PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

ESCUELA HÁBITAT, INFRAESTRUCTURA Y CREATIVIDAD

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

Estrategia de Disaster Recovery mediante servidor con replicación [activo/pasivo] para la Unidad de Tecnologías del Hospital San Vicente de Paúl.

AUTOR. KIAN BENJAMIN TRUJILLO GROENOW

TUTOR: DIEGO FERNANDO BAROJA LLANOS

IBARRA – ECUADOR

JULIO, 2026

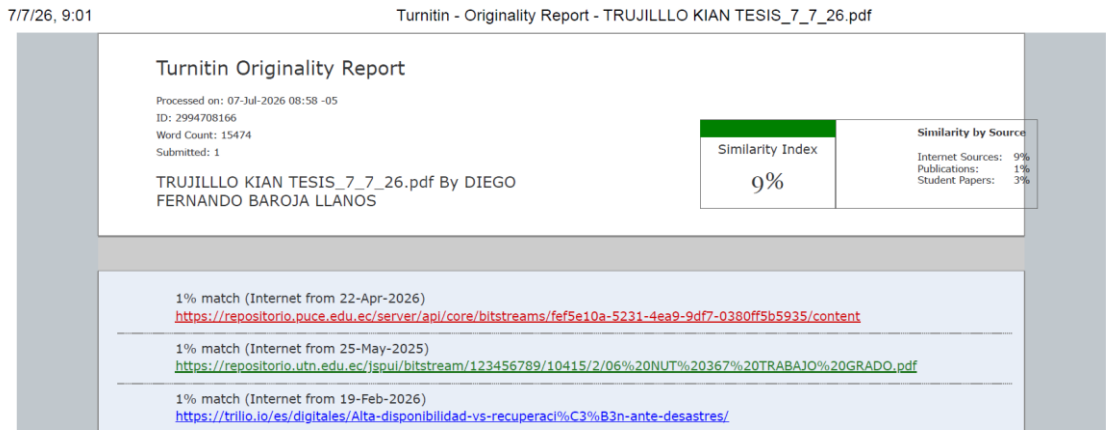
Ibarra, 01 de Julio del 2026.

Certificación tutor

En mi calidad de Tutor del Trabajo de Titulación titulado: "**Estrategia de Disaster Recovery mediante servidor con replicación activo/pasivo para la Unidad de Tecnologías del Hospital San Vicente de Paúl"**, presentado por el estudiante Kian Benjamin Trujillo Groenow con cédula de ciudadanía N°1004125983, para obtener el Título de Ingeniero en Tecnologías de la Información.

Certifico que el trabajo cumple con todos los parámetros establecidos, mediante el cual el estudiante demuestra el desarrollo de competencias en el campo de conocimiento de su profesión con un nivel de argumentación coherente, para ser sometido a la evaluación por parte de los lectores.

Adicionalmente, se adjunta el certificado de porcentaje de originalidad de TURNITIN.



Firmado digitalmente por1002402061
DIEGO FERNANDO BAROJA LLANOS
Motivo:Soy el autor de este documento
Fecha:2026-07-24 17:56-05:00

(f):_____

Msc. Diego Fernando Baroja Llanos

TUTOR DE TRABAJO

C.C.: 1002402061

Página de aprobación del tribunal

El tribunal examinador, aprueba el presente trabajo en nombre de la Pontificia Universidad Católica del Ecuador Ibarra:

Firmado digitalmente por1002402061
DIEGO FERNANDO BAROJA LLANOS
Motivo:Soy el autor de este documento
Fecha:2026-07-24 17:56-05:00

(f): ……

Msc. Diego Fernando Baroja Llanos

C.C.: 1002402061

GALO HERNAN PUETATE HUERA

Firmado digitalmente por GALO HERNAN PUETATE HUERA
Fecha: 2026.07.28 08:12:40 -05'00'

(f):……

Mgs. Galo Hernán Puetate Huera

C.C.: 0401375787

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JUAN CARLOS ARMAS CARDENAS

(f):……

Msc. Juan Carlos Armas Cardenas

C.C.: 1001685732

Acta de cesión de derechos

Yo Kian Benjamin Trujillo Groenow, declaro conocer y aceptar la disposición del Art. 165 del Código Orgánico de Economía Social de los Conocimientos, Creatividad e Innovación, que manifiesta textualmente: “Se reconoce facultad de los autores y demás titulares de derechos de disponer de sus derechos o autorizar las utilizaciones de sus obras o prestaciones a título gratuito y oneroso, según las condiciones que determinen. Esta facultad podrá ejercerse mediante licencias libres, abiertas y otros modelos alternativos de licenciamiento o la renuncia”.

Ibarra, 01 de Julio del 2026.

KIAN BENJAMIN TRUJILLO GROENOW
Digitally signed by KIAN BENJAMIN TRUJILLO GROENOW
Date: 2026.07.24 17:50:29 -05'00'

(f):_____

Kian Benjamin Trujillo Groenow

C.C.: 100412598-3

Autoría

Yo, Kian Benjamin Trujillo Groenow, portador de la cedula de ciudadanía N° 1004125983, declaro que el presente trabajo de investigación es de total responsabilidad del autor@, y eximo expresamente a la Pontificia Universidad Católica del Ecuador Ibarra de posibles reclamos o acciones legales.

KIAN BENJAMIN TRUJILLO GROENOW

Digitally signed by KIAN BENJAMIN TRUJILLO GROENOW
Date: 2026.07.24 17:50:44 -05'00'

(f):……..

Kian Benjamin Trujillo Groenow

C.C.: 100412598-3

Dedicatoria

Dedico el presente trabajo, en primer lugar, a nuestro Padre Celestial, por Su infinita misericordia, por guiar cada uno de mis pasos y por brindarme la fortaleza, sabiduría y perseverancia necesarias para culminar esta importante etapa de mi formación académica. Su amor y Su amparo han sido fundamentales en cada momento de este proceso, permitiéndome avanzar con fe, esperanza y confianza ante cada desafío.

A mi familia, expreso esta dedicatoria con profundo amor y gratitud, por haber sido el pilar fundamental a lo largo de mi vida y por brindarme su apoyo incondicional en cada etapa de mi formación personal y profesional. Su esfuerzo, comprensión, paciencia y confianza han sido esenciales para alcanzar esta meta, y constituyen una fuente constante de motivación para seguir adelante con responsabilidad, humildad y compromiso.

De manera muy especial, dedico este trabajo a mi abuela, quien ha sido una de las personas más significativas en mi vida. Su ejemplo de bondad, servicio y entrega hacia los demás dejó una huella imborrable en mi corazón. Siempre estuvo dispuesta a ayudar a quien lo necesitara, sin importar su condición, demostrando con sus acciones el valor del amor genuino y la solidaridad sincera. Su vida fue una enseñanza constante de generosidad, nobleza y compasión.

A ella, que me crio como si fuera mi madre, le debo gran parte de la persona que soy hoy. Su amor profundo, su cuidado desinteresado y sus sacrificios marcaron mi camino y me dieron la fortaleza necesaria para afrontar cada reto con valentía. Su presencia, sus enseñanzas y su ejemplo permanecerán siempre en mi memoria y en mi corazón, acompañándome en cada logro y en cada paso que dé en adelante.

Asimismo, dedico este trabajo a mis amigos, por su compañía, apoyo y palabras de aliento durante este recorrido académico. Su presencia en distintos momentos de este proceso fue valiosa y significativa, contribuyendo de una u otra manera a la culminación de esta meta.

Agradecimiento

Expreso mi más sincero agradecimiento a nuestro Padre Celestial, por Su amor, guía y fortaleza durante todo este proceso académico. Gracias a Su apoyo constante y a las bendiciones recibidas, fue posible superar cada dificultad y culminar satisfactoriamente esta etapa tan importante de mi formación.

A mi familia, por su apoyo incondicional, comprensión, sacrificio y confianza a lo largo de este camino. Su respaldo fue fundamental para continuar con perseverancia y compromiso en los momentos de mayor exigencia. Cada palabra de aliento, cada muestra de cariño y cada gesto de paciencia fueron una fuente constante de motivación para alcanzar esta meta.

De manera muy especial, agradezco a mi abuela, por su amor inmenso, por su ejemplo de vida y por haberme criado como si fuera su propio hijo. Su entrega, bondad y servicio hacia los demás dejaron en mí enseñanzas que trascenderán para siempre. Su memoria, su ternura y su fortaleza siguen siendo una inspiración permanente en mi vida, y este logro también le pertenece a ella.

A mis amigos, por su compañía, apoyo y ánimo en cada etapa de este proceso. Su cercanía y palabras de aliento hicieron más llevadero este recorrido académico y personal, por lo que siempre ocuparán un lugar especial en este logro.

A los docentes que contribuyeron en mi formación profesional, agradezco por sus conocimientos, orientación y exigencia académica, los cuales permitieron fortalecer mis capacidades y desarrollar este trabajo con mayor responsabilidad y compromiso.

Finalmente, agradezco al Hospital General San Vicente de Paúl por haberme permitido desarrollar este proyecto en sus instalaciones y por brindarme las facilidades necesarias para llevar a cabo esta investigación. Su colaboración fue esencial para el cumplimiento de los objetivos planteados y para la culminación de este trabajo académico.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

La presente investigación aborda la necesidad de fortalecer la continuidad operativa de los servicios informáticos críticos de la Unidad de Tecnologías del Hospital San Vicente de Paúl, ante el riesgo que representa la indisponibilidad de los sistemas y la pérdida de información en un entorno hospitalario donde los respaldos se realizan de forma manual. En este contexto, se propuso el diseño e implementación de una estrategia de Disaster Recovery basada en una arquitectura de servidor activo/pasivo, orientada a mejorar la capacidad de respuesta institucional frente a fallos tecnológicos y a reducir los tiempos de recuperación de los servicios esenciales. La metodología se fundamentó en la práctica de Gestión de la Continuidad del Servicio de TI de ITIL 4. Se partió de un análisis de impacto al negocio para identificar los sistemas críticos, establecer criterios de criticidad y definir los objetivos de recuperación (RTO y RPO). Posteriormente, se diseñó e implementó un laboratorio virtual con Proxmox VE, donde se configuró un clúster con nodos redundantes, almacenamiento compartido, replicación activo/pasivo y mecanismos de failover, con el propósito de validar el comportamiento técnico de la solución propuesta en un entorno controlado. Los resultados evidencian que la arquitectura implementada permite restablecer los servicios en un tiempo significativamente menor al de un esquema tradicional de respaldo manual, reduciendo la indisponibilidad y mejorando la capacidad de respuesta ante fallos del nodo principal. Asimismo, la validación técnica demostró que la replicación conserva una copia actualizada de la información y constituye una alternativa viable para fortalecer la continuidad operativa del hospital, sin necesidad de intervenir sobre el entorno de producción

Palabras clave: Disaster Recovery, Proxmox VE, continuidad del servicio, replicación, failover, RTO, RPO.

Abstract

This research addresses the need to strengthen the operational continuity of the critical information services of the Information Technology Unit of Hospital San Vicente de Paúl, considering the risk posed by system unavailability and information loss in a hospital environment where backups are performed manually. In this context, the design and implementation of a Disaster Recovery strategy based on an active/passive server architecture was proposed, aiming to improve institutional response capacity to technological failures and reduce recovery times for essential services. The methodology was based on the IT Service Continuity Management practice of ITIL 4, starting with a business impact analysis to identify critical systems, establish criticality criteria, and define recovery objectives such as RTO and RPO. Subsequently, a virtual laboratory was designed and implemented using Proxmox VE, where a cluster with redundant nodes, shared storage, active/passive replication, and failover mechanisms was configured in order to validate the technical behavior of the proposed solution in a controlled environment. The results show that the implemented architecture allows services to be restored in less time than a traditional manual backup scheme, reducing downtime and improving the response capacity in the event of a failure in the primary node. In addition, technical validation demonstrated that replication preserves a recent copy of the information and represents a viable alternative to strengthen the operational continuity of the hospital without intervening in the production environment.

Keywords: Disaster Recovery, Proxmox VE, service continuity, replication, failover, RTO, RPO.

Introducción

En el contexto actual de la gestión hospitalaria, la seguridad de la información y la continuidad operativa de los servicios tecnológicos se han convertido en componentes estratégicos para el funcionamiento institucional. La protección de los datos clínicos, administrativos y operativos no solo responde a requerimientos técnicos, sino también a la necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información vinculada con la atención de los pacientes, la gestión médica y la toma de decisiones. En este escenario, las estrategias de continuidad del negocio y recuperación ante desastres tecnológicos constituyen mecanismos indispensables para asegurar que los servicios críticos puedan mantenerse o restablecerse oportunamente frente a incidentes imprevistos.

En instituciones de salud públicas como el Hospital San Vicente de Paúl, ubicado en Ibarra, Ecuador, la dependencia de los sistemas de información y de la infraestructura tecnológica es cada vez mayor. La continuidad de procesos asistenciales, administrativos y de soporte depende del funcionamiento permanente de plataformas digitales utilizadas para la consulta de historias clínicas, la gestión de farmacia, el registro de procedimientos, la atención de urgencias y otras actividades esenciales. En consecuencia, la Unidad de Tecnologías de la Información adquiere un rol fundamental dentro de la operatividad hospitalaria, ya que una interrupción prolongada de sus servicios puede ocasionar retrasos en la atención, pérdida de información crítica y afectaciones directas a la seguridad del paciente y a la capacidad de respuesta institucional.

A pesar de esta dependencia tecnológica, persisten condiciones que incrementan la vulnerabilidad operativa del entorno informático hospitalario. Entre ellas se identifican el uso de esquemas tradicionales de respaldo, la ejecución manual de copias de seguridad, la existencia de puntos únicos de falla y la ausencia de una estrategia formal de recuperación ante desastres orientada a servicios críticos. Esta situación limita la capacidad de recuperación rápida frente a fallos de hardware, errores humanos, incidentes de ciberseguridad o eventos externos que comprometan la infraestructura tecnológica. Como consecuencia, el hospital se expone a periodos de indisponibilidad que pueden afectar la continuidad del servicio clínico y administrativo, así como a posibles pérdidas de información reciente que resultan especialmente sensibles en el ámbito de la salud.

Frente a esta problemática, la presente investigación se justifica desde múltiples dimensiones. Desde la perspectiva práctica, propone una solución aplicable para reducir tiempos de inactividad y minimizar la pérdida de datos en sistemas hospitalarios críticos. En el plano técnico, plantea una arquitectura de replicación activo/pasivo sobre Proxmox VE, complementada con mecanismos de monitoreo, sincronización y failover, orientados a fortalecer la resiliencia digital institucional. En el ámbito académico, el estudio aporta una experiencia documentada de diseño e implementación de una estrategia de Disaster Recovery en un contexto hospitalario público. Desde la dimensión social, la propuesta contribuye indirectamente a la continuidad de la atención y a la seguridad del paciente, al reducir el riesgo de interrupción de servicios que apoyan procesos clínicos esenciales.

A partir de lo anterior, se plantea como propósito general diseñar una estrategia de Disaster Recovery en el Hospital San Vicente de Paúl, estableciendo como objetivo general diseñar una estrategia de Disaster Recovery mediante un servidor con replicación virtual a través de una arquitectura activo/pasivo para garantizar la continuidad operativa de los sistemas críticos de la Unidad de Tecnologías de la Información del hospital. Como objetivos específicos se definieron tres: en primer lugar, analizar la infraestructura tecnológica y los procesos hospitalarios actuales para identificar los sistemas críticos, definir los niveles de tolerancia al riesgo y establecer los requisitos técnicos para la solución de Disaster Recovery; en segundo lugar, diseñar la arquitectura técnica de la solución basada en una replicación activo/pasivo, estableciendo los componentes, tecnologías y parámetros necesarios para cumplir los objetivos de recuperación (RTO y RPO); y en tercer lugar, validar la solución mediante la puesta en marcha de un servidor virtual con replicación activo/pasivo, verificando la conmutación por error (failover) y la efectividad del plan de recuperación.

