UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



Proyecto de Curso — Unidad II

“Prototipo de redundancia web IIS y servicios AD DS/DNS en VirtualBox”

Que se presenta para el curso:

“Sistemas Operativos I”

INTEGRANTES:

Atencio Vargas, Emanuel (2024079964)

Cortez Mamani, Julio Samuel (2023077283)

Llampazo Chiroque, Camilo (2024079785)

Neciosup Vargas, Ariana (2024080126)

DOCENTE:

Mtro. Renzo Alberto Taco Coayla

TACNA – PERÚ

2026

Índice General

1 Resumen Ejecutivo **4**

2 Planteamiento del Problema **4**

2.1 Situación Actual 4

2.2 Necesidad Identificada 5

2.3 Justificación de la Propuesta 5

2.4 Evidencia Bibliográfica y Decisiones de Diseño 6

3 Objetivos **8**

3.1 Objetivo General 8

3.2 Objetivos Específicos 8

4 Requerimientos **8**

4.1 Requerimientos Funcionales 9

4.2 Requerimientos No Funcionales 9

5 Diseño de la Arquitectura **9**

5.1 Arquitectura Lógica 9

5.2 Arquitectura Física 10

5.3 Componentes Principales 11

5.4 Flujo de Información 11

5.5 Análisis de Modos de Fallo 12

6 Diseño de Infraestructura **13**

6.1 Servidores y Equipos 13

6.2 Sistemas Operativos 13

6.3 Almacenamiento 14

6.4 Virtualización 14

6.5 Servicios Requeridos 14

7 Diseño de Red **16**

7.1 Topología 16

7.2 Segmentación y VLAN 17

7.3 Direccionamiento IP 17

7.4 Firewall 18

7.5 Acceso Remoto 18

7.6 Comprobaciones de Conectividad 18

8 Diseño de Seguridad **20**

8.1 Riesgos Identificados 20

8.2 Amenazas 20
8.3 Controles Propuestos 20
8.4 Gestión de Accesos 21
8.5 Respaldo y Recuperación 21
8.6 Monitoreo y Auditoría 22
8.7 Matriz de Riesgos y Tratamiento 22
8.8 Método de Valoración y Correspondencia de Controles 23
9 Diseño Operativo 25
9.1 Roles y Responsabilidades 25
9.2 Procedimientos de Operación 25
9.3 Procedimientos de Mantenimiento 26
9.4 Gestión de Incidentes 26
10 Plan de Implementación 26
10.1 Actividades 26
10.2 Recursos Necesarios 27
10.3 Dependencias 27
10.4 Cronograma 27
11 Plan de Pruebas 28
11.1 Qué se Probará 28
11.2 Cómo se Probará 28
11.3 Resultado Esperado 29
11.4 Criterios de Aceptación 29
11.5 Casos Complementarios de Dominio y Anfitrión 29
11.6 Validación del Diseño y Evidencia Pendiente 29
12 Análisis de Factibilidad 31
12.1 Factibilidad Técnica 31
12.2 Factibilidad Económica 32
12.3 Factibilidad Operativa 33
13 Conclusiones 33
14 Referencias Bibliográficas 34

II UNIDAD
Diseño de la Solución Tecnológica

Objetivo:

Diseñar una solución tecnológica basada en los resultados obtenidos durante la investigación bibliográfica, definiendo la arquitectura, infraestructura, seguridad, operación e implementación de la propuesta.

---

1. Resumen Ejecutivo

El proyecto *Prototipo de redundancia web IIS y servicios AD DS/DNS en VirtualBox* propone diseñar un prototipo académico en Oracle VM VirtualBox para estudiar la continuidad de servicios ante fallos controlados. Como arquitectura inicial se plantean dos servidores web IIS, dos controladores de dominio con AD DS y DNS, y una máquina virtual dedicada a IIS con Application Request Routing (ARR) para distribuir tráfico. Esta selección se propone para mantener la administración dentro del entorno Windows y facilitar la configuración desde IIS Manager. La Unidad II comprende el diseño de la solución y la planificación de su implementación y validación en la Unidad III.

La evaluación prevista distinguirá la continuidad del servicio web de la disponibilidad de identidad y resolución de nombres. Se registrarán solicitudes fallidas y tiempos de detección y recuperación, sin anticipar resultados ni extrapolar disponibilidad anual. Las máquinas virtuales se distribuirán entre dos equipos físicos. La pérdida de una estación que aloje un nodo IIS y un controlador dejará sus pares en la otra estación, pero la continuidad web seguirá dependiendo del balanceador único y de la red compartida. La propuesta queda condicionada a la comprobación de conectividad, licenciamiento y restauración en la Unidad III.

2. Planteamiento del Problema

2.1. Situación Actual

El caso de estudio es el montaje de un laboratorio de Sistemas Operativos I en dos estaciones de trabajo de la Universidad Privada de Tacna. El equipo informa 32 GB de RAM y SSD de 512 GB por estación, conexión cableada, permisos administrativos, ISO de Windows Server 2022

y seis IP adicionales del rango local. Es información aportada por los integrantes, pendiente de contrastar con inventario y capturas. El problema de diseño es sostener la atención ante el fallo individual de un servidor virtual usando esos recursos, sin atribuir al sistema informático institucional una indisponibilidad que no se ha investigado.

La dependencia de un único nodo de atención web expone al servicio a interrupciones cuando ese nodo deja de responder. Pereira et al. (2023) estudian la distribución de solicitudes hacia servidores IIS mediante ARR y HAProxy como parte de una solución orientada a disponibilidad y rendimiento. Su trabajo aporta un antecedente para diseñar los ensayos del prototipo, sin trasladar sus resultados al entorno de este proyecto.

Se ha confirmado Oracle VM VirtualBox como plataforma para todas las máquinas virtuales. Se utilizará Windows Server 2022 y se dispone de dos estaciones de trabajo universitarias con 32 GB de RAM cada una. Se propone una aplicación HTML estática con acceso anónimo para simplificar las pruebas web, y ensayos independientes para AD DS y DNS. Quedan por verificar CPU, espacio libre y conectividad entre MAC virtuales; la capacidad nominal del SSD y la red cableada ya fueron confirmadas por el equipo.

2.2. Necesidad Identificada

Se requiere diseñar una alternativa redundante que permita evaluar la atención de solicitudes cuando falla uno de los nodos web, así como la continuidad de DNS y de las operaciones de dominio seleccionadas cuando un controlador deja de estar disponible. La propuesta debe especificar componentes, conexiones, condiciones de operación y límites de protección.

La relación entre IIS y el dominio se documentará según la aplicación elegida. No se asumirá que una página anónima depende de autenticación de dominio en cada solicitud. Las pruebas de identidad y DNS tendrán criterios propios, diferenciados de los ensayos HTTP. También se necesita definir una línea base sin redundancia y un procedimiento repetible de inyección de fallos.

2.3. Justificación de la Propuesta

La propuesta permite relacionar administración de sistemas operativos, servicios de red y tolerancia a fallos en un entorno experimental delimitado. El antecedente de Pereira et al. (2023) respalda la pertinencia de evaluar balanceadores frente a servidores IIS, pero la selección tecnológica y los parámetros del laboratorio deberán justificarse para los recursos realmente disponibles.

Desde el punto de vista académico, VirtualBox permitirá organizar las máquinas virtuales nece-

sarias para las prácticas y documentar su configuración. La comparación entre la línea base y la arquitectura redundante buscará producir evidencia sobre el comportamiento observado durante cada ensayo. La factibilidad económica y el dimensionamiento permanecerán abiertos hasta confirmar hardware y condiciones de uso del software.

El alcance se limita al diseño en la Unidad II y a la preparación de pruebas para la Unidad III. No se afirma alta disponibilidad integral de producción. El balanceador único LB01 seguirá siendo un punto único de fallo; la red y la estación que aloja LB01 también condicionarán la publicación web.

2.4. Evidencia Bibliográfica y Decisiones de Diseño

El inventario aportado permite diseñar una configuración, pero todavía no cuantifica una línea base. Se compararán después un backend y dos backends con la misma página y carga. En el modelo de un solo nodo, detener ese servicio elimina el único camino de atención; es una consecuencia estructural del diseño, no una tasa de fallos medida. El primer ensayo deberá documentar esa diferencia sin extrapolarla a la universidad.

Las revisiones de tolerancia a fallos, balanceo reactivo y resiliencia arquitectónica separan mecanismos y dependencias (Rehman et al., 2022) (Tawfeeg et al., 2022) (Prokhorenko y Babar, 2020). La redundancia de red es otra dimensión (Momoh et al., 2019); aquí el segmento compartido permanece como dependencia. La Tabla 1 enlaza los antecedentes más próximos con decisiones implementables, sus requisitos y su verificación. Los trabajos de SIP y CoRAL atienden continuidad de sesiones y conexiones (Jiang et al., 2012) (Aghdaie y Tamir, 2009); servicios compuestos y Kubernetes añaden estado transaccional o de contenedores (Memon et al., 2021) (Tran et al., 2022). Esa diferencia justifica probar HTML anónimo local: el proyecto medirá atención de nuevas solicitudes, no recuperación transparente de sesiones en curso.

La comparación monolito/microservicios y los servicios educativos concurrentes sitúan la escala de aplicación (Blinowski et al., 2022) (Mihai et al., 2023); el escalado predictivo educativo y las metaheurísticas tratan asignación más compleja (Su, 2026) (Syed et al., 2024). Con seis VMs se prioriza una configuración reproducible y carga controlada. No se convierte el sitio de prueba en una plataforma académica completa.

La migración en vivo, su implementación y el modelo de clúster con migración muestran que mover VMs requiere mecanismos específicos (Choudhary et al., 2017) (Khan y Usmani, 2019) (Riabko et al., 2023). Distribuirlas entre hosts no equivale a migración automática. La detección proactiva por logs (Senevirathne et al., 2024) se compara con el monitoreo básico propuesto para reconocer su menor alcance.

