UNIVERSIDAD DEL AZUAY

Facultad de Ciencias de la Administración

Carrera de Ingeniería en Ciencias de la Computación

MARCO DE REFERENCIA PARA IMPLEMENTAR Y GESTIONAR INFRAESTRUCTURAS HIPERCONVERGENTES BASADAS EN LOS PRINCIPIOS DE LA GESTIÓN DE REDES

Trabajo de titulación previo a la obtención del grado de Ingeniero en Ciencias de la Computación

Autor:
Bryan Ronaldo Arias Gutiérrez

Director:
Ing. Juan Carlos Pauta Ortiz

Cuenca – Ecuador
2025

DEDICATORIA

Este trabajo va dedicado a las personas que me enseñaron que rendirse no es una opción y me han acompañado a lo largo de mi carrera. A mi mamá y mi abuelita, quienes estuvieron ahí cada vez que las necesité. A todos mis amigos y familiares que han sido parte fundamental de este camino; sin su apoyo no estaría aquí en este momento. A un amigo y hermano especial que me cuida siempre, Alexander Heredia (Q.E.P.D.), quien me enseñó a seguir mis sueños. Y especialmente a la mujer que me alentó con su amor y paciencia a culminar este proyecto.

AGRADECIMIENTO

Mi reconocimiento más sincero y sentido va dirigido a mi tutor, quien no solo cumplió su rol académico, sino que se convirtió en un verdadero mentor durante este proceso. Su sabiduría, compartida con generosidad y paciencia, iluminó los momentos de incertidumbre y transformó los obstáculos en oportunidades de aprendizaje. Cada reunión, cada corrección y cada palabra de aliento fueron esenciales para dar forma a este proyecto y, más aún, para fortalecer mi confianza como futuro profesional. De igual manera, agradezco a la universidad por ser mi guía y acompañarme en cada paso de este camino formativo.

Índice de Contenidos

Índice de Figuras

Índice de Tablas

RESUMEN

La infraestructura hiperconvergente constituye un conjunto integrado de tecnologías que permite construir sistemas fundamentados en software, eliminando la separación tradicional entre procesamiento, redes y almacenamiento. Su ventaja principal radica en facilitar el crecimiento horizontal mediante servidores comerciales estándar. Actualmente vivimos una realidad compleja donde las demandas de poder de procesamiento aumentan constantemente. Internet y las comunicaciones móviles convergen y se expanden de manera continua, lo que obliga al desarrollo de aplicaciones capaces de funcionar eficientemente en estos escenarios dinámicos. Por esta razón, cualquier organización moderna requiere contar con infraestructuras prácticas de mantener y escalar sin complicaciones operativas. En este trabajo se contrasta la HCI frente a la infraestructura tradicional mediante el modelo FCAPS, evaluando cinco aspectos fundamentales: gestión de fallos, configuración, contabilización, rendimiento y seguridad. Los hallazgos obtenidos fueron concluyentes: la HCI supera consistentemente a los sistemas tradicionales en todas estas dimensiones analizadas, consolidándose como una solución estratégica para organizaciones que buscan optimizar su gestión tecnológica. Esta superioridad se manifiesta en la simplificación de procesos operativos, reducción de costos de mantenimiento, mayor flexibilidad para adaptarse a cambios en la demanda y mejor aprovechamiento de recursos. En consecuencia, la adopción de HCI representa una decisión acertada para empresas que priorizan la eficiencia operacional, la escalabilidad y la continuidad del negocio en un entorno tecnológico cada vez más exigente y competitivo.

Palabras clave: Gestión de redes, Tecnología de la información, Infraestructura de información, Protección de datos, Virtual.

ABSTRACT

Hyperconverged infrastructure constitutes an integrated set of technologies that enables building software-based systems, eliminating the traditional separation between processing, networks, and storage. Its main advantage lies in facilitating horizontal growth through standard commercial servers. Currently, we live in a complex reality where processing power demands constantly increase. Internet and mobile communications converge and expand continuously, which requires developing applications capable of functioning efficiently in these dynamic scenarios. For this reason, any modern organization needs to have infrastructures that are easy to maintain and scale without operational complications. In this work, HCI is contrasted against traditional infrastructure using the FCAPS model, evaluating five fundamental aspects: fault management, configuration, accounting, performance, and security. The findings obtained were conclusive: HCI consistently surpasses traditional systems in all these analyzed dimensions, establishing itself as a strategic solution for organizations seeking to optimize their technological management. This superiority manifests in the simplification of operational processes, reduction of maintenance costs, greater flexibility to adapt to demand changes, and better resource utilization. Consequently, adopting HCI represents a sound decision for companies that prioritize operational efficiency, scalability, and business continuity in an increasingly demanding and competitive technological environment.

Keywords: Network management, Information technology, Information infrastructure, Data protection , Virtual.

INTRODUCCIÓN

En la actualidad, las empresas enfrentan desafíos en los sistemas tecnológicos, por lo cual deben satisfacer las necesidades de manera eficiente a las demandas del mundo actual. Los centros de datos han usado tradicionalmente equipos separados: uno para procesar información, otro para guardarla y otro más para conectar todo. Este modelo fragmentado genera muchas complicaciones a la hora de adaptarse rápidamente, trabajar de forma eficiente y mantener los costos bajo control (Acceleron Labs Pvt Ltd, 2018; Quantum, 2021). Esta manera inflexible de organizar la tecnología hace muy difícil que las empresas mantengan sus servicios funcionando sin problemas. Además, dificultan que puedan crecer o reducirse según lo necesiten sin gastar de más. Esto resulta vital para no quedarse atrás en un mercado tan cambiante (Jogalekar, 2000; Yang, 2025).

Para resolver estos problemas, surge la Infraestructura Hiperconvergente (HCI), una solución moderna que junta todo lo que necesita un centro de datos en una sola plataforma de software, simplificando todo el proceso (Cisco System, 2025; Nutanix, 2024b). Lo que queremos lograr con esta investigación es ver de cerca y comparar cómo se desempeña realmente la HCI frente a los sistemas tradicionales, usando un marco de trabajo llamado FCAPS (Fault, Configuration, Accounting, Performance, Security), que ayuda a evaluar qué tan bien se gestionan las redes (Fulber-Garcia, 2024; Gillis, 2025). Con este estudio, buscamos identificar los beneficios reales que trae la HCI en las cinco áreas más importantes de la gestión tecnológica, ofreciendo información concreta y útil para que las empresas tomen decisiones más acertadas al momento de mejorar sus sistemas y garantizar que sus operaciones sigan adelante sin interrupciones (Antonenko, 2024; Parmar, 2019).

CAPÍTULO 1
MARCO TEÓRICO

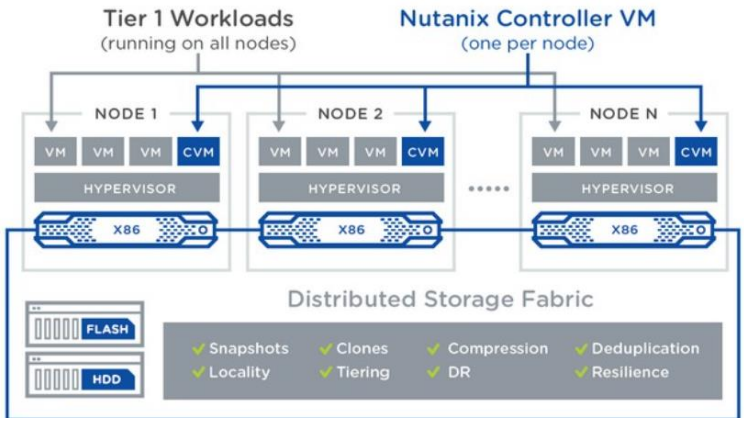
1.1 Concepto de Infraestructura Hiperconvergente (HCI)

Según Schneider & Smalley (2024), una infraestructura hiperconvergente (HCI, por sus siglas en inglés Hyperconverged Infrastructure) es una solución moderna para centros de datos que se basa en plataformas operativas y busca integrar recursos de cómputo, almacenamiento y redes en una sola plataforma, administrada desde la capa de virtualización. A diferencia de las infraestructuras tradicionales, en las que cada función requiere un hardware específico, en la HCI todas las operaciones se consolidan en una sola plataforma que funciona con un software específico de propósito general. Esto supone un avance al integrar diversos elementos de hardware bajo una única capa de virtualización, el hipervisor, que orquesta los componentes virtuales en la plataforma hiperconvergente.

Según, (Nutanix, 2024b) una HCI combina hardware y software y puede operar como un servidor/nodo de centro de datos con dispositivos de almacenamiento. Esto permite eliminar problemas comunes asociados con las infraestructuras legadas. En lugar de una infraestructura tradicional en silos, las HCI adoptan arquitecturas que operan sobre servidores de propósito general, facilitando un uso más eficiente de los recursos y su adaptación a las necesidades de carga de trabajo y de procesamiento de datos. Estas arquitecturas se basan en x86 y emplean almacenamiento híbrido que integra discos duros mecánicos (HDD) y unidades de estado sólido (SSD). Al ser una arquitectura flexible, es posible escalar de manera independiente cada componente: procesador, memoria RAM o almacenamiento, de acuerdo con las necesidades y aplicaciones requeridas en empresas de servicios. Incluso es posible incorporar GPU para mejorar el procesamiento gráfico o acelerar el cómputo intensivo.

Figura 1

Arquitectura de Nutanix en un Entorno de Infraestructura Hiperconvergente



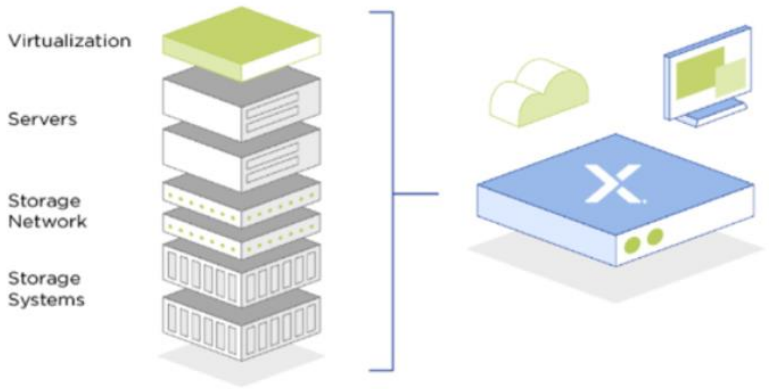
Nota: Elaboración propia a partir de (Nutanix, 2024b)

1.2 Evolución de la Infraestructura Hiperconvergente

Según The Gorilla Guide Team (2019), la evolución hacia la HCI evidencia una continuidad iniciada en las décadas de 1960 y 1970, cuando la computación empresarial se apoyaba en uno o dos mainframes, equipos de gran capacidad para procesar altos volúmenes de datos que centralizaban el cómputo en centros de datos para ejecutar aplicaciones y gestionar cargas de trabajo. A fines de los años setenta y comienzos de los ochenta surgieron alternativas más accesibles y manejables: las minicomputadoras, capaces de operar de forma autónoma e intercambiar información con el sistema central. Durante los noventa, aparecieron enfoques distribuidos que separaron funciones en servidores dedicados, y la plataforma Intel x86, junto con Windows o Linux, se consolidó como estándar de facto. Ya en los primeros años dos mil, la maduración de sistemas operativos, memoria, almacenamiento y redes impulsó implementaciones eficientes, mejorando el desempeño operativo y preparando el terreno para arquitecturas integradas. Este proceso derivó en la infraestructura hiperconvergente, que unifica cómputo, almacenamiento y redes bajo una capa de virtualización y gestión centralizada.

Figura 2

Evolución de la Infraestructura Tradicional hacia la Infraestructura Hiperconvergente (HCI)



Nota: Elaboración propia a partir de (Nutanix, 2024b)

1.3 Características de la Infraestructura Hiperconvergente

La HCI se caracteriza por combinar sistemas de hardware y software, lo que habilita la integración de sistemas virtuales, almacenamiento y redes. Al usar menos recursos, presenta costos de implementación más bajos y facilita la administración. Para los equipos de TI, el hecho de no depender de adquisiciones frecuentes para incrementar la capacidad convierte a la HCI en una alternativa atractiva; su accesibilidad puede traducirse en beneficios económicos tanto para grandes empresas como para PYMES, favoreciendo su expansión (Parmar, 2019).

Según Antonenko (2024), la HCI ofrece soluciones de optimización y administración que, desde su adquisición, reducen gastos en pequeñas y medianas empresas, especialmente en contextos donde escasean la información y los recursos financieros.

1.4 Infraestructura Tradicionales vs Infraestructura Hiperconvergente

Durante años, las infraestructuras tradicionales de TI han sido un pilar importante para operar la mayoría de centros de datos. Estas infraestructuras se caracterizan por tener componentes independientes servidores, almacenamiento SAN/NAS y redes que, por lo general, son operados por equipos especializados; personas con conocimientos (expertos) de cada área se encargan de una integración compleja entre tecnologías heterogéneas (Quantum, 2021). Cada funcionalidad y administración es diferente; en una

infraestructura tradicional, los componentes operan de manera individual, lo que, hasta cierto punto, puede ser una alternativa viable al momento de combinar tecnologías y servidores. Un claro ejemplo es una organización que integra servidores de Hewlett Packard Enterprise (HPE), almacenamiento de (Schneider & Smalley, 2024a) y equipos de red de Cisco, ajustándose a las necesidades de cada área.

Este enfoque permite aumentar la capacidad de cómputo sin afectar los niveles de almacenamiento o de red, ya que están separados por capas. En contraste, la infraestructura hiperconvergente (HCI) consolida cómputo, almacenamiento y redes en una plataforma definida por software y gestionada desde la capa de virtualización, lo que reduce la complejidad de integración, acorta los tiempos de aprovisionamiento y permite escalar de forma modular y centralizada mediante la adición de nodos x86; además, integra capacidades de orquestación y optimización que contribuyen a un menor costo total de propiedad (Antonenko, 2024; Nutanix, 2024b). No obstante, su adopción requiere una planificación cuidadosa del dimensionamiento (CPU, memoria, IOPS) y puede aumentar la dependencia del proveedor; en cargas muy específicas o heredadas, la arquitectura tradicional puede seguir siendo conveniente por su modularidad y control fino por dominio (Acceleron Labs Pvt Ltd, 2018).

1.4 Arquitecturas de la Infraestructura Hiperconvergente (HCI)

La arquitectura de una HCI está definida por los siguientes niveles: (1) Sistemas de almacenamiento: constituyen la base de la infraestructura; allí se ubican los dispositivos físicos que reemplazan a los discos duros tradicionales. Su gestión debe ser realizada por personal técnico especializado. (2) Red de almacenamiento: conecta los servidores y suele estar compuesta por fibra óptica o Ethernet dedicadas exclusivamente al tráfico de almacenamiento; en este nivel existe un alto grado de dificultad, pues se generan costos de materiales, hardware y mantenimiento por especialistas. (3) Servidores: Son máquinas físicas que ejecutan aplicaciones y servicios dentro de la infraestructura; a menudo se instalan en racks (estructuras metálicas), lo que puede dificultar la gestión de expansión de recursos y, en algunos casos, resultar insuficiente la capacidad disponible. (4) Virtualización: es la capa superior que, sobre el hardware físico, permite crear máquinas virtuales que se ajustan a los niveles inferiores; una planificación deficiente puede dificultar la escalabilidad y la eficiencia operativa (Nutanix, 2024b).

1.5 Beneficios de las Infraestructuras Hiperconvergentes

Las infraestructuras han surgido como una solución eficiente para una buena gestión al momento de integrar centros de datos modernos, por lo cual enlistamos los beneficios más notorios:

1.5.1 Escalabilidad y Flexibilidad

La escalabilidad es un beneficio notorio dentro de la HCI por su capacidad de escalar de manera modular, permitiendo que las organizaciones amplíen recursos informáticos, almacenamiento y red dependiendo de las necesidades sin interrupción de las operaciones. Esta escalabilidad se logra al añadir nodos al clúster, lo que facilita una expansión y, de tal modo, también se vuelve eficiente para ser instalada y que así se tenga más capacidad (Sheldon, 2020).

1.5.2 Gestión de Simplificación y Automatización

La gestión se caracteriza por su capacidad para simplificar y administrar los entornos tecnológicos empresariales mediante una plataforma unificada. A diferencia de las HCI tradicionales, donde todo su funcionamiento es totalmente separado y normalmente son incompatibles, este enfoque permite al encargado de TI aprovechar una sola plataforma de administración centralizada, tener la visibilidad completa del entorno de trabajo, permitiendo realizar tareas de supervisión y mantenimiento desde una sola interfaz, resolviendo de manera ágil los cambios ante una operativa. La simplificación no solo se encarga de reducir las cargas de trabajo, sino que disminuye los errores humanos, lo cual evita la necesidad de configurar y sincronizar múltiples sistemas de gestión y maximiza la automatización mediante flujos de trabajo definidos por la plataforma. Las plataformas HCI actuales incluyen herramientas avanzadas de automatización, balanceo de carga de trabajo, recuperación ante desastres y monitoreo predictivo. Estas herramientas no solo optimizan, sino que permiten organizar prácticas de gestión alineadas con los principios de TI ágil y DevOps. Esto también facilita la escalabilidad al detectar automáticamente nuevos recursos sin afectar el trabajo en curso, lo que representa una ventaja en entornos donde el tiempo y la eficiencia son vitales (Stephen Pritchard, 2021).

