

Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación
IIC2523 — Sistemas Distribuidos

Interrogación 2 (2025-2)

Jueves 30 de Octubre 2025

Instrucciones

- La evaluación consta de 31 preguntas de alternativas. Para obtener el 7.0 en la evaluación, se deben tener 30 preguntas correctas.
- Recibirás una hoja de respuestas que deberás rellenar con tus datos y las respuestas correspondientes a cada alternativa. Sólo se corregirá la hoja de respuestas. **Ten mucha precaución de anotar correctamente tus datos y respuestas**.
- Puedes separar la hoja de respuesta del enunciado para responder con mayor facilidad, pero debes garantizar que las respuesta de dicha hoja no queden a la vista de los demás estudiantes.
- Cada pregunta de selección múltiple tiene únicamente 1 alternativa correcta. Responder con 2 o más alternativas implicará dejar inválida esa pregunta y se considerará incorrecta. Además, cada pregunta presenta el mismo puntaje y no se descontará por respuesta incorrecta.
- Solo podrás retirarte de la sala una vez hayan transcurrido 20 minutos desde que inició de la evaluación.
- Durante la evaluación se realizarán 2 rondas de preguntas. Estas preguntas únicamente serán respondidas por el profesor del ramo. La ronda comenzará 20 minutos después de empezar la prueba, se recomienda leer el enunciado antes de la primera ronda.
- Puedes devolver el enunciado si quieres que este sea reciclado.

Selección múltiple

1. Una aplicación crítica de monitoreo industrial debe seguir funcionando incluso si uno de sus componentes falla. Para ello, se implementaron varias estrategias:

   - E1. Se agregan discos de respaldo que almacenan copias de los datos.
   - E2. El sistema ejecuta ciertas operaciones múltiples veces y compara resultados.
   - E3. Existen procesos de respaldo listos para activarse si uno falla.

   ¿Cuál de las siguientes alternativas asocia **correctamente** cada tipo de redundancia con la estrategia descrita en el caso?

	E1	**E2**	**E3**
A)	*Software*	Información	Tiempo
B)	*Hardware*	Tiempo	*Software*
C)	Información	*Hardware*	*Software*
D)	*Hardware*	*Software*	Tiempo
E)	Información	Tiempo	*Hardware*

2. Según lo visto en el curso, ¿cuáles de las afirmaciones describen **correctamente** el tipo de *masking* indicado y su funcionamiento real?

   I. *Hardware* pasivo: Se replica el *hardware* varias veces y se vota la respuesta final. En caso de detectar un componente fallido, se reemplaza por uno no defectuoso.

   II. Tiempo: Se repiten operaciones críticas varias veces y se comparan los resultados para detectar fallos intermitentes.

   III. Información: Se utilizan procesos adicionales para monitorear el estado de los componentes y, a partir de esa información, detectar posibles fallos.

   IV. *Software*: Se utilizan programas adicionales para procesar los datos y agregar información extra (como bits de verificación o códigos) que permita detectar y corregir errores en los mensajes.

   A) Solo II
   B) I y II
   C) I y III
   D) III y IV
   E) I, II, III y IV

3. En un sistema distribuido de almacenamiento de archivos, algunos nodos pueden corromper fragmentos de datos durante la replicación. Para evitar pérdida de información, los datos se envían junto con códigos adicionales que permiten a los nodos detectar y reconstruir cualquier fragmento dañado.

   ¿Cuál de las siguientes alternativas indica **correctamente** el tipo de *masking* utilizado por este sistema?

   A) *Hardware* pasivo.

   B) Información.

   C) Tiempo.

   D) *Software*.

   E) *Hardware* activo.

4. En un clúster distribuido de 4 nodos (A, B, C y D), se necesitan mecanismos para detectar nodos que han dejado de funcionar. Se observan dos estrategias posibles:

   - Estrategia 1: El Nodo A envía periódicamente un mensaje a los demás nodos (Nodo B, C, D) preguntando si siguen activos. Si algún nodo no responde, Nodo A lo marca como sospechoso de fallo.
   - Estrategia 2: Cada nodo (Nodo B, C, D) envía periódicamente señales de vida a Nodo A. Nodo A espera estas señales y, si alguna no llega en el tiempo esperado, interpreta que el nodo correspondiente ha fallado.

