

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

Examen (2026-1)

Lunes 06 de Julio 2026

Instrucciones

- La evaluación consta de 37 preguntas de alternativas. Para obtener el 7.0 en la evaluación, se deben tener 36 preguntas correctas.
- Recibirás una hoja de respuestas que deberás rellenar con tus datos y las respuestas correspondientes a cada alternativa. Solo se corregirá la hoja de respuestas. **Ten mucha precaución de anotar correctamente tus datos y respuestas**.
- Puedes separar la hoja de respuestas del enunciado para responder con mayor facilidad, pero debes garantizar que las respuestas de dicha hoja no queden a la vista de los demás estudiantes.
- A no ser que se indique lo contrario, 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.
- Si te equivocas con una alternativa, puedes poner una cruz encima de ella y pintar la correcta. Se asignará el puntaje a aquella que **no tiene la cruz encima**.
- Solo podrás retirarte de la sala una vez hayan transcurrido 30 minutos desde el inicio de la evaluación.
- Durante la evaluación se realizarán 2 rondas de preguntas. Estas preguntas únicamente serán respondidas por el profesor del ramo. La primera ronda comenzará 40 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 plataforma en la nube debía reiniciar varios servidores al mismo tiempo. Sin embargo, uno de los nodos tenía su reloj desfasado respecto de los demás, por lo que ejecutó la acción más tarde y repercutió finalmente en la caída completa del servicio por más de 1 hora. A partir de la situación descrita, ¿cuál de los siguientes **problemas clásicos** de los sistemas distribuidos se ve **representado** en este caso?

    I. Complejidad Inherente de los sistemas distribuidos.

    II. Problemas de Latencia y Ancho de Banda.

    III. Gestión de fallos parciales.

    A) Solo I.

    B) Solo II.

    C) I y III.

    D) II y III.

    E) I, II y III.

2. Una empresa de detectores de humo tenía un sistema en el que el detector notificaba a un servidor en caso de humo, y este a su vez enviaba mensajes a los bomberos y al propietario. Sin embargo, cuando el sensor comenzó a fallar, fue necesario reemplazarlo por uno más moderno. El principal problema fue que la empresa tuvo que actualizar por completo el servidor para integrar el nuevo sensor.

    Desde una perspectiva de los Sistemas Distribuidos, ¿Cuál es el **principal objetivo fundamental que no se logró** asegurar en este caso?

    A) Apertura.

    B) Confiabilidad.

    C) Compartir Recursos.

    D) Escalabilidad.

    E) Seguridad.

3. Considerando los paradigmas de comunicación en sistemas distribuidos, ¿cuál de las siguientes afirmaciones es **correcta** según los criterios presentados en clases?

    I. La comunicación directa se distingue por ser la forma más sencilla de paso de mensajes, pero estableciendo una fuerte dependencia temporal y referencial.

    II. La comunicación remota se caracteriza por invocar acciones en otros servidores y suele encapsular el paso de mensajes en una capa adicional.

    III. Para la Comunicación Remota, las 2 opciones que existen son: *Remote Procedure Call* (RPC) y *Remote Method Invocation* (RMI).

    A) Solo I.

    B) Solo II.

    C) I y II.

    D) II y III.

    E) I, II y III.

4. Considerando las características de la comunicación de red, ¿cuál de las siguientes afirmaciones describe **con mayor precisión** el término RPC y el propósito de los *stubs*?

    A) Es una forma de comunicación indirecta, donde los *stubs* actúan como intermediarios entre el emisor y múltiples receptores.

    B) Es un tipo de comunicación acoplado temporalmente, y los *stubs* permiten la transparencia al convertir llamadas de funciones locales en mensajes de red y viceversa.

    C) Es un protocolo de transporte que garantiza la entrega de paquetes en orden, mientras que los *stubs* se encargan del reenvío de datos perdidos.

    D) Es un tipo de comunicación asíncrona y desacoplada temporalmente, donde los *stubs* se encargan de la persistencia de los mensajes.

    E) Es un tipo de comunicación donde los mensajes son *human readable*, y los *stubs* se encargan de definir las distintas URLs para interactuar con cada nodo.

5. ¿Cuál de las siguientes afirmaciones sobre los protocolos de comunicación es **correcta**?

