EJERCICIO A.2 - EXAMEN DE CONOCIMIENTOS TIPO TEST

Especialista en Sistemas de Información y Transformación Digital - ICO

Instrucciones

- El ejercicio consta de 50 preguntas ordinarias y 5 preguntas de reserva.
- Duración: 60 minutos.
- Cada pregunta tiene cuatro opciones de respuesta (A, B, C y D) y una única respuesta correcta.
- Sistema de corrección: acierto +1 punto directo; error -0,25 puntos directos; pregunta no contestada 0 puntos.
- Las preguntas de reserva se utilizarán, por su orden, solo si fuera necesario anular preguntas ordinarias.

Preguntas ordinarias

1. Una entidad financiera pública rediseña su modelo de atención a ciudadanos mediante un portal de servicios digitales. Al analizar los sistemas implicados, el equipo detecta que varios procesos de negocio críticos no tienen un sistema que los soporte directamente. ¿Cuál es la relación que debería existir entre los procesos de negocio y los sistemas de información?

A) Los sistemas de información son herramientas técnicas autónomas que funcionan con independencia de los procesos de negocio de la organización.

B) Los sistemas de información deben diseñarse para soportar y habilitar los procesos de negocio, creando valor para la organización.

C) Los sistemas de información deben replicar exactamente la estructura organizativa, independientemente de los procesos que soporten.

D) Cada proceso de negocio debe estar soportado por un sistema de información dedicado y exclusivo.

2. Un proveedor externo gestiona la plataforma de pagos digitales de una entidad pública. Han surgido incidencias recurrentes sin resolución en los plazos acordados. Desde la perspectiva de la relación proveedor-cliente en servicios TI, ¿cuál es el enfoque más adecuado?

A) Revisar los acuerdos de nivel de servicio vigentes y activar los mecanismos de supervisión y exigencia previstos en el contrato.

B) Sustituir inmediatamente al proveedor por otro que ofrezca las mismas condiciones contractuales.

C) Asumir internamente la gestión de la plataforma para evitar dependencias externas.

D) Escalar el problema a la dirección para que negocie directamente sin intervención técnica.

3. Un equipo debate si un módulo de reporting debería considerarse un 'sistema de información' independiente o simplemente una funcionalidad del ERP corporativo. ¿Cuál de los siguientes criterios es más relevante para resolver esta cuestión?

A) El número de usuarios que lo utilizan habitualmente.

B) Si cumple una función de soporte a la toma de decisiones con entradas, procesos y salidas de información diferenciadas.

C) Si ha sido desarrollado por un proveedor distinto al del ERP.

D) Si dispone de base de datos propia e independiente del ERP.

4. La dirección solicita al área de TI que justifique la inversión en la renovación del sistema de gestión documental. ¿Cuál de los siguientes argumentos refleja mejor el concepto de 'creación de valor' de los servicios tecnológicos?

A) El nuevo sistema incorpora las últimas tecnologías del mercado y mejorará la imagen de la entidad.

B) El sistema actual ha superado su vida útil técnica y debe reemplazarse conforme al plan de obsolescencia.

C) El proveedor actual ya no ofrece soporte para la versión instalada, lo que obliga a la renovación.

D) La renovación reducirá los tiempos de recuperación documental, disminuirá errores en auditoría y mejorará el cumplimiento normativo.

5. El área de TI detecta que varios proyectos de desarrollo se están ejecutando sin seguir los estándares arquitectónicos aprobados. ¿Cuál es la diferencia fundamental entre gobierno técnico y gestión operativa en este contexto?

A) El gobierno técnico establece los marcos de decisión, responsabilidades y control; la gestión operativa ejecuta dentro de esos marcos.

B) El gobierno técnico resuelve los problemas del día a día; la gestión operativa establece las reglas a largo plazo.

C) El gobierno técnico es responsabilidad exclusiva de la dirección general, sin participación técnica.

D) No existe diferencia real; son la misma actividad con distinto nivel de formalidad.

6. Una entidad pública tiene comités de arquitectura, seguridad y datos, pero los responsables de negocio perciben que las decisiones técnicas se toman sin considerar sus necesidades. ¿Qué elemento del modelo de gobierno está fallando?

A) La segregación de funciones entre los comités técnicos.

B) La frecuencia de las reuniones de los comités técnicos.

C) La ausencia de un CIO con suficiente autoridad jerárquica.

D) La alineación entre el gobierno de TI y los objetivos de negocio, y los mecanismos de participación de los interesados.

7. En el marco de un servicio TI externalizado, ¿cuál de las siguientes prácticas contribuye mejor a la trazabilidad y rendición de cuentas?

A) Exigir al proveedor un informe mensual de actividad en formato libre.

B) Establecer indicadores de desempeño medibles, umbrales de cumplimiento y procedimientos de escalado documentados.

C) Designar un responsable técnico interno para que asista a todas las reuniones del proveedor.

D) Auditar el código fuente desarrollado por el proveedor en cada entrega.

