptados está deshabilitado.
D. El IDS es colocado entre la zona desmilitarizada y el firewall.

5-2
¿Cuál de las siguientes opciones es la MEJOR para controlar el acceso a los datos de nómina que se procesan en un servidor local?
A. Registrar el acceso a la información personal
B. Usar contraseñas separadas para las transacciones sensibles
C. Utilizar software que restrinja las reglas de acceso al personal autorizado
D. Restringir el acceso al sistema a horas de trabajo

5-3
Un auditor de SI acaba de completar una revisión de una organización que tiene una computadora central y dos servidores de bases de datos donde residen todos los datos de producción. ¿Cuál de las siguientes debilidades se consideraría la más grave?
A. El responsable de seguridad también es el administrador de la base de datos.
B. No se administran controles de contraseñas en los dos servidores de bases de datos.
C. No hay un plan de continuidad del negocio para las aplicaciones no críticas del sistema mainframe.
D. La mayoría de las redes de área local no respaldan los discos fijos de los servidores de archivos regularmente.

5-4
Una organización se propone instalar un sistema de inicio de sesión único que dé acceso a todos los sistemas. La organización la organización debería ser consciente de que:
A. sería posible un acceso no autorizado máximo si se revela una contraseña.
B. los derechos de acceso de los usuarios estarían restringidos por los parámetros de seguridad adicionales.
C. la carga de trabajo del administrador de seguridad aumentaría.
D. los derechos de acceso de los usuarios serian incrementados.

5-5
Cuando se revisa una implementación de un sistema de Voz sobre Protocolo de Internet sobre una red de área amplia corporativa de área amplia corporativa, un auditor de SI debe esperar encontrar:

A. Un enlace de datos de red digital de servicios integrados.
B. ingeniería de tráfico.
C. una encriptación de privacidad equivalente a la de los datos por cable.
D. terminales telefonicos analogicos.

5-6
Una compañía de seguros está usando computación de nube pública para una de sus aplicaciones críticas para reducir costos. ¿Cuál de los siguientes puntos es el que más preocupa al auditor de SI?
A. La incapacidad de recuperar el servicio en un escenario de fallo técnico importante
B. El acceso a los datos del entorno compartido por parte de otras empresas
C. Que el proveedor de servicios no incluya el apoyo a la investigación de incidentes
D. La viabilidad a largo plazo del servicio si el proveedor quiebra

5-7
¿Cuál de las siguientes opciones es la que MEJOR determina si existen protocolos completos de encriptación y autenticación para proteger la información mientras se transmite?
A. Se ha implementado una firma digital con RSA.
B. Se está trabajando en modo túnel con los servicios anidados de cabecera de autenticación (AH) y carga útil de seguridad encapsulada (ESP).
C. Se están utilizando certificados digitales con RSA.
D. Se está trabajando en modo transporte con los servicios anidados de AH y ESP.

5-8
¿Cuál de las siguientes preocupaciones sobre la seguridad de un mensaje electrónico se resolvería con firmas digitales?
A. Lectura no autorizada
B. Robo
C. Copia no autorizada
D. Alteración

5-9
¿Cuál de las siguientes características es un ataque de denegación de servicio distribuido?
A. Iniciación central de computadoras intermediarias para dirigir el tráfico de mensajes espurios simultáneos en un sitio objetivo especificado
B. Iniciación local de ordenadores intermediarios para dirigir el tráfico de mensajes espurios simultáneos en un sitio de destino especificado
C. Iniciación central de un ordenador primario para dirigir el tráfico simultáneo de mensajes espurios en múltiples sitios de destino
D. Iniciación local de ordenadores intermedios para dirigir el tráfico de mensajes espurios escalonados en un sitio de destino especificado

5-10
¿Cuál de los siguientes es el control antivirus preventivo más eficaz?

A. Escanear los archivos adjuntos del correo electrónico en el servidor de correo
B. Restaurar los sistemas a partir de copias limpias
C. Desactivar los puertos de bus serie universales
D. Un análisis antivirus en línea con definiciones de virus actualizadas

CASO DE ESTUDIO CAP 5

1.

¿Cuál de los siguientes aspectos es el que más preocupa a un auditor de SI que revisa la implementación de una VPN? Los ordenadores de la red que se encuentran:
A. en la red interna de la empresa.
B. en el sitio de respaldo.
C. en los hogares de los empleados.
D. en las oficinas remotas de la empresa.

2.

Cual de los siguientes niveles provee un mayor grado de protección al aplicar el software de control de acceso de acceso para evitar el riesgo de acceso no autorizado?
A. Nivel de red y SO
B. Nivel de aplicación
C. Nivel de la base de datos
D. Nivel de archivo de registro / log file

3.