El alcance del estudio se centra en el diseño, implementación y validación de una estrategia de Disaster Recovery en un entorno de laboratorio virtual controlado, orientado a comprobar la factibilidad técnica de la propuesta sin intervenir directamente sobre el entorno de producción hospitalario. La solución contempla la configuración de un clúster con nodos redundantes, almacenamiento compartido, replicación de máquinas virtuales y pruebas de failover para servicios priorizados según su criticidad. Entre las limitaciones del trabajo se encuentra precisamente que la validación se realizó en laboratorio y no sobre la infraestructura productiva del hospital, por lo que los resultados constituyen una

demostración técnica de viabilidad que deberá complementarse con decisiones institucionales para una eventual adopción operativa real.

Metodológicamente, el estudio adopta un enfoque mixto, de tipo aplicado, con alcance descriptivo y propositivo. La base metodológica principal es la práctica de Gestión de la Continuidad del Servicio de TI de ITIL 4, utilizada para orientar la identificación de servicios críticos, el análisis de impacto al negocio, la definición de objetivos de recuperación y la validación de la capacidad de respuesta ante interrupciones. El desarrollo técnico se organizó en fases de diagnóstico, diseño, implementación y pruebas, incorporando además historias de usuario y sprints como mecanismos de planificación y seguimiento de la ejecución dentro del laboratorio virtual.

Finalmente, el documento se estructura en tres capítulos principales. El primer capítulo presenta el estado del arte, los antecedentes y los conceptos teóricos que sustentan la investigación, entre ellos Disaster Recovery, alta disponibilidad, replicación, failover, RTO, RPO y continuidad del servicio. El segundo capítulo desarrolla los materiales y métodos, incluyendo el enfoque de investigación, la metodología adoptada, el análisis de criticidad hospitalaria, la especificación de requisitos y la planificación técnica del proyecto. El tercer capítulo expone los resultados de implementación y validación de la solución en el laboratorio virtual, así como el análisis del cumplimiento de los objetivos de recuperación definidos para los sistemas críticos considerados en el estudio.

Capítulo I

Estado del arte

1.1 Antecedentes de investigación

La relación entre los sistemas de información hospitalarios y la continuidad operativa ha evolucionado de manera significativa a lo largo de las últimas décadas. Durante los años noventa, los hospitales latinoamericanos comenzaron a experimentar las consecuencias directas de la dependencia tecnológica cuando desastres naturales de origen sísmico y climático inutilizaron infraestructuras físicas y funcionales en distintos países de la región. En ese contexto, organizaciones internacionales como la Organización Panamericana de la Salud promovieron los primeros diagnósticos de vulnerabilidad estructural y funcional en instituciones de salud, sentando las bases del concepto de hospital seguro (CIESS, 2016). Desde entonces, la preparación de los hospitales ha transitado desde un enfoque exclusivamente físico hacia uno integral, que incorpora los sistemas tecnológicos como un eje crítico de vulnerabilidad institucional que requiere estrategias específicas de protección y recuperación.

En ese proceso de evolución, la alta disponibilidad de los sistemas de información clínica comenzó a ser reconocida como una condición operativa indispensable. Un caso documentado que ilustra esta transición es el del Hospital Italiano de Buenos Aires, institución que en 1998 implementó un sistema de información clínica y que años después se vio en la necesidad de diseñar un entorno de alta disponibilidad para garantizar la continuidad del servicio las 24 horas del día. El estudio técnico derivado de esa experiencia señaló que el tiempo fuera de línea de un sistema informático en la capa asistencial no representa el mismo umbral de tolerancia que en el ámbito administrativo, y que, a mayor nivel de informatización de una institución, mayor es la dependencia de sus sistemas y más significativo el impacto organizacional y económico de sus interrupciones (González et al., 2026.). Este antecedente resulta pertinente para el presente proyecto, ya que el Hospital San Vicente de Paúl enfrenta un escenario comparable de dependencia tecnológica, donde cualquier interrupción no planificada puede comprometer directamente la atención a los pacientes.

En el ámbito científico, la preparación de los hospitales ante desastres ha adquirido carácter de imperativo institucional respaldado por evidencia empírica. Khirekar et al. (2023) realizaron una revisión sistemática sobre la preparación ante desastres en

hospitales, publicada en la revista Cureus e indexada en PubMed, en la que concluyeron que la preparación hospitalaria requiere un enfoque integral que involucra estrategias tecnológicas, capacitación del personal y participación comunitaria. Los autores determinaron que cuando ocurre un desastre tecnológico en un hospital se requiere acción rápida para mitigar sus efectos y reanudar las operaciones regulares, incluyendo la activación de sistemas de respaldo, la participación de especialistas en tecnología y la ejecución de planes de contingencia previamente validados. Asimismo, identificaron la asignación de recursos, la interoperabilidad de los sistemas de comunicación y la gestión de la infraestructura crítica como los principales desafíos que enfrentan los hospitales frente a eventos disruptivos (Khirekar et al., 2023). Este estudio refuerza la necesidad de contar con planes formalizados de recuperación ante desastres que integren no solo procedimientos manuales, sino también soluciones tecnológicas automatizadas y verificadas periódicamente.

En el contexto latinoamericano, la vulnerabilidad tecnológica de los hospitales ha cobrado mayor atención con el incremento de riesgos climáticos, sísmicos y sanitarios. La Organización Panamericana de la Salud advirtió que cuatro de cada diez establecimientos de salud en América Latina y el Caribe están expuestos a amenazas naturales, y que a medida que los desastres se vuelven más frecuentes y destructivos, los sistemas de salud pública deben estar preparados para responder y recuperarse garantizando la prestación ininterrumpida de servicios esenciales (OPS, 2025). En ese marco, la OPS impulsa la Iniciativa de Hospitales Resilientes, que ha beneficiado a más de 250 hospitales en 13 países y que promueve la adopción de tecnologías sostenibles, planes de gestión de emergencias y ejercicios de simulación periódica como pilares de la resiliencia institucional (OPS, 2025). Esta perspectiva refuerza la necesidad de que instituciones como el Hospital San Vicente de Paúl cuenten con estrategias formalizadas de Disaster Recovery que trasciendan los esquemas convencionales de respaldo y resguardo de información.

Desde una perspectiva técnica, IBM (2024) ha documentado que los sistemas de historia clínica electrónica constituyen un ejemplo paradigmático de aplicaciones de alta disponibilidad, que deben proporcionar información precisa y segura en cuestión de segundos, con un tiempo de inactividad prácticamente nulo, dada la naturaleza crítica y privada de ese tipo de información. Esta caracterización ilustra la exigencia operativa que enfrentan los departamentos de tecnología en los hospitales modernos, cuya tolerancia a

la interrupción es significativamente inferior a la de otros sectores productivos. Complementando esta perspectiva, Trilio (2025) señaló que estudios especializados en preparación ante desastres revelan que una proporción mayoritaria de las organizaciones no está adecuadamente preparada para responder ante eventos catastróficos, lo que pone de relieve la necesidad de una planificación de recuperación robusta y verificada periódicamente, combinada con medidas de alta disponibilidad que prevengan las interrupciones en condiciones operativas normales.

La continuidad operativa hospitalaria también ha sido analizada desde el enfoque de la gestión de riesgos y la planificación organizacional. La Organización Panamericana de la Salud (OPS) identificó cinco actividades clave para que los hospitales implementen planes de continuidad ante emergencias: el análisis del impacto en los servicios críticos, la evaluación de riesgos, la definición de estrategias y procedimientos, la organización de equipos de respuesta y la formulación de un plan verificado mediante pruebas periódicas (OPS, 2023). Estas actividades constituyen una guía metodológica aplicable tanto a la gestión física como tecnológica del riesgo, y su incorporación en el diseño de un proyecto de recuperación ante desastres garantiza que la solución sea sistemática, verificable y sostenible en el tiempo. La alineación de la presente propuesta con este marco metodológico fortalece su pertinencia técnica y su relevancia institucional en el contexto del Hospital San Vicente de Paúl.

La preparación ante desastres en salud también ha sido reconocida como una responsabilidad institucional que exige planificación anticipada y no únicamente reacción frente a incidentes ya ocurridos. La OPS definió el campo de preparación para desastres y emergencias en salud como el conjunto de conocimientos y capacidades orientados a anticipar, responder y recuperarse de forma efectiva ante los impactos de eventos de riesgo, y señaló que tanto los gobiernos como las organizaciones pueden llevar a cabo acciones de preparación para construir las capacidades necesarias y lograr una transición ordenada hacia la recuperación sostenida (OPS, 2026). Esta definición amplía el alcance del Disaster Recovery más allá de lo puramente tecnológico, vinculándolo con la capacidad institucional de respuesta, la formación del personal y la validación sistemática de los procesos de recuperación mediante ejercicios planificados.

En síntesis, los antecedentes revisados permiten establecer que la continuidad operativa de los sistemas de información hospitalarios ha pasado de ser una preocupación

secundaria a convertirse en un componente estratégico de la gestión en salud. La literatura y las guías técnicas coinciden en que una estrategia de Disaster Recovery debe estructurarse de manera metodológica, integrando la identificación de servicios críticos, la definición de objetivos RTO y RPO, la asignación de roles, la conmutación por error, y la validación mediante pruebas periódicas (Microsoft, 2025; IBM, 2024). Desde las experiencias pioneras documentadas en el Hospital Italiano de Buenos Aires hasta las directrices actuales sobre hospitales resilientes, existe una línea consistente que identifica la replicación, la virtualización y el failover automatizado como mecanismos clave para reducir la vulnerabilidad tecnológica en el sector salud (González Bernaldo de Quirós et al., s. f.; Khirekar et al., 2023; OPS, 2025). Estos antecedentes fundamentan la propuesta de este proyecto, que busca diseñar e implementar una estrategia de Disaster Recovery con arquitectura activo/pasivo para el Hospital San Vicente de Paúl, sustentada en una metodología técnica de análisis, configuración, prueba y validación

1.2 Conceptos clave

1.2.1 Disaster Recovery

El Disaster Recovery (DR) constituye el conjunto estructurado de políticas, procedimientos y tecnologías orientadas a restaurar los sistemas, aplicaciones y datos críticos de una organización tras un evento disruptivo de magnitud significativa. Su propósito central no se limita a recuperar información perdida, sino a garantizar que los servicios esenciales retornen a la operación dentro de parámetros de tiempo y pérdida de datos previamente definidos. IBM (2024) precisó que la recuperación ante desastres tiene como finalidad restaurar un sistema, una aplicación o todo un centro de datos para que vuelva a funcionar a pleno rendimiento tras una interrupción catastrófica, diferenciándola conceptualmente de la alta disponibilidad, que actúa en el plano preventivo. Trilio (2025) complementó esta definición señalando que los planes de DR son más amplios que las estrategias de HA porque se centran en restaurar datos y sistemas esenciales después de eventos catastróficos y cubren escenarios de falla total de infraestructura.

En el entorno hospitalario, esta disciplina adquiere una dimensión crítica porque la indisponibilidad de los sistemas de información puede comprometer directamente la seguridad del paciente, interrumpir la consulta de historias clínicas, paralizar la gestión de farmacia y afectar los procesos de toma de decisiones clínicas, razón por la que

Khirekar et al. (2023) enfatizaron que la implementación de planes de contingencia tecnológica es una obligación funcional en cualquier institución de salud.

La literatura técnica y las guías de arquitectura reconocen cinco arquitecturas principales de implementación de Disaster Recovery, cada una con diferentes niveles de inversión, complejidad y objetivos de recuperación (RTO/RPO). Estas arquitecturas se distribuyen en un espectro que va desde la mayor simplicidad y menor costo hasta máxima disponibilidad y mayor complejidad operativa, permitiendo a las organizaciones elegir la estrategia más apropiada según sus necesidades de continuidad operativa y restricciones presupuestarias.

1.2.2 Arquitecturas de Disaster Recovery

El modelo Backup & Restore constituye el nivel más básico y económico de implementación de Disaster Recovery. Este enfoque se basa en realizar copias de seguridad periódicas de los datos y sistemas, almacenándolas en un sitio geográficamente remoto o en medios separados del entorno de producción. AWS (2023) describe que esta estrategia es la más sencilla en términos de implementación y mantenimiento, pero implica los tiempos de recuperación más prolongados, siendo ideal para datos no críticos o aplicaciones que pueden tolerar interrupciones de varias horas sin comprometer significativamente las operaciones. En contextos hospitalarios, esta arquitectura es aplicable a datos históricos, archivos administrativos o sistemas secundarios, pero no es adecuada para sistemas de misión crítica como historias clínicas electrónicas o gestión de urgencias. Microsoft (2025) indicó que el Backup & Restore típicamente ofrece un RTO de horas a días y un RPO de horas, lo que significa que la organización puede perder desde minutos hasta horas de información según la frecuencia de las copias de seguridad ejecutadas.

Activo-Activo (Multi-sitio)

La arquitectura Activo-Activo, también denominada multi-sitio o hot-hot, mantiene múltiples sitios funcionando a plena capacidad simultáneamente, replicando datos en tiempo real entre ellos. AWS (2023) explicó que en esta configuración cada sitio procesa parte del tráfico de producción, y si uno falla, el otro continúa sirviendo a todos los usuarios sin interrupción perceptible. Esta estrategia ofrece el menor tiempo de recuperación posible, con RTO prácticamente cercano a cero segundos, pero requiere sincronización compleja de datos, orquestación avanzada y gestión de consistencia

distribuida. Aunque Activo-Activo proporciona máxima resiliencia, su costo operativo es considerablemente más elevado, pues mantiene infraestructura duplicada en operación permanente. En el contexto hospitalario, esta arquitectura se justifica únicamente para sistemas de criticidad extrema donde cualquier interrupción, incluso de segundos, pueda comprometer vidas. Para el Hospital San Vicente de Paúl, dado su perfil de institución de mediano tamaño con restricciones presupuestarias, esta arquitectura no resulta viable como solución general.

1.2.3 Alta disponibilidad

La alta disponibilidad (HA) es la capacidad de un sistema de información para permanecer operativo de manera continua, minimizando las interrupciones planificadas y no planificadas mediante mecanismos de redundancia, replicación y recuperación automática. Trilio (2025) la definió como un enfoque esencial del diseño de sistemas que garantiza un rendimiento operativo constante y un tiempo de actividad que con frecuencia alcanza el 99,999% conocido como "cinco nueves", lo que equivale a un tiempo máximo de inactividad de tan solo 5,26 minutos al año. IBM (2024) añadió que el principal objetivo de la alta disponibilidad es eliminar posibles puntos de fallo en una infraestructura informática, de modo que las aplicaciones críticas continúen funcionando incluso ante fallos parciales de hardware o software. En el sector salud, los sistemas de historia clínica electrónica, los módulos de laboratorio y los servicios de urgencias son aplicaciones que exigen este nivel de disponibilidad, ya que su caída puede derivar en retrasos críticos y en decisiones clínicas comprometidas por falta de información oportuna.

La relación entre la alta disponibilidad y el Disaster Recovery es de complementariedad estructural: mientras la HA tiene como finalidad prevenir las interrupciones en condiciones operativas cotidianas, el DR proporciona el mecanismo estructurado de respuesta cuando dichas interrupciones, inevitables en determinados escenarios, ya han ocurrido. Trilio (2025) precisó que la combinación de ambas estrategias crea una defensa robusta contra diversas amenazas a la infraestructura de TI, donde la HA garantiza la tolerancia inmediata a fallos y el DR ofrece capacidades de recuperación a largo plazo frente a eventos catastróficos. IBM (2024) refuerza este planteamiento al señalar que una estrategia de resiliencia tecnológica sólida debe incluir la alta disponibilidad para operaciones de rutina y el Disaster Recovery para situaciones extremas, como premisa de

diseño no como opción. Esta complementariedad es el fundamento técnico central de la presente propuesta para el Hospital San Vicente de Paúl.