    A) TCP es comúnmente utilizado en aplicaciones en tiempo real como juegos en línea o llamadas, ya que prioriza la velocidad, entrega de datos y no reenvía paquetes perdidos.

    B) HTTP, FTP y SSH son ejemplos de protocolos que utilizan UDP para asegurar la rapidez de comunicación por internet.

    C) DNS es un protocolo centralizado que permite obtener la dirección IP de destino a partir de una URL.

    D) TCP establece una conexión previa a empezar la comunicación. Además, garantiza la entrega de los mensajes.

    E) UDP garantiza la integridad de los datos, pero no necesariamente el orden de estos.

6. Considerando los distintos paradigmas de comunicación y sus características vistos en clases, ¿cuál de las siguientes afirmaciones es **correcta**?

    I. Los *sockets* exigen un acoplamiento temporal y referencial.

    II. El sistema de colas es un ejemplo de comunicación indirecta en el que, por defecto, se necesita que ambas partes (emisor y receptor) estén activos durante la transmisión.

    III. Una comunicación asíncrona implica que la comunicación sea temporal.

    A) Solo I.

    B) Solo II.

    C) I y II.

    D) II y III.

    E) I, II y III.

7. ¿Cuál de las siguientes acciones describe **correctamente el funcionamiento principal del algoritmo de Berkeley** para sincronización de relojes?

    A) Un líder solicita la hora a los demás nodos, calcula un valor de ajuste común y luego indica cuánto debe corregir cada reloj.

    B) Cada nodo consulta varios servidores de tiempo externos y ajusta su reloj privilegiando la referencia cuya respuesta presenta menor retardo estimado.

    C) Los nodos intercambian sus horas entre sí y adoptan automáticamente la mayor de ellas.

    D) Un nodo consulta a un servidor de tiempo, estima el retardo de comunicación y ajusta su reloj usando la hora recibida.

    E) Un nodo líder entrega su hora exacta y todos los demás la adoptan.

8. Una empresa opera una plataforma distribuida de venta de entradas para conciertos. Los usuarios pueden comprar entradas desde distintas ciudades del país, y los servidores utilizan relojes lógicos de Lamport para ordenar los eventos. Considerando las propiedades de este mecanismo, ¿cuál de las siguientes conclusiones es **incorrecta**?

    A) Si un servidor procesa una compra y luego envía una solicitud para reservar un asiento en otro servidor, entonces el *timestamp* lógico de la compra será menor que el de la reserva.

    B) Si en un mismo servidor se registra un pago y luego se genera la entrada electrónica correspondiente, entonces el *timestamp* lógico del pago será menor que el de la generación de la entrada.

    C) Si el *timestamp* lógico de una compra es menor que el de otra compra realizada en un servidor distinto, se puede concluir que la primera ocurrió antes que la segunda.

    D) Dos compras realizadas simultáneamente en servidores distintos podrían recibir el mismo *timestamp* lógico, ya que son eventos concurrentes.

    E) Ninguna de las anteriores.

9. En un sistema distribuido con tres nodos A, B y C, cada evento se representa mediante un vector lógico con la estructura `[nodo A, nodo B, nodo C]`. Si en cierto instante el nodo A posee un evento con vector `[3,2,4]` y el nodo C posee un evento con vector `[3,5,6]`, ¿cuál de las siguientes conclusiones es **correcta**?

   A) Ambos eventos son concurrentes entre sí.

   B) Uno de los eventos podría representar el envío de un mensaje y el otro su posterior recepción entre nodos distintos.

   C) El evento en C ocurrió antes que el evento en A.

   D) No es posible comparar vectores lógicos de nodos distintos.

   E) El evento en A ocurrió antes que el evento en C.

10. Estás implementando el algoritmo de *Chandy-Lamport* para obtener un *snapshot* distribuido. Luego de programar el registro del estado local de un nodo, das por finalizado el algoritmo en dicho nodo, pero un colega te indica que también faltó considerar el estado de los canales de comunicación. ¿Cuál de las siguientes afirmaciones evalúa **correcta** la observación del colega?

    A) Es correcta, ya que deben registrarse todos los mensajes enviados por cada nodo luego del *snapshot* local.

    B) Es parcialmente correcta, ya que basta registrar la cantidad total de mensajes por canal.