Tabla 1
Correspondencia entre evidencia, decisión y prueba

Evidencia consultada	Decisión y límite	Trazabilidad
IIS con ARR/HAProxy y caché (Pereira et al., 2023)	Granja ARR con dos IIS; controlar caché y reintentos.	RF-02; CP-02/03.
Comparación de algoritmos WLC/RR (Fawwazi et al., 2025); Nginx (Ma y Chi, 2022); laboratorio Nginx (Fernández et al., 2023)	RR como referencia simple; no afirmar rendimiento óptimo.	RNF-03; CP-02.
Laboratorio HTTP con HAProxy (Mejía Viteri et al., 2018); middleware (Godino González, 2013)	Documentar línea base y diferencias de plataforma.	RF-01/02; CP-01/03.
Virtualización y recuperación FIEC (Campos Bustos y Vera Chávez, 2015); marco de recuperación (Kassim et al., 2018)	Separar pares por host y distinguir respaldo de continuidad.	OE2/3; CP-07/13.
Métricas de incidentes (Talluri et al., 2025); medición de failover (Abuibaid et al., 2022); disponibilidad empresarial (Malhotra et al., 2023)	Medir desde cliente y nodos; conservar errores y tiempos.	RF-04; CP-03/06.
Pruebas de elasticidad (Su y Li, 2021); rendimiento web (Samad et al., 2018); laboratorio remoto (Villar-Martínez et al., 2021)	Mantener carga y archivo constantes; separar detección y recuperación.	RNF-01/03; CP-02/03.
AD DS (Microsoft Corporation, 2025); separación de DC (Amazon Web Services, 2026)	Dos DC de escritura con DNS; RPC y SYSVOL verificados.	RF-03; CP-04/05/12.
Recuperación ante desastres (Choppadandi et al., 2024)	Ensayo aislado con copia y destino independiente confirmado.	RF-05; CP-07.

Nota. Síntesis propia de las fuentes; la transferencia se limita a los mecanismos o criterios indicados, no a sus resultados numéricos.

La elección de líder, Raft y el quórum balanceado estudian consenso o disponibilidad de datos (Shiozaki y Nakamura, 2026) (Kondru y Rajiakodi, 2024) (Mohd Ali et al., 2021). Delimitan lo que no se debe atribuir a AD DS: el diseño utiliza su protocolo documentado, sin instalar otro consenso. Asimismo, multi-cloud y failover DNS operan sobre dependencias distintas (Li et al., 2025) (Zaelani y Suranegara, 2026); un DNS alternativo no elimina el punto único de fallo de ARR.

Esta comparación fundamenta una contribución aplicada: un protocolo acotado de pruebas web y de dominio con recursos del laboratorio. La validación empírica sigue pendiente. Las fuentes de contraste justifican límites y alternativas; no se presentan como instrucciones de configuración de Windows Server 2022.

3. Objetivos

3.1. Objetivo General

Diseñar, para la entrega de la Unidad II, un prototipo académico de servicios IIS y AD DS/DNS en seis máquinas virtuales distribuidas entre dos estaciones con VirtualBox, especificando requerimientos verificables, cuatro vistas gráficas y un protocolo de validación para la Unidad III.

3.2. Objetivos Específicos

1. **OE1:** establecer los requerimientos funcionales y no funcionales con identificador, criterio de aceptación y correspondencia con casos de prueba.
2. **OE2:** definir la distribución de las seis VMs, sus recursos iniciales, flujos de red y cuatro diagramas, delimitando los fallos cubiertos y los puntos únicos de fallo.
3. **OE3:** diseñar controles de acceso, riesgos priorizados, respaldo y auditoría, asignando responsables y metas de recuperación sujetas a prueba.
4. **OE4:** elaborar el cronograma de implementación y el protocolo de ensayos repetibles, con evidencias y condiciones para aceptar o revisar el diseño en la Unidad III.

4. Requerimientos

Los requisitos de esta sección son decisiones de diseño del equipo. Sus umbrales son metas de aceptación propuestas para el prototipo, no cifras obtenidas ni niveles de servicio institucionales. Si la línea base no permite cumplirlos, se documentará la causa y se someterá el cambio a

revisión antes de repetir los ensayos. Las Tablas 2 y 3 establecen la correspondencia con el plan de pruebas.

4.1. Requerimientos Funcionales

Tabla 2
Requerimientos funcionales y verificación

ID	Requerimiento	Aceptación
RF-01	Publicar el mismo sitio estático en WEB01 y WEB02	CP-01: ambas copias comunes tienen hashes iguales y responden HTTP 200.
RF-02	Distribuir tráfico desde LB01 y excluir un backend caído	CP-02/03: ambos nodos reciben tráfico; tras un fallo, el superviviente atiende las nuevas solicitudes.
RF-03	Mantener AD DS y DNS en dos DC de escritura	CP-04: objeto de prueba replicado; CP-05: consulta DNS y operación de dominio con un DC apagado.
RF-04	Conservar registros de ensayos y recuperación	CP-06: CSV de cliente y logs de IIS exportados con identificador y hora.
RF-05	Respaldar y restaurar contenido y configuración	CP-07: restauración aislada e integridad comprobada; dominio según procedimiento validado.

Nota. Requisitos del prototipo y pruebas asociadas; metas sujetas a validación.

4.2. Requerimientos No Funcionales

La disponibilidad se acota a la ventana de ensayo; no se extrapolará a un año. La metodología separa respuesta HTTP, fallo de backend y recuperación desde respaldo, de modo que el objetivo de 30 s no se confunda con el de 60 min. Los errores transitorios también se registrarán aunque el sistema se recupere.

5. Diseño de la Arquitectura

5.1. Arquitectura Lógica

El prototipo se organiza en cuatro bloques funcionales: cliente de pruebas, proxy inverso, servidores web y servicios de identidad y nombres. Esta separación describe funciones del laboratorio; no corresponde a una arquitectura tradicional de tres niveles con base de datos. CLIENT01 origina solicitudes; LB01 distribuye tráfico HTTP mediante IIS, ARR y URL Rewrite; WEB01 y WEB02 publican el sitio; DC01 y DC02 proporcionan AD DS y DNS.

Se propone balanceo Round Robin con pesos iguales para los dos nodos web, sujetos a comprobación en la configuración instalada. La igualdad de recursos virtuales no implica rendimiento

Tabla 3
Requerimientos no funcionales medibles

ID	Categoría	Meta propuesta
RNF-01	Disponibilidad experimental	CP-03: recuperación observada de nuevas peticiones en hasta 30 s tras fallo de un backend.
RNF-02	Seguridad	CP-08: HTTP backend permitido desde LB01; acceso de prueba no autorizado bloqueado y documentado.
RNF-03	Rendimiento	CP-02: al menos 99 % HTTP exitoso y percentil 95 hasta 2 s en carga base de 5 solicitudes/s durante 5 min.
RNF-04	Escalabilidad	CP-09: procedimiento de incorporación de un nodo revisado y recursos calculados; no se exige una séptima VM.
RNF-05	Mantenibilidad	CP-07/10: recuperación desde copia y reintegración del nodo documentadas; RPO propuesto 24 h y RTO de respaldo 60 min.
RNF-06	Usabilidad operativa	CP-10: otro integrante reproduce la lista de verificación sin omitir pasos críticos, en hasta 20 min.

Nota. Umbrales propuestos por el equipo, no resultados de rendimiento.

físico idéntico entre anfitriones. La comparación de algoritmos exige mantener condiciones de carga y documentar su contexto (Fawwazi et al., 2025) (Ma y Chi, 2022). ARR permite definir una granja de servidores y pruebas HTTP de estado (Microsoft, s. f.-a). El antecedente de Pereira et al. (2023) aporta una referencia experimental para el uso de ARR e IIS, sin garantizar los mismos resultados en este laboratorio.

5.2. Arquitectura Física

Se utilizarán dos estaciones universitarias con 32 GB de RAM cada una y Oracle VM VirtualBox. HOST01 alojará DC01, WEB01 y LB01; HOST02 alojará DC02, WEB02 y CLIENT01. Así, los dos nodos de cada servicio redundante residen en equipos distintos; se aplica la separación de dependencias estudiada en (Prokhorenko y Babar, 2020). Cada estación dispone de SSD de 512 GB y permisos de administrador; ambas están conectadas a una red cableada existente. Se dispone de tres direcciones IP adicionales por estación, suficientes para la propuesta de tres VMs por anfitrión. Quedan pendientes los valores de esas direcciones, la máscara, la conectividad entre VMs en modo puente y las características de CPU.

Las estaciones ya están conectadas a la red cableada del laboratorio. Se propone configurar adaptadores puente sobre ese segmento. La velocidad del enlace y la admisión de las interfaces virtuales aún deben comprobarse. La Red Interna de VirtualBox no conecta máquinas de

anfitriones diferentes (Oracle, s. f.).

5.3. Componentes Principales

- **LB01:** Windows Server 2022 con IIS, ARR y URL Rewrite. Será el único punto de entrada HTTP publicado para la granja. Su dirección será la IP propia de la VM; no se presupone una IP virtual flotante ni redundancia del balanceador.
- **WEB01 y WEB02:** Windows Server 2022 con IIS y contenido HTML estático local. Se propone autenticación anónima con identidad local y permisos de lectura. El contenido común se copiará manualmente y se verificará antes de cada ensayo; una página de diagnóstico independiente identificará el nodo que responde.
- **DC01 y DC02:** controladores de dominio de escritura del mismo dominio, con DNS integrado en AD. DC01 será el primer controlador y titular inicial de los roles FSMO; DC02 será un controlador adicional, no un servidor pasivo. La referencia técnica para el diseño del directorio es Microsoft Corporation (2025).
- **CLIENT01:** VM de navegación y medición. Su sistema operativo y herramienta de carga están pendientes de selección; se priorizará una opción que el equipo pueda administrar con facilidad.

5.4. Flujo de Información

Solicitudes web. CLIENT01 resuelve el nombre del portal y establece una conexión HTTP con LB01. ARR selecciona un backend disponible, envía la solicitud y devuelve su respuesta al cliente. Una ruta propuesta, `/health.html`, permitirá comprobar el servicio de cada backend. Los intervalos y condiciones de exclusión se definirán y medirán durante las pruebas. Se documentarán caché, afinidad y reintentos para evitar que alteren la interpretación del balanceo observado.

Resolución de nombres. Los clientes y servidores miembros utilizarán DC01 y DC02 como servidores DNS. El registro del portal apuntará a la IP de LB01. La selección de un DNS alternativo puede incluir esperas y depende de las condiciones del cliente y de su caché; no se promete conmutación instantánea.

Operaciones de dominio. Las consultas de autenticación y administración del dominio se distinguirán de la entrega de HTML anónimo. Los cambios de AD DS se replicarán entre los controladores según su topología y configuración. No se trasladarán archivos de base de da-

tos manualmente. La replicación de los archivos de SYSVOL se verificará por separado de la replicación del directorio. Aunque estos flujos tienen finalidades distintas, comparten recursos físicos y pueden competir por CPU, disco y red.

