

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

Examen (2025-2)

Lunes 01 de Diciembre 2025

Instrucciones

- La evaluación consta de 35 preguntas de alternativas. Para obtener el 7.0 en la evaluación, se deben tener 34 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 30 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 30 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. ¿Cuál de las siguientes situaciones **representa** un ***pitfall* de diseño** dentro de los problemas clásicos de los sistemas distribuidos?

   A) La red se satura y los mensajes comienzan a demorar más de lo esperado.

   B) Una falla momentánea causada por la caída de un servidor.

   C) Un proceso intenta acceder a un recurso compartido que otro proceso ya está usando.

   D) Se asume que la red es segura, rápida y siempre confiable.

   E) Los relojes de los distintos nodos se desincronizan y causan inconsistencias.

2. En relación con los procesos y los *threads*, ¿cuál de las siguientes afirmaciones es **correcta**?

   A) Los *threads* siempre son más eficientes que los procesos porque se ejecutan en paralelo.

   B) Los procesos acceden directamente al disco duro, mientras que los *threads* necesitan un intermediario para hacerlo.

   C) Los *threads* son más livianos de crear, ya que comparten el mismo espacio de memoria del proceso al que pertenecen.

   D) Si un *thread* falla, el error solo afecta a ese *thread* y no al proceso ni a los demás *threads*.

   E) Tanto los procesos como los *threads* deben definir mecanismos de comunicación para poder compartir información entre ellos.

3. ¿Cuál de las siguientes acciones **NO corresponde** a un objetivo principal de los sistemas distribuidos?

   A) Permitir el acceso remoto a los archivos sin importar su ubicación o sistema operativo.

   B) Evitar el acoplamiento de los diversos componentes del sistema distribuido.

   C) Asegurar que las operaciones puedan ejecutarse con éxito incluso ante fallos parciales.

   D) Garantizar un correcto funcionamiento a medida que crece el sistema en número de usuarios.

   E) Mantener múltiples copias sincronizadas de todos los datos en cada máquina del sistema.

4. ¿Cuál de las siguientes afirmaciones es **correcta** sobre el protocolo DNS?

   A) Se apoya en múltiples servidores que colaboran de forma jerárquica y con responsabilidades distintas en la búsqueda de la IP.

   B) Los DNS *resolver* son quienes almacenan las IPs de todos las URL existentes.

   C) El cliente siempre tendrá que hablar con el DNS *resolver* para conseguir la IP de un sitio.

   D) Se construye la IP de destino de forma dinámica a medida que lee fragmentos de la URL.

   E) Para garantizar que la IP llegue de forma íntegra, siempre se recurre al protocolo TCP.

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

   I. *Remote Procedure Call* es, por defecto, un paradigma de comunicación síncrono y acoplado temporalmente.

   II. La comunicación directa, como la que utiliza *sockets*, requiere que el emisor conozca la dirección e identidad del receptor, lo que implica acoplamiento referencial.

   III. Tanto la comunicación *Rest* como RPC se caracterizan por ser *Stateless*, es decir, no conservan información entre solicitudes.

   A) Solo I.

   B) Solo II.

   C) Solo III.

   D) I y II.

   E) II y III.

6. Asumiendo que los *delays* de red entre nodos son constantes y tan bajos que pueden considerarse despreciables, ¿en cuál de las siguientes situaciones el nodo A quedará **más cercano a la hora UTC** después de sincronizarse?

   A) El nodo A está muy alejado de UTC y aplica el método de Cristian con un nodo que se sincronizó recientemente mediante NTP con un servidor de estrato 0.

   B) El nodo A está muy alejado de UTC y aplica el método de Cristian con un nodo que se sincronizó recientemente mediante NTP con un servidor de estrato 1.

   C) El nodo A está sincronizado a UTC y aplica el método de Cristian con un nodo que se sincronizó recientemente mediante NTP con un servidor de estrato 5.

   D) El nodo A está sincronizado a UTC y aplica el método de Cristian con un nodo que se sincronizó recientemente mediante NTP con un servidor de estrato 10.

   E) El nodo A está sincronizado a UTC y, como nodo líder, inicia el algoritmo de Berkeley con 10 nodos que tienen altas desviaciones respecto a UTC.

7. En el contexto de una red distribuida, donde los mensajes pueden estar en tránsito y los nodos no comparten un reloj global, ¿cuál de las siguientes afirmaciones refleja **correctamente** lo qué busca lograr el algoritmo de ***Chandy–Lamport***?

