UNIVERSIDAD INTERNACIONAL SEK

DIGITAL SCHOOL

TRABAJO DE INVESTIGACIÓN DE FIN DE CARRERA

TITULADO:

ADMINISTRACIÓN CENTRALIZADA DE LOS SERVICIOS INFORMÁTICOS EN LA DIRECCIÓN GENERAL DE INTELIGENCIA

Realizado por:
Ing. Carlos Andrés Mafla
Ing. Jorge Luis Mendieta

Director del proyecto:
Ing. Fabián Hurtado Vargas, MGS. Seguridad telemática.

Como requisito para la obtención del título de:
MAGISTER EN CIBERSEGURIDAD

QUITO, 6 agosto del 2020

Administración centralizada de los servicios informáticos en la DGI

DECLARACIÓN JURAMENTADA

Por la presente, yo, Carlos Andrés Mafla Carvajal, con cédula de ciudadanía Nro. 1715527915, declaro bajo juramento, que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de esta declaración cedo mis derechos de propiedad intelectual de autora a la UNIVERSIDAD INTERNACIONAL SEK UISEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

CARLOS ANDRÉS MAFLA CARVAJAL

CC: 1715527915

Administración centralizada de los servicios informáticos en la DGI

DECLARACIÓN JURAMENTADA

Por la presente, yo, Jorge Luis Mendieta Piedra, con cédula de ciudadanía Nro. 0103748190, declaro bajo juramento, que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de esta declaración cedo mis derechos de propiedad intelectual de autora a la UNIVERSIDAD INTERNACIONAL SEK UISEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

JORGE LUIS MENDIETA PIEDRA

CC: 0103748190

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro que el presente trabajo de investigación titulado:

"ADMINISTRACIÓN CENTRALIZADA DE LOS SERVICIOS INFORMÁTICOS EN LA DIRECCIÓN GENERAL DE INTELIGENCIA"

Realizado por:

CARLOS ANDRÉS MAFLA CARVAJAL

JORGE LUIS MENDIETA PIEDRA

Como requisito para la obtención del Título de

MASTER EN CIBERSEGURIDAD

Ha sido dirigido por mi persona a través de reuniones periódicas con los estudiantes cumple con todas las disposiciones que rigen los trabajos de titulación**.**

_____

Ing. Fabián Hurtado Vargas, MGS.

DIRECTOR DEL PROYECTO

CC: 0913563326

LOS PROFESORES INFORMANTES

Los profesores informantes:

Ing. Paul F. Bernal Barzallo, Mg.

Ing. Juan Xavier Játiva Álvarez, MGS.

.

Después de revisar el trabajo han calificado como apto

para su defensa oral ante el tribunal examinador

_____ _____

Ing. Paul F. Bernal Barzallo, Mg. Ing. Juan Xavier Játiva Álvarez, MGS.

Quito, agosto de 2020

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaramos que este trabajo es de nuestra autoría, que se han citado las fuentes correspondientes y
que en su desarrollo se respetaron las disposiciones legales vigentes, que protegen los derechos de autor.

Carlos Andrés Mafla Carvajal	Jorge Luis Mendieta Piedra
CC:1715527915	CC: 0103748190

AGRADECIMIENTO

Agradezco a Dios por haberme acompañado y guiado a lo largo de la Maestría en Ciberseguridad y haber podido culminarla con éxito.

A mis padres por apoyarme y guiarme en todo momento, por los consejos, valores y principios que me han inculcado.

A mi hermana Lorena, por siempre creer en mí, su amor y su apoyo incondicional.

A Jorge Luis, a quien tuve la oportunidad de conocerle durante la Maestría y hemos formado una linda amistad, gracias por estar conmigo cuando más lo he necesitado, por todos los momentos que hemos compartido y tu apoyo.

Agradezco a los docentes de la Universidad SEK, por todos los conocimientos compartidos durante la Maestría en Ciberseguridad.

De igual forma, un agradecimiento especial a mi director de tesis MGS Fabian Hurtado, por su conocimiento y colaboración en el desarrollo de esta tesis.

Carlos Andrés Mafla Carvajal

AGRADECIMIENTO

Quiero agradecer a Dios por darme la oportunidad de culminar mi carrera de la Maestría en Ciberseguridad con salud y lleno de bendiciones.

También quiero agradecer, a los docentes de la Universidad por ser parte de mi formación profesional, fortaleciéndome en varias áreas de conocimiento e investigación, a mis compañeros de las Universidad que día a día, se compartían distintas experiencias y vivencias, creando solidos lazos de amistad, que nos ayuda a ser mejores personas.

Un agradecimiento muy especial, al MGS Fabián Hurtado, por brindarnos todo su apoyo, para el desarrollo de este tema de tesis, guiándonos en la parte conceptual.

Jorge Luis Mendieta Piedra

DEDICATORIA

Todo el esfuerzo vertido en este trabajo de tesis está dedicado con todo el cariño a mis padres Carlos y Jacqueline; y a mi hermana Lorena que con su amor, confianza y apoyo incondicional permitieron que logre cumplir una meta más en mi vida.

Carlos Andrés Mafla Carvajal

DEDICATORIA

Quiero dedicar, esta nueva meta cumplida a mis padres, por darme todo el amor y apoyo que necesito, para seguir adelante formándome, quiero dedicar también a todos mis hermanos por su cariño incondicional y consejos brindados a lo largo de mi vida, a mis sobrinos, sobrinas que llegaron a mi vida, para hacerme más responsable en mi formación profesional y ser un ejemplo a seguir como persona.

Quiero también dedicar de manera muy especial a Pamela Badillo y mi hij@ que se encuentra en camino si Dios me lo permite, ya que cuento con su amor y apoyo incondicional, que es demostrado todos los días a mi lado, dando más motivos de seguir adelante, superándome en mi vida profesional y personal.

Quiero agradecer a todas las familias que me ayudaron, para alcanzar esta nueva meta, en especial a la familia de mi compañero de tesis Carlos Mafla, que siempre estaban al pendiente
de nuestra carrera profesional.

Jorge Luis Mendieta Piedra

RESUMEN

Este trabajo de tesis se basa en la implementación una infraestructura como servicio (IaaS) de computación en la nube privada en la Dirección General de Inteligencia de la Policía Nacional del Ecuador, con la finalidad de centralizar la administración de los servicios informáticos para mejorar la administración, control de los servicios informáticos y la seguridad en la infraestructura tecnológica. Para lo cual, primero fue necesario identificar y analizar los activos informáticos con los que contaba la organización, para ser utilizados en este proyecto; después, se diseñó la infraestructura de computación en la nube, donde se realizó el dimensionamiento de la infraestructura tecnológica, se mostró la arquitectura de la infraestructura tecnológica de computación en la nube, el diseño de las redes de comunicación tomando en cuenta las seguridades en ellas, el diseño de topología de red jerárquica y un diagrama general de la topología de red física con dispositivo de seguridad perimetral, un controlador de dominio y un sistema de monitoreo y gestión de incidentes informáticos; después se procedió con la implementación de la infraestructura como servicio IaaS de computación en la nube, para la cual se utilizaron las herramientas de virtualización del fabricante VMware (VSphere Enterprise, VMware vCenter y VMware Integrated OpenStack); finalmente se implementaron seguridades en la infraestructura tecnológica, en donde, se implementó seguridad

perimetral, un Directorio Activo, un SIEM y seguridades a nivel del entorno de la infraestructura de computación en la nube IaaS.

Palabras claves: Computación en la nube, IaaS, Seguridad, Administración centralizada de la Infraestructura Tecnológica.

ABSTRACT

This thesis paper is based on the implementation of an Infrastructure as a computing service (IaaS) at the General Intelligence Directorate of the National Police of Ecuador private cloud, in order to centralize the administration of computer services to improve the administration, computer services control and the technological infrastructure security. For which, it was necessary to identify and analyze the computer assets that the organization had, to be used in this project; Later, the cloud computing infrastructure was designed, where the Sizing of the technological infrastructure was carried out, the architecture of the technological infrastructure of cloud computing, the design of communication networks taking into account the security in them, the hierarchical network topology design and a general diagram of the physical network topology with perimeter security device, a domain controller and a computer incident monitoring and management system; then, the cloud computing infrastructure as a IaaS service was implemented, for which the virtualization tools of the manufacturer VMware (VSphere Enterprise, VMware vCenter and VMware Integrated OpenStack) were used; finally, safeguards were implemented in the technological infrastructure, where Perimeter security, an Active Directory, a SIEM and safeguards were implemented at the environment level of the IaaS cloud computing infrastructure.

Keywords: Cloud computing, IaaS, Security, Centralized Administration of Technological Infrastructure.

Tabla de Contenidos

Contenido

40

45

Figuras y tablas

Capítulo I

Introducción

1.1 Planteamiento del Problema

> La Dirección General de Inteligencia de la Policía Nacional del Ecuador como órgano central, encargado de dirigir sistemáticamente la planificación, búsqueda, procesamiento y difusión de la información relacionada con los riesgos y amenazas al mantenimiento del orden público, seguridad del Estado, seguridad pública y ciudadana; la institucionalidad del Estado; la delincuencia común y organizada, nacional y transnacional; permite con su accionar la oportuna toma de decisiones en los distintos organismos gubernamentales y policiales. (Policia Nacional del Ecuador, n.d.)

Actualmente la DGI cuenta con departamentos situados en las distintas ciudades del país. Mediante observación en sitio se logró identificar que en los departamentos se tiene implementado varios servicios informáticos de manera descentralizada. Esta descentralización provoca los siguientes problemas:

- Dificultad para el control de los recursos tecnológicos acceso a la información que se encuentra en los departamentos.
- Desperdicio de recursos de memoria de procesamiento y almacenamiento al contar con sistemas instalados de manera nativa.
- Los recursos tecnológicos no son asignados de manera óptima para los servicios implementados.
- Latencia en el tiempo de respuesta a la solución de incidentes y toma de decisiones.
- Incremento de equipos tecnológicos y espacio físico.
- Duplicidad en los servicios informáticos y riesgo de pérdida de información.

Además de los problemas mencionados por la descentralización de los servicios informáticos, la DGI no cuenta con un servicio informático que proporcione seguridad al control de acceso a la información y tampoco de un sistema que permita el monitoreo y control de los activos de información tecnológicos de la organización.

1.2 Objetivo General

Centralizar la administración de los servicios informáticos en la Dirección General de Inteligencia con la implementación de una Infraestructura como Servicio (IaaS) de computación en la nube, para disminuir el tiempo de respuesta, en los requerimientos solicitados al departamento de Tecnologías de la Información (TI).