   ¿Cuál de las siguientes alternativas describe **correctamente** la diferencia entre estas dos estrategias?

   A) En la primera estrategia el Nodo A recurre a *Heartbeats*, mientras que en la segunda estrategia el Nodo A recurre a *Probes*.

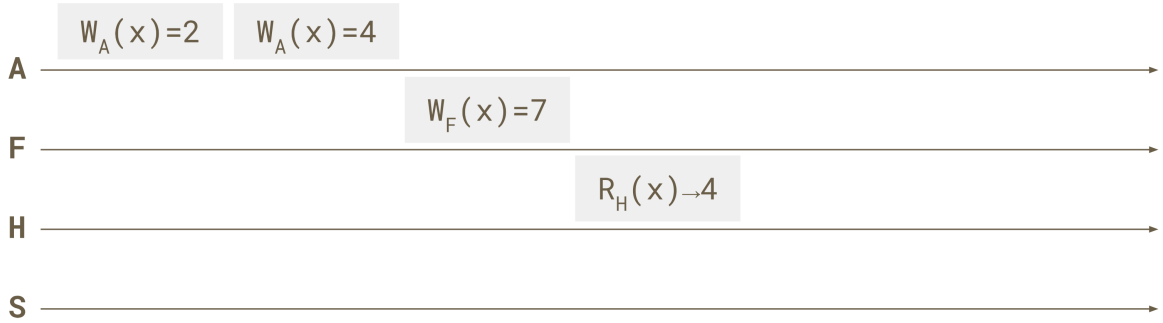
   B) En la primera estrategia el Nodo A recurre a *Probes*, mientras que en la segunda estrategia el Nodo A recurre a *Timeouts*.

   C) En la primera estrategia el Nodo A recurre a *Heartbeats*, mientras que en la segunda estrategia el Nodo A recurre a *Timeouts*.

   D) En la primera estrategia el Nodo A recurre a *Probes*, mientras que en la segunda estrategia el Nodo A recurre a *Heartbeats*.

   E) En la primera estrategia el Nodo A recurre a *Timeouts*, mientras que en la segunda estrategia el Nodo A recurre a *Probes*.

5. ¿Cuál de las siguientes afirmaciones es **correcta** respecto a los modelos de consistencia de la siguiente situación? Considera cada afirmación de forma independiente.



I. Si se hace un R(X) en F que retorne 4 después del W(X)=7, la situación respeta consistencia eventual.

II. Esta situación respeta la consistencia causal.

III. Si el R(X) del nodo H que retorna 4 no existiera, la situación respeta consistencia fuerte.

A) Solo II

B) Solo III

C) I y II

D) II y III

E) I, II y III

6. Una plataforma de noticias cuenta con cuatro servidores, A, B, C y D, que replican datos entre sí. En un tiempo T, los servidores A y B comienzan a publicar noticias distintas: A publica “Noticia A” y B publica “Noticia B”. Posteriormente, cuando la noticia es publicada exitosamente en el servidor de origen, este servidor envía notificaciones a los demás para que sepan de la existencia de la noticia, aunque la entrega de estas notificaciones puede experimentar distintos retrasos entre pares de servidores.

   Considerando que los servidores respetan la consistencia secuencial ¿cuál de los siguientes escenarios **NO es posible** respecto a lo que ven los servidores C y D?

   A) El servidor C indica que existe la noticia de A, mientras que el servidor D indica que existe la noticia de B.

   B) Tanto el servidor C como el servidor D indican que ninguna noticia ha sido publicada hasta el momento.

   C) Tanto el servidor C como el servidor D indican que primero se publicó la noticias de A y luego la de B.

   D) El servidor C indica que primero se publicó la noticias de A y luego la de B, mientras que el servidor D indica que únicamente se encuentra disponible la noticia de A.