Cuando un empleado notifica a la empresa que ha olvidado su contraseña, ¿qué debe hacer PRIMERO el administrador de seguridad?
A. Permitir que el sistema genere aleatoriamente una nueva contraseña
B. Verificar la identificación del usuario mediante un sistema de desafío/respuesta
C. Proporcionar al empleado la contraseña por defecto y explicarle que debe cambiarla lo antes posible
D. Pedir al empleado que se dirija al terminal del administrador para generar una nueva contraseña con el fin de asegurar la confidencialidad

4.

¿Qué prueba es la más importante que debe realizar el auditor de SI como parte de la revisión de los controles de acceso telefónico dial-up?
A. Marcar el servidor desde líneas telefónicas autorizadas y no autorizadas
B. Determinar los requisitos de ancho de banda del mantenimiento remoto y la capacidad máxima de la línea
C. Comprobar si la disponibilidad de la línea está garantizada para permitir el acceso remoto en cualquier momento
D. Comprobar si no se utiliza la devolución de llamadas (call back) y el coste de las mismas se carga a terceros

5.

¿Cuál es el riesgo más importante que el auditor de SI debe evaluar en relación con la práctica de acceso remoto existente?

A. El módem no está encendido o apagado cuando se necesita
B. Un acuerdo de no divulgación no fue firmado por el tercero
C. El intercambio de datos a través de la línea no está encriptado
D. Los controles del cortafuegos se han saltado (bypass)

6.
¿Cuál de las siguientes recomendaciones es la más probable para reducir el nivel actual de riesgo de acceso remoto?
A. Mantener un registro de acceso con la fecha y hora en que el modem fue encendido/apagado
B. Encriptar el tráfico a través de la línea telefónica
C. Migrar el acceso telefónico a una solución VPN de Internet
D. Actualizar las políticas del firewall e implementar un IDS

7.
¿Qué control debe ser implementado para prevenir un ataque a la red interna que se inicie a través de una conexión VPN de Internet?
A. Las reglas del firewall son revisadas periódicamente
B. Todas las VPNs terminan en un solo concentrador
C. Se implementa un IPS capaz de analizar el tráfico cifrado
D. Se instala un software antivirus en todos los servidores de producción

Preguntas cuestionario online ISACA gratis:

Una carta de auditoría debería:

D. describir la autoridad general, el alcance y las responsabilidades de la función de auditoría.

EXPLICACIÓN: Una carta de auditoría establecerá la autoridad y los requisitos de información para la auditoría, pero no los detalles del mantenimiento de los controles internos.

Un auditor de SI encuentra un pequeño número de solicitudes de acceso de usuarios que no habían sido autorizadas por los gerentes a través de los pasos normales de flujo de trabajo predefinidos y las reglas de escalamiento. El auditor de SI debería:

A. realizar un análisis adicional.
EXPLICACIÓN: El auditor de SI debe determinar primero la causa raíz y el impacto de los hallazgos y no tiene suficiente información para recomendar la solución de los problemas de flujo de trabajo.

Un auditor de SI observa que una empresa ha subcontratado el desarrollo de software a un tercero que es una empresa nueva. Para garantizar la protección de la inversión de la empresa en software, ¿cuál de las siguientes medidas debería recomendar el auditor de SI?

C. Debería existir un acuerdo de custodia del código fuente.

EXPLICACIÓN: Aunque la diligencia debida es una buena práctica, no garantiza la disponibilidad del código fuente en caso de fallo del proveedor.

El apetito de riesgo de una empresa es lo MEJOR que se puede establecer:

D. el comité de dirección.

EXPLICACIÓN: El comité de auditoría no es responsable de establecer la tolerancia o el apetito de riesgo de la empresa.

A la hora de identificar un plazo de finalización del proyecto más temprano, que se obtendrá pagando una prima por la finalización anticipada, las actividades que deben seleccionarse son las siguientes:

B. que tienen un tiempo de holgura cero.

EXPLICACIÓN: El camino crítico es el tiempo más largo de las actividades, pero no se basa en el tiempo más largo de ninguna actividad individual.

A un auditor de SI se le asigna la auditoría de un proyecto de desarrollo de software, que está completado en más de un 80 por ciento, pero que ya ha superado el tiempo en un 10 por ciento y los costes en un 25 por ciento. ¿Cuál de las siguientes acciones debería tomar el auditor de SI?

D. Revisar el desarrollo del proyecto y el caso de negocio.

EXPLICACIÓN: Antes de hacer cualquier recomendación, un auditor de SI necesita entender el proyecto y los factores que han contribuido a que el proyecto sobrepase el presupuesto y el calendario.

Un programador modificó maliciosamente un programa de producción para cambiar los datos y luego restauró el código original. ¿Cuál de las siguientes opciones detectaría con mayor eficacia la actividad maliciosa?

B. Revisar los archivos de registro del sistema

EXPLICACIÓN: Las comparaciones del código fuente son ineficaces porque los programas originales se restauraron y el programa modificado no existe.