1.3 Objetivo Específicos

- Identificar los activos informáticos existentes en la Dirección General de Inteligencia.
- Diseñar una infraestructura virtual que permita la escalabilidad vertical[1] y horizontal[2] en función de necesidades específicas de la organización.
- Implementar una infraestructura de computación en la nube basados en IaaS para la administración y control de los servicios informáticos.
- Implementar un servicio que proporcione seguridad al control de acceso a la información.

[1] **Escalabilidad Vertical:** Consiste en crecer el hardware de uno de los nodos, es decir aumentar los recursos del servidor por unos más potentes, en los que respecta a capacidad de procesamiento, memoria y almacenamiento (León, 2019).

[2] **Estabilidad Horizontal:** Consiste en aumentar el número de servidores que atienden a una aplicación., cada uno los servidores se conocen como nodos, el escalado se realiza simplemente agregando un nuevo nodo al clúster (León, 2019).

- Implementar un sistema de seguridad de la información y gestión de eventos informáticos, para el monitoreo y control de los activos de información tecnológicos de la organización.
- Implementar controles de seguridad en la infraestructura tecnológica, mediante la aplicación de buenas prácticas, para preservar las propiedades de la información: confidencialidad, integridad y disponibilidad.

1.4 Justificación

La Dirección General de Inteligencia es una institución que maneja información clasificada para la prevención de riesgos y amenazas, que pueden afectar la seguridad del estado ecuatoriano, por lo tanto, es necesario que la organización, disponga herramientas tecnológicas que permitan controlar y monitorear los servicios informáticos en tiempo real; manteniendo la confidencialidad, disponibilidad e integridad de la información digital que es procesada, almacenada y transmitida.

Es importante que el Eje de Inteligencia de la Policía Nacional se encuentre adecuadamente equipado, a fin de combatir los delitos nacionales, trasnacionales, delincuencia organizada, terrorismo, entre otros y minimizar el impacto de los atentados en el territorio ecuatoriano.

La implementación de una infraestructura de computación en la nube privada basada en IaaS en la DGI ayudará con solución al problema planteado. Los servicios informáticos serán manejados de forma centralizada y organizada, y de esta manera mejorar la administración, control de los servicios informáticos y la seguridad en la infraestructura tecnológica. Los recursos informáticos podrán escalarse fácilmente según se requiera. También mejorará el tiempo de respuesta a la solución de incidentes y toma de decisiones.

1.5 Estado del Arte

Para el desarrollo del estado del arte se revisó literatura de varios artículos científicos que sirvieron de referencia, para la elaboración de este trabajo de tesis. Se consideraron los siguientes temas como principales: Gestión de recursos tecnológicos para infraestructura como Servicios (IaaS), Diseño e implementación de una plataforma de computación en la nube privada (IaaS) y Seguridades en computación en la nube (IaaS).

Gestión de recursos tecnológicos para infraestructura como Servicios (IaaS)

El siguiente tema referencia artículos que realizaron un análisis sobre gestión de recursos tecnológicos para infraestructuras como Servicios (IaaS). El objetivo principal de referenciar estos artículos es adoptar el tipo de infraestructura tecnológica, para la administración de los recursos tecnológicos mediante software de virtualización, en base a computación en la nube.

Manvi y Shyamb en su documento “GESTIÓN DE RECURSOS PARA INFRAESTRUCTURA COMO SERVICIO (IAAS) EN COMPUTACIÓN EN LA NUBE” (Manvi & Krishna Shyam, 2014) mencionan lo siguiente:

Una nube se define como un lugar sobre la infraestructura de red donde la tecnología de la información (TI) y los recursos informáticos como hardware, sistemas operativos, redes, almacenamiento, bases de datos y aplicaciones de software están disponibles al instante (Buyya & Ranjan, 2010).

La computación en la nube es un modelo que se basa en el uso de recursos tecnológicos de hardware y software los cuales se entregan como un servicio a través de una red (generalmente Internet). Si bien, la computación en la nube puede no involucrar muchas tecnologías nuevas, representa una nueva forma de administrar los recursos tecnológicos de una

organización. En muchos casos, esto no solo cambiará el flujo de trabajo dentro de la organización de TI además que dará como resultado una reorganización completa del departamento de TI. El ahorro de costos y la escalabilidad se pueden lograr altamente desde la computación en la nube (Manvi & Krishna Shyam, 2014).

Gestión de recursos: Los recursos en cualquier momento se asignarán para manejar de manera efectiva las fluctuaciones de la carga de trabajo, al mismo tiempo que brindan garantías de calidad de servicio a los usuarios finales. Los recursos informáticos y de red son limitados y deben compartirse de manera eficiente entre los usuarios. Para efectuar una gestión eficiente de los recursos, se debe considerar el mapeo, aprovisionamiento, asignación y la adaptación de recursos (Manvi & Krishna Shyam, 2014).

El principal desafío en la gestión de los recursos, es determinar la demanda de éstos en cada aplicación en su nivel de carga de solicitud actual y asignar los recursos eficientemente(Chase et al., 2010).

Sushil, Leena y Sandeep en su artículo “COMPUTACIÓN EN LA NUBE: ESTUDIO DE INFRAESTRUCTURAS COMO SERVICIOS(IAAS)” (Sushil et al., 2010) señalan lo siguiente:

La computación en la nube es un modo de referirse al uso de recursos informáticos compartidos y una alternativa a que los servidores locales manejen las aplicaciones. La computación en la nube agrupa grandes cantidades de servidores de cómputo y otros recursos, por lo general ofrece su capacidad combinada según demanda y pago por ciclo.

Los usuarios finales de una red de computación en la nube generalmente desconocen dónde se encuentran físicamente los servidores: simplemente activan su aplicación y comienzan

a trabajar. De acuerdo con Wang, Laszewski, Kunzeand, & Tao (2010), la computación en la nube se puede definir como “un conjunto de servicios habilitados para la red, que proporcionan plataformas de computación bajo demanda escalables, garantizadas por la calidad de servicios, normalmente personalizadas y económicas, a las que se puede acceder de una manera simple y de manera generalizada ". Según Wei, Vasilakos, Zheng, & Xiong, (2010), “la computación en la nube es una evolución natural para los centros de datos y computación con gestión automatizada de sistemas, equilibrio de carga de trabajo y tecnologías de virtualización”. Los servicios basados en la nube integran recursos distribuidos globalmente en plataformas informáticas integradas. Recientemente, una gran cantidad de aplicaciones se están centrando cada vez más en recursos de terceros alojados en Internet y cada uno tiene una capacidad variable.

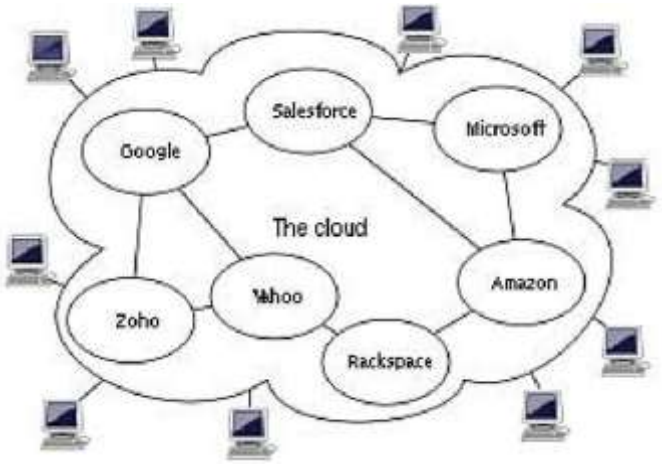


Figura 1: Diagrama lógico de la computación en la nube Fuente:(Sushil et al., 2010) Los principales beneficios de Computación en la Nube son (Sushil et al., 2010):

- La tecnología en la nube se paga de forma incremental, ahorrando dinero a las organizaciones.
- Las organizaciones pueden almacenar más datos que en sistemas informáticos privados.

- Tecnología más flexible a comparación con los métodos informáticos convencionales.
- Los empleados pueden acceder a la información donde sea que estén, en lugar de tener que permanecer en sus escritorios.
- Infraestructura que puedan aprovecharse de inmediato.
- Naturaleza elástica de la infraestructura para asignar y desasignar rápidamente recursos masivamente escalables a servicios empresariales según demanda.
- Flexibilidad para la migración a otras infraestructuras orientadas como servicios.
- Implementación más rápida de nuevos servicios en las organizaciones.

Diseño e Implementación de una plataforma de computación en la nube privada (IaaS)

El siguiente tema referencia artículos que realizaron un análisis sobre el diseño e implementación de una plataforma de computación en la nube privada (IaaS). El objetivo principal del estudio de estos artículos es tener un diseño en base a buenas prácticas y la selección de las herramientas tecnológicas para la implementación de este proyecto.

Los autores Gonzáles, Vigil, García y Garófalo en su artículo “PROPUESTA DE LAS ARQUITECTURAS DE SERVIDORES, RED Y VIRTUALIZACIÓN DE UNA NUBE PRIVADA QUE BRINDE INFRAESTRUCTURA COMO SERVICIO (IAAS1)” (González et al., 2012) señalan lo siguiente:

La crisis económica que se vive actualmente a nivel mundial imposibilita a muchas empresas y/u organizaciones poder comprar o adquirir software y hardware, para la implementación de arquitecturas de red, servidores y virtualización de centros de datos para brindar un modelo IaaS. Por tal motivo los autores de este artículo científico propusieron la implementación una nube privada IaaS con el uso de software libre.

Las arquitecturas propuestas por González et al. (2012) son tres: Arquitectura de virtualización, servidores y red.

La arquitectura de virtualización permite la agrupación de varios servidores de un centro de datos, para optimizar la asignación de los recursos hardware disponibles y permite la automatización de tareas de monitorio y control, como la migración de VMs en caliente, garantizando la disponibilidad de los servicios brindados a los usuarios sin interrupciones(González et al., 2012).

En cuanto con la arquitectura de servidores, se procura establecer la relación existente entre los recursos físicos de los servidores y sus semejantes en VM. Los niveles ideales de aseguramiento se logran reservando más recursos para el proceso de virtualización. Para evitar la sobreexplotación de los recursos, los recursos virtuales deben constituir entre el 60% y el 80% de los recursos físicos(González et al., 2012).

En cuanto a la arquitectura de red, definen una topología de red para la correcta prestación de los servicios informáticos de TI y de comunicaciones que reúnen las siguientes características: disponibilidad, escalabilidad, seguridad y adaptabilidad; manteniéndose dentro del presupuesto del cliente(González et al., 2012).