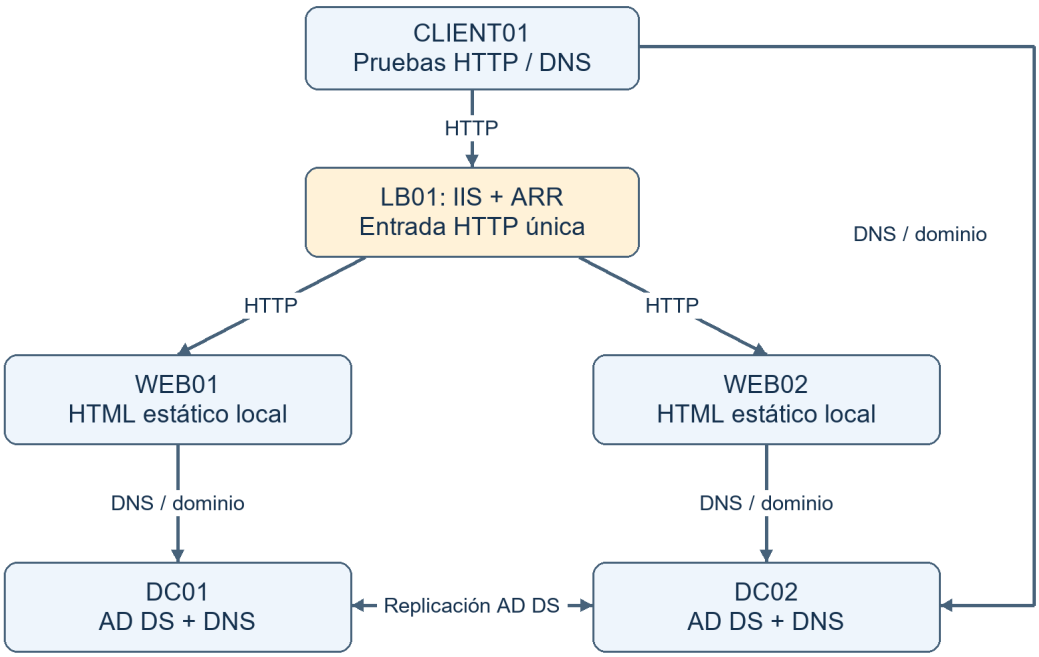
5.5. Análisis de Modos de Fallo

Los siguientes comportamientos son previsiones de diseño que deberán contrastarse con registros y mediciones, no resultados obtenidos.

- **Fallo de WEB01 o WEB02:** ARR deberá excluir el nodo no disponible y dirigir nuevas solicitudes al superviviente una vez detectado el fallo. Se medirán errores y solicitudes pendientes durante esa transición; no se garantiza ausencia de interrupción.
- **Fallo de DC01:** DC02 podrá atender las operaciones de directorio y DNS para las que esté correctamente configurado y sincronizado. Las operaciones dependientes de roles FSMO requieren evaluación específica. No se presupone que toda creación de cuentas falle inmediatamente ni que todas las funciones continúen sin degradación.
- **Fallo de DC02:** DC01 permanecerá como proveedor de dominio y DNS, con pérdida temporal de redundancia. Se registrarán tiempos de respuesta, errores y recuperación de la replicación al reintegrar DC02.
- **Fallo de LB01:** el acceso publicado al portal dejará de estar disponible aunque los backends continúen activos. Este punto único de fallo está reconocido dentro de las limitaciones del prototipo.
- **Fallo de HOST01:** se perderán DC01, WEB01 y LB01. WEB02 y DC02 podrán seguir ejecutándose, pero no se mantendrá el acceso publicado a través de LB01.
- **Fallo de HOST02:** se perderán DC02, WEB02 y CLIENT01. HOST01 conservará el camino de publicación web, sujeto a la detección del backend caído. Para medir este ensayo se ejecutará previamente el observador desde el sistema anfitrión HOST01, como prevé CP-14; CLIENT01 no puede observar la falla de su propio host.

La Figura 1 representa las decisiones descritas en esta sección.

Figura 1
Arquitectura lógica del prototipo



Nota. Elaboración propia. La conectividad real y el dimensionamiento se validarán en la Unidad III.

6. Diseño de Infraestructura

6.1. Servidores y Equipos

Se confirman dos estaciones de trabajo de la universidad con 32 GB de RAM por equipo. Se propone asignar inicialmente tres VMs de 4 GB por anfitrión: 12 GB de memoria virtual asignada y 20 GB no asignados a VMs. Estos 20 GB deberán absorber el sistema anfitrión, VirtualBox y sus sobrecargas; no constituyen memoria libre garantizada. Se verificará el rendimiento antes de fijar la carga experimental.

Se confirma SSD de 512 GB por estación, permisos de administrador y conexión cableada existente. La capacidad del disco se registra como especificación del equipo. Queda pendiente registrar CPU, núcleos e hilos, espacio libre, sistema operativo anfitrión y versión de VirtualBox. No se ha confirmado la velocidad de la red.

6.2. Sistemas Operativos

DC01, DC02, WEB01, WEB02 y LB01 utilizarán Windows Server 2022. Se confirma disponibilidad de la ISO de Windows Server 2022 con Experiencia de Escritorio, modalidad seleccionada para facilitar la administración gráfica de AD DS, DNS, IIS y ARR. La edición y las

condiciones de licencia están por confirmar. La existencia de la ISO no acredita autorización de uso; como alternativa temporal se verificará la opción de evaluación publicada por Microsoft (Microsoft, s. f.-d). El ciclo de vida de Windows Server 2022 se comprobará con el registro del fabricante (Microsoft, s. f.-e). No se presupone que la universidad proporcione licencias. Se propone Windows con PowerShell para CLIENT01. Este cliente observará fallos de VMs y de HOST01; medir la caída completa de HOST02 requerirá trasladar previamente la función de observación al anfitrión HOST01, sin añadir otra VM.

6.3. Almacenamiento

Se proponen discos VDI de 60 GB con asignación dinámica por VM. Con tres VMs, cada estación tendrá 180 GB de capacidad lógica inicial. El consumo real y el espacio adicional para actualizaciones, registros y respaldos se verificarán en disco; no se fija un tamaño de instalación limpia. La asignación dinámica no elimina la necesidad de reservar capacidad para el crecimiento.

El sitio web se almacenará localmente en ambos nodos IIS, sin NAS ni almacenamiento compartido en el alcance inicial. Se propone verificar el contenido común mediante hashes después de cada copia manual. La ruta de diagnóstico por nodo se excluirá de esa comparación cuando tenga contenido distinto por diseño.

6.4. Virtualización

Todas las VMs se ejecutarán en Oracle VM VirtualBox. Las 2 vCPU, 4 GB de RAM y 60 GB de disco por VM son parámetros iniciales de diseño, pendientes de validación contra el hardware disponible.

La Tabla 4 resume el dimensionamiento inicial.

Las instantáneas podrán apoyar el trabajo previo a configuraciones, pero no se establecerá una restauración indiscriminada de controladores de dominio como procedimiento de recuperación. Se deberá verificar el comportamiento del hipervisor y diseñar respaldos del estado del sistema. Las salvaguardas de restauración virtual no sustituyen esos respaldos (Microsoft, s. f.-c).

6.5. Servicios Requeridos

Se instalarán AD DS y DNS en DC01/DC02; IIS para contenido estático en WEB01/WEB02; e IIS con ARR y URL Rewrite en LB01. La viabilidad de instalación de los módulos se comprobará en la imagen de Windows Server 2022 elegida antes de desplegar el entorno completo. CLIENT01 requerirá navegador y herramienta de medición. Se propone direccionamiento es-

Tabla 4
Recursos virtuales iniciales y dependencias de las máquinas

Host	VM	RAM / vCPU	Rol y dependencias
HOST01	DC01	4 GB / 2	AD DS y DNS; IP estable, hora y conectividad del segmento.
HOST01	WEB01	4 GB / 2	IIS; contenido local, DNS y pertenencia al dominio.
HOST01	LB01	4 GB / 2	ARR y URL Rewrite; acceso HTTP a ambos nodos y resolución de sus nombres.
HOST02	DC02	4 GB / 2	AD DS y DNS; contacto con DC01 para promoción y replicación.
HOST02	WEB02	4 GB / 2	IIS; contenido local, DNS y pertenencia al dominio.
HOST02	CLIENT01	4 GB / 2	Navegación y medición; acceso a LB01 y ambos DNS.

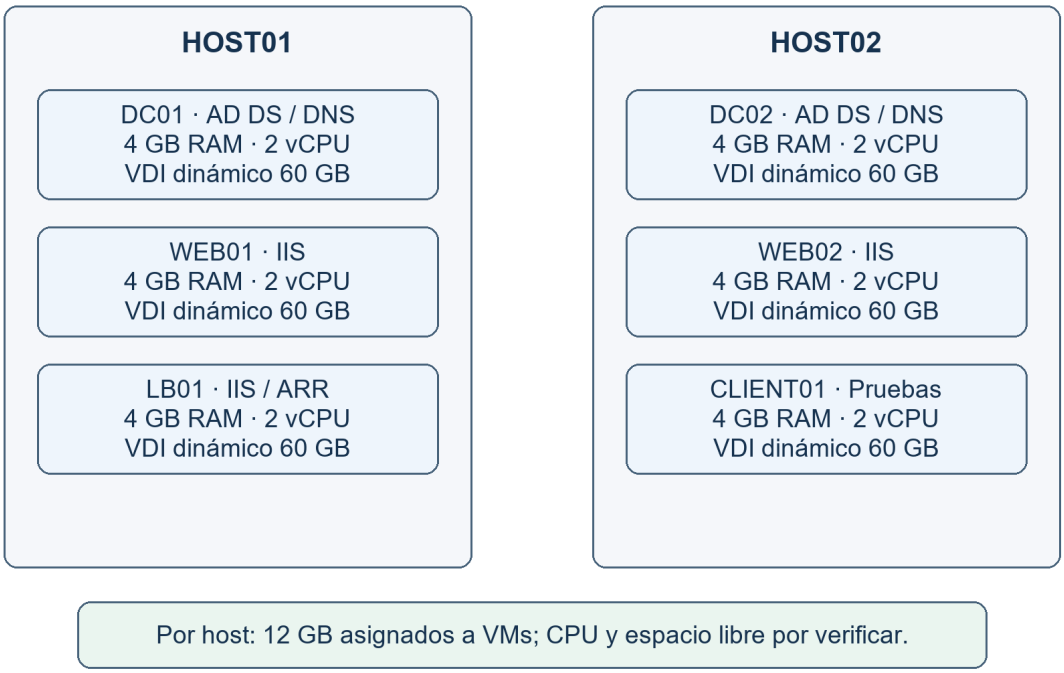
Nota. Elaboración propia; asignación inicial pendiente de validación.

tático; no se incluye DHCP en el alcance inicial.