    C) Es incorrecta, porque registrar el estado local del nodo basta para construir el *snapshot* global.

    D) La observación puede ser correcta o incorrecta, dependiendo de si el sistema posee relojes físicos sincronizados o no.

    E) Es correcta, ya que también deben registrarse los mensajes en tránsito asociados a ciertos canales de entrada.

11. En una implementación de Paxos con 2 nodos proponentes y 7 nodos aceptantes, se busca tomar consenso sobre cuál será la cena de Navidad, para esto un proponente envía un mensaje `prepare(10)` antes de proponer el valor ~~`'Papas duquesas'`~~ `'Pavo'`.

    Las respuestas recibidas son:

    - Un aceptante ya había aceptado ~~`(7, 'Puré de manzana')`~~ `(7, 'Papa duquesa')`.
    - Otro aceptante ya había aceptado ~~`(8, 'Pavo')`~~ `(8, 'Choripán')`.
    - Los 4 aceptantes restantes responden con `OK`.

    ¿Cuál debe ser la acción que el proponente debe realizar para que el **consenso continúe correctamente según Paxos**?

    A) Hacer `accept(10, 'Papas duquesas')`.

    B) Hacer `accept(10, 'Choripán')`.

    C) Hacer `accept(10, 'Puré de manzana')`.

    D) Hacer `accept(8, 'Pavo')`.

    E) Hacer `accept(8, 'Papas duquesas')`.

12. Una empresa utiliza un sistema distribuido para coordinar pedidos entre varias sucursales. Durante una reunión técnica, Jorge M. afirmó que el sistema está bajo un ataque bizantino. ¿Cuál de las siguientes situaciones constituye **evidencia** que respalda su afirmación?

    A) Un nodo informa a una sucursal que un pedido fue aprobado y a otra que el mismo pedido fue rechazado.

    B) Un nodo deja de aceptar pedidos después de una interrupción eléctrica.

    C) Los mensajes demoran más de lo habitual en llegar a su destino.

    D) Un nodo rechaza todas las solicitudes que recibe debido a un error en su configuración.

    E) Los relojes de algunos nodos presentan diferencias de algunos milisegundos.

13. En un sistema distribuido con 4 nodos que emplea el algoritmo de Raft, la situación de los *logs* es la siguiente:

    - Nodo A: contiene el *log* más actualizado.
    - Nodos B y C: poseen un *log* idéntico, pero menos actualizado que A.
    - Nodo D: tiene el log vacío.

    Se inicia un proceso de elección de líder. ¿Cuál de las siguientes alternativas indica correctamente todos los **nodos que podrían llegar a ser líder**?

    A) Solo el nodo A.

    B) Solo el nodo D.

    C) Solo los nodos A y D.

    D) Solo los nodos B y C.

    E) Solo los nodos A, B y C.

14. En un sistema distribuido de 5 nodos, donde se utiliza el algoritmo *Raft* para consenso, ¿cuál de las siguientes afirmaciones es **correcta**?

    A) Si se caen 2 nodos y uno de ellos es el líder, el algoritmo no logrará continuar con su correcto funcionamiento.

    B) Si se caen 3 nodos y ninguno de ellos es el líder, el algoritmo logrará continuar con su correcto funcionamiento.

    C) El algoritmo es tolerante a particiones siempre y cuando en cada partición quede la misma cantidad de nodos.

    D) Ante un cambio de líder, algunas acciones registradas previamente por el líder saliente podrían no formar parte del estado final del sistema.

    E) Si una acción no fue consolidada durante el mandato (*term*) en que fue registrada por el líder, no podrá ser consolidada en un mandato (*term*) posterior.

15. En una red de servidores distribuida, cada nodo puede solicitar acceso exclusivo a un recurso compartido. Se asume que todos los nodos tienen relojes que se sincronizan a UTC a las 00:00 de cada día y que ningún nodo falla. No obstante, la velocidad de envío y recepción de mensajes entre nodos es variable. Se requiere garantizar que la propiedad de *safety* y *ordering* se cumpla. ¿Cuál de los siguientes algoritmos **cumple esta condición**?

    I. *Multicast* de Ricart & Agrawala.

    II. Servidor Central.

    III. *Token Ring*.

    A) Solo I.

    B) Solo II.

    C) I y III.