8. Una entidad financiera pública desarrolla un nuevo sistema de gestión de riesgos con plazo fijo impuesto por regulación, pero los requisitos funcionales aún no están completamente definidos. ¿Qué enfoque de desarrollo sería más adecuado?

A) Iterativo o híbrido, porque permite entregar valor de forma incremental mientras los requisitos se van precisando, dentro del plazo regulatorio.

B) Predictivo (en cascada), porque el plazo está fijo y es necesario planificarlo todo desde el inicio.

C) Exclusivamente ágil (Scrum), porque los requisitos no están definidos y la flexibilidad debe ser máxima.

D) Diferir el inicio del proyecto hasta que los requisitos estén completamente definidos.

9. La dirección encarga la implantación de una nueva plataforma de gestión documental y el equipo propone ejecutarla como proyecto. ¿Cuál es la característica que distingue fundamentalmente un proyecto de una operación continuada?

A) Un proyecto siempre tiene mayor presupuesto que una operación continuada.

B) Un proyecto es gestionado exclusivamente por personal técnico; las operaciones las gestiona el negocio.

C) La diferencia es formal: los proyectos requieren acta de constitución y las operaciones no.

D) Un proyecto es temporal y produce un resultado único; la operación gestiona servicios de forma continua y repetitiva.

10. Un proyecto de transformación digital se entrega en plazo y dentro del presupuesto, pero los usuarios no utilizan el sistema porque no se adapta a sus procesos de trabajo. Desde la perspectiva de la dirección de proyectos orientada a resultados, ¿qué ha fallado?

A) La gestión del alcance técnico, porque el sistema no cumple las especificaciones.

B) La creación de valor: el proyecto cumplió los parámetros técnicos pero no generó el resultado esperado para la organización.

C) La gestión de costes, porque un sistema que no se usa representa un gasto innecesario.

D) La gestión del tiempo, porque se debería haber dedicado más tiempo a las pruebas de aceptación.

11. ¿Cuál es la relación más adecuada entre un proyecto tecnológico y las operaciones de servicio que le suceden?

A) El proyecto concluye con la entrega técnica; la relación con operaciones es responsabilidad exclusiva del área de sistemas.

B) Las operaciones se planifican de forma independiente una vez que el proyecto ha finalizado completamente.

C) El proyecto debe contemplar desde su inicio la transición al servicio, incluyendo documentación, formación y acuerdos de soporte.

D) El director del proyecto debe asumir también la responsabilidad operativa durante el primer año de funcionamiento.

12. Un proyecto de implantación de ERP lleva tres meses en ejecución y el alcance ha crecido de forma no controlada por peticiones de usuarios. ¿Qué práctica de gestión de proyectos debería haberse aplicado para evitar esta situación?

A) Congelar los requisitos en la fase inicial y no admitir ningún cambio durante la ejecución.

B) Asignar un responsable de negocio que filtre todas las peticiones antes de que lleguen al equipo técnico.

C) Ampliar presupuesto y plazo para absorber las nuevas funcionalidades solicitadas.

D) Gestionar el alcance mediante un proceso formal de control de cambios que evalúe el impacto de cada solicitud antes de su aprobación.

13. Un proyecto de desarrollo lleva seis meses con retrasos acumulados. El director propone incorporar más desarrolladores para comprimir el calendario. ¿Cuál es el principal riesgo de esta decisión?

A) Que incorporar recursos en fases avanzadas puede aumentar la complejidad de coordinación y no recuperar el retraso, especialmente si las tareas pendientes son interdependientes.

B) Que los nuevos desarrolladores no estén familiarizados con las tecnologías del proyecto.

C) Que el coste total supere el presupuesto aprobado.

D) Que la dirección interprete la incorporación de recursos como señal de mala gestión.

14. En la planificación de un proyecto de transformación digital, varios grupos de interesados tienen expectativas contradictorias sobre el alcance del sistema. ¿Cuál es el enfoque más adecuado desde la gestión de interesados?

A) Dar prioridad a las expectativas de la dirección general, que es quien aprueba el presupuesto.

B) Delimitar el alcance técnicamente y comunicarlo a todos los grupos una vez aprobado por TI.

C) Documentar las expectativas de todos los grupos, analizar los conflictos y facilitar un proceso de alineación antes de fijar el alcance.

D) Excluir del proceso de planificación a los grupos con expectativas más complejas para agilizar la toma de decisiones.

15. ¿Cuál de las siguientes actividades forma parte de la medición del desempeño del proyecto, en contraposición a la gestión de las operaciones del servicio?

A) Asegurar la disponibilidad del sistema en producción conforme a los SLA acordados.

B) Gestionar las incidencias de los usuarios del sistema en explotación.

C) Ejecutar los procedimientos de backup y recuperación del sistema implantado.

D) Comparar el avance real del proyecto con la línea base de alcance, plazo y coste, e identificar desviaciones que requieran acción.