   A) Sincronizar la ejecución de todos los nodos para que capturen su estado exactamente al mismo tiempo físico.

   B) Reemplazar la necesidad de coordinar relojes mediante un mecanismo alternativo de seguimiento causal.

   C) Coordinar una pausa en el envío de mensajes entre nodos para poder hacer una copia de la base de datos de cada nodo.

   D) Resolver el problema de consenso ante valores propuestos por distintos nodos.

   E) Obtener una vista global del sistema que pueda construirse aun cuando existan mensajes viajando entre los nodos.

8. 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'`.

   Las respuestas recibidas son:

   - Un aceptante ya había aceptado `(7, 'Puré de manzana')`.
   - Otro aceptante ya había aceptado `(8, 'Pavo')`.
   - 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, 'Pavo')`.

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

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

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

9. ¿Cuál de los siguientes escenarios **NO corresponde** a un comportamiento bizantino?

   A) En Raft, existiendo un líder activo, un nodo que no es líder recibe una petición del cliente y la ignora porque este nodo no es el líder actual.

   B) En *Ring-based Election*, el nodo solo re-envía mensajes de nodos cuyo ID sea menor al suyo.

   C) En Paxos, un proponente reemplaza el valor previamente aceptado por uno nuevo asociado a una propuesta con un ID mayor.

   D) En una red con cuatro nodos activos, se ejecuta el algoritmo *Bully* y el proceso con el ID más bajo se autoproclama líder.

   E) En *multicast* de Exclusión Mutua, un proceso ingresa a la sección crítica tras recibir permisos de la mayoría, sin esperar las respuestas de todos los nodos.

10. Considerando un sistemas distribuido donde tenemos varios nodos interactuando con una base de datos en común, ¿Cuál de las siguientes alternativas es **correcta** a los conceptos *Deadlock* y *Livelock*?

    A) *Livelock* se refiere al estado donde un nodo bloquea de forma permanentemente un registro o tabla de la base de datos, mientras que *Deadlock* se refiere al estado donde los demás nodos quedan bloqueados al intentar acceder a un recurso ya bloqueado previamente.

    B) La diferencia principal del nombre es la cantidad de nodos involucrados: *Livelock* ocurre solo con 1 o 2 nodos, mientras que *Deadlock* requiere necesariamente más de 2 nodos intentando acceder a los mismos datos.

    C) *Livelock* describe el caso donde dos nodos no pueden enviar mensajes entre ellos, mientras que *Deadlock* describe cuando los *threads* de cada nodo no pueden ejecutar ninguna acción.

    D) Ambos conceptos se refieren al problema donde los nodos del sistema, actuando simultáneamente, no pueden finalizar su operación sobre la base de datos.

    E) *Deadlock* es un problema exclusivo de *threads* en un nodo, mientras que *Livelock* es un problema exclusivo de la comunicación entre nodos de un sistema distribuido.

11. Un sistema distribuido con forma de anillo está compuesto por 6 nodos conectados en el orden $A \rightarrow B \rightarrow C \rightarrow D \rightarrow E \rightarrow F \rightarrow A$, donde los identificadores (IDs) de los nodos son: A(4), B(6), C(8), D(1), E(4), F(7), se utiliza el algoritmo de elección de líder basado en anillo (*ring-based election algorithm*). Si el nodo D da inicio al proceso de elección, ¿**cuántos mensajes** se enviarán en total desde que el nodo D empieza el proceso hasta que el algoritmo finalice completamente?

    A) 12.

    B) 14.

    C) 17.

    D) 18.

    E) 19.

12. Respecto a los algoritmos de exclusión mutua, ¿cuál de las siguientes afirmaciones es **incorrecta**?

    A) En *Token Ring*, cada nodo solo necesita conocer a sus nodos vecinos para poder participar en el algoritmo.

    B) En el algoritmo de Servidor Central, hay situaciones donde el servidor da permiso a un nodo sin esperar que el que tenía acceso al recurso crítico indique que lo liberó.

    C) El algoritmo de Servidor Central exige siempre que cada nodo conozca a todos los demás nodos para funcionar correctamente.

    D) En *Token Ring*, si un nodo no necesita la sección crítica, debe reenviar inmediatamente el *token* a su siguiente vecino.