    D) II y III.

    E) Ninguno de los algoritmos.

16. Un equipo propone modificar un algoritmo distribuido agregando temporizadores (*timeouts*) para decidir cuándo ignorar nodos lentos. Afirman que con esto se elimina la imposibilidad demostrada por el Teorema de Fischer, Lynch y Paterson (FLP), que establece límites para alcanzar consenso en sistemas distribuidos asíncronos.

    ¿Cuál alternativa evalúa **correctamente esta afirmación**?

    A) Es incorrecta, porque los *timeouts* introducen supuestos adicionales que no forman parte de FLP.

    B) Es correcta, porque los *timeouts* eliminan completamente la asincronía.

    C) Es correcta, porque FLP solo aplica cuando existen fallos bizantinos.

    D) Es incorrecta, porque FLP demuestra que ningún algoritmo puede alcanzar consenso bajo ninguna condición.

    E) Es correcta, porque mientras los *timeouts* sean suficientemente largos siempre será posible distinguir entre un nodo lento y uno que ha fallado.

17. Una empresa financiera opera una base de datos distribuida entre varias sucursales. El objetivo es que, al finalizar cada jornada, todos los servidores mantengan exactamente el mismo resultado acumulado. Sin embargo, debido a restricciones regulatorias, también se exige que cada operación confirmada sea visible inmediatamente en todos los servidores y que cualquier consulta refleje siempre el valor más reciente disponible.

    Considerando este escenario, ¿qué modelo de **consistencia** resulta más **adecuado**?

    A) Consistencia fuerte.

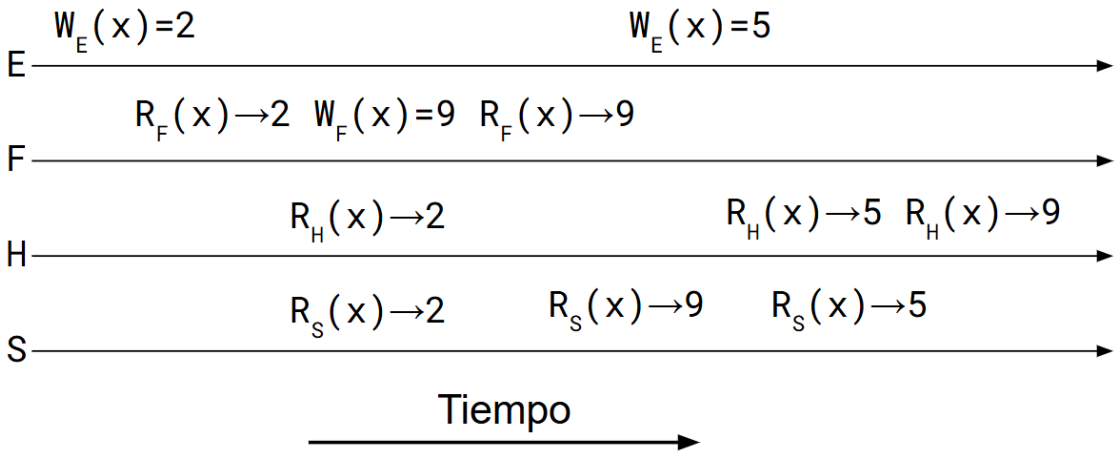
    B) Consistencia secuencial.

    C) Consistencia eventual.

    D) Consistencia causal.

    E) Ninguno, porque en un sistema distribuido no existe un modelo de consistencia que permita garantizar simultáneamente sincronización inmediata y resultados idénticos entre todos los servidores.

18. Considere el historial de operaciones mostrado en la figura, donde (W) representa escritura y (R) la lectura sobre la variable (x).



    Suponiendo que no existen más operaciones posteriores a las mostradas y evaluando únicamente las garantías observables en el historial, ¿cuál de los siguientes modelos de **consistencia** puede afirmarse que se **cumple**?

    A) Solo consistencia eventual.

    B) Solo consistencia secuencial.

    C) Solo consistencia causal.

    D) Consistencia secuencial y causal.

    E) Consistencia eventual y causal.

19. ¿Cuál de las siguientes afirmaciones es **correcta** respecto a los protocolos de replicación *Primary-Based Protocols* y *Replicated-Write Protocols*?