Los nombres, direcciones y reglas de firewall se definirán en el diseño de red. No se considerará suficiente una lista parcial de puertos: se identificarán los flujos necesarios para DNS, autenticación, administración y replicación conforme a la configuración elegida. HTTP se limitará al segmento de laboratorio durante los ensayos iniciales; HTTPS permanece pendiente de diseño.

La Figura 2 representa las decisiones descritas en esta sección.

Figura 2
Despliegue de seis VMs en dos anfitriones



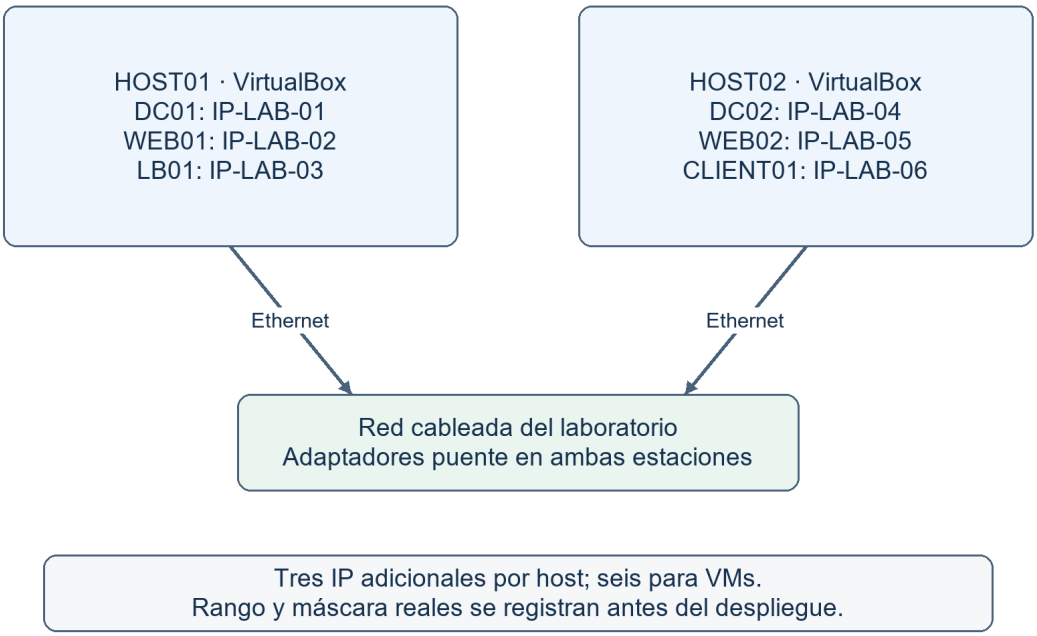
Nota. Elaboración propia. La conectividad real y el dimensionamiento se validarán en la Unidad III.

7. Diseño de Red

7.1. Topología

Las estaciones ya están conectadas a la red cableada del laboratorio. Cada VM utilizará un adaptador puente de VirtualBox sobre la interfaz Ethernet activa. Se verificará que los puertos del laboratorio admitan las MAC de las tres VMs por equipo; no se presume que disponer de IP libres garantice ese permiso (Oracle, s. f.). La Figura 3 muestra el enlace propuesto.

Figura 3
Topología cableada con adaptadores puente



Nota. Elaboración propia; no se presupone velocidad del switch ni acceso a Internet.

7.2. Segmentación y VLAN

Se utiliza el segmento existente del laboratorio. No se crearán VLAN ni rutas adicionales en el alcance inicial. La ausencia de segmentación propia se reconoce como límite de aislamiento. La red será una dependencia compartida; no se promete tolerancia a su fallo.

7.3. Direccionamiento IP

El equipo informa tres IP adicionales por PC, dentro del rango del laboratorio y no utilizadas, independientes de la IP de cada anfitrión. Sus valores y máscara se registrarán antes de implementar. La Tabla 5 usa identificadores simbólicos; no se configura un rango inventado. Se confirmará que las direcciones no se superpongan con DHCP. Un ping sin respuesta no demuestra disponibilidad. Se propone el dominio de prueba `ad.so1.test` y el portal `portal.ad.so1.test`. El sufijo reservado para pruebas evita inventar un dominio institucional (Eastlake y Panitz, 1999). El portal apuntará a la IP propia de LB01, sin IP flotante. La máscara M y el prefijo N serán los del segmento autorizado; antes de configurar se comprobará que las seis IP sean hosts distintos de N/M y no direcciones de red o difusión. El gateway G sólo se empleará si el segmento necesita alcanzar otras redes. No se inventará una subred distinta de la asignada. Sin salida de laboratorio, DNS se limitará a las zonas del dominio y no tendrá reenviadores externos; con

Tabla 5
Asignación simbólica de las seis IP disponibles

VM	Host	IP asignable	DNS
DC01	HOST01	IP-LAB-01	Según fase de promoción y réplica con DC02.
WEB01	HOST01	IP-LAB-02	DC01 y DC02.
LB01	HOST01	IP-LAB-03	DC01 y DC02.
DC02	HOST02	IP-LAB-04	DC01 para promoción; luego ambos según validación.
WEB02	HOST02	IP-LAB-05	DC01 y DC02.
CLIENT01	HOST02	IP-LAB-06	DC01 y DC02.

Nota. Identificadores simbólicos. Cada VM recibirá una IP real adicional del rango autorizado.

salida autorizada se configurarán exclusivamente los reenviadores indicados por el responsable de red.

7.4. Firewall

La Tabla 6 define flujos de destino para el diseño. Se implementarán mediante reglas de los roles y servicios, restringidas por origen; no como apertura indiscriminada de todos los puertos. Se comprobará el tráfico efectivo con registros y pruebas funcionales. La referencia de puertos de Microsoft es un inventario de servicios y no reemplaza la configuración de Windows Firewall (Microsoft, s. f.-b). SYSVOL entre DC se verificará como servicio DFSR con sus reglas correspondientes; no se confundirá con el acceso SMB de los miembros. No se habilita LDAP sobre TLS ni catálogo cifrado como si se hubieran instalado certificados. Cualquier cambio de servicio deberá actualizar la matriz y su prueba.

7.5. Acceso Remoto

Se elige administración local por consola de VirtualBox, con los permisos de administrador confirmados. RDP, WinRM, VPN y MFA remoto no se despliegan en el prototipo inicial porque no hay acceso administrativo externo previsto. Si se habilita RDP, se exigirá revisión de alcance, NLA y equipos de origen definidos antes de cambiar el diseño; no se afirmará MFA inexistente.

7.6. Comprobaciones de Conectividad

Antes de instalar roles se comprobarán IP y máscara, ausencia de conflictos y comunicación cruzada entre VMs de anfitriones distintos. Después se validarán resolución directa y registros SRV, acceso HTTP, autenticación, SYSVOL y replicación. Se usarán consultas a cada DNS por separado y pruebas de operación, no únicamente apertura TCP. Los resultados se registrarán como evidencia de Unidad III.

Tabla 6
Matriz de comunicaciones y política de acceso

Origen	Destino	Puerto/protocolo	Acción y finalidad
CLIENT01	LB01	TCP 80	Permitir HTTP del ensayo.
LB01	WEB01/WEB02	TCP 80	Permitir proxy y sondeos.
Miembros y DC	DC01/DC02	UDP/TCP 53	Permitir DNS.
Miembros y DC	DC01/DC02	UDP/TCP 88, 464	Permitir Kerberos y cambio de contraseña.
Miembros y DC	DC01/DC02	UDP/TCP 389	Permitir LDAP y localización de DC.
Miembros y DC	DC01/DC02	TCP 445, 135	Permitir SYSVOL/SMB y mapeador RPC.
Miembros y DC	DC01/DC02	TCP 49152–65535	Reglas de servicio para RPC necesario, incluida replicación entre DC.
Miembros y DC	DC01/DC02	TCP 3268	Permitir consultas al catálogo global cuando se utilicen.
Miembros	Jerarquía de dominio	UDP 123	Permitir sincronización de hora; validar fuente del PDC.
VM de diagnóstico	VMs del proyecto	ICMPv4	Permitir diagnóstico durante comprobaciones.
Otros orígenes	Servicios del proyecto	No autorizados	Bloquear entradas ajenas a reglas documentadas.

Nota. Flujos previstos; aplicar reglas de servicio y verificar el comportamiento efectivo.

8. Diseño de Seguridad

Los controles de esta sección son propuestas para implementar y verificar en la Unidad III. Se priorizan las herramientas nativas de Windows Server 2022 y la administración local de VirtualBox. No se afirma que los controles ya estén implementados.

8.1. Riesgos Identificados

Se identifican la interrupción de LB01 como punto único de fallo, la pérdida simultánea de las VMs de un anfitrión, la exposición de servicios en la red compartida, los cambios inconsistentes del contenido web y los errores administrativos propagados en el directorio. La redundancia entre nodos no sustituye un respaldo recuperable.

8.2. Amenazas

Se contemplan accesos no autorizados, privilegios excesivos, borrado accidental, fallos de red y saturación por pruebas de carga mal dimensionadas. Las pruebas deberán limitarse a las máquinas del proyecto. Las anomalías de replicación y de sincronización horaria se investigarán como condiciones operativas, sin atribuirles automáticamente un origen malicioso.

8.3. Controles Propuestos

- Mantener Windows Firewall habilitado. Permitir HTTP hacia LB01 desde clientes autorizados y hacia WEB01/WEB02 desde LB01. Las pruebas directas de backend requerirán una excepción temporal documentada.
- Revisar las reglas de los roles de dominio y limitar su alcance al proyecto. No se tomará una lista abreviada de puertos como configuración completa: deberán contemplarse los flujos de autenticación, DNS, SYSVOL y RPC que correspondan.
- Utilizar un grupo de aplicaciones dedicado en IIS con identidad de mínimos privilegios. La identidad del proceso y la identidad anónima se comprobarán por separado.
- Registrar versiones y parches antes de medir, evitando reinicios durante las ventanas de ensayo sin suspender indefinidamente las actualizaciones.
- Verificar el contenido común mediante hashes tras cada copia manual, manteniendo separada la página de diagnóstico que identifica al backend.