1.5.3 Costo Total de Propiedad (TCO)

El costo en una HCI es la capacidad de disminuir el costo total de propiedad (TCO, por sus siglas en inglés), abarcando no solo los gastos iniciales de adquisición de tecnologías, sino también los costos de operación y mantenimiento a lo largo de todo el ciclo de vida. Al tener un enfoque integral, permite consolidar múltiples funciones como red y almacenamiento en una sola plataforma virtualizada, lo que optimiza la adquisición de nuevos equipos y el aprovechamiento de los componentes existentes. Al integrar estos componentes, la empresa puede reducir significativamente los gastos totales sin invertir en múltiples sistemas independientes de almacenamiento (SAN/NAS), ya que es posible construir sobre arquitectura x86, generalmente más económica y sostenible en reemplazos y actualizaciones. En algunos casos, las organizaciones obtienen un ROI (retorno de inversión) más rápido al implementar soluciones hiperconvergentes, pues no requieren configuraciones complejas ni recursos costosos para alcanzar rendimientos equivalentes a los de arquitecturas tradicionales. Esto se convierte en una alternativa atractiva para pequeñas y medianas empresas que buscan avances tecnológicos sin comprometer sus recursos financieros (World Financial Review, 2023).

1.5.4 Compatibilidad con Entornos Híbridos y Modernos

Dentro de la HCI, la compatibilidad se distingue por su naturaleza definida por software y su escalabilidad, caracterizándose por su facilidad de integración en los entornos de nubes híbridas y la adopción de tecnologías emergentes (Intel, 2025).

Al unificar almacenamiento, cómputo y virtualización en nodos medulares, HCI puede desplegar rápidamente las herramientas automatizadas modernas, las cuales suelen ser soportes de máquinas virtuales como para contenedores, habilitando arquitecturas de los microservidores distribuidos. Según el estudio de 451 Research, el 45% de organizaciones que utilizan HCI han implementado Kubernetes sobre plataformas hiperconvergentes, así logrando acelerar actualizaciones, facilitando los microservidores y, en casos posteriores, al momento de migrar aplicaciones a la nube (CRN, 2022).

Intel (2025), enfatiza que la HCI es un camino directo hacia una nube privada o híbrida, lo cual conlleva desplegar rápidamente y trabajar con herramientas híbridas; también tiene la idea de ser portable para la colocación de cargas de trabajo.

1.6 Limitaciones de las Infraestructuras Hiperconvergentes

1.6.1 Inversión Inicial Elevada

La HCI, si bien promete bajar los costos totales de propiedad (TCO) a medio o largo plazo, su inversión inicial es significativa. Esto conlleva que, a gran medida que requieren el hardware netamente para su uso, las licencias de software, en algunos casos, el costo también se da al momento de configurar los equipos; también al momento de hacer consultas puede generar algún costo adicional, a diferencia de las infraestructuras tradicionales que únicamente el costo es de adquisición; puede ser de cualquier tipo de fabricante, ya que funcionan de manera independiente. Cada recurso de la HCI se caracteriza por tener un costo alto, ya que no se obliga a adquirir nodos únicamente completos, sino equipos funcionales (Longbottom, 2020).

Además, las licencias de las principales soluciones suelen ser suscripciones o contratos multianuales; estas empresas son (VMware vSAN, Nutanix o HPE SimpliVity); con dichas empresas implican un compromiso financiero desde los inicios. Esto no siempre es viable para algunas pequeñas y medianas empresas, que cuentan con un presupuesto limitado al iniciar operaciones; por ello, su adopción de este tipo de tecnologías suele retrasarse (Arnav Sharma, 2023).

1.6.2 Falta de Granularidad de la Escalabilidad

Una limitación dentro de las HCI radica en su modelo de escalabilidad; si bien es modular y sencillo de implementar, muchas veces carece de la gradualidad que ofrecen ciertas arquitecturas tradicionales. En su entorno de almacenamiento y red de otros nodos preconfigurados, lo que significa ampliación de recursos, por ejemplo, en un entorno de nodos completos que incluyan procesamiento (CPU) y memoria (RAM), estos recursos adicionales que no son estrictamente necesarios para las cargas de trabajo (Longbottom, 2020).

Este modelo se escala de manera forzada, lo que puede derivar en un uso ineficiente de la infraestructura e incrementar el costo energético, pues las organizaciones podrían verse obligadas a adquirir tecnología nueva para operar hardware no requerido. En estos entornos, a veces existe un desbalance entre componentes: se requieren grandes volúmenes de almacenamiento mientras el uso de CPU es bajo. Esta falta de flexibilidad

resulta determinante al evaluar la viabilidad de la HCI, en comparación con otras opciones más ajustadas a su realidad (World Financial Review, 2023).

1.6.3 Curvas de Aprendizaje para el Personal Técnico

La adopción de nuevas tecnologías de HCI implica un cambio significativo en la forma de gestión, operatividad y mantenimiento de equipos de TI, ya que estas plataformas están basadas en un enfoque definido por software que integra tanto las redes, virtualización y almacenamiento en un sistema unificado. Se exige personal capacitado en sistemas unificados, que adquiera nuevos conocimientos para considerar al relacionarlos con la administración, la automatización y la centralización de procesos virtuales; en muchas circunstancias, estos procesos son realizados mediante contenedores en entornos híbridos (Saty, 2023).

En las arquitecturas tradicionales, cada equipo se especializa en su propia área: unos manejan las redes, otros el almacenamiento y otros los servidores. Con HCI, el reto es diferente: los profesionales necesitan ampliar sus conocimientos más allá de su especialidad para manejar estas nuevas plataformas y entender cómo trabajan juntos el cómputo, el almacenamiento y la red. Si no se invierte en capacitación constante, el equipo pierde eficiencia y la empresa termina sin aprovechar realmente las ventajas que promete esta tecnología (Arnav Sharma, 2023).

1.7 Tecnologías Definidas por Software

1.7.1 Software Definida por Redes (SDN)

Es una arquitectura en ascenso que es ágil, controlable, rentable y versátil, lo que la convierte en la opción perfecta para el dinamismo de gran ancho de banda de las aplicaciones contemporáneas. Estas redes facilitan el aumento de las ventajas de la virtualización de los centros de datos, mejorando la adaptabilidad y el uso de recursos, disminuyendo de esta manera los costos globales y los relacionados con la infraestructura (Vega, Andrade, & Pinos Castillo, 2022).

1.7.2 Almacenamiento Definido por Software (SDS)

Se trata de un método de almacenamiento de datos en el que se emplea una capa de software para extraer (abstraer) los recursos de almacenamiento de la infraestructura de

hardware físico que los respalda. Este proceso de abstracción del software de almacenamiento respecto del hardware permite que las organizaciones separen la compra del software de la compra del hardware. Con el almacenamiento definido por software (SDS), los clientes pueden aprovechar servidores básicos y medios de almacenamiento para construir una infraestructura de almacenamiento más económica (Schneider & Smalley, 2024).

1.7.3 Computación Definida por Software (SDC)

Es un modelo de informática en la nube establecido por software que automatiza y regula la administración y suministro de recursos en la nube a través de software (Red Hat, 2020). La SDC alberga una capa de software que se encuentra sobre la infraestructura física que la sostiene. Adquiere el hardware físico necesario y lleva a cabo todo el control, manejo y coordinación de los recursos de la nube mediante el software (Vstack, 2025).

La SDC también puede implementarse en infraestructuras híbridas que combinan recursos de nube pública y privada. Este componente ofrece la habilidad de suministrar y administrar de manera dinámica los recursos informáticos, además de incrementar el uso y la adaptabilidad de la computación (Vstack, 2025).

El SDC proporciona adaptabilidad, escalabilidad y automatización en la administración y uso de la capacidad de la nube. Permite extraer los recursos físicos (CPU, memoria, dispositivos de almacenamiento) para convertirlos en máquinas virtuales o contenedores. Los cuales pueden gestionarse con facilidad desde un servidor independiente (Red Hat, 2025). La capa informática o infraestructura definida por software permite que las cargas de trabajo realizadas en la nube, así como las aplicaciones en contenedores, se ejecuten de manera en entornos híbridos y multicloud. Las SDC se integran con hipervisores y plataformas de orquestación concentradas. Kubernetes es un claro ejemplo de esto, ya que facilita la asignación automática y dinámica de recursos. De esta manera, las empresas cuentan con las herramientas necesarias para administrar múltiples tareas complejas de forma simultánea.

1.7.4 Virtualización

Se trata de una tecnología capaz de generar representaciones virtuales de servidores, almacenamiento, redes y otras maquinarias físicas (Amazon, 2025). El software virtual replica las características del hardware tangible para operar múltiples máquinas virtuales simultáneamente en una sola máquina física. Las compañías utilizan la virtualización para emplear sus recursos físicos de forma eficaz y lograr rendimientos superiores de sus inversiones. Además, impulsa los servicios de computación en la nube que asisten a las entidades en la gestión eficiente de la infraestructura.

1.8 Modelos de Redes: Gestión de Fallas, Gestión de Configuración, Gestión de Contabilidad, Gestión de Rendimiento y Gestión de Seguridad (FCAPS)

Los modelos de referencia FCAPS (por sus siglas en inglés) son un marco de referencia que fue propuesto por la International Organization for Standardization (ISO) a mediados de los 80 como parte de un estándar Open Systems Interconnection (OSI). El propósito principal es proporcionar una estrategia estandarizada que permita sus funciones esenciales al momento de la gestión de redes en cinco áreas claves: Fault (Gestión de fallos), Configuration (Gestión de configuración), Accounting (Configuración de contabilidad), Performance (Configuración de rendimiento) y Security (Gestión de seguridad).

Dichas normas fueron plasmadas en las especificaciones ISO/IEC 10040:1998 (ISO/IEC, 1998), documento que establece principios y objetivos necesarios para garantizar una administración eficiente en redes de telecomunicaciones y centros de datos. Posteriormente, estos lineamientos fueron adoptados por la Unión Internacional de Telecomunicaciones. Desde la creación del modelo FCAPS, fue un pilar fundamental para el diseño de sistemas de gestión tanto en los entornos corporativos como en los entornos de telecomunicaciones, ya que, por su gran capacidad de desglosar una compleja tarea de administrar redes funcionales, muy bien definidos y, dependiendo de su categoría, pueden abordar aspectos de operación y mantenimiento, permitiendo no solo la supervisión y control de recursos, sino también la planificación, seguridad y optimización de las infraestructuras. Ya que en la actualidad existen modelos más recientes como el eTom (Enhanced Telecom Operation Maps) o ITIL (Information Technology Infraestructura Library),Infrastructure a pesar de estos nuevos modelos, la

predecesora es la gestión de redes FCAPS debido a su simplicidad conceptual en las arquitecturas tradicionales e incluso en la HCI. Los modelos FCAPS están definidos por cinco principales niveles operativos para la gestión de redes:

1.8.1 Gestión de Fallos (Fault Management)

La gestión de fallos se está enfocando en la disponibilidad y buena gestión durante el funcionamiento de la red. Lo que abarca es un ciclo continuo de actividades primordiales: aislamiento, detección, localización, correlación, verificación y restauración; dichos fallos permiten que una red sea efectiva ante una catástrofe de red. Después de identificar los problemas y ser solucionados, comienzan a trabajar con normalidad; a este paso se lo denomina restauración. Una misión crítica de la gestión de fallas es contemplar la implementación de redundancia; esto implica la recuperación de escenarios ante desastres mayores; estos pueden ser: fallo de componente, interrupción de energía o la sustracción de equipo vital para su funcionamiento (Fulber-Garcia, 2024).

1.8.2 Gestión de Configuración (Configuration Management)

La gestión de configuración dentro del modelo FCAPS es fundamental para su documentación y control ya que contiene distintos parámetros al momento de brindar una estabilidad, coherencia y trazabilidad de los servicios de red. Este proceso implica la recopilación y almacenamiento de configuración ya sea esta de manera remota o local, esto beneficia ya que rastrea los cambios en la configuración del software y software de la red. Por ello la Gestión de configuración previene errores y los ayuda revertirlos reduciendo riesgo operativo y mejorando la capacidad de respuesta ante incidentes sin comprometer la infraestructura haciendo que sea confiable y alineada con los objetivos operacionales (Fulber-Garcia, 2024)

1.8.3 Gestión de Contabilidad (Accounting Management)

La gestión de contabilidad en los modelos FCAPS se enfoca en recopilar, analizar, medir y reportar el uso de la red dentro de las organizaciones. Su objetivo es garantizar eficiencia y flexibilidad en entornos empresariales o de servicios, tomando como base únicamente el entorno operativo real. Este proceso implica registrar meticulosamente diversos aspectos, como el ancho de banda utilizado, los volúmenes de datos transferidos,

el consumo de recursos de almacenamiento y las conexiones activas. Todo esto permite establecer cobros justos a los clientes, identificar patrones de uso, detectar posibles abusos o sobreutilización de recursos y optimizar costos de manera más efectiva (Gillis, 2025).

Una gestión de contabilidad bien implementada se convierte en un soporte fundamental para la toma de decisiones al momento de adoptar HCI (Fulber-Garcia, 2024), Esto incluye consideraciones sobre cargas de trabajo, su balanceo adecuado y la priorización de recursos, tal como señala (Nutanix, 2024b) Al implementar plataformas hiperconvergentes, las organizaciones pueden lograr un ahorro del 40% en el costo total de propiedad. Esto se debe a que estas soluciones requieren menos espacio físico, reducen el consumo energético, disminuyen la necesidad de personal de mantenimiento y eliminan el uso de licencias redundantes. En consecuencia, las empresas experimentan beneficios económicos significativos al adoptar esta tecnología.

1.8.4 Gestión de Rendimiento (Performance Management)

La gestión de rendimiento dentro de los modelos FCAPS engloba la vigilancia constante, la optimización y el análisis de las métricas críticas de una red de internet, como la latencia, estabilidad, tasas de errores, el uso de ancho de banda y la disponibilidad, esto con tal de garantizar un servicio óptimo dentro de las infraestructuras, cumpliendo así niveles esperados de satisfacción del servicio. Esto facilita el monitoreo en tiempo real y el seguimiento de redes; así posteriormente se evitan congestiones o accidentes que afecten la operatividad (Nwakeze, 2024).

Asimismo, la operación en tiempo real mejora la detección temprana de fallos y acorta los tiempos de respuesta, lo que reduce la pérdida de paquetes y las caídas de señal, evitando la degradación del servicio (Nwakeze, 2024).

Dentro de las HCI modernas, donde las tecnologías de cómputo y redes interactúan entre sí, la aplicación de supervisión resulta aún más valiosa por su integración estrecha con el almacenamiento y el cómputo; no solo supervisa aplicaciones empresariales desde el apartado funcional. Este enfoque progresivo se implementa en organizaciones con visión holística y dinámica del estado, asegurando su continuidad, evolución y eficiencia dentro de las estructuras tecnológicas (Cisco System, 2025; Nutanix, 2024b).

1.8.5 Gestión de Seguridad (Security Management)

La gestión de seguridad, pilar del modelo FCAPS, protege los recursos de red y cómputo mediante la definición de políticas, el control de accesos y la respuesta coordinada a incidentes; integra funciones AAA (autenticación, autorización y auditoría) e IAM, con registro centralizado y trazabilidad. Incluye segmentación (VLAN, microsegmentación) y cifrado de datos en tránsito y en reposo, con gestión de claves; administra firewalls, listas de control e IDS/IPS para detección y prevención de intrusiones, además de aplicar hardening, escaneo de vulnerabilidades, priorización de parches y control de cambios para preservar la integridad. Se apoya en plataformas SIEM para la correlación de eventos y en SOAR para orquestar respuestas automáticas, monitoreando métricas como MTTD y MTTR para mejora continua. Conforme a ISO/IEC, se integra con los sistemas generales de administración, asegurando alertamiento y escalamiento formales, así como continuidad del negocio y recuperación ante desastres. En entornos HCI, la centralización y la automatización refuerzan confidencialidad, integridad y disponibilidad, reducen el riesgo operativo y elevan la resiliencia del servicio. Estas técnicas, según (Nutanix, 2024a), proponen un modelo de técnicas que evalúan la eficiencia de los controles de seguridad en la red usando el paradigma de Goal-Question-Metric (GQM), permitiendo alinear las mediciones con los estándares de las ISO/IEC 27001 y facilitando la gestión de seguridad.

Este enfoque consolida la gestión de seguridad como uno de los pilares más importantes porque, en un marco centralizado, marca una diferencia en su metodología, asegurando que las defensas de las redes respondan de manera efectiva y eficiente ante amenazas emergentes.

1.9 Concepto de Escalabilidad, Alta Disponibilidad y Tolerancia a Fallos

1.9.1 Concepto de escalabilidad

La escalabilidad es un diseño de sistemas distribuidos que busca mantener o mejorar su rendimiento a medida que aumenta la carga de trabajo, sin recurrir a gastos innecesarios ni bajando la calidad del servicio. Un sistema escalable puede desplegarse en diferentes sectores para su operatividad de forma eficaz, manteniendo la calidad y servicio del trabajo. Esto permite evaluar a distintos diseños que puedan mantenerse efectivos y enfocados conforme se expandan las cargas de trabajo (Jogalekar, 2000).

Una orientación más reciente dentro de los sistemas distribuidos: la escalabilidad efectiva no depende del crecimiento de los recursos únicamente, sino de una arquitectura coherente, estratégica, con protocolos que optimicen el despliegue de recursos, minimizando el cuello de botella (Yang, 2025).

1.9.2 Escalabilidad Horizontal

Escalado o reducción horizontal, en el que se incorporan más bases de datos o se segmenta una base de datos de gran envergadura en nodos más reducidos, a través de la generación de particiones de datos (sharding), que pueden gestionarse de manera más ágil y simple en múltiples servidores (Microsoft, 2025).

1.9.3 Escalabilidad Vertical

Escalado o disminución vertical, en el que se incrementa o disminuye la capacidad de proceso o bases de datos de acuerdo a la necesidad, ya sea modificando los niveles de desempeño o utilizando grupos de bases de datos elásticas para adaptar automáticamente la capacidad a la necesidad de la carga labora (Hewlett Packard , 2025).