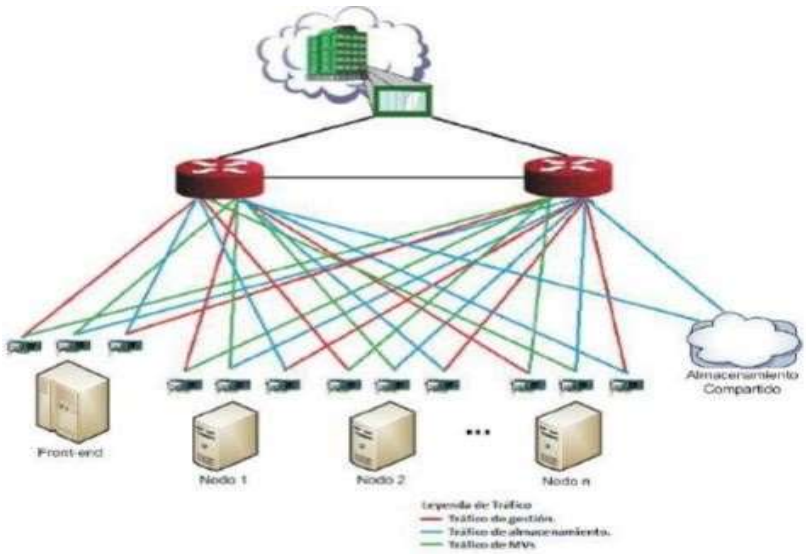


Figura 2: Topología de re. Fuente:(González et al., 2012)

De acuerdo con la investigación realizada por Rafael Moreno Vozmediano, Rubén S. Montero e Ignacio M. Llorente en su documento “Infrastructure as a Service (IaaS): A Comparative Performance Analysis of Open-Source Cloud Platforms” (Shahzadi et al., 2017) señalan lo siguiente:

La computación en la nube ha sido reconocida como un modelo de informático eficiente y adoptado por grandes, pequeñas y medianas empresas. La cantidad de servicios basados en la nube está creciendo de manera gradual y rápidamente.

Los autores realizaron un análisis comparativo de rendimiento entre las plataformas de código abierto basadas en IaaS OpenStack y DevStack de 3 niveles en diferentes escenarios de servicios. Los resultados mostraron que la implementación de OpenStack de 3 niveles es mucho mejor que el método de implementación automática que usa DevStack.

Rajat Kandpal y Vishal Kumar en su documento “IAAS IMPLEMENTATION OF A PRIVATE CLOUD USING OPEN SOURCE TECHNOLOGY” (Kandpal & Kumar, 2013) mencionan lo siguiente:

La computación en la nube es un campo de TI que puede revolucionar las instalaciones informáticas tradicionales. La computación en la nube ofrece hacer las instalaciones de hardware y software más elásticas. El sistema puede ampliarse o reducirse según las necesidades del usuario. El uso de tecnología de código abierto es un punto de inflexión en el suministro de infraestructura de computación en la nube para reducir el costo en gran medida. Se puede crear nubes privadas propias y compartir recursos de hardware y software sin realizar ninguna inversión. Los autores construyeron una nube privada basada en IaaS con la herramienta de

código abierto eucaliptus donde lograron compartir el hardware y otros recursos de una organización a un bajo costo y satisfaciendo las necesidades de la organización.

Sefraoui Omar, Aissaoui Mohammed, Eleuldj Mohsine en su documento "OPENSTACK: TOWARD AN OPEN-SOURCE SOLUTION FOR CLOUD COMPUTING" (Sefraoui et al., 2012) mencionan lo siguiente:

La computación en la nube es virtualizar recursos que se extienden dinámicamente y brindarlos como servicios en Internet. Realizaron un estudio comparativo entre las soluciones de IaaS Eucalyptus, OpenNebula y OpenStack. Finalmente terminan adoptando la solución OpenStack porque está diseñado para permitir a los administradores e investigadores implementar infraestructuras IaaS, proporciona herramientas para crear y administrar máquinas virtuales además de recursos existentes, es fácil de usar en la experimentación al ser modular y ofrece características potentes mientras sigue los estándares abiertos emergentes.

Seguridades en computación en la nube (IaaS).

El siguiente tema referencia artículos, que realizaron un análisis de seguridad en plataformas de computación en la nube. El objetivo principal del estudio de estos artículos es tener presente las diferentes medidas de seguridad en sistemas de computación en la nube y poder aplicar en el proyecto.

González y Rilo en su artículo "CLOUD COMPUTING Y SEGURIDAD" (Gonzales & Rilo, 2012) mencionan lo siguiente:

La computación en la nube ha presentado una nueva oportunidad para las organizaciones tanto en el ámbito comercial y de investigación en aspectos de seguridad. Los métodos y técnicas de

seguridad convencionales no cumplen con el objetivo deseado y no alertan adecuadamente contra fugas de información, accesos no autorizados o ataques MitM (Hombre en el medio).

La computación en la nube es un conjunto de sistemas de software, para la prestación de servicios informáticos rápidos y económicos. Sin embargo, cuestiones como la confidencialidad, la disponibilidad y la integridad de la información requieren salvaguardas contra las nuevas amenazas de seguridad, que han aparecido (Gonzales & Rilo, 2012).

La infraestructura tecnológica de una organización se encuentran expuestos a varios riesgos, entre los cuales están: Fugas de información, tecnología compartida, usuarios internos mal intencionados, perfiles desconocidos de riesgo(Gonzales & Rilo, 2012).

Según la industria de la ciberseguridad, la criptografía es la mejor opción para la protección de la información y los servicios en la nube. La encriptación es fundamental para evitar que la información sea interpretada por personas o servicios no autorizados. De la misma manera, la criptografía otorga un escenario ideal para asegurar la integridad de los mensajes con el uso de la de firma electrónica, facilitando la creación de identidades digitales para la administración de los accesos de usuarios, servicios y dispositivos a datos en la nube. Asimismo, proporciona un marco de evidencias y controles, para auditores y clientes, que asegura su integridad con protección legal (Gonzales & Rilo, 2012).

Las áreas de inmediata aplicación de la criptografía son: encriptación de red, almacenamiento encriptado, integridad de datos, software y sistemas, autenticación criptográfica y; trazabilidad y auditoría(Gonzales & Rilo, 2012) .

Rahul Pangam en su artículo “7 MEJORES PRÁCTICAS PARA ASEGURAR SU SERVICIO EN LA NUBE” mencionan lo siguiente (Pangam, 2017):

La seguridad en la nube no es igual a la seguridad en un centro de datos corporativo. En la nube se aplican diferentes reglas y pensamiento para asegurar una infraestructura tecnológica de la cual no se tiene un control físico real.

En esta publicación, se mencionan algunas de las mejores prácticas y pautas para aprovechar de manera segura los beneficios de la nube mediante el uso de sus puntos fuertes para superar los problemas que tradicionalmente se han calificado de debilidades.

En el artículo mencionan 7 mejores prácticas para asegurar la seguridad en la nube, las cuales son:

1. El cifrado de datos en transición debe ser de extremo a extremo, toda interacción con los servidores se debe realizar con transmisión SSL.
2. El cifrado es importante para los datos en reposo, los datos almacenados en la nube deben cifrarse con AES-256. Las claves de cifrado deben realizarse con claves maestras rotadas regularmente.
3. Las pruebas de vulnerabilidad deben ser rigurosas y continua, se deben emplear herramientas de respuestas a incidentes y vulnerabilidades líderes en la industria.
4. Tener una política de eliminación de datos definida y aplicada.
5. Agregar capas protectoras con seguridad de datos a nivel de usuario, el servicio en la nube debe proporcionar funciones de control de acceso basado en roles y permitir la segregación forzada de tareas dentro de la organización.
6. Obtenga una red y nube privada virtual.
7. Insistir en certificaciones rigurosas de cumplimiento.

Galarza, Zaccardi, Belizán, Duarte, Morales y Encimas en su artículo “PERFORMANCE DE CLOUD COMPUTING PARA HPC: DESPLIEGUE Y SEGURIDAD” mencionan lo siguiente (Galarza et al., 2018):

La computación en la nube es un paradigma que ha estado en constante crecimiento, cada día existen más empresas y grupos de investigación trabajando conjuntamente para explotar las oportunidades ofrecidas por esta tecnología.

Los principales riesgos y problemas de seguridad que se presenta en la computación en la nube son:

> Falta de controles en los datos, ambigüedad de responsabilidad entre el usuario y el proveedor, autenticación y autorización, error de aislamiento, cumplimiento y riesgos legales, la gestión incidentes de seguridad, las vulnerabilidades que presentan las interfaces de administración, protecciones en las aplicaciones y en los datos, la perdida de disponibilidad en los servicios, bloqueo del proveedor, eliminación de datos basura, datos inseguros o incompletos, visibilidad y auditoría y seguridad en software de virtualización. (Cloud Standards Customer Council, 2017, p. 5)

Se debe elaborar un modelo de seguridad, que prevenga los problemas antes mencionados y brinde seguridad en (Balu, 2015):

- "Datos para procesar, con encriptación homomórfica, por ejemplo: Unpadded RSA".(Galarza et al., 2018, p. 919)
- "Datos de transmisión, uso de certificados SSL, por ejemplo: HTTPS". (Galarza et al., 2018, p. 919)
- "Datos de almacenamiento, con encriptación para los almacenes de datos virtuales, por ejemplo: AES".(Galarza et al., 2018, p. 919)
- "Administración correcta de contraseñas, por ejemplo: HSM".(Galarza et al., 2018, p. 919)
- "Autenticación y autorización, con doble factor de autenticación, por ejemplo: Token".(Galarza et al., 2018, p. 919)

- “Protección de usuario, encriptar datos sensibles antes de cargarlos”.(Galarza et al., 2018, p. 919)
- “Controles de seguridad perimetral, implementación de cortafuegos”.(Galarza et al., 2018, p. 919)

Capítulo II

Marco Teórico

En este capítulo se describen los principales conceptos para la comprensión de infraestructuras tecnológicas, tipos de infraestructuras, gestión de infraestructuras tecnológicas, computación en la nube, modelos para el despliegue de una infraestructura de computación en la nube, modelos de servicio en la nube y las medidas de seguridad.

2.1 Infraestructura Tecnológicas

Es el conjunto de recursos físicos y virtuales que admiten el flujo, almacenamiento, procesamiento y análisis de datos. La infraestructura puede estar de manera centralizada o descentralizada, administrados por la misma organización o por terceros (Rouse, 2017). La infraestructura Tecnológica se divide en cuatro elementos: servidores, almacenamiento interno, redes de comunicación y seguridad (Saavedra, 2018).

2.2 Tipos de Infraestructuras Tecnológicas

Las organizaciones cuentan con varias opciones de tipos de infraestructuras de centros de datos, para cumplir con los objetivos en base al giro de negocio.