    E) En *Multicast* de Ricart & Agrawala, un nodo manda un mensaje a todos los demás nodos para pedir permiso.

13. Una empresa multinacional busca garantizar que su servicio distribuido de correo electrónico continúe operativo incluso frente a fallas de *hardware*, errores de red o caídas parciales de servidores. El diseño debe priorizar la continuidad del servicio por sobre la eficiencia de recursos.

    ¿Cuál de las siguientes estrategias permite lograr **correctamente** dicho objetivo?

    A) Utilizar un sistema centralizado, pero con varios nodos de respaldo ante fallas.

    B) Incorporar mecanismos de redundancia para el procesamiento de consultas.

    C) Implementar *timeouts* adaptativos para detectar retrasos o caídas de nodos lo más rápido posible.

    D) Sincronizar constantemente los relojes entre procesos para evitar inconsistencias temporales en los mensajes.

    E) Restringir el número de nodos en el sistema para minimizar la probabilidad de errores.

14. ¿Cuál afirmación es **correcta** sobre el Teorema de Imposibilidad de Fischer, Lynch y Paterson (FLP) en el contexto de los sistemas distribuidos?

    A) Justifica que es imposible alcanzar consenso si la red tiene retardos variables entre los mensajes.

    B) Demuestra que es imposible lograr consenso sin designar un "dictador" que decida por todos.

    C) Los autores de este teorema fueron nominados al premio Dijkstra en 2001, pero no lo recibieron.

    D) Sostiene que si los algoritmos no utilizan quórum, es imposible garantizar consenso.

    E) Indica que en un sistema asíncrono, no se puede garantizar el consenso si algún nodo puede fallar.

15. 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". Tras la publicación, cada servidor envía notificaciones a los demás, 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 dan evidencia que **la consistencia secuencial se romperá**?

    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) Ninguno de los escenarios entrega evidencia de que se romperá la consistencia secuencial.

16. 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”. Tras la publicación, cada servidor envía notificaciones a los demás, aunque la entrega de estas notificaciones puede experimentar distintos retrasos entre pares de servidores.

    Considerando que los servidores respetan la consistencia causal ¿cuál de los siguientes escenarios dan evidencia que la **consistencia causal se romperá**?

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

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

    C) 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.

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

    E) Ninguno de los escenarios entrega evidencia de que se romperá la consistencia causal.

17. La empresa CambiosSeguros Ltda. permite a los usuarios comprar y vender diferentes tipos de monedas (dólares, yenes, euros, etc.) de forma remota. Para esto, poseen más de 30 servidores distribuidos globalmente con la información del valor de cada moneda, la cual se actualiza a medida que los usuarios realizan transacciones. Todos estos servidores pueden ser utilizados por los clientes tanto para consultar valores como para procesar operaciones de compra/venta.

    Para que el sistema funcione correctamente, se necesita un protocolo de replicación que asegure que los usuarios —aunque con mayor latencia— siempre vean el valor de cada moneda actualizado inmediatamente después de cada operación de compra o venta, sin importar desde qué servidor accedan.

    ¿Qué protocolo de replicación sería el **apropiado** para CambiosSeguros Ltda.?

    A) *Primary-Based Protocols*.

    B) *Replicated-Write Protocols*.

    C) *Quorum-Based*.

    D) *Gossip Protocols*.

    E) Ninguno de las anteriores.

18. La *startup* GlobalRide implementó un sistema de reservas de vehículos con varias réplicas de su base de datos distribuidas en diferentes regiones. Para mejorar el rendimiento, las transacciones de reserva se enrutan a distintas réplicas según la cercanía del usuario, pero el equipo de ingeniería le asegura al negocio que el sistema, aunque es distribuido, estará restringido ante la propiedad de *one-copy serializability*.

    En términos del comportamiento observable del sistema, ¿qué significa que se **satisfaga dicha propiedad**?

    A) Que solo la base de datos de un único servidor puede ser serializada, para luego ser compartida con los demás servidores.

    B) Que el sistema de reservas se comportará como si existiera una única base de datos con todas las reservas.

    C) Que todas las reservas que puedan tener conflicto serán siempre procesadas en la misma réplica para mantener la consistencia.

    D) Que cada réplica pueda aplicar las reservas en órdenes distintos siempre que se ejecute una o ninguna.

    E) Que se garantiza que al menos una réplica tendrá el resultado correcto de todas las reservas procesadas de forma secuencial.