8.4. Gestión de Accesos

Se utilizarán cuentas nominativas y permisos ajustados a cada tarea. La pertenencia a grupos privilegiados se limitará a lo necesario; administrar IIS en un servidor miembro no requiere utilizar permanentemente una cuenta de administrador del dominio.

El contenido web utilizará permisos NTFS de lectura para la identidad que realmente acceda a los archivos; la modificación se limitará a los responsables del despliegue. Se comprobará la configuración efectiva de IUSR y del grupo de aplicaciones antes de fijar las ACL. No se utilizarán datos personales reales ni se guardarán contraseñas en el sitio o en las evidencias.

La administración se realizará preferentemente por las consolas de VirtualBox. RDP será opcional, con autenticación a nivel de red y acceso limitado a equipos administrativos identificados. No se presupone WinRM o RSAT sin definir sus requisitos ni se publicará administración hacia Internet.

8.5. Respaldo y Recuperación

Se propone Windows Server Backup para respaldar el estado del sistema de los controladores de dominio. Para LB01 y los nodos web se conservarán configuraciones, contenido y documentación de módulos y permisos necesarios para reconstruir el servicio. Copiar únicamente un archivo de configuración no demuestra una recuperación completa.

El destino independiente de respaldo está **pendiente de confirmación**. Se evaluará un medio externo con capacidad suficiente para las copias medidas. Un VDI adicional en el mismo SSD puede servir para practicar, pero no protege frente a la pérdida de ese SSD o del anfitrión. No se afirma disponibilidad de un medio externo ni se fija una capacidad sin verificarla.

Las instantáneas no sustituirán al respaldo del estado del sistema ni se restaurarán controladores de dominio indiscriminadamente. Las salvaguardas de restauración virtual no reemplazan los respaldos requeridos (Microsoft, s. f.-c).

Se proponen como metas iniciales respaldo diario, RPO de hasta 24 horas y RTO de recuperación desde respaldo de hasta 60 minutos. Su viabilidad depende del destino, las sesiones de laboratorio y una restauración de prueba: no son resultados demostrados. El tiempo de restauración se distinguirá del tiempo de conmutación entre nodos (Choppadandi et al., 2024). No se propone incautar roles FSMO por un apagado temporal durante las pruebas.

8.6. Monitoreo y Auditoría

Se revisarán los registros de Seguridad, Sistema, Servicio de directorio y DNS según cada rol, conservando hora, origen y contexto de errores de autenticación, interrupciones y anomalías de replicación. Los identificadores de eventos se verificarán según el proveedor y la configuración instalada.

Se propone registrar en IIS formato W3C: fecha, hora, IP de origen, método, ruta, estado y tiempo de atención. Se distinguirán las solicitudes del proxy, sus sondeos y el tráfico de prueba. La dirección de LB01 se registrará con su IP real durante la implementación; no se adoptará una IP de ejemplo.

Los logs de cliente, balanceador y backends se correlacionarán mediante una referencia horaria documentada. En el backend la IP de origen puede ser la del proxy, por lo que no se interpretará automáticamente como la del usuario final. Las evidencias se exportarán después de cada ensayo y su acceso se limitará a los responsables del proyecto.

8.7. Matriz de Riesgos y Tratamiento

La Tabla 7 presenta amenazas y controles; la priorización ordinal se detalla posteriormente.

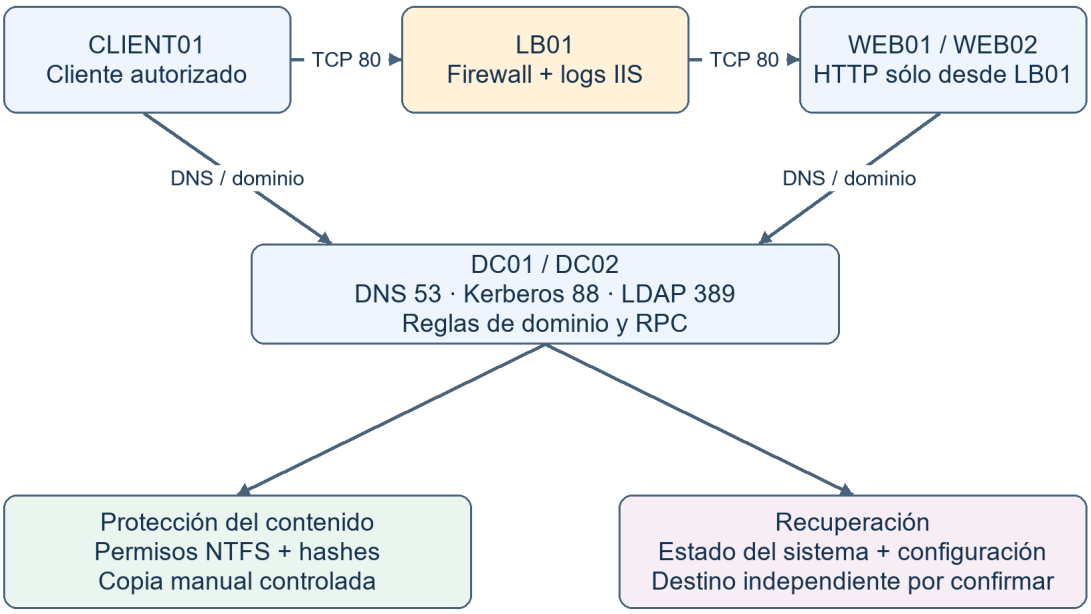
Tabla 7
Riesgos y controles propuestos

ID	Activo y amenaza	Impacto	Control	Riesgo residual
R-01	LB01/HOST01: interrupción	Crítico	Logs y procedimiento de recuperación	Balanceador sin redundancia.
R-02	IIS: caída o saturación	Moderado	ARR y carga controlada	Errores durante detección.
R-03	AD DS/DNS: caída de un DC	Moderado	Dos DC en hosts distintos	Pérdida de redundancia; funciones FSMO por evaluar.
R-04	Red: acceso no autorizado	Alto	Firewall limitado por origen	Dependencia de red compartida.
R-05	Contenido: cambios o borrado	Moderado	ACL, copia e integridad	Despliegue manual sujeto a errores.
R-06	Directorio: cambio destructivo	Crítico	Respaldo y restauración de prueba	Destino pendiente y pérdida de cambios recientes.

Nota. Elaboración propia; asignación inicial pendiente de validación.

La Figura 4 representa las decisiones descritas en esta sección.

Figura 4
Controles de seguridad y flujos autorizados



Nota. Elaboración propia. La conectividad real y el dimensionamiento se validarán en la Unidad III.

8.8. Método de Valoración y Correspondencia de Controles

Se adapta el enfoque de identificación de amenazas, probabilidad e impacto de NIST SP 800-30 (Joint Task Force Transformation Initiative, 2012). La escala interna usa probabilidad P de 1 (baja) a 3 (alta) e impacto I de 1 (limitado), 2 (servicio parcial o contenido afectado) y 3 (interrupción de entrada web, exposición administrativa o pérdida del directorio). En la matriz descriptiva, Moderado equivale a I=2 y Crítico/Alto a I=3; el nivel de riesgo de la matriz de priorización es P por I, no la etiqueta de impacto aislada. El producto P por I es una priorización ordinal del equipo: 1–2 bajo, 3–4 medio y 6–9 alto. No son probabilidades estadísticas ni certificación de cumplimiento.

Los controles se relacionan con las funciones de NIST CSF 2.0 (National Institute of Standards and Technology, 2024): Govern para responsables y aceptación de límites; Identify para inventario y riesgos; Protect para cuentas, ACL y firewall; Detect para logs y comprobaciones; Respond para registro y contención; Recover para respaldo y ensayo de restauración. El marco orienta resultados y no obliga a instalar un SIEM en este laboratorio. La Tabla 8 resume los valores propuestos. La probabilidad es juicio preliminar del equipo: P=3 en cambios de contenido por su repetición manual; P=1 en modificación destructiva del directorio por ser una operación excepcional; P=2 en los restantes casos por exposición o dependencia existente sin historial de

Tabla 8
Priorización preliminar y correspondencia con NIST CSF 2.0

Riesgo	P	I	P×I	Control y función
R-01	2	3	6 alto	Logs, recuperación y aceptación del SPOF: GV/DE/RC.
R-02	2	2	4 medio	ARR, sondeos y carga acotada: PR/DE.
R-03	2	2	4 medio	DC separados, DNS y diagnóstico: PR/DE/RC.
R-04	2	3	6 alto	Restricción por IP/servicio: PR.
R-05	3	2	6 alto	ACL, hashes y copia recuperable: PR/RC.
R-06	1	3	3 medio	Estado del sistema y restauración: RC.

Nota. Valoración ordinal preliminar; no equivale a frecuencia estadística.

ocurrencias. Se revisará con los incidentes registrados. R-03 usa I=2 para pérdida de un DC con su par disponible; la pérdida conjunta del directorio corresponde a R-06. El número de riesgos no constituye por sí solo una medida de calidad; se comprobará que cubran los activos y dependencias identificados.

Como objetivo de evolución se propone la regla 3-2-1: tres copias, dos tipos de medio y una copia fuera del equipo o ubicación afectada. No se declara satisfecha: sólo se han confirmado los SSD de las estaciones y falta acordar el destino independiente. La revisión de ese recurso condiciona la prueba de recuperación y la aceptación del riesgo de pérdida común.

9. Diseño Operativo

9.1. Roles y Responsabilidades

Se proponen cuatro funciones para los integrantes consignados en la carátula: coordinación, dominio/red, web/balanceo y pruebas/evidencia. La asignación nominal se acordará antes del despliegue. En la Tabla 9, R ejecuta, A aprueba y responde por el cierre, C es consultado e I informado. Se mantiene una función A por actividad; una persona podrá apoyar otra función si conserva la revisión cruzada.

Tabla 9
Matriz RACI propuesta por función

Actividad	Coord.	Dominio	Web	Pruebas
Cerrar configuración y cambios	A	C	C	R
Configurar AD DS y DNS	A	R	C	I
Configurar IIS y ARR	A	C	R	I
Respaldar y comprobar recuperación	A	R	R	C
Ejecutar ensayos y custodiar evidencias	A	C	C	R
Registrar incidentes y aprobar cierre	A	R	R	C

Nota. R ejecuta; A responde por el cierre; C es consultado; I es informado. Asignación nominal pendiente.