Entre los diferentes tipos de Infraestructuras se tiene:

Infraestructura Inmutable: Es un enfoque para administrar servicios e implementaciones de software en recursos de TI, donde los componentes se reemplazan en lugar de modificarse. Una aplicación o servicios se vuelven a implementar de manera efectiva cada vez que se produce un cambio (Rouse, 2017).

Infraestructura componible: Los recursos físicos de computación, almacenamiento y red son tratados como un servicio, pueden ser gestionados por los administradores con herramientas de software, utilizando un alto nivel de automatización y orquestación (Rouse, 2017).

Infraestructura Dinámica: Es un marco de trabajo puede implementarse y ajustarse automáticamente a medida que la demanda de carga de trabajo cambia. Minimiza el tiempo para la administración una infraestructura tecnológica, reduce los errores y asigna los recursos de manera óptima (Rouse, 2017).

Infraestructura Crítica: Es el conjunto de sistemas, redes y activos que requieren operación continua, para garantizar la seguridad, economía y salud de una nación (Rouse, 2017).

Infraestructura en la nube: Se refiere a los componentes de hardware y software, como servidores, almacenamiento, redes de comunicación y herramientas de virtualización, que son necesarios para soportar los requerimientos informáticos de un modelo de computación en la nube, incluye una capa de abstracción que virtualiza los recursos y los presenta lógicamente a los usuarios a través de interfaces de programas de aplicación o línea de comandos (Rouse, 2017).

Infraestructura Oscura: Se refiera al software o servicios indocumentados, pero activos, cuya existencia y función es desconocida para los administradores del sistema, a pesar de que puede ser integral para la operación continua de la infraestructura documentada. Esto se conoce como TI paralela, y puede convertirse en una grave vulnerabilidad de seguridad o cumplimiento para la organización(Rouse, 2017).

2.3 Gestión de una infraestructura Tecnológica

Es la administración de componentes operativos esenciales, tales como procesos, políticas, datos, equipos, contactos externos y recursos humanos, para la eficiencia general. Las categorías en las que se divide la administración de una infraestructura tecnológica son: administración de sistemas, administración de redes y administración de almacenamiento. Entre los propósitos de la gestión de la infraestructura tecnológica se busca: reducir la duplicación de esfuerzos, avalar el cumplimiento de normas, optimar el flujo de información mediante un sistema de informático, fomentar la flexibilidad necesaria ante un entorno cambiante, asegurar la interoperabilidad entre unidades organizativas internas y externas, mantener políticas y prácticas efectivas de gestión del cambio (Rouse, 2018).

2.4 Virtualización

Tecnología manejada por modelos de computación en la nube, para la asignación de recursos tecnológicos y proporcionar servicios informáticos de manera eficiente, dinámica y

elástica, consiste en una capa abstracta en la que varias VMs con sistemas operativos (SO) heterogéneos pueden ejecutarse de forma independiente y operar en la misma máquina física. Cada una de las máquinas virtuales cuenta hardware virtual propio. De tal manera que la máquina física administra el uso de sus recursos, para que varios SO funcionen al mismo tiempo e independientemente (Ordoñez Pacheco, 2009).

2.5 Computación en la nube

Modelo de computación que permite la prestación de servicios informáticos mediante internet (Martín, 2018), proporciona al usuario acceso de red ubicuo a un grupo compartido de recursos informáticos configurables tales como redes, servidores, almacenamiento, aplicaciones y servicios, permitiendo aprovisionar y liberar raudamente con mínimo esfuerzo de administración o intercomunicación con el proveedor de servicios (Mell et al., 2011).

2.5.1 Modelos de despliegue en la nube

La computación en la nube según el despliegue de las infraestructuras y servicios se clasifica en:

Nube Privada: Infraestructura de la nube aprovisionada exclusivamente para el uso de una única organización con varios usuarios, solo puede ser gestionada y operada por técnicos de la organización. Este tipo de nube puede estar dentro o fuera de las instalaciones de la organización (Mell et al., 2011).

Nube Colaborativa: Infraestructura de la nube exclusivamente para el uso de una comunidad de consumidores específicos de organizaciones con ideologías compartidas (Mell et al., 2011).

Nube Pública: Son nubes de infraestructuras provisionadas para el uso abierto del público en general (Mell et al., 2011).

Nube Híbrida: Infraestructura de nube compuesta por más de un tipo de infraestructura, reconocidas como entidades únicas, aunque juntas son estandarizadas para habilitar la portabilidad de datos y aplicativos en una organización (Mell et al., 2011).

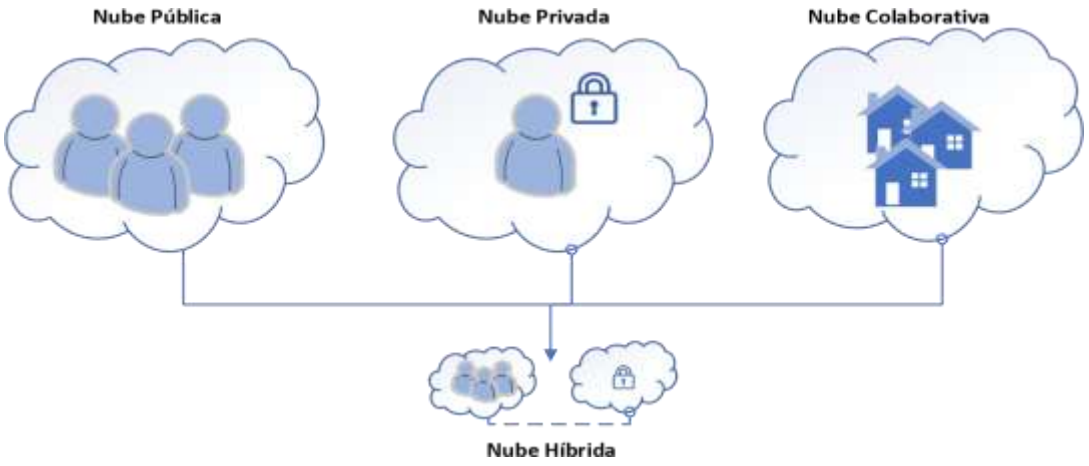


Figura 3: Tipo de nubes Fuente: Elaboración propia

2.5.2 Modelos de servicio en la nube

Los servicios de computación en la nube se dividen en tres modelos que están basados en lo que ofrece el proveedor y las necesidades del cliente; y las responsabilidades de cada uno según el contrato de servicio (Malisow, 2020).

Los tres modelos de computación en la nube son: Infraestructuras como servicio (IaaS), Software como servicio (SaaS) y Plataformas como servicio (PaaS), estos modelos se describen a continuación (Alberto et al., 2012):

SaaS: Modelo orientado a clientes donde el proveedor de esta tecnología cuenta con una aplicación estándar producida, administrada y mantenida por él, con la que proporciona servicios a usuarios mediante la red, sin tener que instalar programas adicionales en los computadores o equipos de los usuarios. Las aplicaciones son repartidas como servicios y se acceden a ellas bajo demanda.

PaaS: Servicios basados en la nube que proporciona a desarrolladores de software una variedad de plataformas computacionales destinadas para desarrollar software, realizar pruebas, desplegar aplicaciones, alojamiento de sitios web, mantenimiento de SO y aplicaciones del cliente.

IaaS: Es un modelo donde el proveedor ofrece una infraestructura informática presentada como un servicio, a través de interfaces y una plataforma de virtualización, el cliente ya no debe preocuparse de comprar equipos tecnológicos costosos como servidores, contar con el espacio necesario para un centro de datos o equipamiento de redes. Este modelo de infraestructura tecnológica permite contar con la característica de escalabilidad, de modo que pueda obtener y agregar más recursos cuando se requiera.

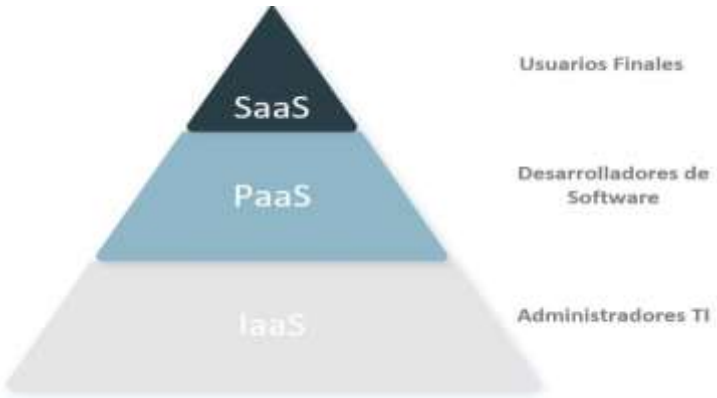


Figura 4: Pirámide Modelos Computación en la Nube Fuente: (Gleb, 2020)

2.6 Seguridad en la nube

Es una evolución de la seguridad informática, red e información, se basa en el conjunto de políticas de seguridad, tecnologías y controles implementados para la protección de los datos, aplicaciones e infraestructura tecnológica asociada a la computación en la nube.

El control de la seguridad en infraestructuras tecnológicas de computación en la nube no difiere mucho del control de seguridad de infraestructuras tecnológicas tradicionales. Sin embargo, puede presentar algunos nuevos riesgos debido a los modelos de servicio en la nube

empleados, procesos operativos y herramientas informáticas empleadas para habilitar los servicios informáticos en la nube, éstos riesgos suelen ser diferentes a los presentados en TI tradicionales (Hamouda, 2012).

2.6.1 Controles de seguridad en la nube

Una arquitectura de seguridad de una infraestructura de computación en la nube llega a ser efectiva al implementar defensas en los lugares correctos, reconociendo donde pueden aparecer determinados problemas, y estableciendo controles para proteger cualquier debilidad y disminuir el efecto de los ataques.

Existen varios tipos de controles detrás de una arquitectura en la nube, usualmente se pueden hallar en una de las siguientes categorías (Infotecs, 2019):

Controles disuasivos: Su objetivo es disminuir los ataques en una infraestructura de computación en la nube. Tienen el propósito de advertir a los atacantes potenciales que tendrán consecuencias negativas si prosiguen con el ataque.

Controles preventivos: Fortalecen el sistema frente a incidentes, disminuyendo o eliminando las vulnerabilidades. Proveen autenticaciones sólidas de los usuarios, lo que reduce la posibilidad de que usuarios no autorizados accedan al sistema y mejorando su identificación.

Controles de detección: Está diseñados para identificar y responder apropiadamente ante incidentes de seguridad. El monitoreo de la seguridad en la red y del sistema incluyen configuraciones para detectar y prevenir intrusos, generalmente son utilizados para la detección de ataques en el sistema de computación en la nube y fortalecer a la infraestructura tecnológica.