Escalado o disminución vertical, en el que se incrementa o disminuye la capacidad de proceso o bases de datos de acuerdo a la necesidad, ya sea modificando los niveles de desempeño o utilizando grupos de bases de datos elásticas para adaptar automáticamente la capacidad a la necesidad de la carga laboral (Microsoft, 2025).

Consiste en añadir recursos similares para gestionar la carga de trabajo. Un ejemplo de este tipo escalado acontece cuando una aplicación se ejecuta en un servidor dedicado; por ende, la carga de trabajo aumenta (Hewlett Packard , 2025). La escalabilidad horizontal en este caso ayuda a añadir más servidores para distribuir la carga adicional. Se utilizan procesos como el equilibrio de cargas, la computación distribuida y la agrupación en clústeres para lograr la escalabilidad horizontal.

1.9.4 Alta Disponibilidad

La alta disponibilidad (HA, por sus siglas en inglés, High Availability) se refiere a la capacidad de un sistema que opera de manera continua durante periodos prolongados, comprimiendo el tiempo de inactividad. Según (Gray & Siewiorek, 1991), los sistemas de alta disponibilidad ofrecen niveles de orden del 99.9999%, lo que tiene una interrupción de aproximadamente 5 minutos al año. Citando a (Gray & Siewiorek, 1991), esta precisión es de suma importancia, ya que, al tratarse de sistemas en los que incluso breves fallos pueden desencadenar pérdidas económicas, riesgos operativos o comprometer vidas humanas, como ocurre en aeropuertos, centros de salud e instituciones de telecomunicaciones.

La siguiente tabla representa una clasificación de sistema según el nivel de disponibilidad, expresado en porcentaje como en minutos de inactividad permitidos en el año, permitiendo diferenciar entre sistema gestionado y aquellos con tolerancia a fallos.

Tabla 1

Clases de disponibilidad de sistemas según el tiempo de inactividad anual estimado en inglés(adaptado de Gray 1990, p.250).

System type	Unavailability (minutes/year)	Availability (%)	Availability class
Unmanaged	50,000	90.00	1
Managed	5,000	99.00	2
Well-managed	500	99.90	3
Fault-tolerant	50	99.99	4
High-availability	5	99.999	5
Very-high-availability	0.5	99.9999	6
Ultra-availability	0.05	99.99999	7

Para que sea más fácil entender los niveles de disponibilidad en los sistemas tecnológicos, se incluye a continuación la tabla de clases de disponibilidad que propuso Gray (1990), adaptada al español. Esta versión mantiene la estructura original, pero presenta de manera más accesible los rangos de tiempo que un sistema podría estar fuera de servicio al año, medidos en minutos, junto con el porcentaje de disponibilidad y su categoría. Esta tabla resulta muy útil para medir qué tan fiable es una infraestructura y definir estándares que aseguren la continuidad del servicio, especialmente en ambientes donde es crítico que el sistema esté disponible la mayor parte del tiempo, como sucede con los sistemas hiperconvergentes y los centros de datos de las empresas.

Tabla 2

Clases de disponibilidad de sistemas según el tiempo de inactividad anual estimado traducido al español (adaptado de Gray 1990, p.250).

Tipo de sistema	Indisponibilidad (minutos/año)	Disponibilidad (%)	Clase de disponibilidad
No gestionado	50,000	90.00	1
Gestionado	5,000	99.00	2
Bien gestionado	500	99.90	3
Tolerante a fallos	50	99.99	4
Alta disponibilidad	5	99.999	5
Disponibilidad muy alta	0.5	99.9999	6
Ultra-disponibilidad	0.05	99.99999	7

1.9.5 Tolerancia a Fallos

La tolerancia a fallos en sistemas distribuidos se entiende como una propiedad fundamental que garantiza la continuidad del servicio en entornos críticos. Según (M. Shah, 2001), hace referencia a este concepto como la capacidad de un sistema para mantener funcionando normal a pesar de que algunos errores se presenten en sus componentes, evitando que las fallas se propaguen o afecten a los usuarios finales. Un sistema tolerante a fallos, al detectar problemas tanto en software como en hardware, debe buscar la mejor manera de solucionarlo automáticamente, de manera que se aísle, recupere y sustituya los elementos comprometidos.

1.10 Conceptos de Modelos Hiperconvergentes en la Nube

1.10.1 Infraestructura como Servicios (IaaS)

Las infraestructuras con servicios (IaaS) forman parte importante dentro del paradigma de computación de la nube, brindando servicios de capacidad de aprovisionamiento y gestión de recursos informativos esenciales como almacenamiento, administración, procesamiento y redes y otros componentes mediante los entornos virtuales que se administran por un solo proveedor. Según Mell & Grance (2011), establece como un modelo que permite consumir, implementar y manejar sistemas operativos, con sus configuraciones y aplicaciones propias, sin la necesidad de administrar un software físico establecido (Mell & Grance, 2011).

En definitiva, los servicios IaaS, al involucrarse con las tecnologías actuales, se convierten en una alternativa flexible y escalable, ya que representan cambios de paradigma hacia modelos de consumos tecnológicos más eficientes, donde la infraestructura deja de ser un activo fijo y costos para convertirse en un servicio dinámico alineado a sus objetivos estratégicos (Mell & Grance, 2011).

1.11 Herramientas de Virtualización

Las plataformas HCI son importantes al momento de implementar servicios en un centro de datos, pues se busca maximizar la rentabilidad y asegurar escalabilidad, administración, flexibilidad y soporte. En términos prácticos, se clasifican en tres herramientas importantes:

1.11.1 Proxmox Virtual Environment

Es una herramienta central y empresarial de código abierto basada en Debian GNU/Linux y la licencia basada en GNU AGPLv3. Desde sus inicios en 2008 ha venido evolucionando al paso de los años con la combinación de virtualización mediante KVM y contenedores logrados con LXC; eso se gestiona a través de una plataforma web centralizada. Proxmox llegó a ser una solución flexible, de bajo costo para las infraestructuras hiperconvergentes HCI y en los entornos distribuidos; se destaca por su escalabilidad, protegiendo los entornos virtuales complejos de forma sencilla y abierta (Proxmox Server Solutions GmbH, 2025).

Figura 3
Logotipo de Proxmox

Nota: Elaboración propia a partir de (Proxmox Server Solutions GmbH, 2025)

1.11.2 VMware ESXI/ vSphere

Al ser un hipervisor de tipo 1, al ser diseñado para ejecutarse sobre el hardware físico, no tiene la necesidad de un sistema operativo adicional, al tener una ventaja que administra todos los recursos de la máquina huésped mediante un microkernel llamado vmkernes. Esta arquitectura, al ser ligera, reduce la superficie de ataque, mejorando así el rendimiento en los entornos virtuales (Perneel et al., 2015).

1.11.3 Nutanix AHV

Nutanix Prism es una interfaz de usuario que se especializa en simplificar la gestión de infraestructura hiperconvergente, centralizando la administración de clústeres en un solo panel y ofreciendo administración visual para integrar los recursos de cómputo, almacenamiento y red. Esta plataforma, gracias a su facilidad de uso, reduce la carga de trabajo de manera considerable; la complejidad operativa también mejora mediante mecanismos inteligentes basados en machine learning, que optimizan recursos y prevén incidentes que podrían afectar la disponibilidad de los servicios. Su diseño intuitivo la convierte en una plataforma híbrida que integra el mundo virtual con componentes normalmente utilizados, como almacenamiento, memoria y redes (Nutanix, 2024a).

Tabla 3

Cuadro comparativo entre herramientas: Proxmox, VMware ESXi/vSphere y Nutanix AHV

Herramienta	Proxmox Virtual Environment	Vmware ESXi/vSphere	Nutanix AHV
Tipo de hipervisor	Basado en KVM (tipo 1) + LXC (contenedores)	Hipervisor bare-metal tipo 1 (vmkernel)	Basado en KVM (customizado como AHV)
Licenciamiento y costos	Gratuito, open source (modelo libre, sin costos de licencia)	Licencia comercial costosa, modelo escalonado según recursos	Modelo de suscripción, intermedio en costos; incluye integración con todo el stack HCI
Administración	Interfaz web propia (Proxmox GUI); requiere más conocimientos técnicos y scripting	vCenter como consola de gestión centralizada; maduro y robusto	Prism como interfaz única para cómputo, red, almacenamiento y virtualización
Alta disponibilidad (HA)	Implementada mediante Corosync y pmxcfs	Opciones avanzadas: HA, vMotion, DRS, Fault Tolerance	HA integrada con administración automática en entornos híbridos y multinube
Escalabilidad	Escalable horizontalmente, pero requiere ajustes manuales	Altamente escalable, probado en grandes corporaciones	Escalable nativamente, diseñado para crecer en entornos HCI multinube
Almacenamiento	Soporte nativo para ZFS, Ceph, LVM, iSCSI	Integración con VSAN, NFS, iSCSI y soluciones de terceros	Integración automática con almacenamiento definido por software de Nutanix
Uso típico	Pymes, laboratorios, entornos académicos, entusiastas	Grandes corporaciones, bancos, hospitales, entornos críticos	Empresas que adoptan HCI, entornos híbridos o multinube, transformación digital

Nota: Los costos/licencias pueden variar por edición, bundle y soporte contratado. Selecciona la opción considerando TCO (CAPEX + OPEX), skills del equipo, requisitos de HA/DR, y estrategia (on-prem, híbrido o multinube).

1.11.4 Hiperconvergencia en la Nube

En el ámbito de la hiperconvergencia, la cloud HCI representa la evolución natural: integra capacidades nativas de nube y ofrece plataformas modulares, escalables y definidas por software. Según Cisco, una HCI combina cómputo virtualizado, almacenamiento y redes en un clúster único, con aprovisionamiento y operación automatizados (Cisco System, 2025).

CAPÍTULO 2
ESTADO DEL ARTE

Respecto a los estudios realizados sobre infraestructuras hiperconvergentes, se han identificado diferentes propuestas que analizan los beneficios y el impacto que genera la adopción de este tipo de tecnologías en las organizaciones. Estas investigaciones destacan cómo la HCI optimiza recursos, reduciendo la complejidad operativa y mejorando la calidad frente a las tecnologías actuales. En el trabajo de (Turkkan et al., 2025), compara diferentes sistemas distribuidos, desde algoritmos básicos hasta aplicaciones complejas como ZooKeeper o Spanner; comparten un problema en general al no existir herramientas que estandaricen la evaluación, lo que obliga a improvisar sus propias pruebas, ignorando aspectos fundamentales como la consistencia de datos y la tolerancia a fallos, al identificar las métricas que son importantes para su evaluación de los sistemas (rendimiento, escalabilidad, disponibilidad y consistencia) y los factores que afecten el comportamiento de la práctica, en proporción entre operaciones, tanto lectura como escritura; estos se superponen a los accesos a los mismos datos. El análisis reveló que incluso herramientas conocidas como YCSB (Yahoo! Cloud Serving Benchmark) tiene limitaciones significativas al no contar con entornos distribuidos; se reflejan en la falta de parámetros cruciales para evaluar los sistemas adecuadamente.

En el trabajo de (Malhotra et al., 2025) detalla la comparación de tres sistemas de archivos distribuidos que manejan el entorno de fallo y la escalabilidad dependiendo de las necesidades, como Google File System (GFS), Hadoop Distributed File System (HDFS) y MinIO. Los autores destacan que los sistemas, al tener una gran carga de trabajo, es necesario que trabajen conjuntamente de manera confiable y eficiente; al momento de acceder a los archivos, es de suma importancia en el centro de investigaciones acceder a esta información.

HDFS fue diseñado pensando en equipos convencionales y económicos. Su arquitectura gira en torno a un NameNode que se encarga de organizar y administrar toda la información del sistema. Está optimizado para procesar grandes volúmenes de datos de forma secuencial, aunque esto implica sacrificar velocidad de respuesta inmediata. Funciona mejor en escenarios donde los datos se escriben una vez y se leen muchas veces.

GFS toma un camino diferente: relaja algunas garantías de consistencia para ganar flexibilidad y poder crecer más fácilmente. Trabaja con bloques grandes de 64 MB y usa un sistema de permisos temporales para coordinar cuando varios usuarios quieren escribir al mismo tiempo.

MinIO representa una generación más reciente, pensada específicamente para la nube. Lo interesante es que no depende de un nodo central, lo que lo hace más robusto. Además, usa una técnica llamada erasure coding que protege los datos ocupando menos espacio que simplemente hacer copias, y consume menos recursos de procesador y memoria. El estudio plantea que no hay un sistema perfecto para todos los casos. La elección depende de qué tan crítica sea la disponibilidad continua, qué tan bien deba resistir fallos el sistema y si necesita integrarse con plataformas cloud, factores que varían según las necesidades de cada organización.

Tal y como menciona (A. Shah, 2025), intenta normalizar el funcionamiento real de los sistemas distribuidos, centrándose en tres ideas principales: cómo crecen cuando hay más demanda, cómo se organizan en piezas independientes y cómo siguen funcionando, aunque algo falle. También comenta la importancia de que todos los componentes tengan información coherente. Los autores cuentan que las empresas han dejado atrás poco a poco las aplicaciones tradicionales que eran un solo bloque gigante, optando por dividirlas en servicios más pequeños e independientes. Este cambio tiene sentido; necesitan sistemas que puedan adaptarse rápido y crecer sin colapsar cuando llegan picos de uso.

Sobre el crecimiento del sistema, explican dos formas de hacerlo: puedes conseguir servidores más potentes, o mejor aún, repartir el trabajo entre muchos servidores más pequeños. La idea de modularidad es bastante intuitiva: si divides tu aplicación en partes más chicas, cada equipo puede trabajar en su pedazo sin romper lo que están haciendo los demás. Para que estas partes se enlacen entre sí, usan desde comunicación directa hasta sistemas de mensajes que funcionan como una bandeja de entrada, con mecanismos inteligentes que reintentan varias veces si algo no funciona a la primera.

Lo interesante de la tolerancia a fallos es que básicamente tienes copias de todo lo importante. Y más allá de eso, el sistema puede darse cuenta solo cuando algo anda mal y arreglarlo sin que nadie tenga que intervenir manualmente.

En el estudio de (Kreutz et al., 2014), hace referencia a redes definidas por software (SDN), que básicamente representan una forma completamente nueva de pensar cómo funcionan las redes.

Como, por ejemplo, cuando uno imagina que antes cada switch o router en una red tomaba sus propias decisiones sobre por dónde enviar los datos. Con SDN, separas la parte que piensa y decide de la parte que simplemente ejecuta las órdenes. Se trata de separar la capa de decisión estratégica de la capa de ejecución operativa. Esto equivale a transitar desde un modelo donde cada nodo toma decisiones autónomas de manera independiente, hacia una arquitectura donde existe un elemento coordinador centralizado que gestiona y supervisa todas las operaciones de forma coherente y eficiente.

Para que esto funcione, hay dos canales de comunicación fundamentales: uno "hacia abajo" (la interfaz Southbound) que conecta el controlador con los equipos de red reales, donde OpenFlow es el lenguaje más usado; y otro "hacia arriba" (la interfaz Northbound) que básicamente abre la puerta para que cualquier programador pueda crear aplicaciones que hablen directamente con la red, como si fuera una plataforma más de desarrollo.

Algo interesante que resaltan los autores es que, aunque SDN habla de control centralizado, en la práctica esto no significa poner todo en un solo servidor. Las implementaciones reales distribuyen el controlador entre múltiples nodos precisamente para evitar que todo se caiga si algo falla. Controladores como ONOS, Onix e HyperFlow demuestran cómo esta arquitectura distribuida mantiene el sistema funcionando incluso cuando algún componente tiene problemas, garantizando tanto el rendimiento como la continuidad del servicio. Los sistemas reales reparten el trabajo entre varios controladores para que, si uno falla, los demás sigan funcionando. Proyectos como ONOS, Onix e HyperFlow demuestran que esto funciona bien.

En base al estudio de (Leiva Vilaplana et al., 2023), examina cómo la virtualización está cambiando los sistemas de protección y control en subestaciones eléctricas, evaluando si esta transformación realmente justifica la inversión desde una perspectiva tanto económica como social. La idea se basa en reemplazar equipos físicos por soluciones de software (máquinas virtuales o contenedores) que realizan las mismas funciones, pero con mayor flexibilidad y capacidad de adaptación. Se emplean

herramientas de análisis financiero junto con modelos de simulación dinámica para proyectar el comportamiento de los costos en el tiempo. Al comparar dispositivos físicos tradicionales con sus equivalentes virtualizados, considerando diferentes estrategias de mantenimiento, los resultados muestran ahorros significativos: un 20% en la inversión inicial y hasta un 60% en actualizaciones posteriores.

La virtualización también trae beneficios ambientales y operativos: menos tiempos muertos cuando algo falla, menor consumo de energía y, por tanto, una huella de carbono más pequeña. Esto hace que el sector eléctrico sea más sostenible; no es todo color de rosa. Hay riesgos que considerar: la tecnología todavía está madurando, hay que pagar licencias de software, los servidores tienen una vida útil más corta que los equipos tradicionales (lo que puede encarecer el mantenimiento a largo plazo) y hay que planificar bien cómo implementarlo.

En base al estudio de (Al-Kubaisi et al., 2025), explora cómo optimizar los centros de datos en la nube, poniendo especial atención en algoritmos que aprovechan las energías renovables al momento de asignar recursos. Debido a que estos centros consumen demasiada electricidad a nivel global, hacerlos eficientes no es solo cuestión de ahorrar dinero, sino también de reducir su impacto ambiental. La idea es bastante ingeniosa al ajustar automáticamente cuándo y dónde se procesan las tareas según haya más o menos energía limpia disponible.