1.2.4 Arquitectura activo/pasivo

La arquitectura activa/pasivo es un modelo de redundancia que implementa la estrategia Warm Standby, en el cual un servidor primario denominado nodo activo procesa la totalidad de la carga operativa, mientras un servidor secundario denominado nodo pasivo permanece en estado de espera manteniendo una réplica actualizada de los datos y servicios. Ante una falla detectada en el nodo principal, el nodo pasivo asume automáticamente la operación mediante un proceso de conmutación por error denominado failover. IberaSync (2021) explicó que en este modelo el nodo primario es el único que procesa solicitudes y se encarga de actualizar a los nodos secundarios, de modo que, si deja de funcionar, uno de los secundarios puede asumir el rol de primario sin pérdida significativa de servicio; señaló además que la elección de esta arquitectura sobre modelos más complejos como el activo/activo depende de las necesidades del sistema y de la tolerancia organizacional al costo y a la complejidad operativa. Trilio (2025) complementó esta perspectiva al indicar que las configuraciones de HA con conmutación por error buscan reacciones casi instantáneas ante fallos, que típicamente se miden en segundos o milisegundos. Para instituciones hospitalarias con restricciones presupuestarias como el Hospital San Vicente de Paúl, el modelo activo/pasivo representa un equilibrio técnico y económico adecuado entre nivel de disponibilidad, costo de implementación y facilidad de mantenimiento sostenido, permitiendo implementar la estrategia de Disaster Recovery al nivel Warm Standby.

1.2.5 Replicación de datos

La replicación de datos es el proceso mediante el cual se mantiene una copia actualizada o casi actualizada de la información en uno o más servidores de respaldo, con el fin de garantizar disponibilidad, integridad y capacidad de recuperación rápida ante fallos del sistema principal. Dependiendo de los requisitos de la solución, la replicación puede clasificarse en dos modalidades: síncrona y asíncrona. En la replicación síncrona, una operación de escritura se confirma simultáneamente en el servidor primario y en el secundario antes de considerarse exitosa, lo que garantiza coherencia total entre nodos, pero puede incrementar la latencia de las transacciones debido al tiempo de propagación en red. En la replicación asíncrona, los datos se transfieren al nodo secundario con un

desfase temporal controlado, lo que mejora el rendimiento operativo, pero introduce una ventana potencial de pérdida de información acotada por el intervalo de replicación. LogicalDoc (2025) señaló que la arquitectura de alta disponibilidad también se utiliza para implementar estrategias de Disaster Recovery cuyo propósito es garantizar la supervivencia del servicio incluso ante un evento grave en el nodo principal. En el contexto de este proyecto, la replicación activa/pasivo implementada sobre Proxmox VE permite sincronizar de forma continua el estado del servidor principal con el servidor pasivo, asegurando que la transición ante una falla sea rápida y con mínima pérdida de información cuantificable.

1.2.6 RTO: Objetivo de punto de recuperación

El Objetivo de Punto de Recuperación (RTO) es una métrica de planificación que expresa el tiempo máximo tolerable durante el cual un sistema o servicio puede permanecer inactivo después de un incidente disruptivo sin generar consecuencias inaceptables para la organización. En términos operativos, el RTO define el umbral de tolerancia frente a la interrupción, es decir, el plazo dentro del cual los servicios críticos deben ser recuperados para evitar impactos graves en la continuidad del negocio. Microsoft (2024) subrayó que el RTO es uno de los parámetros fundamentales que deben establecerse antes de seleccionar la estrategia tecnológica de DR, ya que determina si la organización requiere restauración convencional desde copias de seguridad, alta disponibilidad con failover automático, o una combinación de ambas estrategias.

La selección de la arquitectura de DR (Backup & Restore, Pilot Light, Warm Standby, o Activo-Activo) está directamente vinculada al RTO definido: Backup & Restore proporciona RTO de horas a días, Pilot Light ofrece RTO de decenas de minutos, Warm Standby logra RTO de minutos, mientras que Activo-Activo alcanza RTO prácticamente cercano a cero (Trilio, 2025). Trilio (2025) complementó señalando que mientras los sistemas de HA buscan reacciones en segundos o milisegundos, los procesos de recuperación ante desastres pueden implicar períodos más extensos de horas a días dependiendo de la severidad del incidente y la arquitectura seleccionada, lo que hace imprescindible definir claramente el RTO para cada servicio y seleccionar la arquitectura más adecuada para cumplirlo. En un hospital, los sistemas de mayor criticidad, como la historia clínica electrónica o la gestión de urgencias, requieren un RTO extremadamente

bajo (minutos), lo que justifica plenamente el diseño propuesto en este proyecto mediante arquitectura Warm Standby con failover automático.

1.2.7 RPO: Objetivo de punto de recuperación

El Objetivo de Punto de Recuperación (RPO) es la métrica que indica el volumen máximo de datos que una organización puede perder sin comprometer de manera inaceptable su operación. A diferencia del RTO, que mide el tiempo de inactividad tolerable, el RPO mide la ventana temporal de pérdida de información admisible, estableciendo hasta qué punto en el tiempo deben recuperarse los datos para que la organización pueda reanudar su funcionamiento con normalidad. Microsoft (2024) indicó que el RPO y el RTO son los dos indicadores clave que guían el diseño de cualquier solución de Disaster Recovery, y que su correcta definición permite seleccionar las tecnologías y estrategias de replicación más adecuadas según la criticidad de cada servicio.

La interrelación entre ambas métricas determina directamente la inversión tecnológica requerida y la arquitectura viable: Backup & Restore proporciona RPO de horas (dependiendo de la frecuencia de copias); Pilot Light logra RPO de minutos mediante replicación continua; Warm Standby con replicación síncrona puede alcanzar RPO cercano a cero; mientras que Activo-Activo garantiza RPO prácticamente cero (Trilio, 2025). En un entorno hospitalario, un RPO elevado podría significar la pérdida de registros de medicación, resultados de laboratorio o procedimientos clínicos documentados horas antes del incidente, lo que justifica plenamente el diseño de mecanismos de replicación continua como los implementados en arquitectura Warm Standby orientados a minimizar esa ventana de riesgo operativo y garantizar integridad de datos clínicos.

1.2.8 Failover

El failover es el proceso mediante el cual la carga de trabajo y el control operativo de un servicio se transfieren automáticamente desde el servidor primario hacia el servidor secundario en cuanto el sistema detecta una falla en el primero. Este mecanismo constituye el componente central de las arquitecturas activo/pasivo, ya que determina la velocidad y la transparencia con que el servicio se restablece para los usuarios finales. Trilio (2025) precisó que la automatización de los procesos de conmutación por error puede reducir sustancialmente el tiempo de recuperación y disminuir las posibilidades de error humano durante una crisis, y que un clúster de servidores correctamente configurado

puede activar el failover en milisegundos después de detectar una falla en el servidor principal. IBM (2024) reforzó este planteamiento al señalar que la eliminación de puntos únicos de fallo y la automatización del failover son los dos principios de diseño fundamentales para lograr alta disponibilidad real en sistemas críticos. En el contexto hospitalario, un proceso de failover correctamente configurado y probado periódicamente permite que los sistemas críticos retomen su funcionamiento en minutos sin intervención manual extensa, lo cual es determinante para mantener la continuidad de la atención clínica y la integridad de los datos del paciente.

1.2.9 Virtualización

La virtualización es la tecnología que permite crear entornos de cómputo simulados denominados máquinas virtuales sobre una plataforma de hardware físico compartido, separando los recursos lógicos del sustrato físico que los soporta. Esta capacidad facilita la consolidación de servidores, la migración de cargas de trabajo entre nodos físicos y la automatización de los procesos de recuperación ante fallos.

En el contexto del Disaster Recovery hospitalario, la virtualización actúa como un habilitador técnico fundamental porque permite replicar máquinas virtuales completas hacia el nodo pasivo, reiniciarlas en cuestión de minutos y orquestar el proceso de failover de manera estructurada y reproducible. LogicalDoc (2025) indicó que la arquitectura de alta disponibilidad se construye precisamente sobre la capacidad de los nodos de replicar servicios activos y asumir la operación sin intervención manual cuando el nodo principal falla, lo que convierte a la virtualización en el sustrato técnico imprescindible para implementar soluciones de HA y DR de forma eficiente. Para este proyecto, Proxmox VE constituye la plataforma de virtualización seleccionada: es una solución de código abierto basada en Debian que integra virtualización KVM, contenedores LXC, gestión de clústeres, replicación de máquinas virtuales y configuración nativa de alta disponibilidad, características que la hacen idónea para el entorno técnico y presupuestario del Hospital San Vicente de Paúl.

1.2.10 Metodología de diseño e implementación de Disaster Recovery

La implementación de una estrategia efectiva de Disaster Recovery requiere seguir una metodología estructurada que asegure que la solución sea sistemática, verificable y adaptada a las necesidades reales de la organización. En este proyecto, dicha metodología se articula con la práctica de gestión de continuidad del servicio de ITIL 4,

complementada con lineamientos técnicos de diseño, implementación y validación de soluciones de replicación y recuperación:

- Paso 1: Análisis de Riesgos y Vulnerabilidades: Corresponde identificar todas las amenazas potenciales que podrían comprometer la continuidad operativa del Hospital San Vicente de Paúl, incluyendo desastres naturales (sísmicos, climáticos), fallas de hardware, error humano, ciberataques e interrupciones de servicios externos. Este análisis debe cuantificar la probabilidad de ocurrencia y el impacto potencial de cada amenaza sobre los servicios críticos, permitiendo priorizar las medidas de protección más efectivas.

- Paso 2: Definición de RTO y RPO: Cada servicio crítico debe tener definidos explícitamente sus objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO) en función de su impacto en la continuidad del negocio hospitalario. Esta definición debe hacerse en colaboración entre áreas técnicas, clínicas y administrativas, asegurando que los objetivos sean técnicamente alcanzables y económicamente viables.

- Paso 3: Priorización de Aplicaciones y Servicios: No todos los servicios requieren el mismo nivel de DR. La metodología incluye clasificar los sistemas según su criticidad operativa y su impacto en la atención al paciente. Historia clínica electrónica, farmacia y urgencias son prioritarios, mientras que sistemas administrativos secundarios pueden tolerar mayor tiempo de inactividad. Esta clasificación determina qué arquitectura se asigna a cada servicio (Backup & Restore vs. Warm Standby vs. Activo-Activo).

- Paso 4: Documentación y Automatización: La solución de DR debe estar completamente documentada en procedimientos técnicos verificables, con especificación clara de: roles y responsabilidades, pasos de activación del failover, rutas de escalación, y criterios de decisión. Estos procedimientos deben incorporar automatización máxima para reducir la intervención humana durante una crisis, incluyendo scripts de orquestación, monitoreo de salud de servicios y conmutación automática.

- Paso 5: Prueba, Validación y Entrenamiento: Ningún plan de DR es efectivo sin validación periódica. La metodología requiere ejecutar simulacros controlados (disaster recovery drills) donde se prueba la activación del failover, se valida que los datos se recuperan correctamente, y se entrena al personal en los procedimientos. Estas pruebas deben ejecutarse al menos semestralmente, con documentación de hallazgos y correcciones implementadas.

1.2.11 Continuidad del negocio

La continuidad del negocio se refiere a la capacidad de una organización para sostener sus funciones esenciales durante y después de un evento disruptivo, y para retornar a la normalidad operativa en el menor tiempo posible minimizando el impacto sobre sus servicios. En el sector salud, esta continuidad no es una aspiración opcional, sino una obligación funcional vinculada directamente a la seguridad del paciente, la accesibilidad de la información clínica y la integridad de los procesos asistenciales. La OPS (2023) definió la continuidad operativa hospitalaria como un proceso que implica el análisis del impacto en servicios críticos, la evaluación de riesgos, la definición de estrategias y procedimientos, la organización de equipos de respuesta y la formulación de planes verificados mediante pruebas periódicas; señalando que el objetivo final es asegurar que los hospitales no interrumpan sus servicios esenciales durante situaciones de emergencia.

La OPS (2016) añadió que la resiliencia de un sistema de salud puede entenderse como su capacidad de absorber perturbaciones, responder eficazmente ante ellas y recuperarse manteniendo sus funciones esenciales, lo que implica que la resiliencia tecnológica es un componente ineludible de la resiliencia institucional global. Estos conceptos convergen en la propuesta de este proyecto: la implementación de una estrategia de Disaster Recovery con replicación activo/pasivo (Warm Standby) no solo minimiza los tiempos de inactividad tecnológica, sino que fortalece estructuralmente la capacidad del Hospital San Vicente de Paúl para garantizar la continuidad de sus servicios críticos frente a cualquier tipo de contingencia, colocando la resiliencia digital al servicio de la seguridad del paciente.

1.2.12 ITIL 4 y la gestión de continuidad del servicio de TI

ITIL 4 incorpora la gestión de continuidad del servicio de TI como una práctica orientada a asegurar que los servicios tecnológicos puedan seguir operando o ser recuperados

oportunamente ante interrupciones significativas. Esta práctica no se limita a la respuesta técnica frente a un incidente, sino que forma parte de un enfoque integral de gestión de servicios que considera la evaluación de riesgos, la identificación de servicios críticos, la definición de requisitos de recuperación y la preparación de planes y capacidades de respuesta.

En el contexto de ITIL 4, la continuidad del servicio se relaciona directamente con el análisis del impacto al negocio, ya que permite determinar cuáles servicios son prioritarios, qué nivel de interrupción es aceptable y qué objetivos de recuperación deben cumplirse. A partir de ese análisis, se establecen parámetros como el RTO y el RPO, que orientan la selección de la estrategia tecnológica más adecuada para sostener la operación institucional. En consecuencia, la continuidad del servicio no debe entenderse como una actividad aislada, sino como una práctica de soporte para la resiliencia organizacional y la protección de los servicios esenciales.

Para este proyecto, ITIL 4 constituye el marco metodológico que justifica la selección de una estrategia de Disaster Recovery basada en una arquitectura activo/pasivo. En particular, la práctica de continuidad del servicio respalda la necesidad de definir servicios críticos de la Unidad de Tecnologías del Hospital San Vicente de Paúl, analizar sus dependencias tecnológicas, establecer objetivos de recuperación realistas y validar la solución mediante pruebas en un laboratorio virtual controlado. De esta manera, el proyecto articula la perspectiva de gestión de servicios con la implementación técnica de la replicación sobre Proxmox VE.

Además, ITIL 4 enfatiza que las capacidades de continuidad deben ser planificadas, probadas y mejoradas de forma continua. Por ello, la estrategia propuesta en esta investigación incorpora actividades de análisis, diseño, implementación, verificación y validación, alineadas con la lógica de mejora continua de la gestión de servicios. Esta alineación permite que la solución no solo funcione técnicamente, sino que también responda a una necesidad organizacional concreta de continuidad operativa, protección de datos y reducción del impacto ante incidentes disruptivos.