19. ¿Cuál de las alternativas es **correcta** respecto a lo expuesto en la siguiente frase sobre validación *forward* y *backward*?

    "*Bajo un esquema de validación forward, no se recomienda abortar las transacciones con conflicto, pero bajo un esquema de validación backward sí se recomienda.*"

    A) Es incorrecta, porque ambos tipos de validación requieren abortar de inmediato cualquier transacción que presente conflicto en la validación.

    B) Es incorrecta, porque en *backward* tampoco se recomienda abortar las transacciones.

    C) Es correcta, porque en *forward* se permite el conflicto mientras pueda resolverse más adelante. En cambio, en *backward* no se acepta ningún conflicto.

    D) Es incorrecta, porque la afirmación está invertida: en *backward* se recomienda no abortar ante un conflicto, y en *forward* sí se recomienda abortar.

    E) Es correcta, porque en *forward* todavía existe la posibilidad de que una transacción con conflicto deje de tenerlo más adelante, mientras que en *backward*, una vez surge el conflicto, este se mantendrá siempre.

20. Un equipo de trabajo utiliza una pizarra digital en línea donde varios usuarios pueden añadir, mover o modificar notas simultáneamente. El sistema debe garantizar que todos los cambios concurrentes se integren correctamente, de manera que al final todos los usuarios vean la misma pizarra, sin importar el orden en que se realizaron los cambios y sin intervención manual.

    ¿Cuál de las siguientes estrategias sería la más **adecuada** para evitar conflicto y respetar las condiciones del sistema?

    A) *Last Write Wins*.

    B) *Operational Transformation*.

    C) *Merge* manual.

    D) Versiones.

    E) Ninguna de las anteriores.

21. Un hospital utiliza un sistema digital para registrar continuamente el estado de los pacientes. Enfermeras y sensores registran distintos tipos de información (signos vitales, medicación administrada, observaciones clínicas, entre otros) en el registro del paciente. La cantidad de información generada es tan alta que el sistema está limitado a guardar un único registro por paciente con toda su información. Además, el sistema debe estar disponible en todo momento, incluso cuando no hay personal supervisando los datos, y cualquier pérdida o combinación incorrecta de información podría afectar seriamente la atención de los pacientes.

    El problema surge cuando varias enfermeras o sensores actualicen información del paciente simultáneamente. ¿Cuál de las siguientes estrategias sería la más **adecuada** para evitar conflicto y respetar las condiciones del sistema?

    A) Aplicar *Last Write Wins*.

    B) Utilizar *Merge* manual.

    C) Utilizar versionamiento.

    D) Aplicar control pesimista.

    E) Ninguna de las anteriores.

22. Una base de datos distribuida opera con dos centros de datos: uno en São Paulo y otro en Frankfurt. Durante una caída de red entre ambos, las escrituras en São Paulo se bloquean hasta restablecer la conexión. En condiciones normales, cada escritura se considera completada solo cuando ambos centros confirman la actualización, lo que provoca demoras visibles en las aplicaciones que hacen muchas escrituras simultáneas.

    Según el teorema PACELC, ¿qué tipo de sistema **describe** este comportamiento?

    A) Prefiere disponibilidad en partición y baja latencia en condiciones normales (PA/EL).

    B) Prefiere consistencia en partición y baja latencia en condiciones normales (PC/EL).

    C) Prefiere disponibilidad en partición y consistencia en condiciones normales (PA/EC).

    D) Prefiere consistencia en partición y consistencia en condiciones normales (PC/EC).

    E) No se aplica el teorema PACELC porque no se producen particiones reales.

23. Respecto a los teoremas CAP y PACELC en sistemas distribuidos, ¿Cuáles de las siguientes afirmaciones es **correcta**?

    A) Según CAP, un sistema distribuido debe garantizar Consistencia y Disponibilidad cuando existen Particiones de Red.

    B) PACELC introduce una clasificación más completa que CAP.

    C) Según PACELC, solo ante ausencia de particiones se debe elegir entre dos propiedades.

    D) CAP y PACELC son modelos excluyentes: un sistema que sigue PACELC no está sujeto a las limitaciones de CAP.

    E) Según CAP, un sistema distribuido puede garantizar simultáneamente Consistencia, Disponibilidad y Tolerancia a particiones si está bien diseñado.