16. En la planificación de un proyecto de migración de sistemas críticos, el equipo identifica el riesgo de indisponibilidad del servicio durante el proceso. ¿Cuál es la respuesta al riesgo más adecuada?

A) Aceptar el riesgo, ya que toda migración implica cierta indisponibilidad inevitable.

B) Planificar una estrategia que minimice la ventana de indisponibilidad, establecer un plan de rollback y comunicar el impacto previsto a los interesados.

C) Transferir el riesgo al proveedor de migración mediante cláusulas contractuales de penalización.

D) Evitar el riesgo cancelando la migración y manteniendo el sistema actual indefinidamente.

17. El director de proyecto decide no registrar formalmente un riesgo identificado verbalmente en una reunión, argumentando que es poco probable. ¿Cuál es el principal error conceptual de este razonamiento?

A) Confundir la probabilidad de ocurrencia con la urgencia del riesgo: solo deben registrarse los riesgos urgentes.

B) No atender a lo que exigen los procedimientos del proyecto, que requieren registrar todos los riesgos sin excepción.

C) Tomar decisiones de gestión del riesgo usando solo la probabilidad e ignorando el impacto: un riesgo de baja probabilidad pero alto impacto puede ser crítico y debe gestionarse.

D) Delegar en el equipo la responsabilidad de identificar riesgos, cuando corresponde al director hacerlo.

18. Existe incertidumbre significativa en el coste de los componentes de integración con los sistemas legacy de la entidad. ¿Cuál es la herramienta de planificación más adecuada para gestionar esta incertidumbre?

A) Incluir una reserva de contingencia en el presupuesto, dimensionada en función del análisis de riesgos de integración.

B) Establecer un precio fijo con el proveedor de integración para eliminar la variabilidad de coste.

C) Reducir el alcance del proyecto para eliminar las integraciones con los sistemas legacy.

D) Esperar a tener mayor información antes de iniciar la planificación del proyecto.

19. En un contexto de alta incertidumbre tecnológica (nuevo proveedor, tecnología no probada en la entidad), ¿qué enfoque de toma de decisiones es más coherente con una buena gestión del riesgo?

A) Tomar todas las decisiones al inicio del proyecto para evitar cambios durante la ejecución.

B) Delegar todas las decisiones técnicas al proveedor para que asuma el riesgo tecnológico.

C) Exigir al proveedor garantías contractuales totales que cubran cualquier incidencia tecnológica.

D) Tomar las decisiones de forma progresiva: utilizar pruebas de concepto o prototipos para reducir activamente la incertidumbre tecnológica, y posponer las decisiones irreversibles hasta disponer de información suficiente.

20. Los usuarios del sistema de gestión de expedientes se quejan de lentitud en las consultas. El responsable técnico verifica que el sistema cumple el SLA firmado, que únicamente incluye un indicador de disponibilidad del 99,9%. ¿Cuál es la actuación más adecuada?

A) Comunicar a los usuarios que el sistema cumple el SLA y que no existen motivos técnicos para actuar.

B) Revisar y ampliar los indicadores del SLA para incorporar métricas de experiencia de uso —tiempos de respuesta, satisfacción percibida— y establecer objetivos de mejora sobre ellas.

C) Redimensionar inmediatamente la infraestructura para aumentar la capacidad de procesamiento del sistema.

D) Escalar al proveedor para que resuelva el problema de rendimiento dentro de los términos del contrato vigente.

21. En el Sistema de Valor del Servicio (SVS) de ITIL 4, ¿cuál es el propósito principal de la cadena de valor del servicio?

A) Definir los contratos y acuerdos de nivel de servicio con los proveedores externos.

B) Establecer la jerarquía organizativa del departamento de TI y sus responsabilidades.

C) Proporcionar un modelo operativo flexible que describe las actividades necesarias para crear, entregar y mejorar servicios de valor.

D) Documentar los procesos técnicos de desarrollo e implantación de sistemas.

22. Una entidad pública externaliza el soporte de su plataforma de gestión tributaria. Seis meses después, el equipo interno ha perdido el conocimiento técnico suficiente para supervisar al proveedor con criterio. ¿Qué riesgo de gestión de servicios ilustra este escenario?

A) Riesgo de dependencia tecnológica y pérdida de capacidad de gobierno, que impide evaluar la calidad del servicio y gestionar el contrato con criterio técnico.

B) Riesgo de continuidad del servicio, porque la entidad no podría restablecerlo en caso de fallo del proveedor.

C) Riesgo de seguridad, porque el proveedor accede a información sensible sin supervisión adecuada.

D) Riesgo reputacional, porque los ciudadanos podrían percibir la externalización como pérdida de control público.

23. Un nuevo sistema de gestión de expedientes está a punto de entrar en producción y el responsable de TI detecta que nadie ha definido aún los SLA operativos ni los procedimientos de soporte. ¿En qué momento del ciclo de vida del servicio debería haberse planificado su incorporación al catálogo de servicios?

