UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

CASO DE ESTUDIO SOBRE EL DESPLIEGUE DE UNA NUBE COMUNITARIA PARA EL SECTOR SALUD EN CENTROAMÉRICA: VIABILIDAD DE UNA INFRAESTRUCTURA DE NUBE BASADA EN OPEN SOURCE PARA REGISTROS MÉDICOS Y SERVICIOS DE SALUD.

Integrantes:

Miguel Angel Amaya Rodríguez - AR19085

Jairo Josué Hurtado Muñoz - HM17017

Jose Alberto Flores Barillas - FB16004

Carlos René Martínez Rivera - MR11139

DOCENTE ASESOR: MSc. Julio Damián Morales Ayala

CIUDAD UNIVERSITARIA, 27 DE AGOSTO DE 2024

UNIVERSIDAD DE EL SALVADOR

RECTOR:

MSC. JUAN ROSA QUINTANILLA

SECRETARIO GENERAL:

LIC. PEDRO ROSALÍO ESCOBAR CASTANEDA

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DECANO:

ING. LUIS SALVADOR BARRERA MANCÍA

SECRETARIO:

ARQ. RAÚL ALEXANDER FABIÁN ORELLANA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

DIRECTOR:

ING. CÉSAR AUGUSTO GONZÁLEZ RODRÍGUEZ

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

Trabajo de Graduación previo a la opción al Grado de:

INGENIERO(A) DE SISTEMAS INFORMÁTICOS

Título:

CASO DE ESTUDIO SOBRE EL DESPLIEGUE DE UNA NUBE COMUNITARIA PARA EL SECTOR SALUD EN CENTROAMÉRICA: VIABILIDAD DE UNA INFRAESTRUCTURA DE NUBE BASADA EN OPEN SOURCE PARA REGISTROS MÉDICOS Y SERVICIOS DE SALUD.

Presentado por:

MIGUEL ANGEL AMAYA RODRÍGUEZ

JAIRO JOSUÉ HURTADO MUÑOZ

JOSE ALBERTO FLORES BARILLAS

CARLOS RENÉ MARTÍNEZ RIVERA

Trabajo de Graduación Aprobado por:

Docente Asesor:

MSC. JULIO DAMIÁN MORALES AYALA

SAN SALVADOR, NOVIEMBRE DE 2024

Trabajo de Graduación Aprobado por:

Docente Asesor:

MSc. Julio Damián Morales Ayala

Índice

Índice de Figuras.

Índice de Tabla

1. Introducción

En la región centroamericana, se ha observado un creciente número de empresas del sector salud que requieren sistemas médicos cada vez más sofisticados para ofrecer los servicios que sus usuarios demandan. Estos sistemas, en su mayoría, están siendo desplegados a través de plataformas en la nube, lo que permite a las instituciones acceder a la información de manera rápida y en el momento necesario. La adopción de estas tecnologías se ha vuelto indispensable para garantizar el correcto funcionamiento de los sistemas de salud.

Sin embargo, a pesar de las ventajas que ofrecen los sistemas basados en la nube, las entidades médicas enfrentan el reto de contar con la infraestructura adecuada para implementar estas soluciones. Esto se debe a que se requiere el uso de tecnologías especializadas y un diseño de infraestructura que se ajuste a las necesidades particulares de estas instituciones.

El objetivo de este trabajo de investigación es diseñar y desarrollar un prototipo de nube pública que ofrezca el soporte necesario a las entidades de salud para desplegar sus sistemas especializados. Este prototipo se basa en tecnologías de código abierto, lo que lo convierte en una solución viable tanto desde el punto de vista económico como tecnológico. El prototipo incluirá tecnologías para el escalamiento y la administración de la infraestructura, como interfaces web en tiempo real, servicios de bases de datos, autenticación de usuarios, entre otros.

Con el uso de estas tecnologías, se busca que el prototipo sea de fácil adopción para las entidades de salud y aplicable a la mayoría de sus casos de uso.

2. Definición del Proyecto

2.1. Identificación de la organización

Para esta investigación se utilizara una organización ficticia la cual será equivalente a empresas que brindan servicios médicos a nivel Centro Americano, las cuales demandan el uso de tecnologías cloud para poder operar sus sistemas. Se analizarán sus

requerimientos y limitaciones para plantear una solución que le permita desplegar de manera confiable los sistemas que necesiten acorde a sus necesidades.

2.2. Contexto del Proyecto

En la región centroamericana, las instituciones de salud enfrentan desafíos tecnológicos significativos debido al creciente volumen de datos médicos que deben gestionar y la necesidad de integrar sus sistemas de manera eficiente. La digitalización de los registros médicos y la interconexión entre diversos sistemas hospitalarios han creado una demanda urgente de soluciones tecnológicas que permitan no solo el almacenamiento seguro de la información, sino también su intercambio rápido y confiable entre diferentes proveedores de servicios de salud.

Este panorama se agrava por la falta de infraestructura tecnológica adecuada en muchas instituciones, que no cuentan con los recursos necesarios para implementar plataformas robustas y escalables. Aunque las tecnologías en la nube han surgido como una opción viable para resolver estos problemas, la adopción generalizada de estas tecnologías sigue siendo limitada debido a factores como la complejidad técnica y los costos asociados.

2.3. Antecedentes

Las tecnologías de nube han transformado radicalmente el sector salud, ofreciendo soluciones avanzadas para la gestión de datos, la interoperabilidad de sistemas y la prestación de servicios médicos ("Cloud Computing in Health Care", s.f.). Este contexto es esencial para comprender cómo las organizaciones han implementado infraestructuras de nube para mejorar sus operaciones.

Las nubes regionales surgieron como una respuesta a la necesidad de descentralizar los servicios de computación en la nube para mejorar la eficiencia y la seguridad de los datos. A medida que las empresas y las instituciones comenzaron a

enfrentar desafíos relacionados con la latencia de la red, la soberanía de los datos y las regulaciones específicas de cada país o región, se hizo evidente la necesidad de adaptar las soluciones de nube a contextos geográficamente específicos.

En los primeros días de la computación en la nube, los grandes proveedores (como Amazon Web Services, Microsoft Azure y Google Cloud Platform) centralizaban sus operaciones en limitados centros de datos. No obstante, con la expansión global del uso de la nube y una mayor preocupación por la privacidad de los datos, estos proveedores empezaron a establecer regiones de nube específicas (Amazon Web Services, 2014). Estas regiones estaban estratégicamente diseñadas para almacenar y procesar datos lo más cerca posible de los usuarios finales, con lo que se logró atender de mejor manera sus necesidades y expectativas. Diversas organizaciones han logrado implementar con éxito infraestructuras de nube regional para atender a estos desafíos, entre las que destacan:

Walmart: Utilizando OpenStack, Walmart ha equipado su infraestructura para gestionar extensas cargas de trabajo de e-commerce, particularmente durante eventos de alta demanda como el Black Friday. Esta solución les ha permitido atender a millones de usuarios simultáneamente y procesar transacciones de manera eficiente, un factor crucial para garantizar una experiencia de usuario positiva y lograr el éxito comercial en momentos críticos.

AT&T: Por su parte, AT&T ha integrado OpenStack en su plataforma de nube interna, conocida como AT&T Integrated Cloud (AIC). Esta plataforma ha sido fundamental para que AT&T maneje grandes volúmenes de datos de red y mejore la eficiencia operativa, además de acelerar la introducción de nuevos servicios para sus clientes. Gracias a OpenStack, AT&T ha podido gestionar sus recursos de computación y red con mayor precisión y facilitar la incorporación de tecnologías emergentes, como la 5G ("AT&T’s Cloud Strategy has Never Been Clearer", s.f.).

Estos ejemplos demuestran cómo la implementación de nubes regionales puede adaptarse efectivamente a las necesidades operativas y estratégicas de las organizaciones,

permitiéndoles no solo cumplir con las exigencias legislativas locales sino también mejorar significativamente la administración de sus recursos tecnológicos.

2.4. Justificación

La creciente generación de datos médicos en Centroamérica exige soluciones efectivas para su almacenamiento y gestión. La implementación de una nube comunitaria multiregional, basada en tecnologías open source, proporciona una infraestructura escalable y flexible, capaz de adaptarse a las demandas cambiantes de las instituciones de salud. Esta flexibilidad no solo facilita la integración de sistemas existentes, sino que también permite un desarrollo ágil de nuevas funcionalidades, promoviendo la interoperabilidad entre diferentes entidades.

Estas herramientas permiten implementar medidas robustas de protección de datos y eviten la dependencia de proveedores comerciales, lo que resulta en un enfoque más accesible y económico, esto sumará al desarrollo de capacidades locales, contribuyendo a la autonomía tecnológica de la región y mejorando la calidad de atención al permitir una visión integral del paciente. La creación de una solución de nube comunitaria no solo responde a las necesidades actuales, sino que establece un camino hacia un futuro en el que los datos se utilicen estratégicamente para el beneficio de la población.

2.5. Alcances

- Diseñar y construir un prototipo de nube comunitaria multiregional enfocada a entidades relacionadas con el área de la salud.
- Configuración del servicio de base de datos para gestionar los datos de las entidades sin importar la región.
- Configuración de acceso a la infraestructura mediante el uso de usuarios federados y persistencia de la sesión.
- Implementación de interfaz web de administración de la infraestructura y servicios del prototipo.

2.6. Limitaciones

En el sector salud en Centroamérica puede haber diversas normativas y regulaciones específicas de cada país las cuales no han sido tomadas en cuenta para este trabajo de investigación en cuanto a requerimientos mínimos o medidas de seguridad obligatorias.

Aunque el caso de estudio valida que la infraestructura es compatible con OpenEMR, algunas configuraciones específicas del sistema (como la gestión de Nginx o Apache) pueden requerir ajustes adicionales en un entorno de producción.

La gestión de bases de datos distribuidas y el acceso simultáneo en tiempo real también podrían necesitar ajustes en función del crecimiento de la demanda.

3. Marco Teórico

Es crucial contar con una base teórica sólida que abarque los distintos tipos de nubes, sus beneficios y desafíos, así como la importancia de los EMR en el sector salud. Además, el marco teórico permitirá contextualizar cómo la nube comunitaria puede ofrecer una solución efectiva a los problemas específicos que enfrentan las instituciones de salud en Centroamérica, como la interoperabilidad, la seguridad de los datos y el cumplimiento normativo (Marinos & Briscoe, 2009; Mense & Page, 2015).

3.1. Conceptos Fundamentales

3.1.1. Virtualización e Hipervisores

La virtualización es una tecnología esencial en la computación en la nube, ya que permite la abstracción y gestión eficiente de los recursos de hardware, facilitando la creación de entornos flexibles y escalables (Buyya, Broberg & Goscinski, 2011). Los hipervisores son los componentes clave que permiten la virtualización, permitiendo que múltiples sistemas operativos compartan los mismos recursos de hardware físico sin interferencias.

3.1.2. Virtualización

La virtualización es el proceso de crear una versión virtual (en lugar de física) de un recurso de hardware, como un servidor, almacenamiento, o red (Kavis, 2014). A través de la virtualización, se pueden ejecutar múltiples sistemas operativos y aplicaciones en un solo servidor físico, utilizando los recursos de manera más eficiente y flexible. Esta tecnología permite a las organizaciones reducir costos, mejorar la utilización de recursos y aumentar la agilidad operativa.

3.1.2.1. Tipos de Virtualización

Virtualización de Hardware: Consiste en crear máquinas virtuales (VMs) que simulan hardware físico, permitiendo ejecutar varios sistemas operativos en un solo servidor físico. Cada máquina virtual actúa como si fuera un sistema independiente, con su propio sistema operativo y aplicaciones. Esta es la forma más común de virtualización y es la base de muchas infraestructuras de nube (Buyya et al., 2011).

Virtualización de Red: Implica la combinación de recursos de red que tradicionalmente eran hardware específico (como routers, switches y firewalls) en recursos virtuales. Esto permite la creación de redes virtuales que pueden ser gestionadas y configuradas de manera centralizada, mejorando la flexibilidad y la capacidad de respuesta a las necesidades cambiantes de la red (Kavis, 2014).

Virtualización de Almacenamiento: Agrupa recursos de almacenamiento físicos en un único almacenamiento virtual que puede ser gestionado de manera más eficiente. Esto permite que el almacenamiento se distribuya dinámicamente según las necesidades de las aplicaciones, mejorando la utilización y reduciendo el desperdicio de espacio de almacenamiento (Buyya et al., 2011).

3.1.2.2. Beneficios de la Virtualización en el Contexto de la Computación en la Nube

Eficiencia de Recursos: La virtualización permite un uso más eficiente del hardware al permitir que múltiples VMs compartan los recursos de un solo servidor físico.

Esto reduce la necesidad de adquirir y mantener múltiples servidores físicos, disminuyendo costos operativos y de energía (Armbrust et al., 2010).

Escalabilidad: Los entornos virtualizados pueden escalar fácilmente para satisfacer las necesidades de recursos adicionales. Las organizaciones pueden añadir nuevas VMs rápidamente sin necesidad de adquirir nuevo hardware físico (Buyya et al., 2011).

Flexibilidad y Movilidad: Las máquinas virtuales pueden ser movidas fácilmente entre servidores físicos, lo que permite una mayor flexibilidad en la gestión de recursos y la recuperación ante desastres (Kavis, 2014).

Aislamiento y Seguridad: Cada VM está aislada de las demás, lo que significa que un fallo en una VM no afecta a las otras. Esto también mejora la seguridad, ya que los ataques en una VM no se propagan a las demás (Pearson & Benameur, 2010).

3.1.3. Hipervisores: Tipos y Funcionamiento

El hipervisor es el software o firmware que permite la virtualización al crear y gestionar máquinas virtuales. Actúa como una capa intermedia entre el hardware físico y los sistemas operativos de las VMs, permitiendo que múltiples VMs compartan los mismos recursos físicos de manera eficiente y segura (Kavis, 2014). El hipervisor asigna dinámicamente recursos de hardware como CPU, memoria y almacenamiento a cada VM, gestionando la distribución de estos recursos y asegurando que las VMs funcionen correctamente sin interferir entre sí.

3.1.3.1. Tipos de Hipervisores

Tipo 1 (Bare Metal): Estos hipervisores se ejecutan directamente sobre el hardware físico sin necesidad de un sistema operativo subyacente. Ejemplos de hipervisores de Tipo 1 incluyen KVM (Kernel-based Virtual Machine), Xen, y VMware ESXi. Debido a que operan directamente en el hardware, ofrecen un mejor rendimiento y seguridad en comparación con los hipervisores de Tipo 2 (Buyya et al., 2011).

Tipo 2 (Hosted): Estos hipervisores se ejecutan sobre un sistema operativo anfitrión, lo que significa que dependen de un sistema operativo subyacente para interactuar

con el hardware. Ejemplos incluyen VirtualBox y VMware Workstation. Aunque son más fáciles de configurar y utilizar, tienden a tener un rendimiento menor y más sobrecarga debido a la capa adicional del sistema operativo anfitrión (Kavis, 2014).

3.1.4. Integración de Hipervisores en OpenStack

En OpenStack, los hipervisores son responsables de la gestión de las máquinas virtuales que se ejecutan en la nube. OpenStack Nova, el componente de computación, interactúa con el hipervisor para provisionar, iniciar, detener y destruir VMs según las necesidades del usuario (OpenStack Foundation, s. f.). OpenStack es compatible con varios hipervisores, incluyendo KVM, Xen, VMware ESXi, y Hyper-V, lo que ofrece flexibilidad a las organizaciones en la elección del hipervisor que mejor se adapte a sus necesidades.

La elección del hipervisor en OpenStack depende de varios factores, incluyendo el rendimiento requerido, la compatibilidad con las aplicaciones existentes, y las consideraciones de licencias y costos. KVM es uno de los hipervisores más comunes utilizados con OpenStack debido a su integración nativa con Linux y su código abierto, lo que lo convierte en una opción atractiva para muchas organizaciones (OpenStack Foundation, s. f.). La configuración de un hipervisor en OpenStack implica la instalación y configuración del hipervisor en los nodos de cómputo y la integración con los demás servicios de OpenStack para asegurar un funcionamiento eficiente y seguro.

La elección del hipervisor puede tener un impacto significativo en la eficiencia y seguridad de la nube. Los hipervisores de Tipo 1, como KVM y Xen, suelen ofrecer un mejor rendimiento y seguridad, lo que es crucial en entornos de nube donde múltiples inquilinos comparten recursos. Además, la compatibilidad del hipervisor con las herramientas de seguridad y monitoreo de OpenStack es esencial para garantizar que se puedan aplicar políticas de seguridad robustas y que las operaciones de la nube sean eficientes (OpenStack Foundation, s. f.).

3.1.5. Computación en la Nube

La computación en la nube es un modelo de entrega de servicios tecnológicos que permite a las organizaciones acceder a recursos computacionales a través de internet, eliminando la necesidad de poseer y mantener una infraestructura física interna (Armbrust et al., 2010). La nube ofrece flexibilidad, escalabilidad y ahorro de costos, ya que los recursos se pueden ajustar según las necesidades en tiempo real. Este modelo ha revolucionado la forma en que las empresas y organizaciones gestionan su infraestructura tecnológica, facilitando el acceso a servicios avanzados sin las barreras tradicionales de entrada.

3.1.6. Definición y Tipos de Nube (Pública, Privada, Comunitaria e Híbrida)

Nube Pública: Es un modelo en el que los servicios y recursos son proporcionados por terceros, como Amazon Web Services (AWS), Microsoft Azure o Google Cloud, y están disponibles para cualquier organización o individuo que desee utilizarlos. Los recursos se comparten entre múltiples usuarios, y los costos se distribuyen según el uso (Buyya et al., 2011).

Nube Privada: Este modelo se refiere a una infraestructura de nube exclusiva para una sola organización. Puede estar alojada en las instalaciones de la organización o en un centro de datos externo, pero los recursos no se comparten con otras entidades. Ofrece mayor control sobre la seguridad y la personalización, pero a un costo mayor (Kavis, 2014).

Nube Comunitaria: En este modelo, la infraestructura es compartida por varias organizaciones que tienen intereses o necesidades comunes, como es el caso de instituciones del sector salud que necesitan gestionar EMRs de manera colaborativa. Las nubes comunitarias combinan la seguridad y personalización de las nubes privadas con la eficiencia de costos de las nubes públicas (Marinos & Briscoe, 2009).

Nube Híbrida: Es una combinación de nubes públicas, privadas y/o comunitarias, donde los datos y aplicaciones pueden moverse entre los diferentes entornos según las necesidades de la organización. Esto permite a las organizaciones aprovechar las ventajas

de cada tipo de nube mientras mantienen control sobre datos sensibles (Buyya et al., 2011).

3.1.7. Beneficios y Desafíos de la Computación en la Nube

3.1.7.1. Beneficios

Escalabilidad: Las organizaciones pueden escalar sus recursos según la demanda sin tener que invertir en infraestructura adicional.

Flexibilidad: Los servicios en la nube permiten a las organizaciones adaptarse rápidamente a los cambios en el mercado o en sus operaciones.

Reducción de Costos: La computación en la nube elimina la necesidad de grandes inversiones iniciales en hardware y software, ya que los recursos se alquilan según el uso.

Acceso Global: Los servicios en la nube están disponibles en cualquier lugar con conexión a internet, lo que facilita la colaboración y el acceso remoto a los recursos.

3.1.7.2. Desafíos

Seguridad: La protección de datos en la nube es crítica, especialmente en sectores sensibles como el de la salud.

Dependencia de Proveedores: Las organizaciones deben confiar en los proveedores de servicios para la seguridad, disponibilidad y cumplimiento de normativas.

Cumplimiento Normativo: Las diferentes regulaciones sobre la protección de datos pueden complicar el uso de la nube, especialmente cuando los datos cruzan fronteras.

3.2. Nube Comunitaria

La nube comunitaria es un modelo de infraestructura en la que varios participantes con necesidades similares comparten un entorno de nube, gestionado internamente o por un proveedor externo (Marinos & Briscoe, 2009). Este modelo es especialmente relevante para sectores donde la colaboración y la seguridad son primordiales, como en el sector

salud, donde múltiples instituciones pueden beneficiarse de una infraestructura compartida para la gestión de datos de pacientes.

La nube comunitaria se basa en la cooperación entre organizaciones con intereses comunes, lo que permite compartir costos y recursos de manera eficiente. Algunas de las características clave incluyen:

Personalización: La infraestructura puede ser adaptada a las necesidades específicas de la comunidad.

Seguridad y Privacidad: Ofrece un control más estricto sobre la seguridad y la privacidad de los datos, comparado con la nube pública.

Colaboración: Facilita la colaboración entre organizaciones, permitiendo un intercambio seguro de información y recursos.

3.2.1. Comparación con Otros Modelos de Nube

3.2.1.1. Comparada con la nube pública

La nube comunitaria ofrece mayor control y seguridad, pero a un costo generalmente más alto. Sin embargo, puede ser más económica que una nube privada debido al uso compartido de recursos.

3.2.1.2. Comparada con la nube privada

La nube comunitaria ofrece muchas de las ventajas de la nube privada, como la personalización y la seguridad, pero con la posibilidad de compartir costos entre varias organizaciones.

3.2.1.3. Comparada con la nube híbrida

La nube comunitaria no tiene la misma flexibilidad que una nube híbrida, pero es más adecuada cuando las organizaciones tienen necesidades muy específicas y comunes que pueden abordarse de manera colaborativa.

3.2.2. Casos de Uso en Diferentes Sectores

3.2.2.1. Sector Salud

Las nubes comunitarias pueden facilitar la gestión de EMRs y el cumplimiento de normativas específicas para el intercambio de información entre aplicaciones del rubro de la salud, tal es el caso del despliegue de EMRs que siguen el estándar FHIR (Mandel et al., 2016).

3.2.2.2. Educación

Universidades y escuelas pueden compartir una infraestructura de nube comunitaria para gestionar recursos educativos y administrativos de manera eficiente.

3.2.2.3. Gobierno

Las agencias gubernamentales pueden utilizar nubes comunitarias para compartir recursos y datos, mejorando la eficiencia operativa y la seguridad.

3.3. Registros Médicos Electrónicos (EMR)

Los Registros Médicos Electrónicos (EMR) son sistemas que almacenan la información de salud de los pacientes de manera digital, reemplazando los registros en papel (Benson, 2012). Los EMR facilitan el acceso a la información médica, mejoran la coordinación del cuidado, y permiten un seguimiento más preciso del historial médico de los pacientes.

3.3.1. Definición e Importancia en el Sector Salud

Un EMR es un registro digital de la información de salud de un paciente, que puede incluir datos como el historial médico, diagnósticos, tratamientos, resultados de pruebas y notas de los médicos (Benson, 2012). La importancia de los EMR en el sector salud radica en su capacidad para mejorar la eficiencia, reducir errores médicos, y facilitar un cuidado continuo y coordinado.

3.3.2. Desafíos en la Gestión de EMRs

3.3.2.1. Seguridad de los Datos

Los EMR contienen información altamente sensible que debe protegerse contra accesos no autorizados y ciberataques (Rindfleisch, 1997).

3.3.2.2. Interoperabilidad

Diferentes sistemas de EMR deben ser capaces de comunicarse entre sí para permitir un intercambio fluido de información entre distintas instituciones de salud.

3.3.2.3. Cumplimiento Normativo

Los EMR deben cumplir con las regulaciones locales e internacionales sobre la protección de datos de salud, como FHIR o HL7.

3.3.3. Soluciones Tecnológicas disponibles para EMRs

3.3.3.1. Diversidad de EMRs

Existen en el mercado, diversidad de aplicaciones para la gestión de registros médicos, tanto OpenSource, como de pago, entre ellos tenemos:

OpenMRS: Es una plataforma de código abierto diseñada para gestionar los registros médicos electrónicos en entornos de atención médica de recursos limitados. Es altamente configurable y extensible.

GNU Health: Un sistema de información de salud gratuito y de código abierto que se utiliza en hospitales y centros de salud de todo el mundo. GNU Health incluye módulos para la gestión hospitalaria, los registros médicos electrónicos, y la salud pública.

OpenEMR: Otro EMR de código abierto ampliamente utilizado, que ofrece una solución completa para la gestión de prácticas médicas, con funciones que incluyen la programación de citas, la facturación, y la interoperabilidad con otros sistemas de salud.

VistA: El sistema de información hospitalaria y de EMR de código abierto desarrollado por el Departamento de Asuntos de Veteranos de EE. UU. Es un sistema robusto y probado que se utiliza en numerosos hospitales y clínicas.

Epic Systems: Uno de los EMR más conocidos y utilizados en grandes hospitales y sistemas de salud. Epic ofrece una amplia gama de funcionalidades, desde la gestión de

registros médicos hasta la coordinación de la atención, con un fuerte enfoque en la interoperabilidad y la personalización.

Cerner: Otro sistema EMR de pago muy popular, utilizado globalmente en hospitales y clínicas. Cerner ofrece soluciones para la gestión de registros médicos, flujos de trabajo clínicos, y la integración de datos de salud para mejorar la atención al paciente.

3.3.3.2. Nubes Comunitarias

Ofrecen un entorno seguro y compartido para la gestión de EMRs, facilitando la colaboración entre diferentes instituciones de salud.

3.3.3.3. Cifrado de Datos

Implementar cifrado en tránsito y en reposo es esencial para proteger la información contenida en los EMR.

3.3.3.4. Autenticación y Control de Acceso

Sistemas de autenticación robustos y controles de acceso basados en roles son cruciales para garantizar que solo el personal autorizado tenga acceso a los datos médicos

3.4. Infraestructura Tecnológica en el Sector Salud

La infraestructura tecnológica en el sector salud es crucial para garantizar que las instituciones puedan ofrecer servicios de alta calidad de manera eficiente, segura y conforme a las regulaciones (Mense & Page, 2015). A medida que el volumen de datos médicos crece y la complejidad de los sistemas de salud aumenta, es esencial contar con una infraestructura tecnológica robusta que soporte la gestión de información crítica, como los registros médicos electrónicos (EMR), y que permita la interoperabilidad entre diferentes sistemas y organizaciones.