Los investigadores distinguen entre métodos tradicionales (como ajustar voltaje y frecuencia de los procesadores, o juntar varias tareas en menos servidores) y enfoques más modernos que usan modelos de predicción para anticipar cuánta energía solar o eólica habrá disponible y planificar en consecuencia. Aquí es donde la inteligencia artificial y el machine learning están marcando diferencia, permitiendo que los sistemas aprendan patrones y tomen decisiones cada vez más precisas de forma automática.

Los ejemplos reales son interesantes: Google usa un sistema que mueve cargas de trabajo hacia centros de datos en regiones donde la electricidad es más limpia en ese momento, mientras que Azure tiene un mecanismo que ajusta qué recursos usa dependiendo de cuánta energía renovable esté entrando al sistema.

Los autores Assiri & Sheneamer (2025), presenta una propuesta innovadora que usa deep learning para que los sistemas distribuidos puedan seguir funcionando, aunque fallen algunos de sus componentes. El problema más común es qué hacer cuando uno de los procesadores deja de funcionar correctamente. En lugar de repetir todo el trabajo desde cero, se encargan de entrenar un modelo de aprendizaje profundo con los datos de los procesadores estén funcionando de manera correcta, ese modelo aprende a predecir el resultado que habrá dado el procesador que falló, esto acelera mucho la recuperación y hace que el sistema sea más eficiente.

La investigación evaluó el sistema ante tres tipos de fallos que suelen ocurrir en la práctica: el primero, donde los datos que llegan son válidos pero el procesador genera resultados incorrectos; el segundo, donde tanto los datos de entrada como la salida están comprometidos; y el tercero, donde el procesador recibe información completamente ajena a su tarea, produciendo respuestas sin sentido.

Los trabajos Heredia (2023) y Curto (2023) aportan un Modelo hiperconvergente basado en software libre. Brinda una solución gratuita que sirve para la creación de infraestructuras hiperconvergentes encaminada a pequeñas y medianas empresas, a través de la generación de un prototipo en donde se utiliza la metodología de empresa-academia hasta la etapa de validación. Como consecuencia en este trabajo se consiguió una matriz de comparación de software libre de virtualización de servidores que se iguala a Proxmox VE como la mejor opción de hipervisor, conjuntamente se identificó seis pasos para la creación un prototipo.

El trabajo de investigación de Lara (2023) analizó las amenazas emergentes a la infraestructura de redes y especificar estrategias óptimas para su protección. En donde se utilizó una metodología cualitativa para la revisión de literatura especializada. Los resultados mostraron una creciente sofisticación de los ciberataques dirigidos a la infraestructura de red. En donde se destaca el requerimiento de implementar medidas de seguridad proactivas y adaptativas. Se establecieron varias estrategias de protección, que incluye el uso de inteligencia artificial y aprendizaje automático para detectar y mitigar amenazas en tiempo real. En este trabajo se analizó como la convergencia tecnológica, las infraestructuras deben evolucionar. La hiperconvergencia que es definida por software, que representa una evolución de los centros de datos. Ya que se ofrece una

mayor eficiencia y seguridad. El trabajo de (Moreira et al., 2019) corrobora que la seguridad en redes inalámbricas es un ámbito de investigación creciente debido a la demanda de conectividad elevada.

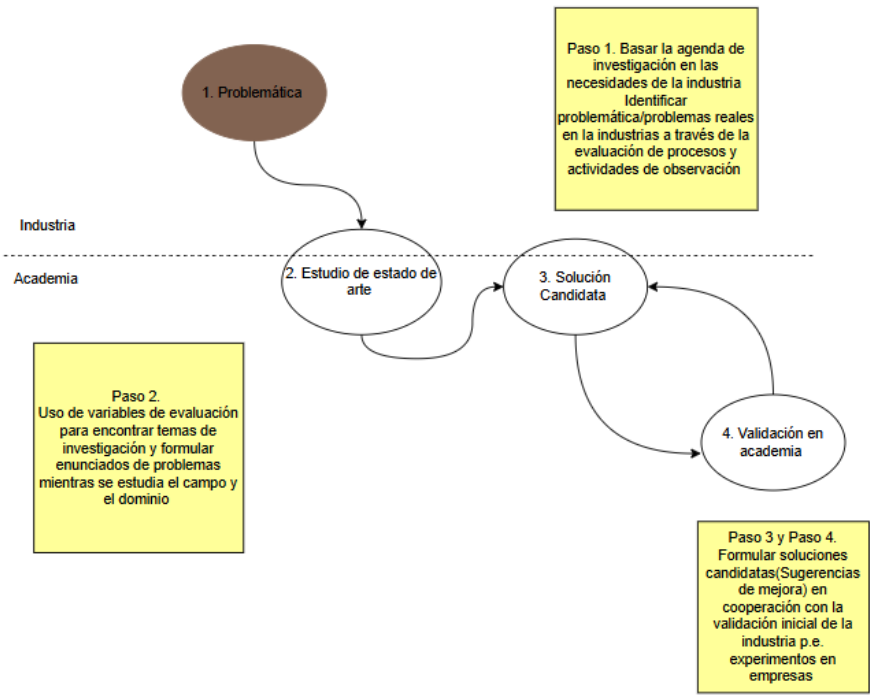
CAPÍTULO 3
MATERIALES Y MÉTODOS

3.1 Metodología

El presente trabajo se basa sobre el Modelo de Transferencia de Tecnología propuesto por Gorschek & Larsson (2006), en el cual se establece un proceso investigativo que permitirá plasmar el conocimiento teórico orientado a la implementación práctica. Este modelo busca identificar las necesidades reales de las industrias o sectores de servicios. Se desarrolló en cuatro etapas debido a los requerimientos del trabajo de titulación. Las cuatro etapas antes mencionadas son: i) Plantear una investigación en base a las necesidades de las industrias; ii) Realizar una investigación exhaustiva de literatura sobre infraestructuras tradicionales e infraestructuras hiperconvergentes; iii) Generar una solución candidata en base a la revisión de literatura, lo cual aporta enfoques innovadores hacia la construcción final de manera que sea implementado el Marco de Referencia y, finalmente, iv) Validación de soluciones. A continuación, se presenta el modelo adaptado para titulación que conlleva estas cuatro fases del Modelo de Transferencia Tecnológica de Gorschek & Larsson, (2006), obteniendo un entorno académico más eficiente.

Figura 4

Metodología de investigación



Nota. Adaptada de (Gorschek & Larsson, 2006)

3.1.1 Análisis del Problema

En esta fase de análisis, el propósito principal es identificar la problemática existente en torno a la gestión de las infraestructuras tecnológicas, fundamentándose en la observación sistemática y en el estudio de las necesidades reales que presentan las organizaciones en el ámbito de las tecnologías de la información. Se ha evidenciado que muchas empresas aún enfrentan dificultades en la administración de infraestructuras hiperconvergentes e incluso carecen del conocimiento suficiente sobre estas tecnologías, las cuales integran en una sola plataforma los recursos de cómputo, almacenamiento y red. Esta situación se ve agravada por la ausencia de marcos de referencia estandarizados que orienten su gestión de manera eficiente, lo que genera vacíos en la administración y en la toma de decisiones. Ante este panorama, resulta pertinente considerar los principios del modelo de gestión FCAPS (Fault, Configuration, Accounting, Performance y Security), que buscan garantizar la comunicación efectiva, la escalabilidad, la seguridad, la operatividad y la optimización de costos de los servicios. Dicho modelo permite un monitoreo integral de las infraestructuras y la implementación de mecanismos de seguridad que reduzcan vulnerabilidades, con lo cual se fortalece el aprovechamiento y el rendimiento de las soluciones hiperconvergentes.

3.1.2 Revisión de la Literatura

En esta etapa se realizó una investigación sistemática de análisis y recopilación de información, orientándose a comprender los principios de la infraestructura hiperconvergente (HCI). La búsqueda y selección de la información se obtuvo de bases de datos y repositorios científicos de alto prestigio, tales como: Scopus, Scielo e IEEE Xplore, las cuales permiten acceder de manera gratuita y de calidad alta. Para garantizar la veracidad de los documentos encontrados y su pertenencia, se prioriza el idioma español, contribuyendo a las lenguas predominantes en la producción científica y técnica del área.

3.1.3 Formulación de la Solución Candidata

En esta etapa se realizó una matriz de comparación de infraestructura tradicional contra una infraestructura hiperconvergente (HCI). El propósito de la matriz es identificar de manera estructurada, tomando como base los modelos de la gestión de redes FCAPS (Fault, Configuration, Accounting, Performance y Security). Este estudio permitió tener

ambos enfoques, considerando aspectos como la gestión de fallos, gestión de configuración, gestión de contabilidad, gestión de rendimiento y gestión de seguridad.

La gestión de redes es un pilar fundamental dentro de la gestión tecnológica; encuentra las falencias en los entornos actuales de escalabilidad, flexibilidad y eficiencia de las infraestructuras hiperconvergentes, ya que cuenta con mayores ventajas en cuanto a indicadores; esto lo convierte en una opción más estratégica y adecuada para organizaciones que buscan modernizar su infraestructura tecnológica y optimizar mayor calidad operativa.

3.1.4 Procedimiento Metodológico

En esta etapa se procede con la validación del modelo propuesto; se considera el desempeño técnico como su comparación ante una infraestructura tradicional. Para ello se diseñó un marco de referencia basado en el modelo FCAPS (Fault, Configuration, Accounting, Performance y Security) que permite integrar indicadores específicos en cada dimensión del modelo. Dicho marco permitirá medir la escalabilidad, operatividad y las tolerancias a fallos, incluyendo pruebas de servicios en tiempo real, interrupción controlada de servicios con el fin de medir la efectividad de los mecanismos de alta disponibilidad.

3.2 Materiales

Para la generación del marco de referencia, se implementaron diversos recursos de carácter documental, los cuales permitieron fundamentar y validar la propuesta de la implementación y gestión de infraestructuras hiperconvergentes (HCI), bajo los principios del modelo de gestión de redes. En la búsqueda de bibliografía científica, informes técnicos y normas internacionales, obtenidos en las bases de datos académicas como: Scopus, IEEE, Xplore y Scielo. Nos permiten identificar de manera fundamental conceptos técnicos de la hiperconvergencia; al profundizar en el estudio, se identificaron los pilares fundamentales que sustentan la gestión de redes, conocidos como FCAPS (Fault, Configuration, Accounting, Performance y Security); para ello es necesario realizar una comparación frente a la infraestructura tradicional. En este contexto se destaca información relevante de (Acceleron Labs Pvt Ltd, 2018),(Antonenko,

2024),(Cisco System, 2025),(Nutanix, 2024b) , (Intel, 2025), que ayudan a la mejor comprensión de HCI. En cambio, los trabajos de (Fulber-Garcia, 2024) y (Gillis, 2025), aportan elementos clave para la comprensión de los entornos que abarcan los modelos de la gestión de redes. A continuación, se presenta la matriz comparativa, fundamentada en los indicadores del modelo de gestión de redes FCPAS (Fault, Configuration, Accounting, Performance y Security). Cada uno de estos indicadores posee métricas específicas, las cuales son detalladas:

Tabla 4

Indicadores Principales por Dimensión del Modelo FCAPS

Indicador del modelos FCAPS	Indicadores Principales
Fault (Gestión de Fallos	Tiempo medio de detección de fallas (MTTD) Tiempo medio de recuperación (MTTR) Número de incidentes críticos reportados Nivel de redundancia / tolerancia a fallos
Configuration (Gestión de configuración)	Nivel de automatización en la configuración Control y trazabilidad de cambios Facilidad de despliegue de nuevos servicios Escalabilidad en la configuración
Accounting (Gestión de Contabilidad)	Costos operativos (OPEX) Costos de inversión (CAPEX) Eficiencia en el uso de recursos (CPU, RAM, almacenamiento) Transparencia y monitoreo del consumo de servicios
Performance (Gestión de Rendimiento)	Latencia promedio Ancho de banda disponible Porcentaje de disponibilidad del servicio (SLA) Escalabilidad ante cargas de trabajo variables
Security (Gestión de Seguridad)	Nivel de autenticación y control de accesos Cumplimiento de políticas y normativas Integridad y respaldo de la información Detección y prevención de intrusiones

Nota: La tabla resume los indicadores principales del modelo FCAPS y compara su comportamiento en infraestructura tradicional y en HCI

Para comparar de forma ordenada una infraestructura tradicional con una hiperconvergente (HCI), diseñamos una matriz basada en el modelo FCAPS de gestión de redes. Este modelo es reconocido mundialmente como un estándar que ofrece indicadores confiables para medir eficiencia, escalabilidad, costos, rendimiento y seguridad en cada arquitectura.

La matriz incorpora una valoración porcentual para las distintas dimensiones de cada elemento de gestión. Esto nos permite identificar con claridad qué infraestructura responde mejor a las necesidades actuales, evaluando aspectos como flexibilidad y optimización de recursos. De esta manera, establecemos una base sólida para validar las

soluciones propuestas en la investigación y determinar cuál se adapta mejor a los requerimientos organizacionales modernos.

Tabla 5

Comparación FCAPS: Infraestructura Tradicional vs. HCI con fuentes

Dimensión FCAPS	Indicadores a evaluar	Infraestructura Tradicional	Infraestructura HCI	Autor/Fuente
Fault (Fallas)	Tiempo medio de detección (MTTD) Tiempo medio de recuperación (MTTR) Nivel de redundancia	Alta dependencia de hardware físico; detección lenta; recuperación prolongada; redundancia limitada y costosa.	Monitoreo en tiempo real; recuperación más rápida por virtualización y orquestación; redundancia integrada/alta disponibilidad.	(Fulber-Garcia, 2024) y (Gillis, 2025): definición FCAPS (Gray & Siewiorek, 1991): alta disponibilidad y tolerancia a fallos (Acceleron Labs Pvt Ltd, 2018),(Cisco System, 2025),(Intel, 2025),(Nutanix, 2024a, 2024b): como la HCI integra la HA y simplifica recuperación. (Nwakeze, 2024):monitoreo para detección
Configuration (Configuración)	Automatización de procesos Control de cambios Escalabilidad	Configuración manual propensa a errores; cambios lentos; baja elasticidad por silos.	Configuración centralizada definida por software; cambios ágiles (IaC/plantillas); escalabilidad por adición de nodos.	(Fulber-Garcia, 2024); (Gillis, 2025): "Configuration" de FCAPS (Cisco System, 2025),(Intel, 2025); (Schneider & Smalley, 2024a):definición de HCI, gestion unificada (Nutanix, 2024a, 2024b):(Parmar, 2019): automatización, SDS y gestión de software. (Quantum, 2021): comparación de arquitecturas y operaciones
Accounting (Recursos y costos)	Costos operativos (OPEX) Uso de recursos Transparencia en el consumo	Costos elevados por silos; bajo aprovechamiento; visibilidad limitada del consumo por servicio.	Menor OPEX por consolidación; mayor eficiencia de cómputo/almacenamiento; showback/chargeback y visibilidad por servicio.	(Fulber-Garcia, 2024); (Gillis, 2025): "Accounting" de FCAPS (Cisco System, 2025),(Intel, 2025); (Schneider & Smalley, 2024a): definición de HCI, (Antonenko, 2024; Arnav Sharma, 2023; CRN, 2022; Sheldon, 2020; Stephen Pritchard, 2021; World Financial Review, 2023): Casos de uso beneficios
Performance (Rendimiento)	Latencia Disponibilidad (SLA) Escalabilidad ante carga	Rendimiento dependiente de hardware específico; disponibilidad limitada por puntos únicos de fallo; escalabilidad lenta y costosa (dimensionamiento vertical o por silos).	Latencia optimizada por cercanía de cómputo-almacenamiento; metas de alta disponibilidad; escalabilidad modular/elástica por nodos.	(Fulber-Garcia, 2024); (Gillis, 2025): "Performance" de FCAPS (Cisco System, 2025),(Intel, 2025); (Schneider & Smalley, 2024a):definición de HCI, (Antonenko, 2024; Arnav Sharma, 2023; CRN, 2022; Sheldon, 2020; Stephen Pritchard, 2021; World Financial Review, 2023): casos de uso beneficios
Security (Seguridad)	Control de accesos Cumplimiento normativo Respaldo de datos	Seguridad fragmentada; cumplimiento parcial; respaldos externos poco integrados.	Seguridad integrada por software (segmentación, políticas centralizadas); autenticación/autoría unificada; copias automáticas y gestionadas.	(Fulber-Garcia, 2024); (Gillis, 2025): "Secutiry" de FCAPS (Cisco System, 2025),(Intel, 2025); (Schneider & Smalley, 2024a): definición de HCI, (Antonenko, 2024; Arnav Sharma, 2023; CRN, 2022; Sheldon, 2020; Stephen Pritchard, 2021; World Financial Review, 2023): casos de uso beneficios

Tras desarrollar la investigación y aplicar la matriz comparativa basada en el modelo FCAPS (Fault, Configuration, Accounting, Performance y Security), llegamos a una conclusión importante: la infraestructura hiperconvergente HCI representa una de las opciones más destacadas en tecnología actual, demostrando superioridad en casi todas las dimensiones evaluadas respecto a la infraestructura tradicional.