    A) *Primary-Based Protocols* es conocido como replicación activa, mientras que *Replicated-Write Protocols* es conocido como replicación pasiva.

    B) *Primary-Based Protocols* presenta una mayor cantidad de mensajes que *Replicated-Write Protocols* para funcionar correctamente.

    C) *Replicated-Write Protocols* transmite cambios de estado entre réplicas, mientras que *Primary-Based Protocols* replica las operaciones para que las demás réplicas las ejecuten.

    D) *Replicated-Write Protocols* tiene la capacidad de garantizar consistencia eventual, mientras que *Primary-Based Protocols* no.

    E) Tanto *Primary-Based Protocols* como *Replicated-Write Protocols* tienen la capacidad de garantizar consistencia secuencial.

20. Cuando trabajamos con transacciones distribuidas, aparece el desafío de lograr que una transacción tome una decisión única entre múltiples servidores participantes. Para enfrentar este problema se diseñaron protocolos como el *commit* de 2 fases (2PC), que permite coordinar una decisión conjunta para confirmar o cancelar una transacción.

    ¿Qué **contribución** incorpora el protocolo de *commit* de 3 fases respecto al de 2 fases?

    A) Permite que cada participante confirme la transacción de manera independiente si ya terminó sus operaciones.

    B) Reduce la posibilidad de que los participantes queden esperando indefinidamente una decisión cuando falla el coordinador.

    C) Elimina la necesidad de reservar recursos antes del *commit*.

    D) Garantiza que las transacciones logren ser commiteadas en un entorno distribuido.

    E) Optimiza la cantidad de mensajes intercambiados entre servidores.

21. ¿Cuál de los siguientes mecanismos **garantiza** que todas las transacciones iniciadas eventualmente serán commiteadas?

    A) Aplicando Control de Concurrencia Pesimista.

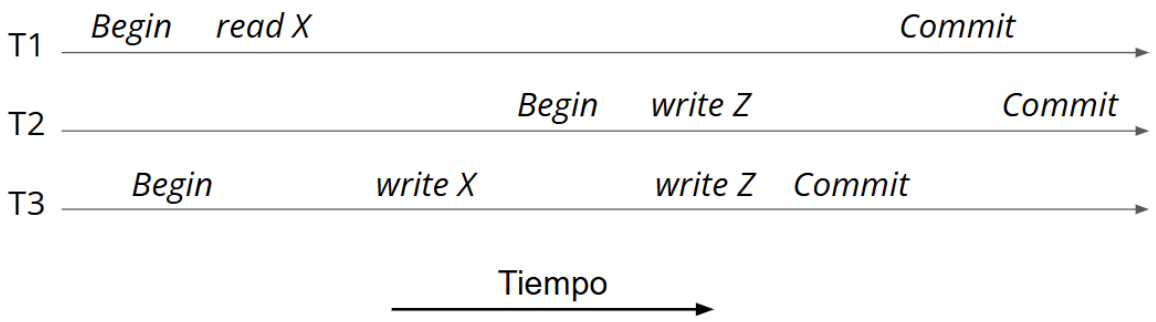
    B) Aplicando Control de Concurrencia Optimista con validación *backward*.

    C) Aplicando Control de Concurrencia Optimista con validación *forward*.

    D) Aplicando el protocolo 3PC.

    E) Ninguna de las anteriores.

22. Considere la siguiente ejecución usando validación ***forward***.



¿En cuál alternativa se indica y justifica **correctamente** el momento donde se detecta el primer conflicto?

A) En T3, al intentar hacer `COMMIT`, porque al validar se detecta que escribió una variable utilizada por una transacción activa.

B) En T1, al intentar hacer `COMMIT`, porque detecta que otra transacción commiteada modificó una variable que T1 había leído previamente.

C) En T3, al ejecutar `WRITE X`, porque una transacción no puede escribir una variable que otra transacción ya leyó.

D) En T2, al ejecutar `BEGIN`, porque al iniciar una transacción se valida que el estado actual del sistema permita continuar sin conflictos.

E) No se detecta conflicto porque las transacciones realizan sus escrituras en momentos distintos.

23. Una empresa multinacional utiliza un sistema distribuido para aprobar movimientos financieros. Debido a desconexiones temporales, una misma solicitud puede ser aprobada concurrentemente por distintos responsables.