Controles correctivos: Disminuyen las consecuencias de un incidente generalmente evitando los daños. La reacción se produce mientras ocurre el ataque o después del mismo.

Comúnmente están diseñados para para restablecer el sistema comprometido por medio de buckups, garantizando la continuidad de negocio (copias de respaldo).

2.6.2 Ventajas de las seguridades en la computación en la nube

Las ventajas de la seguridades en la computación en la nube son (Hamouda, 2012):

- Tolerancia a fallos y fiabilidad.
- Soluciones de recuperación de desastres y almacenamiento de datos a bajo costo.
- Protección del hipervisor contra ataques de red.
- Particionamiento y replicación de datos.
- Mejora de la resiliencia.

Capítulo III

Análisis Situacional de los Recursos Tecnológicos

El análisis situacional de los recursos tecnológicos fue realizado en las instalaciones de la Dirección General de Inteligencia, donde se categorizó en activos tecnológicos tangibles e intangibles de la institución, para cumplir los siguientes objetivos:

- Clasificar los activos tecnológicos tangibles según sus características, mismos que se reutilizaran para este proyecto.
- Inventariar los activos intangibles de software: sistemas operativos, aplicativos y los servicios tecnológicos que cuenta la institución.
- Realizar el diagrama de topología de red física que se encuentra implementada en las instalaciones.

Para realizar este proceso se dividió en tres grupos: Hardware de TI, Software de Infraestructura y computadores.

Hardware de TI: Equipos tecnológicos tangibles en la organización:

- Servidores.
- Equipos de Redes de Comunicación.
- Computadores.

Software de Infraestructura: Activos intangibles, sistemas operativos de los servidores y servicios que están disponibles en la organización:

- Sistema Operativo de los Servidores y Servicios.

Software de Computadores: Estaciones de trabajo que se conectan a la red interna de la organización:

- Sistema Operativo.
- Aplicaciones de Ofimática.
- Aplicaciones de Seguridad.

3.1 Inventario de Hardware de TI

En el presente trabajo de tesis, fueron identificados los activos tangibles tecnológicos que conformaban la infraestructura tecnológica en ese momento y también fue considerado el hardware de una infraestructura tecnológica de un proyecto que se encontraba fuera de servicio. Estos recursos de hardware y software fueron utilizados para el diseño e implementación de una infraestructura tecnológica de computación en la nube IaaS. Se clasificaron en dos tipos de equipos: Servidores y Equipos de Redes de Comunicación, como se describen en la siguiente tabla resumen.

Tabla 1: Resumen de Servidores. Fuente: Elaboración propia.

Descripción del Servidor	Cantidad	CPU	RAM (GB)	Almacenamiento (TB)
Servidor IBM X3550 M4	3	24	32	4

Servidor HP Proliant DL380 G10	1	32	64	8
Servidor HP Proliant DL380 G8	1	24	64	4

Tabla 2: Resumen Equipos de Redes de Comunicación. Fuente: Elaboración propia.

Descripción Switches	Cantidad	# Puertos	Agregación de enlaces (LACP)	Protocolo de árbol de extensión (STP)
Cisco SG300-24	6	24	802.3ad	802.1d, 802.1w

Fue realizado el inventario de los computadores que formaban parte de la organización y que accedían a los servicios de la infraestructura tecnológica, también se verificaron si estos computadores contaban con las características necesarias para formar parte de un esquema de directorio activo, que serviría para el control de acceso, compartimentación de la información y gestión de políticas de seguridad a las estaciones de trabajo de los usuarios.

Tabla 3: Resumen de Computadores. Fuente: Elaboración propia.

Descripción Computador	Cantidad	CPU	RAM (GB)	Almacenamiento (TB)
Dell Vostro 3470	14	i3	4	1
Dell Inspirion 2350	20	i7	8	1
HP Envy	20	i7	8	2

3.2 Inventario de Software de Infraestructura

Este inventario de activos intangibles tiene como objetivo: identificar los distintos tipos de Sistemas Operativos y los servicios disponibles en la infraestructura tecnológica, para la virtualización y migración a la infraestructura tecnológica de computación en la nube IaaS propuesta.

Tabla 4: Resumen Software de Infraestructura. Fuente: Elaboración propia.

Descripción del Servicio	Sistema Operativo	Cantidad	CPU	RAM (GB)	Almacenamiento (TB)

Servidor de Archivos FTP	Windows Server 2003	1	4	16	2
Servidor de Correo Electrónico	Centos 6	1	4	16	2
Servidor de Respaldos Correos	Centos 7	1	4	8	3
Servidor de Respaldos de Archivos	Centos 7	1	4	8	3

Tabla 5: Resumen Software Computadores. Fuente: Elaboración propia.

Sistema Operativo / Aplicaciones	# Licencias
Windows 10 Professional	50
Office 2016 Professional	50
Antivirus	50

3.3 Diagramas de Topología de Red Física

En el siguiente diagrama se muestra el diagrama de la topología de red física que se encontraba implementada en la organización.

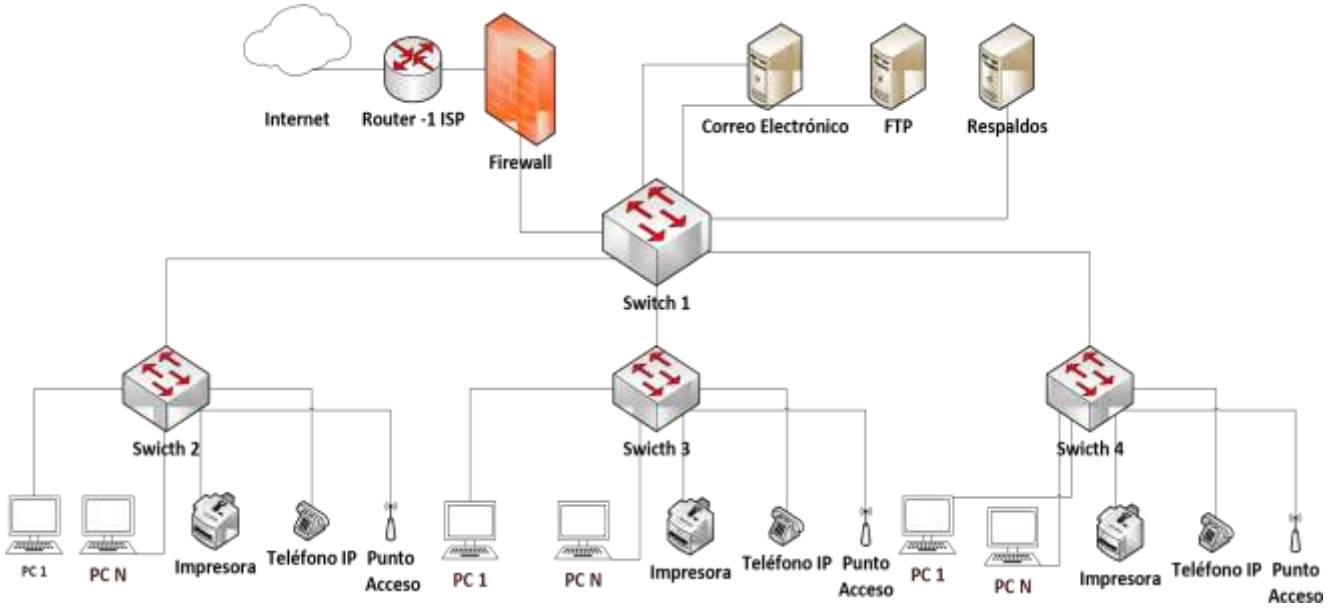


Figura 5: Diagrama de Topología de Red Fuente: Elaboración propia.

3.4 Identificación Debilidades

La topología red con la que contaba la DGI no mostraba una segmentación de tráfico por VLAN, por lo tanto, era una topología red plana, esto provocaba latencia en las peticiones de los usuarios al momento de acceder a los servicios de la infraestructura.

Los equipos de redes de comunicación, no se encontraban configurados de manera óptima, por ejemplo, no aprovechaban todas las características de un Switch de capa tres: enlaces de redundancia, agrupación de puertos, configuración de VLAN's y puertos de seguridad.

La información que se encontraba en el servidor de archivo no estaba compartimentada por departamentos. Provocando una visibilidad total de la información que existe en el servidor y ocasionando la perdida de confidencialidad de la información en cada departamento de la Institución.

También fue evidenciado que no existían controles de acceso a la información, provocando desconfianza por parte de los usuarios, además la información estaba almacenada de una manera descentralizada.

No contaban con implementación de sistemas de detección de intrusos en las estaciones de trabajo y en el tráfico de red.

El firewall configurado por la parte técnica no cumplía con las características necesarias para la administración integral que necesita un dispositivo de seguridad perimetral.

Capítulo IV

Diseño de una infraestructura de computación en la nube privada (IaaS)

4.1 Características de la Infraestructura de computación en la nube

La infraestructura tecnológica basada en el paradigma de computación en la nube IaaS privada para la Dirección General de Inteligencia en sus fases de diseño e implementación fueron consideradas las siguientes características:

Escalabilidad: La infraestructura debe ser flexible, para su escalabilidad en hardware y software.

Seguridad: Debe contar con medidas y herramientas de seguridad.

Administración: Fácil administración de los recursos, para el departamento de TI.

Virtualización: Permita la virtualización del recurso tecnológico por medio de software.

Disponibilidad: Diseñar una infraestructura de alta disponibilidad.

Propiedad: La infraestructura tecnológica física y virtual es de propiedad de la organización.

4.2 Dimensionamiento de la Infraestructura Tecnológica

Tomando en cuenta las características que debe cumplir la infraestructura, fue realizado el dimensionamiento de la capacidad total en almacenamiento, procesamiento y memoria, considerando un crecimiento de nuevos recursos virtuales implementados y el crecimiento de la información almacenada en la organización para dos años.

4.2.1 Dimensionamiento para los Servicios Virtuales

En base al análisis situacional, se identificaron los principales servicios tecnológicos con los que cuenta actualmente la organización y las características de los recursos de hardware. A continuación, se muestra una comparativa de los recursos asignados/utilizados según su procesamiento, memoria y almacenamiento, para los servicios tecnológicos en la organización.

Tabla 6: Resumen de Recursos Hardware Asignados/Utilizados. Fuente: Elaboración propia.