3.4.1. Requerimientos Tecnológicos para el Sector Salud

3.4.1.1. Seguridad y Privacidad de los Datos

En el sector salud, la seguridad y privacidad de los datos son de máxima prioridad debido a la sensibilidad de la información médica de los pacientes. Las instituciones de salud deben implementar medidas de seguridad rigurosas para proteger los datos contra accesos

no autorizados, violaciones de seguridad y ciberataques. Esto incluye el uso de cifrado de datos en tránsito y en reposo, controles de acceso estrictos, y auditorías regulares de seguridad.

Además, es fundamental cumplir con las regulaciones específicas de protección de datos, como la Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA) en los Estados Unidos o el Reglamento General de Protección de Datos (GDPR) en la Unión Europea. Estas normativas establecen directrices sobre cómo se deben manejar, almacenar y compartir los datos médicos, imponiendo sanciones severas en caso de incumplimiento.

3.4.1.2. Escalabilidad y Rendimiento

Las instituciones de salud deben estar preparadas para manejar grandes volúmenes de datos y un número creciente de usuarios, lo que requiere una infraestructura tecnológica escalable. La escalabilidad permite que los sistemas crezcan y se adapten a las necesidades cambiantes sin comprometer el rendimiento. Esto es especialmente importante en situaciones de emergencia o durante pandemias, cuando la demanda de servicios de salud puede aumentar drásticamente.

El rendimiento también es un aspecto crítico, ya que los sistemas de salud deben ser capaces de procesar y acceder a la información rápidamente para asegurar una atención médica eficiente y oportuna. Una infraestructura en la nube bien diseñada puede ofrecer la escalabilidad y el rendimiento necesarios para satisfacer estas demandas.

3.4.1.3. Interoperabilidad entre Sistemas

La interoperabilidad es la capacidad de los diferentes sistemas y organizaciones de salud para trabajar juntos e intercambiar información de manera fluida y segura. Es un desafío crítico en el sector salud, ya que muchas instituciones utilizan sistemas de gestión de salud y EMR distintos, que a menudo no son compatibles entre sí.

Para abordar este desafío, se han desarrollado estándares como HL7 (Health Level Seven) y FHIR (Fast Healthcare Interoperability Resources). HL7 es un conjunto de estándares para el intercambio, integración y recuperación de información electrónica de salud. FHIR, por su parte, es una especificación más moderna que facilita el intercambio de

datos de salud a través de interfaces de programación de aplicaciones (APIs). FHIR ha ganado popularidad debido a su capacidad para integrarse fácilmente con aplicaciones web y móviles, lo que lo convierte en un estándar clave para la interoperabilidad en la era de la computación en la nube.

3.4.2. Open Source en la Nube para Salud

El uso de software de código abierto (Open Source) en la nube ha ganado popularidad en el sector salud debido a su flexibilidad, costo-efectividad y capacidad de personalización. Herramientas como OpenStack, permiten a las instituciones de salud construir y gestionar infraestructuras de nube personalizadas que se ajustan a sus necesidades específicas.

El uso de Open Source también fomenta la innovación y la colaboración entre diferentes organizaciones, lo que es particularmente beneficioso en el desarrollo de soluciones interoperables y seguras. Por ejemplo, OpenStack se puede integrar con soluciones de gestión de EMR y estándares de interoperabilidad como FHIR, facilitando el intercambio de datos de salud entre diferentes sistemas.

3.5. OpenStack como Solución de Nube Comunitaria

OpenStack es una plataforma de software de código abierto que permite la implementación y gestión de infraestructuras de nube (OpenStack Foundation, s. f.). Su flexibilidad y modularidad lo convierten en una solución ideal para crear nubes comunitarias, especialmente en sectores que requieren un alto nivel de personalización y control, como el sector salud.

OpenStack fue lanzado en 2010 como un proyecto conjunto entre Rackspace Hosting y la NASA (OpenStack Releases, s. f.). El objetivo inicial era crear una plataforma de computación en la nube que fuera flexible, escalable y de código abierto. Desde entonces, OpenStack ha crecido significativamente, convirtiéndose en una de las plataformas de nube más utilizadas en todo el mundo.

El proyecto OpenStack es mantenido por la Fundación Open Infrastructure (anteriormente conocida como la Fundación OpenStack), y cuenta con el apoyo de una amplia comunidad de desarrolladores y empresas de tecnología. A lo largo de los años, OpenStack ha evolucionado para incluir una amplia gama de servicios que permiten a las organizaciones gestionar recursos de cómputo, almacenamiento y red, además de ofrecer herramientas para la automatización, la gestión de identidades y la seguridad.

3.5.1. Componentes Principales de OpenStack

OpenStack se compone de varios componentes modulares que trabajan juntos para proporcionar una infraestructura de nube completa.

3.5.1.1. Nova (Cómputo)

Es el servicio de computación de OpenStack que gestiona y provisiona máquinas virtuales (VMs). Nova permite la creación y gestión de instancias de servidor virtualizadas, proporcionando el motor de cómputo para la nube.

3.5.1.2. Swift (Almacenamiento de Objetos)

Es el servicio de almacenamiento de objetos de OpenStack, similar a Amazon S3. Swift permite almacenar y recuperar grandes cantidades de datos no estructurados, como archivos multimedia, backups y archivos de datos.

3.5.1.3. Cinder (Almacenamiento en Bloque)

Proporciona almacenamiento en bloque persistente para las instancias de cómputo de OpenStack. Es ideal para bases de datos y sistemas de archivos que requieren un almacenamiento duradero y de alto rendimiento.

3.5.1.4. Neutron (Redes)

Es el componente de redes de OpenStack que permite la configuración y gestión de redes virtuales, subredes, routers y firewalls. Neutron proporciona la conectividad de red necesaria para las instancias de cómputo.

3.5.1.5. Keystone (Identidad)

Es el servicio de gestión de identidades de OpenStack. Keystone maneja la autenticación y autorización de usuarios, y permite la creación de políticas de acceso para los recursos de la nube.

3.5.1.6. Glance (Imágenes)

Glance gestiona las imágenes de las máquinas virtuales que se utilizan para lanzar instancias en la nube. Permite almacenar, descubrir y recuperar imágenes de VM.

3.5.1.7. Horizon (Dashboard)

Es la interfaz web de OpenStack, que permite a los administradores y usuarios interactuar con la nube de manera gráfica. Horizon facilita la gestión de todos los servicios de OpenStack a través de una interfaz de usuario intuitiva.

3.5.2. Uso de OpenStack en la Nube Comunitaria

OpenStack ha demostrado ser una solución efectiva para la creación de nubes regionales, donde la infraestructura se adapta a las necesidades específicas de una región geográfica o sector industrial. En el contexto de una nube comunitaria para el sector salud, OpenStack permite la creación de una infraestructura compartida que puede ser gestionada de manera centralizada o descentralizada, según los requisitos de las organizaciones participantes.

La integración de OpenStack en nubes regionales permite a las instituciones de salud compartir recursos, mejorar la interoperabilidad entre sistemas, y garantizar el cumplimiento de las regulaciones locales. Además, OpenStack ofrece la flexibilidad de personalizar la

infraestructura para satisfacer las necesidades específicas de las instituciones de salud, como la gestión de registros médicos electrónicos (EMR), la seguridad de los datos y la gestión de identidades.

3.5.3. Desafíos en la Implementación de OpenStack en el Sector Salud

3.5.3.1. Configuración y Personalización

Uno de los desafíos más significativos en la implementación de OpenStack en el sector salud es la configuración y personalización de la plataforma para satisfacer las necesidades específicas de las instituciones de salud. Dado que OpenStack es altamente modular, se requiere una planificación cuidadosa para seleccionar y configurar los componentes adecuados que permitan la gestión eficiente de los recursos de cómputo, almacenamiento y red.

La personalización también implica la integración de sistemas de gestión de registros médicos electrónicos (EMR) y otras aplicaciones críticas para el sector salud.

3.5.3.2. Seguridad y Cumplimiento Normativo

La seguridad es una preocupación central en cualquier infraestructura de nube, pero es especialmente crítica en el sector salud debido a la naturaleza sensible de los datos médicos. La implementación de OpenStack en este contexto requiere el establecimiento de medidas de seguridad robustas, como el cifrado de datos, la autenticación de usuarios y el monitoreo continuo de amenazas.

Además, las instituciones de salud deben cumplir con normativas estrictas como HIPAA y GDPR, que establecen requisitos específicos para la protección de datos de salud. OpenStack ofrece herramientas y servicios que pueden ayudar a las organizaciones a cumplir con estas normativas, pero es necesario un enfoque integral que incluya la auditoría y el control de acceso a los datos.

3.6. Marco Legal

Este marco legal hace un repaso sobre las disposiciones legales, normativas y estándares aplicables para garantizar el cumplimiento de la legislación nacional e internacional en el ámbito tecnológico y de protección de datos en salud.

1. Legislación Nacional e Internacional Aplicable

a. Protección de Datos Personales:

i. **Ley de Protección de Datos Personales,** aplicable según cada país centroamericano involucrado, como El Salvador: *Ley de Protección de Datos Personales*.

ii. **Ley de Ciberseguridad y Seguridad de la Información,** aplicable según cada país centroamericano involucrado, como El Salvador, con la recién aprobada Ley de Ciberseguridad y Seguridad de la Información

iii. **Reglamento General de Protección de Datos (GDPR)**, aplicable en caso de intercambios internacionales con países de la Unión Europea.

b. Seguridad de la Información:

i. **ISO/IEC 27001**: Estándar internacional para la gestión de la seguridad de la información.

ii. **NIST Cybersecurity Framework**: Aplicable para la gestión de riesgos en infraestructuras tecnológicas.

iii. Legislación nacional sobre delitos informáticos y ciberseguridad.

c. Salud Pública y Registros Médicos:

i. **Normas nacionales de salud** (ejemplo: normas del *Ministerio de Salud de El Salvador* y equivalentes en la región).

d. Propiedad Intelectual y Licencias de Software:

i. **Licencias OpenStack** bajo Apache License 2.0.

ii. Legislación nacional sobre propiedad intelectual y uso de software libre.

2. Principios Rectores

a. **Confidencialidad, Integridad y Disponibilidad:** El manejo de la información de salud deberá garantizar estos principios básicos de seguridad.
b. **Consentimiento Informado:** Los datos de pacientes se procesarán únicamente con el consentimiento explícito de los titulares, salvo excepciones previstas por ley.
c. **Transparencia:** Los usuarios del sistema tendrán derecho a conocer cómo se almacenan y utilizan sus datos personales.
d. **Interoperabilidad:** La plataforma cumplirá estándares internacionales para garantizar la conectividad y el intercambio de datos entre instituciones.

3. Obligaciones Legales

a. Para los Administradores del Sistema:

i. Garantizar la implementación de medidas de seguridad tecnológica, como el cifrado de datos en reposo y en tránsito.
ii. Realizar auditorías regulares de seguridad y cumplimiento normativo.
iii. Mantener la confidencialidad de los registros médicos y limitar el acceso a personal autorizado.

b. Para los Usuarios (Instituciones de Salud):

i. Cumplir con las políticas de uso del sistema establecidas en el contrato de servicio.
ii. Designar responsables de la seguridad de la información en sus organizaciones.
iii. Asegurar el correcto ingreso y actualización de datos en el sistema.

c. Para los Proveedores de Infraestructura:

i. Garantizar la continuidad del servicio y planes de recuperación ante desastres (DRP).
ii. Cumplir con las cláusulas contractuales relacionadas con la localización de datos y soberanía digital.

Este Marco Legal deberá revisarse periódicamente para incorporar cambios normativos y tecnológicos que puedan impactar la operación del sistema y la protección de los datos de salud procesados en la infraestructura cloud.

4. Marco de Investigación

4.1. Pregunta de Investigación

¿Es posible diseñar y configurar una infraestructura de nube comunitara multiregional utilizando herramientas open source que permite a entidades del área de la salud a nivel centroamericano alojar sus herramientas de gestión de información?

4.2. Objetivos

4.2.1. Objetivo General

Diseñar y configurar un prototipo de infraestructura de nube comunitaria basado en herramientas open source que permitirá a entidades del área de salud en Centroamérica contar con un servicio de base de datos, usuarios federados, interfaz web para la gestión de servicios de la infraestructura.

Objetivos Específicos

1. Configurar un sistema de autenticación que permita a los usuarios mantener su sesión activa y acceder a recursos de múltiples regiones sin necesidad de múltiples inicios de sesión, mejorando la eficiencia y la experiencia del usuario en la plataforma.
2. Desplegar una interfaz web centralizada que permita a los administradores supervisar y gestionar eficazmente las operaciones de salud, los recursos y los datos a través de las diversas regiones, asegurando una gestión unificada y coherente.
3. Desplegar una solución de base de datos como servicio que centralice el almacenamiento, procesamiento y recuperación de datos de salud, garantizando la

seguridad, la integridad de los datos y la conformidad con las regulaciones locales de protección de datos.

5. Metodología

5.1. Enfoque de la Investigación

Este estudio adopta una combinación de enfoques cualitativos y cuantitativos para evaluar la factibilidad de diseñar una infraestructura escalable en la nube para entidades médicas en Centroamérica. La investigación seguirá las directrices de Piergiorgio Corbetta, quien destaca la importancia de la relación entre el objeto de estudio y el proceso de investigación. Dada la complejidad del problema y la necesidad de considerar tanto aspectos técnicos como sociales, es por ello que se utilizarán ambos enfoques para proporcionar una visión más integral.

5.1.1. Enfoque cuantitativo

El enfoque cuantitativo nos permitirá prototipar la infraestructura propuesta. Esto con el fin de poder medir el rendimiento y la capacidad de escalabilidad ante distintos niveles de demanda. Durante este proceso, también se recopilaran datos clave sobre aspectos como la persistencia de sesión, la seguridad en la identificación de usuarios y la eficiencia en la gestión de bases de datos dentro de estos entornos simulados. Donde con ello sé llevará a cabo un análisis de los resultados obtenidos, lo que permitirá evaluar la viabilidad de la infraestructura para entidades hospitalarias (Corbeta, 2007).

5.1.2. Enfoque cualitativo

En este enfoque nos centraremos en comprender a fondo las necesidades de las entidades médicas en la región. Para ello, se realizará una entrevista con representantes de diversas instituciones médicas, con el fin de identificar los desafíos actuales y las expectativas en torno a una solución basada en la nube. Por otro lado, se revisará la documentación técnica y las normativas de seguridad y privacidad de datos de salud en

Centroamérica, asegurando que las soluciones propuestas se alineen con las leyes vigentes de protección de datos (Cobeta, 2007). El análisis de la entrevista y el estudio permitirá identificar las infraestructura, conectividad y capacidades tecnológicas, factores clave que influyen en el diseño de una solución.

5.2. Diseño de la Investigación

La investigación emplea un enfoque mixto, combinando métodos cualitativos y cuantitativos que se alinean con nuestros objetivos y con nuestro caso de estudio. El enfoque cualitativo se aplica mediante entrevistas dirigidas a encargados de TI en hospitales, clínicas y otras instituciones de salud, con el propósito de explorar y comprender sus percepciones, experiencias y necesidades relacionadas con la implementación de una nube comunitaria en el sector salud de Centroamérica. Paralelamente, el enfoque cuantitativo consiste en encuestas estructuradas destinadas al mismo grupo objetivo, con el fin de recopilar datos concretos y medibles sobre su conocimiento, actitudes y expectativas respecto a los servicios de nube comunitaria.

5.3. Población y Muestreo

Debido al caso de estudio y los objetivos establecidos se ha definido como población objetivo a encargados de Tecnología de la Información (TI) en hospitales, clínicas y otras instituciones de salud. Este grupo es esencial para el estudio debido a su conocimiento y responsabilidad en la toma de decisiones sobre la infraestructura tecnológica y la implementación de soluciones en la nube dentro de sus respectivas instituciones.

Dado que el acceso a los encargados de TI en las instituciones de salud de la región es limitado, se utilizó un muestreo no probabilístico por conveniencia, esto permitió seleccionar 20 participantes disponibles y dispuestos a colaborar, lo que garantiza la relevancia de la información recopilada.

5.4. Instrumentos y Técnicas de recopilación de datos.

5.4.1. Entrevista semiestructurada

Una entrevista semiestructurada es una técnica de investigación cualitativa que combina preguntas abiertas y cerradas, permitiendo al entrevistador guiar la conversación en torno a temas específicos mientras también deja espacio para que el entrevistado ofrezca respuestas más detalladas y espontáneas. Para nuestro caso, se ha diseñado una entrevista, en la cual las preguntas se estructuran en torno a un guión, mostrado en el Anexo 1.

Dado que el tema de la infraestructura tecnológica y la implementación de nubes comunitarias puede ser complejo y variado, esta entrevista semiestructurada nos permite, como entrevistadores, adaptar las preguntas en función de las respuestas iniciales. Esto es útil para profundizar en áreas donde el entrevistado tiene más experiencia o donde surgen cuestiones inesperadas. Entonces, en este contexto, obtenemos un equilibrio entre estructura y flexibilidad, lo que es crucial para explorar temas técnicos complejos y obtener una visión completa y matizada de las percepciones y experiencias de los responsables de TI en el sector salud.

5.4.2. Encuesta

Se diseñaron encuestas, cuyos detalles se encuentran en el Anexo 2, dirigidas a jefes, encargados y coordinadores del área de TI en entidades hospitalarias, quienes poseen conocimientos en computación en la nube y gestión de infraestructura tecnológica. El propósito principal de estas encuestas es recolectar datos e información cuantitativa sobre temas específicos relacionados con las nubes comunitarias, tales como seguridad, confiabilidad, velocidad de acceso a la información, y otros beneficios percibidos por el uso de la nube en el entorno hospitalario.

Esto permitirá comprender las opiniones, necesidades y expectativas de los responsables de TI respecto a la adopción de soluciones en la nube comunitaria, contribuyendo así al desarrollo de un prototipo que responda efectivamente a las demandas del sector y que

potencialmente mejore la gestión de la información y los procesos operativos en las instituciones de salud.

5.5. Análisis de Resultados Cualitativos

Para el análisis de resultados, se toma en cuenta el enfoque hermenéutico de Hans-Georg Gadamer, el cual se centra en la interpretación profunda de los significados, considerando no solo lo dicho explícitamente, sino también los contextos, experiencias previas y expectativas de los entrevistados y, dado que las entrevistas con persona de TI de dos contextos distintos: una empresa encargada de gestionar servidores de múltiples hospitales y un hospital nacional que gestiona su infraestructura localmente. El objetivo es interpretar los significados subyacentes, comprendiendo cómo experiencias, prejuicios y contextos institucionales condicionan sus percepciones sobre la posibilidad de implementar una nube comunitaria en el sector salud. Entonces, dicho enfoque nos muestra que la comprensión no es una tarea meramente técnica, sino un proceso en el que se interpretan los mensajes a partir del diálogo entre las perspectivas del investigador y el entrevistado. Este enfoque es ideal para el análisis de las entrevistas realizadas, dado que aborda las percepciones y desafíos en la gestión de servidores, infraestructura y el posible uso de una nube comunitaria, situando estas experiencias en su contexto institucional y cultural.

5.5.1. Etapas del Enfoque Hermenéutico Gadameriano y su Adaptación al Análisis de las Entrevistas

5.5.1.1. Fusión de Horizontes

Esta es una de las nociones más importantes en la hermenéutica de Gadamer. La fusión de horizontes implica unir los diferentes contextos de comprensión del entrevistado y del investigador, para generar una nueva interpretación enriquecida.

Ambas entrevistas revelan que los técnicos manejan infraestructuras locales y desfasadas, con poca automatización y control manual. A pesar de que los contextos operativos varían (empresa externa vs. hospital nacional), ambos grupos coinciden en que el control local es crucial para garantizar la continuidad de los servicios. Sin embargo, sus

horizontes se complementan al coincidir en que una nube comunitaria podría ofrecer beneficios, especialmente en términos de interoperabilidad, respaldo y reducción de costos.

Interpretación:

En la empresa externa, la escalabilidad y el mantenimiento eficiente de los servidores son desafíos constantes. La nube es vista como una posible solución a largo plazo, siempre que ofrezca flexibilidad para adaptarse a múltiples hospitales.

En el hospital nacional, la burocracia institucional representa un obstáculo mayor, ralentizando la renovación de equipos y la adopción de nuevas tecnologías. La nube es vista con potencial, pero se percibe que la falta de autonomía y control directo podría generar resistencia por parte del hospital.

Fusión:

La nube comunitaria debe integrar las preocupaciones sobre el control y la autonomía con la necesidad de escalabilidad. Una infraestructura híbrida, que permita mantener ciertos sistemas críticos localmente mientras aprovecha la nube para interoperabilidad y respaldo, podría generar aceptación en ambos contextos.

5.5.1.2. Prejuicios y Tradición: Desconfianza y Mantenimiento del Control Local

Para Gadamer, todos interpretamos el mundo desde ciertos prejuicios o preconcepciones que provienen de nuestra tradición y experiencia pasada. En este contexto, los prejuicios no son necesariamente negativos; más bien, son el punto de partida para la comprensión.

Ambos técnicos muestran prejuicios hacia el control manual y la infraestructura local. Estos prejuicios reflejan una tradición operativa basada en servidores físicos y una desconfianza hacia la nube, vista como un sistema menos tangible y menos controlable.

Interpretación:

En el caso de la empresa externa, la experiencia en la gestión manual ha creado un enfoque pragmático: los técnicos valoran la estabilidad de lo que pueden controlar directamente. Esto refuerza la idea de que migrar a la nube implicaría un riesgo si no se garantiza un control equivalente.

En el hospital nacional, el prejuicio hacia la nube está más influido por la incertidumbre burocrática. La desconfianza hacia sistemas externos se debe a experiencias previas de falta de apoyo institucional, donde los cambios tecnológicos no han tenido continuidad.

Estrategia:

Para superar estos prejuicios, la comunicación clara sobre los niveles de control disponibles en la nube comunitaria será clave. La solución debe garantizar autonomía parcial y acceso a los datos bajo términos definidos por cada institución.

5.5.1.3. Diálogo Hermenéutico: Retos en Interoperabilidad y Escalabilidad

Para Gadamer, la comprensión se da a través del diálogo, donde cada interpretación es provisional y se enriquece con la interacción. El investigador entra en un proceso continuo de preguntas y respuestas, tanto con los datos obtenidos como con las teorías y conceptos que se manejan.

Las respuestas de ambas entrevistas revelan que la interoperabilidad es un desafío importante. En ambos contextos, la falta de estandarización y los problemas de compatibilidad entre sistemas obstaculizan el intercambio eficiente de información entre hospitales. La posibilidad de implementar una nube comunitaria es vista como una forma de mejorar esta situación.

Interpretación:

En la empresa externa, la nube es vista como una herramienta que podría facilitar la integración y colaboración entre múltiples hospitales, mejorando el acceso a los expedientes médicos desde cualquier institución.

En el hospital nacional, la interoperabilidad es percibida como una necesidad urgente, pero las barreras administrativas y presupuestarias dificultan cualquier intento de modernización.

Diálogo:

El análisis muestra que ambas perspectivas coinciden en que la nube puede optimizar la interoperabilidad, pero existen diferencias en la percepción del proceso de implementación.

El hospital nacional sugiere que la aceptación de la nube requerirá pruebas piloto y acuerdos de colaboración para superar las resistencias institucionales.

5.5.1.4. Contextualización Histórica y Cultural

Gadamer sostiene que toda comprensión está condicionada por factores históricos y culturales. No podemos interpretar un fenómeno sin tener en cuenta el contexto particular en el que ocurre.

Las entrevistas reflejan que la burocracia y la falta de recursos son desafíos comunes en la gestión de infraestructura tecnológica, aunque con matices diferentes en cada contexto. En la empresa externa, la falta de automatización y la gestión manual generan una carga operativa adicional. En el hospital nacional, la burocracia institucional ralentiza la adopción de nuevas tecnologías, limitando la capacidad de modernización.

Interpretación:

En ambos casos, el contexto histórico de dependencia de infraestructura física ha generado una cultura de conservadurismo tecnológico, donde cualquier cambio significativo requiere un esfuerzo considerable.

La escasez de recursos y apoyo institucional en el hospital nacional refuerza la necesidad de soluciones que no dependan totalmente de la infraestructura local, pero sin perder el control sobre los datos sensibles.

Estrategia:

El análisis sugiere que la nube comunitaria debe diseñarse teniendo en cuenta este contexto cultural y administrativo, ofreciendo soluciones adaptables y flexibles que puedan ajustarse al ritmo de cada institución.

5.5.1.5. Horizonte Abierto: Revisión Constante del Sentido

El proceso hermenéutico nunca es definitivo; cada interpretación es provisional y puede enriquecerse con nuevas perspectivas. El análisis debe permanecer abierto a nuevas interpretaciones y revisiones a medida que el estudio avanza.

Ambos técnicos reconocen que la capacitación es esencial para adoptar una nube comunitaria. La falta de experiencia en el manejo de tecnologías en la nube es vista como un obstáculo, pero también como una oportunidad de crecimiento si se ofrece la formación adecuada.

Interpretación:

En la empresa externa, la capacitación se enfoca en gestionar entornos híbridos y garantizar la continuidad de los servicios durante la migración.

En el hospital nacional, la capacitación se percibe como un requisito fundamental para reducir la resistencia del personal de TI y facilitar la transición hacia la nube.

Horizonte Abierto:

El análisis muestra que existe disposición a participar en proyectos piloto y estudios adicionales sobre la nube comunitaria. Esto refleja una apertura hacia la innovación, siempre que se respeten las preocupaciones sobre control, seguridad y autonomía.