A) Tras la puesta en producción, una vez que el servicio se haya estabilizado durante los primeros meses de operación.

B) Cuando el proveedor entregue la documentación técnica final del sistema desarrollado.

C) Cuando la dirección apruebe formalmente el presupuesto de operación del nuevo servicio.

D) Durante la fase de diseño y transición del servicio, antes de su puesta en producción, definiendo SLA, responsabilidades operativas y criterios de aceptación.

24. ¿Cuál es la diferencia principal entre una incidencia y una petición de servicio en la gestión de servicios TI?

A) Una incidencia es una interrupción no planificada o degradación del servicio; una petición es una solicitud formal de algo que forma parte del servicio normal.

B) Una incidencia afecta a muchos usuarios y una petición solo a uno.

C) Las incidencias las gestiona el proveedor y las peticiones el equipo interno.

D) Una petición requiere aprobación de la dirección, mientras que una incidencia se resuelve sin autorización.

25. El SLA con el proveedor de servicios cloud establece disponibilidad del 99,9% mensual y no contempla ventanas de mantenimiento excluidas del cómputo. En un mes de 30 días, el sistema estuvo indisponible 6 horas. ¿Cuál es la valoración correcta?

A) El SLA se ha cumplido, ya que 6 horas representa menos del 1% del tiempo total del mes.

B) No es posible determinarlo sin conocer si la indisponibilidad fue planificada o no planificada.

C) El SLA se ha cumplido parcialmente; corresponde negociar una penalización proporcional con el proveedor.

D) El SLA se ha incumplido: el 99,9% mensual permite un máximo de ~43 minutos de indisponibilidad; 6 horas supera ese umbral más de 8 veces.

26. En la supervisión de un proveedor que gestiona la plataforma de pagos, ¿cuál de las siguientes prácticas aporta mayor valor para el control continuo de la calidad del servicio?

A) Revisar mensualmente las facturas del proveedor para verificar que los servicios facturados coinciden con los prestados.

B) Mantener reuniones de seguimiento periódicas basadas en indicadores de desempeño acordados, revisando tendencias y no solo el cumplimiento puntual de umbrales.

C) Realizar visitas anuales a las instalaciones del proveedor para auditar sus procedimientos internos.

D) Exigir al proveedor la certificación ISO 27001 como garantía suficiente de calidad del servicio.

27. Una entidad financiera pública, sujeta tanto al ENS como a la regulación del Banco de España, recibe una auditoría que señala que sus medidas de seguridad no alcanzan el nivel exigido por el ENS. ¿Cuál es la interpretación correcta sobre el ámbito de aplicación del ENS?

A) El ENS solo aplica a las administraciones públicas estrictas; las entidades financieras públicas pueden optar por seguir únicamente la regulación bancaria.

B) Cuando existe regulación sectorial específica, esta prevalece sobre el ENS y exime de su cumplimiento.

C) El ENS aplica a las entidades del sector público, con independencia de que también les aplique regulación sectorial adicional. Ambos marcos son acumulativos.

D) El ENS aplica exclusivamente a los sistemas de información que tratan datos de carácter personal.

28. En el ENS (RD 311/2022), ¿qué principio básico establece que la selección de las medidas de seguridad debe basarse en el análisis de riesgos y ser equilibrada y proporcionada a la naturaleza de la información, los servicios prestados y los riesgos existentes?

A) Gestión de la seguridad basada en los riesgos: el análisis y la gestión de riesgos deben realizarse de forma continua y las medidas han de aplicarse de forma equilibrada y proporcionada a la naturaleza de la información, los servicios prestados y los riesgos existentes.

B) Seguridad integral: la seguridad debe abarcar todas las fases del ciclo de vida del sistema y todos los elementos del entorno, sin excepción.

C) Líneas de defensa: las medidas de seguridad se organizan en capas independientes de modo que el fallo de una no comprometa el conjunto.

D) Vigilancia continua y reevaluación periódica: las condiciones de seguridad deben revisarse de forma continua y periódica para mantener la adecuación de las medidas al entorno de amenazas.

29. El responsable de seguridad propone que el mismo técnico pueda crear usuarios, aprobar accesos y auditar los registros de actividad en el sistema de gestión de créditos. ¿Qué principio de seguridad se estaría vulnerando principalmente?

A) Principio de mínimo privilegio, porque el técnico dispondría de más permisos de los estrictamente necesarios para cualquiera de sus funciones individuales.

B) Principio de continuidad, porque si ese técnico no está disponible, las tres funciones quedan simultáneamente sin cobertura.

C) Principio de autenticación, porque el técnico debería utilizar credenciales distintas para acceder a cada una de las tres funciones.

D) Principio de segregación de funciones, porque acumular en la misma persona la capacidad de crear, aprobar y auditar elimina los controles cruzados diseñados para detectar irregularidades.

30. El responsable de seguridad propone implementar 'defensa en profundidad' para proteger el sistema de gestión de expedientes. ¿Qué implica este enfoque?