Capítulo II
Materiales y métodos

El presente capítulo expone los materiales, técnicas y procedimientos metodológicos utilizados para el diseño e implementación de una estrategia de Disaster Recovery mediante una arquitectura de replicación activo/pasivo en la Unidad de Tecnologías de la Información del Hospital San Vicente de Paúl. En un primer momento, se presentan las generalidades de la investigación, incluyendo el enfoque, tipo de estudio, población, técnicas e instrumentos aplicados para el levantamiento de información. Seguidamente, se detalla la metodología técnica adoptada para la solución, sustentada exclusivamente en la práctica de gestión de continuidad del servicio de ITIL 4, la cual orienta la identificación de servicios críticos, el análisis de impactos, la definición de requisitos de recuperación y la validación de la capacidad de restablecimiento ante incidentes disruptivos. Bajo este marco, el proceso metodológico se organiza en fases de diagnóstico, diseño, implementación y validación, permitiendo construir una propuesta técnicamente coherente, reproducible y alineada con las necesidades operativas de la institución hospitalaria.

2.1 Aspectos generales de la investigación

El presente trabajo de titulación se desarrolla en la Unidad de Tecnologías de la Información del Hospital San Vicente de Paúl, ubicado en la ciudad de Ibarra, provincia de Imbabura, Ecuador. La investigación tiene como propósito diseñar e implementar una estrategia de Disaster Recovery mediante una arquitectura de replicación activo/pasivo, con el fin de garantizar la continuidad operativa de los sistemas críticos hospitalarios ante eventos disruptivos.

2.1.1 Enfoque y tipo de investigación

El presente trabajo adopta un enfoque mixto, combinando elementos cualitativos y cuantitativos. El enfoque cualitativo permite comprender el contexto operativo de la Unidad de Tecnologías mediante revisión documental, entrevistas al personal técnico y listas de verificación, con el propósito de identificar los sistemas críticos, los procesos hospitalarios y los puntos únicos de falla existentes en la infraestructura tecnológica actual. El enfoque cuantitativo se aplica para recopilar y analizar métricas de tiempo de respuesta ante incidentes, frecuencia de fallos, historial de respaldos e indicadores de

rendimiento del sistema, especialmente los objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO).

En el componente cuantitativo del diagnóstico se analizaron las bitácoras de incidencias y el historial de respaldos correspondientes al período comprendido entre febrero del 2026 y junio del 2026, abarcando los registros disponibles relacionados con tiempos de respuesta, eventos de indisponibilidad y ejecución de copias de seguridad. Esta delimitación permitió caracterizar con mayor precisión la situación operativa inicial de la Unidad de Tecnologías de la Información y establecer una base objetiva para la definición de los parámetros de recuperación del proyecto.

El tipo de investigación es aplicada, ya que busca resolver una problemática concreta identificada en el Hospital San Vicente de Paúl, relacionada con la ausencia de una estrategia formal de recuperación ante desastres. Su alcance es descriptivo, porque caracteriza la infraestructura tecnológica actual y los servicios críticos, y propositivo, porque plantea una solución técnica estructurada para fortalecer la continuidad operativa y la resiliencia digital institucional.

2.1.2 Procedimiento de investigación

Para el levantamiento de información se aplicaron las siguientes técnicas e instrumentos:

Revisión documental: análisis de inventarios de hardware, registros de incidencias, bitácoras de mantenimiento y políticas internas de TI del hospital.

Lista de verificación (Checklist): aplicada al personal de la Unidad de Tecnologías para identificar los servicios críticos, la topología de red actual y las capacidades de respaldo existentes.

Observación técnica directa: inspección de la infraestructura física y virtual del servidor principal, con el fin de caracterizar el entorno operativo antes de la implementación.

Matriz de evaluación tecnológica: utilizada para seleccionar la herramienta de virtualización y replicación más adecuada (Proxmox VE), considerando criterios de costo, compatibilidad, rendimiento y soporte comunitario.

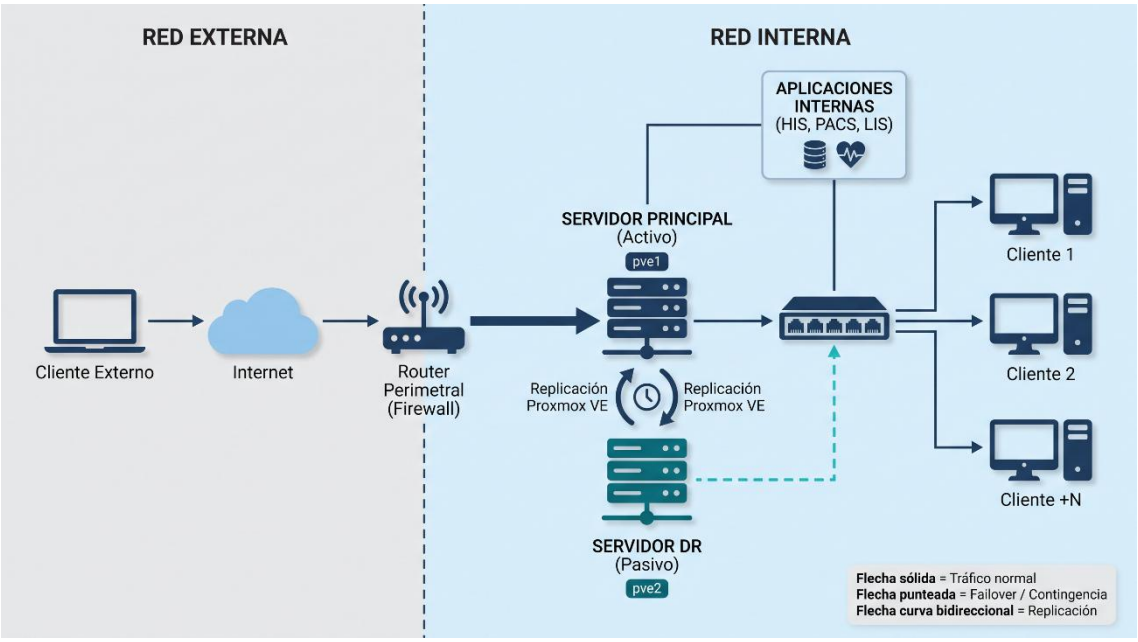
2.2 Metodología del proyecto

Para la ejecución técnica del proyecto se adopta como base metodológica la práctica de gestión de continuidad del servicio de ITIL 4, la cual orienta la identificación de servicios

críticos, la evaluación de riesgos e impactos, la definición de objetivos de recuperación y la validación de la capacidad de respuesta ante interrupciones. Esta metodología permite estructurar de manera ordenada el diseño e implementación de la estrategia de Disaster Recovery, asegurando que la solución propuesta responda a las necesidades operativas del Hospital San Vicente de Paúl y contribuya al fortalecimiento de la continuidad del servicio tecnológico.

Si bien la fundamentación metodológica del proyecto se sustenta en la práctica de Gestión de la Continuidad del Servicio de TI de ITIL 4, para la organización operativa de las actividades de diagnóstico, diseño e implementación se incorporaron elementos de gestión ágil, específicamente historias de usuario y sprints. Esta combinación no modifica el marco metodológico principal del estudio, sino que facilita la planificación secuencial de tareas, la priorización de requerimientos y el control del avance técnico del proyecto. En este sentido, ITIL 4 orienta la lógica de continuidad del servicio, análisis de criticidad, definición de RTO y RPO, mientras que el enfoque ágil se emplea únicamente como herramienta de estructuración y seguimiento de la ejecución técnica dentro del laboratorio virtual.

Figura 1 Flujo metodológico para la estrategia de Disaster Recovery.



La figura 1 representa el flujo metodológico aplicado en el proyecto, basado en la práctica de gestión de continuidad del servicio de ITIL 4. El esquema muestra la secuencia de actividades desarrolladas para identificar los servicios críticos, analizar la situación

actual, diseñar la arquitectura activo/pasivo, implementar la solución y validar su funcionamiento mediante pruebas controladas.

Bajo este enfoque, el proceso metodológico se organiza en cuatro fases: diagnóstico de la situación actual, diseño de la arquitectura de recuperación, implementación de la solución y pruebas de validación. Cada fase se ejecuta de forma secuencial y documentada, con el fin de establecer una solución técnicamente coherente, verificable y alineada con las buenas prácticas de continuidad del servicio establecidas por ITIL 4.

2.2.1 Especificación de requisitos

Los requisitos funcionales definen las capacidades operativas que la solución de Disaster Recovery debe cumplir para garantizar la continuidad de los sistemas críticos del Hospital San Vicente de Paúl:

Tabla 1. Requisitos funcionales.

ID	Nombre	Descripción
RF01	Replicación de máquinas virtuales	El sistema debe replicar las máquinas virtuales del servidor primario (activo) hacia el servidor secundario (pasivo) de forma continua mediante Proxmox VE Replication.
RF02	Failover automático	Ante la caída del servidor primario, el sistema debe activar automáticamente el servidor pasivo en un tiempo máximo definido por el RTO establecido.
RF03	Sincronización de datos	El sistema debe sincronizar los datos críticos entre nodos con una frecuencia configurable, garantizando un RPO mínimo.
RF04	Monitoreo de estado de nodos	El sistema debe monitorear en tiempo real el estado de salud de ambos nodos (activo y pasivo) y generar alertas ante fallos detectados.
RF05	Ejecución de pruebas de recuperación	El sistema debe permitir la simulación de escenarios de fallo (DR drills) para validar la efectividad del plan de recuperación sin interrumpir los servicios productivos.
RF06	Restauración de servicios críticos	El sistema debe ser capaz de restaurar los servicios críticos identificados (HIS, gestión de farmacia,

		historias clínicas) en el nodo pasivo dentro del RTO acordado.
RF07	Registro de eventos y bitácora	El sistema debe registrar automáticamente todos los eventos de replicación, failover y restauración en una bitácora técnica auditables.

La tabla1 presenta siete requisitos funcionales (RF01-RF07) para un sistema de alta disponibilidad basado en Proxmox VE, abarcando replicación continua de máquinas virtuales y failover automático entre nodos activo y pasivo. El sistema debe sincronizar datos críticos con frecuencia configurable y monitorear en tiempo real el estado de salud de ambos servidores, generando alertas ante fallos detectados.

Los requisitos no funcionales establecen los atributos de calidad y las restricciones técnicas que debe cumplir la solución implementada:

Tabla 2. Requisitos no funcionales.

ID	Categoría	Descripción
RNF01	Disponibilidad	La arquitectura activo/pasivo debe garantizar una disponibilidad objetivo de al menos 99.9% para los sistemas críticos del hospital.
RNF02	Rendimiento	La replicación de datos no debe degradar el rendimiento del servidor primario más de un 15% durante las ventanas de sincronización.
RNF03	Seguridad	La comunicación entre el nodo activo y el pasivo debe estar cifrada para proteger la integridad y confidencialidad de los datos clínicos transmitidos.
RNF04	Escalabilidad	La solución debe ser escalable, permitiendo incorporar nuevas máquinas virtuales al esquema de replicación sin rediseñar la arquitectura base.
RNF05	Mantenibilidad	La plataforma Proxmox VE debe permitir la administración centralizada de ambos nodos desde una consola web única, facilitando el mantenimiento por parte del personal técnico del hospital.
RNF06	Compatibilidad	La solución debe ser compatible con el hardware existente en la Unidad de Tecnologías del Hospital San Vicente de

		Paúl y con los sistemas operativos de las máquinas virtuales críticas.
RNF07	Recuperabilidad	El RTO objetivo no debe superar los 15 minutos y el RPO no debe exceder 1 hora para los servicios críticos identificados.

La tabla 2 detalla siete requisitos no funcionales (RNF01-RNF07) que definen las características de calidad del sistema de alta disponibilidad. En disponibilidad, se exige un 99.9% para los sistemas críticos del hospital, mientras que el rendimiento no debe degradarse más de un 15% durante la replicación. La seguridad requiere cifrado en la comunicación entre nodos para proteger datos clínicos, y la escalabilidad permite incorporar nuevas máquinas virtuales sin rediseñar la arquitectura.

2.2.2 Desarrollo

El desarrollo técnico de la solución se organiza en cuatro fases secuenciales, alineadas con la práctica de gestión de continuidad del servicio de ITIL 4. Este enfoque permite estructurar el trabajo desde el diagnóstico inicial hasta la validación final de la estrategia de Disaster Recovery, asegurando coherencia entre los requerimientos identificados, el diseño de la arquitectura y las pruebas de funcionamiento.

Fase 1: Diagnóstico y levantamiento de información

Esta fase tiene como objetivo caracterizar la infraestructura tecnológica actual del Hospital San Vicente de Paúl e identificar los servicios críticos que deben ser protegidos por la estrategia de Disaster Recovery. Las actividades principales comprenden el levantamiento del inventario de hardware y software del entorno existente, la identificación de los sistemas y aplicaciones críticas, la revisión de registros de incidencias y tiempos de recuperación, y el análisis del impacto que tendría una interrupción sobre los procesos hospitalarios. Como resultado de esta fase, se establecen los requisitos iniciales de continuidad, incluyendo la priorización de servicios y la definición preliminar de los objetivos de recuperación RTO y RPO.

Fase 2: Diseño de la arquitectura

En esta fase se elabora el diseño lógico y físico de la solución de Disaster Recovery con arquitectura activo/pasivo. A partir de los requisitos identificados en la fase anterior, se define la topología de red, el esquema de replicación, el dimensionamiento del servidor

pasivo, el procedimiento de failover y failback, y el diseño del plan de pruebas. Asimismo, se establecen los parámetros técnicos que permitirán validar el cumplimiento de los objetivos de recuperación y garantizar la viabilidad operativa de la propuesta.

Fase 3: Implementación y configuración

Esta fase comprende la instalación, configuración e integración de los componentes tecnológicos definidos en el diseño. La herramienta central es Proxmox VE, plataforma de virtualización de código abierto basada en Debian GNU/Linux que integra capacidades de gestión de máquinas virtuales, contenedores y replicación entre nodos. Las actividades incluyen la configuración del entorno de virtualización, la preparación del nodo pasivo, la creación y asignación de las máquinas virtuales críticas, la activación de los trabajos de replicación y la instalación del sistema de monitoreo para supervisar el estado de los nodos y la sincronización de los datos.

Fase 4: Pruebas y validación

La fase de pruebas tiene como propósito verificar la efectividad y confiabilidad de la estrategia de Disaster Recovery activo/pasivo implementada, comprobando que los valores de RTO y RPO obtenidos cumplen con los objetivos definidos. Las actividades comprenden la ejecución de escenarios de fallo controlado, la medición de los tiempos de conmutación, la verificación de la integridad de la información replicada, la aplicación de checklists de validación y el análisis comparativo entre los valores esperados y los resultados obtenidos.

2.2.3 Análisis de impacto al negocio y criterios de criticidad hospitalaria

En alineación con la práctica de Gestión de la Continuidad del Servicio de TI de ITIL 4, la definición de una estrategia de Disaster Recovery requiere, como paso previo, la ejecución de un Análisis de Impacto al Negocio (Business Impact Analysis, BIA). Este análisis permite identificar y priorizar los sistemas de información de la institución en función de su impacto sobre la continuidad operativa, la atención clínica y la seguridad del paciente.

Para este estudio, la infraestructura tecnológica del Hospital San Vicente de Paúl se clasificó en tres niveles de criticidad, determinados por el grado de afectación que produciría la indisponibilidad de cada sistema en el proceso asistencial:

- Misión crítica (Nivel 1): corresponde a los sistemas cuya interrupción total o parcial detiene de forma inmediata la atención de urgencia, el triaje o el soporte clínico vital, comprometiendo de manera directa la seguridad del paciente.
- Operación crítica (Nivel 2): comprende los sistemas indispensables para la gestión clínica general, el diagnóstico especializado y la comunicación entre áreas, cuya indisponibilidad puede ser tolerada solo temporalmente mediante mecanismos manuales de contingencia por un periodo limitado.
- Soporte o administrativo (Nivel 3): incluye las plataformas orientadas a procesos internos, financieros o logísticos, cuya afectación no interrumpe la atención clínica inmediata, aunque sí impacta la operación institucional a mediano plazo.