9.2. Procedimientos de Operación

Arranque. Encender los anfitriones, comprobar red y espacio libre; iniciar DC01 y DC02; verificar hora, DNS y replicación; iniciar WEB01 y WEB02 y comprobar su contenido; iniciar LB01 y revisar estado de la granja; iniciar CLIENT01 y registrar una solicitud al portal. No se considerará listo el entorno sólo porque las ventanas de las VMs estén abiertas.

Inicio de sesión de trabajo. Registrar fecha, versiones, responsable y cambios desde la sesión anterior. Resolver el portal con cada DNS, revisar el estado de los backends y conservar la línea base antes de inducir fallos. Utilizar una cuenta ordinaria para navegar y una cuenta administrativa sólo cuando la tarea lo requiera.

Actualización del sitio. Conservar la versión anterior, copiar el contenido común a ambos nodos, comprobar hashes y respuestas, y registrar la versión. Si difieren, detener el ensayo y corregir antes de medir; la página de diagnóstico distinta por nodo se documentará como excepción prevista.

Apagado. Detener el generador y exportar evidencias; apagar CLIENT01, LB01 y los servidores web; comprobar que no haya cambios pendientes y apagar los DC de forma ordenada; apagar las estaciones al final. El apagado forzado queda reservado a ensayos previamente definidos, no al cierre ordinario.

9.3. Procedimientos de Mantenimiento

Antes de cada sesión se revisarán espacio libre, conectividad, servicios, logs y existencia del respaldo requerido. Los parches se aplicarán fuera de las ventanas de medición, con versión anterior y nueva registradas. Los logs no se borrarán antes de exportarlos. Una vez por ciclo de implementación se ensayará recuperación aislada y reincorporación de un nodo; cualquier cambio de firewall o contenido se reflejará en el registro de configuración.

9.4. Gestión de Incidentes

Se adapta la integración de detección, respuesta y recuperación propuesta por Nelson et al. (2025). Primero se anotará incidente, hora, síntoma, VM afectada y responsable. Luego se clasificará como crítico (LB01, pérdida común o directorio no recuperable), alto (un servicio redundante sin par) o medio (degradación sin corte general). Se detendrá la carga si pone en riesgo otras prácticas.

Se preservarán logs, se identificará la capa afectada y se contendrá mediante la acción mínima del procedimiento: excluir un backend, corregir una regla documentada o recuperar la copia aprobada. No se promoverá otro DC ni se incautarán FSMO como reacción automática a una caída temporal. El cierre exigirá comprobación funcional, causa identificada o hipótesis explícita, acciones y evidencia. Un fallo previsto de prueba se etiquetará como ensayo para no confundirlo con un incidente real.

10. Plan de Implementación

10.1. Actividades

La implementación se propone para cuatro semanas relativas de la Unidad III. No se presentan fechas oficiales del curso. Las estimaciones suman 40 horas de trabajo de laboratorio planificadas; se ajustarán a la disponibilidad real sin omitir la comprobación de roles o recuperación.

10.2. Recursos Necesarios

Se usarán las dos estaciones confirmadas, la red cableada, VirtualBox, la ISO de Windows Server 2022 y las seis IP adicionales. Se requieren instaladores compatibles de ARR y URL Rewrite, PowerShell para medición y un destino independiente de respaldo por confirmar. Antes de la sesión se preparará un paquete local con ISO, instaladores, actualizaciones aplicables, versiones y hashes. Las descargas se realizarán en un equipo con acceso autorizado fuera de la ventana de ensayo; la instalación del laboratorio no depende de una salida a Internet no confirmada. Las condiciones de licencia se comprobarán antes de instalar; no se presupone convenio institucional ni compra aprobada.

10.3. Dependencias

La Tabla 10 define predecesores. La cadena A1–A9 constituye una secuencia conservadora: no se valida ARR antes de tener contenido y resolución, ni se ejecutan fallos sin registros y recuperación. Si se paralelizan tareas, el coordinador deberá mantener sus condiciones de entrada y salida.

Tabla 10
Actividades, dependencias y esfuerzo de implementación

ID	Actividad	Prev.	Duración	Sem.
A1	Inventario, IP y conectividad puente	–	2 h	1
A2	VMs, SO, nombres y parches	A1	10 h	1
A3	Primer dominio y DNS en DC01	A2	2 h	2
A4	DC02 y validación de réplica	A3	2 h	2
A5	IIS, contenido y hashes en WEB01/02	A4	2 h	3
A6	ARR/URL Rewrite y granja LB01	A5	2 h	3
A7	Firewall, cuentas, logs y respaldo	A6	6 h	3
A8	Línea base y ensayos repetidos	A7	8 h	4
A9	Análisis y paquete de evidencias	A8	6 h	4

Nota. Horas de laboratorio estimadas; ajustar según disponibilidad y duración real de tareas.

10.4. Cronograma

El Gantt relativo de la Tabla 11 permite comprobar el orden sin inventar fechas de calendario. Un hito sólo se cerrará con evidencia: A4 requiere réplica comprobada; A6 dos backends accesibles; A7 copia recuperable o riesgo documentado; A8 resultados brutos exportados. Si no se confirma el respaldo independiente, no se presentará CP-07 como aprobado. Si no funcionan los adaptadores puente, la implementación se detendrá para revisar el segmento; no se cambiará a una arquitectura distinta sin actualizar el diseño.

Tabla 11
Gantt relativo de la Unidad III

Bloque	S1	S2	S3	S4
A1–A2: preparación	X			
A3–A4: dominio y DNS		X		
A5–A7: web, balanceo y controles			X	
A8–A9: ensayos e informe				X

Nota. Semanas relativas de Unidad III; no representa un calendario oficial.

11. Plan de Pruebas

11.1. Qué se Probará

Se comprobarán contenido, distribución HTTP, caída de un backend, réplica y disponibilidad de AD DS/DNS, logs, restricciones de acceso y recuperación. La Tabla 12 enlaza requisitos con pruebas. CP-13 observará la caída de HOST01 desde CLIENT01. En CP-14, un script ejecutado en el sistema anfitrión HOST01 observará la caída de HOST02; antes se comprobará que HOST01 puede resolver el portal y alcanzar LB01. Si no se habilita esa observación, CP-14 se registrará no ejecutado, no aprobado.

11.2. Cómo se Probará

Se realizará una comprobación en línea base sin redundancia de backend y otra con ambos nodos activos, manteniendo sitio y carga. Se propone PowerShell en CLIENT01 para registrar cada solicitud, código, error, duración y backend observado. Se documentarán versión del script, tamaño del contenido, caché, afinidad, reintentos, URL de sondeo y configuración de ARR antes de medir.

La carga inicial será de 5 solicitudes por segundo durante 300 segundos, con timeout de solicitud propuesto de 5 s. Se registrará la tasa realmente alcanzada; si el generador no sostiene la tasa, el ensayo no es comparable. Esta separación entre carga y respuesta se apoya en (Samad et al., 2018) (Su y Li, 2021). Se propone iniciar la búsqueda de fallo a los 120 s y repetir cada escenario tres veces, restableciendo el entorno. Los parámetros de comprobación de ARR se fijarán al comprobar las opciones efectivamente disponibles; no se atribuyen a la literatura como configuración universal.

Para CP-03 se tomará t0 al inyectar el fallo, td cuando ARR lo marque no saludable y tr al inicio de 30 s consecutivos de respuestas nuevas correctas. Se calcularán detección td menos t0 y recuperación observada tr menos t0. Si no puede observarse td, se reportará no medido, sin deducirlo del primer éxito. Se informarán percentil 95 de latencia, solicitudes emitidas, fallidas

y tasa alcanzada para cada repetición; no sólo promedios agregados.

11.3. Resultado Esperado

Se espera que un backend superviviente atienda nuevas solicitudes después de la detección y que un DC superviviente permita las operaciones de dominio definidas. Estos resultados son hipótesis de diseño; no se garantiza ausencia de errores. CP-11 debe mostrar la limitación de LB01. La recuperación de respaldo es un escenario distinto y condicionado al medio disponible.

11.4. Criterios de Aceptación

Las metas de las Tablas 2, 3 y 12 se evaluarán por ejecución. Una repetición fallida se conservará y analizará; no se eliminará por conveniencia. CP-04 adopta 120 s como meta del proyecto, no como garantía del protocolo. CP-05 registrará tiempos DNS y autenticación por separado. Los

Tabla 12
Trazabilidad y criterios de aceptación de los ensayos

Caso	Requisito	Procedimiento	Aceptación propuesta
CP-01	RF-01	Consultar cada backend y comparar hashes comunes	HTTP 200 en ambos y hashes iguales, salvo diagnóstico.
CP-02	RF-02/RNF-03	5 solicitudes/s por 5 min, sin fallo; registrar backend	Ambos reciben solicitudes, éxito al menos 99 %, p95 hasta 2 s.
CP-03	RF-02/RNF-01	A los 120 s detener un backend; mantener la carga	Nuevas peticiones estables en hasta 30 s; registrar errores de transición.
CP-04	RF-03	Crear objeto de prueba en un DC y consultar el otro	Objeto visible en hasta 120 s; repetir en sentido inverso.
CP-05	RF-03	Apagar un DC temporalmente; consultar DNS y operar contra el otro	DNS correcto y autenticación nueva comprobada; no usar sólo sesión en caché.
CP-06	RF-04	Exportar CSV del cliente y logs de IIS	Identificador de ensayo, fecha/hora y códigos recuperables.

Nota. Casos planificados; registrar resultados por repetición y conservar fallos.

casos complementarios se presentan en la Tabla 13.

11.5. Casos Complementarios de Dominio y Anfitrión

La Tabla 14 amplía la cobertura sin introducir VMs adicionales. Los apagados se realizarán ordenadamente en la prueba de anfitrión; representan indisponibilidad, no daño físico real.

11.6. Validación del Diseño y Evidencia Pendiente

Se efectuó una comprobación documental de consistencia: seis VMs, tres por host; pares de servicios en estaciones distintas; 12 GB de RAM asignados por equipo frente a 32 GB dispo-

Tabla 13

Casos complementarios de seguridad, recuperación y operación

Caso	Requisito	Procedimiento	Aceptación propuesta
CP-07	RF-05/RNF-05	Restaurar copia en entorno aislado según procedimiento	Integridad y servicio comprobados; meta RPO 24 h y RTO 60 min.
CP-08	RNF-02	Acceso HTTP a backend desde LB01 y origen no autorizado	LB01 permitido; origen de prueba bloqueado sin afectar dominio.
CP-09	RNF-04	Revisar pasos de alta de un nodo y recursos	Procedimiento completo, impacto calculado y revisión cruzada.
CP-10	RNF-05/06	Reintegrar nodo y repetir lista operativa por otro integrante	Estado saludable y lista sin omisiones críticas en hasta 20 min.
CP-11	Límite LB01	Apagar LB01 manteniendo los backends	Detectar corte esperado y registrar que el SPOF no está mitigado.