¿Cuál de las siguientes opciones garantizaría MEJOR la continuidad de una red de área amplia (WAN) en toda la organización?

A. Enrutamiento alternativo incorporado

EXPLICACIÓN: El enrutamiento alternativo garantizaría la continuidad de la red si falla un dispositivo de comunicación o si se corta un enlace, ya que el redireccionamiento de mensajes podría ser automático.

Un auditor de SI está revisando los controles de seguridad física de un centro de datos y observa varias áreas de preocupación. ¿Cuál de las siguientes áreas es la más importante?

D. La puerta de salida de emergencia está bloqueada.

EXPLICACIÓN: El problema del botón de apagado de emergencia es una preocupación importante, pero la seguridad de la vida es la mayor prioridad.

¿Cuál de las siguientes opciones es la que mejor ayuda a los propietarios de la información a clasificar adecuadamente los datos?

B. Formación sobre las políticas y normas de la organización

EXPLICACIÓN: En lo que respecta a la protección de los datos, los requisitos de los usuarios finales son fundamentales, pero si el propietario de los datos no entiende qué esquema de clasificación de datos existe, es probable que conceda un acceso inadecuado a los datos sensibles.

Preguntas en inglés

1-1
Which of the following outlines the overall authority to perform an IS audit?
A. The audit scope with goals and objectives
B. A request from management to perform an audit
C. The approved audit charter **(this)**
D. The approved audit schedule

1-2
In performing a risk-based audit, which risk assessment is completed FIRST by an IS auditor?
A. Detection risk assessment
B. Control risk assessment
C. Inherent risk assessment **(this)**
D. Fraud risk assessment

1-3
Which of the following would an IS auditor MOST likely focus on when developing a risk-based audit program?
A. Business processes **(this)**
B. Administrative controls
C. Environmental controls
D. Business strategies

1-4
Which of the following types of audit risk assumes an absence of compensating controls in the area
being reviewed?
A. Control risk
B. Detection risk
C. Inherent risk **(this)**
D. Sampling risk

1-5
An IS auditor performing a review of an application's controls finds a weakness in system software that could materially impact the application. In this situation, an IS auditor should:
A. Disregard these control weaknesses because a system software
review is beyond the scope of this review.
B. Conduct a detailed system software review and report the control weaknesses.
C. Include in the report a statement that the audit was limited to a review of the application's controls.

D. Review the system software controls as relevant and recommend a detailed system software review. **(this)**

1-6
Which of the following is the MOST important reason why an audit planning process should be reviewed at periodic intervals?
A. To plan for deployment of available audit resources
B. To consider changes to the risk environment **(this)**
C. To provide inputs for documentation of the audit charter
D. To identify the applicable IS audit standards

1-7
Which of the following is MOST effective for implementing a control self-assessment within small business units?
A. Informal peer reviews
B. Facilitated workshops **(this)**
C. Process flow narratives
D. Data flow diagrams

1-8
Which of the following would an IS auditor perform FIRST when planning an IS audit?
A. Define audit deliverables.
B. Finalize the audit scope and audit objectives.
C. Gain an understanding of the business's objectives and purpose. **(this)**
D. Develop the audit approach or audit strategy.

1-9
The approach an IS auditor should use to plan IS audit coverage should be based on:
A. risk. (**this**)
B. materiality.
C. fraud monitoring.
D. sufficiency of audit evidence.

1-10
An organization performs a daily backup of critical data and software files and stores the backup tapes at an offsite location. The backup tapes are used to restore the files in case of a disruption. This is an example of a:
A. preventive control.
B. management control.
C. corrective control. **(this)**
D. detective control.

CASO DE ESTUDIO CAP 1
1.
What should the IS auditor do FIRST?
A. Perform a survey audit of logical access controls.

B. Revise the audit plan to focus on risk-based auditing.
C. Perform an IT risk assessment.
D. Begin testing controls that the IS auditor feels are most critical.

2.
When auditing the logical security, the IS auditor is MOST concerned when observing:
A. The system administrator account is known by everybody.
B. The passwords are not enforced to change frequently.
C. The network administrator is given excessive permissions.
D. The IT department does not have written policy on privilege management.

3.
When testing program change management in this case, how should the sample be selected?
A. Change management documents should be selected at random and examined for appropriateness.
B. Changes to production code should be sampled and traced to appropriate authorizing documentation.
C. Change management documents should be selected based on system criticality and examined for appropriateness.
D. Changes to production code should be sampled and traced back to system-produced logs indicating the date and time of the change.

4.
List three general IT controls the IS auditor would use for substantive testing in this case.
After the preliminary work has been completed, Betatronics decides to plan audits for the next two
years. After accepting the appointment, the IS auditor notes that:
• The entity has an audit charter that details the scope and responsibilities of the IS audit function and specifies the audit committee as the overseeing body for audit activity.
• The entity is subject to regulatory compliance requirements that require its management to certify the effectiveness of the internal control system as it relates to financial reporting.
• The entity has been recording consistent growth over the last two years at double the industry average.
• The entity has seen increased employee turnover as well.