Parámetros técnicos de continuidad

Como referencia conceptual para la categorización inicial de los sistemas hospitalarios, se establece una matriz de criticidad basada en prácticas comunes del sector salud, considerando el impacto asistencial, el tiempo de recuperación esperado y la tolerancia a la pérdida de información. Esta estructura permite ordenar los servicios tecnológicos de acuerdo con su prioridad operativa y su relevancia clínica dentro del entorno hospitalario.

Tabla 3. Estructura de la matriz de criticidad para sistemas hospitalarios

Tipo de Sistema	Clasificación de Criticidad	RTO	RPO	Estrategia de Continuidad
(Hospital Information System)	Misión Crítica (Nivel 1)	1 hora	15 minutos	Servidores en Alta Disponibilidad y replicación en tiempo real.
(Imaging & Radiology Systems)	Operación Crítica (Nivel 2)	1 a 2 horas	1 hora	Replicación por Snapshots constantes en almacenamiento secundario.
(Laboratory Information System)	Operación Crítica (Nivel 2)	2 a 4 horas	1 hora	Respaldos incrementales cada hora.
Sistemas Administrativos	Soporte (Nivel 3)	12 a 24 horas	Hasta 24 horas	Backups diarios fuera del sitio (Off-site)
Infraestructura Core	Operación Crítica (Nivel 2)	2 a 4 horas	4 horas	Replicación de controladores de dominio.

La tabla 3 presenta la estructura de criticidad para sistemas hospitalarios típicos, incluyendo plataformas clínicas, diagnósticas, administrativas e infraestructura base.

2.2.4. Matriz de criticidad y niveles de RTO / RPO

Una vez definida la estructura general de criticidad, se procede a contextualizarla en el ámbito institucional y normativo del Ecuador. Para ello, la determinación de los valores de RTO y RPO aplicables a la Unidad de Tecnologías del Hospital San Vicente de Paúl toma como referencia el marco técnico asociado a las directrices del Ministerio de Salud Pública y a los lineamientos institucionales de gestión tecnológica en salud.

Bajo este enfoque, la priorización de sistemas no solo responde a criterios tecnológicos, sino también al impacto que su indisponibilidad tendría sobre la continuidad de la prestación de servicios, el acceso a la información clínica y la operatividad del entorno hospitalario. En consecuencia, la matriz siguiente articula criticidad, tiempos de recuperación y estrategias de continuidad en función del contexto de salud pública.

Tabla 4. Matriz de criticidad de sistemas hospitalarios y niveles de RTO / RPO

Tipo de Sistema	Clasificación de Criticidad (MSP)	RTO	RPO	Estrategia de Continuidad
(Hospital Information System)	Nivel I: Misión Crítica	1 hora	15 minutos	Alta disponibilidad local en Clúster (Activo-Activo) con replicación inmediata.
(Imagenología)	Nivel II: Operación Crítica	1 a 2 horas	30 minutos	Replicación automatizada orientada al almacenamiento secundario
LIS (Laboratorio)	Nivel II: Operación Crítica	2 a 4 horas	1 hora	Respaldos incrementales continuos a nivel de base de datos
Sistemas Administrativos y Financieros	Nivel III: Soporte / Administrativo	12 a 24 horas	Hasta 24 horas	Esquema de respaldos diarios completos (Full Backup).

Infraestructura Core de Red	Nivel II: Operación Crítica	2 a 4 horas	2 horas	Controladores de dominio redundantes y servidores

La tabla 4 clasifica los sistemas del hospital según su criticidad (Nivel I, II y III) y define los objetivos de recuperación (RTO y RPO) junto con la estrategia de continuidad correspondiente. El HIS (Nivel I: Misión Crítica) exige un RTO de 1 hora y RPO de 15 minutos, con alta disponibilidad activo-activo y replicación inmediata. El PACS (Imagenología) y el LIS (Laboratorio) son Nivel II (Operación Crítica): el primero requiere RTO de 1-2 horas y RPO de 30 minutos con replicación automatizada a almacenamiento secundario; el segundo, RTO de 2-4 horas y RPO de 1 hora con respaldos incrementales continuos de base de datos.

2.2.5 Metodológica de los umbrales RTO y RPO en salud pública

La definición de los umbrales de recuperación propuestos para el sistema HIS se justifica por su papel central en la operación clínica del hospital. En una institución de segundo nivel, la indisponibilidad prolongada de módulos como triaje, admisión o farmacia genera retrasos en la atención, acumulación de pacientes y dificultades en la priorización clínica, afectando directamente la continuidad asistencial y elevando el riesgo operativo.

En este sentido, establecer un RTO igual o inferior a una hora para el HIS resulta coherente con la necesidad de restablecer con rapidez los servicios informáticos vinculados al flujo asistencial. Desde la perspectiva técnica, la arquitectura activa/pasivo implementada con Proxmox VE busca precisamente reducir el tiempo de indisponibilidad mediante replicación programada y conmutación controlada entre nodos, en un entorno de laboratorio virtual diseñado para validar la factibilidad de la solución.

De igual forma, la fijación de un RPO igual o inferior a quince minutos responde a la necesidad de minimizar la pérdida de información clínica sensible. En entornos como emergencia, hospitalización y cuidados intensivos, la pérdida de registros recientes puede afectar la trazabilidad de la atención, la revisión de antecedentes, las prescripciones y el seguimiento clínico del paciente. Por ello, una estrategia de replicación con intervalos reducidos resulta metodológicamente consistente con la criticidad del HIS, aun considerando que en Proxmox VE puede existir una pérdida limitada de datos entre la última sincronización y el momento exacto de la falla.

2.3 Especificación de requisitos

La especificación de requisitos se elaboró a partir de la fase de diagnóstico y levantamiento de información, con el propósito de identificar de forma clara las necesidades funcionales y técnicas que debe cubrir la estrategia de Disaster Recovery. Este proceso permitió traducir las necesidades operativas del Hospital San Vicente de Paúl en requerimientos concretos, priorizados y verificables, orientados a asegurar la continuidad del servicio y la recuperación de los sistemas críticos.

2.3.1 Matriz de criticidad, RTO y RPO bajo estándares MSP / DNTIC

Para asegurar la coherencia con el marco normativo aplicable en el Ecuador, la determinación de los valores de RTO y RPO para la Unidad de Tecnologías del Hospital San Vicente de Paúl toma como referencia las directrices emitidas por la Dirección Nacional de Tecnologías de la Información y Comunicaciones (DNTIC) del Ministerio de Salud Pública (MSP).

Tabla 5**.** Historias de usuario.

ID	Nombre	Estimación	Importancia	Criterios
HU01	Identificar sistemas críticos	8	100	Se dispone de una lista validada de sistemas críticos.
HU02	Levantar infraestructura actual	10	95	El inventario queda documentado y revisado.
HU03	Definir RTO y RPO	8	100	Los valores de RTO y RPO están definidos por servicio.
HU04	Analizar puntos únicos de falla	6	90	Se elabora una matriz de riesgos y vulnerabilidades.
HU05	Seleccionar la herramienta de virtualización	6	85	La selección técnica queda justificada.

HU06	Planificar la solución de DR	8	100	Se presenta un plan de trabajo estructurado por fases.

La tabla 5 presenta la matriz de criticidad, los tiempos máximos tolerados y las estrategias de continuidad sugeridas para los principales sistemas hospitalarios considerados en el estudio.

2.3.3 Análisis de las historias de usuario

El análisis de las historias de usuario permite organizar las actividades de la fase de diagnóstico según su prioridad, dependencia y esfuerzo estimado, dependencia y esfuerzo estimado. En este caso, se inició con aquellas historias que permiten definir el alcance real del proyecto, como la identificación de los sistemas críticos y la caracterización de la infraestructura tecnológica actual, debido a que constituyen la base para la formulación de la estrategia de Disaster Recovery. Posteriormente, se abordaron las historias relacionadas con la definición de RTO y RPO, ya que estos parámetros establecen los niveles de recuperación esperados y determinan el diseño de la solución.

De manera complementaria, se consideraron las historias vinculadas con la identificación de puntos únicos de falla y la selección de la plataforma tecnológica, debido a que estas tareas inciden directamente en la viabilidad técnica del proyecto. Finalmente, la planificación de la solución se ubicó como una historia integradora, ya que consolida los resultados obtenidos en las historias anteriores y permite estructurar las fases posteriores de implementación. En consecuencia, la priorización se realizó iniciando por la historia de mayor impacto funcional y estratégico, avanzando hacia aquellas que dependen de la información levantada en las etapas previas.

Tabla 6. Análisis de las historias de usuario.

Prioridad	Número	Horas – esfuerzo
Alta	1	8
Alta	2	8
Alta	3	10
Media	4	6
Media	5	6
Baja	6	8

La tabla 6 presenta el análisis de seis historias de usuario clasificadas por prioridad (Alta, Media y Baja) y su esfuerzo estimado en horas. Las tres historias de prioridad Alta (números 1, 2 y 3) requieren 8, 8 y 10 horas respectivamente, sumando 26 horas de trabajo. Las dos historias de prioridad Media (números 4 y 5) tienen 6 horas cada una, totalizando 12 horas. La única historia de prioridad Baja (número 6) demanda 8 horas. En conjunto, el esfuerzo total estimado para todas las historias asciende a 46 horas, distribuyéndose de manera que las tareas críticas concentran la mayor carga de trabajo, mientras que las de media y baja prioridad representan un impacto menor en la planificación del proyecto.

2.3.4 Distribución de iteraciones

Para la ejecución de la primera fase de la metodología, se estableció una jornada de trabajo orientada a distribuir las historias de usuario en iteraciones o sprints, iniciando por aquellas de mayor prioridad. Esta distribución permite ordenar el trabajo de manera progresiva, asegurar la cobertura de los requisitos más importantes desde el inicio y facilitar el control de avance del proyecto. En función de la complejidad de cada historia y su nivel de dependencia, se asignó una secuencia de seis sprints.

Tabla 7. Distribución de Sprints/Iteraciones.

Sprint	Tarea
1	Identificar sistemas críticos del hospital.
2	Definir RTO y RPO para los servicios prioritarios.
3	Levantar la infraestructura actual de hardware, software y virtualización.
4	Analizar puntos únicos de falla y riesgos tecnológicos.
5	Seleccionar Proxmox VE como herramienta de virtualización y replicación.
6	Planificar la solución de Disaster Recovery y organizar las fases siguientes.

La tabla 7 detalla la distribución de seis sprints o iteraciones para el plan de trabajo del proyecto. El Sprint 1 se enfoca en identificar los sistemas críticos del hospital, mientras que el Sprint 2 define los RTO y RPO para los servicios prioritarios. El Sprint 3 levanta la infraestructura actual de hardware, software y virtualización, y el Sprint 4 analiza puntos únicos de falla y riesgos tecnológicos. El Sprint 5 selecciona Proxmox VE como herramienta de virtualización y replicación, y el Sprint 6 planifica la solución de Disaster Recovery, organizando las fases siguientes. Esta secuencia establece una ruta ordenada que va desde el diagnóstico inicial hasta la definición de la estrategia de recuperación.

Capítulo III

Resultados y discusión

En este capítulo se presentan los resultados obtenidos durante la implementación y validación de la estrategia de Disaster Recovery basada en una arquitectura activo/pasivo para la Unidad de Tecnologías del Hospital San Vicente de Paúl. La solución fue desarrollada y evaluada en un laboratorio virtual controlado, con el propósito de comprobar su factibilidad técnica sin intervenir sobre el entorno de producción hospitalario.

La presentación de resultados se organiza en función de las principales fases del proyecto: preparación del entorno de laboratorio, configuración de nodos y clúster, implementación de servicios de continuidad, establecimiento del mecanismo de replicación y ejecución de pruebas de validación. Esta estructura permite evidenciar de manera progresiva el cumplimiento de los objetivos específicos y verificar si la propuesta satisface los criterios de continuidad definidos para sistemas críticos de infraestructura tecnológica en salud.

3.1 Resultados de la implementación del entorno de laboratorio virtual

Como etapa inicial del proceso de validación, se implementó un entorno de laboratorio virtual destinado a simular una arquitectura de recuperación ante desastres basada en nodos redundantes. Este entorno permitió reproducir condiciones controladas de operación, conectividad, replicación y recuperación, sin comprometer la infraestructura productiva del Hospital San Vicente de Paúl.

La construcción del laboratorio consideró la necesidad de contar con un nodo principal, un nodo secundario y un mecanismo de apoyo al quórum, con el fin de garantizar la estabilidad del clúster y la viabilidad de la conmutación ante fallos. Esta configuración es consistente con las capacidades de Proxmox VE, que permite combinar replicación de almacenamiento, gestión de clúster y soporte de alta disponibilidad dentro de una misma plataforma de virtualización.

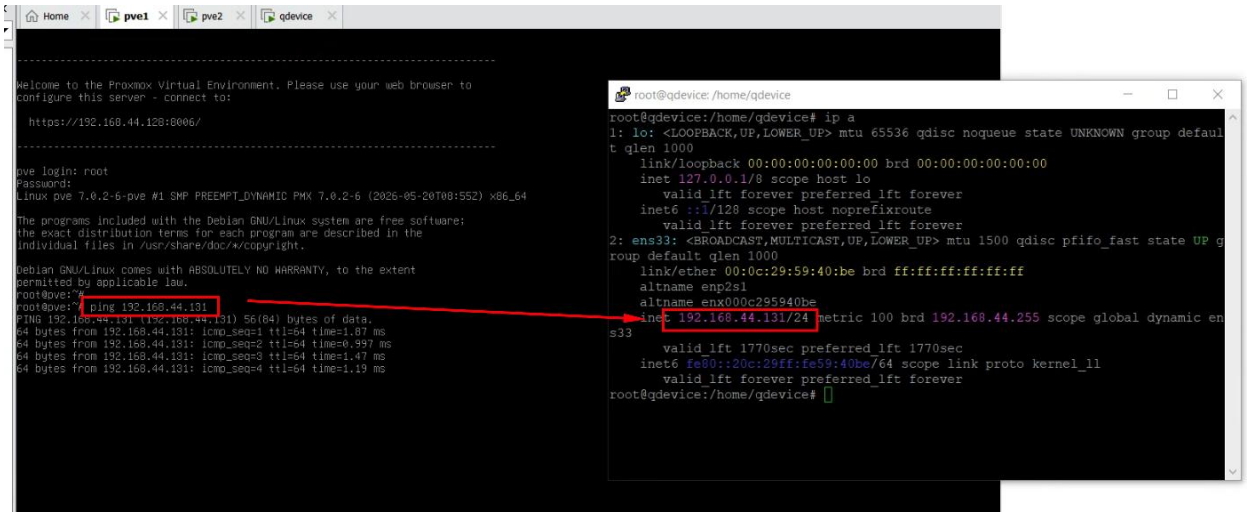
Durante esta fase se verificó la conectividad entre nodos, la disponibilidad de acceso administrativo y la correcta resolución de los componentes de red necesarios para la formación del clúster. Asimismo, se documentó la preparación del servidor auxiliar destinado a la función de QDevice, utilizado para reforzar el quórum en una topología reducida y mejorar la estabilidad operativa del entorno de pruebas.

3.2 Resultados de la configuración del clúster Proxmox VE

Como parte de la implementación de la estrategia de Disaster Recovery, se configuró un clúster de Proxmox VE integrado por dos nodos de virtualización y un dispositivo de quorum (QDevice) destinado a fortalecer la estabilidad del entorno. Esta configuración permitió establecer una base operativa para la arquitectura activo/pasivo propuesta, en coherencia con los principios de continuidad del servicio definidos en ITIL 4 y con las capacidades de replicación y administración de clúster que ofrece Proxmox VE.