5.5.2. Conclusiones del Análisis Hermenéutico

El enfoque hermenéutico gadameriano ha permitido interpretar las respuestas de los técnicos más allá de lo explícito, revelando las preocupaciones subyacentes en cuanto al control, la seguridad y la autonomía. A través de la fusión de horizontes, comprendimos que la resistencia hacia la nube comunitaria no es absoluta, sino que está enraizada en prejuicios y experiencias previas vinculadas a la burocracia y la falta de recursos.

5.5.2.1. Hallazgos Clave:

Control y Autonomía: Los técnicos valoran el control local porque les permite lidiar con la falta de apoyo institucional. La propuesta de nube comunitaria deberá ofrecer mecanismos claros de control y acceso.

Capacitación como Factor Clave: La falta de formación es una barrera importante, pero no insalvable. Los técnicos están abiertos al cambio si reciben el soporte y la capacitación adecuados.

Burocracia como Obstáculo Sistémico: La burocracia es un factor estructural que ralentiza la adopción de nuevas tecnologías, lo que genera una cultura de resistencia al cambio.

Interoperabilidad y Respaldo: Los técnicos reconocen los beneficios potenciales de una nube comunitaria, especialmente en términos de respaldo y seguridad, siempre que se mantenga una autonomía parcial.

5.5.2.2. Recomendaciones Finales:

- Diseñar una solución híbrida que combine infraestructura local y servicios en la nube.
- Implementar un plan de capacitación que prepare al personal para la transición.
- Crear políticas de control y acceso claras que aseguren la autonomía de cada institución.
- Desarrollar un plan piloto para generar confianza en la nube comunitaria antes de su implementación total.

Este análisis permite comprender las necesidades reales de los técnicos y adaptar la propuesta de nube comunitaria para que responda a sus expectativas y desafíos, facilitando una adopción exitosa en el sector salud en El Salvador y la región.

5.6. Análisis de Resultados Cuantitativos

El presente análisis tiene como objetivo interpretar los resultados obtenidos de una encuesta realizada a 20 encargados y coordinadores de TI en hospitales, clínicas y otras instituciones del sector salud. El propósito de esta encuesta es tener una mejor noción de sus conocimientos, percepciones, expectativas y preocupaciones respecto al uso de soluciones de nube comunitaria. Dado que estos profesionales son los responsables de la infraestructura tecnológica en sus instituciones, su opinión es crucial para evaluar la viabilidad y los desafíos que implica la adopción de esta tecnología.

A continuación, se presentan los resultados cuantitativos por pregunta junto con una deducción y análisis de cada una, en función de las respuestas obtenidas.

5.6.1. Análisis y Deducciones por Pregunta

Pregunta 1: ¿Conoce usted qué es una nube comunitaria?

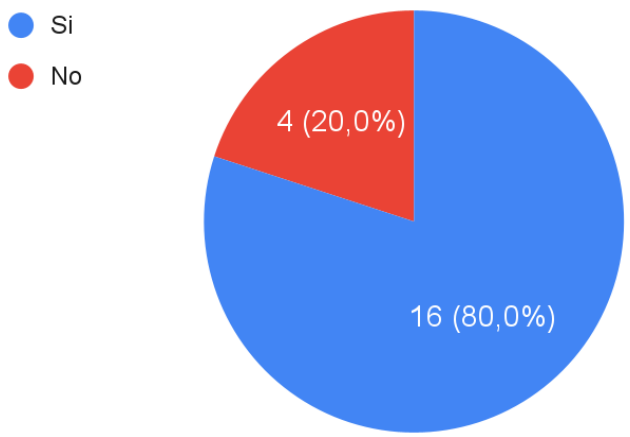


Figura 1. Resultados de la Pregunta 1

Análisis:

El 80% de los encuestados demuestra conocimiento sobre la nube comunitaria, lo cual refleja que esta tecnología no es ajena a los encargados de TI en instituciones de salud. Sin embargo, un 20% que desconoce el concepto sugiere que, aunque se ha avanzado en la difusión, aún existen brechas en la comprensión técnica de nuevas soluciones. Esto podría deberse a que algunas instituciones de salud se encuentran más atrasadas en su modernización y no han explorado este tipo de infraestructura.

El conocimiento sobre la nube comunitaria es crucial para que los encargados de TI puedan evaluar sus beneficios y riesgos. Sin un entendimiento claro, los procesos de adopción se pueden ver obstaculizados por la falta de confianza o comprensión técnica. Por tanto, capacitación específica sobre este tipo de soluciones será necesaria para lograr una adopción eficiente.

Pregunta 2: Está familiarizado con el concepto de una solución de nube comunitaria para el sector salud?

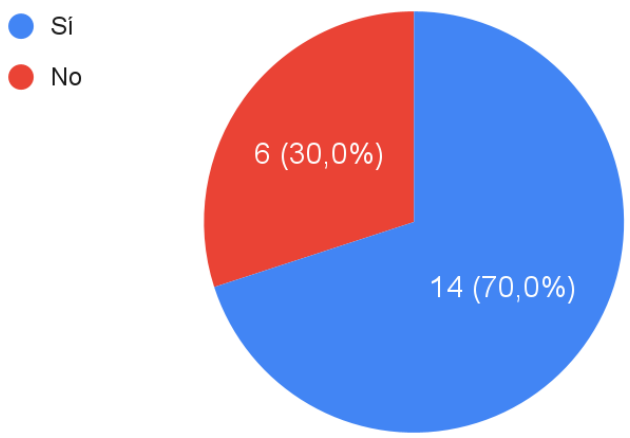


Figura 2. Resultados de la Pregunta 2

Análisis:

Aunque la mayoría de los encuestados conoce el concepto general de nube comunitaria, solo el 70% comprende su aplicación específica al sector salud. Esto refleja una asimetría en la familiaridad con los casos de uso especializados, lo cual podría ser un obstáculo para su implementación. La nube comunitaria no es solo una infraestructura compartida, sino que requiere alineación con normativas de salud, interoperabilidad entre instituciones y características específicas para gestionar datos médicos sensibles.

La falta de familiaridad puede implicar dudas sobre la viabilidad o utilidad de la nube en un entorno clínico. Una estrategia efectiva de implementación debería incluir pruebas piloto o estudios de caso exitosos que muestren su impacto en instituciones similares, ayudando a cerrar esta brecha de conocimiento.

Pregunta 3: ¿Considera que una nube comunitaria podría mejorar la eficiencia operativa de su institución?

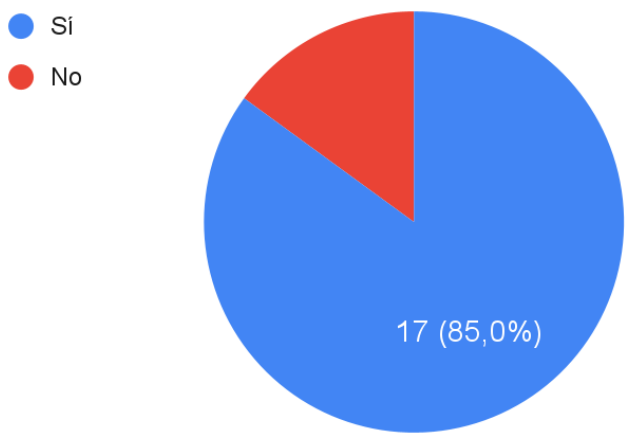


Figura 3: Resultados de la Pregunta 3

Análisis:

El 85% de los encuestados cree que la nube comunitaria podría mejorar la eficiencia operativa, lo que sugiere un reconocimiento generalizado de los beneficios que puede aportar esta tecnología. Las instituciones de salud manejan grandes volúmenes de información y procesos administrativos complejos; la posibilidad de automatización y acceso centralizado en una nube puede optimizar tareas como la gestión de expedientes electrónicos, el procesamiento de datos y el acceso remoto a información médica.

Sin embargo, el 15% que expresó dudas podría indicar preocupaciones sobre los costos de transición, el tiempo de aprendizaje para el personal o posibles interrupciones durante la implementación. Será importante desarrollar planes de transición gradual que mitiguen estos riesgos.

Pregunta 4: ¿Qué tan importante es la seguridad de los datos en la gestión de registros médicos electrónicos dentro de una nube comunitaria?

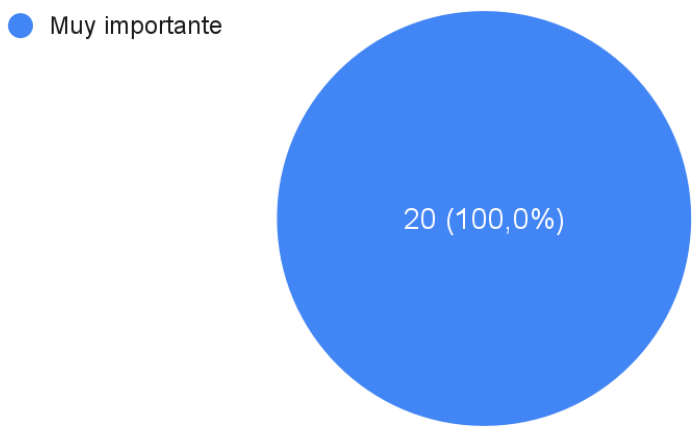


Figura 4: Resultados de la Pregunta 4

Análisis:

El consenso absoluto sobre la importancia crítica de la seguridad refleja la naturaleza altamente sensible de los datos de salud. Las instituciones de salud manejan datos personales, clínicos y financieros que deben protegerse contra accesos no autorizados y posibles ciberataques.

Este resultado subraya la necesidad de que cualquier solución en la nube cuente con protocolos robustos de seguridad: encriptación de extremo a extremo, control de acceso basado en roles y cumplimiento con normativas internacionales como la HIPAA (Health Insurance Portability and Accountability Act) o equivalentes locales.

Pregunta 5: ¿Qué nivel de confianza tendría en una solución en la nube para proteger la información de los pacientes?

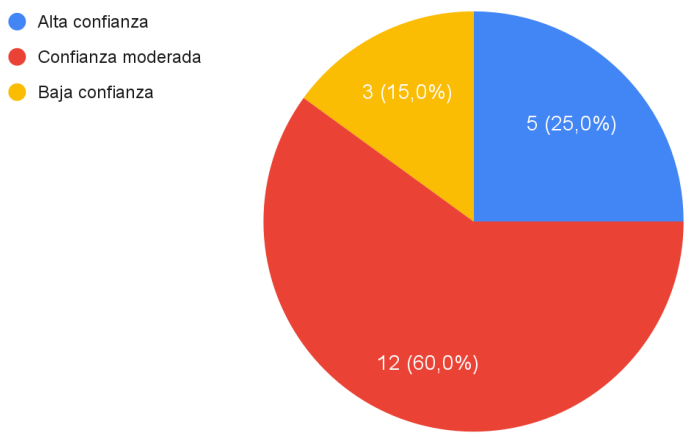


Figura 5: Resultados de la Pregunta 5

Análisis:

Aunque la mayoría tiene confianza moderada en las soluciones en la nube, solo el 25% expresa alta confianza. Esto indica que aún existen reservas importantes sobre la seguridad y fiabilidad de esta tecnología. La baja confianza en algunos casos podría estar relacionada con experiencias previas negativas o con la falta de claridad en los acuerdos de nivel de servicio.

Para aumentar la confianza, las instituciones deben garantizar que los proveedores de la nube ofrezcan transparencia en sus protocolos de seguridad y que los encargados de TI reciban capacitación continua para gestionar los riesgos potenciales.

Pregunta 6: ¿Piensa que una nube comunitaria puede facilitar el cumplimiento de las normativas en el manejo de datos de salud?

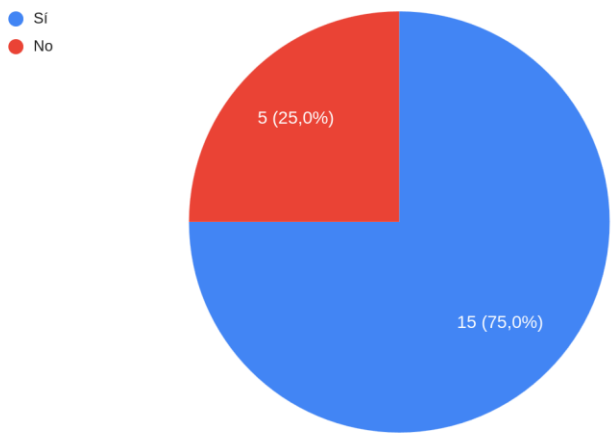


Figura 6: Resultados de la Pregunta 6

Análisis:

El 75% cree que la nube comunitaria facilitaría el cumplimiento normativo, especialmente porque las soluciones en la nube pueden integrar mecanismos de auditoría automática y herramientas para la gestión del consentimiento de los pacientes. Sin embargo, un 25% tiene dudas, probablemente por el temor a perder el control sobre los datos o por incertidumbre sobre la alineación con normativas específicas del sector.

Será necesario trabajar de cerca con los proveedores de servicios en la nube para asegurar la plena conformidad regulatoria y mantener el control adecuado sobre los datos sensibles.

Pregunta 7: ¿Qué beneficio considera más relevante en una solución de nube comunitaria para su institución?

Figura 7: Resultados de la Pregunta 7

Análisis:

Por otro lado, la reducción de costos es menos prioritaria, lo que sugiere que las instituciones valoran más la estabilidad y seguridad que el ahorro financiero inmediato. La mejora en la eficiencia de procesos tiene una menor percepción de importancia, probablemente porque aún no visualizan con claridad cómo la nube puede impactar en procesos internos. Esto implica que es fundamental realizar demostraciones prácticas que muestren cómo la nube puede automatizar y simplificar tareas diarias.

Pregunta 8: ¿Cómo calificaría la importancia de la escalabilidad en una solución de nube para su institución?

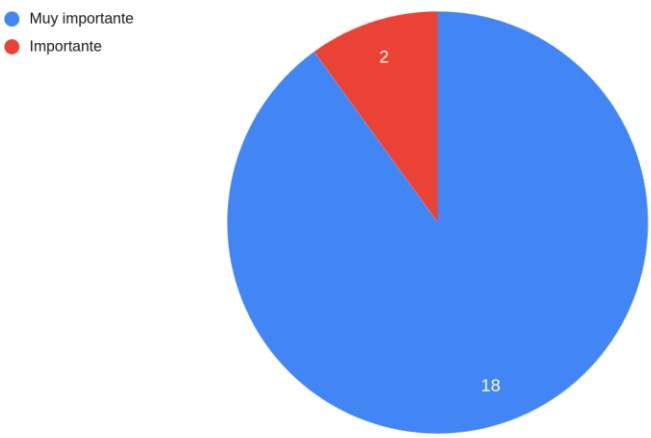


Figura 8: Resultados de la Pregunta 8

Análisis:

El hecho de que casi todos los encuestados consideren la escalabilidad muy importante indica que las instituciones son conscientes de la necesidad de expandir recursos rápidamente sin tener que realizar costosas adquisiciones de hardware. En el sector salud, donde la demanda puede cambiar abruptamente, la escalabilidad es un requisito crítico.

Además, la posibilidad de ajustar los recursos según la carga de trabajo permite a las instituciones optimizar su presupuesto, evitando inversiones innecesarias en infraestructura que no siempre se utiliza al máximo. Sin embargo, para aprovechar completamente esta ventaja, los encargados de TI deberán familiarizarse con herramientas de gestión en la nube, lo que requiere capacitación específica.

Pregunta 9: ¿Consideraría migrar los registros médicos electrónicos de su institución a una nube comunitaria?

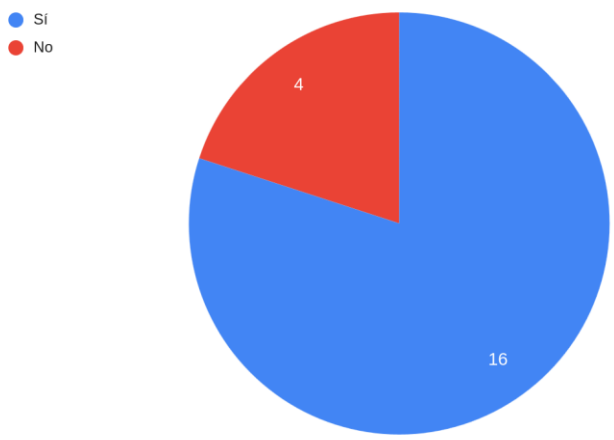


Figura 9: Resultados de la Pregunta 9

Análisis:

La disposición de la mayoría (80%) a migrar los registros médicos electrónicos a la nube comunitaria refleja confianza en los beneficios de la tecnología. Sin embargo, aquellos

que aún no están dispuestos a migrar probablemente tengan preocupaciones sobre la pérdida de control o el riesgo de interrupciones durante la transición.

Esto sugiere que los encargados de la implementación deben ofrecer garantías claras sobre la continuidad operativa y la accesibilidad de los datos durante y después de la migración. Además, podrían beneficiarse de planes de migración gradual, donde las instituciones transfieran datos menos críticos inicialmente para evaluar el rendimiento y seguridad antes de migrar el resto del sistema.

Pregunta 10: ¿Qué tan preocupado estaría por la velocidad de acceso a los datos al usar una nube comunitaria?

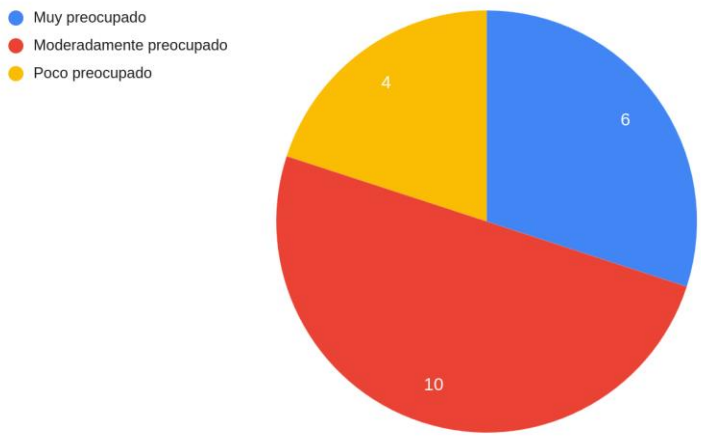


Figura 10: Resultados de la Pregunta 10

Análisis:

El 80% de los encuestados expresa algún grado de preocupación por la velocidad de acceso a los datos, lo que indica que la latencia y la disponibilidad son aspectos críticos en su evaluación de la nube comunitaria. En el sector salud, el acceso rápido a los expedientes es vital, especialmente en situaciones de emergencia.

Esto subraya la importancia de infraestructuras robustas con conexiones rápidas y eficientes. Los proveedores de servicios en la nube deberán garantizar acuerdos de nivel de servicio (SLA) que incluyan tiempos mínimos de respuesta y disponibilidad constante, además de ofrecer opciones de almacenamiento local para datos críticos.

Pregunta 11. ¿Cree que una nube comunitaria podría mejorar la capacidad de respuesta de su infraestructura TI ante demandas crecientes?

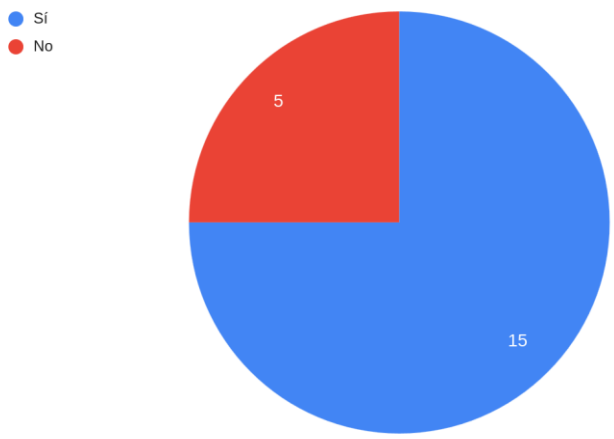


Figura 11: Resultados de la Pregunta 11

Análisis:

El hecho de que el 75% de los encuestados crea que la nube comunitaria mejoraría la capacidad de respuesta de su infraestructura TI indica un reconocimiento del potencial de la nube para gestionar aumentos en la demanda sin comprometer el rendimiento. En situaciones donde el volumen de pacientes o la cantidad de datos aumentan abruptamente, la escalabilidad y elasticidad de la nube permitirían a las instituciones adaptarse rápidamente.

Sin embargo, el 25% que no ve esta ventaja refleja una posible falta de confianza en la capacidad de la nube para responder adecuadamente en tiempo real. Para superar estas reservas, sería útil que las instituciones pudieran experimentar en entornos de prueba y medir cómo la nube se desempeña bajo condiciones de alta demanda.

Pregunta 12: ¿Qué tanto valoraría la capacidad de colaboración entre diferentes entidades hospitalarias a través de una nube comunitaria?

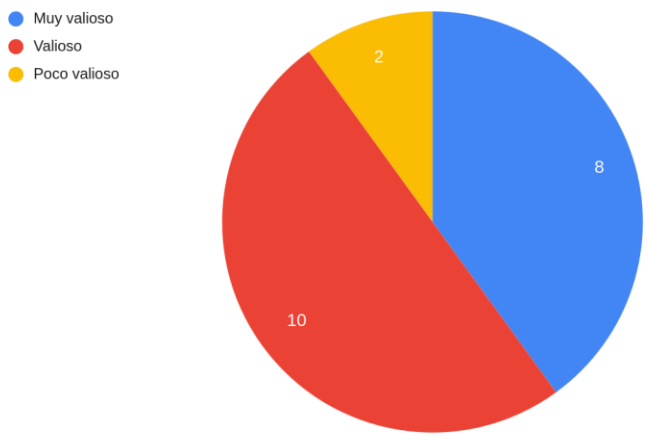


Figura 12: Resultados de la Pregunta 12

Análisis:

La colaboración entre instituciones de salud es vista como un beneficio importante, con 90% de los encuestados valorando la capacidad de trabajar en conjunto. Esto es especialmente relevante en entornos regionales o nacionales, donde compartir información entre hospitales puede mejorar la continuidad de la atención al paciente y facilitar la gestión de emergencias.

A pesar de ello, un pequeño grupo considera esta capacidad como poco valiosa, lo que podría deberse a experiencias previas negativas con sistemas de colaboración o a la falta de una infraestructura interoperable en la actualidad. Esto sugiere la necesidad de promover estándares de interoperabilidad que garanticen un flujo de información fluido y seguro entre instituciones.

Pregunta 13: ¿Qué barrera considera más significativa para el uso de una nube comunitaria en su institución?

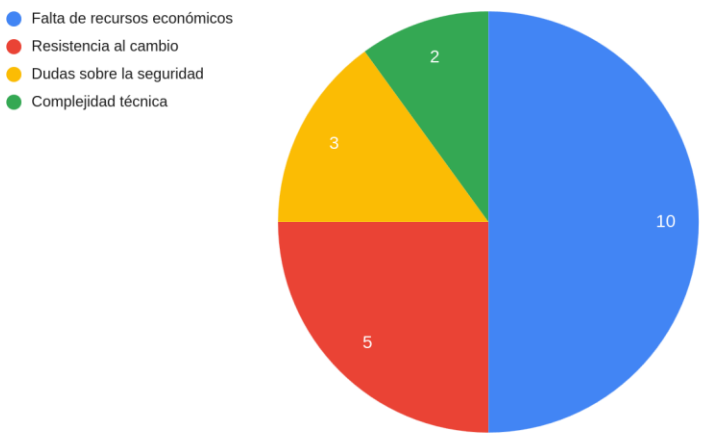


Figura 13: Resultados de la Pregunta 13

Análisis:

La falta de recursos económicos es la principal barrera, lo que indica que el costo inicial de implementación puede ser un obstáculo significativo para muchas instituciones. Aunque la nube comunitaria promete reducción de costos a largo plazo, las instituciones podrían necesitar modelos de financiación o apoyo gubernamental para superar esta barrera.

La resistencia al cambio también aparece como un problema importante, lo que sugiere que será necesario gestionar cuidadosamente el proceso de adopción mediante capacitación y estrategias de cambio organizacional. Las dudas sobre la seguridad reflejan que, aunque se reconoce la seguridad como un beneficio clave, aún existen temores sobre posibles vulnerabilidades en la nube.

Pregunta 14: ¿Qué tan probable es que recomendaría el uso de una nube comunitaria a otras instituciones hospitalarias?

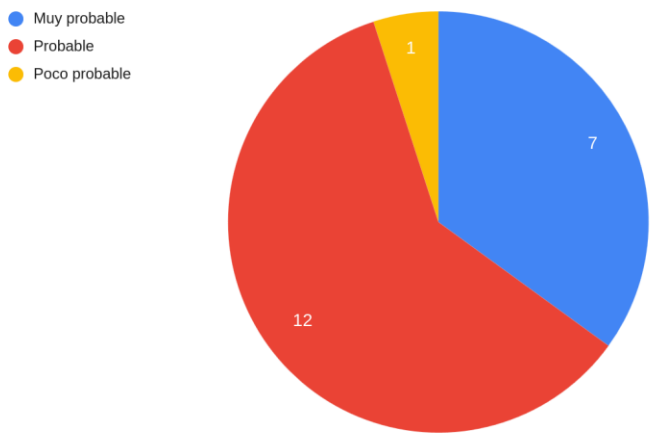


Figura 14: Resultados de la Pregunta 14

Análisis:

La alta disposición a recomendar la nube comunitaria refleja que, en general, los encargados de TI ven esta solución con buenos ojos. Sin embargo, el hecho de que una persona haya indicado que sería poco probable recomendarla sugiere que persisten algunas reservas o escepticismos que deben abordarse.

Es posible que este escepticismo esté relacionado con la falta de experiencias prácticas en la nube o con preocupaciones sobre la interoperabilidad y seguridad. Promover programas piloto que permitan evaluar los beneficios reales podría ayudar a consolidar la confianza y aumentar la disposición a recomendar la solución.