A) Concentrar todas las medidas de seguridad en el perímetro de red, asumiendo que si el perímetro es sólido el interior queda protegido.

B) Aplicar capas múltiples e independientes de controles de seguridad, de modo que si una falla las restantes mantienen la protección.

C) Profundizar en el análisis de riesgos antes de implantar cualquier medida de seguridad.

D) Implementar las medidas de seguridad tecnológicamente más avanzadas disponibles, independientemente de su coste.

31. El comité de seguridad de una entidad financiera pública ha identificado un riesgo sobre su sistema de gestión de préstamos y debe decidir si es aceptable o requiere tratamiento. ¿Qué criterio debe aplicarse para tomar esa decisión?

A) La aceptabilidad del riesgo debe estar definida en la política de seguridad de la organización, en función de sus umbrales de tolerancia al riesgo y el contexto regulatorio aplicable.

B) Un riesgo es aceptable cuando su probabilidad de ocurrencia es inferior al 10% anual, con independencia de su impacto potencial.

C) Un riesgo es aceptable cuando el coste de las medidas para mitigarlo supera el valor estimado del activo protegido.

D) Un riesgo es aceptable si el sistema afectado no ha sufrido ningún incidente de seguridad en los últimos tres años.

32. Tras un incidente de seguridad en el que un sistema fue comprometido, el equipo propone realizar un análisis post-incidente. ¿Cuál es el objetivo principal de este análisis?

A) Determinar la responsabilidad legal del personal implicado en el incidente.

B) Calcular el coste económico del incidente para reclamarlo al proveedor o aseguradora responsable.

C) Identificar las causas raíz del incidente, las lecciones aprendidas y las mejoras a implantar para evitar su repetición.

D) Elaborar el informe de notificación del incidente a la autoridad supervisora en los plazos legales exigidos.

33. Una entidad pública tiene su sistema de gestión de avales alojado en un único centro de datos. Se propone implantar un sistema de recuperación ante desastres en un centro alternativo. ¿Cuál de los siguientes parámetros es más relevante para diseñar correctamente esta solución?

A) El coste de la licencia del software de replicación de datos, que condicionará el presupuesto disponible para la solución y la selección del proveedor tecnológico más adecuado.

B) La distancia geográfica entre el centro principal y el alternativo, que determinará si ambos centros pueden verse afectados por el mismo evento disruptivo simultáneamente.

C) El número de usuarios concurrentes en el momento de mayor carga, que fijará la capacidad mínima que el centro alternativo debe soportar para mantener el nivel de servicio.

D) El RTO (Recovery Time Objective) y el RPO (Recovery Point Objective) definidos para el servicio, que establecen el tiempo máximo admisible de interrupción y la pérdida de datos tolerable, y condicionan la arquitectura técnica necesaria para la solución.

34. En el contexto del ENS, ¿qué significa que una entidad pública deba mantener la 'continuidad del servicio' desde la perspectiva de la seguridad?

A) Que los sistemas deben estar disponibles las 24 horas del día los 365 días del año sin ninguna interrupción.

B) Que la entidad debe tener capacidad para mantener o recuperar sus servicios esenciales ante incidentes o fallos tecnológicos, dentro de los niveles de servicio definidos.

C) Que la entidad debe disponer de alta disponibilidad con redundancia total de todos sus componentes de infraestructura.

D) Que el proveedor de servicios TI debe garantizar contractualmente la continuidad del servicio sin interrupciones bajo cualquier circunstancia.

35. El director técnico debe elegir para un nuevo sistema de gestión de riesgos entre una arquitectura monolítica bien conocida por el equipo o una arquitectura de microservicios con mayor escalabilidad. ¿Qué enfoque refleja una buena toma de decisiones arquitectónicas?

A) Analizar los atributos de calidad requeridos (escalabilidad, mantenibilidad, coste operativo) frente a las capacidades reales del equipo y el contexto organizativo antes de decidir.

B) Elegir la arquitectura de microservicios porque es la tendencia actual del mercado y ofrecerá mayores capacidades técnicas a largo plazo.

C) Elegir la arquitectura monolítica porque el riesgo de adoptar tecnología nueva en sistemas críticos es siempre inaceptable.

D) Solicitar al proveedor que proponga y decida la arquitectura, ya que es quien mejor conoce las capacidades y limitaciones de las tecnologías disponibles.

36. ¿Qué principio arquitectónico favorece la mantenibilidad de un sistema y reduce el riesgo de que un cambio en un módulo afecte a otros?

A) Alta cohesión y alto acoplamiento: los módulos relacionados deben estar fuertemente integrados para maximizar la eficiencia de las comunicaciones internas.

B) Bajo acoplamiento y baja cohesión: los módulos deben ser independientes y genéricos para permitir su reutilización en distintos contextos.

C) El principio de 'caja negra': los módulos no exponen su funcionamiento interno, aunque pueden tener cualquier nivel de acoplamiento entre ellos.