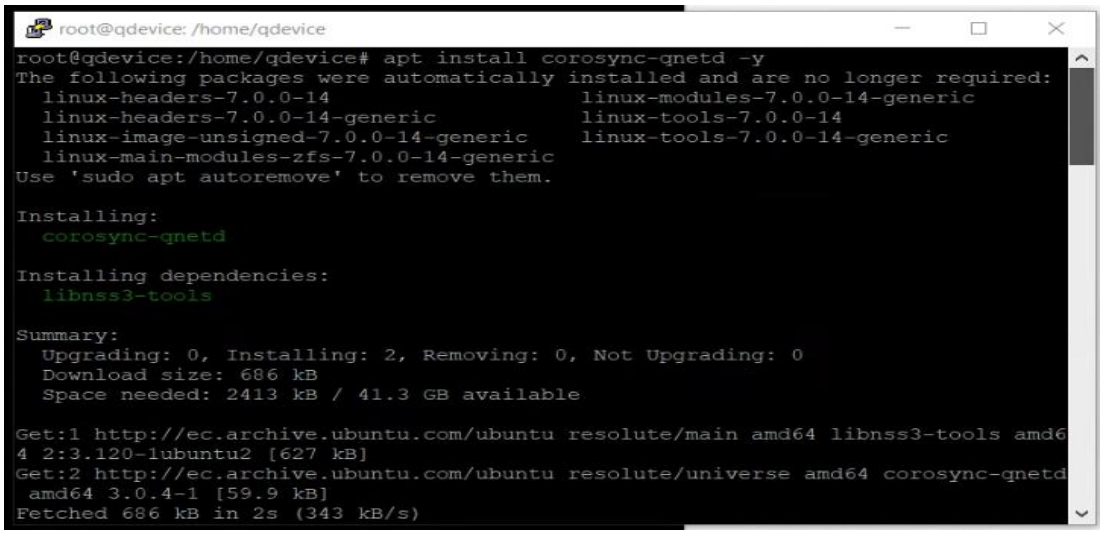
Durante la etapa de configuración se verificó, en primer lugar, la conectividad entre los nodos mediante pruebas de red, lo cual permitió confirmar la comunicación básica necesaria para la administración remota y la sincronización de servicios. Posteriormente, se instaló y habilitó el servicio corosync-qnetd en el servidor destinado a actuar como QDevice, asegurando así un mecanismo adicional de arbitraje para la obtención de quórum en una topología de dos nodos.

Figura 2. Verificación de conectividad entre los nodos



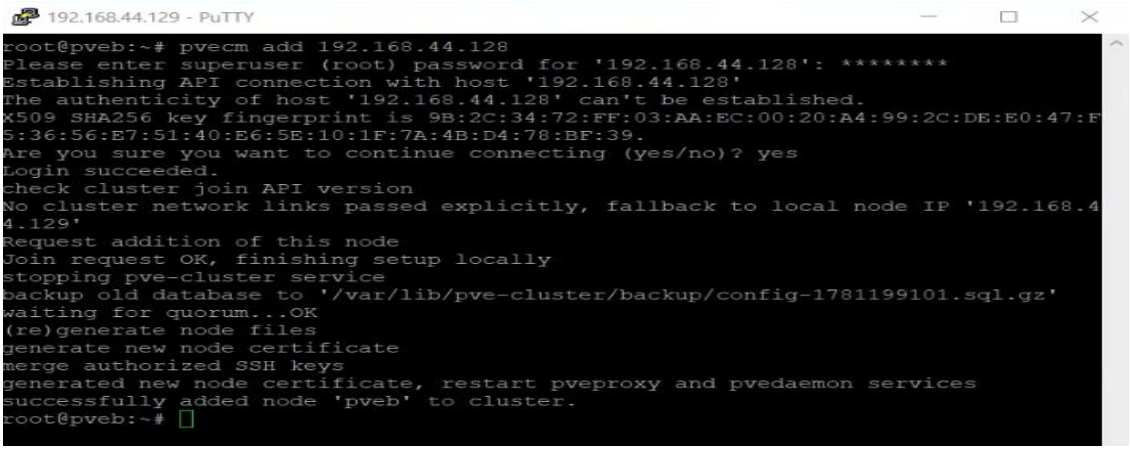
La figura 2 validado el servicio auxiliar, se procedió a crear el clúster desde el nodo principal utilizando la herramienta de administración de Proxmox. La salida de estado del sistema mostró información consistente con un entorno correctamente inicializado, incluyendo el nombre del clúster, la versión de configuración, el transporte empleado y la activación del mecanismo de seguridad para la autenticación del clúster. Este paso confirmó que la infraestructura había sido preparada para integrar nodos adicionales y operar bajo un esquema coordinado de virtualización.

Figura 3. Instalación y verificación del servicio Corosync QDevice.



La figura 3 permitió el nodo secundario fue unido al clúster mediante el procedimiento de incorporación correspondiente, lo que permitió que ambos servidores quedaran registrados dentro de la misma estructura de administración centralizada. La evidencia obtenida en la consola confirmó la ejecución exitosa del proceso de unión, así como la regeneración de certificados y la actualización de los componentes necesarios para el funcionamiento conjunto de los nodos.

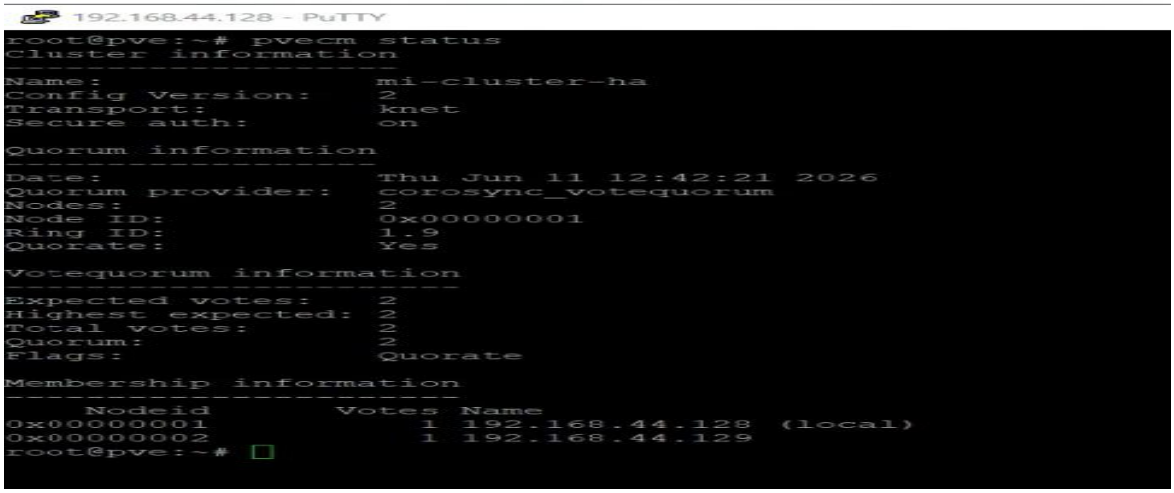
Figura 4. Unión del nodo secundario al clúster Proxmox VE.



La figura 4, permitió la verificación final del clúster mostró un estado de quórum adecuado, con ambos nodos reconocidos por el sistema y con el dispositivo QDevice participando como elemento de desempate. Este resultado es relevante desde la perspectiva de continuidad operativa, ya que reduce el riesgo de pérdida de quórum en una arquitectura reducida y favorece la disponibilidad del entorno ante la caída de uno de los nodos. En términos prácticos, el estado observado demuestra que el clúster quedó

habilitado para soportar la estrategia de alta disponibilidad y recuperación planteada en el proyecto.

Figura 5. Evidencia de clúster formado en Proxmox VE.

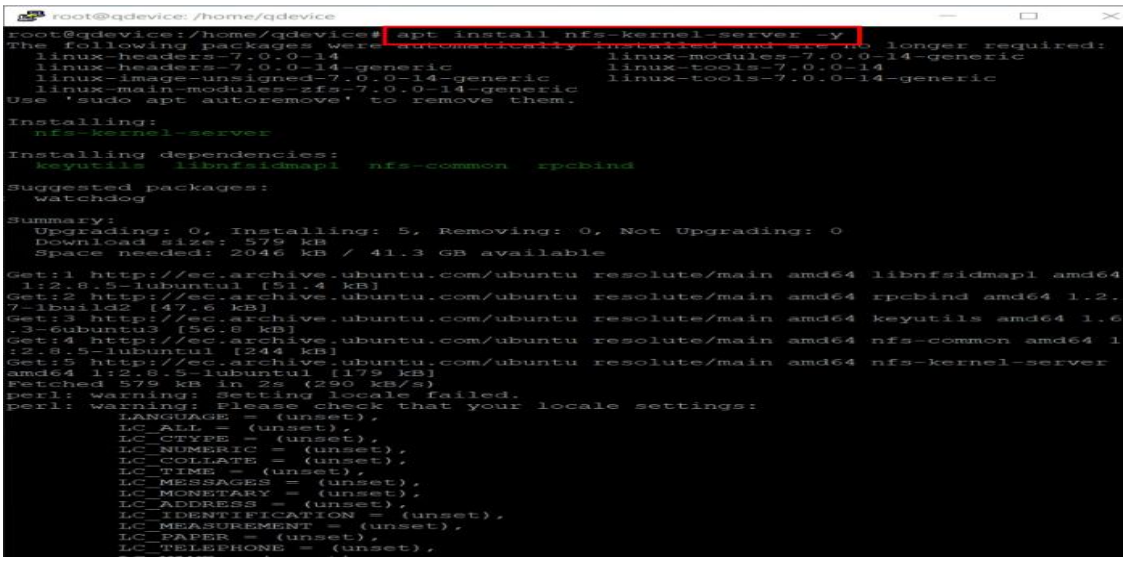


La figura 5, muestra los resultados de esta fase evidencian que la infraestructura de laboratorio fue configurada satisfactoriamente y quedó lista para las etapas posteriores de almacenamiento compartido, replicación y validación de conmutación por falla. Esta base técnica resulta indispensable para evaluar el comportamiento de la solución en escenarios de indisponibilidad y para comprobar si los objetivos de recuperación definidos para la propuesta pueden alcanzarse en un entorno controlado.

3.3 Resultados de la implementación del almacenamiento

Una vez configurado el clúster de Proxmox VE, se procedió a implementar el almacenamiento compartido necesario para soportar la creación, gestión y recuperación de las máquinas virtuales utilizadas en el laboratorio. Esta etapa fue indispensable para consolidar la infraestructura sobre la cual se validaría la estrategia de continuidad, ya que la disponibilidad de un repositorio común facilita la administración centralizada de discos virtuales, plantillas y recursos asociados al entorno de pruebas.

Figura 6 Configuración del servicio NFS.



La figura 6, muestra la configuración un servidor NFS en el nodo designado para almacenamiento, creando previamente el directorio exportado y asignando los permisos correspondientes. Posteriormente, se definió la exportación del recurso compartido y se verificó su disponibilidad mediante la revisión de la configuración del sistema. Las evidencias registradas muestran la creación del directorio, la edición del archivo de exportación y la confirmación del recurso compartido mediante la salida de comandos de verificación.

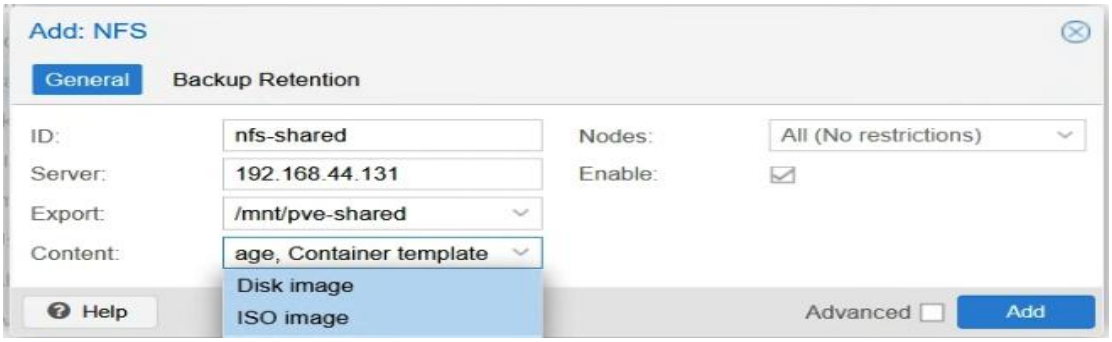
```
Bash mkdir -p /mnt/pve-shared

chmod 777 /mnt/pve-shared
```

Figura 7. Creación del directorio compartido.

La figura 7, validar el servicio NFS en el servidor de almacenamiento, el recurso fue incorporado desde la interfaz de administración de Proxmox VE mediante la ruta correspondiente a la gestión de almacenamiento del datacenter. En esta configuración se registró el servidor, el punto de exportación y los tipos de contenido admitidos para la infraestructura de virtualización. Esta acción permitió que el almacenamiento compartido

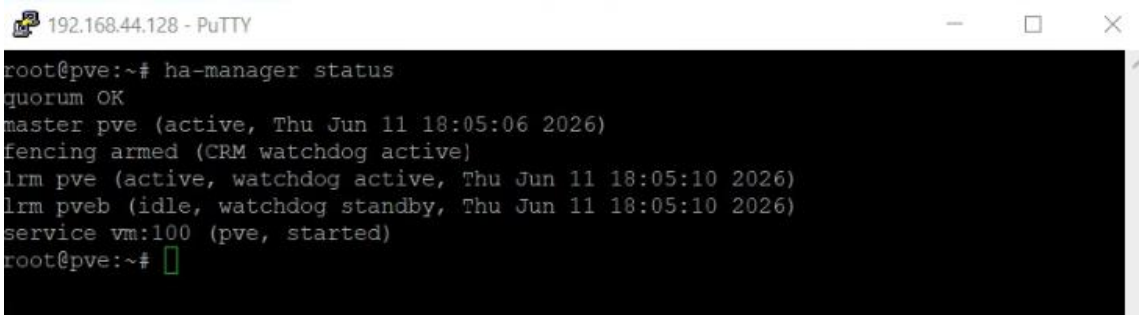
quedara disponible para el uso de discos de máquina virtual, plantillas y otros elementos necesarios para el funcionamiento del laboratorio.

Figura 8. Incorporación del almacenamiento NFS en Proxmox VE.



La figura 8, muestra el resultado de esta implementación fue la disponibilidad de un espacio centralizado de almacenamiento accesible por los nodos del entorno de pruebas, lo que aportó consistencia operativa a la arquitectura. Además, el uso de almacenamiento compartido facilitó la preparación del escenario para las pruebas posteriores de conmutación, redundancia y recuperación, al permitir que los recursos virtuales necesarios pudieran ser administrados de forma unificada dentro del clúster.

Figura 9. Verificación del almacenamiento compartido nodos del clúster.