Descripción del Servicio	Sistema Operativo	# CPU	RAM (GB) Asignado	RAM (GB) Utilizado	Almacenamiento (TB) Asignado	Almacenamiento (TB) / Utilizado
Servidor de Archivos FTP	Windows Server 2003	4	16	8	2	1
Servidor de Correo Electrónico	Centos 6	4	16	12	2	1
Servidor de Respaldos Correos	Centos 7	4	8	6	3	1
Servidor de Respaldos de Archivos	Centos 7	4	8	6	3	1
Total de Recursos Asignados		16	48	32	10	4

4.2.2 Dimensionamiento de la Infraestructura tecnológica de computación de la nube (IaaS).

En los servidores físicos asignados para este proyecto fue instalado un hipervisor, el cual permite mediante software la virtualización y gestión de máquinas virtuales. Los servidores trabajan de manera conjunta como clúster, un solo recurso informático de mayor capacidad en procesamiento, almacenamiento y memoria. En las siguientes tablas se especifican las características técnicas de las capacidades del clúster de la infraestructura tecnológica.

Tabla 7: Característica en procesamiento. Fuente: Elaboración propia.

Descripción del Servidor	# CPU Físicos	# CPU Lógicos	Velocidad CPU (GHz)	Capacidad CPU (GHz)
Servidor IBM 1	12	24	2	24
Servidor IBM 2	12	24	2.1	25.2
Servidor IBM 3	12	24	2	24

Servidor HP 3	32	64	2.1	67.2
Servidor HP 4	12	24	2	24
Características de procesamiento	80	160	10.2	164.4

Tabla 8: Características de almacenamiento. Fuente: Elaboración propia.

Descripción del Servidor	**Almacenamiento (TB)**
Servidor IBM 1	2
Servidor IBM 2	1
Servidor IBM 3	1
Servidor HP 3	8
Servidor HP 4	4
Características de Almacenamiento	16

Tabla 9: Características de memoria. Fuente: Elaboración propia.

Descripción del Servidor	**Memoria RAM (GB)**
Servidor IBM 1	24
Servidor IBM 2	16
Servidor IBM 3	16
Servidor HP 3	64
Servidor HP 4	32
Características de Memoria	152

Para este proyecto fue necesario enumerar las interfaces de red que tiene disponibles cada servidor físico con sus características de velocidades de transmisión de datos, que fueron configuradas y asignadas para las funciones de conectividad y disponibilidad, para la distribución de los servicios tecnológicos a los usuarios en la organización.

Uno de los aspectos más fundamentales de una infraestructura tecnológica son las redes de comunicación, éstas permiten que las aplicaciones y los sistemas se encuentren comunicados, ofreciendo los servicios tecnológicos a los usuarios de la organización. En la siguiente tabla se

muestra las interfaces de red disponibles en cada servidor físico y sus características de velocidades y los estándares soportados para sus configuraciones.

Tabla 10: Características de las interfaces de red. Fuente: Elaboración propia.

Descripción del Servidor	# NIC´s	Tasa de Transferencia de Datos	Estándares IEEE
Servidor IBM 1	4	1000 Base-X (Full Dúplex)	802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, IEEE 802.1Q VLAN, 802.3x Control Flujo
Servidor IBM 2	4	1000 Base-X (Full Dúplex)	802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, IEEE 802.1Q VLAN, 802.3x Control Flujo
Servidor IBM 3	4	1000 Base-X (Full Dúplex)	802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, IEEE 802.1Q VLAN, 802.3x Control Flujo
Servidor HP 3	4	2000 Base-X (Full Dúplex)	802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, IEEE 802.1Q VLAN, 802.3x Control Flujo
Servidor HP 4	4	2000 Base-X (Full Dúplex)	802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, IEEE 802.1Q VLAN, 802.3x Control Flujo
# Interfaces de Red	20		

4.3 Diseño de una infraestructura de computación en la nube privada

Para el diseño de la infraestructura se consideró el siguiente modelo de infraestructura como servicio (IaaS) privado, el cual está compuesto por cinco servidores físicos, un servidor maestro, cuatro servidores configurados como nodos. El servidor maestro es el encargado de orquestar las máquinas virtuales que se encuentran alojados en los servidores nodos, como se muestra en el siguiente diagrama.

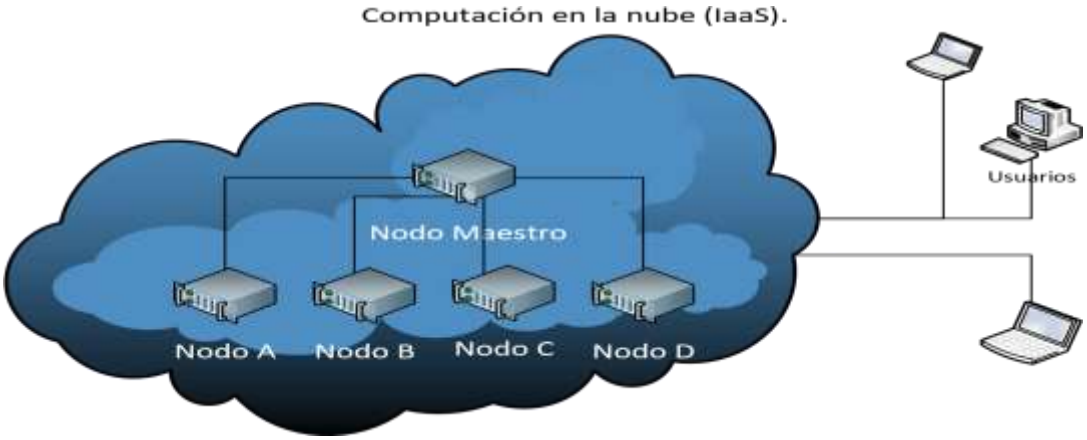


Figura 6: Diagrama de las Conexiones de los Servidores físicos. Fuente: Elaboración propia.

4.3.1 Configuración del clúster

La configuración de un clúster de varios hosts proporciona a la infraestructura tecnológica una gran capacidad de procesamiento, memoria, almacenamiento y red para un entorno. El clúster protege a las máquinas virtuales contra fallos de los servidores físicos habilitando características como: HA (Alta disponibilidad), DRS (Programa de Recursos Compartidos), Migración en Caliente, Tolerancia a fallos. Todas estas funciones del clúster contribuyen a la distribución de los recursos entre los hosts y la tolerancia de la infraestructura contra fallos.

- **Administración de Máquinas Virtuales:** Permite agregar, eliminar o modificar máquinas virtuales de la infraestructura tecnológica, también permite asignación de recursos en caliente, cuando la máquina virtual se encuentra en funcionamiento.
- **Migración en Caliente:** Permite mover las máquinas virtuales entre dos hosts físicos del clúster, sin necesidad de apagarlas.
- **Alta Disponibilidad (HA):** Realiza un monitoreo del estado de las máquinas virtuales y en caso de que una máquina virtual no pueda iniciar en un host, lo inicia desde otro host del clúster.

- **Programación de Recursos Distribuidos (DRS):** Balancea o equilibra la carga de esfuerzo de manera automática evitando la contención de los recursos de hardware, los cual permite equilibrar las máquinas virtuales dentro del clúster.
- **Tolerancia a fallos:** Permite configurar dos máquinas virtuales similares en host distintos del clúster. Si una de las máquinas virtuales llegara a fallar, la otra máquina virtual tiene la capacidad de continuar con el servicio como si se tratara de la máquina virtual principal.

El objetivo principal del clustering es conseguir un alto rendimiento, disponibilidad y balanceo de carga en el procesamiento de información realizado por el centro de datos de la organización. Esta configuración permite a un centro de datos disponer con escalabilidad en la infraestructura tecnológica para agregar o quitar hosts al clúster del centro de datos. El clúster puede formarse con pocos o muchos hosts con el fin de ofrecer redundancia y resiliencia a la infraestructura tecnológica en el caso de daños físicos del hardware o perdidas de conectividad en la red.

En el siguiente diagrama de red física se muestra la conectividad de los servidores y los equipos de red, para la configuración del clúster en la infraestructura tecnológica.

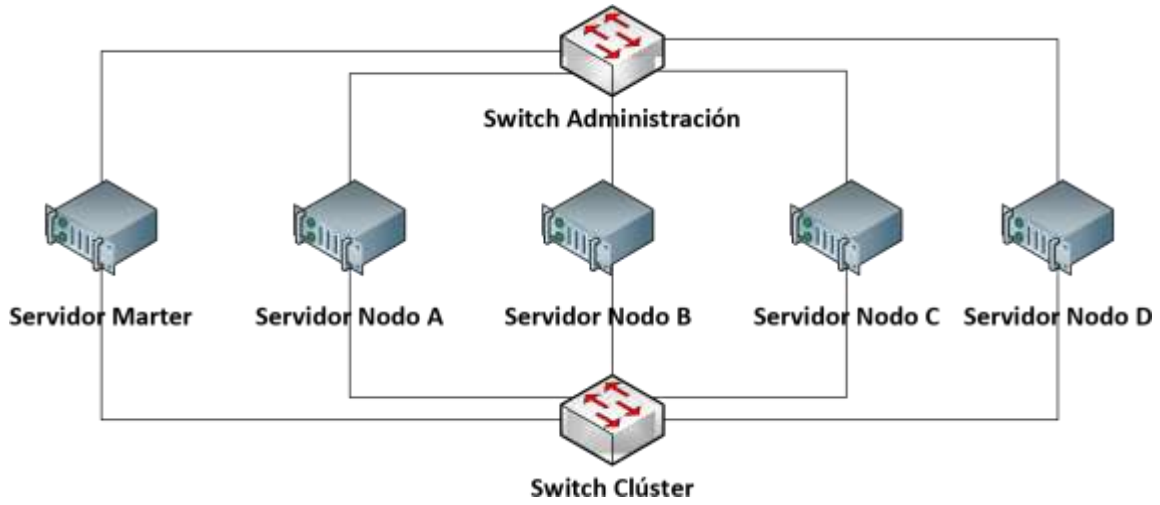


Figura 7: Diagrama de Red Físico del Clúster. Fuente: Elaboración propia

4.4 Arquitectura de la Infraestructura tecnológica de Computación en la Nube

Para la implementación de una infraestructura tecnológica de computación en la nube privada IaaS, los componentes de software que fueron considerados son OpenStack y VMWare vSphere ESXi.

La siguiente figura muestra el diagrama de la arquitectura de las herramientas.