Pregunta 15: ¿Cuánto cree que una solución de nube comunitaria podría ayudar a reducir los tiempos de inactividad en su infraestructura TI?

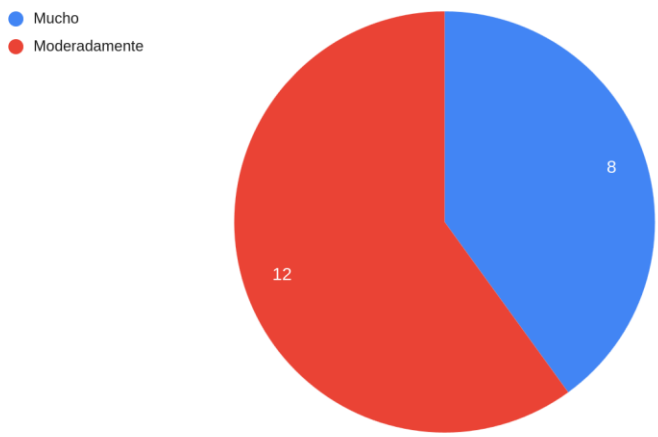


Figura 15: Resultados de la Pregunta 15

Análisis:

Todos los encuestados reconocen que la nube comunitaria podría contribuir a reducir los tiempos de inactividad, aunque la mayoría lo ve con una expectativa moderada. Esto refleja que, si bien confían en la capacidad de la nube para mejorar la disponibilidad del servicio, también son conscientes de que la estabilidad dependerá de la calidad del proveedor y de los acuerdos de nivel de servicio.

Será importante diseñar planes de contingencia y estrategias de recuperación ante desastres para garantizar que las instituciones puedan minimizar las interrupciones y mantener la continuidad operativa en todo momento.

Pregunta 16: ¿Considera que una solución de nube comunitaria podría reducir los costos relacionados con la infraestructura TI en su institución?

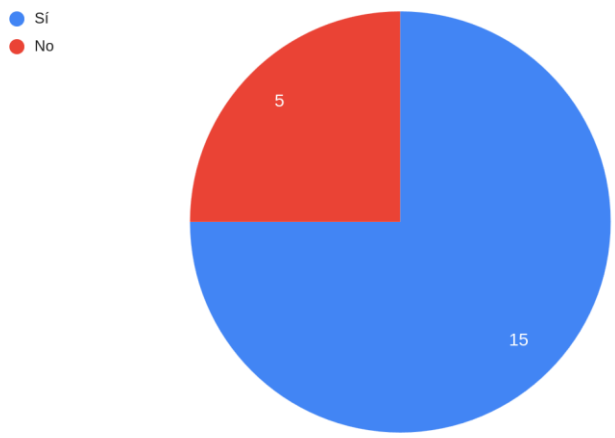


Figura 16: Resultados de la Pregunta 16

Análisis:

El 75% de los encuestados considera que la nube comunitaria podría reducir los costos relacionados con la infraestructura TI, lo que refleja una percepción positiva sobre la capacidad de esta tecnología para optimizar el uso de recursos financieros. Las soluciones en la nube permiten a las instituciones de salud evitar inversiones costosas en servidores físicos y mantenimiento, ya que ofrecen escalabilidad bajo demanda y precios flexibles según el uso.

Sin embargo, un 25% de los encuestados no comparte esta opinión, lo que sugiere que persisten preocupaciones sobre los costos de implementación inicial o dudas sobre el ahorro a largo plazo. Algunos pueden temer que los pagos recurrentes por servicios en la nube se acumulen y terminen superando los costos que enfrentarían con una infraestructura local. Además, la migración y la capacitación pueden representar gastos significativos en la fase de adopción.

Para mitigar estas preocupaciones, será importante que las instituciones reciban asesoría financiera clara, donde se comparen los costos actuales de infraestructura con los beneficios financieros proyectados de la nube a lo largo del tiempo. Modelos de

subvenciones o apoyo gubernamental también podrían acelerar la adopción y mostrar resultados más visibles a corto plazo.

Pregunta 17: ¿Qué tan importante es para usted el soporte técnico continuo en el uso de una solución de nube comunitaria?

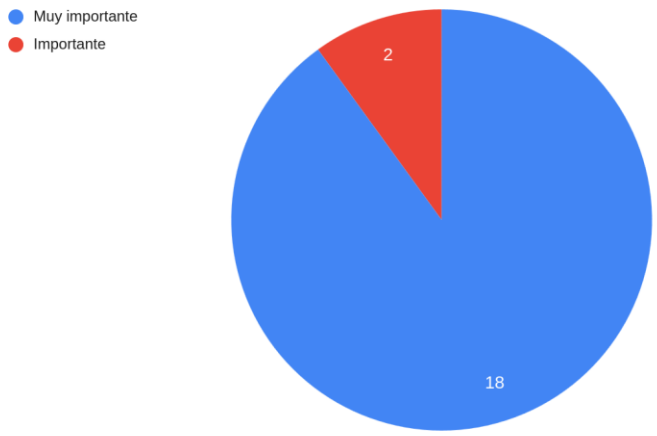


Figura 17: Resultados de la Pregunta 17

Análisis:

El soporte técnico continuo es visto como vital para el éxito de la implementación, con un 90% de los encuestados clasificándose como "muy importante". Esto refleja que las instituciones de salud no pueden permitirse interrupciones prolongadas en sus servicios y necesitan contar con asistencia rápida y eficaz para resolver cualquier problema técnico que pueda surgir.

El entorno hospitalario es especialmente exigente, dado que cualquier interrupción o falla técnica puede afectar la atención al paciente. Los encargados de TI necesitan tener acceso a soporte especializado 24/7, tanto para resolver problemas urgentes como para mantener actualizados los sistemas críticos.

La importancia del soporte técnico también está relacionada con el desarrollo de competencias internas. La adopción de una nube comunitaria implica nuevas habilidades

técnicas que los equipos de TI locales deberán adquirir. Por lo tanto, un proveedor que ofrezca capacitaciones periódicas y asistencia técnica asegurará una transición más fluida y facilitará el uso efectivo de la plataforma a largo plazo.

Pregunta 18: ¿Qué aspecto de una solución de nube comunitaria considera más crucial para la toma de decisiones en su institución?

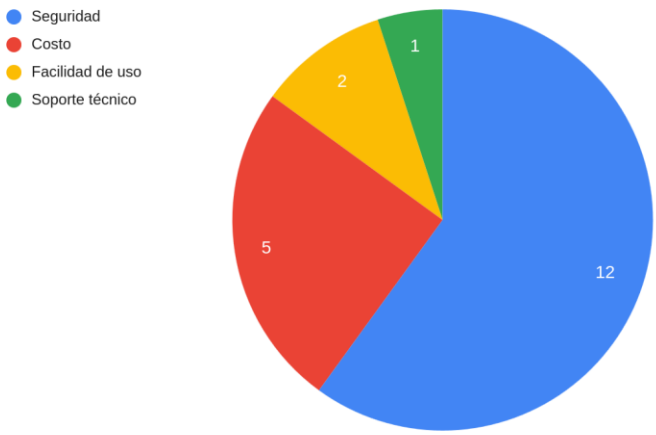


Figura 18: Resultados de la Pregunta 18

Análisis:

La seguridad es, nuevamente, el aspecto más crucial en la toma de decisiones, con un 60% de los encuestados priorizándola por encima de otras consideraciones. Esto refuerza el hecho de que la protección de los datos médicos es el factor decisivo para que las instituciones de salud opten por migrar a la nube. La naturaleza sensible de los datos clínicos exige una infraestructura con protocolos avanzados de seguridad, como encriptación y autenticación multifactorial.

Sin embargo, el costo también ocupa un lugar relevante, indicando que las decisiones no solo se toman en función de la seguridad, sino que también deben ajustarse a los presupuestos institucionales. Esto implica que la propuesta de nube comunitaria debe demostrar ahorros significativos y ofrecer un modelo de precios claro y competitivo.

La facilidad de uso y el soporte técnico recibieron menor prioridad, lo que podría indicar que los equipos de TI están dispuestos a enfrentar una curva de aprendizaje inicial, siempre y cuando la seguridad y el costo estén bien gestionados. Aun así, es importante ofrecer interfaces intuitivas y asegurar un soporte constante para evitar problemas operativos.

Pregunta 19: ¿Está de acuerdo con que una nube comunitaria podría ofrecer una mayor flexibilidad en la gestión de recursos TI?

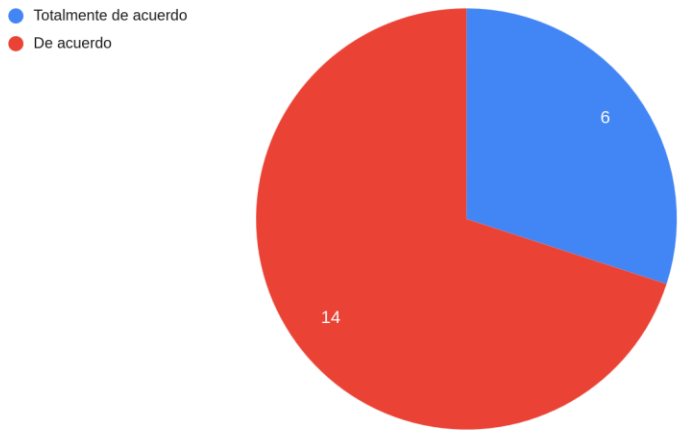


Figura 19: Resultados de la Pregunta 19

Análisis:

Todos los encuestados coinciden en que la nube comunitaria ofrecería mayor flexibilidad en la gestión de recursos TI, aunque con distintos grados de entusiasmo. Esta percepción refleja que las instituciones ven la nube como una forma de adaptarse rápidamente a cambios en la demanda, ya sea para procesar más datos, añadir nuevas funcionalidades o responder a emergencias de salud pública.

La flexibilidad que ofrece la nube comunitaria incluye la escalabilidad inmediata, lo que permite ajustar los recursos según las necesidades, evitando la dependencia de infraestructura física estática. Además, al compartir recursos entre instituciones, se facilita la

creación de plataformas colaborativas que fomenten el intercambio de información y la cooperación interinstitucional.

A pesar del consenso positivo, la falta de respuestas más entusiastas (es decir, más personas totalmente de acuerdo) podría sugerir que algunas instituciones aún tienen dudas sobre cómo se implementaría esta flexibilidad en la práctica. Demostrar esta capacidad mediante proyectos piloto y simulaciones en tiempo real podría reforzar la confianza en esta característica.

Pregunta 20: ¿Qué nivel de adopción de soluciones en la nube tiene actualmente su institución?

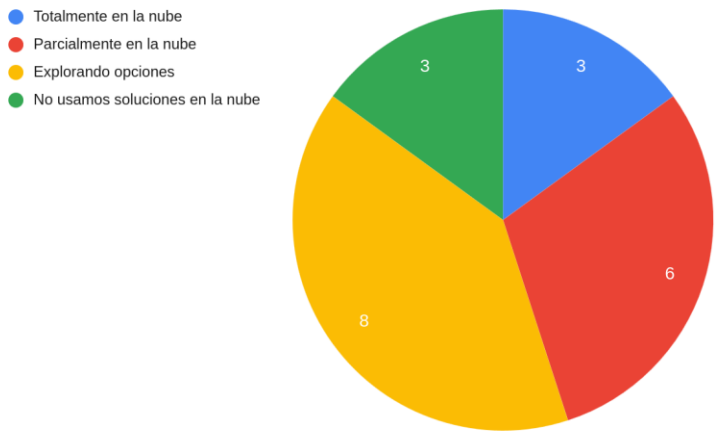


Figura 20: Resultados de la Pregunta 20

Análisis:

Los resultados muestran que solo el 15% de las instituciones han adoptado completamente soluciones en la nube, lo que sugiere que la transformación digital aún se encuentra en una etapa temprana en el sector salud. Sin embargo, la mayoría de las instituciones (70%) están explorando o han adoptado parcialmente soluciones en la nube, lo que indica que ya existe un proceso de transición hacia esta tecnología.

Las instituciones que están explorando opciones probablemente estén evaluando proveedores y modelos para encontrar la solución más adecuada a sus necesidades. Aquellas que ya usan parcialmente la nube pueden estar comenzando con funciones específicas, como almacenamiento de datos no críticos o sistemas administrativos, antes de migrar procesos más sensibles como los expedientes médicos electrónicos.

El hecho de que un 15% de las instituciones aún no utilicen la nube refleja la persistencia de barreras como la falta de recursos económicos, resistencia al cambio y preocupaciones sobre la seguridad. Para acelerar la adopción completa, será fundamental desarrollar casos de éxito y planes de implementación gradual que permitan a las instituciones ver los beneficios reales sin comprometer sus operaciones actuales.

5.6.2. Conclusión General de los Resultados de la Encuesta

Los resultados de la encuesta reflejan que existe una actitud positiva y una apertura significativa hacia la adopción de una nube comunitaria en el sector salud, aunque todavía persisten algunas barreras técnicas, económicas y culturales que deben ser abordadas para lograr una implementación exitosa. A continuación, se resumen los hallazgos más relevantes y las conclusiones extraídas de las respuestas a las 20 preguntas.

5.6.2.1. Alto Reconocimiento del Potencial de la Nube Comunitaria

La mayoría de los encuestados (85%) considera que la nube comunitaria puede mejorar la eficiencia operativa de sus instituciones. Las ventajas más valoradas incluyen la seguridad en el manejo de datos, la escalabilidad de la infraestructura y la reducción de costos operativos. Esto demuestra que las instituciones de salud están conscientes de los beneficios que esta tecnología puede aportar para optimizar sus procesos internos y mejorar la atención al paciente.

A pesar de este reconocimiento, algunas instituciones aún no están completamente familiarizadas con la aplicación de la nube comunitaria en el sector salud, lo que indica que será necesario capacitar y sensibilizar a los equipos de TI sobre los casos de uso específicos en entornos clínicos y hospitalarios.

5.6.2.2. Preocupación Predominante por la Seguridad y el Control de Datos

La seguridad de los datos emerge como la prioridad más importante en la toma de decisiones para la adopción de la nube comunitaria. Esto refleja la naturaleza crítica y sensible de la información médica que manejan las instituciones de salud. Si bien las instituciones reconocen que la nube comunitaria podría proporcionar mejores mecanismos de seguridad y respaldo de datos, todavía persisten ciertas dudas sobre la protección de la información.

La confianza moderada expresada por la mayoría de los encuestados sugiere que, aunque hay optimismo hacia la nube, será necesario que los proveedores de servicios en la nube demuestren con claridad sus protocolos de seguridad y brinden garantías sobre el control y acceso a los datos.

5.6.2.3. La Escalabilidad y Flexibilidad Como Necesidades Críticas

Los resultados muestran que la escalabilidad es considerada un aspecto fundamental para las instituciones de salud, permitiéndoles adaptarse rápidamente a cambios en la demanda sin necesidad de realizar grandes inversiones en infraestructura física. Del mismo modo, la flexibilidad en la gestión de recursos es vista como un valor clave, ya que las instituciones requieren infraestructuras dinámicas que se ajusten a necesidades cambiantes en tiempo real.

Esto resalta la importancia de que la nube comunitaria pueda ofrecer servicios que permitan escalar rápida y eficientemente, garantizando al mismo tiempo la continuidad de las operaciones sin interrupciones.

5.6.2.4. Desafíos en la Adopción: Recursos Económicos y Resistencia al Cambio

Si bien las instituciones ven con buenos ojos los beneficios de la nube, la falta de recursos económicos es señalada como la barrera más significativa para su adopción. Muchas instituciones del sector salud operan con presupuestos limitados y temen que los costos de implementación inicial puedan superar los ahorros proyectados. Por ello, será

necesario desarrollar modelos financieros sostenibles que permitan a las instituciones migrar de manera gradual y sin comprometer su operación.

La resistencia al cambio también aparece como un obstáculo relevante. La transición a nuevas tecnologías en entornos tradicionales puede generar inquietudes entre el personal sobre su capacidad para adaptarse. Será clave diseñar planes de gestión del cambio que incluyan capacitaciones específicas y la participación activa de los equipos de TI en todas las etapas de la implementación.

5.6.2.5. El Rol del Soporte Técnico en la Sostenibilidad de la Solución

El soporte técnico continuo es identificado como un elemento crítico para garantizar el éxito de la nube comunitaria. Las instituciones de salud necesitan tener acceso inmediato a asistencia especializada para resolver problemas técnicos y mantener la estabilidad del servicio. Esto resalta la importancia de establecer acuerdos de nivel de servicio (SLA) con los proveedores, que incluyan tiempos de respuesta rápidos y soporte 24/7.

Además, las instituciones esperan que el soporte técnico vaya acompañado de capacitación continua, permitiendo a los equipos de TI desarrollar las habilidades necesarias para gestionar la infraestructura en la nube de manera eficiente.

En conclusión, aunque las instituciones de salud están abiertas a la transformación digital mediante la nube comunitaria, el éxito de esta implementación dependerá de la capacidad de abordar las preocupaciones sobre seguridad, control, costo y soporte. Una implementación gradual, acompañada de proyectos piloto y planes claros de transición, permitirá consolidar la confianza en esta tecnología y facilitar su adopción a gran escala en el sector salud

6. Prototipo

El prototipo de nube comunitaria se basa en OpenStack y tiene como objetivo brindar servicios tecnológicos de infraestructura compartida para diversas instituciones, con un enfoque particular en el sector salud. Esta nube comunitaria estará compuesta por

múltiples regiones que se conectan a una región maestra central, desde donde se gestionan los recursos, usuarios, y servicios necesarios para garantizar interoperabilidad, escalabilidad y seguridad.

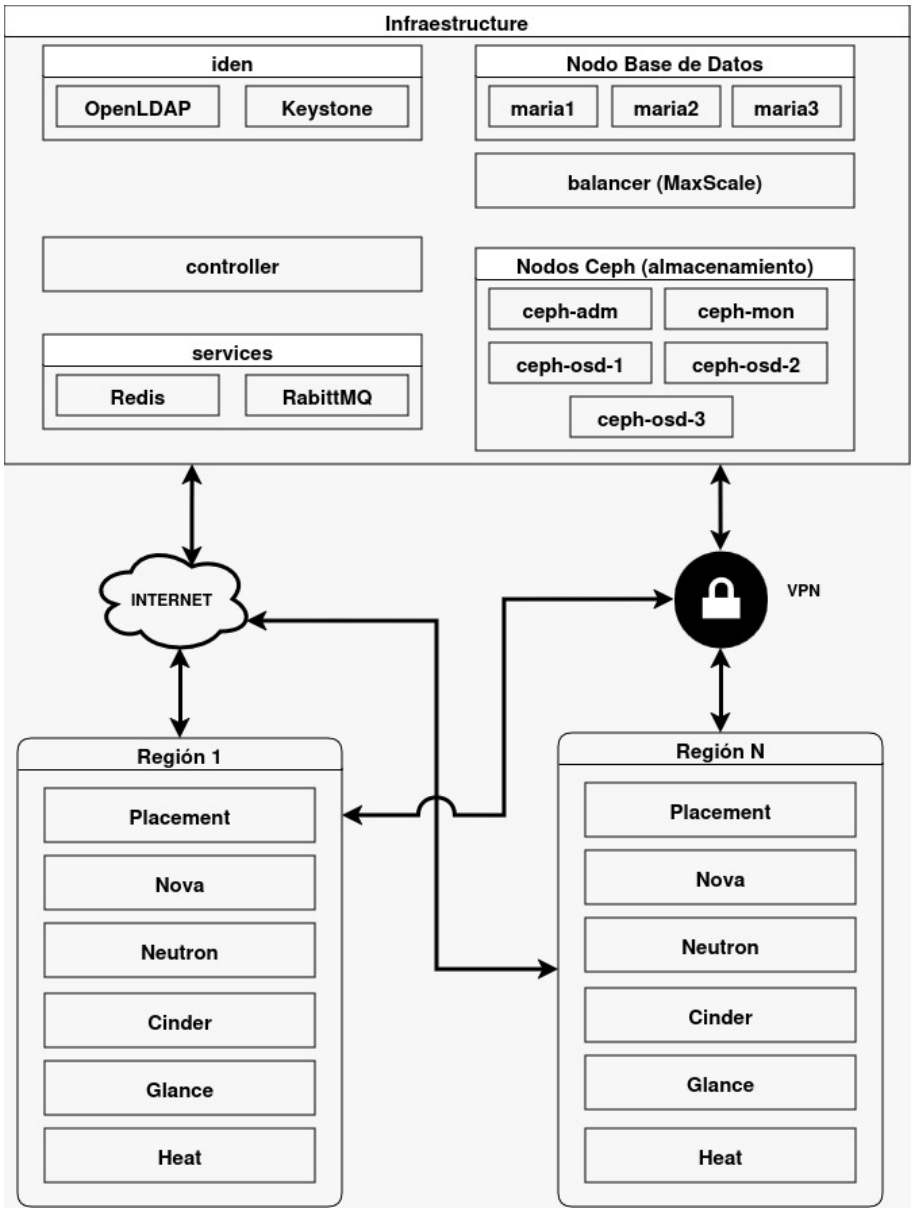


Figura 21: Prototipo de la nube

6.1. Requerimientos

6.1.1. Identidad Unificada y Autenticación Federada

Implementación de un servicio de identidad centralizado (Keystone), encargado de gestionar la autenticación y autorización de usuarios para todas las regiones conectadas.

Federación de usuarios mediante la integración con LDAP u otros repositorios de identidad (por ejemplo, Active Directory) para permitir un repositorio único de usuarios que todas las regiones puedan compartir.

6.1.2. Almacenamiento de Sesiones y Coordinación de Servicios

Uso de Redis como almacenamiento en caché para la gestión de sesiones y soporte de autenticación eficiente.

Implementación de un servicio de mensajería (RabbitMQ) que permita coordinar las operaciones críticas y la sincronización del estado entre los diferentes servicios de OpenStack distribuidos en las regiones.

6.1.3. Base de Datos Centralizada y Alta Disponibilidad

Despliegue de una base de datos centralizada (MariaDB) que almacene la información de configuración y control de todas las regiones, garantizando consistencia y eficiencia.

Implementación de replicación y alta disponibilidad mediante la configuración de clusters de bases de datos, para asegurar continuidad en caso de fallos.

6.1.4. Interfaz de Gestión Centralizada

Implementación de una interfaz web centralizada (Horizon) que permita la gestión y administración de la infraestructura desde la región maestra, proporcionando herramientas de monitoreo y gestión de recursos para las regiones conectadas.

Desarrollo de una API unificada que sirva para la comunicación y coordinación entre la región maestra y las regiones proveedoras de servicios.

6.1.5. Servicios por Regiones Especializadas

La región maestra (o Región 0) no proveerá directamente servicios como cómputo, almacenamiento en bloque o almacenamiento de objetos. Su función será servir como punto de control para las regiones que sí ofrecen estos servicios.

Cada región secundaria ofrecerá recursos específicos según sus necesidades, incluyendo:

- **Cómputo (Nova):** Gestión de máquinas virtuales.
- **Almacenamiento en bloque (Cinder):** Provisión de volúmenes para servidores.
- **Almacenamiento de objetos (Swift):** Gestión de grandes volúmenes de datos.
- **Redes (Neutron):** Conectividad interna y externa para las máquinas virtuales.

6.1.6. Escalabilidad y Aislamiento Regional

La nube comunitaria debe permitir agregar nuevas regiones dinámicamente, sin afectar la operación de las ya existentes. Esto garantiza que la infraestructura pueda escalar según las necesidades de las instituciones que la utilizan.

Las regiones funcionarán de forma semi-independiente, con la posibilidad de definir políticas específicas para cada una, pero sin perder la conexión con el sistema central.

6.1.7. Requerimientos de Hardware y Software

6.1.7.1. Región Maestra (Región 0)

Controladores: Servidores dedicados para gestionar las API, la autenticación y la base de datos.

Servidores de caché y mensajería: Redis y RabbitMQ en alta disponibilidad.

Almacenamiento distribuido: Ceph como backend para la gestión de objetos y volúmenes.

Redundancia: Uso de balanceadores de carga (HAProxy) y servicios de alta disponibilidad (Keepalived) para asegurar tolerancia a fallos.

6.1.7.2. Regiones Secundarias (Regiones de Provisión de Servicios)

Servidores de cómputo: Hosteando nodos de KVM o QEMU para máquinas virtuales.

Almacenamiento distribuido: Configuración de Ceph para volúmenes y objetos.

Redes: Configuración de Neutron para garantizar conectividad segura y aislada entre los recursos.

6.2. Arquitectura

La arquitectura propuesta para esta nube comunitaria basada en OpenStack se centra en una infraestructura distribuida que facilita la cooperación entre múltiples regiones. Cada componente está diseñado para proporcionar servicios esenciales y especializados que optimizan la operación, el almacenamiento y la gestión de recursos. La comunicación entre las regiones y la infraestructura central está protegida mediante VPNs privadas, asegurando la privacidad y eficiencia en los procesos.