Esta conclusión no proviene de apreciaciones subjetivas, sino del contraste sistemático de indicadores técnicos y conocimientos documentados en literatura académica, normas internacionales y reportes industriales. A continuación, detallamos estos hallazgos:

Tabla 6

Comparación FCAPS entre Infraestructura Tradicional y HCI

Dimensión FCAPS	Indicadores clave	Infraestructura Tradicional	Infraestructura HCI	Evaluación
Fault (Gestión de fallas)	MTTD. MTTR. Redundancia.	Recuperación lenta. Redundancia limitada (**50%**).	Recuperación rápida. Monitoreo en tiempo real. Alta disponibilidad (**90%**).	Mejor HCI
Configuration (Configuración)	Automatización. Control de cambios. Escalabilidad.	Configuración manual. Poco flexible (**45%**).	Configuración centralizada. Escalable. Definida por software (**95%**).	Mejor HCI
Accounting (Recursos y costos)	OPEX. Eficiencia. Transparencia.	Altos costos. Baja eficiencia (**40%**).	Menor OPEX. Consolidación eficiente. Visibilidad total (**85%**).	Mejor HCI
Performance (Rendimiento)	Latencia Disponibilidad Escalabilidad	Latencia alta Disponibilidad limitada (**55%**)	Baja latencia. Disponibilidad 99.99%. Escalabilidad modular (**95%**)	Mejor HCI
Security (Seguridad)	Accesos Normativas Respaldo	Seguridad fragmentada Respaldos externos (**50%**)	Seguridad integrada. Autenticación centralizada. Copias automáticas (**90%**)	Mejor HCI

Nota: Los porcentajes y métricas operativas (disponibilidad lograda, porcentajes automatización, porcentajes uso, latencia p95, porcentajes parches/backup) deben calcularse con datos del entorno

Con el fin de tener un análisis económico de la matriz de la infraestructura tradicional con la infraestructura hiperconvergente (HCI), tomamos en cuenta los aspectos claves como la inversión inicial, costos operativos, el mantenimiento, la escalabilidad y el retorno de inversión. Todo esto mencionado se basa en la literatura revisada de (Cisco System, 2025; Nutanix, 2024b; World Financial Review, 2023), las cuales señalan que una HCI no solo reduce costos

de operatividad, sino que consolida recursos, facilitando la expansión modular y acelerando la recuperación de la inversión. A continuación, se detalla la tabla comparativa y los hallazgos obtenidos.

Tabla 7

Comparación económico operativa: Infraestructura Tradicional vs. HCI

Criterio de evaluación	Infraestructura Tradicional	Infraestructura HCI	Base de evaluación	
CAPEX (Inversión inicial)	Muy alto: requiere servidores. Almacenamiento y redes por separado.	Medio: integración en un solo sistema definido por software.	Análisis de inversión inicial en hardware y licencias.	
OPEX (Costos operativos)	Elevados: alto consumo energético. Gran espacio físico. Personal especializado.	Bajos: administración centralizada. Menor consumo energético.	Evaluación de costos recurrentes de operación y mantenimiento.	
Mantenimiento	Costoso: múltiples contratos con distintos proveedores. Soporte fragmentado.	Reducido: soporte unificado Menor necesidad de técnicos especializados.	Cantidad de proveedores y contratos necesarios para soporte.	
Escalabilidad	Limitada y costosa: requiere nuevo hardware e instalación manual.		Modular y ágil: basta con añadir nodos de forma inmediata.	Capacidad de expansión y costos asociados al crecimiento.
ROI (Retorno de inversión)	Bajo a mediano plazo: costos altos retrasan la recuperación.		Alto: rápida recuperación gracias a la reducción de OPEX.	Relación entre inversión inicial y beneficios obtenidos.

Nota: Los calificativos (“alto/medio/bajo”) son cualitativos. Para la tesis, conviértelos en métricas cuantitativas

CAPÍTULO 4
RESULTADOS

Para aplicar el marco FCAPS (Gestión de Fallos, Configuración, Contabilidad, Rendimiento y Seguridad) de la gestión de redes, se realizó una matriz comparativa donde el propósito es medir los indicadores característicos importantes donde se evalúa la confiabilidad y cuantificar la eficiencia de las infraestructuras de las cinco áreas de los FCAPS, la cual se desglosa en una presentación en cuadro de líneas.

De igual manera, se seleccionaron indicadores que permiten construir el modelo, partiendo de áreas fundamentales de la tecnología de la información, específicamente en la gestión de fallos, gestión de configuración, gestión de contabilidad, gestión de rendimiento y gestión de seguridad. Esta delimitación se obtuvo de las siguientes fuentes: (Cisco System, 2025; Fulber-Garcia, 2024; Nutanix, 2024a, 2024b).

Tabla 8

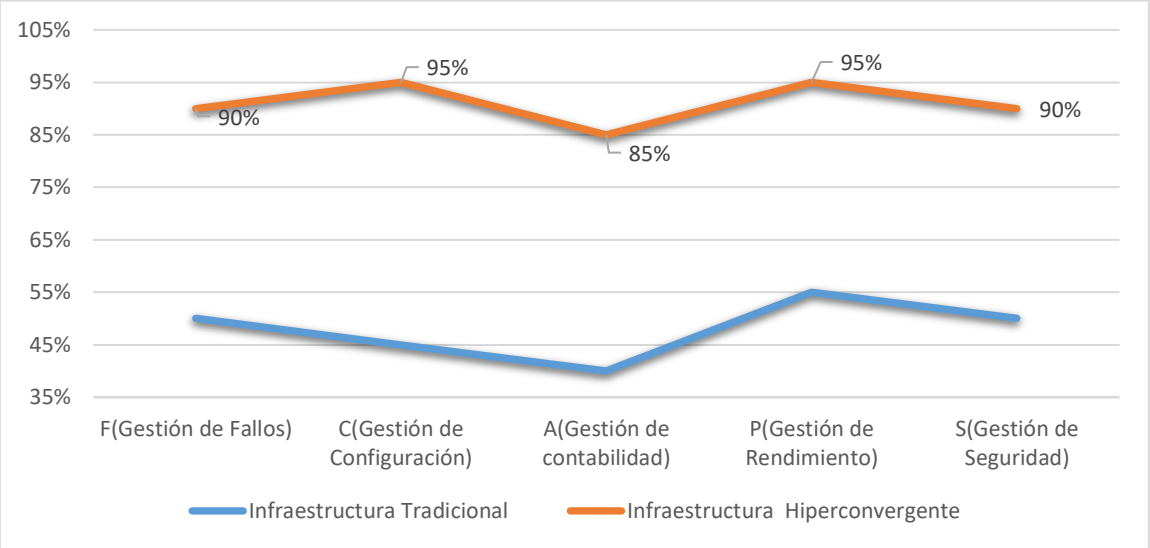
Índice Comparativo FCAPS (0–100) entre Infraestructura Hiperconvergente (HCI) e Infraestructura Tradicional

Pilar	Infraestructura Tradicional	Infraestructura Hiperconvergente
F(Gestión de Fallos)	50%	90%
C(Gestión de Configuración)	45%	95%
A(Gestión de contabilidad)	40%	85%
P(Gestión de Rendimiento)	55%	95%
S(Gestión de Seguridad)	50%	90%

Nota: Los porcentajes representan un índice normalizado (0–100) por dimensión FCAPS, donde 100 = desempeño óptimo respecto a criterios e indicadores operativos definidos Fuente basado en (Acceleron Labs Pvt Ltd, 2018; Antonenko, 2024; Cisco System, 2025; Fulber-Garcia, 2024; Gillis, 2025; Intel, 2025; Nutanix, 2024b)

Figura 5

Comparación de desempeño: Infraestructura Hiperconvergente vs. Tradicional



En el análisis de líneas comparativas del modelo FCAPS, se evidencia de forma clara y precisa que la infraestructura hiperconvergente (HCI) presenta un desempeño superior ante la infraestructura tradicional. Los resultados obtenidos demuestran que la HCI alcanza niveles sobresalientes dentro de los rangos establecidos, con un resultado entre el 85% y el 95%, mientras que la infraestructura tradicional mantiene niveles medios o incluso se evidencian bajos, entre el 40% y el 45%, evidenciando brechas significativas.

El pilar de la gestión de configuración (C), la HCI obtiene un sorprendente 95% de comparación de la infraestructura tradicional que alcanza apenas unos 45%. Esto revela una diferencia de 50 puntos entre infraestructuras; esto influye en varios factores, tanto como software, la automatización y la implementación de servidores.

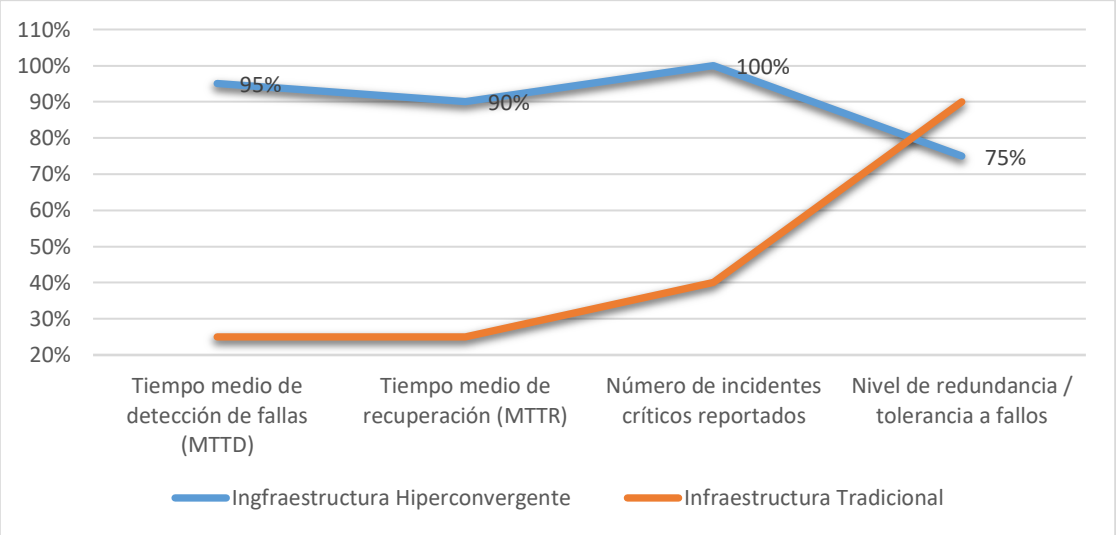
De manera similar, en el pilar de la gestión de contabilidad (A), la HCI obtuvo un 85% a comparación de la infraestructura tradicional, que obtiene un 40%, teniendo unos 45 puntos de diferencia. Esto se debe al uso de los recursos como costo operativo (OPEX) a largo plazo, que son de suma importancia para su análisis.

Finalmente, los pilares de la gestión de fallos (F), la gestión de rendimientos (R) y la gestión de seguridad (S), que respectivamente dentro de la HCI alcanzan un 90%, 95% y 90%, a diferencia de la infraestructura tradicional, que se queda en un 50%, 55% y 50%, con una diferencia de 40 puntos por debajo debido a su mayor continuidad del negocio

en el caso de la gestión de fallos, menor latencia en el caso de gestión de rendimiento y entornos seguros en el caso de la gestión de seguridad.

Figura 6

Gráfico de líneas: Fault (FCPAS) por indicador: HCI vs infraestructura tradicional



La gestión de fallos (F), al ser un pilar fundamental dentro de los FCAPS, desempeña un papel en la continuidad y la confianza que desarrolla en los sistemas de la empresa. Este aspecto de la HCI demuestra una ventaja operativa frente a la infraestructura tradicional. Para tener una mejor precisión en la detección de fallos, la HCI alcanza un 95% en comparación con la infraestructura tradicional, que obtiene 25%, evidenciando una brecha de 70 puntos en comparación de una con la otra. Esto se debe a que la HCI cuenta con una arquitectura de gestión centralizada e integrada donde supervisan todos los recursos desde una sola máquina, a diferencia de la infraestructura tradicional que, debido a un sistema fragmentado de sus sistemas, provoca que el personal encargado realice los procesos de manera manual de las diferentes áreas, como es el almacenamiento, el estado de la red, para poder tener algún tipo de diagnóstico que causan estos percances.

De igual manera, la HCI evidencia un porcentaje mayor en el tiempo medio de recuperación (MTTR), obteniendo un 90% de efectividad en comparación con la infraestructura tradicional, que se obtiene un 25%, con una brecha de 65 puntos. Eso se debe a que la HCI elimina los molestos inconvenientes al realizar actualizaciones o la pérdida de tiempo (downtime), que, al tener automatización y replicación de datos, reduce significativamente la necesidad de una intervención humana. A diferencia de la

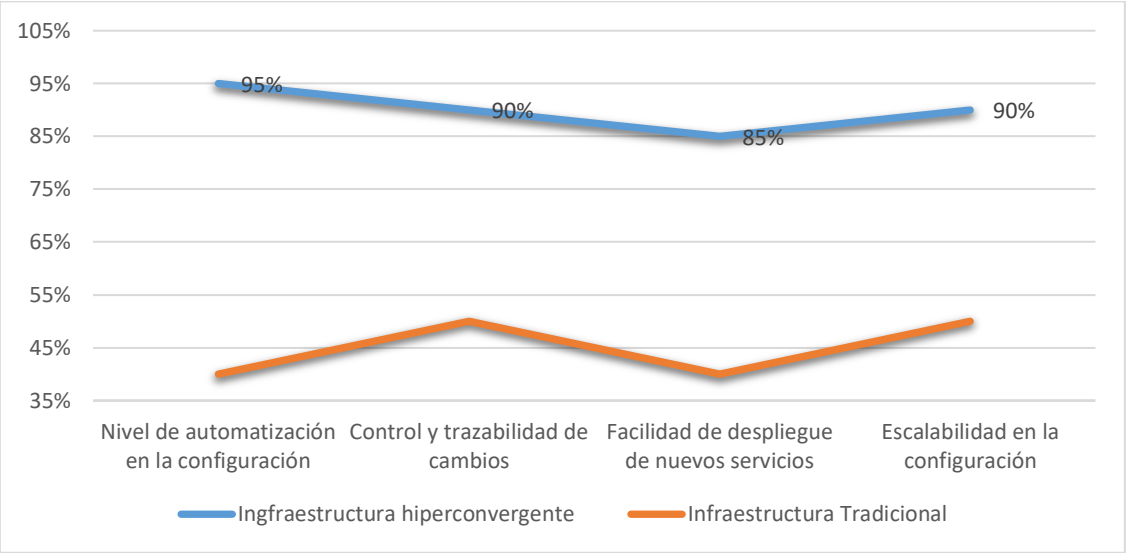
tradicional, que depende considerablemente de tareas humanas en cuanto a restauraciones de servicio, actualización y mantenimiento de equipos, esto exige una coordinación compleja de múltiples equipos, lo que alarga inevitablemente el tiempo de inactividad, elevando el riesgo de errores operativos.

Sin embargo, el indicador de número de incidentes críticos reportados en la HCI obtiene un valor del 100%, A diferencia de la tradicional, que obtiene un 40%, con una brecha de 60 puntos. Esto se debe a que en la HCI la capacidad total de evasión de fallos es importante, ya que previene crisis que son reportadas como críticas, debido a sus mecanismos implementados de autorreparación y la tolerancia a fallos que, al ser integrados en el sistema definido por software, logran solucionar problemas internos antes que notifiquen las alertas en todos los servicios. A diferencia de la tradicional, que no puede mitigar fallos de forma autónoma, ya que necesita la intervención humana y la coordinación de múltiples equipos, lo que se clasifica como incidentes críticos reportados al no ser resueltos de manera inmediata por el sistema.

Por último, tenemos el nivel de redundancia/tolerancia a fallos, que en la HCI obtiene un 75%, a diferencia de la tradicional, que obtiene un 90%, con una brecha de 15 puntos, debido a que en la HCI su redundancia de replicación de datos es a nivel de software; a diferencia de la tradicional, su redundancia de datos se orienta hacia el hardware físico especializado, lo que es una solución costosa, pero históricamente se convierte en una solución segura.

Figura 7

Gráfico de líneas: Configuration (FCPAS) por indicador: HCI vs infraestructura tradicional



Dentro de los pilares de la gestión de configuración (C), valida la simplificación operativa de cada uno de los indicadores en el nivel de automatización en la configuración. La HCI alcanzó un 95%, a diferencia de la tradicional, que alcanzó un corto 40%, con una brecha de 55 puntos. Es debido a que la HCI utiliza scripts y pantallas centralizadas para el despliegue de tareas, eliminando errores humanos o la intervención manual, a diferencia de la tradicional, que su manera de operar es segmentada y, por tal motivo, su implementación es forzada.

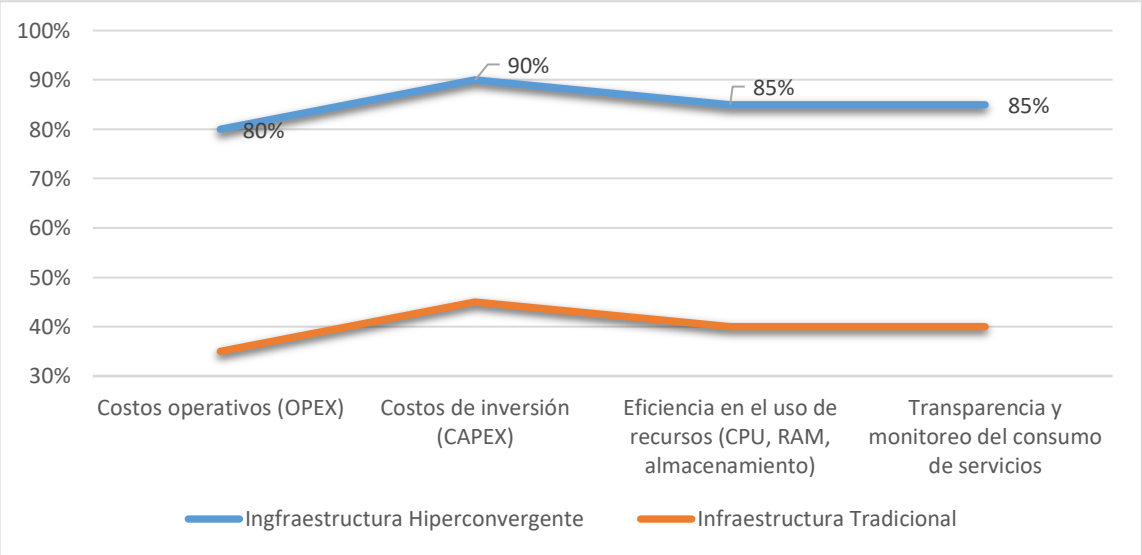
Por tanto, el control de trazabilidad de cambios en la HCI alcanzó un 90%, a diferencia de la tradicional, que alcanzó un 50%, con una brecha de 40 puntos. Esto debido a que registra y documenta cada proceso que se realiza en tiempo real, asegurando un historial completo de lo que permite saber qué se realizó y cuándo se lo hizo, a diferencia de la tradicional, que en ocasiones tiene documentos por separado, dificultando así el consultar los cambios realizados, lo que se convierte en un proceso lento, manual y repetitivo.