Nota. Recuperación condicionada al medio de respaldo; no se declara ejecución.

Tabla 14

Pruebas de funciones de dominio y pérdida de anfitrión

Caso	Procedimiento	Resultado comprobable
CP-12	Registrar titulares FSMO; apagar DC01 temporalmente; consultar DNS y autenticación nueva en DC02. Registrar objeto nuevo si el pool RID local lo permite.	DNS y autenticación medidos; operaciones FSMO documentadas. No agotar RID, modificar esquema ni incautar roles. La pérdida de un titular no implica fallo inmediato de toda creación.
CP-13	Desde CLIENT01 mantener registro HTTP/DNS y apagar HOST01.	Corte de acceso por pérdida de LB01 registrado; DC02 y WEB02 siguen accesibles directamente según reglas de diagnóstico.
CP-14	Preparar observador en HOST01; validar portal; apagar HOST02 y mantener registro.	Tras detección, LB01 atiende por WEB01. Recuperación objetivo hasta 30 s; registrar errores y DNS. Si el observador no está preparado, no ejecutar.

Nota. Ensayos planificados; la prueba de HOST01 demuestra una limitación prevista, no alta disponibilidad integral.

nibles; seis IP adicionales frente a seis VMs; y catorce casos vinculados a requisitos y límites. Esta comprobación no equivale a prototipo ejecutado, simulación ni juicio de experto.

El portal de entrega está publicado en `https://ematevar.github.io/so1-prototipo-iis-adds/` y el repositorio en `https://github.com/ematevar/so1-prototipo-iis-adds`. El portal permite descargar el informe, consultar guías y revisar la validación de una PoC HTTP portable con Python. Esta PoC dispone de CSV de solicitudes reales e incluye fallo y reintegración de backends; no implementa IIS/ARR ni AD DS/DNS.

La publicación y la descarga del PDF fueron comprobadas el 11 de noviembre de 2026. Los controles del portal requieren ejecutar el servidor local; GitHub Pages aloja la vista documental. La validación de Windows Server continúa pendiente: la Unidad III deberá aportar configuración real, capturas, CSV y logs de IIS/ARR y servicios de dominio. Las metas de la Unidad II se conservan como criterios propuestos.

12. Análisis de Factibilidad

12.1. Factibilidad Técnica

La propuesta es técnicamente condicionada: se han confirmado RAM, SSD, permisos, ISO, red cableada y seis IP adicionales. Por host se asignan inicialmente 12 GB a tres VMs, sin afirmar memoria libre neta. Los 180 GB de capacidad lógica VDI por host requieren verificar espacio libre y crecimiento; disponer de SSD de 512 GB no demuestra ese espacio libre. Faltan modelo de CPU, virtualización habilitada, conectividad puente y disponibilidad del destino de respaldo.

La experiencia de escritorio simplifica la administración prevista a costa de recursos. ARR se selecciona por integrar el balanceador en IIS; HAProxy exigiría otra plataforma y NLB requeriría revisar alcance de detección y configuración de red. No se afirma superioridad universal. Se comparan tres opciones con criterios de aprendizaje, recursos y cobertura: ARR único conserva una sola consola y las seis VMs, pero deja LB01 como SPOF; dos ARR requerirían además un mecanismo de entrada redundante y al menos otra VM; NLB cambia el mecanismo de reparto y exige comprobar el modo de red y la supervisión de la aplicación. Se mantiene ARR único para estudiar redundancia de backends. El título se acota a redundancia de nodos, sin prometer disponibilidad extremo a extremo. Si la prueba de instalación no confirma compatibilidad, se revisará formalmente la elección antes de ejecutar el resto del plan.

12.2. Factibilidad Económica

El análisis separa desembolso incremental de costo total. Los equipos, red y SSD ya disponibles no se consideran compras nuevas del proyecto, pero su uso tiene costo institucional no cuantificado. La Tabla 15 distingue recursos existentes y una referencia comercial para un escenario opcional de compra; no es un presupuesto aprobado. Como referencia consultada el 11

Tabla 15
Presupuesto incremental y límites de valoración en soles

Concepto	S/ y condición	Base de valoración
Dos estaciones, SSD y red existentes	S/ 0 de compra incremental prevista	Recursos confirmados por el equipo; no es valor de mercado.
Windows Server 2022	Por verificar; no se asigna costo cero a licencia	ISO disponible; comprobar licencia o evaluación temporal.
Destino independiente de respaldo	S/ 366.00 como escenario opcional	Precio web de HDD externo Toshiba Canvio Basics 1 TB; compra no confirmada.
Electricidad y tiempo de laboratorio	No cuantificados	Requieren potencia, tarifa y horas efectivas.
Trabajo del equipo	40 h de laboratorio planificadas; valor no monetizado	Estimación del cronograma, no horas ejecutadas.

Nota. Recursos existentes y referencia de compra opcional; no es un presupuesto aprobado.

de noviembre de 2026, Memory Kings publica el HDD externo Toshiba Canvio Basics de 1 TB, modelo HDTB510XK3AA, a S/ 366.00, incluido IGV y sin flete (Memory Kings, s. f.). Es una referencia de precio variable, no una compra realizada. El escenario de adquirir una unidad añadiría S/ 366.00 al CAPEX incremental; transporte y adecuación al volumen de respaldos se verificarán antes de comprar. Si se dispone de un medio prestado adecuado, ese desembolso no sería necesario.

Se contrastó el mismo modelo HDTB510XK3AA en Hiraoka, cuya página muestra S/ 499.00 (Hiraoka, s. f.). Frente a S/ 366.00 en Memory Kings, la diferencia publicada es S/ 133.00. Ambas consultas corresponden al 11 de noviembre de 2026 y deben reconfirmarse al comprar; precios de otros proveedores o fechas no invalidan automáticamente el valor consultado. El escenario de reserva para una unidad es de S/ 366.00 a S/ 499.00, sin flete. La selección exige comprobar compatibilidad y volumen real de copias; no acredita disponibilidad del equipo.

El CAPEX incremental confirmado de compra de equipos es S/ 0; no se conoce aún el CAPEX total si se requieren licencias o medio de respaldo. El OPEX y TCO no pueden calcularse con rigor sin consumos, tarifas y horizonte. No se calculan VAN, TIR ni beneficio/costo porque no existe flujo monetario sustentado. Un presupuesto final deberá añadir cotización identificable,

fecha e impuestos cuando corresponda. La factibilidad económica permanece condicionada; no se declara rentabilidad.

12.3. Factibilidad Operativa

Se dispone de permisos de administrador y de los integrantes consignados en la carátula para distribuir las funciones RACI. No se ha confirmado su nivel de experiencia, por lo que se prevén listas de verificación y revisión cruzada. La viabilidad depende de reservar sesiones de laboratorio, conservar configuración entre sesiones, disponer de copia recuperable y cumplir las reglas de la red. El cierre operativo exigirá que otro integrante reproduzca el arranque, diagnóstico y reintegración en CP-10.

13. Conclusiones

1. En relación con OE1, se definieron cinco requerimientos funcionales y seis no funcionales con identificadores, metas y casos de prueba. Los umbrales representan decisiones verificables del diseño, no disponibilidad o rendimiento medidos.
2. Para OE2, se especificaron seis VMs repartidas en dos estaciones, con pares IIS y AD DS/DNS separados físicamente. Las cuatro figuras explican arquitectura, red, seguridad y despliegue. LB01 y la red compartida conservan puntos únicos de fallo; separar anfitriones no resuelve esa dependencia.
3. Respecto de OE3, se propusieron controles de acceso, firewall, registro y recuperación, junto con priorización ordinal de riesgos y funciones responsables. El destino independiente de respaldo y la prueba de restauración son condiciones pendientes; no se declara satisfecha la regla 3-2-1.
4. Para OE4, se planificaron nueve actividades en cuatro semanas relativas y catorce casos de prueba. La validación empírica, el presupuesto completo y las evidencias quedan para la Unidad III. El diseño es reproducible como plan, pero su factibilidad final depende de conectividad, software autorizado y recuperación comprobada.

14. Referencias Bibliográficas

Basadas en la revisión realizada en la primera unidad (en formato APA 7.ª edición).

Abuibaid, M., Ghorab, A. H., Seguin-McPeake, A., Yuen, O., Yungblut, T., y St-Hilaire, M. (2022). Edge workloads monitoring and failover: a StarlingX-based testbed implementation and measurement study. *IEEE Access*, *10*, 97101–97116. https://doi.org/10.1109/ACCESS.2022.3204976

Aghdaie, N., y Tamir, Y. (2009). CoRAL: a transparent fault-tolerant web service. *Journal of Systems and Software*, *82*(1), 131–143. https://doi.org/10.1016/j.jss.2008.06.036

Amazon Web Services. (2026). *Active Directory Domain Services on AWS: AWS Whitepaper*. https://docs.aws.amazon.com/whitepapers/latest/active-directory-domain-services/active-directory-domain-services.html

Blinowski, G., Ojdowska, A., y Przybyłek, A. (2022). Monolithic vs. microservice architecture: a performance and scalability evaluation. *IEEE Access*, *10*, 20357–20374. https://doi.org/10.1109/ACCESS.2022.3152803

Campos Bustos, K. E., y Vera Chávez, J. L. (2015). *Diseño e implementación de una solución de alta disponibilidad usando clúster y virtualización de servidores web y de bases de datos para las aplicaciones de la FIEC* [Tesis de grado, Escuela Superior Politécnica del Litoral]. Repositorio ESPOL. https://www.dspace.espol.edu.ec/xmlui/handle/123456789/30544

Choppadandi, A., Kaur, J., Kumar, P., y Nakra, V. (2024). Fault tolerance and disaster recovery in cloud-based systems. En S. S. Rajest, S. Moccia, B. Singh, R. Regin, y J. Jeganathan (Eds.), *Advancing Intelligent Networks Through Distributed Optimization* (pp.