Some possible answers include:
• The IS auditor can check which account was used for executing a particular system administrator task recently.
• The IS auditor can check if there was a change record for any selected system changes (i.e., server reboot and patching).
• The IS auditor can look into the transactions to see if they separated the incompatible duties.

5.

The FIRST priority of the IS auditor in year one should be to study the:
A. previous IS audit reports and plan the audit schedule.
B. audit charter and plan the audit schedule.
C. impact of the increased employee turnover.
D. impact of the implementation of a new ERP on the IT environment.

6.
How should the IS auditor evaluate backup and batch processing within computer operations?
A. Rely on the service auditor's report of the service provider.
B. Study the contract between the entity and the service provider.
C. Compare the service delivery report to the service level agreement.
D. Plan and carry out an independent review of computer operations.

7.
During the day-to-day work, the IS auditor advises there is a risk that log review may not result in timely detection of errors. This is an example of which of the following:
A. inherent risk
B. residual risk
C. control risk
D. material risk

8.
The IS auditor advised the CIO and team to improve the general IT control environment. COBIT was proposed to be adapted. What recommendations would the IS auditor make when considering this framework?

Possible answer:
The COBIT framework can be leveraged and adapted.
Each process can be classified as fully addressed, partially addressed and not applicable by comparing the standard COBIT framework to the organization's reality.
Further frameworks, standards and practices can be included in each respective process, as COBIT guidance suggests.

2-1
In order for management to effectively monitor the compliance of processes and applications, which of the following would be the MOST ideal?
A. A central document repository
B. A knowledge management system
C. A dashboard **(this)**
D. Benchmarking

2-2
Which of the following would be included in an IS strategic plan?
A. Specifications for planned hardware purchases
B. Analysis of future business objectives **(this)**

C. Target dates for development projects
D. Annual budgetary targets for the IT department

2-3
Which of the following BEST describes an IT department's strategic planning process?
A. The IT department will have either short- or long-range plans depending on the organization's broader plans and objectives.
B. The IT department's strategic plan must be time- and project oriented but not so detailed as to address and help determine priorities to meet business needs.
C. Long-range planning for the IT department should recognize organizational goals, technological advances and regulatory requirements. **(this)**
D. Short-range planning for the IT department does not need to be integrated into the short-range plans of the organization since technological advances will drive the IT department plans much quicker than organizational plans.

2-4
The MOST important responsibility of a data security officer in an organization is:
A. recommending and monitoring data security policies. **(this)**
B. promoting security awareness within the organization.
C. establishing procedures for IT security policies.
D. administering physical and logical access controls.

2-5
What is considered the MOST critical element for the successful implementation of an information security program?
A. An effective enterprise risk management framework
B. Senior management commitment **(this)**
C. An adequate budgeting process
D. Meticulous program planning

2-6
An IS auditor should ensure that IT governance performance measures:
A. evaluate the activities of IT oversight committees. **(this)**
B. provide strategic IT drivers.
C. adhere to regulatory reporting standards and definitions.
D. evaluate the IT department.

2-7
Which of the following tasks may be performed by the same person in a well-controlled information processing computer center?
A. Security administration and change management
B. Computer operations and system development
C. System development and change management
D. System development and system maintenance **(this)**

2-8

Which of the following is the MOST critical control over database administration (DBA)?
A. Approval of DBA activities
B. Segregation of duties in regard to access rights granting/revoking **(this)**
C. Review of access logs and activities
D. Review of the use of database tools

2-9
When a complete segregation of duties cannot be achieved in an online system environment, which of the following functions should be separated from the others?
A. Origination
B. Authorization **(this)**
C. Recording
D. Correction

2-10
In a small organization where segregation of duties (SoD) is not practical, an employee performs the function of computer operator and application programmer. Which of the following controls should the IS auditor recommend?
A. Automated logging of changes to development libraries
B. Additional staff to provide SoD
C. Procedures that verify that only approved program changes are implemented **(this)**
D. Access controls to prevent the operator from making program modifications

CASO DE ESTUDIO CAP 2

1.
Which of the following should be of GREATEST concern to the IS auditor related to Accenco's IT business strategy?
A. Strategy documents are informal and incomplete.
B. The risk management committee seldom meets and does not keep minutes.
C. Budgets do not appear adequate to support future IT investments.
D. There is no full-time CIO.

2.
Which of the following would be the MOST significant issue to address related to Accenco's IT business strategy?
A. The behavior related to the application programmers' access and migration code
B. The lack of IT policies and procedures
C. The risk management practices as compared to peer organizations D. The reporting structure for IT

3.
Given the circumstances described, what would be of GREATEST concern from an IT governance perspective?
A. The organization does not have a full-time CIO.