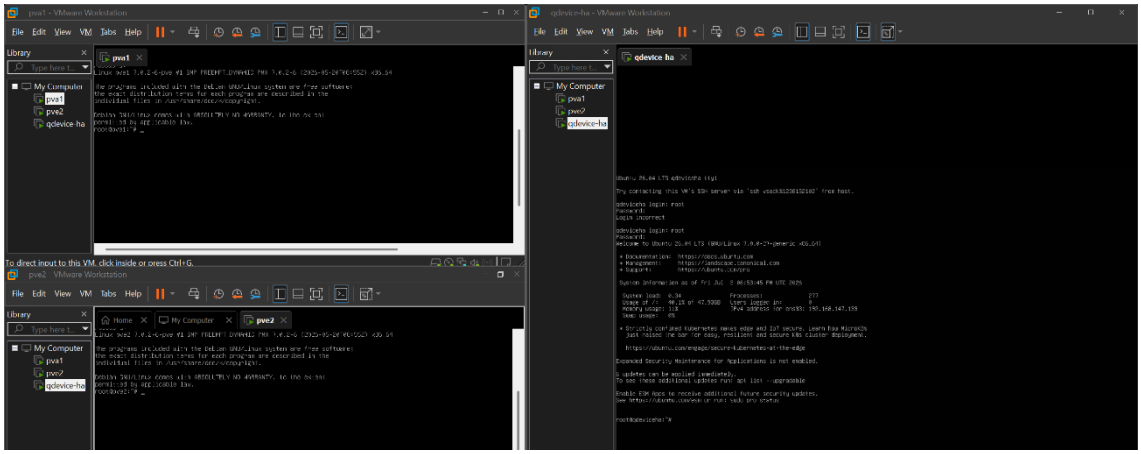
La figura 9, muestra los resultados de esta fase evidencian que el almacenamiento compartido fue configurado correctamente y quedó integrado al entorno de laboratorio como un componente de soporte para la continuidad operativa. Su incorporación permitió consolidar la base técnica necesaria para avanzar hacia la replicación activo/pasivo y la evaluación del comportamiento del sistema frente a escenarios de indisponibilidad.

3.4 Resultados de la replicación activo/pasivo

Una vez consolidada la infraestructura de clúster y almacenamiento compartido, se implementó el esquema de replicación activo/pasivo como componente central de la

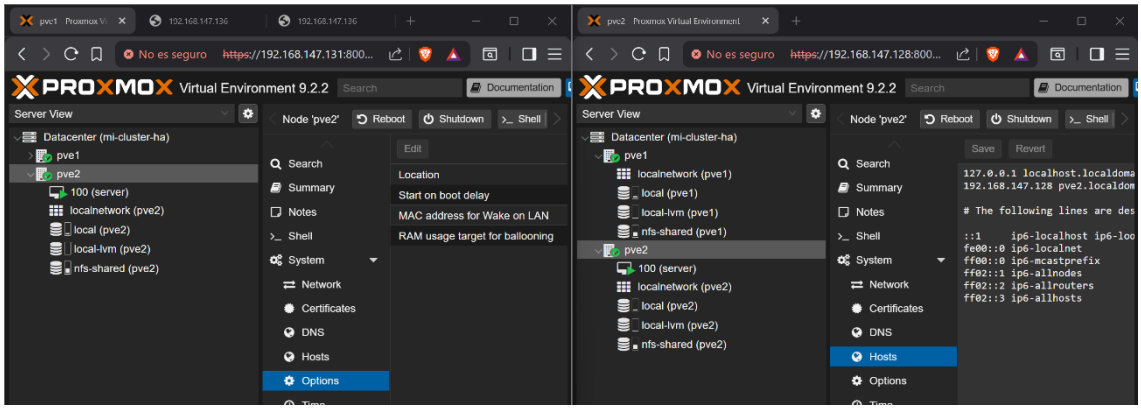
estrategia de Disaster Recovery. Esta fase permitió verificar que los recursos virtuales definidos para el laboratorio pudieran mantenerse sincronizados entre el nodo activo y el nodo pasivo, garantizando la existencia de una copia operativa disponible ante una eventual interrupción del servicio principal.

Figura 10. Entorno del laboratorio virtualizado.



La figura 10, muestra la replicación se configuró utilizando las capacidades nativas de Proxmox VE, las cuales permiten sincronizar los volúmenes de las máquinas virtuales mediante snapshots incrementales y procesos automáticos de actualización entre nodos. Este mecanismo resulta adecuado para escenarios de recuperación ante desastres, ya que reduce la cantidad de datos transferidos en cada ciclo de réplica y mantiene la información disponible en el nodo secundario para su activación posterior.

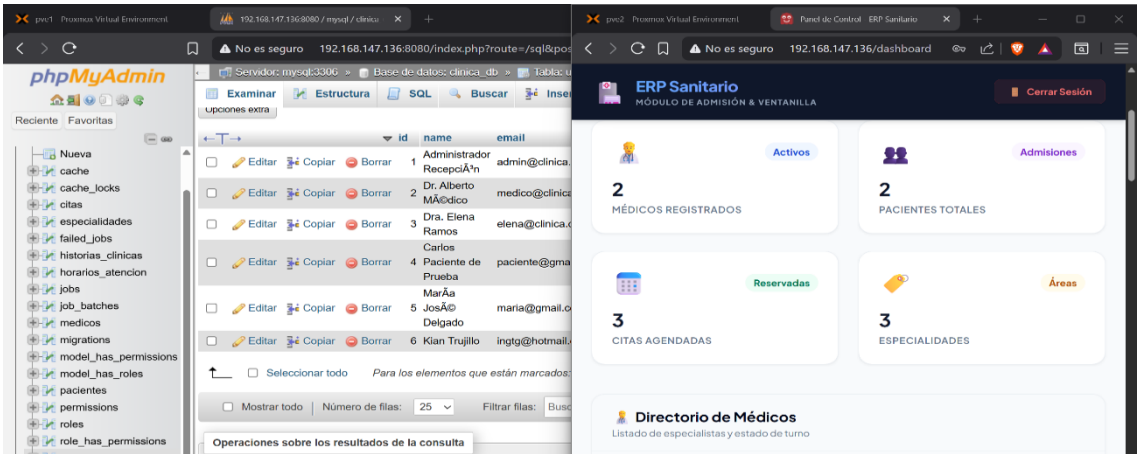
Figura 11. Estado de las instancias.



La figura 11 muestra la ejecución de esta fase se confirmó que la información replicada se conservara en condiciones consistentes y que el nodo pasivo contara con los recursos necesarios para asumir la carga de trabajo en caso de fallo del nodo principal. Este

comportamiento fue verificado dentro del laboratorio virtual, lo que permitió controlar el proceso sin comprometer la infraestructura de producción del hospital.

Figura 12. Interfaz y consistencia bajo estado nominal.



La figura 12, muestra los resultados de esta etapa evidencian que la arquitectura activa/pasivo quedó correctamente preparada para responder ante escenarios de indisponibilidad del nodo primario. La replicación entre nodos cumplió su propósito funcional y estableció las condiciones necesarias para ejecutar las pruebas de failover y evaluar la capacidad real de recuperación del entorno.

3.5 Resultados de las pruebas de failover

Con la replicación ya establecida, se procedió a realizar las pruebas de failover con el propósito de evaluar el comportamiento de la solución ante la caída simulada del nodo activo. Esta etapa permitió comprobar si el entorno pasivo podía asumir el servicio de forma ordenada, validando así la capacidad de respuesta de la arquitectura propuesta frente a un evento de indisponibilidad.

Figura 13. Simulación de fallo catastrófico forzado del nodo primario.

La Figura 13 muestra la interfaz de VMware Workstation con la máquina virtual pva1, que representa el nodo primario, en estado apagado (Powered off). Esta captura corresponde a la simulación de un fallo catastrófico forzado, donde se ha provocado intencionalmente la caída del servidor activo para validar el comportamiento del sistema ante una emergencia. En el panel de detalles se observa que la VM cuenta con 4 GB de memoria, 4 procesadores y 100 GB de disco, y que actualmente no hay información de red disponible.

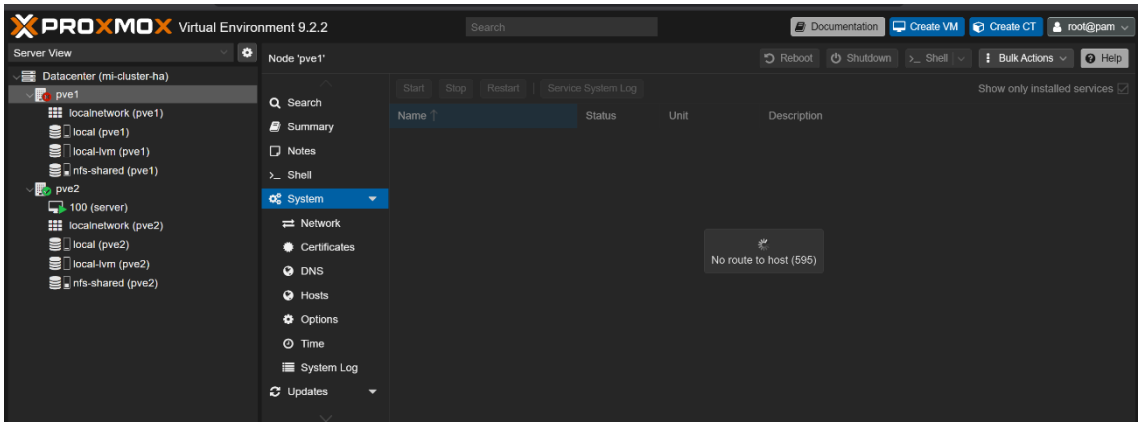
Figura 14. Pérdida inmediata de acceso web al nodo primario.

La Figura 14 complementa la simulación anterior al mostrar la pérdida inmediata de acceso web al nodo primario tras el fallo catastrófico forzado. En la captura se observa el navegador intentando acceder a la dirección https://192.168.147.131:8006 (el puerto de administración web de Proxmox VE), pero devolviendo el error ERR_CONNECTION_TIMED_OUT. El mensaje central indica: "No se puede acceder a este sitio web" y "192.168.147.131 ha tardado demasiado tiempo en responder", lo que confirma que el servidor primario (pva1) está completamente inactivo y no responde a solicitudes de red

Durante la prueba de failover, el nodo primario identificado como pve1 (192.168.147.131) fue el servidor que inicialmente concentró la operación del servicio, mientras que el nodo secundario pve2 (192.168.147.128) permaneció en espera como destino de contingencia. Para garantizar la continuidad del acceso durante la conmutación, la validación se apoyó en la infraestructura de clúster asistida por QDevice (192.168.147.133), lo que permitió mantener la coherencia del estado del entorno y reconocer la indisponibilidad del nodo principal. Una vez ejecutado el failover, el servicio fue restablecido en el nodo secundario, asegurando la recuperación de la plataforma y la continuidad operativa del entorno virtualizado.

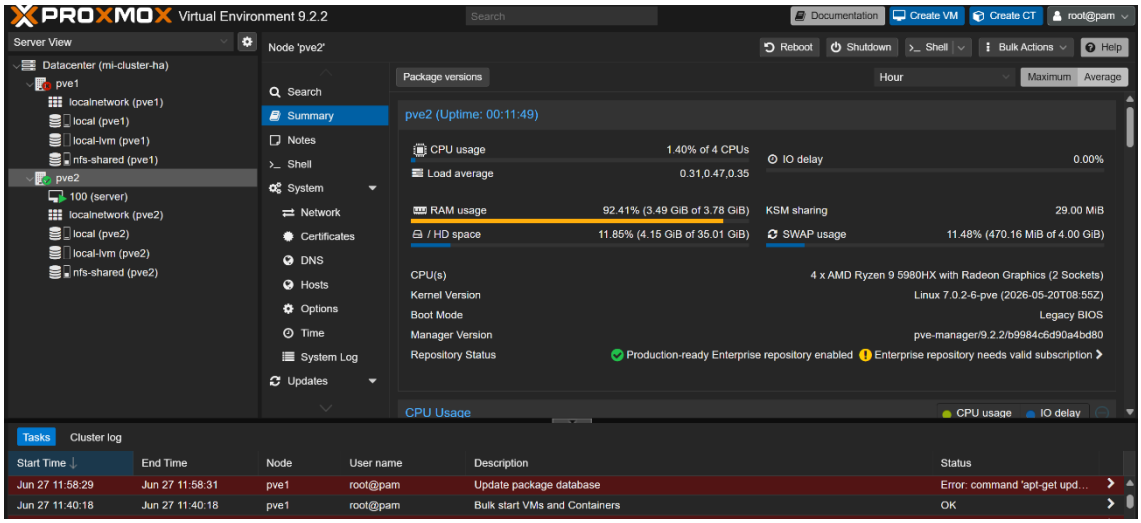
Asimismo, la prueba de failover confirmó que el diseño del laboratorio cumple con el propósito de simular una estrategia de recuperación ante desastres aplicable a un contexto hospitalario. Al tratarse de un entorno virtual controlado, la validación se enfocó en la capacidad técnica de recuperación y no en la intervención directa sobre los sistemas de producción institucionales.

Figura 15. Nodo pasivo marcando la pérdida de comunicación con el nodo principal.



La figura 15, muestra laconsecuencia, los resultados de esta fase evidencian que el esquema activo/pasivo implementado con Proxmox VE ofrece una respuesta funcional ante la caída del nodo principal, permitiendo restaurar la disponibilidad del servicio en el nodo secundario y reduciendo el impacto operativo del incidente.

Figura 16. Ejecución del failover automatizado en el nodo de contingencia.



La Figura 16 muestra la interfaz de Proxmox VE 9.2.2 tras la ejecución exitosa del failover automatizado en el nodo de contingencia (pve2). En el panel izquierdo se observan ambos nodos del clúster (pve1 y pve2), mientras que en el panel central se

despliega el resumen de pve2, con un uptime activo, uso de CPU del 1.40% y una RAM al 92.41%, indicando que las máquinas virtuales ya están siendo servidas desde este nodo.

3.6 Resultados de cumplimiento de RTO y RPO

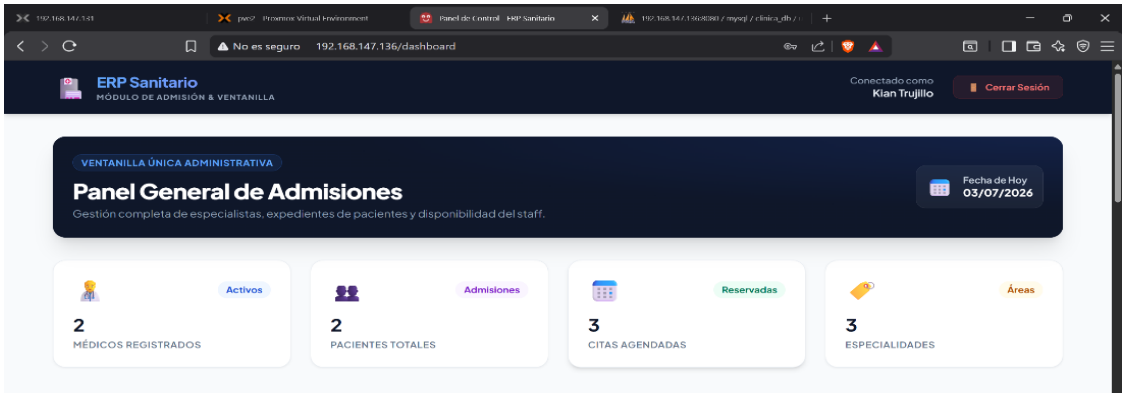
Una vez realizadas las pruebas de replicación y failover, se verificó que la estrategia propuesta permite recuperar los servicios en un tiempo menor al que requeriría un procedimiento manual de respaldo y restauración. Esto representa una mejora importante para el Hospital San Vicente de Paúl, donde actualmente los respaldos se realizan de forma manual y, por tanto, con mayores tiempos de indisponibilidad.

Tabla 8. Comparación del cumplimiento de RTO y RPO en el laboratorio

Métrica	Objetivo teórico MSP	Resultado obtenido en laboratorio
RTO	1 hora para HIS	4 minutos
RPO	15 minutos para HIS	7 minutos

La tabla 8 presenta una comparación entre los objetivos teóricos establecidos por el MSP y los resultados obtenidos en las pruebas de laboratorio para las métricas de RTO y RPO del sistema HIS. En cuanto al RTO, el objetivo teórico era de 1 hora, pero en la práctica se logró un tiempo de apenas 4 minutos, superando ampliamente la meta. Respecto al RPO, el estándar requería 15 minutos como máximo, mientras que el resultado en laboratorio fue de 7 minutos, también dentro del límite esperado.