D) Alta cohesión y bajo acoplamiento: cada módulo tiene una responsabilidad bien definida y las dependencias entre módulos son mínimas y explícitamente controladas.

37. ¿Cuál es la diferencia fundamental entre 'arquitectura' y 'diseño' en el desarrollo de sistemas de información?

A) La arquitectura la realizan consultores externos y el diseño el equipo de desarrollo interno.

B) La arquitectura se documenta en diagramas UML de alto nivel y el diseño en diagramas de clase y código fuente, sin que exista una diferencia conceptual más profunda.

C) La arquitectura define las decisiones estructurales de alto nivel que determinan las propiedades del sistema; el diseño resuelve los detalles de implementación dentro de ese marco.

D) No existe diferencia real; arquitectura y diseño son términos intercambiables que la industria usa indistintamente.

38. Un nuevo sistema de análisis de riesgos debe procesar un volumen de datos diez veces mayor en momentos de crisis de mercado. ¿Cuál es la característica arquitectónica más relevante para satisfacer este requisito?

A) Escalabilidad: el sistema debe poder aumentar su capacidad de procesamiento de forma controlada cuando la demanda lo requiera.

B) Disponibilidad: el sistema debe estar operativo en todo momento con independencia de la carga de trabajo.

C) Seguridad: los datos de riesgo deben estar protegidos también durante los picos de demanda.

D) Mantenibilidad: el sistema debe poder actualizarse y corregirse sin interrumpir el servicio en producción.

39. Una entidad pública evalúa migrar su sistema de gestión de expedientes a la nube. El proveedor ofrece tres modalidades: IaaS, PaaS y SaaS. ¿Cuál de las siguientes descripciones es correcta?

A) La diferencia entre IaaS, PaaS y SaaS es únicamente de precio; técnicamente ofrecen las mismas capacidades de cómputo, almacenamiento y red.

B) IaaS, PaaS y SaaS son tres niveles de seguridad del servicio cloud, siendo SaaS el más seguro por eliminar la responsabilidad del cliente sobre la infraestructura.

C) IaaS proporciona aplicaciones completas listas para usar; PaaS proporciona plataformas de desarrollo; SaaS proporciona infraestructura virtualizada.

D) IaaS proporciona infraestructura virtualizada; PaaS proporciona una plataforma gestionada para desarrollar y desplegar aplicaciones; SaaS proporciona aplicaciones completas como servicio.

40. El sistema A procesa solicitudes de crédito y el sistema B consulta el historial crediticio. La respuesta del sistema B debe obtenerse y mostrarse al usuario en la misma interacción, antes de que el sistema A pueda continuar con la aprobación. ¿Qué tipo de integración es más adecuada entre ambos sistemas?

A) Integración asíncrona mediante mensajería, porque desacopla los sistemas y mejora la resiliencia ante fallos de disponibilidad.

B) Integración síncrona, porque el sistema A necesita la respuesta del sistema B en la misma interacción con el usuario para poder continuar con la aprobación.

C) Ambas opciones son técnicamente equivalentes; la elección depende exclusivamente del volumen de transacciones.

D) Integración basada en eventos, porque el historial debe reaccionar ante los eventos de solicitud de forma asíncrona.

41. Una entidad pública ha implantado un pipeline de CI/CD para el desarrollo de su plataforma digital. ¿Cuál es el principal beneficio de este enfoque desde la perspectiva de la relación entre desarrollo y operación?

A) Elimina la necesidad de pruebas manuales, reduciendo de forma significativa los costes asociados al aseguramiento de la calidad.

B) Garantiza que el software desarrollado cumplirá los requisitos funcionales definidos por el negocio, al automatizar la validación de cada entrega.

C) Permite automatizar la validación y el despliegue del software, reduciendo los errores asociados a la integración y al despliegue, y acortando el tiempo entre el desarrollo de una mejora y su disponibilidad para los usuarios.

D) Permite que el equipo de desarrollo gestione directamente la infraestructura de producción sin intervención del equipo de operaciones.

42. Una entidad financiera pública dispone de un sistema central de gestión de créditos que debe exponer sus funcionalidades a múltiples canales: portal web, app móvil e integraciones con terceros. El equipo propone diseñar una capa de APIs como interfaz de integración. ¿Cuál es el principal beneficio arquitectónico de este enfoque?

A) Garantiza que todos los canales externos tendrán acceso a los mismos datos en tiempo real y sin latencia, independientemente del volumen de peticiones concurrentes.

B) Permite eliminar los sistemas existentes y reemplazarlos de forma inmediata por microservicios de nueva generación sin impacto en los canales.

C) Elimina la necesidad de gestionar acuerdos de nivel de servicio con los canales consumidores, ya que la API gestiona automáticamente las prioridades de acceso.

D) Desacopla los sistemas proveedores de los consumidores, permitiendo que cada uno evolucione de forma independiente sin romper las integraciones existentes, siempre que se mantengan contratos de API compatibles y una política de versionado.