Cuando el sistema detecta versiones conflictivas de una aprobación, conserva aquella emitida por el responsable con mayor nivel de autoridad dentro de la organización. Si existen varias aprobaciones emitidas por responsables con el mismo nivel de autoridad, se mantiene aquella asociada al mayor monto aprobado. En caso de persistir más de una alternativa posible, se selecciona la última aprobación registrada.

¿Qué estrategia de **resolución de conflictos describe mejor** el comportamiento del sistema?

A) Se utiliza únicamente *Last Write Wins*.

B) Se utiliza únicamente *Merge* Semántico.

C) Primero se aplica *Merge* Semántico y luego *Last Write Wins*.

D) Primero se generan Versiones y luego un *Operational Transformation*.

E) Primero se aplica *Last Write Wins* y luego *Merge* Semántico.

24. Una empresa está evaluando distintas arquitecturas para un sistema distribuido global. Durante una discusión técnica surge una analogía entre la elección de TCP o UDP y el *trade-off* que PACELC plantea cuando no existen particiones de red.

    ¿Cuál de las siguientes afirmaciones describe **mejor dicha analogía**?

    A) TCP y UDP representan respectivamente las categorías EC y EL de PACELC, por lo que elegir uno determina automáticamente el comportamiento del sistema distribuido.

    B) TCP suele favorecer menores tiempos de respuesta mientras que UDP suele favorecer mayores garantías de entrega; de forma análoga, PACELC contrapone consistencia y latencia.

    C) La analogía es incorrecta porque PACELC estudia sistemas distribuidos y TCP/UDP pertenecen a una capa distinta, por lo que no existe ninguna relación conceptual entre ambos.

    D) TCP incorpora mecanismos que privilegian la confiabilidad de la comunicación a costa de sobrecarga adicional, mientras que UDP reduce dichas garantías para disminuir costos de comunicación; de manera similar, PACELC contrapone consistencia y latencia como un *trade-off*.

    E) Ninguna de las anteriores.

25. Una plataforma de coordinación distribuida mantiene la información replicada en 20 nodos ubicados en distintos centros de datos. Las escrituras se realizan mediante un protocolo de consenso basado en quórum: una actualización solo se considera confirmada cuando la mayoría de los nodos la registra de forma persistente en su *log*.

    Para optimizar las lecturas, estas se atienden exclusivamente a través de un solo nodo que ejerce el rol de líder, elegido mediante el algoritmo de Raft. Al recibir una solicitud de lectura, el líder ejecuta un mecanismo de verificación de liderazgo según las reglas de Raft para confirmar que la mayoría de los nodos sigue reconociéndolo como tal. Si esta verificación falla, el líder cede su rol y no responde la solicitud. Si la verificación es exitosa, responde utilizando el estado de su log ya consolidado, sin contactar a las demás réplicas para validar la información que enviará.

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

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

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

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

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

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

26. Respecto a los modelos de consistencia en sistemas distribuidos, ¿cuál de las siguientes afirmaciones es **correcta**?

    A) La consistencia centrada en el cliente busca que todos los clientes conectados en un mismo momento observen el mismo estado de los datos, aunque entre distintas sesiones puedan existir inconsistencias.

    B) La consistencia centrada en los datos busca que todas las bases de datos mantengan exactamente los mismos datos en todo momento.

    C) La consistencia centrada en el cliente busca mantener una experiencia coherente para cada cliente, aunque distintos clientes puedan observar estados diferentes de los datos.

    D) La consistencia centrada en los datos y la consistencia centrada en el cliente garantizan las mismas propiedades, pero utilizando protocolos distintos.

    E) La consistencia centrada en el cliente solo puede aplicarse cuando existe una única réplica de los datos.

27. Su profesor estaba procrastinando por *Instagram* desde su celular cuando observa que el influencer Cristian Ruz ha publicado una nueva historia. El profesor la visualiza, le da "like" y continúa revisando otras historias. Horas más tarde, al llegar a su casa, accede a *Instagram* desde su computador. La plataforma le indica nuevamente que existe una nueva historia de Cristian Ruz. Al abrirla esperando encontrar contenido nuevo, descubre que se trata de la misma historia que ya había visto anteriormente y, además, el "like" que había realizado ya no aparece.