B. The organization does not have an IT steering committee. C. The board of directors plays a major role in monitoring IT initiatives.
D. The information systems manager reports to the CFO.

4.
Given the circumstances described, what would be of GREATEST concern from a SoD perspective?
A. Application programmers are required to obtain approval only from the DBA for direct-write access to data.
B. Application programmers are required to turn over the developed program code to the program librarian for migration to production.
C. The internal audit department reports to the CFO.
D. Business performance reviews are required to be signed off only by the business managers.

5.
Which of the following would BEST address data integrity from a mitigating control standpoint?
A. Application programmers are required to obtain approval from DBA for direct access to data.
B. Application programmers are required to hand over the developed program codes to the program librarian for transfer to production.
C. The internal audit department reports to the CFO.
D. Business performance results are required to be reviewed and signed off by the business managers.

6.
As this is a small organization, assume the CFO performs the CIO role. What should an IS auditor suggest regarding the governance structure?

7.
The IS budgeting process should be integrated with business processes and aligned with organizational budget cycles. What advice would an IS auditor give to the organization to ensure the budget covers all aspects and can be accepted by the board?

8.
The internal auditor is reporting to CFO, who is the owner of IT initiatives and operations. The reporting relationship inhibits the auditor’s independence. What compensating controls could be enabled have to improve the audit efforts?

3-1
To assist in testing an essential banking system being acquired, an organization has provided the vendor with sensitive data from its existing production system. An IS auditor’s PRIMARY concern is that the data should be:
A. sanitized. **(this)**

B. complete.
C. representative.
D. current.

3-2
Which of the following is the PRIMARY purpose for conducting parallel testing?
A. To determine whether the system is cost-effective
B. To enable comprehensive unit and system testing
C. To highlight errors in the program interfaces with files
D. To ensure the new system meets user requirements **(this)**

3-3
When conducting a review of business process reengineering, an IS auditor found that an important preventive control had been removed. In this case, the IS auditor should:
A. inform management of the finding and determine whether management is willing to accept the potential material risk of not having that preventive control. **(this)**
B. determine if a detective control has replaced the preventive control during the process, and if it has not, report the removal of the preventive control.
C. recommend that this and all control procedures that existed before the process was reengineered be included in the new process.
D. develop a continuous audit approach to monitor the effects of the removal of the preventive control.

3-4
Which of the following data validation edits is effective in detecting transposition and transcription errors?
A. Range check
B. Check digit **(this)**
C. Validity check
D. Duplicate check

3-5
Which of the following weaknesses would be considered the MOST serious in enterprise resource planning software used by a financial organization?
A. Access controls have not been reviewed. **(this)**
B. Limited documentation is available.
C. Two-year-old backup tapes have not been replaced.
D. Database backups are performed once a day.

3-6
When auditing the requirements phase of a software acquisition, an IS auditor should:
A. assess the reasonability of the project timetable.
B. assess the vendor’s proposed quality processes.
C. ensure that the best software package is acquired.

D. review the completeness of the specifications. **(this)**

3-7
An organization decides to purchase a software package instead of developing it. In such a case, the design and development phases of a traditional system development life cycle would be replaced with:
A. selection and configuration phases **(this)**
B. feasibility and requirements phases
C. implementation and testing phases
D. nothing, as replacement is not required.

3-8
User specifications for a software development project using the traditional (waterfall) system development life cycle methodology have not been met. An IS auditor looking for a cause should look in which of the following areas?
A. Quality assurance
B. Requirements
C. Development **(this)**
D. User training

3-9
When introducing thin client architecture, which of the following types of risk regarding servers is significantly increased?
A. Integrity
B. Concurrency
C. Confidentiality
D. Availability **(this)**

3-10 Which of the following procedures should be implemented to help ensure the completeness of inbound transactions via electronic data
interchange (EDI)?
A. Segment counts built into the transaction set trailer **(this)**
B. A log of the number of messages received, periodically verified with the transaction originator
C. An electronic audit trail for accountability and tracking
D. Matching acknowledgment transactions received to the log of EDI messages sent

CASO DE ESTUDIO CAP 3
CASO DE ESTUDIO CAP 3
1.
Which of the following would present the MOST significant risk to the retailer?
A. Database patches are severely out of date.
B. Wireless POS registers use WEP encryption.
C. Credit cardholder information is sent over the Internet.
D. Aggregate sales data are mailed to a third party.

2.
Based on the case study, which of the following controls would be the MOST important to implement?
A. POS registers should use two-factor authentication, with enforced complex passwords.
B. Wireless access points should use MAC address filtering. !
C. The current ERP system should be patched for compliance with GDPR.
D. Aggregate sales data should be anonymized and encrypted prior to distribution.!