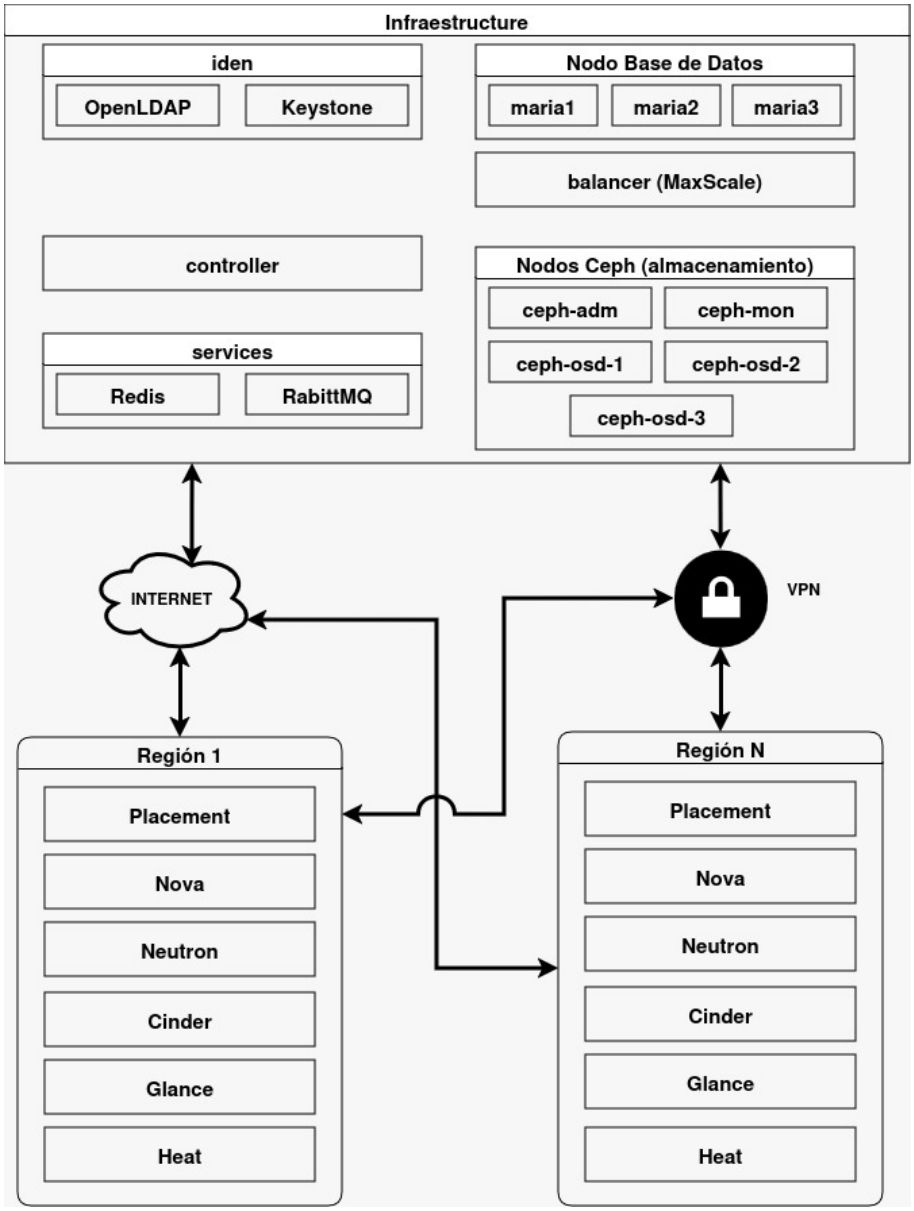


Figura 22: Arquitectura del Prototipo

6.2.1. Infraestructura Central (Región Principal o "Infraestructura")

La región principal actúa como punto de control y gestión para las regiones subordinadas. No proporciona directamente servicios de cómputo o almacenamiento a los usuarios finales, sino que facilita servicios de backend críticos mediante diversas APIs que habilitan la coordinación y operación fluida entre las regiones.

6.2.1.1. Servicio de Caché Redis

Redis ofrece almacenamiento en caché para mejorar la velocidad y eficiencia de las aplicaciones. Este servicio permite que las regiones recuperen datos de forma rápida, minimizando el tiempo de acceso y mejorando el rendimiento general.

6.2.1.2. Cola de Mensajes con RabbitMQ

RabbitMQ facilita la comunicación asíncrona entre los diferentes componentes del sistema. Mediante este servicio, las tareas se procesan en segundo plano, permitiendo que las aplicaciones respondan rápidamente.

Vhosts dedicados para cada región garantizan una gestión independiente de las colas de mensajes, evitando colisiones o retrasos en la transmisión de eventos entre regiones.

6.2.1.3. Base de Datos Centralizada con MariaDB

Un clúster de MariaDB actúa como la base de datos principal, proporcionando alta disponibilidad y consistencia en los datos para todas las regiones. Esto garantiza que las operaciones de las regiones puedan acceder y actualizar información de manera centralizada y segura.

6.2.1.4. Almacenamiento Distribuido con Ceph

La infraestructura utiliza Ceph para brindar almacenamiento redundante y distribuido, asegurando la alta disponibilidad y la integridad de los datos. Este sistema permite gestionar grandes volúmenes de datos sin comprometer la fiabilidad, y asegura que las regiones puedan acceder a los recursos de almacenamiento sin interrupciones.

6.2.1.5. Gestión de Recursos a través de Horizon

Horizon proporciona una interfaz de administración centralizada, facilitando la gestión de los recursos de las distintas regiones. Desde esta plataforma, los administradores pueden monitorear, aprovisionar y gestionar los recursos de la nube comunitaria.

6.2.1.6. Servicio de Autenticación y Autorización con Keystone

La autenticación de usuarios se realiza mediante Keystone, que se comunica con un servidor LDAP para administrar los usuarios federados. Este enfoque permite que todas las regiones compartan un repositorio único de usuarios, mejorando la gestión y simplificando los accesos.

6.2.1.7. DNS Centralizado con Bind9

Para evitar la gestión basada en IPs y facilitar la comunicación, se ha configurado Bind9 como servidor DNS. Esto permite la resolución de nombres de dominio tanto para la infraestructura central como para las regiones, asegurando que las comunicaciones sean consistentes y eficientes.

6.2.2. Regiones de Provisión de Servicios (Región Uno a N)

Cada región adicional (Región 1, Región 2, etc.) se encarga de proveer servicios específicos de OpenStack, tales como cómputo, redes y almacenamiento. Estas regiones funcionan de manera semi-independiente, pero siguen dependiendo de la infraestructura central para autenticación, administración y control.

6.2.2.1. Servicios Disponibles por Región

Placement: Optimización de recursos disponibles para garantizar el uso eficiente de cómputo y almacenamiento.

Nova: Administración de máquinas virtuales y recursos de cómputo.

Neutron: Gestión de la red y conectividad segura entre máquinas virtuales.

Swift: Almacenamiento de objetos para gestionar archivos grandes y datos no estructurados.

Cinder: Almacenamiento en bloque para volúmenes de datos conectados a servidores.

Glance: Gestión de imágenes de sistemas operativos y recursos de despliegue rápido.

6.2.3. Red Privada Virtual (VPN)

6.2.4. Integración y Coordinación de Recursos

La arquitectura permite que cada región funcione de forma semi-independiente, pero mantiene la integración con la infraestructura central mediante APIs y servicios federados. Esto proporciona:

- **Escalabilidad dinámica**, permitiendo agregar nuevas regiones sin afectar el rendimiento del sistema.
- **Interoperabilidad entre las regiones**, facilitando la colaboración entre distintas instituciones.
- **Redundancia y alta disponibilidad**, asegurando que las operaciones críticas se mantengan en funcionamiento aun en caso de fallos.

6.2.5. Conclusiones sobre arquitectura

Esta arquitectura de nube comunitaria basada en OpenStack ofrece una solución robusta, segura y escalable para las necesidades de múltiples instituciones del sector salud. La infraestructura centralizada facilita la gestión eficiente de usuarios y recursos, mientras que las regiones individuales proveen servicios específicos para satisfacer las demandas locales. La comunicación segura mediante VPN y la gestión federada de usuarios aseguran que la nube comunitaria cumpla con los requisitos de privacidad y control necesarios para aplicaciones críticas, como las del sector salud.

6.3. Hardware a Utilizar

La infraestructura de la nube comunitaria que se implementará se compone de varios nodos especializados que cumplen funciones críticas para garantizar autenticación, almacenamiento, balanceo de carga, gestión de recursos y alta disponibilidad. A continuación, se detalla la configuración del entorno, especificando los requerimientos de hardware para cada uno de los nodos clave de esta implementación.

6.3.1. Nodo Controlador

Este nodo es fundamental para la gestión de la infraestructura, ya que proporciona el servicio de identidad y permite la autenticación y autorización de usuarios. Además, alberga la interfaz de gestión Horizon, desde donde los administradores supervisan y configuran los servicios.

Tabla 1: Requerimiento nodo controller

Nodo	Núcleos	Memoria (GB)	Almacenamiento (GB)	SO
controller	8	12	300	Ubuntu

6.3.2. Nodo de Identidad

Este nodo se encarga exclusivamente de administrar usuarios, permisos y roles, permitiendo una autenticación centralizada para toda la infraestructura y las regiones.

Tabla 2: Requerimiento nodo iden

Nodo	Núcleos	Memoria (GB)	Almacenamiento (GB)	SO
iden	4	6	50	Ubuntu

6.3.3. Nodo de Servicios

Este nodo contiene los servicios de Redis para mejorar el rendimiento mediante el almacenamiento temporal en memoria. También se encarga de la coordinación de tareas asíncronas mediante RabbitMQ y aloja el clúster de bases de datos.

Tabla 3: Requerimiento nodo services

Nodo	Núcleos	Memoria (GB)	Almacenamiento (GB)	SO
services	4	8	100	Ubuntu

6.3.4. Nodo DNS

Este nodo utiliza Bind9 para resolver nombres de dominio dentro de la infraestructura, evitando el uso de direcciones IP directas para la comunicación entre instancias y recursos.

Tabla 4: Requerimiento dns

Nodo	Núcleos	Memoria (GB)	Almacenamiento (GB)	SO
dns	4	4	50	Ubuntu

6.3.5. Nodo Balanceador de Carga

El nodo MaxScale se encarga de balancear las peticiones hacia los servidores de base de datos del clúster. Además, proporciona un panel de administración que permite monitorear las operaciones y el tráfico.

Tabla 5: Requerimiento balanceador de carga

Nodo	Núcleos	Memoria (GB)	Almacenamiento (GB)	SO
balancer	2	4	25	Ubuntu

6.3.6. Nodo Base de Datos

Estos nodos contienen la base de datos MySQL distribuida que proporciona almacenamiento centralizado y acceso eficiente a los datos.

Tabla 6: Requerimiento nodos de base de datos

Nodo	Núcleos	Memoria (GB)	Almacenamiento (GB)	SO
maria1	2	2	100	Ubuntu
maria2	2	2	100	Ubuntu

maria3	2	2	100	Ubuntu

6.3.7. Nodos Ceph

Estos nodos forman el clúster de Ceph, proporcionando almacenamiento distribuido con alta disponibilidad. Se dividen en nodos administradores y nodos OSD (Object Storage Daemons) que almacenan los datos.

Tabla 7: Requerimiento nodos de Ceph

Nodo	Núcleos	Memoria (GB)	Almacenamiento (GB)	SO
ceph-adm	2	4	25	Ubuntu
ceph-mon	2	2	25	Ubuntu
ceph-osd-1	2	2	200	Ubuntu
ceph-osd-2	2	2	200	Ubuntu
ceph-osd-3	2	2	200	Ubuntu

6.3.8. Conclusión de Configuración de Hardware

La configuración del entorno para esta nube comunitaria basada en OpenStack está diseñada para optimizar la operación y garantizar la alta disponibilidad de los servicios. La infraestructura incluye nodos especializados, desde controladores y balanceadores de carga hasta clústeres de almacenamiento distribuido y bases de datos replicadas. Cada nodo cumple un rol específico dentro del sistema, asegurando que la infraestructura funcione de manera coordinada, segura y eficiente.

Este diseño asegura la escalabilidad y el rendimiento de la infraestructura, permitiendo agregar nuevas regiones o servicios sin afectar la estabilidad general. Gracias a la utilización de componentes críticos como Keystone para la autenticación, RabbitMQ para la mensajería, y Ceph para el almacenamiento distribuido, esta solución garantiza que la nube comunitaria cumpla con las necesidades operativas y de seguridad del sector salud.

6.4. Topología de Red

La topología de red diseñada para esta infraestructura está optimizada para garantizar seguridad, disponibilidad y eficiencia en la comunicación entre los diferentes componentes. Esta topología define varias redes específicas que gestionan las operaciones internas de la infraestructura, el acceso público a los servicios y la comunicación segura entre regiones mediante VPN. Cada red está orientada a un propósito específico, asegurando que el tráfico de datos esté correctamente aislado y optimizado.

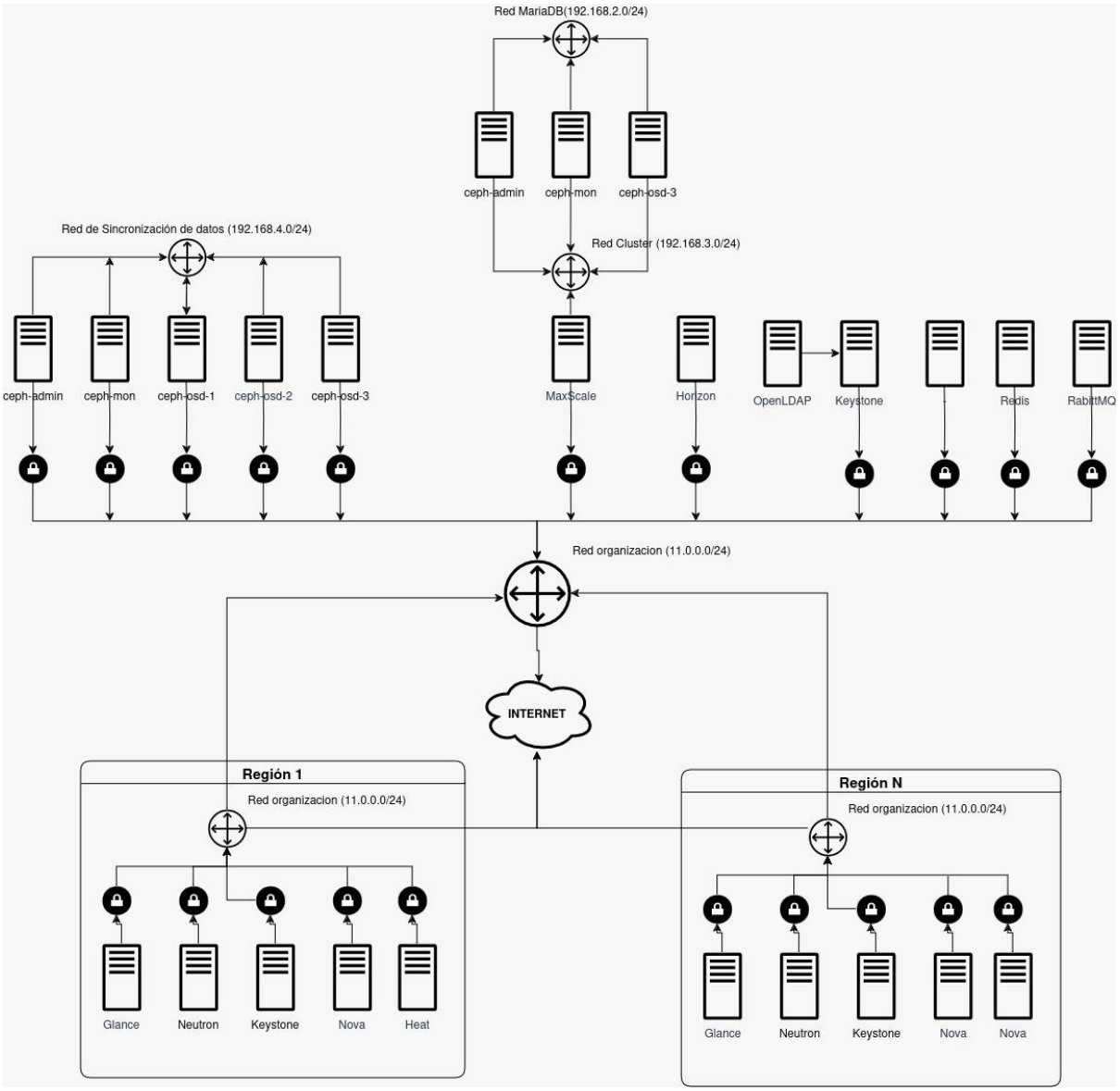


Figura 23: Topología de Red

6.4.1. Red de la Organización (Red Principal)

Esta es la red expuesta a internet que permite a los servicios internos de la infraestructura ser accesibles públicamente.

IP Rango: 11.0.0.0/24

Esta red conecta los servicios de Keystone, Horizon, RabbitMQ y OpenLDAP, asegurando que las solicitudes públicas puedan ser autenticadas y gestionadas de manera eficiente.

6.4.2. Red de Balanceo de Carga

El balanceador MaxScale utiliza esta red para distribuir la carga entre los nodos del clúster de bases de datos MariaDB.

IP Rango: 192.168.2.0/24

Esta red permite que el tráfico de datos hacia las bases de datos se distribuya de manera eficiente, evitando cuellos de botella.

6.4.3. Red del Clúster de Bases de Datos

Los nodos de MariaDB están interconectados mediante esta red para sincronizar información y mantener la integridad de los datos a través de replicación continua.

IP Rango: 192.168.3.0/24

Esta red es de alta velocidad para garantizar redundancia y coherencia en tiempo real entre los nodos de base de datos.

6.4.4. Red de Sincronización de Datos (Ceph)

Esta red es utilizada por los nodos del clúster de Ceph (OSD, Administrador y Monitor) para sincronizar los datos almacenados.

IP Rango: 192.168.4.0/24

Esta red permite mantener la alta disponibilidad de los datos distribuidos, asegurando que las fallas en un nodo no afecten la accesibilidad de los recursos.

6.4.5. Red VPN (Red Privada Virtual)

La red VPN proporciona comunicación segura entre la infraestructura central y las distintas regiones.

IP Rango: 10.147.17.0/24

Esta red garantiza que las regiones de la nube comunitaria puedan acceder a las APIs de la infraestructura de forma segura y privada, evitando el tráfico no autorizado.

6.4.6. Redes Regionales de Proveedor y Organización

Cada región (por ejemplo, Región Uno y Región Dos) cuenta con redes internas independientes para gestionar sus recursos y servicios.

Región Uno:

- **Red de Organización:** 11.0.0.0/24
- **Red Provider:** 203.0.21.0/24
- Esta región contiene servicios esenciales como **Nova, Neutron y Glance** para gestión de máquinas virtuales y almacenamiento de imágenes.

Región Dos:

- **Red de Organización:** 12.0.0.0/24
- **Red Provider:** 203.0.22.0/24
- Provee servicios adicionales para escalabilidad y balanceo de cargas internas con **Keystone y Neutron**.

6.4.7. Resumen del Flujo de Datos en la Infraestructura

1. Acceso a Servicios (Comunicación Segura): La VPN conecta las regiones con la infraestructura, permitiendo el acceso seguro a servicios y recursos. Las solicitudes llegan a través de la VPN para ser autenticadas por Keystone.

2. Distribución de Carga: MaxScale recibe tráfico desde los servicios de aplicación y distribuye las peticiones hacia los nodos de MariaDB.

3. Sincronización Interna: Los nodos de MariaDB mantienen coherencia de datos a través de la red del clúster.

4. Almacenamiento Distribuido: Los nodos de Ceph intercambian datos a través de la red de sincronización, asegurando redundancia.

5. Acceso Público: Pueden realizarse solicitudes a Internet para realizar actualización de paquetes y otros componentes de los sistemas operativos que conforman la infraestructura.

6.4.8. Conclusión sobre Topología

Esta topología de red permite que la infraestructura de la nube comunitaria funcione de manera segura, eficiente y escalable. Las redes segmentadas por propósito aseguran que los servicios críticos no interfieran entre sí, mientras que la VPN garantiza que las comunicaciones entre regiones y la infraestructura se mantengan privadas y controladas. Con esta configuración, se logra una infraestructura robusta que puede crecer dinámicamente y responder a las necesidades del sector salud.

6.5. Construcción de Prototipo

6.6. Pruebas

7. Caso de Estudio

El presente caso de estudio plantea cómo una infraestructura de nube comunitaria basada en OpenStack puede ser implementada en instituciones del sector salud la cual les puede ser factible utilizar para el despliegue de sistemas de gestión de registros médicos electrónicos (EHR), tales como OpenMRS, reconocida por su aplicación en el sector salud. Esta infraestructura se centra en proporcionar un entorno seguro, escalable y eficiente para la gestión de la información médica, facilitando el acceso rápido y protegido a los datos clínicos en instituciones distribuidas.

La arquitectura permite conectar diferentes instituciones mediante una red privada virtual (VPN), garantizando una comunicación segura y sin interrupciones entre los nodos participantes. Esto asegura que los datos se mantengan sincronizados y accesibles desde cualquier sede que forme parte de la red, sin importar su ubicación geográfica. Si se desplegara una solución como OpenMRS, la infraestructura facilitaría que sus módulos más importantes, como el de gestión de pacientes y administración de consultas, funcionen sin interrupciones, optimizando los tiempos de respuesta y permitiendo que los profesionales de salud accedan a la información en tiempo real.

La infraestructura de nube comunitaria también ofrece redundancia y alta disponibilidad, lo que garantiza que los datos permanezcan accesibles incluso si alguno de los nodos regionales sufre una interrupción. El control de acceso se gestiona mediante servicios de autenticación centralizados, permitiendo a cada institución regular quién puede acceder a los registros médicos, reforzando así la seguridad de la información sensible.

El rendimiento se optimiza mediante la implementación de caché de sesión y sistemas de mensajería asíncrona, que aseguran la eficiencia operativa y mantienen la continuidad de los servicios, incluso en momentos de alta demanda. Además, el balanceo de carga en la infraestructura permite que las solicitudes se distribuyan equitativamente entre los diferentes recursos, asegurando que las bases de datos funcionen de manera eficiente y sin retrasos.

Con este enfoque, la infraestructura de nube comunitaria no solo proporciona recursos compartidos y escalables, sino que también permite que las instituciones de salud operen de manera más eficiente, asegurando la disponibilidad de la información médica en todo momento. Esta solución facilita la colaboración entre distintas entidades, optimiza los costos operativos al compartir recursos, y contribuye a mejorar la calidad del servicio al paciente mediante un acceso ágil y seguro a los registros clínicos.

8. Factibilidad

La factibilidad del análisis es una parte vital durante el prototipado de una infraestructura de nube comunitaria en base de OpenStack. Para la creación y análisis se evaluó desde dos aspectos diferentes: técnico y económico. En este estudio se busca demostrar que implementar una solución de nube comunitaria con OpenStack es factible en ambos aspectos y puede proporcionar una alternativa accesible, segura y adecuada en comparación los servicios brindados por grandes empresas del mercado.

8.1. Factibilidad Técnica

OpenStack es una plataforma de código abierto ampliamente utilizada para construir infraestructuras en la nube. A diferencia de los servicios comerciales como AWS y Google Cloud, permite a las organizaciones gestionar sus propios recursos con un control total sobre la infraestructura.

Parte de las ventajas de utilizar OpenStack son:

Escalabilidad y Flexibilidad: la infraestructura puede crecer según la demanda y necesidades de las empresas, algo crucial para una nube comunitaria donde las necesidades pueden variar, esto ofrece un control màs propio a comparación de otras empresas que brindan servicios.

Integración: OpenStack es compatible con múltiples sistemas operativos y motores de bases de datos, esto permite que se puedan hacer integraciones diversas según las necesidades.

Seguridad Personalizable: OpenStack permite la integración de seguridad a medida utilizando Keystone para la autentificación y protocolos como SAML y OpenID para usuarios Federados.

Tabla 8: Cuadro comparativo entre otros proveedores que brindan servicios de nube

Características	OpenStack (Nube Comunitaria)	AWS	Google Cloud
Implementación	Control total	Control limitado a servicios	Control limitado a servicios
Costos	Costos de implementación altos	Pago por servicios	Pago por servicios
Compatibilidad	Alta flexibilidad para	Infraestructura predefinida	Infraestructura predefinida
Autentificación	Configurable según necesidades(Keystone + SAML/OpenID)	AWS IAM	Identity Platform (OpenID/SAML)

Base de datos	Soportar múltiples motores de DB	Amazon RDS, Aurora	Cloud SQL, MySQL,Postgres

OpenStack brinda más control y flexibilidad que otros servicios por terceros ya sea AWS y Google Cloud. Esto lo convierte en una buena opción para la integración de una nube comunitaria de múltiples regiones escalables.

8.2. Factibilidad Económica

La factibilidad económica se evalúa considerando la inversión de inicio que se requeriría para realizar la implementación de una nube comunitaria y cuál es la inversión al contratar servicios a proveedores como AWS y Google Cloud. Mediante este estudio comparativo, se determinará la factibilidad económica del proyecto.

Tabla 9: Componentes

Componente	Descripción	Cantidad
Nodo Admin	Servidor para la gestión y administración de OpenStack.	1
Nodos de Control	Servidores que manejan servicios centrales de OpenStack.	3
Nodos MariaDB	Clúster de bases de datos para alta disponibilidad y replicación síncrona.	3
Nodo MaxScale	Balanceador de carga para distribuir el tráfico entre los nodos de la base de datos.	1
Nodo Ceph Admin	Nodo para la administración del clúster Ceph.	1
Nodo Monitor (Ceph MON)	Supervisión del clúster Ceph.	1

Nodos de Almacenamiento (Ceph OSD)	Almacenamiento de datos y replicación.	3
Rack para Servidores	Estructura para montar y organizar los servidores.	1
Switch de Red	Conmutador para interconectar los servidores.	1

Tabla 10: Presupuesto Inicial

Componente	Especificación	Costo Total
Nodo Admin	Intel Xeon E-2136 de 6 núcleos a 3.3 GHz, 64 GB DDR4, SSD de 4 TB	$2,399.00
Nodos de Control	Intel Xeon E-2136 de 6 núcleos a 3.3 GHz, 64 GB DDR4, SSD de 4 TB	$7,197.00
Nodos MariaDB	Intel Xeon E-2136 de 6 núcleos a 3.3 GHz, 64 GB DDR4, SSD de 4 TB	$7,197.00
Nodo MaxScale	Intel Xeon E-2136 de 6 núcleos a 3.3 GHz, 64 GB DDR4, SSD de 4 TB	$2,399.00
Nodo Ceph Admin	Intel Xeon E-2136 de 6 núcleos a 3.3 GHz, 64 GB DDR4, SSD de 4 TB	$2,399.00
Nodo Monitor (Ceph MON)	Intel Xeon E-2136 de 6 núcleos a 3.3 GHz, 64 GB DDR4, SSD de 4 TB	$2,399.00
Nodos de Almacenamiento (Ceph OSD)	Intel Xeon E-2136 de 6 núcleos a 3.3 GHz, 64 GB DDR4, SSD de 8 TB	$8,397.00
Rack para Servidores	Rack de servidor de marco abierto de 25U, capacidad de 800 libras.	$203.99
Switch de Red	Conmutador para interconectar los servidores.	$249.99
Total inversión inicial		$32,840.98

Nota: Los costos se basan en precios obtenidos de Amazon.