Por otro lado, la facilidad de despliegue de nuevos servicios en la HCI alcanzó un 85%, a diferencia de la tradicional, que obtuvo un 40%, con una brecha de 45 puntos. Por esta razón, en la HCI los equipos de TI permiten solucionar problemas tanto en el sistema en cuestión de minutos utilizando plantillas estándares. Por lo contrario, en la tradicional se requiere de personas capacitadas para su configuración; todo este proceso se vuelve

tedioso, el conectar puntos de redes, almacenamiento de cómputo y realizar pruebas, lo que incrementa su tiempo de comercialización; esto conlleva una alta probabilidad de riesgo en el momento de configurar.

Por último, escalabilidad en la configuración: en la HCI obtuvo un 90%, a diferencia de la tradicional, que obtuvo un 40%, dejando una brecha de 50 puntos. Esto se debe a que en la HCI no se requiere nueva reconfiguración manual, rediseñar la arquitectura de la red o ver si el almacenamiento es suficiente o, en caso contrario, expandirlo más. A diferencia de la tradicional, que de configuración se realizan de forma manual tanto los componentes de hardware como los de software, lo que resulta en un proceso costoso, lento y propenso a errores de configuración.

Figura 8
Gráfico de líneas: Accounting (FCPAS) por indicador: HCI vs infraestructura tradicional



En la gestión de contabilidad (A), aborda los ámbitos económicos de las infraestructuras, un factor primordial para la toma de decisiones al momento de su implementación. El costo de implementación (OPEX) en la HCI obtuvo un 80%, a diferencia de la tradicional, que obtuvo un 35%, lo que se diferencia con una brecha de 45 puntos de diferencia. Esto es debido a que la HCI simplifica procesos al momento de gestionar procesos de tareas rutinarias, requiere menos personal especializado para realizar trabajos de mantenimiento, reduce también el costo de energía y así también disminuye el mantenimiento de refrigeración, a diferencia de la tradicional, que necesita un personal capacitado para manejar de manera eficiente cada área que necesita ser

revisada. Esto conlleva un alto costo de recursos humanos, incluyendo el uso de energía a largo plazo.

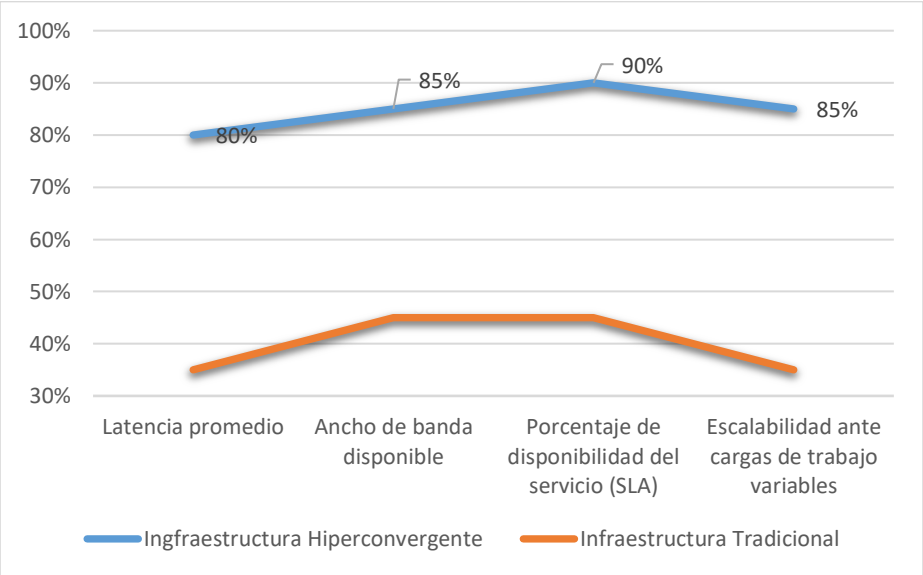
De igual manera, el costo de inversión (CAPEX) en la HCI obtuvo un valor del 90% a comparación de la tradicional, que obtuvo un 45%, dejando una brecha de 55 puntos de diferencia. Esto se debe a que la HCI puede escalar de manera progresiva gracias a su arquitectura, que permite agregar nodos individuales solo y cuando sea necesario, así eliminando la necesidad de sobrecargar la infraestructura. A diferencia de la tradicional, que requiere una inversión significativa al iniciar, ya que los hardware que utilizamos son costosos; además, ocupa almacenamiento que a lo largo del tiempo requeriría más por su forma de manejar los sistemas.

De tal manera, la eficiencia en el uso de recursos en la HCI obtuvo un 85%, a diferencia de la tradicional, que obtuvo un 40%; se evidencia una brecha de 35 puntos. Es debido a que la HCI, mecanismos integrados en el balance de carga de trabajo y la duplicación de datos, juega un papel fundamental al momento de optimizar al máximo la capacidad instalada, así ningún recurso esté desocupado. A diferencia de la tradicional, posee pocas herramientas unificadas para el consumo y tendencia al sobreaprovisionamiento, donde la capacidad de almacenamiento de cómputo suele compararse y configurarse en exceso, anticipando los picos de demanda.

Por último, y no menos importante, la transparencia y monitoreo del consumo de servicios; dentro de las HCI obtiene un valor del 85% a comparación de la tradicional, que obtuvo un 40%, dejando una brecha de 45 puntos de diferencia. Esto se debe a que la HCI facilita un tablero de control (dashboards) centralizados; esto permite visualizar en tiempo real el uso de la CPU, RAM y almacenamiento lo que permite implementar un almacenamiento, sistema de facturación interna. A diferencia de la tradicional, no cuenta con las plataformas que unifiquen la información sobre el consumo de la red y cómputo, lo que provoca un proceso lento y complejo con la precisión real de cada servicio.

Figura 9

Gráfico de líneas: Performance (FCPAS) por indicador: HCI vs infraestructura tradicional



La gestión de rendimiento (P): Este pilar es crítico, ya que la importancia radica en el impacto directo de los usuarios sobre la experiencia final. Este pilar lo que mide es si el sistema puede responder eficazmente ante los picos de demanda; para ello se analizaron los indicadores, obteniendo los siguientes resultados.

La latencia promedio dentro de la HCI obtuvo un valor de 80% a comparación de la tradicional, que obtuvo un 35%, dejando una brecha de 45 puntos de diferencia. Esto se debe a que en la HCI los recursos de cómputo están integrados en el hardware físico o muy cercanos, lo que elimina el tráfico excesivo de la red, a diferencia de un tradicional que se encuentra disperso en varios espacios. Esta información, al viajar por la red, evidentemente provoca demoras en el tiempo de respuesta y así aumenta la latencia.

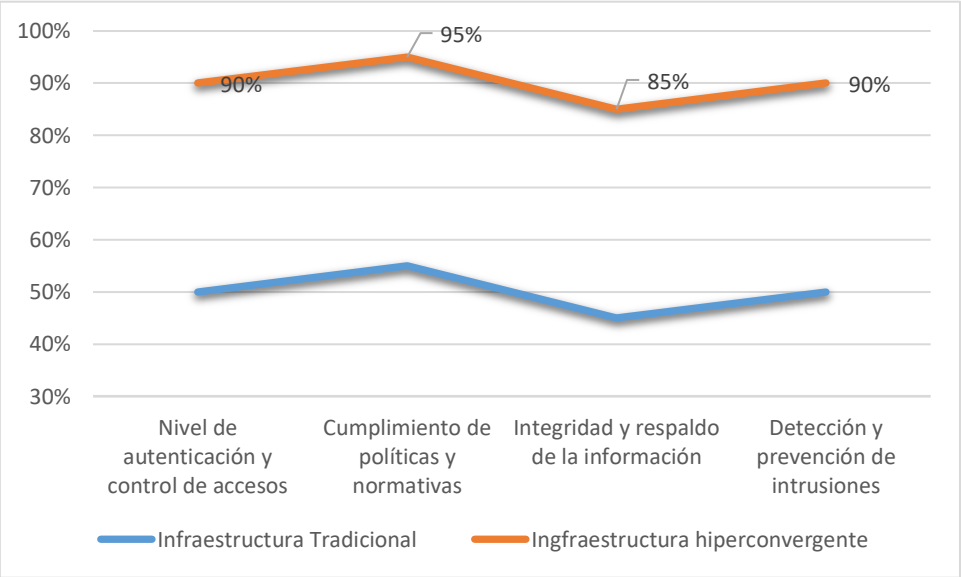
De igual manera, el ancho de banda disponible en la HCI obtuvo un 85% ante la tradicional, que obtuvo un 45%, teniendo una brecha de 40 puntos de diferencia. Esto se debe a que la HCI, al contar con virtualización de alta velocidad, logra que el tráfico principal de almacenamiento entre nodos sea gestionado y así lograr minimizar el impacto de ancho de banda. Por otro lado, también es importante la mensajería peer-to-peer (P2P), que no necesita un servidor central para tener una comunicación. A diferencia de la tradicional, que al utilizar demasiados datos para mover de un lado a otro a través de la red, crean cuellos de botella que limitan el ancho de banda disponible para aplicaciones del usuario.

De tal manera que el porcentaje de disponibilidad de servicios (SLA) en la HCI obtuvo un 90%, a diferencia de la tradicional, que obtuvo un 45%, dejando una brecha de 45 puntos. Esto se debe a que la HCI tiene la posibilidad de replicar datos de forma automática y migrar de manera caliente a través de nodos sin detener su funcionamiento, a diferencia de la tradicional, que requiere un tiempo delimitado programado para realizar servicios de mantenimiento, escalabilidad, lo que limita su diseño para cumplir con su nivel de acuerdo de servicio (SLA).

Por último, la escalabilidad de cargas de trabajo variables en la HCI obtuvo un 85%, a diferencia de la tradicional, que obtuvo un 35%, dejando una brecha de 50 puntos de diferencia. Eso se debe a que la HCI distribuye las cargas de trabajo entre nodos, permitiendo así el crecimiento de recursos como almacenamiento o equipo de cómputo sin alterar el servicio. Todo esto se realiza en tiempo real, a diferencia de la tradicional, que no logra hacer este crecimiento; más bien deben programar tiempo para incrementar su capacidad e integrar nuevos recursos.

Figura 10

Gráfico de líneas: Security (FCPAS) por indicador: HCI vs infraestructura tradicional



La gestión de seguridad dentro de los FCAPS forma parte de un pilar no negociable cuya importancia es crítica, ya que es el encargado de proteger la información valiosa en los entornos digitales ante amenazas. Este pilar no solo implica defensa perimetral, sino también la integración de políticas de seguridad para proteger las cargas de trabajo críticas.

El vial de autenticación y control de accesos en la HCI obtuvo un valor de 90%, a diferencia de la tradicional, que obtuvo un 50%, dejando una brecha de 40 puntos entre sí. Esto se debe a que la HCI logra tener políticas que regulan la autenticación y autorización de manera uniforme

y centralizada dentro de las máquinas virtuales, a diferencia del tradicional, que cada servidor y red exigen una propia configuración de acceso; eso incrementa la probabilidad de error en los permisos.

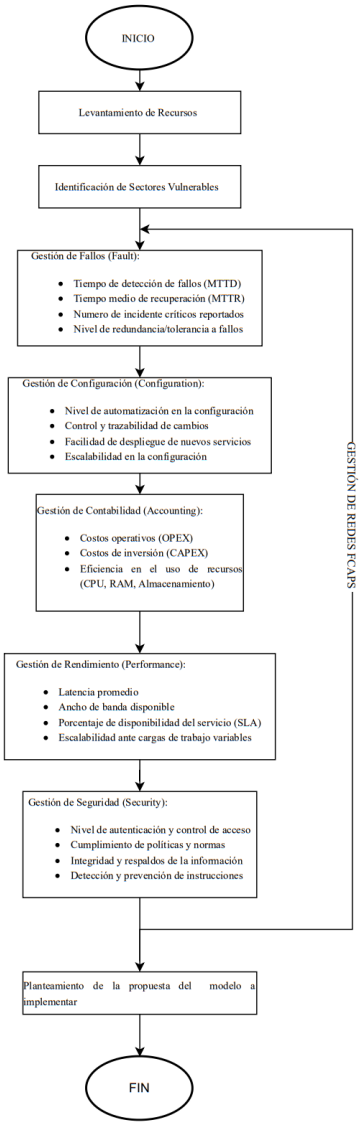
De igual manera, el cumplimiento de políticas y normativas dentro de la HCI obtuvo un 95%, a diferencia de la racional, que obtuvo un 55%, dejando una brecha de 40 puntos de diferencia. Esto se debe a que la HCI logra automatizar políticas de cumplimiento gracias a su software que controla de manera automática las configuraciones contra las normativas internas y externas, aplicando sus parches o asegurando su vulnerabilidad, a comparación de la tradicional, en que este proceso se realiza de manera manual y lenta, lo que requiere configuraciones de hardware fragmentado y la coordinación de equipos para aplicar las correcciones.

De tal manera, y no menos importante, la integridad y respaldo de la información en la HCI obtuvo un 85% a comparación de la tradicional, que obtuvo un 45%, con una brecha de 45 puntos de diferencia. Eso se debe a que la HCI facilita mucho al momento de realizar respaldos y replicación de datos, ya que, al ser nativas del software, asegura una consistencia e integración de la información. A diferencia de la tradicional, se ve limitado al uso de soluciones de respaldo externas y operadas, añadiendo complejidad y teniendo errores al momento de realizar mantenimiento de rutina.

Por último, la detección de prevención de instrucciones en la HCI obtuvo un 90%, a diferencia de la tradicional, que obtuvo un 50%, obteniendo una brecha de 40 puntos de diferencia. Es debido a que la HCI aplica reglas de firewall entre máquinas virtuales (microsegmentación), lo que limita el movimiento lateral de amenazas dentro de los data centers. En contraste con la tradicional, el nivel de seguridad que maneja es clásico, dejando cargas de trabajo que compartan la misma red de vulnerabilidad; si una de ellas es comprometida, todas se vuelven más eficaces a nivel interno.

En base a los resultados obtenidos de cada dimensión del modelo FCAPS, podemos observar que las HCI nos brindan un desempeño significativamente superior a la infraestructura tradicional. En Fault, destaca por su rápida detección y recuperación ante fallos; en Configuration, por su alto nivel de automatización y control centralizado; en Accounting, por la optimización de costos y el uso eficiente de los recursos; en Performance, por su mayor disponibilidad, baja latencia y capacidad de adaptación a distintas cargas de trabajo; y en Security, por su enfoque integral, automatizado y preventivo de la protección de datos.

Figura 11
Marco de Referencia Propuesto



4.1 Marco de Referencia Propuesto

La implementación efectiva de una HCI requiere un marco de gestión robusto que permita administrar, monitorear y optimizar cada componente del sistema de forma coherente. Sin este enfoque estructurado, las organizaciones no logran aprovechar plenamente las capacidades de esta tecnología.

El marco de referencia que se propone parte del desarrollo de una matriz comparativa cuyo propósito radica en medir los indicadores que evalúan la confiabilidad, como en cuantificar la eficiencia de las infraestructuras sobre los pilares FCAPS, la cual se desglosa en una presentación en cuadro de líneas.

Para determinar el marco de referencia con el modelo FCAPS, se desarrolló la propuesta desde lo general hasta lo específico, estructurando de manera efectiva el marco referido. Lo que conlleva a seguir los siguientes pasos:

4.1.1 Inicio del Proceso

El proceso de gestión de redes comienza preparando el entorno tecnológico y definiendo hacia dónde queremos ir con la implementación del modelo. En esta primera etapa, lo importante es establecer las reglas, lineamientos, políticas y parámetros que nos van a guiar, basándonos en buenas prácticas probadas. Para comenzar de la mejor manera, se debe analizar la dirección que se desea conseguir con un resultado esperado. Aquí es donde definimos objetivos concretos y alcanzables usando el método SMART, que sean específicos, medibles, alcanzables, relevantes y con plazos claros. También se arma el equipo: identificando quién va a liderar cada área, desde los coordinadores técnicos hasta los analistas de seguridad y administradores de sistemas, dejando clara su función y puesto. Además, necesitamos un calendario de trabajo actual, con fechas clave marcadas para establecer cómo se va a comunicar a todos los que conforman el equipo, ya que, si no existe una buena comunicación, nada funciona. Por supuesto, desde el principio se debe definir cómo se va a medir para observar si se está entregando lo prometido. Y como en todo proyecto, ahí se debe pensar en los inconvenientes que se pueden presentar durante el proceso de inicio, para lo cual se debe identificar los posibles problemas y tener un plan de alternativas que ayuden a solventar los problemas. Toda esta preparación inicial se hace enfocándose en los puntos clave que nos permitirán tener un control real, ordenado y medible de toda nuestra infraestructura.