3.
In the preliminary report to management, regarding the state of the database upgrade, which of the following is MOST important for the IS auditor to include?
A. Internal audit should be included among the steering committee approvals. !
B. There is a possibility that the new database may not be compatible with the existing ERP solution.
C. An ERP upgrade and/or patch is required in order to ensure updated database compatibility.
D. Internal audit should be able to review the upgraded database to ensure compliance with Payment Card Industry Data Security Standard (PCI-DSS).

4.
In order to contribute more directly to help address the problems around the database upgrade, the IS auditor should:
A. Review the validity of the functional project specifications as the basis for an improved software baselining definition.
B. Propose to be included in the project team as a consultant for QC of deliverables.
C. Research the problems further to identify root causes and define appropriate countermeasures.!
D. Contact the project leader and discuss the project plans and recommend redefining the delivery schedule using the PERT methodology

4-1
Which one of the following provides the BEST method for determining the level of performance provided by similar information processing facility environments?
A. User satisfaction
B. Goal accomplishment
C. Benchmarking (this)
D. Capacity and growth planning

4-2
For mission critical systems with a low tolerance to interruption and a high cost of recovery, the IS auditor, in principle, recommends the use of which of the following recovery options?
A. Mobile site

B. Warm site
C. Cold site
D. Hot site (this)

4-3
Which of the following is the MOST effective method for an IS auditor to use in testing the program change management process?
A. Trace from system-generated information to the change management documentation (this)
B. Examine change management documentation for evidence of accuracy
C. Trace from the change management documentation to a system-generated audit trail
D. Examine change management documentation for evidence of completeness

4-4
Which of the following would allow an enterprise to extend its intranet across the Internet to its business partners?
A. Virtual private network (this)
B. Client-server
C. Dial-up access
D. Network service provider

4-5
The classification based on criticality of a software application as part of an IS business continuity plan is determined by the:
A. nature of the business and the value of the application to the business. (this)
B. replacement cost of the application.
C. vendor support available for the application.
D. associated threats and vulnerabilities of the application.

4-6
When conducting an audit of client-server database security, the IS auditor should be MOST concerned about the availability of:
A. system utilities. (this)
B. application program generators.
C. systems security documentation.
D. access to stored procedures.

4-7

When reviewing a network used for Internet communications, an IS auditor will FIRST examine the:
A. validity of password change occurrences.
B. architecture of the client-server application.
C. network architecture and design. (this)
D. firewall protection and proxy servers.

4-8
An IS auditor should be involved in:
A. observing tests of the disaster recovery plan. (this)
B. developing the disaster recovery plan.
C. maintaining the disaster recovery plan.
D. reviewing the disaster recovery requirements of supplier contracts.

4-9
Data mirroring should be implemented as a recovery strategy when:
A. recovery point objective (RPO) is low. (this)
B. recovery point objective (RPO) is high.
C. recovery time objective (RTO) is high.
D. disaster tolerance is high.

4-10
Which of the following components of a business continuity plan is PRIMARILY the responsibility of an organization's IS department?
A. Developing the business continuity plan
B. Selecting and approving the recovery strategies used in the business continuity plan
C. Declaring a disaster
D. Restoring the IT systems and data after a disaster (this)

CASO DE ESTUDIO CAP. 4
1. In reviewing the information for this project, what would be the MOST important concern regarding the use of microwave radio systems based on the above scenario?
A. Susceptibility for interception of transmitted data. (this)
B. Lack of available data transmission encryption solutions
C. Likelihood of a service outage
D. Cost overruns in implementation

2. Which of the following would BEST reduce the likelihood of business systems being successfully attacked from the public internet through the wireless network?
A. Scanning all connected devices for malware
B. Segmenting internal network & public internet access through a firewalled subnet (this)
C. Logging all access and issuing alerts for failed logon attempts
D. Limiting all network access to regular business hours and standard protocols

3. When negotiating new contracts with the vendor, which of the following should the IS auditor recommend to management concerning the hot site in this situation?
A. Desktops at the hot site should be increased to 750.
B. An additional 35 servers should be added to the hot site contract.
C. All backup media should be stored at the hot site to shorten the RTO.
D. Desktop and server equipment requirements should be reviewed quarterly. (this).

4. When negotiating new contracts with the vendor, which of the following should the IS auditor recommend to management concerning branch office recovery?
A. Add each of the branches to the existing hot site contract.
B. Ensure branches have sufficient capacity to back each other up. (this)
C. Relocate all branch mail and file/print servers to the data center.
D. Add additional capacity to the hot site contract equal to the largest branch.

5-1
An IS auditor reviewing the configuration of a signature-based intrusion detection system would be MOST concerned if which of the following is discovered?
A. Auto-update is turned off.
B. Scanning for application vulnerabilities is disabled.
C. Analysis of encrypted data packets is disabled.
D. The IDS is placed between the demilitarized zone and the firewall.