   E) Ninguna de las anteriores. Todos los escenarios descritos respetan la consistencia secuencial.

7. En clases se estudió que la replicación de datos se utiliza para permitir una serie de propiedades en el sistema. ¿Cuál de las siguientes afirmaciones son **correctas** respecto a dichas **propiedades**?

    I. Reducir los cuellos de botella para determinadas consultas.

    II. Permitir acceder a determinados servicios incluso sin conectarse al servidor.

    III. Ofrecer una mayor disponibilidad a los datos.

    IV. Reducir el tiempo de respuesta a solicitudes de lectura.

    A) Solo II

    B) Solo III

    C) I y IV

    D) I, III, y IV

    E) I, II, III y IV

8. Dos usuarios ubicados en distintas partes del mundo trabajan con una red social. Saben que, a veces, la información que ven no coincide entre usuarios, pero después de un tiempo la red social termina sincronizando los datos. También saben que el sistema entrega los mensajes entre nodos en el orden en que fueron enviados y ahora desean modificar el tipo de consistencia percibida por los usuarios a alguno de los vistos en el curso IIC2523.

    ¿Cuál de las siguientes acciones **permite lograr este cambio**?

    A) Reducir el número de réplicas a un nodo por país máximo.

    B) Permitir que cada réplica aplique actualizaciones sin coordinarse con otras.

    C) Los mensajes incluyen un mecanismo para determinar la dependencia entre actualizaciones.

    D) Aumentar la frecuencia con la que las réplicas intercambian actualizaciones entre sí.

    E) Priorizar la propagación de ciertas actualizaciones críticas sobre otras.

9. Dos usuarios ubicados en distintas partes del mundo están conversando por videollamada sobre lo que observan al interactuar con la misma aplicación web, la cual utiliza un sistema distribuido.

    Considerando este contexto, ¿cuál de los siguientes escenarios **garantiza la transparencia de distribución**?

    A) El sistema utiliza *Primary-Based Protocol* y permite leer desde cualquier réplica.

    B) El sistema utiliza *Replicated-Write Protocol* con resolución de conflictos automática en todas las réplicas.

    C) El sistema utiliza *Quorum-Based Protocol*.

    D) El sistema utiliza *Gossip Protocol*.

    E) Ninguna de las anteriores.

10. El próximo mes se viene *Black Friday* (28 de noviembre) y una tienda de compras en línea decide utilizar un sistema distribuido con *Totally Ordered Multicast* (TOM) para procesar la gran cantidad de compras. ¿Qué **implica** esto en el sistema?

    A) Las compras se procesan según el rol del cliente que las registra, de modo que algunos clientes siempre tengan prioridad.

    B) Existen compras con un marcador "totally" que siempre se ejecutan antes de todas las demás.

    C) Todas las compras se registran en todos los nodos en el mismo orden, aunque puedan llegar con retrasos distintos.

    D) Las compras más recientes se procesan primero, priorizando la rapidez de atención.

    E) Solo un número limitado de nodos puede registrar compras al mismo tiempo.

11. Durante la noche de *Halloween*, un juego distribuido de "*trick or treat*" permite que los jugadores recojan dulces de distintas casas conectadas a servidores diferentes. Un jugador envía una solicitud para transferir 50 dulces de la Casa de la Bruja a su inventario. Justo después de que el servidor de la casa descuenta los dulces, el servidor del jugador falla. Al reiniciar el sistema, se detecta que los dulces fueron retirados de la casa, pero nunca aparecieron en el inventario del jugador. Respecto a las propiedades ACID, ¿Cuál afirmación es **correcta**?

    A) Dentro de las propiedades ACID, la consistencia se está vulnerando.

    B) Dentro de las propiedades ACID, la atomicidad se está vulnerando.

    C) Dentro de las propiedades ACID, el aislamiento se está vulnerando.

    D) Dentro de las propiedades ACID, la disponibilidad se está vulnerando.

    E) No se vulnera ninguna propiedad ACID, esto fue solo un fallo del servidor.