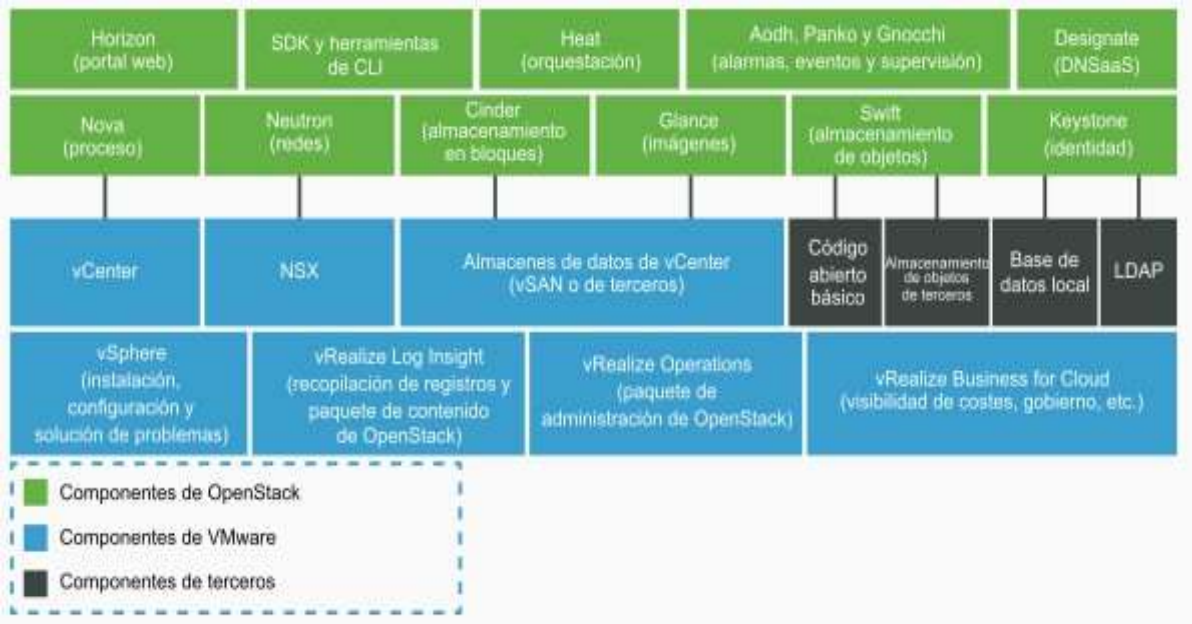


Figura 8: Arquitectura de las herramientas OpenStack y VMware. Fuente: (VMware, 2020b).

4.4.1 Componentes OpenStack

Los principales componentes de OpenStack son: Componente de Infraestructura computacional, Almacenamiento de Objetos e imágenes y Servicios de red (Hinojosa & Ulloa, 2014).

- **Horizon**: Servicio de tablero, proporciona una interfaz web para la administración de todos los servicios de OpenStack (Guerrero, n.d.).

- **Nova:** Servicio de infraestructura computacional encargado del almacenamiento y recuperación de imágenes de discos virtuales y recursos asociados al servicio de Glance; y asigna recursos necesarios para su ejecución (Hinojosa & Ulloa, 2014).
- **Glance:** Servidor de imágenes encargado del almacenamiento y recuperación de discos virtuales activos en el Swift (Hinojosa & Ulloa, 2014).
- **Swift:** Servicio de almacenamiento de objetos, proporciona almacenamiento de imágenes y copias de seguridad (Guerrero, n.d.).
- **Keystone:** Servicio de panel de control, utilizado para la autenticación de todos los servicios mediante un ID y contraseña única para el acceso a sus recursos (Hinojosa & Ulloa, 2014).
- **Cinder:** Servicio de bloque de almacenamiento, encargado de la gestión y aprovisionamiento de volúmenes a la instancia y copias de seguridad (Guerrero, n.d.).
- **Neutron:** Servicio de Red, maneja las redes y direcciones IP para la conectividad entre los servicios de OpenStack (Hinojosa & Ulloa, 2014).
- **Ceilometer:** Servicio de telemetría, para la medición y uso de la nube (Hinojosa & Ulloa, 2014).
- **Heat:** Servicio de Orquestación, encargado de la organización y coordinación de las plantillas predefinidas de acuerdo a las aplicaciones requeridas por el usuario (Hinojosa & Ulloa, 2014).

4.4.2 Componentes VMware.

VMware está conformado por los siguientes componentes:

- **ESXi vSphere:** Sistema operativo que se instala en los servidores físicos, es el hipervisor encargado de la administración de las instancias de máquinas virtuales (VMware Docs, 2019).
- **vCenter:** Servicio de infraestructura computacional, actúa como administrador central para los host VMware conectados a una red (VMware Docs, 2019).
- **NSX:** Servicio de red, ofrece conectividad integral y generalizada para las aplicaciones y los datos (vmware, 2020).
- **Almacenes de datos vCenter:** Área de almacenamiento persistente, mantiene el estado de cada máquina virtual, host y usuario administrados en el entorno de vCenter Server (VMware Docs, 2019).
- **VMware vRealize Suite:** Plataforma de gestión de nubes, herramientas NSX o vSAN y herramientas de terceros como Amazon Web Service (AWS), OpenStack, etc., compuesto por cuatro productos (Serrano, 2018):
    - vRealize Automation: Automatización de procesos, incluye el orquestador vRealize Orchestrator.
    - vRealize Operations Manager: Administración de operaciones en la nube.
    - vRealize Business for Cloud: Gestión de medición de uso de la nube ○ vRealize Log Insight: Administración de logs.

4.5 Diseño de las Redes de Comunicación

Para el diseño del diagrama de topología de red de la infraestructura tecnológica de computación en la nube (IaaS) fue considerada la integración del clúster con el orquestador de las

máquinas virtuales, para esto se requirió la asignación de varios segmentos VLAN´s[3] independientes, encargadas de proporcionar seguridad y segmentar el tráfico de red, limitando la comunicación entre puertos de un segmento de VLAN con otros puertos de un segmento diferente de red o VLAN.

Las VLAN ‘s que se consideraron son las siguientes: VLAN de Administración, VLAN de Zona Desmilitarizada (DMZ), VLAN Intranet, VLAN del Departamento de Análisis de la Información (DAI), VLAN de la Dirección General Inteligencia (DGI), VLAN de Servicios y VLAN del Departamento de Tecnologías (TIC´s). En la siguiente tabla se describe los segmentos de red VLAN’s configuradas en la infraestructura tecnológica de la Dirección General de Inteligencia.

Tabla 11: Tabla Descriptiva de la Segmentación de Red Infraestructura Tecnológica. Fuente: Elaboración propia.

VLAN	Descripción
VLAN vKernel	Segmento de red asignado para la administración y configuración del clúster de host físicos del centro de datos.
VLAN vMotion	Segmento de red asignado para la migración de las máquinas virtuales en caliente entre host físicos, Programación de Recursos Distribuidos (DRS), Alta Disponibilidad configuración de máquinas virtuales para Alta Disponibilidad (HA).
VLAN DMZ	Segmento de red asignado para el servicio de correo electrónico de la organización.
VLAN DAI	Segmento de red asignado para el acceso y distribución de los servicios a los usuarios del Departamento de Análisis de la Información.
VLAN DGI	Segmento de red asignado para el acceso y distribución de los servicios a los usuarios del Departamento de la Dirección General de Inteligencia.
VLAN TIC	Segmento de red asignado para la administración de la infraestructura tecnológica, control y monitoreo de los servicios, acceso a los servicios de la infraestructura tecnológica del Departamento de TIC`s.
VLAN ADMIN	Segmento de red asignado para la administración del aplicativo de la infraestructura

[3] **VLAN:** Es la representación lógica de un segmento de red, que son configurados en dispositivos de comunicaciones Switch, permite la conectividad de varios host y servidores en una organización, son utilizadas para la representación lógica de un grupo de usuarios, que son parte de un departamento, las VLAN´s proporcionan segmentación de tráfico de datos en una topología de red, aislando el tráfico generado por departamentos, disminuyendo el tiempo de respuesta para solicitudes de acceso al medio, manteniendo la disponibilidad y mejorando el rendimiento en una red de comunicaciones.

	tecnológica.
VLAN SERVICIOS	Segmento de red asignado para los servicios que son publicados en la infraestructura tecnológica de computación en la Nube (IaaS).

Nota: *Los nombres de las VLAN's son los acrónimos de los departamentos y servicios que se necesitan de manera descriptiva para el desarrollo del documento, y no corresponden a los nombres que se encuentran configurados en producción.*

4.6 Diseño de la Topología de Red Jerárquica

La topología de red jerárquica está compuesta de 3 capas: núcleo, distribución y acceso. Las capas se encuentran interconectadas y es flexible para agregar nuevos nodos a la topología de red, para la conexión de más dispositivos host. Existen dos tipos de topología en árbol: la topología de árbol binario, donde cada nodo se divide en dos enlaces y la topología de árbol backbone, en el cual un tronco backbone tiene nodos ramificados con enlaces redundantes que surgen de cada nodo.

- **Capa de núcleo o core:** Se encarga de dirigir el tráfico de red por enlaces de alta velocidad para los servicios que pueden ser internos o externos a la organización, este tráfico es dirigido y transportado para los usuarios de la organización.
- **Capa de Distribución:** Se encuentra entre las capas de núcleo y acceso, encargada del enrutamiento, acceso y filtrado. Esta capa es el punto de concentración de los dispositivos de la capa de acceso, ayuda a segmentar el tráfico de los distintos departamentos de la organización, proporcionar servicios de seguridad y filtrado.

- **Capa de Acceso:** Encargada de la conexión de los hosts a la red de la organización, en esta capa se puede encontrar múltiples grupos de usuarios con sus recursos correspondientes y el tráfico generado por esta capa es dirigido por la capa de distribución.

Para el diseño del diagrama de topología de red jerárquica fue considerado la asignación de los enlaces redundantes para la capa de núcleo o core y la capa de distribución, enlaces troncales por fibra óptica y agrupación de puertos. El diseño fue realizado en base a las características que soportan los equipos de redes de comunicación como se muestra en el siguiente diagrama.