5-2
Which of the following BEST provides access control to payroll data being processed on a local server?
A. Logging access to personal information
B. Using separate passwords for sensitive transactions
C. Using software that restricts access rules to authorized staff D. Restricting system access to business hours

5-3
An IS auditor has just completed a review of an organization that has a mainframe computer and two database servers where all production data reside. Which of the following weaknesses would be considered the MOST serious?
A. The security officer also serves as the database administrator.
B. Password controls are not administered over the two database servers.
C. There is no business continuity plan for the mainframe system’s noncritical applications.
D. Most local area networks do not back up file-server-fixed disks regularly.

5-4
An organization is proposing to install a single sign-on facility giving access to all systems. The organization should be aware that:
A. maximum unauthorized access would be possible if a password is disclosed.
B. user access rights would be restricted by the additional security parameters.

C. the security administrator's workload would increase.
D. user access rights would be increased.

5-5
When reviewing an implementation of a Voice-over Internet Protocol system over a corporate wide area network, an IS auditor should expect to find:
A. an integrated services digital network data link.
B. traffic engineering.
C. wired equivalent privacy encryption of data.
D. analog phone terminals.

5-6
An insurance company is using public cloud computing for one of its critical applications to reduce costs. Which of the following would be of MOST concern to the IS auditor?
A. The inability to recover the service in a major technical failure scenario
B. The data in the shared environment being accessed by other companies
C. The service provider not including investigative support for incidents
D. The long-term viability of the service if the provider goes out of business

5-7
Which of the following BEST determines whether complete encryption and authentication protocols for protecting information while being transmitted exist?
A. A digital signature with RSA has been implemented.
B. Work is being done in tunnel mode with the nested services of authentication header (AH) and encapsulating security payload (ESP).
C. Digital certificates with RSA are being used.
D. Work is being done in transport mode with the nested services of AH and ESP.

5-8
Which of the following concerns about the security of an electronic message would be addressed by digital signatures?
A. Unauthorized reading
B. Theft
C. Unauthorized copying
D. Alteration

5-9
Which of the following characterizes a distributed denial-of-service attack?
A. Central initiation of intermediary computers to direct simultaneous spurious message traffic at a specified target site
B. Local initiation of intermediary computers to direct simultaneous spurious message traffic at a specified target site
C. Central initiation of a primary computer to direct simultaneous spurious message traffic at multiple target sites
D. Local initiation of intermediary computers to direct staggered spurious message traffic at a specified target site

5-10
Which of the following is the MOST effective preventive antivirus control?
A. Scanning email attachments on the mail server
B. Restoring systems from clean copies
C. Disabling universal serial bus ports
D. An online antivirus scan with up-to-date virus definitions

CASO DE ESTUDIO CAP 6

1.
Which of the following would be of MOST concern to an IS auditor reviewing a VPN implementation? Computers on the network that are located:
A. on the enterprise's internal network.
B. at the backup site.
C. in employees' homes.
D. at the enterprise's remote offices.

2.
Which of the following levels provides a higher degree of protection in applying access control software to avoid unauthorized access risk?
A. Network and OS level
B. Application level
C. Database level
D. Log file level

3.
When an employee notifies the company that he/she has forgotten his/her password, what should be done FIRST by the security administrator?
A. Allow the system to randomly generate a new password
B. Verify the user's identification through a challenge/response system
C. Provide the employee with the default password and explain that it should be changed as soon as possible
D. Ask the employee to move to the administrator terminal to generate a new password in order to assure confidentiality

4.
What test is MOST important for the IS auditor to perform as part of the review of dial-up access controls?
A. Dial the server from authorized and unauthorized telephone lines
B. Determine bandwidth requirements of remote maintenance and the maximum line capacity
C. Check if the availability of the line is guaranteed to allow remote access any time
D. Check if call back is not used and the cost of calls is charged to the third party

5.

What is the MOST significant risk that the IS auditor should evaluate regarding the existing remote access practice?
A. Modem is not powered on/off whenever is needed
B. A nondisclosure agreement was not signed by the third party
C. Data exchanged over the line is not encrypted
D. Firewall controls are bypassed

6.
Which of the following recommendations is MOST likely to reduce the current level of remote access risk?
A. Maintain an access log with the date and time when the modem was powered on/off
B. Encrypt the traffic over the telephone line
C. Migrate the dial-up access to an Internet VPN solution
D. Update firewall policies and implement an IDS

7.
What control should be implemented to prevent an attack on the internal network being initiated through an Internet VPN connection?
A. Firewall rules are periodically reviewed
B. All VPNs terminate at a single concentrator
C. An IPS capable to analyze encrypted traffic is implemented
D. Antivirus software is installed on all production servers

Preguntas cuestionario ISACA online gratis:

An audit charter should:

CORRECT ANSWER: D. outline the overall authority, scope and responsibilities of the audit function.
EXPLANATION: An audit charter will state the authority and reporting requirements for the audit but not the details of maintenance of internal controls.