12. Un sistema bancario distribuido implementa un protocolo por fases para coordinar transacciones entre varias sucursales. Durante una operación, el coordinador envía el mensaje correspondiente para consultar si es posible ejecutar la transacción, y todos los participantes responden afirmativamente. Sin embargo, el coordinador solo alcanza a recibir todas las confirmaciones antes de fallar, por lo que la segunda fase de este protocolo nunca ocurre. ¿Cuáles de las siguientes afirmaciones son **correctas**?

    I. Entre las propiedades ACID, se está comprometiendo el Aislamiento.

    II. Entre las propiedades ACID, se está comprometiendo la Disponibilidad.

    III. Esta situación repercute en que los nodos bloqueen ciertos datos para evitar que otras transacciones los modifiquen.

    A) Solo II

    B) Solo III

    C) I y III

    D) I y II

    E) I, II y III

13. ¿Cuál de las siguientes afirmaciones es **correcta** respecto al protocolo **3PC**?

    A) La transacción en este protocolo solo puede ser abortada por quien la inicia.

    B) Si falla el coordinador, los demás nodos participantes quedan bloqueados indefinidamente.

    C) Los nodos participantes solo conocen al coordinador.

    D) Este protocolo tiene casos en los que la cantidad de mensajes es menor que en 2PC.

    E) Ninguna de las anteriores.

14. Dispones de un sistema distribuido que utiliza control de concurrencia basado en validación. Cada transacción aplica exclusivamente un tipo de validación (*forward* o *backward*). Además, el sistema no aborta automáticamente las transacciones rechazadas, sino que estas pueden esperar y volver a intentar la validación si las condiciones cambian. Dado este contexto, ¿Cuáles de las siguientes afirmaciones son **correctas**?

    I. Si utiliza validación *forward*, pueden existir interbloqueos entre transacciones.

    II. Si utiliza validación *backward*, pueden existir interbloqueos entre transacciones.

    III. Si utiliza validación *forward*, una transacción rechazada podría ser aceptada posteriormente.

    IV. Si utiliza validación *backward*, una transacción rechazada podría ser aceptada posteriormente.

    A) Solo I

    B) Solo II

    C) I y III

    D) II y IV

    E) Todas las afirmaciones son correctas.

15. Un sistema de gestión de paquetes para grandes empresas implementó un sistema donde cualquier usuario de la misma empresa puede actualizar el pedido que hizo su empresa, lo cual permite que múltiples usuarios editan simultáneamente un pedido. Para resolver conflictos, se desea que el sistema conserve automáticamente y únicamente la actualización realizada por el usuario con mayor rol de prioridad. En un caso donde no hay empate (un único usuario tiene la prioridad más alta), ¿qué tipo de **resolución de conflicto** se debe **implementar** en el sistema?

    A) *Merge* semántico.

    B) *Last Write Wins*.

    C) *Merge* manual.

    D) Versiones.

    E) *Operational Transformation*.

16. En un sistema distribuido de control de inventario, se produce la siguiente secuencia:

    - Tiempo 1: Se modifica exitosamente el *stock* del producto P.
    - Tiempo 2: Dos nodos acceden y leen el *stock* actualizado de P.
    - Tiempo 3: Se modifica nuevamente y exitosamente el *stock* del producto P por un nodo diferente al del Tiempo 1 y cuando los dos nodos del Tiempo 2 ya no están observando el *stock*.

    ¿Cuál de las siguientes afirmaciones es **correcta**?

    A) Hay un conflicto de lectura-lectura cuando se permite que dos nodos accedan al mismo valor.

    B) Hay conflicto de escrituras por intentar modificar dos veces el mismo *stock*.

    C) Hay conflicto lectura-escritura por modificar algo que fue leído anteriormente.

    D) Si en Tiempo 2 se intenta modificar el *stock* en función de lo leído, ahí sí se generaría un conflicto lectura-lectura.

    E) La situación actual no muestra conflicto por concurrencia.

17. ¿Cuales de las siguientes afirmaciones son correctas respecto a la **tercera tarea** del curso?