207–226). IGI Global. https://doi.org/10.4018/979-8-3693-3739-4.ch011

Choudhary, A., Govil, M. C., Singh, G., Awasthi, L. K., Pilli, E. S., y Kapil, D. (2017). A critical survey of live virtual machine migration techniques. *Journal of Cloud Computing: Advances, Systems and Applications*, *6*(1), Artículo 23, 1–41. https://doi.org/10.1186/s13677-017-0092-1

Eastlake, D., y Panitz, A. (1999). *Reserved top level DNS names* (RFC 2606). RFC Editor. https://doi.org/10.17487/RFC2606

Fawwazi, M. M., Putra, E., y Putri, N. A. (2025). Evaluation and comparison of load balancing algorithm performance in the implementation of weighted least connections and round robin in cloud computing environment. *Journal of Computer Science, Information Technology and Telecommunication Engineering (JCoSITTE)*, *6*(1), 741–747. https://doi.org/10.30596/jcositte.v6i1.21731

Fernández, A. C., Merlo, V. S., Jordán, M. Á., y Rios, L. J. (2023). Análisis de balanceo de carga con Nginx. En *Memorias de las 52 JAIIO – Concurso de Trabajos Estudiantiles (EST)* (pp. 208–217). https://revistas.unlp.edu.ar/JAIIO/article/download/18211/17879/81772

Godino González, F. (2013). *Diseño de una arquitectura escalable y de alta disponibilidad para un sistema middleware* [Trabajo de Fin de Grado, Universidad Politécnica de Madrid, Facultad de Informática].

Hiraoka. (s. f.). *Disco duro externo Toshiba HDTB510XK3AA 1 TB*. Recuperado el 11 de noviembre de 2026, de https://hiraoka.com.pe/disco-duro-externo-toshiba-hdtb510xk3aa-1tb

Jiang, H., Iyengar, A., Nahum, E., Segmuller, W., Tantawi, A. N., y Wright, C. P. (2012).

Design, implementation, and performance of a load balancer for SIP server clusters. *IEEE/ACM Transactions on Networking*, *20*(4), 1190–1202. https://doi.org/10.1109/TNET.2012.2183612

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (SP 800-30 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Kassim, M., Mohd Sahalan, M., y Uzir, N. I. (2018). Framework architecture on high data availability server virtualization for disaster recovery. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *10*(1-5), 163–169. https://jtec.utem.edu.my/jtec/article/view/3649

Khan, A. W., y Usmani, S. A. A. (2019). Achieving high availability in cloud through live migration. *KIET Journal of Computing & Information Sciences (KJCIS)*, *2*(1), 12–25. https://doi.org/10.51153/kjcis.v2i1.17

Kondru, K. K., y Rajiakodi, S. (2024). RaftOptima: an optimised raft with enhanced fault tolerance, and increased scalability with low latency. *IEEE Access*, *12*, 105974–105989. https://doi.org/10.1109/ACCESS.2024.3435978

Li, W., Ma, G., Fang, W., He, X., y Li, J. (2025). Multi-cloud management architecture design and disaster recovery strategy for high availability. *Journal of Cyber Security and Mobility*, *14*(5), 1173–1198. https://doi.org/10.13052/jcsm2245-1439.1456

Ma, C., y Chi, Y. (2022). Evaluation test and improvement of load balancing algorithms of Nginx. *IEEE Access*, *10*, 14311–14324. https://doi.org/10.1109/ACCESS.2022.3146422

Malhotra, A., Elsayed, A., Torres, R., y Venkatraman, S. (2023). Evaluate solutions for

achieving high availability or near zero downtime for cloud native enterprise applications. *IEEE Access*, *11*, 85384–85394. https://doi.org/10.1109/ACCESS.2023.3303430

Mejía Viteri, J. T., Gonzáles Valero, M. I., y España León, Á. R. (2018). Programming algorithms of load balancing with HA-Proxy in HTTP services. *Journal of Science and Research: Revista Ciencia e Investigación*, *3*(CITT2017), 100–105. https://doi.org/10.26910/issn.2528-8083vol3issCITT2017.2018pp100-105

Memon, N., Vighio, M. S., Muhammad, Y., y Abro, Z. H. (2021). Fault tolerance framework for composite web services. *IEEE Access*, *9*, 95469–95480. https://doi.org/10.1109/ACCESS.2021.3094980

Memory Kings. (s. f.). *Disco duro USB 1 TB Toshiba Canvio Basics Black*. Recuperado el 11 de noviembre de 2026, de https://www.memorykings.pe/producto/346537/disco-duro-usb-1tb-toshiba-canvio-basics-black

Microsoft Corporation. (2025). *[MS-ADTS]: Active Directory Technical Specification* (v20251112). Microsoft Open Specifications. https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/

Microsoft. (s. f.-a). *HTTP Load Balancing using Application Request Routing*. Microsoft Learn. https://learn.microsoft.com/en-us/iis/extensions/configuring-application-request-routing-arr/http-load-balancing-using-application-request-routing

Microsoft. (s. f.-b). *Service overview and network port requirements for Windows*. Microsoft Learn. https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements

Microsoft. (s. f.-c). *Virtualized domain controller deployment and configuration*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/virtualized-domain-controller-deployment-and-configuration

Microsoft. (s. f.-d). *Windows Server 2022*. Microsoft Evaluation Center. https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022

Microsoft. (s. f.-e). *Windows Server 2022: Lifecycle*. Microsoft Learn. https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2022

Mihai, D., Mihailescu, M.-E., Carabas, M., y Tapus, N. (2023). Integrated high-workload services for e-learning. *IEEE Access*, *11*, 8441–8454. https://doi.org/10.1109/ACCESS.2023.3238967

Mohd Ali, F., Latip, R., Alrshah, M. A., Abdullah, A., y Ibrahim, H. (2021). Vigorous replication strategy with balanced quorum for minimizing the storage consumption and response time in cloud environments. *IEEE Access*, *9*, 121771–121785. https://doi.org/10.1109/ACCESS.2021.3108765

Momoh, M. O., Muhammad, S., y Atumoshi, A. Y. (2019). Fault-tolerance techniques for an enterprise network. *International Journal of Advances in Scientific Research and Engineering (IJASRE)*, *5*(11), 58–66. https://doi.org/10.31695/IJASRE.2019.33602

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Nelson, A., Rekhi, S., Souppaya, M., y Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0*

community profile (SP 800-61 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Oracle. (s. f.). *Virtual Networking*. Oracle VirtualBox User Guide, Release 7.2. https://docs.oracle.com/en/virtualization/virtualbox/7.2/user/networkingdetails.html

Pereira, D. S., Bezerra, L. F. V., Nunes, J. S., Barroca Filho, I. M., y Lopes, F. A. S. (2023). Performance efficiency evaluation based on ISO/IEC 25010:2011 applied to a case study on load balance and resilient. En *Anais do XXIV Workshop de Testes e Tolerância a Falhas (WTF 2023)* (pp. 108–120). Sociedade Brasileira de Computação (SBC). https://doi.org/10.5753/wtf.2023.787

Prokhorenko, V., y Babar, M. A. (2020). Architectural resilience in cloud, fog and edge systems: a survey. *IEEE Access*, *8*, 28078–28095. https://doi.org/10.1109/ACCESS.2020.2971007

Rehman, A. U., Aguiar, R. L., y Barraca, J. P. (2022). Fault-tolerance in the scope of cloud computing. *IEEE Access*, *10*, 63422–63441. https://doi.org/10.1109/ACCESS.2022.3182211

Riabko, A. V., Vakaliuk, T. A., Zaika, O. V., Kukharchuk, R. P., y Kontsedailo, V. V. (2023). Investigating the effect of virtual machine migration accounting on reliability using a cluster model. *Journal of Edge Computing*, *2*(1), 37–63. https://doi.org/10.55056/jec.585

Samad, H., Hanizan, S. H., Din, R., Murad, R., y Tahir, A. (2018). Performance evaluation of web application server based on request bit per second and transfer rate parameters. *Journal of Physics: Conference Series*, *1018*, 012007.

https://doi.org/10.1088/1742-6596/1018/1/012007

Senevirathne, P., Cooray, S., Herath, J. D., y Fernando, D. (2024). Virtual machine proactive fault tolerance using log-based anomaly detection. *IEEE Access*, *12*, 178951–178970. https://doi.org/10.1109/ACCESS.2024.3506833

Shiozaki, K., y Nakamura, J. (2026). Dynamic tuning of election parameters for timely leader failover in state machine replication. *IEEE Access*, *14*, 128472–128487. https://doi.org/10.1109/ACCESS.2026.3724865

Su, X. (2026). Design and implementation of a high-availability network infrastructure for large-scale interactive e-learning. *Journal of Web Engineering*, *25*(4), 475–496. https://doi.org/10.13052/jwe1540-9589.2542

Su, X., y Li, X. (2021). Elastic performance test method of web server in cloud computing environment. *Journal of Web Engineering*, *20*(5), 1641–1658. https://doi.org/10.13052/jwe1540-9589.20514

Syed, D., Shaikh, G. M., Alshahrani, H. M., Hamdi, M., Alsulami, M., Shaikh, A., y Rizwan, S. (2024). A comparative analysis of metaheuristic techniques for high availability systems. *IEEE Access*, *12*, 7382–7398. https://doi.org/10.1109/ACCESS.2024.3352078

Talluri, S., Niewenhuis, D., Chu, X., Kyselica, J., Cetin, M., Balgavy, A., y Iosup, A. (2025). *Cloud uptime archive: Open-access availability data of web, cloud, and gaming services* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2504.09476

Tawfeeg, T. M., Yousif, A., Hassan, A., Alqhtani, S. M., Hamza, R., Bashir, M. B., y Ali, A. (2022). Cloud dynamic load balancing and reactive fault tolerance techniques: a systematic literature review (slr). *IEEE Access*, *10*, 71853–71873.

https://doi.org/10.1109/ACCESS.2022.3188645

Tran, M.-N., Vu, X. T., y Kim, Y. (2022). Proactive stateful fault-tolerant system for Kubernetes containerized services. *IEEE Access*, *10*, 102181–102194. https://doi.org/10.1109/ACCESS.2022.3209257

Villar-Martínez, A., García-Zubía, J., Angulo, I., y Rodríguez-Gil, L. (2021). Towards reliable remote laboratory experiences: a model for maximizing availability through fault-detection and replication. *IEEE Access*, *9*, 45032–45054. https://doi.org/10.1109/ACCESS.2021.3065742

Zaelani, C., y Suranegara, G. M. (2026). Performance evaluation of multi-cloud failover using domain name system. *Journal of Applied Informatics and Computing (JAIC)*, *10*(1), 910–922. https://jurnal.polibatam.ac.id/index.php/JAIC/article/view/11788