    Con respecto a las garantías de consistencia centrada en el cliente, ¿Cuál de las siguientes afirmaciones es **correcta**?

    I. Se vulnera la garantía *Read Your Writes*.

    II. Se vulnera la garantía *Monotonic Reads*.

    III. Se vulnera la garantía *Monotonic Writes*.

    A) Solo I.

    B) Solo II.

    C) Solo III.

    D) I y II.

    E) I, II y III.

28. Una empresa opera un sistema distribuido que registra detalladamente todas las acciones realizadas por sus usuarios. Debido al alto costo monetario de almacenar los *logs*, el equipo propone eliminar el sistema de monitoreo y sus *logs*. Para compensar esta decisión y garantizar todavía la seguridad, se incorporan protocolos de cifrado en todas las comunicaciones y autenticación de 2 pasos para los usuarios.

    Considerando los *trade-off* vistos en clases, ¿cuál de las siguientes afirmaciones describe **correctamente** esta propuesta?

    A) La propuesta mejora el rendimiento del sistema, pero a costa de su usabilidad.

    B) La propuesta mejora la usabilidad del sistema, pero a costa de su rendimiento.

    C) La propuesta mejora simultáneamente la privacidad, el rendimiento y la usabilidad del sistema.

    D) La propuesta mejora la seguridad sin generar efectos sobre otras propiedades del sistema.

    E) La propuesta mejora la privacidad de los usuarios, pero puede afectar negativamente el rendimiento y la usabilidad del sistema.

29. ¿Cuáles de las siguientes afirmaciones son **correctas** sobre firmas digitales?

    I. La función *hash* utilizada en una firma digital garantiza la confidencialidad del documento firmado.

    II. Incorporar una función *hash* en el proceso de firma digital no garantiza el no-repudio del documento.

    III. Incorporar una función *hash* en una firma digital basada en criptografía asimétrica mejora la eficiencia del proceso de firma.

    A) Solo I.

    B) Solo II.

    C) Solo III.

    D) I y II.

    E) II y III.

30. Durante el establecimiento de una sesión segura en TLS 1.3, ¿**cuándo** se utiliza criptografía simétrica?

    A) Luego de acordar una clave de sesión mediante criptografía asimétrica.

    B) Solo en la verificación del certificado del servidor.

    C) Desde que se intercambian los “Hello”, antes de cualquier autenticación.

    D) Solo si el cliente no puede validar la llave pública del servidor.

    E) Nunca, TLS es completamente asimétrico.

31. ¿Cuál de las siguientes acciones **compromete** el objetivo principal de una Infraestructura de Clave Pública (PKI)?

    A) Recurrir a criptografía asimétrica con la Autoridad Certificadora.

    B) Mantener la llave pública del servidor separada del certificado digital para facilitar su actualización.

    C) Firmar el certificado del Servidor con la llave privada de la Autoridad Certificadora.

    D) Verificar que la Autoridad Certificadora sea confiable.

    E) Incluir la llave pública del servidor dentro del certificado antes que la Autoridad Certificadora lo procese.

32. Una empresa ofrece diversos servicios de uso de IA como corrección de texto, crear videos, editar imágenes, etc. Cada servicio está en un servidor distinto, y para facilitar el sistema de autenticación, deciden utilizar un sistema Kerberos. Suponga que un día, un atacante logra comprometer completamente el *Ticket Granting Server* (TGS) sin que la empresa se percate. ¿Cuál de los siguientes escenarios **podría ocurrir**?

    A) El atacante podría obtener las llaves secretas (criptografía simétrica) de todos los usuarios registrados en la empresa.

    B) Los usuarios ya no podrán autenticarse ante el servidor de Autenticación.

    C) El atacante podría cambiar las contraseñas de cualquier usuario registrado en la empresa.

    D) El atacante podría generar *tickets* válidos para acceder a cualquiera de los servicios de IA de la empresa.

    E) Los servicios de IA dejarían de aceptar *tickets* emitidos por Kerberos.

33. Una empresa opera una plataforma distribuida compuesta por decenas de micro-servicios. Tras sufrir un incidente de seguridad originado por una cuenta interna comprometida, decide implementar una política de seguridad *Zero Trust*. ¿En qué **consiste** principalmente esta política?