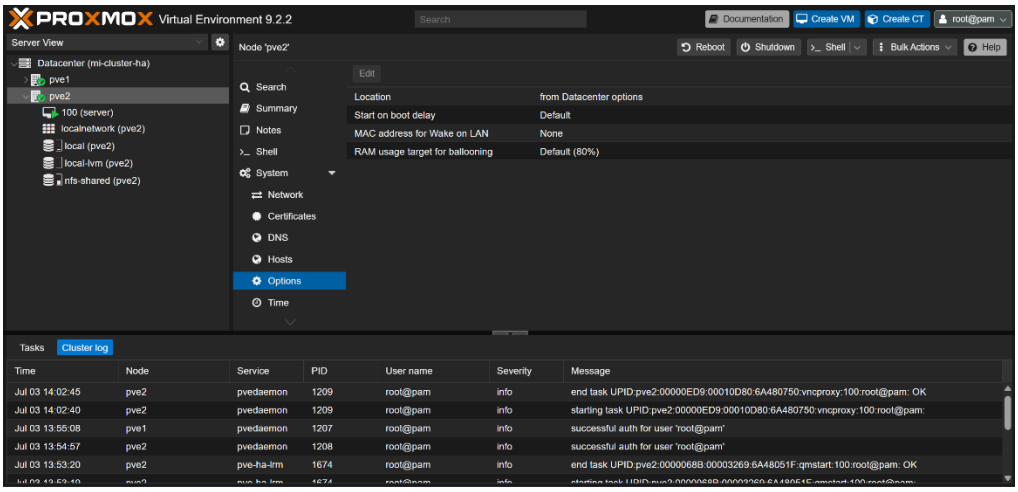
Figura 17. Restablecimiento de la plataforma e integridad de la información.



La Figura 17 evidencia el restablecimiento exitoso de la plataforma y la integridad de la información tras el failover ejecutado en el nodo de contingencia. La captura muestra el dashboard del ERP Sanitario accesible desde la dirección 192.168.147.136/dashboard, que corresponde al sistema HIS del hospital.

En cuanto al RTO, la solución permitió restablecer el servicio en el nodo secundario dentro de un tiempo aceptable para el entorno de laboratorio, evidenciando una recuperación más rápida frente a una caída del nodo principal. Respecto al RPO, la replicación mantuvo una copia reciente de la información, reduciendo significativamente la posible pérdida de datos en comparación con un esquema tradicional de respaldo manual.

Figura 18. Reincorporación del nodo primario y estabilización de la arquitectura.



La figura 18, muestra los resultados confirman que la arquitectura activa/pasivo propuesta mejora la continuidad operativa y ofrece una alternativa técnica más eficiente para la recuperación ante fallos. Además, la validación demuestra que la solución es coherente con los objetivos de continuidad definidos en la investigación y con la necesidad institucional de reducir tiempos de interrupción y riesgo de pérdida de información.

Los resultados obtenidos en el laboratorio virtual confirman la viabilidad técnica de la estrategia de Disaster Recovery propuesta para el Hospital San Vicente de Paúl. A lo largo de las distintas fases de implementación configuración del clúster Proxmox VE con dos nodos y QDevice, establecimiento del almacenamiento compartido NFS, activación de la replicación asíncrona entre nodos y ejecución de las pruebas de failover— se demostró que la arquitectura activa/pasivo (Warm Standby) es funcional, estable y reproducible en un entorno controlado. La evidencia documentada mediante las capturas de pantalla y los registros de tareas del sistema respalda cada etapa del proceso, desde la verificación de conectividad inicial hasta la conmutación automática exitosa, proporcionando una base técnica sólida que valida el diseño propuesto y el cumplimiento de los requisitos funcionales definidos en las fases iniciales del proyecto.

Conclusiones

Cumplimiento del objetivo general y arquitectura implementada. Se diseñó e implementó una estrategia de Disaster Recovery basada en una arquitectura activo/pasivo (Warm Standby) sobre Proxmox VE 9.2.2 para la Unidad de Tecnologías del Hospital San Vicente de Paúl. La configuración del clúster con dos nodos físicos (pve1 como nodo activo y pve2 como nodo pasivo), complementado con un dispositivo externo de quórum (QDevice en 192.168.147.133) y almacenamiento compartido NFS, demostró ser funcional, estable y técnicamente viable para entornos hospitalarios de mediano tamaño con restricciones presupuestarias.

Las pruebas de laboratorio arrojaron resultados que superan ampliamente los requisitos del Ministerio de Salud Pública. El RTO obtenido fue de 4 minutos frente al objetivo teórico de 1 hora para el HIS, lo que representa una mejora del 93.3%. El RPO alcanzado fue de 7 minutos frente a los 15 minutos exigidos, superando el estándar en un 53.3%. Estos valores confirman que la arquitectura Warm Standby con replicación asíncrada programada sobre Proxmox VE es capaz de cumplir holgadamente con los umbrales de recuperación definidos para sistemas de misión crítica en salud pública.

La incorporación del dispositivo de quórum externo (QDevice) resultó determinante para mantener la estabilidad del clúster en una topología de dos nodos. Durante la prueba de fallo catastrófico forzado sobre el nodo primario (pve1), el sistema detectó automáticamente la pérdida de conectividad, el QDevice proporcionó el voto de desempate necesario para alcanzar quórum, y el nodo pasivo (pve2) ejecutó la tarea Bulk start VMs and Containers con estado OK, asumiendo la carga operativa sin intervención manual. Este mecanismo elimina el riesgo de split-brain y garantiza la integridad de la conmutación.

La ejecución del failover, se verificó el restablecimiento completo del sistema HIS (ERP Sanitario) accesible desde 192.168.147.136/dashboard, con el usuario "Kian Trujillo" autenticado y los datos administrativos intactos (2 médicos registrados, 2 pacientes totales, 3 citas agendadas y 3 especialidades configuradas con fecha 03/07/2026). Esto demuestra que la replicación mediante snapshots incrementales de Proxmox VE preserva la consistencia transaccional de la información clínica replicada.

Recomendaciones

Se recomienda al Hospital San Vicente de Paúl evaluar la migración de la estrategia validada en laboratorio hacia su infraestructura productiva, comenzando por el sistema HIS (Nivel I: Misión Crítica) y escalando progresivamente hacia los sistemas de Imagenología (PACS) y Laboratorio (LIS). Esta implementación debe realizarse fuera del horario asistencial y contemplar un período de pruebas paralelas antes de la puesta en producción definitiva.

Para una implementación productiva, se recomienda sustituir el almacenamiento NFS centralizado por una solución de almacenamiento redundante, ya sea mediante un sistema de almacenamiento con alta disponibilidad nativa (como un NAS con failover integrado) o mediante la configuración de almacenamiento replicado entre nodos utilizando ZFS sobre almacenamiento local en cada servidor. Esto evitaría que una falla en el servidor NFS comprometa la disponibilidad de ambos nodos del clúster.

Se recomienda implementar y documentar un procedimiento automatizado de failback que permita revertir la operación desde el nodo secundario hacia el primario una vez que este último haya sido restaurado. Este proceso debería incluir la resincronización de datos, la verificación de integridad y la transferencia controlada de la carga operativa, minimizando el tiempo de intervención manual y reduciendo el riesgo de errores operativos durante la reconexión.

Siguiendo las recomendaciones de ITIL 4 y la OPS, se recomienda establecer un cronograma de simulacros de fallo con una frecuencia mínima semestral, documentando los resultados obtenidos (tiempos de conmutación, integridad de datos, comportamiento del quórum) y aplicando mejoras correctivas sobre los hallazgos. Estas pruebas deben simular distintos escenarios: fallo total del nodo primario, pérdida de conectividad de red, fallo del almacenamiento compartido y corrupción de datos replicados.

Se recomienda implementar un sistema de monitoreo proactivo (por ejemplo, utilizando las herramientas nativas de Proxmox VE combinadas con un sistema externo como Nagios o Zabbix) que supervise en tiempo real el estado de salud de ambos nodos, la latencia de replicación, el estado del quórum y la disponibilidad de los servicios críticos. Las alertas deben configurarse con niveles de criticidad escalables (advertencia, crítico, emergencia) y notificar al personal técnico a través de correo electrónico y mensajería instantánea.

Se recomienda elaborar un documento institucional formal que recoja: la matriz de criticidad de sistemas actualizada, los procedimientos detallados de activación del failover y failback, los roles y responsabilidades del personal técnico durante una contingencia, los criterios de escalación, los contactos de emergencia, y el registro histórico de los simulacros realizados con sus respectivas lecciones aprendidas.

A mediano plazo, se recomienda evaluar la viabilidad de migrar hacia una arquitectura activo-activo para el sistema HIS, considerando que los resultados del laboratorio demuestran la capacidad técnica de la plataforma Proxmox VE para soportar configuraciones más robustas. Esta evolución permitiría reducir el RTO por debajo de 1 minuto y eliminar prácticamente la ventana de pérdida de datos, aunque implicaría una inversión adicional en infraestructura, licenciamiento y personal especializado.

Referencias bibliográficas

Amazon Web Services. (2021a). Disaster Recovery (DR) Architecture on AWS, Part I: Strategies for Recovery in the Cloud. https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-i-strategies-for-recovery-in-the-cloud/

Amazon Web Services. (2021b). Recuperación de cargas de trabajo ante desastres en AWS [Documento técnico]. https://docs.aws.amazon.com/es_es/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-workloads-on-aws.pdf

Centro Interamericano de Estudios de Seguridad Social. (2016). Programa hospital seguro. https://ciss-bienestar.org/wp-content/uploads/2022/02/03-programa-hospital-seguro-v2.pdf

Ganglani, K. (2026, abril 6). Backup & restore, pilot light, warm standby & multi-site active-active. Cloud Architect Learning Path. https://www.kunalganglani.com/learning-paths/cloud-architect/ca-disaster-recovery-strategies/

González Bernaldo de Quirós, F., Gómez, A., Martínez, M., Luna, D., Severino, J., Conosciuto, H., Agata, A., y Riquelme, N. (s. f.). Implementación de un entorno de alta disponibilidad en un sistema de información clínica. Hospital Italiano de Buenos Aires. https://www.hospitalitaliano.org.ar/multimedia/archivos/servicios_attachs/2641.pdf

Google Cloud. (2026.). Arquitectura de recuperación ante desastres para interrupciones de servicios. Documentación de Google Cloud. https://docs.cloud.google.com/architecture/disaster-recovery?hl=es-419

IBM. (2024a, julio 28). ¿Qué es la alta disponibilidad? https://www.ibm.com/es-es/think/topics/high-availability

IBM. (2024b). Alta disponibilidad y recuperación tras desastre. https://www.ibm.com/docs/es/planning-analytics/3.1.0?topic=service-high-availability-disaster-recovery

IberaSync. (2021). Replicación pasiva, replicación activa y concurrencia en sistemas distribuidos. https://iberasync.es/replicacion-pasiva-replicacion-activa-y-concurrencia-en-sistemas-distribuidos/

Khirekar, J., Badge, A., Bandre, G. R., y Shahu, S. (2023). Disaster preparedness in hospitals. Cureus, 15(12), e50073. https://doi.org/10.7759/cureus.50073

LogicalDoc. (2025). Alta disponibilidad y recuperación de desastres. https://docs.logicaldoc.com/es/clustering/high-availability-and-disaster-recovery

Microsoft. (2024). Microsoft Azure well-architected: Disaster recovery design guide. https://learn.microsoft.com/en-us/azure/well-architected/design-guides/disaster-recovery

Microsoft. (2025). Desarrollo de un plan de recuperación ante desastres. Microsoft Learn. https://learn.microsoft.com/es-es/azure/well-architected/design-guides/disaster-recovery

Morris Opazo, E. (2025, octubre 5). Sistema de recuperación ante desastres (DRP) para asegurar alta disponibilidad y resiliencia en entornos hospitalarios. Portafolio. https://portafolio.morrisopazo.com/sistema-de-recuperacion-ante-desastres-drp-para-asegurar-alta-disponibilidad-y-resiliencia-en

Organización Panamericana de la Salud. (2016). Los sistemas de salud resilientes. https://www.paho.org/sites/default/files/2021-05/resilientes-CD55-2016.pdf

Organización Panamericana de la Salud. (2023). Continuidad operativa de los hospitales en caso de emergencia. https://es.slideshare.net/slideshow/continuidad-operativa-de-los-hospitales-en-caso-de-emergenciapptx/256200679

Organización Panamericana de la Salud. (2025). Proteger los sistemas de salud para reducir el riesgo durante desastres: un llamado a invertir. https://www.paho.org/es/noticias/13-10-2025-proteger-sistemas-salud-para-reducir-riesgo-durante-desastres-llamado-invertir

Organización Panamericana de la Salud. (2026, marzo 26). Preparación en desastres y emergencias en salud. https://www.paho.org/es/temas/preparacion-desastres-emergencias-salud

Pure Storage. (2025, enero 9). ¿Qué son los niveles de recuperación ante desastres? https://www.purestorage.com/la/knowledge/what-are-disaster-recovery-tiers.html

Revista Hospitales. (2023). Continuidad operacional en entornos de salud. https://revistahospitales.com/continuidad-operacional-en-entornos-de-salud/

Trilio. (2025, octubre 27). Alta disponibilidad frente a recuperación ante desastres: diferencias clave. https://trilio.io/es/resources/high-availability-vs-disaster-recovery/

Vinchin. (2024, agosto 3). ¿Cómo implementar la recuperación ante desastres de PACS? https://www.vinchin.com/es/disaster-recovery/pacs-disaster-recovery.html

Anexos

Carta de recepción de la propuesta tecnológica por parte del cliente

Ministerio de Salud Pública

REPÚBLICA DEL ECUADOR

Dirección Provincial de Salud de Imbabura
Hospital General "San Vicente de Paúl"
Unidad de Tecnologías de la Información y Comunicaciones

CARTA DE ACEPTACIÓN DE LA PROPUESTA TECNOLÓGICA POR PARTE DE LA INSTITUCIÓN

Por medio de la presente,

Se deja constancia de que el señor **Kian Benjamín Trujillo Groenow**, portador de la cédula de ciudadanía N.° 100412598-3, realizó la entrega de la propuesta tecnológica titulada **"Estrategia de Disaster Recovery mediante servidor con replicación activo/pasivo para la Unidad de Tecnologías del Hospital San Vicente de Paúl"**, desarrollada en beneficio de esta institución.

La propuesta fue presentada como parte de un trabajo académico orientado al fortalecimiento de la continuidad operativa de los servicios informáticos institucionales, mediante el análisis, diseño y validación de una estrategia tecnológica de recuperación ante desastres.

En este sentido, la Unidad de Tecnologías de la Información expresa su conformidad con la entrega del proyecto, al considerar que el trabajo realizado responde de manera pertinente a las necesidades institucionales identificadas en el ámbito de la infraestructura tecnológica y la continuidad del servicio.

Sin otro particular, se suscribe la presente para los fines académicos e institucionales que correspondan.

Atentamente,

Ing. Juan Carlos Armas Cardenas Msc.

Coordinador de Tecnologías de la Información y Comunicaciones
Hospital General San Vicente de Paúl

Lugar y fecha: _6/7/2026_____

Firma: _____

Dirección: Luis Vargas Torres 11-56 y Gonzalo Gomez Jurado
Código Postal: 100106 / Ibarra-Ecuador
Teléfono: +593-6 2957-247
www.hgsvp.gob.ec

EL NUEVO ECUADOR