Esta inversión es crítica para la gestión de la nube asegurando la estabilidad del servicio desde el inicio, permitiendo una operación sin contratiempos y sentando las bases para la expansión futura del negocio.

Tabla 11: Costos de servicios de otros proveedores

Proveedor	Servicio	Costo Mensual por Instancia	Costo Anual
AWS EC2	t2.medium (2 vCPU, 4 GB RAM)	$33.87	$405.72
AWS EC2	m5.4xlarge(16 vCPU, 64 GB RAM)	$355.51	$4,266.12
Google Cloud Compute	e2-standard-2 (2 vCPU, 8 GB RAM)	$52.61	$631.32

Nota: Los costos fueron obtenidos de las calculadoras oficiales de precios de AWS y Google Cloud al 26 de noviembre de 2024 (Amazon Web Services, 2024; Google Cloud, 2024). Los precios son estimaciones para instancias Linux en la región de EE.UU. Este y no incluyen costos adicionales como almacenamiento o transferencia de datos.

Como es de esperarse, la inversión inicial del prototipo es mayor en comparación con utilizar los servicios de AWS, sin embargo, al utilizar AWS la inversión es constante y a

largo plazo superará la inversión inicial, si bien es cierto, a la infraestructura física se le dará mantenimiento cada 6 meses esto en comparación con las mensualidades permanentes de los servicios de AWS serán pequeños y el beneficio de la infraestructura física se podrá ver reflejado a medida que pase el tiempo, además del beneficio económico a largo plazo, una infraestructura física con la implementación de la nube comunitaria multirregional, proporciona mayor control sobre los recursos utilizados y evita costos variables a largo plazo. De igual forma brinda la libertad de poder escalar según las necesidades sin depender de terceros.

Ventajas de implementar una nube comunitaria basada en OpenStack

Reducción de costos a largo plazo

Control total de recursos

Escalabilidad según demanda

Potencial para reutilización de equipos

La implementación de una nube comunitaria basada en OpenStack es factible económicamente, teniendo en cuenta si el proyecto es para largo plazo, ya que la inversión inicial es bastante considerable mayor ante otras opciones ya puestas en el mercado, nos podemos beneficiar de la facilidad de control y la escalabilidad de la nube.
Se implementará un modelo de negocio competitivo para recuperar la inversión inicial y lograr rentabilidad mediante la venta de infraestructura como servicio a organizaciones de salud en Centroamérica. El modelo de negocio enfatizará los beneficios de una nube comunitaria multirregional. La estrategia principal es ganar clientes con precios más bajos en comparación con AWS o Google Cloud y, al mismo tiempo, ofrecer costos fijos y control total de los datos, lo cual es muy importante para el sector. Cabe destacar que también se ofrecerán productos de código abierto, como sistemas de registros médicos electrónicos, los cuales estarán disponibles para los clientes con solo unos clics.

El aumento de la base de clientes permitirá amortizar el retorno de la inversión inicial. Los costos operativos se mantendrán bajo control debido a la infraestructura física propia y al pequeño costo de los mantenimientos. Con un ingreso estable, el modelo puede eventualmente escalar para brindar más servicios adicionales, como almacenamiento seguro, copias de seguridad, análisis de datos médicos y soporte técnico personalizado. De esta manera, se maximiza el retorno de la inversión y se consolida la ventaja competitiva en la región.

9. Conclusiones

La infraestructura desarrollada permite gestionar el acceso de manera centralizada mediante un sistema de autenticación federada, proporcionando una experiencia segura y fluida para los usuarios. Esto facilita que los profesionales de salud accedan a los servicios desde cualquier región sin necesidad de múltiples inicios de sesión, asegurando así operaciones coordinadas y eficientes entre las instituciones participantes.

El prototipo validó que la interfaz web centralizada ofrece una plataforma efectiva para la gestión integral de recursos y servicios distribuidos en distintas regiones. Esta herramienta permite a los administradores supervisar y controlar las operaciones de forma coherente y en tiempo real, facilitando la toma de decisiones estratégicas y garantizando que las instituciones funcionen bajo un marco unificado de gestión.

La infraestructura confirmó su capacidad para gestionar bases de datos distribuidas, asegurando que los registros de salud estén siempre accesibles y seguros. Esta arquitectura permite que la información se mantenga íntegra y disponible en tiempo real para los usuarios autorizados, garantizando la continuidad operativa incluso en situaciones de alta demanda o interrupciones imprevistas en alguno de los nodos de la red.

Se mostró que la infraestructura de nube comunitaria es compatible con sistemas EMR como OpenEMR, proporcionando el entorno adecuado para su despliegue eficiente. La

arquitectura facilita la gestión autónoma de múltiples instancias distribuidas entre distintas regiones, permitiendo que cada institución opere de forma independiente sin comprometer la colaboración y el intercambio de información entre las entidades. El diseño modular asegura que el sistema pueda adaptarse a las necesidades cambiantes del entorno sanitario, mientras que la autenticación centralizada y la gestión de datos en tiempo real garantizan la seguridad y eficiencia en la operación, consolidando así esta solución como una alternativa robusta y sostenible para el sector salud.

10. Recomendaciones

Capacitación y adopción de tecnologías: Se recomienda que las entidades del área de salud inviertan en la capacitación continua de su personal para asegurar un manejo adecuado de la infraestructura de nube comunitaria. Esto facilitará la adopción de herramientas open source y promoverá una cultura de innovación dentro de las organizaciones.

Desarrollo de políticas de autenticación robustas: Es crucial establecer políticas claras y efectivas para la autenticación de usuarios, garantizando que los mecanismos de acceso sean seguros y eficientes. Implementar autenticación multifactor puede ser una opción viable para aumentar la seguridad del sistema y proteger la información sensible.

Interoperabilidad y colaboración: Se sugiere fomentar la interoperabilidad entre los diferentes sistemas de información de salud mediante el uso de estándares abiertos. Esto facilitará el intercambio de datos entre las entidades y contribuirá a una atención médica más integrada.

Monitoreo y evaluación continua: Implementar un sistema de monitoreo para evaluar el rendimiento del prototipo y su impacto en las operaciones de salud permitirá identificar áreas de mejora y ajustes necesarios. Esta evaluación debe ser parte integral del ciclo de vida del proyecto, asegurando su adaptabilidad a las necesidades cambiantes de las entidades de salud en la región.

11. Referencias

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

Amazon Web Services. (2024). AWS Pricing Calculator. Recuperado el 26 de noviembre de 2024 de https://calculator.aws/#/

Amazon.com: Cisco Interruptor Catalyst 9300L-48P-4X-E : Electrónica. (2024). Retrieved November 29, 2024, from Amazon.com website: https://www.amazon.com/-/es/C9300L-48P-4X-Cisco-Interruptor-Catalyst-9300L-48P-4X-E/dp/B07WXS26T5?__mk_es_US=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=31YXMDW9N5GUZ&dib=eyJ2IjoiMSJ9.Cu75HVIMfGREKYb84hMXILeFlWVzjkvugjzvFrWdbADf_7koeg7MJurdBQPBLWcfAqbLTAS-Obkvb-dU2DojBRYZWFrLPjVawLAgESru8gsVmg8I6nsMqxetGCFdTKpVHmVc9yLIvCPQyjJej1Yd0g6yku9cBUbejQU8VaZ0lyewkhxE92h0RvsjmVRU1zWgmDCX9zKNd_tDx3Bp3c2QdCi8iTMDpkjovnCno-j0ew0.r5I4V8LmIcwAnd2_6DfMCL16LqyQDYImwHs5Y4JbT8s&dib_tag=se&keywords=cisco+catalyst+9300&qid=1732849792&sprefix=cisco+catalyst+9300%2Caps%2C237&sr=8-10

AT&T's Cloud Strategy has never been clearer. (s. f.-b). Recuperado de https://about.att.com/innovationblog/2019/08/cloud_strategy.html

Benson, T. (2012). Principles of Health Interoperability HL7 and SNOMED. Springer.

Buyya, R., Broberg, J., & Goscinski, A. M. (2011). Cloud Computing: Principles and Paradigms. Wiley.

Corbetta, P. (2007b). Metodología y técnicas de investigación social.

Dell Technologies. (2023). Dell PowerEdge R750 Rack Server. Recuperado de https://www.dell.com/en-us/work/shop/povw/poweredge-r750

Google Cloud. (2024). Google Cloud Pricing Calculator. Recuperado el 28 de noviembre de 2024 de https://cloud.google.com/products/calculator

Kavis, M. J. (2014). Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). Wiley.

Mandel, J. C., Kreda, D. A., Mandl, K. D., Kohane, I. S., & Ramoni, R. B. (2016). SMART on FHIR: a standards-based, interoperable apps platform for electronic health records. Journal of the American Medical Informatics Association, 23(5), 899-908.

Marinos, A., & Briscoe, G. (2009). Community cloud computing. En Proceedings of the 1st International Conference on Cloud Computing (pp. 472-484). Springer.

Mense, A., & Page, S. (2015). Data protection and privacy regulation for cloud computing in the healthcare sector. International Journal of Medical Informatics, 84(11), 889-900.

OpenStack Foundation. (s. f.). OpenStack Documentation. Recuperado de https://docs.openstack.org

OpenStack Releases: OpenStack Releases. (s. f.). Recuperado de https://releases.openstack.org

Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. En Proceedings of the 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 693-702). IEEE.

Rindfleisch, T. C. (1997). Privacy, information technology, and health care. Communications of the ACM, 40(8), 92-100.

Router Switch Limited. (2022). Precio NetApp FAS2700 - Lista de precios NetApp 2022. Retrieved November 29, 2024, from Itprice.com website: https://itprice.com/es/netapp-price-list/fas2700.html

Superuser. (2016, 5 de octubre). Inside WalmartLabs and its OpenStack core. Recuperado de ttps://superuser.openinfra.dev/articles/inside-walmartlabs-and-its-openstack-core/

Cloud Computing in Health Care. (s.f.). Recuperado de https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/cloud-ai-computing-healthcare.html

Now Open – AWS Germany (Frankfurt) Region – EC2, DynamoDB, S3, and Much More | Amazon Web Services. (s.f.). Recuperado de https://aws.amazon.com/blogs/aws/aws-region-germany/

Asamblea Legislativa de El Salvador. (2013). Ley de Protección de Datos Personales. Diario Oficial No. 123, Tomo 399. Recuperado de https://www.asamblea.gob.sv/leyes-y-decretos/ultimos-aprobados

U.S. Department of Health and Human Services. (1996). Health Insurance Portability and Accountability Act (HIPAA). Recuperado de https://www.hhs.gov/hipaa/

International Organization for Standardization. (2013). ISO/IEC 27001:2013 - Information Security Management Systems. ISO Standards. Recuperado de https://www.iso.org/standard/54534.html

12. Anexos

Anexo 1: Entrevista Semiestructurada

Universidad de El Salvador

Facultad de Ingeniería y Arquitectura.

Escuela de Ingeniería de Sistemas Informáticos.

Guía para entrevista

Dirigida a: Encargados de TI en hospitales, clínicas, y otras instituciones de salud.

I. **Objetivo:** Obtener información detallada sobre la infraestructura tecnológica actual, las preferencias y conocimientos en servicios de nube, y las percepciones sobre la implementación de una nube comunitaria en el sector salud en Centroamérica.

II. Preguntas

A. Experiencia y Responsabilidades en TI

1. ¿Cuáles son sus funciones en el área de TI y cuánto tiempo lleva desempeñando este rol en la organización?
2. ¿Cómo está compuesto el equipo de TI en el que se desempeña?

B. Infraestructura Tecnológica Actual

1. ¿Qué tipo de infraestructura tecnológica tienen actualmente para la gestión de EMR y otros datos de salud?
2. ¿Qué software de gestión hospitalaria utilizan y cómo se integra con sus EMR?
3. ¿Están utilizando servicios en la nube actualmente? Si es así, ¿cuáles son los servicios que más emplean?

C. Interoperabilidad y Gestión de Datos

1. ¿Cómo manejan la interoperabilidad entre diferentes sistemas de salud y entre distintas organizaciones?

2. ¿Cuáles han sido los mayores desafíos en este aspecto?

D. Opiniones sobre una Nube Comunitaria

1. ¿Ve factible la idea de implementar una nube comunitaria específica para el sector salud en Centroamérica?
2. De ser así ¿Cuáles cree que serían los principales beneficios para su institución y para la región al adoptar una solución de este tipo?

E. Capacidades y Necesidades del Personal

1. ¿Cree que su equipo de TI está preparado para implementar y mantener una solución de nube comunitaria?
2. ¿Qué tipo de capacitación o soporte adicional consideraría necesario?

F. Expectativas y Sugerencias

1. Si tuviera la oportunidad de implementar una solución en la nube que se ajuste a las necesidades de su organización, ¿cuáles serían las características esenciales que consideraría imprescindibles?
2. ¿Qué recomendaciones ofrecería para garantizar una implementación exitosa de una nube comunitaria en el sector salud?
3. ¿Estaría dispuesto a participar en estudios adicionales o proyectos piloto relacionados con la nube comunitaria para el sector salud?

Anexo 2: Encuesta

Universidad de El Salvador

Facultad de Ingeniería y Arquitectura.

Escuela de Ingeniería de Sistemas Informáticos.

Encuesta

Objetivo: El objetivo de esta encuesta es recolectar información cuantitativa de los jefes, encargados y coordinadores del área de TI en entidades hospitalarias sobre sus conocimientos, percepciones y expectativas relacionadas con el uso de soluciones de nube comunitaria en el sector salud.

Indicaciones: Encierre en un círculo la opción con la que más se identifique.

1. ¿Conoce usted qué es una nube comunitaria?

- Sí
- No

2. ¿Está familiarizado con el concepto de una solución de nube comunitaria para el sector salud?

- Sí
- No

3. ¿Considera que una nube comunitaria podría mejorar la eficiencia operativa de su institución?

- Sí
- No

4. En su opinión, ¿qué tan importante es la seguridad de los datos en la gestión de registros médicos electrónicos dentro de una nube comunitaria?

- Muy importante
- Importante

- Poco importante
- No es importante

5. ¿Qué nivel de confianza tendría en una solución en la nube para proteger la información de los pacientes?

- Alta confianza
- Confianza moderada
- Baja confianza
- Ninguna confianza

6. ¿Piensa que una nube comunitaria puede facilitar el cumplimiento de las normativas en el manejo de datos de salud?

- Sí
- No

7. ¿Qué beneficio considera más relevante en una solución de nube comunitaria para su institución?

- Seguridad en el manejo de datos
- Escalabilidad de la infraestructura
- Reducción de costos operativos
- Mejora en la eficiencia de procesos

8. ¿Cómo calificaría la importancia de la escalabilidad en una solución de nube para su institución?

- Muy importante
- Importante
- Poco importante
- No es importante

9. ¿Consideraría migrar los registros médicos electrónicos de su institución a una nube comunitaria?

- Sí
- No

10. ¿Qué tan preocupado estaría por la velocidad de acceso a los datos al usar una nube comunitaria?

- Muy preocupado
- Moderadamente preocupado
- Poco preocupado
- No estaría preocupado

11. ¿Cree que una nube comunitaria podría mejorar la capacidad de respuesta de su infraestructura TI ante demandas crecientes?

- Sí
- No

12. ¿Qué tanto valoraría la capacidad de colaboración entre diferentes entidades hospitalarias a través de una nube comunitaria?

- Muy valioso
- Valioso
- Poco valioso
- No valioso

13. ¿Qué barrera considera más significativa para el uso de una nube comunitaria en su institución?

- Falta de recursos económicos
- Resistencia al cambio

- Dudas sobre la seguridad
- Complejidad técnica

14. ¿Qué tan probable es que recomendaría el uso de una nube comunitaria a otras instituciones hospitalarias?

- Muy probable
- Probable
- Poco probable
- Nada probable

15. ¿Cuánto cree que una solución de nube comunitaria podría ayudar a reducir los tiempos de inactividad en su infraestructura TI?

- Mucho
- Moderadamente
- Poco
- No ayudaría

16. ¿Considera que una solución de nube comunitaria podría reducir los costos relacionados con la infraestructura TI en su institución?

- Sí
- No

17. ¿Qué tan importante es para usted el soporte técnico continuo en el uso de una solución de nube comunitaria?

- Muy importante
- Importante
- Poco importante
- No es importante

18. ¿Qué aspecto de una solución de nube comunitaria considera más crucial para la toma de decisiones en su institución?

- Seguridad
- Costo
- Facilidad de uso
- Soporte técnico

19. ¿Está de acuerdo con que una nube comunitaria podría ofrecer una mayor flexibilidad en la gestión de recursos TI?

- Totalmente de acuerdo
- De acuerdo
- En desacuerdo
- Totalmente en desacuerdo

20. ¿Qué nivel de adopción de soluciones en la nube tiene actualmente su institución?

- Totalmente en la nube
- Parcialmente en la nube
- Explorando opciones
- No usamos soluciones en la nube

Transcripción entrevista a Jefe Aplicacionista de Grupo RAF: Ing. Oscar Armando Vela Benavides

Realizada el: Míercoles 25 septiembre de 2024 a las 15:30

Duración: 30:00 minutos

Lugar: Sala de videoconferencias Google Meet

Funciones en el área de TI y tiempo en el rol

Oscar: Bueno, básicamente me encargo de gestionar el equipo de TI que da mantenimiento a los servidores locales y equipos biomedicos en diversos hospitales, en estos servidores guardamos y manejamos toda la info médica, como los expedientes electrónicos, imágenes de rayos X y tomografías, y los historiales clínicos. También me toca resolver los problemas técnicos que puedan afectar el funcionamiento de varios sistemas en varios hospitales.

Ya llevo 5 años en esto, así que me ha tocado aprender bastante sobre cómo manejar la infraestructura tecnológica en salud. Te hacés maña con las limitaciones y todo eso.

Composición del equipo de TI

Oscar: Somos un equipo de 5 en TI. Cada quien tiene su área, pero al final todos hacemos de todo: mantener los servidores, dar soporte a los usuarios (médicos, administrativos) y manejar la red. El problema es que, como casi siempre hay pocos recursos y los trámites son lentos, a veces nos toca hacer magia con lo que tenemos a mano.

Tipo de infraestructura tecnológica para la gestión de EMR y otros datos de salud

Oscar: Lo que tenemos es una infraestructura local con servidores físicos, que son buenos, pero ya se sienten un poco viejos. Ahí guardamos los expedientes electrónicos y las imágenes médicas. Cada servidor lo configuramos manualmente, a la antigua. Así que toca estar pendiente de todo el tiempo para que el almacenamiento y el procesamiento sean los

adecuados. De hecho hace poco tuvimos un problema por falta de espacio y nos tocó hacer magia para poder incrementar el espacio.

Software de gestión hospitalaria e integración con EMR

Oscar: Usamos un software privativo que está hecho para hospitales públicos. Nos sirve para gestionar citas, historiales médicos y cosas administrativas de los hospitales, pero no está bien integrado con los EMR. Esto hace que a veces sea un poco lento acceder a la información.

Uso actual de servicios en la nube

Oscar: Por ahora, todo lo manejamos localmente en los servidores. Hemos considerado la nube para respaldos, pero los trámites son una odisea, no hemos podido avanzar en esa dirección.

Manejo de interoperabilidad entre sistemas de salud

Oscar: Este es un relajo. Cada hospital o centro de salud tiene un sistema diferente, y eso complica el intercambio de información. Muchas veces nos toca exportar los datos a mano o usar formatos que no son muy eficientes para compartir información con otros hospitales.

Mayores desafíos en la interoperabilidad

Oscar: Yo creo que lo más complicado es que no hay estándares comunes para compartir datos. Los sistemas no son compatibles entre sí, y por esto mismo siempre hay preocupación por la seguridad y privacidad cuando se comparte info.

Factibilidad de implementar una nube comunitaria para el sector salud en Centroamérica

Oscar: Creo que una nube es buena idea para el sector salud, pero no va a ser fácil. Hay varios desafíos, sobre todo con la aceptación de las instituciones públicas y la burocracia

interna. Aun así, si se logra implementar, facilita el acceso a los expedientes y haría más ágil el intercambio de información entre hospitales, que hoy por hoy es una de las cosas a las que nos dedicamos acá en RAF.

Beneficios para la institución y la región

Oscar: Desde mi punto de vista creo que lo más importante es optimizar el trabajo médico, teniendo acceso rápido a la información de los pacientes. Por supuesto que reducir los costos operativos, ya que no dependeríamos tanto de la infraestructura física local y creo que tendríamos mayor seguridad y respaldo de los datos..

Preparación del equipo para implementar una nube comunitaria

Oscar: Tenemos experiencia en gestionar servidores locales, pero no estamos del todo preparados para manejar algo en la nube. Nos falta capacitación y recursos, pero con el entrenamiento adecuado, creo que podríamos adaptarnos.

Capacitación o soporte adicional necesario

Oscar: Necesitaríamos entrenamiento en administración y seguridad en la nube. También sería clave tener soporte técnico para la migración de los datos y asegurarnos de que no haya interrupciones en los servicios durante la transición, eso creo que es un tema delicado, por eso lo veo difícil, pero no imposible.

Características esenciales para una solución en la nube

Oscar: Quiza lo más importante es que sea compatible con los sistemas que ya usamos en el hospital. Tener acceso rápido a los expedientes médicos desde cualquier lugar y por supuesto, es indispensable escalabilidad para aumentar la capacidad de almacenamiento según se necesite.

Recomendaciones para una implementación exitosa

Oscar: Creo que yo les recomendaría involucrar a no solo hospitales privados, sino también a los públicos en la planificación del proyecto. Hacer pruebas piloto antes de implementarlo a gran escala y asegurar que haya capacitación continua para el equipo de TI.

Participación en estudios adicionales o proyectos piloto:

Oscar: Sí definitivamente me animaría a participar en proyectos piloto o estudios relacionados con la nube comunitaria. Es una buena oportunidad para modernizar los servicios de salud y mejorar la calidad de la atención médica en toda la región.

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DOCUMENTO DE DISEÑO DE ALTO NIVEL

HIGH LEVEL DESIGN DOCUMENT

DESPLIEGUE DE UNA NUBE COMUNITARIA PARA EL SECTOR SALUD EN CENTROAMÉRICA: VIABILIDAD DE UNA INFRAESTRUCTURA DE NUBE BASADA EN OPEN SOURCE PARA REGISTROS MÉDICOS Y SERVICIOS DE SALUD.

OCTUBRE 2024

VERSIÓN 1.0

20 de Octubre de 2024

Índice

Introducción

En este documento se describe el diseño del prototipo de infraestructura de nube comunitaria multirregional, orientada a proporcionar servicios esenciales para instituciones de salud a un nivel regional. La infraestructura conecta múltiples regiones geográficamente distribuidas, permitiendo a diversas instituciones compartir recursos y beneficiarse de los servicios centrales que ofrece este tipo de infraestructura, garantizando un acceso seguro y eficiente a los datos.

El prototipo se basa en la plataforma de código abierto OpenStack, y aprovecha componentes clave como Keystone, para la autenticación y gestión de usuarios federados, y Horizon, como la interfaz web para la administración de la infraestructura. Además, se incorpora Ceph para ofrecer almacenamiento escalable y flexible, abarcando almacenamiento en bloque, objetos y archivos, lo que permite satisfacer las diversas necesidades de manejo de datos de las entidades de salud.

En este documento, se presenta una visión de alto nivel del diseño del sistema, destacando los aspectos fundamentales de la solución. Posteriormente, en otro documento, se incluirán detalles técnicos y una guía práctica para implementar el prototipo, siguiendo un enfoque paso a paso que permitirá replicar la infraestructura propuesta.

Objetivos

- Proporcionar una visión general de la infraestructura de nube comunitaria multirregional diseñada.
- Describir de manera general los componentes del sistema, tomando en cuenta los servicios de autenticación, almacenamiento y administración, explicando cómo se integran para ofrecer una solución integral y escalable.
- Presentar la arquitectura de alto nivel del prototipo, detallando los componentes principales y proporcionando una visión de la topología de red empleada para conectar las diferentes regiones.