An IS auditor finds a small number of user access requests that had not been authorized by managers through the normal predefined workflow steps and escalation rules. The IS auditor should:

CORRECT ANSWER: A. perform an additional analysis.

EXPLANATION: The IS auditor must first determine the root cause and impact of the findings and does not have enough information to recommend fixing the workflow issues.

An IS auditor observes that an enterprise has outsourced software development to a third party that is a startup company. To ensure that the enterprise's investment in software is protected, which of the following should be recommended by the IS auditor?

CORRECT ANSWER: C. There should be a source code escrow agreement in place.

EXPLANATION: While due diligence is a good practice, it does not ensure availability of the source code in the event of vendor failure.

An enterprise's risk appetite is BEST established by:

CORRECT ANSWER: D. the steering committee.

EXPLANATION: The audit committee is not responsible for setting the risk tolerance or appetite of the enterprise.

When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

CORRECT ANSWER: B. that have zero slack time.

EXPLANATION: The critical path is the longest time length of the activities, but is not based on the longest time of any individual activity.

An IS auditor is assigned to audit a software development project, which is more than 80 percent complete, but has already overrun time by 10 percent

and costs by 25 percent. Which of the following actions should the IS auditor take?

YOUR ANSWER: D. Review the conduct of the project and the business case.
EXPLANATION: Before making any recommendations, an IS auditor needs to understand the project and the factors that have contributed to bringing the project over budget and over schedule.

A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST **effectively detect the malicious activity?**

CORRECT ANSWER: B. Reviewing system log files
EXPLANATION: Source code comparisons are ineffective because the original programs were restored and the changed program does not exist.

Which of the following would BEST **ensure continuity of a wide area network (WAN) across the organization?**

YOUR ANSWER: A. Built-in alternative routing
EXPLANATION: Alternative routing would ensure that the network would continue if a communication device fails or if a link is severed because message rerouting could be automatic.

An IS auditor is reviewing the physical security controls of a data center and notices several areas for concern. Which of the following areas is the MOST **important?**

CORRECT ANSWER: D. The emergency exit door is blocked.
EXPLANATION: The emergency power off button issue is a significant concern, but life safety is the highest priority.

Which of the following choices BEST helps information owners to properly classify data?

CORRECT ANSWER: B. Training on organizational policies and standards
EXPLANATION: In terms of protecting the data, the data requirements of end users are critical, but if the data owner does not understand what data classification schema is in place, it would be likely that inappropriate access to sensitive data might be granted by the data owner.

OTRO LIBRO

1. What is the difference between a policy and a procedure?
C. A policy is a high-level document signed by a person of authority and compliance is mandatory. A procedure defines the mandatory steps to attain compliance.

2. Which of the following in a business organization will be held liable by the government for failures of internal controls?
A. President, vice presidents, and other true corporate officers

3. What does fiduciary responsibility mean?
B. To act for the benefit of another person and place the responsibilities to be fair and honest ahead of your own interest.

4. What are the different types of audits?
B. Integrated, operational, compliance, administrative

5. What is the difference between the word should and shall when used in regulations?
D. Should indicates actions that are discretionary according to need, whereas shall means the action is mandatory regardless of financial impact.

6. Highest authority for a project manager is in the _____ organizational structure.
A. Projectized, followed by the strong matrix

7. Which of the following is not defined as a nonaudit role?
C. Auditor

8. Why is it necessary to protect audit documentation and work papers?
D. Audit documentation work papers may reveal confidential information that should not be lost or disclosed.

9. Which of the following is a network diagram that shows the critical path for a project?

A. Program evaluation review technique

10. What is the purpose of standard terms of reference?
C. To ensure honest and unbiased communication

11. What does the statement “auditor independence” relate to?
B. It is required for an external audit.

12. Which of the following is true concerning the roles of data owner, data user, and data custodian?
C. The data owner specifies controls.

13. What is the definition of a work breakdown structure?
D. Decomposition of tasks

14. What is the definition of a standard as compared to a guideline?
B. Standards are mandatory controls designed to support a policy. Following guidelines is discretionary.

15. Who should issue the organizational policies?
D. The policy should be signed and enforced by the highest level of management.

16. The auditor’s final opinion is to be based on:
D. The results of evidence and testing

17. What is the purpose of ISACA’s professional ethics statement?
A. To clearly specify acceptable and unacceptable behavior

18. How does the auditor derive a final opinion?
A. From evidence gathered and the auditor’s observations

19. What are the three competing demands to be addressed by project management?
B. Time, cost, and scope

20. What is the difference between a threat and a vulnerability?
C. Vulnerabilities are a path that can be taken by a threat, resulting in a loss.