43. Una entidad financiera pública tiene información de clientes, operaciones y riesgos dispersa en más de veinte sistemas sin visión integrada. El responsable de datos propone implantar un gobierno del dato. ¿Cuál debería ser el primer paso?

A) Definir la política de gobierno del dato: principios, roles (data owners, data stewards), responsabilidades y criterios de calidad, antes de seleccionar herramientas o plataformas.

B) Adquirir una herramienta de catálogo de datos para inventariar todos los activos de datos de la organización.

C) Migrar todos los datos a un repositorio centralizado para establecer una única fuente de verdad.

D) Contratar un consultor externo especializado que diseñe el modelo de gobierno adecuado para la entidad.

44. El responsable de datos detecta que el campo 'fecha de alta del cliente' tiene formatos y valores distintos en tres sistemas diferentes. ¿Qué dimensión del gobierno del dato está fallando principalmente?

A) La disponibilidad del dato, porque el dato no está accesible desde un único punto de acceso centralizado.

B) La calidad e integridad del dato: la inconsistencia entre sistemas indica ausencia de estándares de dato maestro y de controles de calidad.

C) La trazabilidad del dato, porque no se puede rastrear con certeza el origen y la cadena de transformación de cada versión del campo.

D) La seguridad del dato, porque distintos sistemas pueden aplicar distintos niveles de protección al mismo campo de datos.

45. En el modelo de gobierno del dato de una organización, ¿cuál es la responsabilidad principal del 'data owner' (propietario del dato)?

A) Gestionar técnicamente la base de datos donde se almacena el dato, aplicando las políticas de seguridad y backup definidas por TI.

B) Auditar el cumplimiento de las políticas de datos definidas por la dirección de TI y reportar las desviaciones al comité de gobierno.

C) Ser responsable de la calidad, disponibilidad y uso adecuado del dato en su dominio de negocio, con autoridad para definir políticas y estándares sobre ese dato.

D) Desarrollar los procesos ETL que alimentan los sistemas analíticos con ese dato, garantizando la integridad de las transformaciones.

46. Una entidad pública debate entre un modelo de Data Warehouse y un modelo Lakehouse. ¿Qué característica diferencia principalmente el Lakehouse del Data Warehouse tradicional?

A) El Lakehouse combina la flexibilidad de almacenamiento del Data Lake con capacidades de gestión de esquemas, calidad, ACID y consulta estructurada propias del Data Warehouse, soportando tanto datos en bruto como análisis estructurado.

B) El Lakehouse es una solución exclusivamente cloud, mientras que el Data Warehouse puede implantarse tanto en la nube como en infraestructura on-premise.

C) El Lakehouse es más económico que el Data Warehouse porque utiliza almacenamiento en objeto en lugar de motores de bases de datos relacionales de alto coste.

D) El Lakehouse elimina la necesidad de procesos ETL, ya que los datos se consumen directamente en su formato original sin transformación previa.

47. Un equipo construye un Data Warehouse para análisis de operaciones de crédito. ¿Cuál de los siguientes esquemas de modelado dimensional es más adecuado para un entorno de reporting con consultas analíticas complejas sobre múltiples dimensiones?

A) Esquema en copo de nieve, porque normaliza las dimensiones eliminando redundancia, lo que facilita la actualización de valores de dimensión y reduce el espacio de almacenamiento a costa de introducir joins adicionales en las consultas.

B) Modelo entidad-relación normalizado, porque garantiza la integridad referencial y evita la redundancia de datos en el sistema analítico.

C) Modelo de datos en grafo, porque permite representar de forma eficiente las relaciones complejas entre clientes, operaciones, garantías y colaterales en el sistema de crédito.

D) Esquema en estrella, porque centraliza las métricas en la tabla de hechos y conecta directamente con tablas de dimensiones desnormalizadas, optimizando el rendimiento de las consultas analíticas.

48. En el diseño de un proceso ETL para alimentar el Data Warehouse de una entidad pública, ¿cuál es el propósito específico de la fase de transformación?

A) Mover los datos desde los sistemas fuente al sistema destino de la forma más rápida y eficiente posible.

B) Convertir, limpiar, validar y enriquecer los datos de los sistemas fuente para que cumplan las reglas de negocio y los estándares de calidad del Data Warehouse.

C) Eliminar los datos duplicados de los sistemas fuente para reducir el volumen de información antes de la carga.

D) Cifrar los datos durante el tránsito entre los sistemas fuente y el Data Warehouse para garantizar su confidencialidad.

49. La dirección solicita un análisis que permita anticipar qué clientes tienen mayor probabilidad de incurrir en mora en los próximos seis meses. ¿Qué tipo de analítica requiere este caso de uso?

A) Analítica descriptiva, porque utiliza datos históricos de comportamiento crediticio de los clientes para generar informes sobre patrones de mora pasados.

B) Analítica prescriptiva, porque el modelo no solo anticipa el comportamiento sino que también recomienda acciones concretas para prevenir la mora de cada cliente identificado.