Audiencia Objetivo

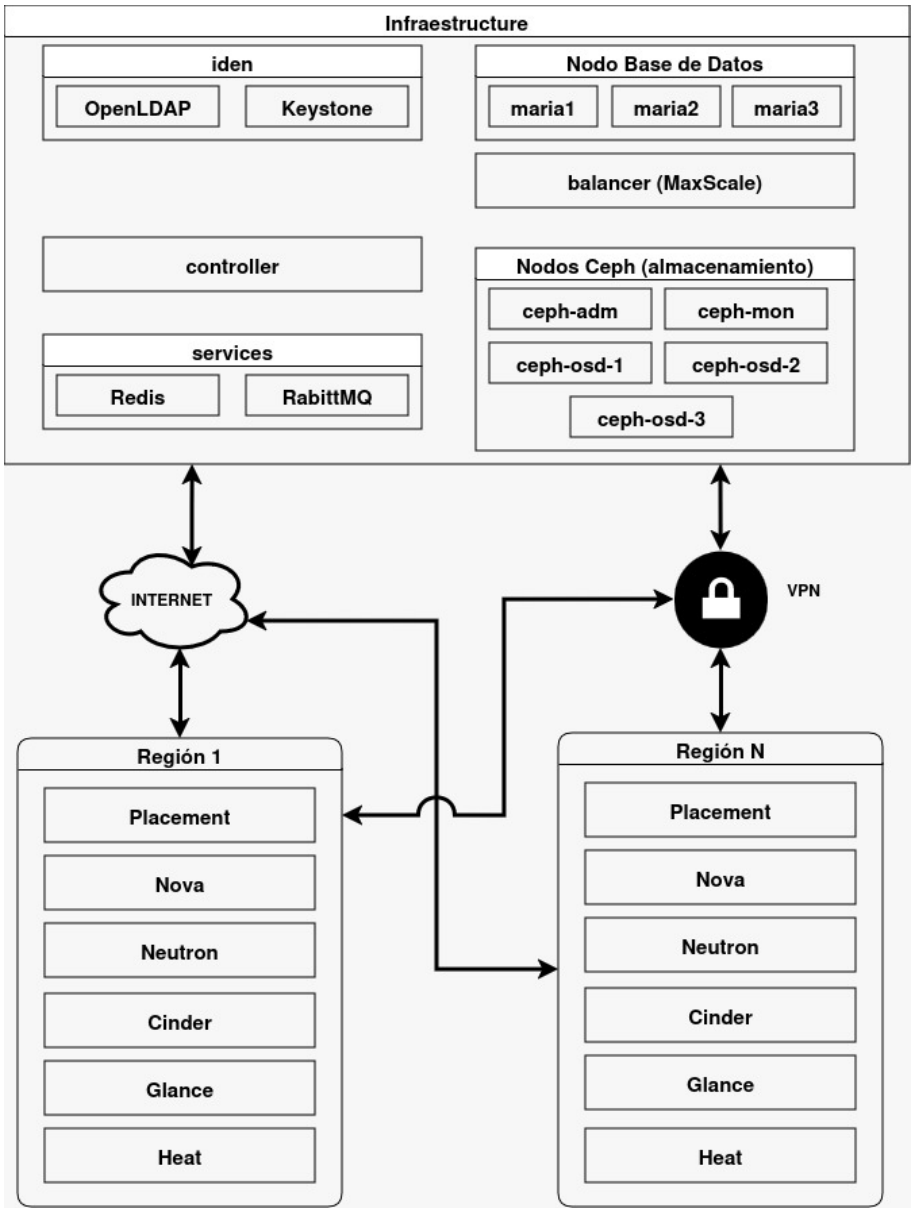
El informe está orientado a una audiencia que abarca tanto perfiles ejecutivos y técnicos:

- Ejecutivos y directivos de entidades de la salud que requieren comprender la relevancia estratégica y las ventajas operativas de una infraestructura en la nube multirregional.
- Arquitectos de soluciones y asesores que deseen examinar los elementos esenciales del diseño y aportar sugerencias acerca de la arquitectura y la puesta en marcha del sistema.
- Directores de proyectos que participan en la organización y realización de infraestructuras de nube, buscando entender los propósitos y la magnitud del proyecto.
- Equipos de Tecnología de la Información y personal operativo encargados de la gestión, conservación y perfeccionamiento constante de infraestructuras en la nube, ya sean mixtas, públicas o privadas.

Este documento proporciona una visión de gran alcance, enfocada en brindar un entendimiento global de la solución. Los pormenores técnicos particulares se detallarán en un informe de diseño de nivel inferior complementario.

Arquitectura

Se describen los servicios que son utilizados por las múltiples regiones conectadas, ofreciendo una base sólida y escalable para soportar las operaciones en la nube.



Componentes Infraestructura

- **Keystone**: Proporciona servicios de autenticación y autorización en la nube. Actúa como el sistema de identidad central, facilitando el acceso seguro a los servicios distribuidos en todas las regiones.
- **OpenLDAP**: Funciona como servicio de directorio, gestionando información de usuarios y grupos. Junto con Keystone valida credenciales y se gestiona la autenticación.
- **Bind9 (DNS)**: Servicio de DNS de la infraestructura, facilita resolución de nombres de dominio para las conexiones y el acceso a los servicios.
- **RabbitMQ**: Actúa como sistema de mensajería que coordina comunicaciones entre los servicios de OpenStack. Permite separar y organizar mensajes entre las distintas regiones.
- **Redis**: Proporciona almacenamiento de caché para datos efímeros, mejorando el rendimiento al reducir el tiempo de acceso a la información almacenada temporalmente.
- **Clúster de Base de Datos**: Compuesto por servidores MariaDB, este clúster asegura la alta disponibilidad y la sincronización de datos. MaxScale actúa como un balanceador de carga para distribuir el tráfico de consultas de manera eficiente.
- **Clúster de Ceph**: Proporciona almacenamiento distribuido, tanto en bloques como en objetos y archivos. Los nodos de administración y monitoreo gestionan el clúster, mientras que los nodos OSD se encargan del almacenamiento y la replicación de los datos.
- **Heat**: Componente de orquestación de OpenStack que facilita la automatización de la provisión, gestión y eliminación de recursos mediante plantillas. A través de la creación de "pilas" de recursos, Heat permite la implementación, actualización y eliminación automatizada de recursos de cómputo, almacenamiento y red. Facilita la gestión de la infraestructura como código, mejorando la eficiencia, reduciendo el

riesgo de errores humanos y permitiendo una mayor escalabilidad de los servicios en la nube.

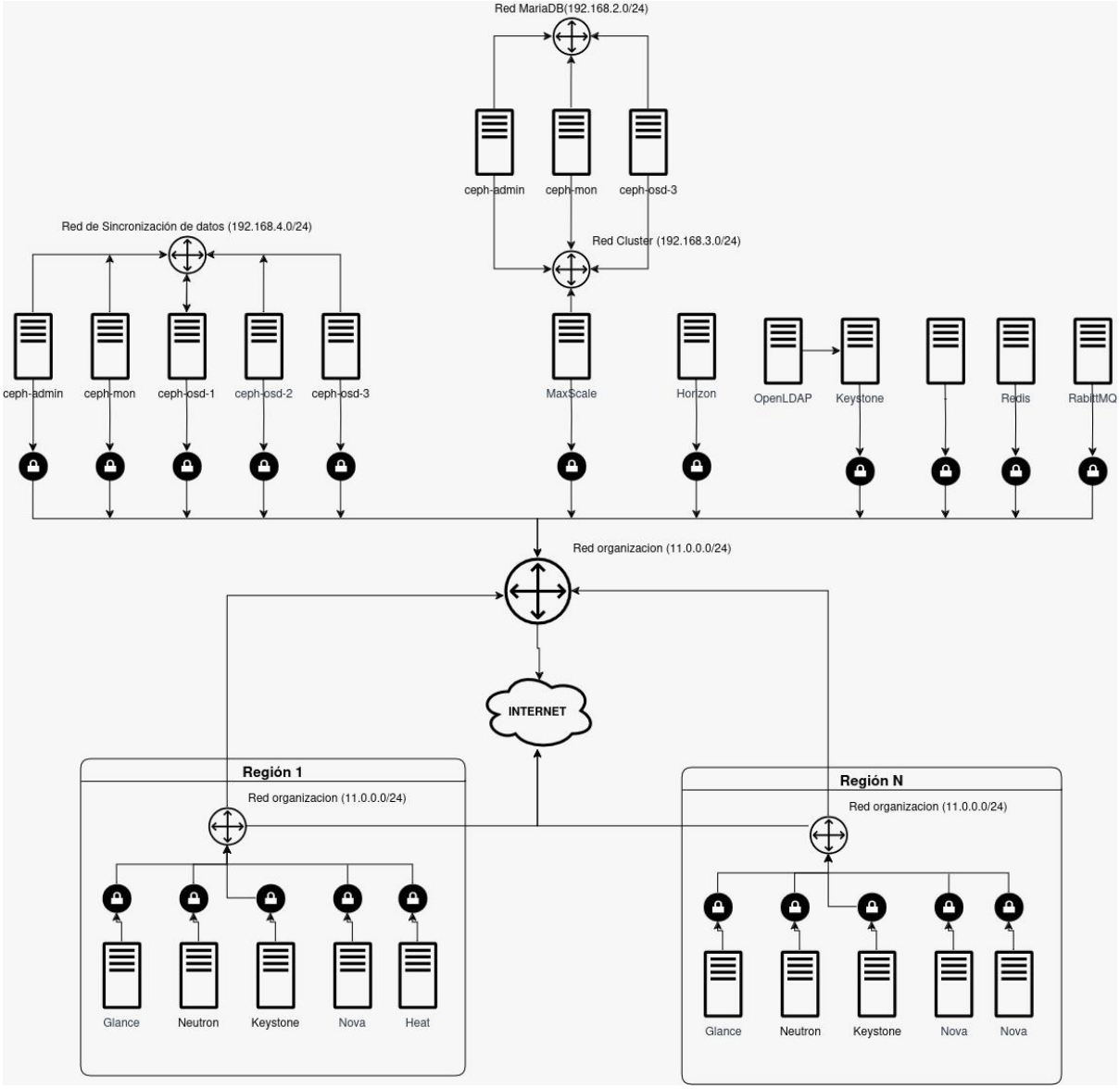
Componentes regiones

- **Nova**: Gestiona recursos de cómputo, máquinas virtuales y contenedores.
- **Neutron**: Gestiona las redes definidas, proporcionando redes como servicio para entornos de virtualización.
- **Cinder**: Administra almacenamiento en bloques, permitiendo la creación y gestión de volúmenes de almacenamiento persistente, y puede integrarse con Ceph para aprovechar su capacidad de almacenamiento distribuido.
- **Swift**: Ofrece almacenamiento de objetos, lo que permite la gestión y el almacenamiento escalable de datos no estructurados. También puede aprovechar los recursos de Ceph para el almacenamiento distribuido.
- **Glance**: Es el servicio de gestión de imágenes de máquinas virtuales, utilizado para registrar, almacenar y recuperar las imágenes de sistemas operativos.
- **Placement**: Realiza un seguimiento de los recursos disponibles y en uso, permitiendo una gestión eficiente de la capacidad de cómputo y almacenamiento en la nube.

Conectividad y Seguridad

- **Internet**: Permite el acceso global a servicios públicos como paneles de administración y proporciona conexiones para el acceso remoto.
- **VPN**: La Red Privada Virtual garantiza la comunicación segura y privada entre las regiones, protegiendo la transferencia de datos en el entorno de la nube.

Topología de Red



La infraestructura está organizada en varias redes y segmentos, cada uno destinado a funciones específicas para garantizar la eficiencia y la seguridad en la comunicación entre los componentes.

- **Red de Sincronización de Datos (192.168.4.0/24)**: Conecta nodos del clúster Ceph, incluyendo los nodos OSD, de administración y monitoreo. Se utiliza para sincronizar datos entre los nodos OSD, garantizando la redundancia y la alta disponibilidad del almacenamiento. La red también permite el acceso a los servicios

de almacenamiento a través de la VPN para que las regiones puedan consumir estos servicios.

- **Red del Clúster de Ceph (192.168.3.0/24)**: Es la red dedicada para las operaciones internas del clúster de Ceph, utilizada para la comunicación entre los nodos de almacenamiento y los servicios de administración.
- **Red del Clúster de Bases de Datos (192.168.2.0/24)**: Conecta los servidores MariaDB del clúster para la sincronización de datos.
- **Red de la Organización (11.0.0.0/24)**: Esta red actúa como la columna vertebral que conecta todos los servidores de la infraestructura, permitiendo el acceso a servicios internos y la comunicación con servicios externos a través de Internet. Es la red principal utilizada para la administración y para el tráfico general entre los componentes del sistema.
- **Internet**: Proporciona acceso a servicios públicos y permite la conectividad externa para los usuarios y administradores. Sirve como medio para que los usuarios accedan a los servicios web, como el panel de administración (Horizon).
- **VPN (Red Privada Virtual)**: Es el enlace seguro que conecta las regiones con la infraestructura principal, garantizando una comunicación protegida para el consumo de servicios fundamentales. A través de la VPN, los servicios críticos como la autenticación, almacenamiento y bases de datos son accesibles de forma segura desde cada región.

Conectividad de las Regiones

Cada región, como Región 1 y Región N en el esquema, está conectada a la red principal y accede a la infraestructura a través de la VPN. Cada una tiene servicios locales como Nova, Neutron, Glance y Keystone para proporcionar computación, redes, almacenamiento y autenticación en la nube. Estas regiones dependen de los servicios centrales para la autenticación y otros servicios clave, pero operan de manera semiautónoma.

Caso de Estudio

Este caso de estudio analiza la viabilidad de utilizar la infraestructura de nube comunitaria multiregional basada en OpenStack para alojar sistemas de gestión de registros médicos electrónicos (EMR), tomando como referencia las necesidades de OpenEMR. El enfoque del análisis se centra en validar que esta infraestructura pueda ofrecer un entorno seguro, eficiente y escalable para implementar soluciones de este tipo en instituciones de salud, permitiendo gestionar recursos y datos de manera colaborativa y optimizada. La arquitectura propuesta responde a los desafíos del sector al ofrecer soporte para la infraestructura necesaria, utilizando Ubuntu como sistema operativo, con opciones de despliegue de servicios críticos mediante el stack LAMP o Nginx para optimizar la gestión y el rendimiento.

La infraestructura plantea la posibilidad de que cada región, como en el caso de El Salvador, aloje múltiples instancias de OpenEMR, permitiendo a diferentes instituciones de salud operar sus sistemas de forma autónoma. Esta distribución garantiza que las cargas de trabajo se administren de manera eficiente entre los distintos nodos Compute de la región, aprovechando el balanceo de carga para evitar saturaciones y mantener un desempeño constante. El entorno distribuido asegura que las instituciones participantes puedan acceder a sus sistemas sin interrupciones, incluso ante altas demandas de recursos o fallos en algún nodo, gracias a la redundancia incorporada en la arquitectura.

El uso de un clúster de bases de datos distribuido con MariaDB permite gestionar la información de forma centralizada, manteniendo la seguridad, integridad y disponibilidad de los datos en todo momento. Esta configuración asegura que los registros médicos electrónicos puedan mantenerse sincronizados y accesibles para los profesionales de salud en tiempo real. De esta forma, el sistema permite operar de manera eficiente y garantiza la continuidad del servicio, aspectos esenciales para la gestión de información médica crítica. El diseño asegura también la posibilidad de expandirse sin comprometer el rendimiento, permitiendo añadir nuevas instituciones o regiones a medida que crezca la demanda.

La seguridad es un aspecto clave en esta infraestructura, y el uso de Keystone como sistema de autenticación centralizada permite gestionar de manera controlada los accesos a cada instancia de OpenEMR. Esto garantiza que únicamente el personal autorizado tenga acceso a los registros clínicos, manteniendo la confidencialidad de la información. La conexión entre las distintas regiones e instituciones se realiza a través de una VPN segura, lo que refuerza la privacidad y estabilidad de las comunicaciones, facilitando la colaboración eficiente entre las entidades de salud.

El análisis de este caso de estudio evidencia que la infraestructura de nube comunitaria multiregional diseñada no solo es compatible con sistemas como OpenEMR, sino que también ofrece las condiciones necesarias para que estos sistemas operen de forma óptima. La flexibilidad del diseño permite una gestión eficiente de recursos y facilita la adaptación a futuras necesidades del sector salud, promoviendo un entorno colaborativo que mejora la calidad del servicio mediante la gestión eficaz de la información clínica.

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DOCUMENTO DE DISEÑO DE BAJO NIVEL

LOW LEVEL DESIGN DOCUMENT

DESPLIEGUE DE UNA NUBE COMUNITARIA PARA EL SECTOR SALUD EN CENTROAMÉRICA: VIABILIDAD DE UNA INFRAESTRUCTURA DE NUBE BASADA EN OPEN SOURCE PARA REGISTROS MÉDICOS Y SERVICIOS DE SALUD.

OCTUBRE 2024

VERSIÓN 1.0

20 de Octubre de 2024

Índice

Introducción

En este documento de Diseño de Bajo Nivel (LLD) se complementa el Diseño de Alto Nivel (HLD) presentado anteriormente, proporcionando un enfoque técnico más detallado del prototipo de nube comunitaria multirregional. Se especifican los aspectos prácticos de la implementación, con instrucciones detalladas sobre configuraciones necesarias, pasos de instalación, y pruebas para asegurar que cada componente funcione correctamente. El objetivo es ofrecer una guía técnica clara para llevar a cabo la instalación y configuración del sistema según lo planteado en el HLD.

Objetivos

- Brindar una guía detallada para la implementación de la infraestructura de nube comunitaria según los lineamientos establecidos en el HLD.
- Especificar configuraciones internas, ajustes y estructuras de archivo requeridos para cada componente del sistema, incluyendo redes, almacenamiento y autenticación.
- Proporcionar instrucciones paso a paso para la integración y conexión de los diferentes servicios y regiones del sistema.

Audiencia Objetivo

- **Profesionales de TI y Operaciones** encargados de la implementación y mantenimiento de infraestructuras en la nube, ya sea en entornos híbridos, públicos o privados.
- **Administradores de Sistemas y Especialistas en DevOps** que participen en la configuración y despliegue de tecnologías de nube como OpenStack.
- **Arquitectos de Soluciones en la Nube** que necesiten profundizar en la configuración técnica y los pasos necesarios para implementar una nube distribuida multirregional.

Configuraciones Generales

VirtManager

Antes de comenzar, es recomendable actualizar la lista de paquetes para asegurar que se está instalando las versión más recientes

```
sudo apt update
sudo apt upgrade -y
```

Instalar VirtManager

```
sudo apt install virt-manager qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils -y
```

Verificar la instalación de KVM

```
egrep -c '(vmx|svm)' /proc/cpuinfo
```

Si el resultado es mayor a cero, significa que el procesador soporta virtualización.

Agregar usuario al grupo libvirt

```
sudo usermod -aG libvirt $(whoami)
```

Habilitar y arrancar el servicio de libvirtd

```
sudo systemctl enable libvirtd
sudo systemctl start libvirtd
```

Configuración de archivo /etc/hosts

Se agregaron entradas para el controlador y los nodos de cómputo con sus respectivas direcciones IP. El siguiente es un ejemplo de uno de los archivos de hosts

```
10.0.0.11       controller

10.0.0.31       compute1
10.0.0.32       compute2

192.168.122.52  backend-1
192.168.122.53  backend-2
```

```
192.168.122.54  backend-3

192.168.3.50  balanceador-1
192.168.3.51  balanceador-2

192.168.3.55  redis-1
192.168.3.56  redis-2

192.168.4.52  db-node-1
192.168.4.53  db-node-2
192.168.4.54  db-node-3

192.168.4.51 maxscale

192.168.3.52  ceph-node-1
192.168.3.53  ceph-node-2
192.168.3.54  ceph-node-3

192.168.3.60  ceph-mon
192.168.3.61  ceph-admin
```

Configuración del nombre de host

Para cada una de las máquinas virtuales, se estableció el nombre del nodo controlador con hostnamectl y se reinició la sesión para aplicar los cambios.

```
sudo hostnamectl set-hostname controller
exec bash
```

VPN (Tailscale)

Es una solución de red privada virtual (VPN) que utiliza el protocolo WireGuard para establecer conexiones seguras entre dispositivos en una red privada. En cada una de las máquinas virtuales, se hizo instalación de la aplicación.

```
curl -fsSL https://tailscale.com/install.sh | sh
```

El siguiente comando abre un enlace en un navegador para iniciar sesión en Tailscale y autorizar el dispositivo. Después de esto, el nodo conecta a la red Tailscale.

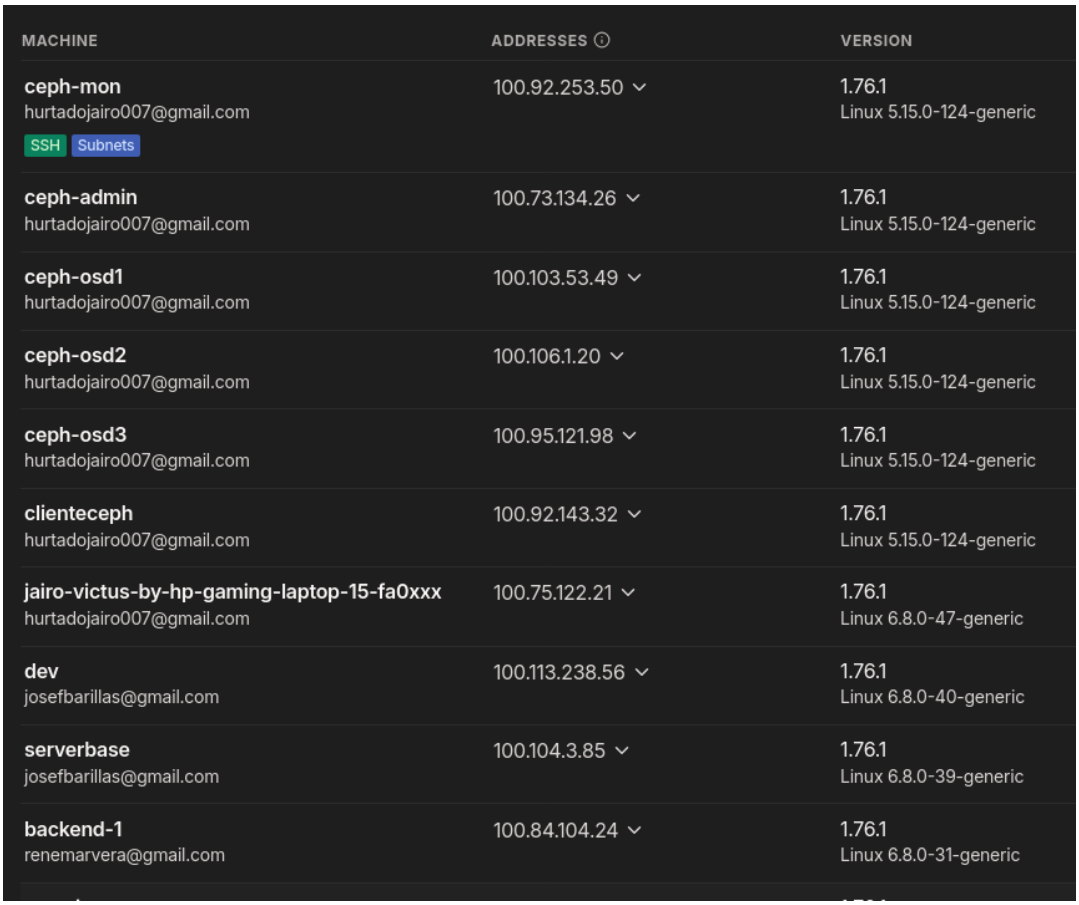
```
sudo tailscale up
```

Una vez autorizado, es necesario hacer que Tailscale actúe como un enrutador para la red que deseamos trabajar, 192.168.5.0/24, haciendo que el tráfico hacia esa red sea accesible a otros dispositivos conectados a Tailscale.

```
sudo tailscale up --advertise-routes=192.168.5.0/24
```

Con esto, le indicamos a los equipos que el nodo de Tailscale anunciará la ruta para la red 192.168.5.0/24 a otros dispositivos en la red de Tailscale. Significa que el tráfico dirigido a la red 192.168.5.0/24 puede ser enrutado a través de este nodo.

Una vez hechas estas configuraciones, podemos acceder al dashboard de Tailscale para gestionar las máquinas virtuales conectadas a la red.



MACHINE	ADDRESSES	VERSION
ceph-mon hurtadojairo007@gmail.com SSH Subnets	100.92.253.50	1.76.1 Linux 5.15.0-124-generic
ceph-admin hurtadojairo007@gmail.com	100.73.134.26	1.76.1 Linux 5.15.0-124-generic
ceph-osd1 hurtadojairo007@gmail.com	100.103.53.49	1.76.1 Linux 5.15.0-124-generic
ceph-osd2 hurtadojairo007@gmail.com	100.106.1.20	1.76.1 Linux 5.15.0-124-generic
ceph-osd3 hurtadojairo007@gmail.com	100.95.121.98	1.76.1 Linux 5.15.0-124-generic
clienteceph hurtadojairo007@gmail.com	100.92.143.32	1.76.1 Linux 5.15.0-124-generic
jairo-victus-by-hp-gaming-laptop-15-fa0xxx hurtadojairo007@gmail.com	100.75.122.21	1.76.1 Linux 6.8.0-47-generic
dev josefbarillas@gmail.com	100.113.238.56	1.76.1 Linux 6.8.0-40-generic
serverbase josefbarillas@gmail.com	100.104.3.85	1.76.1 Linux 6.8.0-39-generic
backend-1 renemarvera@gmail.com	100.84.104.24	1.76.1 Linux 6.8.0-31-generic

Instalación y configuración de Chrony

Se instaló el servicio Chrony para la sincronización de la hora y se configuró para permitir conexiones desde la red local.

```
sudo apt install chrony openssh-server curl -y
sudo systemctl enable --now chrony
```

Todas las máquinas virtuales toman como servidor de referencia al nodo controlador, entonces es este el que se encarga de sincronizar los horarios.