    I. Consistía en simular transacciones con un mecanismo de control de concurrencia optimista.

    II. Se recurrió al protocolo 3PC junto con quórum.

    III. Los *tests* venían en formato JSONC.

    IV. Las validaciones se realizaban exclusivamente en la primera fase del protocolo utilizado.

    A) Solo I

    B) I y III

    C) II y IV

    D) III y IV

    E) I, II, III y IV

18. Una plataforma para subir exclusivamente videos de gatitos cuenta con réplicas distribuidas para optimizar el rendimiento en el mundo. Los usuarios acceden y publican videos desde réplicas regionales, que luego se sincronizan con un servidor central. En condiciones normales, los videos publicados quedan inmediatamente disponibles en la réplica regional correspondiente para que se pueda ver. Posteriormente, el contenido se replica mediante el protocolo *gossip* a las demás réplicas y servidor central. Sin embargo, cuando el video llega eventualmente al servidor central, éste revisa su contenido y puede eliminarlo si no cumple con tener gatitos, lo que provoca que las réplicas regionales comienzan a denegar el acceso a dicho video.

    Finalmente, si alguna región pierde conexión con el servidor central, los usuarios pueden seguir viendo los videos que están disponibles en dicha región y publicar videos, los cuales serán validados cuando la conexión se recupere.

    ¿Cuál de las siguientes afirmaciones es **correcta** respecto a la descripción del sistema bajo el teorema **PAC y PACELC**?

    A) Ante partición, el sistema prioriza consistencia para publicación de videos.
    Sin partición, se prioriza la latencia para ambas operaciones.

    B) Ante partición, el sistema prioriza consistencia para visualizar videos.
    Sin partición, se prioriza la latencia para la publicación de videos.

    C) Ante partición, el sistema prioriza disponibilidad para visualizar los videos.
    Sin partición, se prioriza la latencia para la publicación de videos.

    D) Ante partición, el sistema prioriza disponibilidad para visualizar y publicar videos.
    Sin partición, se prioriza consistencia en ambas operaciones.

    E) El sistema prioriza la consistencia para visualizar y publicar videos, tanto en partición como sin partición.

19. Un sistema distribuido de base de datos replica la información entre tres nodos en distintas regiones. Durante una partición de red, el sistema permite lecturas locales desde cualquier nodo, aunque puedan devolver valores desactualizados, pero bloquea las escrituras hasta que se recupere la conexión. En condiciones normales, las lecturas se sirven localmente para responder más rápido, mientras que las escrituras requieren confirmación de al menos dos nodos antes de completarse.

    Según el teorema **PACELC**, ¿qué clasificación describe **correctamente** el comportamiento del sistema?

    A) Lecturas: PC/EC — Escrituras: PA/EL.

    B) Lecturas: PA/EC — Escrituras: PA/EL.

    C) Lecturas: PC/EL — Escrituras: PC/EL.

    D) Lecturas: PA/EL — Escrituras: PC/EC.

    E) Lecturas y escrituras comparten el mismo PACELC: PA/EC.

20. Respecto al teorema **PACELC**, ¿cuál de las siguientes afirmaciones describe **correctamente** su aporte frente al teorema CAP?

    A) PACELC reemplaza el teorema CAP al eliminar la necesidad de elegir entre disponibilidad y consistencia durante una partición.

    B) PACELC mantiene la lógica del CAP durante una partición, pero agrega un segundo análisis para el comportamiento del sistema cuando la red funciona normalmente.

    C) PACELC se aplica sólo a sistemas que garantizan consistencia eventual, por lo que no describe sistemas fuertemente consistentes.

    D) PACELC amplía el teorema CAP incorporando dos nuevos términos a este análisis.

    E) PACELC es una simplificación del teorema CAP que elimina una variable de la discusión para enfocarse únicamente en la consistencia y disponibilidad.

21. Respecto al teorema CAP visto en clases, ¿cuáles de las siguientes afirmaciones representan **críticas reales** sobre su aplicabilidad en sistemas distribuidos modernos?