4.1.2 Levantamiento de Recursos

Para el levantamiento de recursos debemos conocer a fondo los recursos disponibles para gestionarlos de manera eficiente. El levantamiento de recursos se hace de manera cuidadosa y de forma ordenada, se debe realizar un inventario completo de todos los elementos tecnológicos de la organización. En el caso del hardware, se documenta todo el equipamiento: servidores físicos y virtuales con sus características técnicas como: procesadores, memoria, almacenamiento, sistema operativo y la ubicados de los equipos de red como: routers, switches, firewalls, indicando su versión de firmware, puertos disponibles y capacidades, dispositivos de almacenamiento especificando su capacidad total, espacio usado y sistemas de redundancia, equipos de respaldo energético con su

capacidad y tiempo de autonomía, además de computadoras y dispositivos móviles contengan configuraciones de la organización. En cuanto al software, se debe registran los sistemas operativos instalados con sus versiones y actualizaciones, aplicaciones empresariales críticas, bases de datos, middleware, mantenimiento preventivo y mantenimiento correctivos, además de verificar que las licencias estén vigentes y en regla. La documentación de infraestructura incluye diagramas actualizados de la red que muestran las conexiones físicas y lógicas, los esquemas de direcciones IP con sus subredes y VLANs, el mapeo de sistemas de almacenamiento con sus políticas de respaldo, el registro de conexiones externas especificando proveedores y anchos de banda contratados, además de información sobre centros de datos y controles de acceso. Para agilizar este trabajo se utilizan herramientas de descubrimiento automático que detectan los dispositivos en la red y complementan el inventario manual. Asimismo, se implementa una base de datos centralizada donde se gestiona toda esta información de forma organizada, se establecen procedimientos claros para mantener el inventario actualizado definiendo responsables y períodos de revisión, y se emplean sistemas de etiquetado que facilitan la identificación rápida de los equipos. Este levantamiento resulta fundamental porque proporciona una visión precisa del estado actual del entorno y permite detectar dependencias o limitaciones que podrían dificultar la gestión efectiva de la red.

4.1.3 Identificación de sectores vulnerables

Descubrir los puntos débiles es clave al gestionar las redes, buscando sin demora esos fallos que amenazan la seguridad, la firmeza, el acceso o el desempeño de la estructura. Analizar esto exige verlo todo en conjunto, uniendo la mirada técnica con la revisión de cómo se hacen las cosas y chequeos a fondo. Primero, se miran las vulnerabilidades técnicas con programas como Nessus, OpenVAS, Qualys o Rapid7, revisando cada sistema y aparato de la red, y sumando pruebas de ataque ético que imitan ataques de dentro y fuera para ver por dónde podrían entrar. Además, se chequean cómo están armados los sistemas operativos, las apps y los dispositivos, comparándolos con normas conocidas como NIST o ISO 27001; se ven los sistemas y apps sin soporte que urgen actualizar, se pesan las reglas de acceso y contraseñas, y se repasan los registros del sistema buscando cosas raras o intentos de entrar sin permiso. Luego, se evalúa la estructura para ver dónde podría fallar todo en la arquitectura, servidores importantes sin repuesto o conexiones sin respaldo. Se mira si lo que hay alcanza para lo que se espera, se evalúa qué tan viejos son los equipos y cuánto les queda de vida, se inspeccionan las

instalaciones como el cableado, los paneles y los puntos de reparto buscando fallas, y se chequea la separación de la red para que cada parte esté bien aislada. Al final, se anota todo y se informa, creando reportes fáciles de entender para los jefes y reportes técnicos detallados para los equipos de TI, diciendo cómo arreglar las cosas, quiénes son los responsables, los tiempos y los recursos, creando un sistema para seguir que se cumplan las correcciones y que los puntos débiles sean cada vez menos. Esta etapa da una idea completa de cómo está la seguridad de la tecnología, dejando ver las amenazas antes, haciendo más fuerte el sistema y asegurando que la empresa siga funcionando.

4.1.4 Gestión de Fallos

El manejo de errores, parte vital del esquema FCAPS, busca asegurar que los servicios tecnológicos siempre estén disponibles y sean confiables. Esto se logra encontrando, separando, solucionando y evitando problemas que puedan interrumpir el trabajo. Para hacerlo, se usan tácticas que giran en torno a cuatro puntos clave: el tiempo que se tarda en notar un fallo (MTTD), el tiempo que se necesita para volver a la normalidad (MTTR), el registro y estudio de los problemas más graves y la creación de sistemas que sigan funcionando, aunque haya errores. Primero, el MTTD mide cuánto tiempo pasa desde que ocurre un fallo hasta que alguien lo ve. Es fundamental tener sistemas que vigilen todo el tiempo, usando herramientas como Nagios, Zabbix, PRTG, Datadog o SolarWinds, ajustadas para que no den falsas alarmas ni envíen demasiados avisos. Además, se usan formas de avisar a diferentes niveles, se vigilan los servicios de manera simulada, se hacen revisiones automáticas cada pocos segundos y se usan paneles que muestran información en vivo al equipo técnico, buscando detectar fallos graves en menos de dos minutos. En cuanto al MTTR, se busca que la recuperación sea lo más rápida posible, con guías detalladas, creación automática de avisos con datos para entender el problema, escalamientos automáticos, tener repuestos importantes a mano, usar programas que automaticen tareas y tener acuerdos con proveedores que aseguren una respuesta rápida. También se anima a guardar las soluciones en bases de datos y a hacer simulacros de recuperación de vez en cuando para que el personal técnico esté preparado.

4.1.5 Gestión de Configuración

Manejar la configuración es vital en entornos hiperconvergentes; garantiza que cada ajuste en la tecnología se controle, se registre y se deshaga si es preciso, bajando los riesgos y dando estabilidad operativa. Busca cuidar el sistema con automatización, control de cambios, despliegue fácil y escalabilidad. Primero, la automatización reduce fallos humanos y agiliza el lanzamiento de servicios con herramientas de IaC como Terraform y sistemas como Ansible, Puppet o Chef, que unifican los servidores. Aparte, usar GitOps, playbooks y orquestradores tipo Kubernetes permite despliegues constantes, controlados y con autorecuperación, superando el 80% de automatización. Segundo, el seguimiento de los cambios asegura una gestión segura y auditable, siguiendo ITIL. Esto abarca un Change Advisory Board (CAB), calendarios de cambios, versiones con Git, revisiones post implementación y métricas de éxito para medir cada cambio. Luego, desplegar servicios fácilmente implica pipelines CI/CD, separar desarrollo, pruebas y producción, y usar contenedores con Docker y despliegues blue-green o canary, bajando riesgos y mejorando los tiempos. Finalmente, la escalabilidad asegura que los sistemas crezcan sin grandes cambios, aplicando arquitecturas cloud-native, autoescalado, balanceo de carga, bases de datos distribuidas y planes de capacidad según la demanda. En breve, estandarizar, automatizar y rastrear fortalece la estabilidad, seguridad y eficiencia, impulsando una gestión proactiva y sostenible de la tecnología.

4.1.6 Gestión de Contabilidad

Para manejar bien las infraestructuras hiperconvergentes, la contabilidad es clave porque te da una idea clara de lo que gastas en el día a día y en inversiones. Esto te ayuda a usar la tecnología de la mejor manera posible para alcanzar las metas de tu empresa. Al hacerlo, tendrás una mejor administración financiera de TI, asegurándote de que cada gasto valga la pena, resuelva las necesidades de tu negocio y busque ser lo más eficiente posible.

Primero, para cuidar los gastos diarios (OPEX), hay que administrar bien los costos continuos de los sistemas usando prácticas FinOps y herramientas como CloudHealth o AWS Cost Explorer. Estas te permiten ver en qué se va el dinero, encontrar qué no está funcionando bien, quitar recursos que no se están usando mucho y programar el apagado o ajuste automático de la capacidad según lo que se necesite.

Segundo, la administración de los costos de inversión (CAPEX) se centra en planear y revisar proyectos de infraestructura a largo plazo usando análisis financieros como el ROI (Retorno de la Inversión), TCO (Costo Total de Propiedad) y VAN (Valor Actual Neto). Así, le das prioridad a las inversiones que tengan un gran impacto y duren mucho. Esto significa tener un inventario al día de los activos, crear reglas para renovar la tecnología, pensar si es mejor alquilar o comprar y hacer auditorías financieras de vez en cuando.

Para aprovechar al máximo los recursos como CPU, memoria y espacio de almacenamiento a nivel técnico y de costos, se usan herramientas de monitoreo como Prometheus, Grafana o Datadog. Estas herramientas ayudan a encontrar dónde se pone lento el sistema, ajustar el tamaño de los recursos según el uso real, juntar servidores y usar reglas para manejar el tiempo de vida de los datos. En resumen, la gestión contable dentro del modelo FCAPS asegura un control total de los costos y el uso correcto de los recursos, lo que ayuda a tomar buenas decisiones financieras basadas en datos reales y a que la infraestructura hiperconvergente se mantenga en el tiempo a nivel operativo y de costos.

4.1.7 Gestión de Rendimiento

Para manejar bien las infraestructuras hiperconvergentes, la contabilidad es clave porque te da una idea clara de lo que gastas en el día a día y en inversiones. Esto te ayuda a usar la tecnología de la mejor manera posible para alcanzar las metas de tu empresa. Al hacerlo, tendrás una mejor administración financiera de TI, asegurándote de que cada gasto valga la pena, resuelva las necesidades de tu negocio y busque ser lo más eficiente posible. Primero, para cuidar los gastos diarios (OPEX), hay que administrar bien los costos continuos de los sistemas usando prácticas FinOps y herramientas como CloudHealth o AWS Cost Explorer. Estas te permiten ver en qué se va el dinero, encontrar qué no está funcionando bien, quitar recursos que no se están usando mucho y programar el apagado o ajuste automático de la capacidad según lo que se necesite.

Segundo, la administración de los costos de inversión (CAPEX) se centra en planear y revisar proyectos de infraestructura a largo plazo usando análisis financieros como el ROI (Retorno de la Inversión), TCO (Costo Total de Propiedad) y VAN (Valor Actual

Neto). Así, le das prioridad a las inversiones que tengan un gran impacto y duren mucho. Esto significa tener un inventario al día de los activos, crear reglas para renovar la tecnología, pensar si es mejor alquilar o comprar y hacer auditorías financieras de vez en cuando. Para que los servicios de red funcionen bien y cumplan con lo que necesita el negocio y los usuarios, hay que estar vigilando constantemente. Así, podemos ver y arreglar los problemas antes de que causen líos. Lo importante es usar herramientas que midan qué tan rápido les llega la información a los usuarios. Se puede usar algo como Real User Monitoring para ver cómo navegan de verdad, y también hacer pruebas simuladas desde distintos lugares para encontrar problemas en el servicio.

Hay que medir varias cosas: cuánto tarda en ir y volver la información en la red, cuánto tardan en responder las aplicaciones y qué tan rápido funcionan las bases de datos. Se definen valores normales para cada cosa y se configuran alertas para cuando esos valores se pasen. No basta con ver promedios, hay que fijarse en los peores momentos para saber cómo funciona todo de verdad. También hay que vigilar cuánto ancho de banda se está usando, con herramientas que revisen el tráfico en la red. Así, se ven patrones de uso, si hay saturación y dónde hay más actividad. Con esta información, se puede decidir mejor cómo optimizar y distribuir los recursos.

Cada servicio importante debe tener sus propios indicadores y acuerdos de nivel de servicio. Debe haber paneles que muestren si se cumplen estos acuerdos, para que los usuarios lo vean claro y se puedan tomar decisiones rápidas si algo falla. Para entender problemas complicados en aplicaciones modernas, es bueno tener sistemas que rastreen todo el recorrido de una solicitud a través de los servicios. Así, se ve dónde se producen los retrasos y qué componentes están dando más problemas.

Por último, el sistema debe poder adaptarse a los cambios en la demanda. Esto se hace con estrategias para repartir la carga entre servidores y ajustar la capacidad según lo que se necesite. Se hacen pruebas para confirmar que la infraestructura aguanta picos de uso sin problemas.

4.1.8 Gestión de Seguridad

La seguridad es superimportante en la administración de redes. Se trata de cuidar la infraestructura y lo que se guarda ahí. La idea es que la data esté segura, sin cambios y siempre a la mano, evitando rollos técnicos o errores humanos. ¿Cómo se hace? Pues, con sistemas de identificación que piden varias pruebas para confirmar quién eres, controlados desde un mismo lugar con cosas como LDAP o Active Directory. Así, cada quien tiene acceso solo a lo que necesita, y se revisa seguido para que no tengan permisos de más que puedan causar problemas.

También hay reglas de seguridad basadas en estándares internacionales como ISO 27001, NIST o CIS Controls, que son como guías con buenas ideas. Y se entrena a la gente para que la seguridad sea cosa de todos, porque la tecnología sola no basta si la gente no entiende por qué es importante. Para que la información no se dañe, se hacen copias de respaldo siguiendo la regla 3-2-1: tres copias de los datos, en dos lugares distintos y una copia fuera. También se usan métodos para revisar que la información esté bien, como firmas digitales, y se encripta la información cuando viaja o está guardada, para que nadie la cambie o la robe sin que nos demos cuenta.

Para detectar y evitar broncas, hay sistemas que revisan el tráfico y buscan cosas raras, juntan datos de seguridad de varios lados para ver si hay patrones de ataque y analizan todo lo que pasa en el sistema. Y siempre se actualiza todo para tapar huecos de seguridad, una buena seguridad ayuda a evitar problemas antes de que pasen y a reaccionar rápido si hay amenazas. Así todo sigue funcionando bien y tenemos un lugar seguro para la tecnología, que aguanta ataques y sigue las mejores ideas de ciberseguridad.

4.1.9 Planteamiento de la Propuesta del Modelo a implementar

La etapa de presentar la propuesta del modelo a implementar es el punto clave del proceso de diseño y análisis. Aquí, todos los descubrimientos, datos y planes ya hechos se juntan en un documento formal. Este documento servirá como guía para poner en marcha el modelo de gestión que proponemos.

En esta fase, se organiza con detalle la parte técnica, las reglas de operación, los pasos a seguir, los puestos y tareas de cada uno, el calendario de trabajo, el dinero que creemos que costará y las formas de medir si el sistema funciona bien.

Este documento debe mostrarse a los interesados para que lo aprueben y aseguren que tenemos lo que necesitamos para hacerlo. Es bueno empezar con una prueba en un área o servicio importante. Así, vemos si el modelo funciona antes de usarlo en todo. Además, hacer que todo sea automático desde el principio ayuda a evitar errores humanos, hacer las cosas más rápido y que todo funcione igual. También es importante tener una documentación completa y al día donde se apunte cada paso, configuración y lo que aprendemos. Así, podemos saber de dónde viene todo y mejorar el sistema.

Capacitar al equipo es muy importante, ya que el modelo funciona si todos saben bien qué tienen que hacer. Por último, es clave revisar y cambiar el modelo siempre que sea necesario, para que se adapte a lo que el negocio necesita. Con esto, la propuesta no solo muestra todo de forma clara, da control sobre lo que se hace y ayuda a responder a los problemas, sino que también hace que la infraestructura de la red sea más eficiente, confiable y que dure más.

4.1.10 Fin del Proceso

La última parte es cuando el modelo de gestión se pone en marcha por completo. Se ven los resultados y se formaliza cómo funcionará el sistema en la empresa. Una vez que la propuesta está aprobada y funcionando, el modelo está listo para usarse. Esto significa que hay procesos para revisar constantemente, hacer auditorías de vez en cuando y programar revisiones para asegurarse de que todo vaya según lo planeado.

Esta etapa no es el final, sino el comienzo de un sistema donde siempre se busca mejorar. Se revisa la infraestructura tecnológica para que se adapte a los cambios en el entorno, las reglas y la seguridad. Como el modelo es cíclico, cada revisión ayuda a corregir errores, usar mejor los recursos y responder mejor a los problemas nuevos. Así, la empresa se asegura de que su tecnología mejore de forma segura y controlada, manteniendo un buen desempeño y siendo confiable a largo plazo.

Al juntar estos cinco pilares del modelo FCAPS, logramos armar un sistema de gestión sólido y práctico que realmente funciona. Ahora podemos administrar mejor toda la infraestructura, responder más rápido cuando algo sale mal y estar preparados para

cambios o amenazas. En resumen, conseguimos una gestión más moderna, automática y alineada con lo que la organización necesita para seguir creciendo.

CAPÍTULO 5
DISCUSIÓN

Ante los resultados obtenidos de la presente investigación se demuestra que la infraestructura hiperconvergente (HCI) obtuvo un rendimiento superior a la infraestructura tradicional en todos los pilares del modelo FCAPS, de manera que las tendencias observadas en diferentes estudios previos alcancen los objetivos planteados y se obtengan resultados que merecen ser discutidos.

Tal y como corrobora Antonenko (2024) y Cisco System (2025), la HCI es una tecnología moderna para la implementación de los centros de datos, destacando por su capacidad de simplificar la gestión, optimizar recursos, reduciendo los costos operativos; además, integra datos de cómputo, almacenamiento y red en una sola plataforma centralizada, reduciendo la complejidad operativa y los puntos de fallo.

Partiendo del contexto de la gestión de fallos (F), se observa una mayor capacidad de recuperación; la tolerancia ante fallos, mecanismos de replicación automática y la redundancia crítica permiten mantener disponibilidad de servicios frente a fallos críticos. Gray & Siewiorek, (1991) y (M. Shah, 2001) sostienen que los sistemas tolerantes a fallos representan un avance clave dentro de la comunidad operativa, mientras que (Nutanix, 2024b) y (Proxmox Server Solutions GmbH, 2025) afirman que las soluciones hiperconvergentes son una alternativa eficiente, ya que incluyen funciones nativas que reducen los tiempos de inactividad, fortalecen la estabilidad general del sistema, un factor primordial para el sector empresarial.