En el nodo controlador, la configuración del archivo /etc/chrony/chrony.conf:

```
server ntp.ues.edu.sv iburst
allow 10.0.0.0/24
```

Mientras que en los demas nodos, la configuracion solamente apunta a este servidor.

```
server controller iburst
```

Configuración de red con Netplan

Para cada una de las máquina virtuales, se realiza la respectiva configuración de red, se configuró el archivo 50-cloud-init.yaml para ajustar la red, creando una interfaz de puente (ovs-internal) y especificando las direcciones IP, la puerta de enlace y los servidores de nombres.

```
network:
  ethernets:
        enp1s0:
        dhcp4: false
        enp7s0:
        dhcp4: false
        addresses: [10.0.0.32/24]
  bridges:
        ovs-internal:
        interfaces: [enp1s0]
        dhcp4: false
        addresses: [192.168.122.32/24]
        gateway4: 192.168.122.1
        nameservers:
        addresses: [8.8.8.8, 8.8.4.4]

  version: 2
```

Se aplicaron los cambios con netplan apply.

```
sudo netplan apply
```

Configuraciones de Componentes

Configuraciones de Ceph

Docker

Agregamos el repositorio de Docker para instalarlo

```
apt install apt-transport-https ca-certificates curl gnupg-agent software-properties-common -y
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
echo "deb [arch=amd64] https://download.docker.com/linux/ubuntu $(lsb_release -sc) stable" | sudo tee /etc/apt/sources.list.d/docker-ce.list
```

Instalación de Docker y habilitación

```
apt update
apt install docker-ce docker-ce-cli containerd.io -y
systemctl enable --now docker
```

Nodo Administrador

Creamos un usuario para la administración de Ceph

```
useradd -m -s /bin/bash cephadmin
passwd cephadmin
echo "cephadmin ALL=(ALL:ALL) NOPASSWD:ALL" >> /etc/sudoers.d/cephadmin
chmod 0440 /etc/sudoers.d/cephadmin
```

Permitimos acceso remoto a usuario root a traves de SSH, configuramos el archivo /etc/ssh/sshd_config

```
PermitRootLogin yes
```

Descarga de cephadm y hacerlo ejecutable:

```
wget -q https://github.com/ceph/ceph/raw/quincy/src/cephadm/cephadm -P /usr/bin/
chmod +x /usr/bin/cephadm
```

Inicia el cluster de Ceph utilizando cephadm

```
sudo cephadm bootstrap --cluster-network 192.168.3.0/24 --mon-ip 192.168.122.161
```

Una vez completado el bootstrap, se proporcionará una URL para acceder al dashboard de Ceph, en nuestro caso https://ceph-admin:8443

Nodos OSD

Copiamos la clave pública de SSH a los nodos de Ceph para permitir el acceso

```
for i in ceph-node-1 ceph-node-2 ceph-node-3; do sudo ssh-copy-id -f -i
/etc/ceph/ceph.pub root@$i; done
```

Añadir los nodos al clúster

```
sudo ceph orch host add ceph-node-1
sudo ceph orch host add ceph-node-2
sudo ceph orch host add ceph-node-3
```

Etiquetamos los nodos para que sean utilizados como OSD

```
for i in ceph-node-1 ceph-node-2 ceph-node-3; do sudo ceph orch host label add $i osd;
done
```

Crear un grupo de volúmenes y un volumen lógico en cada nodo

```
vgcreate vg01 /dev/vdb
lvcreate -L 19G -n lv01 vg01
```

Añadir los volúmenes como OSD en el clúster de Ceph

```
sudo ceph orch daemon add osd ceph-node-1:vg01/lv01
sudo ceph orch daemon add osd ceph-node-2:vg01/lv01
sudo ceph orch daemon add osd ceph-node-3:vg01/lv01
```

En este punto, podemos hacer montajes de almacenamiento Ceph, para ello montamos el sistema de archivos Ceph en un directorio local

```
mount -t ceph 192.168.122.41:6789:/ /mnt/cloud/ -o name=admin,secret=[clave_secreta]
```

Y con esto, podemos consumir el almacenamiento montado desde diferentes aplicaciones.

Instalación de MariaDB

Actualización del sistema e instalación de MariaDB con soporte para Python (python3-pymysql).

```
sudo apt install mariadb-server python3-pymysql
```

Configuración de MariaDB para enlazarse a la IP del controlador y ajustar opciones como el motor de almacenamiento y la configuración de conexiones. La siguiente es la configuración del archivo 99-openstack.cnf.

```
[mysqld]
bind-address = 10.0.0.11

default-storage-engine = innodb
innodb_file_per_table = on
max_connections = 4096
collation-server = utf8_general_ci
character-set-server = utf8
```

Reiniciamos el servicio

```
sudo service mysql restart
```

Configuración de MaxScale con MariaDB/Galera

Para el nodo de MaxScale, descargar el paquete.

```
wget
https://dlm.mariadb.com/3776522/MaxScale/24.02.1/packages/ubuntu/jammy/x86_64/maxscale_24.02.1~jammy-1_amd64.deb
```

Instalamos dependencias requeridas

```
sudo apt install libodbc2
```

```
sudo dpkg -i libicu70_70.1-2_amd64.deb
```

Instalación de MaxScale

```
sudo dpkg -i maxscale_24.02.1~jammy-1_amd64.deb
```

Configuramos el archivo /etc/maxscale.cnf para agregar los nodos de las bases de datos

```
[db-node-1]
type=server
address=192.168.4.52
port=3306
protocol=MariaDBBackend

[db-node-2]
type=server
address=192.168.4.53
port=3306
protocol=MariaDBBackend

[db-node-3]
type=server
address=192.168.4.54
port=3306
protocol=MariaDBBackend
```

Reiniciamos el servicio de MaxScale

```
sudo systemctl restart maxscale
```

Nodos MariaDB

En cada uno de los nodos editar archivo de configuración en /etc/mysql/conf.d/mariadb.cnf

```
[mysqld]
query_cache_size=0
binlog_format=ROW
default-storage-engine=innodb
innodb_autoinc_lock_mode=2
query_cache_type=0
bind-address=0.0.0.0

# Configuración del Proveedor Galera
wsrep_on=ON
wsrep_provider=/usr/lib/galera/libgalera_smm.so
```

```
# Configuración del Clúster Galera
wsrep_cluster_name="ClusterMaria"
wsrep_cluster_address="gcomm://db-node-1,db-node-2,db-node-3"

# Configuración de Sincronización
wsrep_sst_method=rsync

# Configuración del Nodo Galera
wsrep_node_address="192.168.4.52"  # Cambiar según el nodo
wsrep_node_name="db-node-1"       # Cambiar según el nodo
```

Detener el servicio MariaDB y arranca el clúster en el primer nodo

```
sudo service mariadb stop
sudo galera_new_cluster
```

Configuración de Usuarios en MariaDB para MaxScale

Dentro de MySQL, crea el usuario de MaxScale y conceder los permisos necesarios

```
CREATE USER 'maxscale'@'%' IDENTIFIED BY 'icc115';
GRANT SELECT ON mysql.user TO 'maxscale'@'%';
GRANT SELECT ON mysql.db TO 'maxscale'@'%';
GRANT SELECT ON mysql.tables_priv TO 'maxscale'@'%';
GRANT SELECT ON mysql.columns_priv TO 'maxscale'@'%';
GRANT SELECT ON mysql.proxies_priv TO 'maxscale'@'%';
GRANT SELECT ON mysql.procs_priv TO 'maxscale'@'%';
GRANT SELECT ON mysql.roles_mapping TO 'maxscale'@'%';
GRANT SHOW DATABASES ON *.* TO 'maxscale'@'%';
GRANT REPLICATION CLIENT ON *.* TO 'maxscale'@'%';
GRANT ALL ON infinidb_vtable.* TO 'maxscale'@'%';

CREATE USER 'maxscale_monitor'@'%' IDENTIFIED BY 'icc115-monitor';
GRANT REPLICATION CLIENT, FILE, SUPER, RELOAD, PROCESS, SHOW
DATABASES, EVENT ON *.* TO 'maxscale_monitor'@'%';
```

Instalación de RabbitMQ

Instalación del servidor RabbitMQ y creación de un usuario con permisos específicos para OpenStack.

```
sudo apt install rabbitmq-server

sudo rabbitmqctl add_user openstack icc1152024

sudo rabbitmqctl set_permissions openstack ".*" ".*" ".*"
```

Instalación de Memcached

Instalación del servicio de caché en memoria y ajuste de la configuración.

```
sudo apt install memcached python3-memcache

sudo nano /etc/memcached.conf

sudo service memcached restart
```

Instalación y configuración de etcd

Configuración del servicio etcd, incluyendo la especificación de su nombre, URLs de cliente y peer, así como el estado inicial del clúster.

```
sudo apt install etcd-server
```

La siguiente es la configuracion definida en el archivo /etc/default/etcd

```
ETCD_NAME="controller"
ETCD_DATA_DIR="/var/lib/etcd"
ETCD_INITIAL_CLUSTER_STATE="new"
ETCD_INITIAL_CLUSTER_TOKEN="etcd-cluster-01"
ETCD_INITIAL_CLUSTER="controller=http://10.0.0.11:2380"
ETCD_INITIAL_ADVERTISE_PEER_URLS="http://10.0.0.11:2380"
ETCD_ADVERTISE_CLIENT_URLS="http://10.0.0.11:2379"
ETCD_LISTEN_PEER_URLS="http://0.0.0.0:2380"
ETCD_LISTEN_CLIENT_URLS="http://10.0.0.11:2379"
```

Reiniciamos el servicio y lo habilitamos

```
sudo systemctl enable etcd
sudo systemctl restart etcd
```

Instalación del cliente OpenStack

Instalación del cliente de línea de comandos de OpenStack para administrar el entorno en todas las máquinas.

```
sudo apt install python3-openstackclient
```

Configuración de la base de datos Keystone

Creación de la base de datos keystone en MariaDB, otorgando permisos al usuario y configurando Keystone para conectarse a esta base de datos.

```
mysql
CREATE DATABASE keystone;
GRANT ALL PRIVILEGES ON keystone.* TO 'keystone'@'localhost' \
IDENTIFIED BY 'icc1152024';
GRANT ALL PRIVILEGES ON keystone.* TO 'keystone'@'%' \
IDENTIFIED BY 'icc1152024';
FLUSH PRIVILEGES;
exit
```

Configuración de Keystone para usar Fernet como proveedor de tokens.

```
sudo apt install keystone

sudo nano /etc/keystone/keystone.conf
[database]
connection = mysql+pymysql://keystone:icc1152024@controller/keystone

[token]
provider = fernet

sudo su -s /bin/sh -c "keystone-manage db_sync" keystone

keystone-manage fernet_setup --keystone-user keystone --keystone-group keystone

keystone-manage credential_setup --keystone-user keystone --keystone-group keystone

keystone-manage bootstrap --bootstrap-password icc1152024 \
  --bootstrap-admin-url http://controller:5000/v3/ \
  --bootstrap-internal-url http://controller:5000/v3/ \
  --bootstrap-public-url http://controller:5000/v3/ \
  --bootstrap-region-id RegionOne
```

Configuración de Apache para Keystone

Ajuste del archivo de configuración de Apache para soportar Keystone y reinicio del servicio, es decir, el archivo /etc/apache2/apache2.conf

```
ServerName controller
```

Reiniciamos el servicio

```
sudo service apache2 restart
```

Creación de archivos de entorno (admin-openrc y demo-openrc)

Configuración de los archivos de entorno para facilitar la autenticación de usuarios en OpenStack.

Archivo admin-openrc

```
export OS_PROJECT_DOMAIN_NAME=Default
export OS_USER_DOMAIN_NAME=Default
export OS_PROJECT_NAME=admin
export OS_USERNAME=admin
export OS_PASSWORD=icc1152024
export OS_AUTH_URL=http://controller:5000/v3
export OS_IDENTITY_API_VERSION=3
export OS_IMAGE_API_VERSION=2
```

Archivo demo-openrc

```
export OS_PROJECT_DOMAIN_NAME=Default
export OS_USER_DOMAIN_NAME=Default
export OS_PROJECT_NAME=myproject
export OS_USERNAME=myuser
export OS_PASSWORD=icc1152024
export OS_AUTH_URL=http://controller:5000/v3
export OS_IDENTITY_API_VERSION=3
export OS_IMAGE_API_VERSION=2
```

Creación de dominios, proyectos, usuarios y roles en OpenStack

Uso de comandos openstack para crear dominios, proyectos, usuarios y roles, y asignar roles a los usuarios. En primer lugar, nos encargamos de cargas las variables de entorno con el comando

```
. admin-openrc
```

Una vez cargadas, procedemos a crear el dominio, usuario y roles

```
openstack domain create --description "An Example Domain" example

openstack project create --domain default \
  --description "Service Project" service

openstack project create --domain default \
  --description "Demo Project" myproject

openstack user create --domain default \
  --password-prompt myuser

openstack role create myrole

openstack role add --project myproject --user myuser myrole

openstack --os-auth-url http://controller:5000/v3 \
  --os-project-domain-name Default --os-user-domain-name Default \
  --os-project-name admin --os-username admin token issue

openstack --os-auth-url http://controller:5000/v3 \
  --os-project-domain-name Default --os-user-domain-name Default \
  --os-project-name myproject --os-username myuser token issue
```

Configuración de la base de datos Glance

Creación de la base de datos glance y configuración del servicio Glance para usar esta base de datos.

```
mysql
CREATE DATABASE glance;
GRANT ALL PRIVILEGES ON glance.* TO 'glance'@'localhost' \
  IDENTIFIED BY 'icc1152024';
GRANT ALL PRIVILEGES ON glance.* TO 'glance'@'%' \
  IDENTIFIED BY 'icc1152024';
exit
```

Configuración de autenticación de Keystone para Glance, dominio, usuario y roles

```
. admin-openrc

openstack user create --domain default --password-prompt glance

openstack role add --project service --user glance admin

openstack service create --name glance \
  --description "OpenStack Image" image
```

```
openstack endpoint create --region RegionOne \
  image public http://controller:9292

openstack endpoint create --region RegionOne \
  image internal http://controller:9292

openstack endpoint create --region RegionOne \
  image admin http://controller:9292

sudo apt install glance
```

Sincronización de la base de datos y reinicio del servicio Glance

Sincronización de la base de datos Glance y reinicio del servicio para aplicar los cambios.

La siguiente es la configuración en el archivo /etc/glance/glance-api.conf

```
[database]
connection = mysql+pymysql://glance:icc1152024@controller/glance

[keystone_authtoken]
www_authenticate_uri  = http://controller:5000
auth_url = http://controller:5000
memcached_servers = controller:11211
auth_type = password
project_domain_name = Default
user_domain_name = Default
project_name = service
username = glance
password = icc1152024


[paste_deploy]
flavor = keystone

[DEFAULT]
enabled_backends=fs:file

[glance_store]
default_backend = fs

[fs]
filesystem_store_datadir = /var/lib/glance/images/

[oslo_limit]
auth_url = http://controller:5000
auth_type = password
user_domain_id = default
```

```
username = glance
system_scope = all
password = icc1152024
endpoint_id = 838807aaf53444029737ffb426b577a7
region_name = RegionOne
```

Configuración de la base de datos Placement

Creación de la base de datos placement, configuración del servicio Placement y establecimiento de endpoints.

```
mysql
CREATE DATABASE placement;
GRANT ALL PRIVILEGES ON placement.* TO 'placement'@'localhost' \
  IDENTIFIED BY 'icc1152024';
GRANT ALL PRIVILEGES ON placement.* TO 'placement'@'%' \
  IDENTIFIED BY 'icc1152024';
exit
```

Configuración de autenticación de Keystone para Placement, dominio, usuario y roles

```
. admin-openrc

openstack user create --domain default --password-prompt placement

openstack role add --project service --user placement admin

openstack service create --name placement \
  --description "Placement API" placement

openstack endpoint create --region RegionOne \
  placement public http://controller:8778

openstack endpoint create --region RegionOne \
  placement internal http://controller:8778

openstack endpoint create --region RegionOne \
  placement admin http://controller:8778
```

Instalación de Placement

```
apt install placement-api
```

La siguiente es la configuracion del archivo /etc/placement/placement.conf

```
[placement_database]
```

```
connection = mysql+pymysql://placement:icc1152024@controller/placement

[api]
auth_strategy = keystone

[keystone_authtoken]
auth_url = http://controller:5000/v3
memcached_servers = controller:11211
auth_type = password
project_domain_name = Default
user_domain_name = Default
project_name = service
username = placement
password = icc1152024
```

Ahora, la sincronizacion con la base de datos respectiva

```
sudo su -s /bin/sh -c "placement-manage db sync" placement
service apache2 restart
openstack --os-placement-api-version 1.2 resource class list --sort-column name
```

Instalación y configuración de Nova (Compute)

Configuración de bases de datos para Nova, ajuste de archivos de configuración para servicios y autenticación.

```
mysql
CREATE DATABASE nova_api;
CREATE DATABASE nova;
CREATE DATABASE nova_cell0;
GRANT ALL PRIVILEGES ON nova_api.* TO 'nova'@'localhost' \
  IDENTIFIED BY 'icc1152024';
GRANT ALL PRIVILEGES ON nova_api.* TO 'nova'@'%' \
  IDENTIFIED BY 'icc1152024';
GRANT ALL PRIVILEGES ON nova.* TO 'nova'@'localhost' \
  IDENTIFIED BY 'icc1152024';
GRANT ALL PRIVILEGES ON nova.* TO 'nova'@'%' \
  IDENTIFIED BY 'icc1152024';
GRANT ALL PRIVILEGES ON nova_cell0.* TO 'nova'@'localhost' \
  IDENTIFIED BY 'icc1152024';
GRANT ALL PRIVILEGES ON nova_cell0.* TO 'nova'@'%' \
  IDENTIFIED BY 'icc1152024';
exit
```

Usuario, dominio y rol para la gestión de nova.

```
. admin-openrc
```

```
openstack user create --domain default --password-prompt nova

openstack role add --project service --user nova admin

openstack service create --name nova \
  --description "OpenStack Compute" compute

openstack endpoint create --region RegionOne \
  compute public http://controller:8774/v2.1

openstack endpoint create --region RegionOne \
  compute internal http://controller:8774/v2.1

openstack endpoint create --region RegionOne \
  compute admin http://controller:8774/v2.1

sudo apt install nova-api nova-conductor nova-novncproxy nova-scheduler
```

La siguientes es la configuración del archivo sudo nano /etc/nova/nova.conf

```
[api_database]
connection = mysql+pymysql://nova:icc1152024@controller/nova_api

[database]
connection = mysql+pymysql://nova:icc1152024@controller/nova

[DEFAULT]
transport_url = rabbit://openstack:icc1152024@controller:5672/
my_ip = 10.0.0.11

[api]
auth_strategy = keystone

[keystone_authtoken]
www_authenticate_uri = http://controller:5000/
auth_url = http://controller:5000/
memcached_servers = controller:11211
auth_type = password
project_domain_name = Default
user_domain_name = Default
project_name = service
username = nova
password = icc1152024

[service_user]
send_service_user_token = true
#auth_url = https://controller/identity
auth_url = http://controller:5000/identity
auth_strategy = keystone
auth_type = password
project_domain_name = Default
project_name = service
user_domain_name = Default
```

```
username = nova
password = icc1152024

[vnc]
enabled = true
server_listen = $my_ip
server_proxyclient_address = $my_ip

[glance]
api_servers = http://controller:9292

[oslo_concurrency]
lock_path = /var/lib/nova/tmp

[placement]
region_name = RegionOne
project_domain_name = Default
project_name = service
auth_type = password
user_domain_name = Default
auth_url = http://controller:5000/v3
username = placement
password = icc1152024

[scheduler]
discover_hosts_in_cells_interval = 300
```

Configuración de OpenLDAP

Instalar OpenLDAP y las herramientas de administración necesarias

```
sudo apt update
sudo apt install slapd ldap-utils -y
```

Durante la instalación, se pide que configurar la contraseña del administrador de LDAP. Luego, configuramos slapd para definir los parámetros básicos del dominio.

```
sudo dpkg-reconfigure slapd
```

Una vez terminada la configuración, importamos los esquemas necesarios, como cosine, nis y inetorgperson

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif
```

Crear un archivo LDIF para la configuración de la estructura del directorio

```
dn: dc=cloud,dc=com
objectClass: top
objectClass: dcObject
objectclass: organization
o: Example Organization
dc: cloud

dn: ou=People,dc=example,dc=com
objectClass: organizationalUnit
ou: People

dn: ou=Groups,dc=example,dc=com
objectClass: organizationalUnit
ou: Groups
```

Añadir la estructura básica al servidor LDAP

```
sudo ldapadd -x -D cn=admin,dc=example,dc=com -W -f base.ldif
```

Para la integración de OpenLDAP con OpenStack Keystone, editamos la configuración de Keystone para utilizar LDAP como backend de identidad, esto en el archivo /etc/keystone/keystone.conf

```
[identity]
driver = ldap

[ldap]
url = ldap://localhost
user = cn=admin,dc=example,dc=com
password = [admin_password]
suffix = dc=example,dc=com
user_tree_dn = ou=People,dc=example,dc=com
user_objectclass = inetOrgPerson
group_tree_dn = ou=Groups,dc=example,dc=com
group_objectclass = groupOfNames
```

Reiniciar el servicio de Keystone para aplicar los cambios

```
sudo systemctl restart apache2
```

Ahora, podemos crear usuarios, para ello creamos un archivo LDIF, por ejemplo, new_user.ldif

```
dn: uid=cmartinez,ou=People,dc=example,dc=com
objectClass: inetOrgPerson
uid: cmartinez
sn: Carlos
givenName: Martinez
cn: Carlos Martinez
displayName: cmartinez
userPassword: password123
mail: cmartinez@ues.edu.sv
```

Añadimos el usuario al directorio LDAP

```
sudo ldapadd -x -D cn=admin,dc=cloud,dc=com -W -f new_user.ldif
```

De igual manera, podemos definir grupos, y para ello creamos un archivo LDIF, por ejemplo, new_group.ldif

```
dn: cn=admin_group,ou=Groups,dc=example,dc=com
objectClass: groupOfNames
cn: admin_group
member: uid=cmartinez,ou=People,dc=cloud,dc=com
```

Y, parecido a como con los usuarios nuevos, añadimos el grupo al directorio LDAP

```
sudo ldapadd -x -D cn=admin,dc=example,dc=com -W -f new_group.ldif
```

Ahora, aun tenemos que hacer la onfiguración de Keystone para usar usuarios y grupos de LDAP, para ello, editamos el archivo keystone.conf para especificar el uso de LDAP en la configuración de grupos y usuarios. Una vez terminado, podemos verificar que los usuarios y grupos se sincronicen con Keystone, utilizando los comandos OpenStack CLI, por ejemplo:

```
openstack user list
openstack group list
```

Configuración de Heat

Configuración de bases de datos para Heat.

```
CREATE DATABASE heat;

GRANT ALL PRIVILEGES ON heat.* TO 'heat'@'localhost' \
  IDENTIFIED BY 'HEAT_DBPASS';
GRANT ALL PRIVILEGES ON heat.* TO 'heat'@'%' \
  IDENTIFIED BY 'HEAT_DBPASS';
```

Creamos las credenciales del servicio

```
    openstack user create --domain default --password-prompt heat
```

Añade el rol de admin al usuario de heat

```
    openstack role add --project service --user heat admin
```

Crear las entidades de servicio heaty heat-cfn

```
    openstack service create --name heat \
  --description "Orchestration" orchestration

    openstack service create --name heat-cfn \
  --description "Orchestration"  cloudformation
```

Cree los puntos finales de la API del servicio de orquestación

```
openstack endpoint create --region RegionOne \
orchestration public http://controller:8004/v1/%\(tenant_id\)s

openstack endpoint create --region RegionOne \
orchestration internal http://controller:8004/v1/%\(tenant_id\)s

openstack endpoint create --region RegionOne \
orchestration admin http://controller:8004/v1/%\(tenant_id\)s

openstack endpoint create --region RegionOne \
cloudformation public http://controller:8000/v1

openstack endpoint create --region RegionOne \
cloudformation internal http://controller:8000/v1

openstack endpoint create --region RegionOne \
cloudformation admin http://controller:8000/v1
```

Cree el dominio heat que contiene proyectos y usuarios para las pilas

```
openstack domain create --description "Stack projects and users" heat

openstack user create --domain heat --password-prompt heat_domain_admin
```

Agregue el rol admin al usuario heat_domain_admin en el dominio de heat para habilitar privilegios de gestión de pila administrativa por parte del usuario heat_domain_admin

```
openstack role add --domain heat --user-domain heat --user heat_domain_admin admin
```

Crear el rol heat_stack_owner

```
openstack role create heat_stack_owner
```

Agregue el rol heat_stack_owner al proyecto y al usuario para habilitar la administración de la pila por parte del usuario

```
openstack role add --project demo --user demo heat_stack_owner
```

Crear el rol heat_stack_user

```
openstack role create heat_stack_user
```

Para completar la instalación se necesita agregar los siguientes paquetes:

```
apt-get install heat-api heat-api-cfn heat-engine
```

Realizar las siguientes modificaciones al archivo: /etc/heat/heat.conf

```
[database]

connection = mysql+pymysql://heat:HEAT_DBPASS@controller/heat

[DEFAULT]
transport_url = rabbit://openstack:RABBIT_PASS@controller
heat_metadata_server_url = http://controller:8000
heat_waitcondition_server_url = http://controller:8000/v1/waitcondition
stack_domain_admin = heat_domain_admin
stack_domain_admin_password = HEAT_DOMAIN_PASS
stack_user_domain_name = heat

    [keystone_authtoken]
www_authenticate_uri = http://controller:5000
auth_url = http://controller:5000
memcached_servers = controller:11211
auth_type = password
project_domain_name = default
user_domain_name = default
project_name = service
username = heat
password = HEAT_PASS

[trustee]
auth_type = password
auth_url = http://controller:5000
username = heat
password = HEAT_PASS
user_domain_name = default

[clients_keystone]
auth_uri = http://controller:5000
```

Llene la base de datos de orquestación

```
su -s /bin/sh -c "heat-manage db_sync" heat
```

Reinicie los servicios de orquestación

```
service heat-api restart
service heat-api-cfn restart
service heat-engine restart
```