    I. CAP aborda el caso de partición y no describe con detalle qué ocurre cuando la red funciona normalmente.

    II. CAP trata consistencia y disponibilidad como valores absolutos, sin contemplar compromisos parciales entre ambos.

    III. CAP no distingue entre diferentes tipos de fallas de red, tratando todas las particiones como equivalentes.

    IV. CAP ignora la escalabilidad de los sistemas distribuidos.

    A) Solo I

    B) I y II

    C) II y III

    D) I, II y III

    E) I, II, III y IV

22. Te llegó un correo de un príncipe de Nigeria que te está pidiendo los datos de tu tarjeta de crédito para financiar una fiesta de *Halloween*. Encantado por ayudar a este príncipe, empiezas a escribir tus datos y cuando oprimes enviar, el sistema lanza un error dado que ese correo ya no existe porque el *firewall* del correo lo había eliminado, pero la interfaz todavía no mostraba dicho cambio. ¿Qué propiedad de **consistencia centrada en el cliente** se ve **vulnerada** principalmente?

    A) *Monotonic Writes*.

    B) *Monotonic Reads*.

    C) *Read Your Writes*.

    D) *Writes Follow Reads*.

    E) Ninguna propiedad se está fallando.

23. Durante *Halloween*, un sitio web llamado El Foro de los Sustos permite a los usuarios comentar historias paranormales en vivo. La usuaria "Momo" entra desde su computador a leer la historia "El Mac con sistema Windows". Mientras la lee, nota que el contador de comentarios marca 128 y que entre ellos hay uno muy reciente de su amigo "Ken", quien escribió: "Nunca más dejo un Windows y un Mac en la misma habitación"

    Un rato después, "Momo" abre la misma historia desde su celular para mostrarle dicho comentario a otra amiga. Sin embargo, al revisar, el foro muestra solo 121 comentarios, y el texto de "Ken" no aparece. Sorprendida, piensa que quizás "Ken" lo borró, pero cuando vuelve a recargar la página en el computador, el comentario sigue allí. Cuando le pregunta a "Ken" sobre si hizo algo con el comentario, él responde que solamente escribió ese texto desde el celular y no ha vuelto a ingresar al sitio web.

    ¿Qué propiedad de las **consistencias centradas en el cliente** se ve **vulnerada** para el usuario "Ken"?

    A) *Monotonic Writes*.

    B) *Writes Follow Reads*.

    C) *Read Your Writes*.

    D) *Monotonic Reads*.

    E) Ninguna.

24. Un servicio de compras distribuido cuenta con 3 réplicas, de las cuales se garantiza que hay al menos 2 activas en todo momento. Para mejorar la experiencia del cliente se implementan las siguientes medidas:

    - Cada compra se ejecuta solo si fue aceptada exitosamente en una réplica adicional a la réplica donde se originó. Para esto, se envía la orden de compra junto con el *stock* disponible de cada producto según la réplica de origen.
    - Para aceptar una compra, la réplica consultada valida que el *stock* disponible del producto sea igual al informado en la compra.
    - Cada acceso de un cliente se dirige siempre a la réplica que esté más actualizada y contenga registros de la última compra exitosa del cliente.

    Considerando estas medidas, desde la experiencia del cliente, y considerando que los *writes* solo ocurren cuando se realiza la compra con éxito, ¿qué propiedad de consistencia centrada en el cliente **no se puede garantizar** con seguridad?

    A) *Monotonic Reads*.

    B) *Read Your Writes*.

    C) *Monotonic Writes*.

    D) *Writes Follow Reads*.

    E) Existe más de una propiedad que no se garantiza.

25. Dos usuarios, A y B, ingresaron desde su celular al último capítulo del manga que estaban esperando y, al terminar de leerlo, escribieron en la zona de comentarios: "¡Qué gran capítulo! Soy el primero". Una vez que el sistema les indicó que el comentario fue enviado correctamente, ambos cerraron la página sin verificar que apareciera publicado.