C) Analítica predictiva, porque utiliza modelos estadísticos o de aprendizaje automático para anticipar comportamientos futuros a partir de datos históricos.

D) Business intelligence tradicional, porque consiste en analizar el histórico de operaciones de crédito mediante cuadros de mando de seguimiento de morosidad.

50. La dirección quiere implantar un sistema de soporte a la toma de decisiones para el comité de riesgos, que proporcione informes históricos sobre la evolución de los indicadores, predicciones de desviaciones futuras en los mismos y recomendaciones sobre límites de exposición. ¿Qué combinación de capacidades analíticas requiere este sistema?

A) Únicamente analítica descriptiva, ya que el comité necesita ante todo disponer de informes históricos detallados sobre la evolución de los indicadores de riesgo.

B) Business intelligence tradicional con cuadros de mando, ya que la supervisión de indicadores y el seguimiento de límites de exposición son casos de uso propios del BI clásico.

C) Analítica descriptiva (informes históricos), analítica predictiva (predicción de desviaciones futuras) y analítica prescriptiva (recomendaciones sobre límites), en combinación.

D) Únicamente analítica prescriptiva, ya que el principal valor del sistema es generar recomendaciones directamente accionables para el comité.

Preguntas de reserva

51. El responsable de TI propone implantar un proceso de mejora continua de los servicios. ¿Cuál de las siguientes afirmaciones refleja mejor su propósito en el gobierno de servicios TI?

A) Sustituir periódicamente los sistemas para mantenerlos actualizados tecnológicamente.

B) Corregir los errores detectados en los sistemas tras los incidentes en producción.

C) Identificar de forma sistemática oportunidades de mejora en el valor, la eficiencia y la calidad de los servicios, y ejecutarlas de forma controlada.

D) Garantizar que el área de TI cumple los objetivos presupuestarios asignados.

52. A través del CAU (Service Desk) del ICO se canalizan a diario múltiples solicitudes e informes de incidencias. El propósito de esta práctica funcional es:

A) Definir un punto único de contacto (SPOC) encargado de capturar la demanda para la resolución de incidentes y peticiones de servicio

B) Facilitar la realización periódica de auditorías técnicas de configuración.

C) Investigar proactivamente la causa raíz de las interrupciones tecnológicas complejas y programar el despliegue de los parches necesarios.

D) Negociar, auditar y redactar formalmente los SLA con los representantes del negocio.

53. Un sistema legacy de gestión de expedientes integra toda su lógica de negocio, acceso a datos e interfaz en un único componente, y presenta problemas crecientes de mantenimiento. ¿Cómo caracterizaría arquitectónicamente este sistema y cuál es el principal riesgo asociado?

A) Es una arquitectura en capas; el riesgo principal es la complejidad de la capa de presentación.

B) Es una arquitectura monolítica; cualquier cambio, por pequeño que sea, puede afectar a todo el sistema y puede requerir el redespliegue de la aplicación completa.

C) Es una arquitectura orientada a servicios; el riesgo principal es la proliferación de interfaces entre componentes.

D) Es una arquitectura de microservicios mal implementada; el riesgo es la fragmentación del dominio de negocio.

54. El área de intervención solicita poder explicar, auditar y reconstruir el recorrido completo de un indicador mostrado en un cuadro de mando, incluyendo su origen, su movimiento y transformación a través de los sistemas, así como las definiciones y descripciones necesarias para entenderlo correctamente. ¿Qué disciplina del marco DAMA-DMBOK2 responde de forma más directa a esta necesidad?

A) Business Intelligence, porque es la función que presenta el dato al usuario final y, por ello, asume de forma natural la reconstrucción completa de su trazabilidad.

B) Gestión de Seguridad de Datos, porque cualquier trazabilidad suficientemente detallada debe considerarse un problema de control de acceso y auditoría.

C) Gestión de Metadatos, porque habilita el acceso a definiciones, modelos, flujos de datos y otra información crítica para comprender los datos y los sistemas a través de los que se crean, mantienen y acceden.

D) Inteligencia Artificial Prescriptiva, porque mediante inferencia automatizada puede reconstruirse el contexto completo de un KPI corporativo.

55. En un esquema en estrella orientado a analítica avanzada, se necesita distinguir con precisión entre estructuras que describen contexto de negocio y estructuras que almacenan eventos o magnitudes medibles. ¿Qué combinación representa con mayor fidelidad una tabla de hechos?

A) Un conjunto de atributos textuales de cierta longitud, catálogos normativos y metadatos operativos, complementados con identificadores técnicos de trazabilidad.

B) Una estructura compuesta por claves foráneas a tablas de dimensiones y medidas numéricas del negocio, normalmente agregables según el caso de uso analítico.

C) Una entidad relacional altamente normalizada que separa cada medida en tablas autónomas para preservar integridad y evitar redundancia.

D) Un repositorio de descripciones jerárquicas de cliente, producto y tiempo cuyo objetivo principal es etiquetar semánticamente el proceso analizado.