24. 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 100 horas de *League of Legend*". Mientras la lee, nota que el contador de comentarios marca 128 y que entre ellos hay uno muy reciente de su amigo "Okarun", quien escribió: "100 horas ¿tan poco?"

    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 "Okarun" no aparece. Sorprendida, piensa que quizás "Okarun" lo borró, pero cuando vuelve a recargar la página en el computador, el comentario sigue allí. Cuando le pregunta a "Okarun" 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.

    ¿Cuál es la propiedad principal de las consistencias centradas en el cliente **NO se está cumpliendo** con la evidencia presentada para la usuario "Momo"?

    A) *Writes follow reads*.

    B) *Monotonic writes*.

    C) *Monotonic reads*.

    D) *Read your writes*.

    E) Ninguna de las anteriores.

25. El profesor accedió a *Outlook* para revisar su correo de la UC desde su celular y eliminó varios mensajes de SPAM. Al instante, comprobó que los mensajes desaparecieron de su bandeja del celular. Más tarde, se conecta desde su computadora y nota que los mensajes de SPAM que eliminó desde el celular todavía aparecen.

    Considerando este escenario, ¿cuáles de las siguientes propiedades de consistencia centrada en el cliente **NO se cumplen** con la evidencia presentada?

    I. *Monotonic Reads*

    II. *Read Your Writes*

    III. *Monotonic Writes*

    IV. *Writes Follow Reads*

    A) Solo I y II.

    B) Solo II y IV.

    C) Solo III y IV.

    D) Solo I, II y IV.

    E) Solo I, II y III.

26. ¿Cuál es uno de los **problemas** o limitaciones del protocolo Diffie–Hellman?

    A) Requiere generar muchas llaves para cifrar mensajes de gran volumen.

    B) Requiere que las partes compartan previamente sus llaves privadas de manera segura.

    C) No puede usarse junto con criptografía simétrica.

    D) Es vulnerable a ataques de tipo *Man in the Middle* si no se autentican las partes.

    E) Solo puede aplicarse en canales seguros.

27. En el cifrado simétrico, ¿cuál es el principal **desafío** que debe resolverse para que la comunicación sea segura?

    A) La velocidad de cifrado suele ser muy lenta.

    B) La clave privada debe ser almacenada en un servidor central.

    C) La distribución inicial de la clave secreta de forma segura.

    D) No se puede utilizar para grandes volúmenes de datos.

    E) La clave pública puede ser interceptada por un atacante.

28. ¿Qué característica describe **correctamente** a los protocolos híbridos como TLS?

    A) Utiliza únicamente cifrado simétrico para todo el proceso de comunicación.

    B) La clave de sesión se transmite en texto claro porque solo se usa una vez.

    C) Utilizan cifrado asimétrico para intercambiar una clave simétrica segura.

    D) Evitan el uso de claves de sesión efímeras.

    E) No permiten autenticación del servidor.

29. Respecto al establecimiento y uso de un canal seguro, ¿cuál de las siguientes afirmaciones son **correctas**?

    I. Un canal seguro puede prevenir ataques de *replay*.

    II. Durante el *handshake*, las partes intercambian claves públicas con el fin de usar cifrado asimétrico durante toda la comunicación.

    III. En el proceso de establecimiento, las partes negocian y acuerdan los algoritmos criptográficos que utilizarán durante la sesión.

    A) Solo III.

    B) I y II.

    C) I y III.

    D) II y III.

    E) I, II y III.

30. Una empresa desea minimizar la exposición de las contraseñas del usuario por la red y reducir la carga de almacenar llaves secretas, por usuario, en cada servicio distinto que tienen. ¿Qué mecanismo **resuelve** estas necesidades?

    A) Utilizar un sistema de autenticación de *tickets* temporales como Kerberos.

    B) Utilizar autenticación basada en contraseña hasheada para cada servicio.

    C) Que cada servicio genere un certificado mediante la Infraestructura de Clave Pública.

    D) Autenticarse con un protocolo de *Challenge response* con llave simétrica en cada servicio.

    E) Ninguna de las anteriores.

31. La universidad ha desplegado un sistema *anomaly-based IPS* para proteger sus servicios académicos y redes internas. Este sistema ha sido correctamente configurado para soportar una red distribuida de alto tráfico y diversos tipos de usuarios (académicos, estudiantes, administrativos, etc.). ¿Cuál de los siguientes escenarios representa un **riesgo inherente** al uso de este IPS para la universidad?