    Más tarde, el usuario A ingresó desde su computador al mismo capítulo con la intención de editar su comentario para añadir "Gracias por la traducción." Sin embargo, al revisar la zona de comentarios, notó que solo aparecía el comentario del usuario B, y el suyo no estaba en ninguna parte.

    ¿Qué propiedad de la consistencia centrada en el cliente se **vulnera** para el **usuario A**?

    A) *Read Your Writes*.

    B) *Monotonic Reads*.

    C) *Monotonic Writes*.

    D) *Writes Follow Reads*.

    E) Ninguna, ya que el usuario no verificó que su comentario se hubiera reflejado correctamente.

26. Un sistema de compras fue atacado mediante un virus similar a *Stuxnet*, el cuál se encargó únicamente de modificar los permisos de los usuarios, permitiendo a un usuario no autorizado acceder a la base de datos y extraer el historial de compras de los usuarios. Finalmente, volvió a restaurar los permisos de los usuarios para que no quedara evidencia de que había un usuario con permisos inadecuados.

    Según lo enseñado en clases ¿cuáles de las 3 **amenazas** se vieron **aplicadas** en este ataque?

    A) Únicamente *Leakage*.

    B) Únicamente *Tampering*.

    C) Únicamente *Leakage* y *Tampering*.

    D) Únicamente *Tampering* y *Denial of Use*.

    E) *Leakage*, *Tampering* y *Denial of Use*.

27. En el debate sobre la seguridad computacional, se analizan los compromisos (*trade-offs*) que puede implicar la implementación de los diferentes mecanismos de seguridad. ¿Cuáles de las siguientes afirmaciones son **correctas**?

    I. Existen mecanismos de seguridad que comprometen la usabilidad del sistema.

    II. Todos estos mecanismos garantizan una mejor privacidad para el usuario.

    III. El rendimiento y la seguridad suelen competir por recursos en el diseño de un sistema.

    A) Solo I

    B) Solo II

    C) Solo III

    D) Solo I y III

    E) Solo I, II y III

28. ¿Cuál de las siguientes contribuciones **ganó el premio *Dijkstra* el 2001**?

    A) El concepto de Consistencia Eventual.

    B) Teorema de Imposibilidad de Fischer, Lynch y Paterson.

    C) Teorema PACELC.

    D) El protocolo de replicación *Gossip*.

    E) El algoritmo de Chandy-Lamport.

29. ¿Cuál de las siguientes afirmaciones es **correcta** respecto a la propiedad de **no-repudio** en criptografía?

    A) El no-repudio garantiza que un mensaje no pueda ser interceptado ni modificado durante su transmisión.

    B) El no-repudio asegura que el receptor no pueda negar haber recibido el mensaje.

    C) El no-repudio se basa en que ambas partes compartan la misma clave secreta para firmar los mensajes.

    D) El no-repudio se logra mediante funciones *hash* que aseguran que el contenido no sea alterado.

    E) El no-repudio asegura que un nodo no pueda rechazar un mensaje firmado con su clave privada.

30. ¿Cuál de las siguientes afirmaciones describe **correctamente** la criptografía **asimétrica**?

    A) Utiliza un par de llaves distintas por usuario: una se utiliza exclusivamente para cifrar cualquier mensaje y otra exclusivamente para descifrar cualquier mensaje.

    B) Es más rápida que la criptografía simétrica y se suele usar para cifrar grandes volúmenes de datos.

    C) Solo se utiliza para proteger la integridad de los datos, sin garantizar confidencialidad.

    D) Requiere un mecanismo que garantice el intercambio seguro de la llave usada para cifrar algún mensaje.

    E) Ninguna de las anteriores.

31. ¿Cuál es el **objetivo** principal del protocolo **Diffie–Hellman**?

    A) Generar una clave compartida entre dos partes a través de un canal inseguro.

    B) Cifrar mensajes entre dos partes sin usar criptografía simétrica ni asimétrica.

    C) Autenticar la identidad de los participantes.

    D) Firmar digitalmente documentos para garantizar la autenticación de su emisor.

    E) Ninguna de las anteriores.