En resiliencia se ve reflejada la gestión de configuración (C), donde la HCI sobresale por la capacidad de automatizar y centralizar datos para mejorar su administración (Acceleron Labs Pvt Ltd, 2018) y (Parmar, 2019) destaca que la HCI opera mediante interfaces unificadas, reduciendo errores humanos y facilitando la coherencia de políticas de configuración. A su vez, (Intel, 2025) enfatiza que la administración basada en políticas contribuye a una infraestructura más coherente y escalable. A diferencia de la infraestructura tradicional que depende mucho de la interacción humana (Quantum, 2021), menciona que incrementa la posibilidad de errores y se complica en la gestión de errores.

El análisis de la gestión de contabilidad (A), al integrar métricas en tiempo real que permiten y paneles analíticos, es posible supervisar el consumo de recursos y asignar costos con mayor exactitud. (Nwakeze, 2024) sostiene que el continuo monitoreo permite detectar ineficiencia y optimizar la asignación de recursos de forma proactiva.

Siguiendo esta línea, el desempeño del sistema (P) es el resultado natural de todo lo mencionado antes: se aprovechan mejor los recursos disponibles y el sistema responde mucho más rápido ante las demandas. Como explican (Sheldon, 2020) y (Stephen Pritchard, 2021), al virtualizar los componentes y eliminar esas limitaciones físicas que antes frenaban todo, las plataformas hiperconvergentes funcionan de manera mucho más eficiente. Por su parte, (World Financial Review, 2023) y (CRN, 2022) destacan que la HCI usa sistemas inteligentes de distribución de carga y puede crecer o reducirse según lo que se necesite en cada momento, manteniendo un funcionamiento estable incluso cuando hay mucha presión sobre el sistema. En definitiva, lo que encontramos en esta investigación es que la HCI trabaja consistentemente mejor que la infraestructura convencional, y esto se refleja directamente en una mayor productividad a nivel tecnológico.

Sin embargo, cuando nos enfocamos en el tema de la seguridad (S), encontramos una situación interesante con dos caras. Por un lado, especialistas como (Longbottom, 2020) señalan un punto de preocupación: el hecho de que todos los servicios se concentren en una única plataforma de gestión podría hacernos más vulnerables a ciertos riesgos. Pero, por otro lado, investigadores como (Antonenko, 2024) y Schneider & Smalley (2024a) resaltan que las plataformas hiperconvergentes actuales ya vienen equipadas con herramientas de seguridad bastante sofisticadas, como encriptación de datos, separación lógica de recursos y verificación de identidad en múltiples pasos. Esta seguridad incorporada desde el diseño hace que la HCI sea en realidad más sólida y confiable, claro, siempre y cuando se mantenga al día con actualizaciones regulares, controles de acceso bien definidos y supervisión constante. Tanto (Saty, 2023) como (World Financial Review, 2023) coinciden en algo fundamental: la seguridad en HCI no es solo cuestión de tener buena tecnología, sino de qué tan bien la gestionamos día a día, lo que confirma lo importante que es el componente de seguridad (S) dentro del modelo FCAPS.

Todos los hallazgos que obtuvimos y su conexión con la teoría nos permiten afirmar que la infraestructura hiperconvergente va más allá de simplemente mejorar el rendimiento técnico: está cambiando por completo la forma en que las empresas administran sus redes. De acuerdo con (Mell & Grance, 2011) plantearon sobre la computación en la nube, donde se imagina la infraestructura como un servicio que puede adaptarse, crecer y automatizarse según se necesite. Del mismo modo, lo que han aportado (Gillis, 2025) y (Fulber-Garcia, 2024) confirma que el modelo FCAPS funciona muy bien como herramienta de análisis para medir qué tan madura está una operación y cómo se integran las funciones esenciales en estos entornos tecnológicos modernos. Ante los resultados obtenidos de la presente investigación, demostramos que la infraestructura hiperconvergente (HCI) obtuvo un rendimiento superior a la infraestructura tradicional en todos los pilares del modelo FCAPS, de manera que las tendencias observadas en diferentes estudios previos alcancen los objetivos planteados y se obtengan resultados que merecen ser discutidos.

CONCLUSIONES

Esta investigación muestra que a través del modelo FCAPS (Fault, Configuration, Accounting, Performance y Security), que la infraestructura hiperconvergente (HCI) representa un avance tecnológico comparado con la infraestructura tradicional. El análisis reveló que la HCI no solo mejora el manejo de recursos tecnológicos, sino que también transforma completamente la administración de TI, creando entornos más ágiles, seguros, escalables y sostenibles.

En general, la HCI mostró una resistencia operativa muy superior, con una extraordinaria habilidad para detectar, aislar y recuperarse automáticamente de errores mediante mecanismos de autorrecuperación y respaldo de datos, alcanzando un 90% frente al 50% de la infraestructura tradicional en la gestión de fallos (Fault). Asimismo, la HCI se distingue por su automatización avanzada y gestión centralizada basada en políticas, eliminando la dependencia de configuraciones manuales y logrando un impresionante 95%, superando por 50 puntos el 45% de la infraestructura tradicional en la gestión de configuración (Configuration).

Por otro lado, la HCI optimiza significativamente el uso de recursos y reduce el Costo Total de Propiedad mediante la consolidación de componentes y escalabilidad modular, obteniendo un 85% frente al 40% de la tradicional en la gestión de contabilidad (Accounting). Del mismo modo, indicó mayor disponibilidad (90% en SLA), menor latencia y respuesta más estable bajo cargas variables, alcanzando un 95% comparado con el 55% de la infraestructura tradicional en la gestión de rendimiento (Performance).

Finalmente, la HCI estableció un modelo proactivo y automatizado con seguridad integrada en su arquitectura, logrando un 90% en autenticación, control de accesos y cumplimiento normativo (95%), frente al enfoque fragmentado y reactivo de la tradicional, que obtuvo solo un 50% en la gestión de seguridad (Security).

En conjunto, la gestión de redes bajo el modelo FCAPS evidencia que la HCI supera ampliamente a la infraestructura tradicional en todos los dominios críticos, consolidándose como una solución integral que transforma la administración tecnológica empresarial.

REFERENCIAS

Acceleron Labs Pvt Ltd. (2018). *Traditional Data Centers vs. Hyper-Converged Infrastructure: A Comparative Analysis [Centros de Datos Tradicionales vs. Infraestructura Hiperconvergente: Un Análisis Comparativo] Acceleron Labs*. https://www.acceleronlabs.com/traditional-data-centers-vs-hyper-converged-infrastructure-a-comparative-analysis/

Al-Kubaisi, M., Yussof, S., & Mahmoud, M. A. (2025). Review of Cloud Datacenter Operations Optimization of Renewable Energy Aware Resource Scheduling Algorithms. [Revisión de la Optimización de Operaciones en Centros de Datos en la Nube mediante Algoritmos de Programación de Recursos Conscientes de Energía Renovable] In *Journal of Information Systems Engineering and Management* (Vol. 2025, Issue 58s). https://jisem-journal.com/index.php/journal/article/view/12694/5902

Antonenko, D. (2024, December 7). *Hyperconvergence Technology: Understanding Hyperconverged Infrastructure [Tecnología de Hiperconvergencia: Comprendiendo la Infraestructura Hiperconvergente] Businesstechweekly.com*. https://www.businesstechweekly.com/operational-efficiency/cloud-computing/hyperconvergence-technology/

Arnav Sharma. (2023, July 23). *Hyperconverged Infrastructure – Explained –[Infraestructura Hiperconvergente – Explicada] Lets learn something new*. https://arnav.au/2023/07/17/hyperconverged-infrastructure-explained/

Assiri, B., & Sheneamer, A. (2025). *Fault tolerance in distributed systems using deep learning approaches*. *1 [Tolerancia a fallos en sistemas distribuidos mediante enfoques de aprendizaje profundo]*. https://doi.org/10.1371/journal.pone.0310657

Cisco System. (2025). *What Is Hyperconverged Infrastructure? [¿Qué es la Infraestructura Hiperconvergente?]- Cisco*. https://www.cisco.com/site/us/en/learn/topics/computing/what-is-hyperconverged-infrastructure.html

CRN. (2022, February 7). *Top 5 Hyperconverged Infrastructure (HCI) Use Cases For 2022 [Los 5 Principales Casos de Uso de Infraestructura Hiperconvergente (HCI) para 2022] | CRN*. https://www.crn.com/news/data-center/top-5-hyperconverged-infrastructure-hci-use-cases-for-2022

Curto, M. A. (2023). *Escuela Técnica Superior De Ingenieros De Telecomunicación Trabajo Fin De Grado Diseño de un microCPD Edge Hiperconvergente mediante herramientas OpenSource*.[Diseño de un microCPD Edge Hiperconvergente mediante herramientas OpenSource] https://uvadoc.uva.es/bitstream/handle/10324/63073/TFG-G6526.pdf?sequence=1&isAllowed=y

Fulber-Garcia, V. (2024, March 18). *Gestión de redes: el modelo FCAPS | Baeldung sobre informática*. https://www.baeldung.com/cs/network-management-fcaps-model

Gillis, A. S. ; Z. (2025, February 28). *What is FCAPS (Fault, Configuration, Accounting, Performance and Security)?*[¿Qué es FCAPS (Fallo, Configuración, Contabilidad, Rendimiento y Seguridad)?] https://www.techtarget.com/searchnetworking/definition/FCAPS

Gorschek, T., & Larsson, S. B. (2006). *A Model for Technology Transfer in Practice* .[*Un Modelo para la Transferencia de Tecnología en la Práctica]* https://www.wohlin.eu/software06.pdf

Gray, J., & Siewiorek, D. P. (1991). *High-Availability Computer Systems. [Sistemas Informáticos de Alta Disponibilidad]*. https://jimgray.azurewebsites.net/papers/ieee_ha_swieorick.pdf

Heredia, A. A. (2023). *Modelo Hiperconvergente Basado En Software Libre*. http://dspace.uazuay.edu.ec/handle/datos/13102

Intel. (2025). *¿Qué es la infraestructura hiperconvergente?* https://www.intel.com/content/www/us/en/learn/what-is-hyperconverged-infrastructure.html

Jogalekar, P. (2000). *Evaluating the Scalability of Distributed Systems. [Evaluando la Escalabilidad de los Sistemas Distribuidos]* https://www.sce.carleton.ca/faculty/woodside/pubs/scal00.pdf

Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE, 103*(1), 14–76. [Redes Definidas por Software: Una Encuesta Exhaustiva] https://doi.org/10.1109/JPROC.2014.2371999

Lara, E. G. (2023). Seguridad en la Infraestructura de Redes: Desafíos y Estrategias de Protección. *Periodicidad: Semestral*, *4*, 2023. https://portal.amelica.org/ameli/journal/572/5724522015/5724522015.pdf

Leiva Vilaplana, J. A., Kabbara, N., Coste, T., Morais, H., Zerriffi, H., & Gibescu, M. (2023). *Virtualized Protection, Automation, and Control in Electrical Substations: An Open-Source Dynamic Cost-Benefit Assessment Model. [Protección, Automatización y Control Virtualizados en Subestaciones Eléctricas: Un Modelo de Evaluación Costo-Beneficio Dinámico de Código Abierto.]* https://doi.org/10.1109/ACCESS.2023.0322000

Longbottom, C. (2020, July 27). *4 disadvantages of hyper-converged infrastructure systems | TechTarget. [4 desventajas de los sistemas de infraestructura hiperconvergente.]* https://www.techtarget.com/searchdatacenter/tip/Four-disadvantages-of-hyper-converged-infrastructure-systems

Malhotra, S., Yashu, F., Saqib, M., Mehta, D., Jangid, J., & Dixit, S. (2025). *Evaluating Fault Tolerance and Scalability in Distributed File Systems: A Case Study of GFS, HDFS, and MinIO. [Evaluando la Tolerancia a Fallos y Escalabilidad en Sistemas de Archivos Distribuidos: Un Estudio de Caso de GFS, HDFS y MinIO.]* https://arxiv.org/pdf/2502.01981

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology [La Definición NIST de Computación en la Nube: Recomendaciones del Instituto Nacional de Estándares y Tecnología]* https://doi.org/10.6028/NIST.SP.800-145

Moreira, Z. C., Lopez, N. M., & Cusme, R. G. (2019). *1 Infraestructura Hiperconvergente definida por software seguridad y evolución del centro de datos*. https://drive.google.com/file/d/1AUDo1Mkdzs9bgp4tiuHMGeGFxVdfZ3Kq/view

Nutanix. (2024a). *AHV: Virtualization Solution for Enterprise[AHV: Solución de Virtualización para Empresas]* https://www.nutanix.com/products/ahv

Nutanix. (2024b). *What is Hyperconverged Infrastructure (HCI) - FAQs. [¿Qué es la Infraestructura Hiperconvergente (HCI)? - Preguntas Frecuentes]* https://www.nutanix.com/hyperconverged-infrastructure

Nwakeze, O. M. (2024). *The Role of Network Monitoring and Analysis in Ensuring Optimal Network Performance.[El Papel del Monitoreo y Análisis de Redes en Garantizar el Rendimiento Óptimo de la Red]* https://www.researchgate.net/profile/Osita-Nwakeze/publication/382524010_THE_ROLE_OF_NETWORK_MONITORING_AND_ANALYSIS_IN_ENSURING_OPTIMAL_NETWORK_PERFORMANCE/Links/66a151248be3067b4b1575ad/THE-ROLE-OF-NETWORK-MONITORING-AND-ANALYSIS-IN-ENSURING-OPTIMAL-NETWORK-PERFORMANCE.pdf

Parmar, D. (2019). *4 Defining Characteristics of Hyperconvergence in the Enterprise. [4 Características Definitorias de la Hiperconvergencia en la Empresa]* https://www.nutanix.com/theforecastbynutanix/technology/4-defining-characteristics-of-hyperconvergence-in-the-enterprise

Perneel, L., Fayyad-Kazan, H., Peng, L., Guan, F., & Timmerman, M. (2015). Business Hypervisors for Real-time Applications. *Technology & Applied Science Research*, *5*(4), 832–840.*[Hipervisores Empresariales para Aplicaciones en Tiempo Real]* https://etasr.com/index.php/ETASR/article/view/568/300

Proxmox Server Solutions GmbH. (2025). *Proxmox Virtual Environment - Open-Source Server Virtualization Platform. [Proxmox Virtual Environment - Plataforma de Virtualización de Servidores de Código Abierto]* https://www.proxmox.com/en/products/proxmox-virtual-environment/overview

Quantum. (2021, December 15). *Data Center Architecture: Three Approaches to Enterprise Infrastructure | Quantum*. *[Arquitectura de Centros de Datos: Tres Enfoques para la Infraestructura Empresarial]* https://quantumobile.com/blog/data-center-architecture-three-approaches-to-enterprise-infrastructure/

Saty, M. (2023, September 18). *Hyper Converged Infrastructure: Hype or Hope? | by Mohamed Saty | Medium*. *[Infraestructura Hiperconvergente: ¿Exageración o Esperanza?]* https://medium.com/@mosharfy/hyper-converged-infrastructure-hype-or-hope-fd9887258571

Schneider, J., & Smalley. (2024a, February 12). *What is hyperconverged infrastructure? [¿Qué es la infraestructura hiperconvergente?]* https://www.ibm.com/think/topics/hyperconverged-infrastructure

Schneider, J., & Smalley, I. (2024b). *¿Qué es el almacenamiento definido por software (SDS)?* https://www.ibm.com/es-es/topics/software-defined-storage

Shah, A. (2025). Demystifying Distributed Systems: Scalability, Modularity, and Fault Tolerance Explained. *Sarcouncil Journal of Engineering and Computer Sciences*. *[Desmitificando los Sistemas Distribuidos: Escalabilidad, Modularidad y Tolerancia a Fallos Explicadas]* https://doi.org/10.5281/zenodo.16981602

Shah, M. (2001). *Fault Tolerant Distributed Computing*. *[Computación Distribuida Tolerante a Fallos]* https://crystal.uta.edu/~kumar/cse6306/papers/FaultTolerantDistComp.pdf

Sheldon, R. (2020, August 11). *11 main benefits of hyper-converged infrastructure | TechTarget*. *[11 beneficios principales de la infraestructura hiperconvergente]* https://www.techtarget.com/searchdatacenter/tip/11-main-benefits-of-hyper-converged-infrastructure

Stephen Pritchard. (2021, April 22). *Five reasons to look at hyper-converged infrastructure | Computer Weekly*. *[Cinco razones para considerar la infraestructura hiperconvergente]* https://www.computerweekly.com/feature/Five-reasons-to-look-at-hyper-converged-infrastructure

The Gorilla Guide Team. (2019). *In the Beginning… of Hyperconverged Infrastructure - Gorilla Guide*.*[En el Principio... de la Infraestructura Hiperconvergente]* https://www.gorilla.guide/in-the-beginning-of-hyperconverged-infrastructure/

Turkkan, B., Rodrigues, E., Kosar, T., Charapko, A., Ailijiang, A., & Demirbas, M. (2025). *How to Evaluate Distributed Coordination Systems? -- A Survey and Analysis*. *[¿Cómo Evaluar Sistemas de Coordinación Distribuida? -- Una Encuesta y Análisis]* https://arxiv.org/pdf/2403.09445

World Financial Review. (2023, May 22). *Pros & Cons of Hyper-Converged Infrastructure (HCI) - The World Financial Review*.*[Pros y Contras de la Infraestructura Hiperconvergente (HCI)]* https://worldfinancialreview.com/pros-cons-hyper-converged-infrastructure-hci/

Yang, C. (2025). *Theoretical Analysis of Distributed Systems and Their Scalability*.*[Análisis Teórico de Sistemas Distribuidos y su Escalabilidad]* https://doi.org/10.23977/acss.2025.090104