    A) Se detecta un ataque DDoS junto con las direcciones IP responsables, y el IPS notifica al administrador, pero por definición, no puede bloquear ninguna acción automáticamente.

    B) Un estudiante recarga muchas veces la página de inscripción de cursos y el IPS lo bloquea por considerar su comportamiento sospechoso.

    C) Un estudiante logra cambiar la frecuencia de generación de *logs* del IPS de 10 segundos a 1 segundo, lo que eventualmente satura el almacenamiento del servidor de monitoreo.

    D) El IPS comienza a cambiar los permisos sobre información personal de los estudiantes, permitiendo que cualquiera pueda ver las notas de otro alumno.

    E) Un estudiante intenta ingresar un virus al sistema mediante un correo electrónico, y el IPS detecta y bloquea dicho mensaje.

32. Osiris lanzará en 2026 el nuevo juego de carreras de caballo “Uma Musume Re:Dive”, el cual incorporará una arquitectura distribuida con servidores y servicios totalmente nuevos respecto a otros juegos de carrera. Para jugar este nuevo lanzamiento, se implementó OAuth 2.1 como mecanismo que permitirá a los usuarios iniciar sesión utilizando sus cuentas de un antiguo juego llamado “Uma Musume”.

    Para monitorear esta nueva infraestructura desde el primer día, el equipo de seguridad desea implementar mecanismos que permitan detectar comportamientos maliciosos. Para esto, se consideran los siguientes tipos de análisis:

    I. Análisis basado en reglas.

    II. Análisis basado en firmas.

    III. Análisis basado en Inteligencia Artificial.

    ¿Cuáles de estos tipos de análisis estaría **correctamente justificado** para usar inmediatamente en este escenario?

    A) Solo I.

    B) Solo II.

    C) Solo III.

    D) I y II.

    E) I, II y III.

33. ¿Cuál de las siguientes opciones representa una **ventaja clave** de utilizar una *Distributed Hash Table* en redes *Peer to Peer*?

    A) Impide que un atacante pueda insertar nodos maliciosos en la red.

    B) Los nodos pueden elegir libremente qué vecinos tendrán en vez de depender de criterios geográficos.

    C) Evita por completo la redistribución de datos cuando los nodos entran o salen de la red.

    D) Garantiza que todos los nodos almacenen la misma cantidad de datos.

    E) Permite localizar elementos en un número reducido de saltos.

34. ¿Cuál de las siguientes afirmaciones es **incorrecta** respecto a *BitTorrent*?

    A) Para garantizar la integridad de los datos, *Bittorrent* prioriza descargar los datos de nodos que tengan el archivo completo antes de nodos con fragmentos del archivo.

    B) En sus inicios utilizaba una red *peer to peer* no estructurada con ciertos elementos de coordinación centralizada.

    C) Actualmente presenta una arquitectura híbrida, con aspectos centralizados y elementos de una arquitectura *peer to peer* estructurada.

    D) Incluye incentivos para regular el intercambio de datos y no define un canal cifrado seguro por defecto para proteger las comunicaciones.

    E) El acoplamiento utilizado en esta red es del tipo temporal y referencial.

35. Eres un estudiante de la UC de Chile que está de viaje en Japón y te conectas al Eduroam de la Universidad de Nagoya. Quieres buscar información sobre una película recién estrenada en Corea, pero cuya búsqueda o reproducción está prohibida en Japón. Dado esto, evalúas conectarte a la red Tor desde Eduroam hacia un sitio con cifrado seguro para buscar información sobre el estreno.

    En este escenario, ¿cuál de las siguientes afirmaciones describe **correctamente** un posible escenario por usar estas tecnologías mencionadas?

    A) Dependerás de que la Universidad de Nagoya permita el tráfico por Tor, pero no podrá conocer el contenido de tu búsqueda.

    B) Usando o no Tor, la UC sabrá que buscaste sobre dicha película, pero Japón no tiene forma de enterarse.

    C) Si añades un VPN antes de ingresar a la red Tor, tanto la Universidad de Nagoya como el servidor de VPN no podrán ver a dónde estás accediendo.

    D) Si quieres añadir VPN, deberás excluir la opción de Tor porque estos sistemas no son compatibles para usarse en conjunto.

    E) Necesitas autorización de la UC y de la Universidad de Nagoya para poder navegar por este tipo de tráfico.