    A) Verificar la identidad y permisos de usuarios, dispositivos y servicios ante cada solicitud realizada al sistema.

    B) Confiar en cualquier usuario o servicio que haya superado previamente un proceso de autenticación de múltiples factores.

    C) Permitir el acceso a los recursos internos únicamente desde dispositivos conectados a la red corporativa.

    D) Aumentar el nivel de monitoreo para rastrear cada acción realizada por los usuarios, independientemente de sus privilegios.

    E) Exigir el uso de un sistema centralizado de autenticación para todos los microservicios.

34. Respecto a IDS, IPS y *firewalls*, ¿cuál de las siguientes alternativas es **correcta**?

    A) Los IDS pueden ser a nivel de red o de *host*, pero los IPS solo operan a nivel de red.

    B) Un *firewall* y un IPS de red no pueden coexistir en una misma arquitectura porque realizan exactamente la misma función.

    C) El *firewall* tiene potencial para revisar el contenido de los mensajes.

    D) La diferencia entre IDS e IPS es que el primero detecta intrusos mediante los metadatos del mensaje y el segundo los detecta mediante patrones en su comportamiento.

    E) Ninguna de las anteriores.

35. ¿Cuál de las siguientes alternativas corresponde a un **ataque *Sybil*** en redes *Peer-to-Peer*?

    A) Un atacante envía múltiples consultas válidas desde distintos nodos para incrementar la carga del sistema sin alterar su topología.

    B) Un atacante controla directamente un conjunto de nodos dentro de la red y los utiliza para establecer conexiones selectivas que aíslan a un nodo víctima del resto de la red.

    C) Un atacante replica datos en múltiples nodos sin autorización, con el objetivo de mantenerlos disponibles incluso si la red intenta eliminarlos.

    D) Un atacante participa en la red reenviando mensajes de forma estratégica y redundante para aumentar artificialmente su presencia en la propagación de información y obtener mayor influencia en la red.

    E) Un atacante introduce una gran cantidad de identidades falsas en la red con el objetivo de aumentar su influencia y control sobre el sistema.

36. En un sistema peer-to-peer, antes de que un nodo pueda participar activamente en la red debe demostrar esfuerzo computacional resolviendo un problema difícil, lo que limita el ingreso de participantes de forma simple. Además, la información que circula entre nodos no se acepta de inmediato, sino que es contrastada con múltiples nodos independientes para detectar inconsistencias antes de ser incorporada.

    Con estas medidas, ¿qué ataques se ven **mitigados** de forma más directa?

    A) Solo *Eclipse*.

    B) Solo *Poisoning*.

    C) Solo *Free Riding*.

    D) *Free Riding* y *Poisoning*.

    E) *Eclipse* y *Poisoning*.

37. Según lo visto en clases ¿Cuál de las siguientes alternativas **NO es una característica** de utilizar *Distributed Hash Table* (DHT) en sistemas *Peer-to-Peer* estructurados?

    A) Requieren que cada nodo tenga conocimiento de todos los demás nodos para poder enrutar consultas correctamente.

    B) Los nodos no pueden elegir qué datos son asignados bajo su responsabilidad.

    C) Permiten que la red mantenga el servicio de búsqueda incluso ante la entrada y salida frecuente de nodos.

    D) Aumenta el costo de realizar comportamientos maliciosos dentro de la red.

    E) Es difícil secuestrar rutas sin alterar una gran cantidad de nodos en la estructura de enrutamiento.

Pregunta bonus

Con el fin de que la última pregunta de contenidos no quede solita en esta hoja, a continuación se presentan 2 preguntas *bonus*: la 38 y 39. Tener al menos 1 correcta otorga 1 décima más a la nota final del examen. En caso de tener ambas correctas, se otorgará solo 1 décima a la nota del examen.

38. ¿Cuál de los siguientes animes **apareció** en más PPTs del curso?

    A) Spy x Family.

    B) Boku no Hero Academia.

    C) Chō Kaguya-hime!

    D) Detective Conan.

    E) Sword Art Online.

39. ¿Qué día es el **cumpleaños** de Conan Edogawa (protagonista de Detective Conan)?

    A) 1 de enero.

    B) 14 de febrero.

    C) 4 de mayo.

    D) 18 de septiembre.

    E) 3 de octubre.