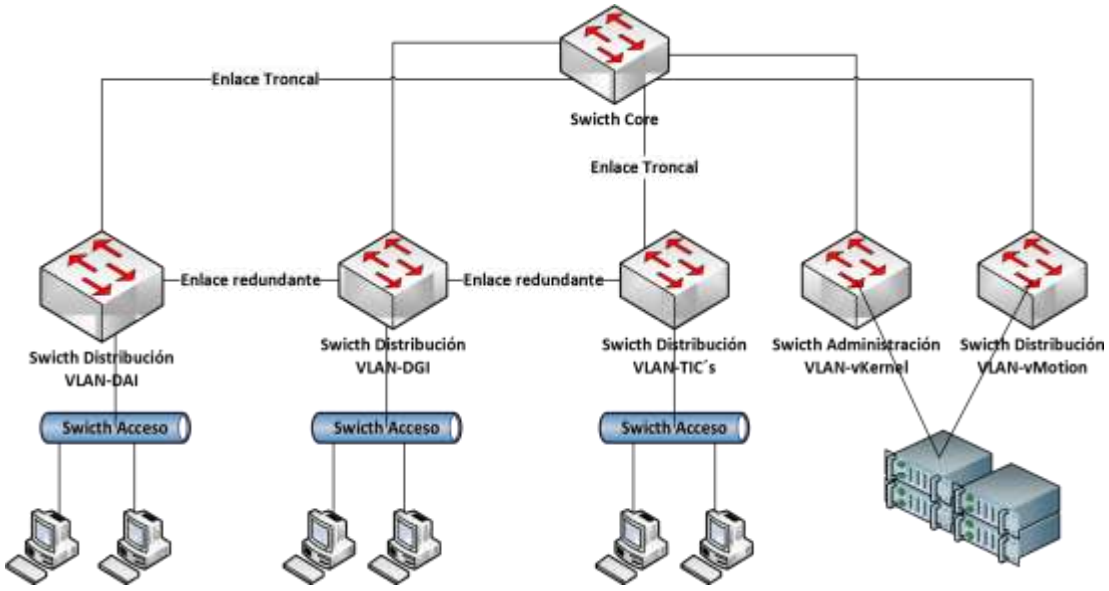


Figura 9 Diseño de Topología de Red Jerárquica. Fuente: Elaboración propia.

4.7 Diseño del Diagrama General de la Topología de la Red Física

El diseño de la topología de red física para la infraestructura tecnológica de computación en la nube (IaaS) privada, fue realizado considerando los dispositivos de seguridad firewall en los principales segmentos de red en esta topología. En el siguiente diagrama muestra el diseño de la topología de red física general.

Nota: *El diagrama general de topología de red física, muestra los servicios básicos para la implementación de este tipo de infraestructura tecnológica, los diagramas de topología reales de la infraestructura tecnológica son entregados en informes clasificados como secretos y manejados por técnicos de la Dirección General de Inteligencia.*

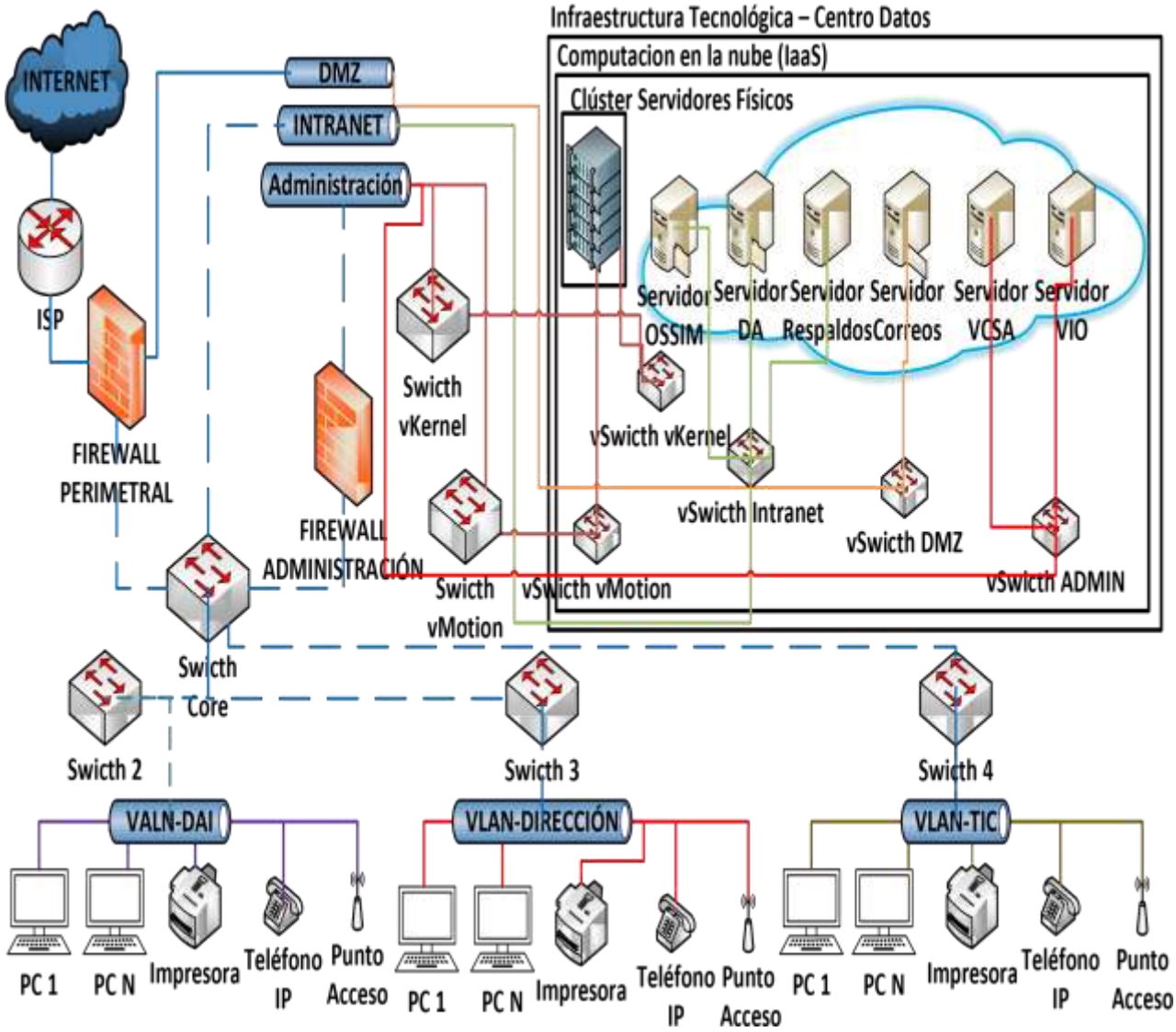


Figura 10: Diseño del diagrama de topología de red física. Fuente: Elaboración propia.

Capítulo V

Implementación de la infraestructura tecnológica de computación en la nube IAAS 5.1 Selección de los componentes de Software que Integran la Infraestructura Tecnológica

El software que fue seleccionado para la implementación y configuración de la infraestructura tecnológica es del fabricante. VMWare es un fabricante que cuenta con varios productos de plataformas de virtualización, usadas para la implementación de una infraestructura tecnológica de computación en la nube (IaaS).

5.1.1 Componentes de Software

VSphere 6.7 Enterprise: Sistema que proporciona la capa de virtualización y permitiendo que varias VMs alojadas en un host compartan los recursos de hardware.

VMware vCenter Server: vCenter Server proporciona funcionalidades de administración centralizada de toda la infraestructura tecnológica virtual y configuración de un clúster de varios hosts.

VMware Integrated OpenStack: Es la distribución de OpenStack para infraestructuras de virtualización VMWare, para la implementación y administración de infraestructuras tecnológicas de un modelo de computación en la nube privada (IaaS).

OpenStack es el sistema operativo de infraestructuras tecnológicas de computación en la nube, permite controlar y administrar grandes grupos de recursos informáticos de un centro de datos, todos los recursos son gestionados y aprovisionados mediante el uso de una aplicación.

5.2 Instalación y configuración del hipervisor VMware vSphere ESXi 6.7

Para la instalación y configuración del hipervisor en los servidores físicos que forman parte de la infraestructura tecnológica de computación en la nube, fue necesario seguir los pasos que del

asistente de VMWare y se configuró la interface de red para la administración, asignando una dirección IPv4. En la siguiente tabla se especifica las direcciones IPv4 utilizadas segmento de red VLAN vMKernel.

Tabla 12: Asignación de Direcciones IP VLAN vMKernel. Fuente: Elaboración propia.

Descripción del Servidor	Interface de Red	Dirección IPv4	Mascara de Red	Puerta de Enlace
Servidor IBM 1	Ethernet 0	192.168.10.1	255.255.255.240	192.168.10.14
Servidor IBM 2	Ethernet 0	192.168.10.2	255.255.255.240	192.168.10.14
Servidor IBM 3	Ethernet 0	192.168.10.3	255.255.255.240	192.168.10.14
Servidor HP 3	Ethernet 0	192.168.10.4	255.255.255.240	192.168.10.14
Servidor HP 4	Ethernet 0	192.168.10.5	255.255.255.240	192.168.10.14

Nota: *La información sobre las direcciones IP's que se encuentran plasmadas en este documento, no pertenecen al ambiente de producción, solo fueron usadas para el desarrollo de este documento.*

5.3 Diagrama de Red Lógico VLAN vKernel para la Administración de los Servidores Físicos

En el siguiente diagrama de red muestran las interfaces y las direcciones IPv4 que fueron asignadas para la configuración del segmento de red VLAN vMKernel y la administración del cada uno de los servidores físicos.

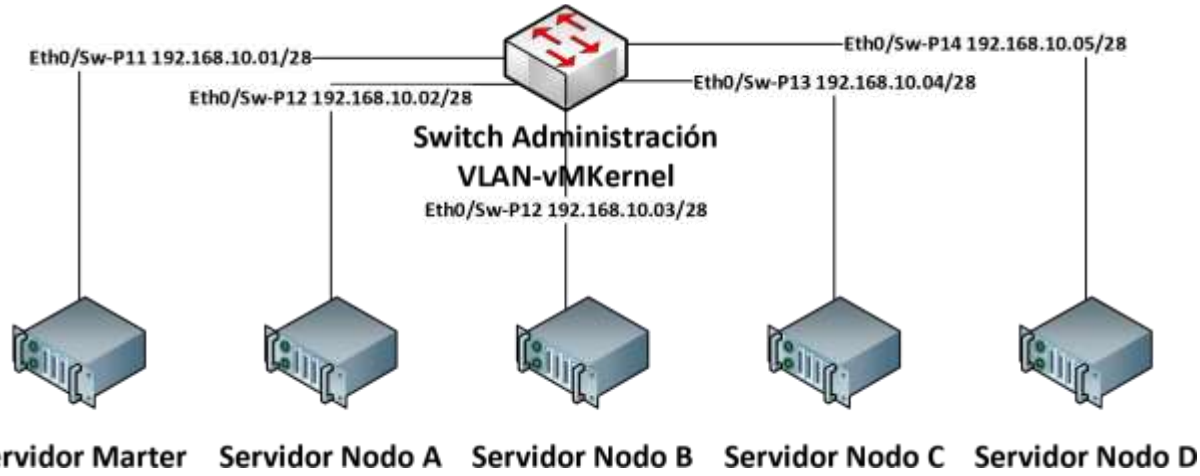


Figura 11: Diagrama de Red Lógico VLAN vMKernel. Fuente: Elaboración propia.

La instalación y configuración de la interface de red de administración de VMware vSphere 6.7 se detalla en el ANEXO 1.

En la siguiente imagen se muestra la interface web de vSphere, para administración y control del servidor físico.

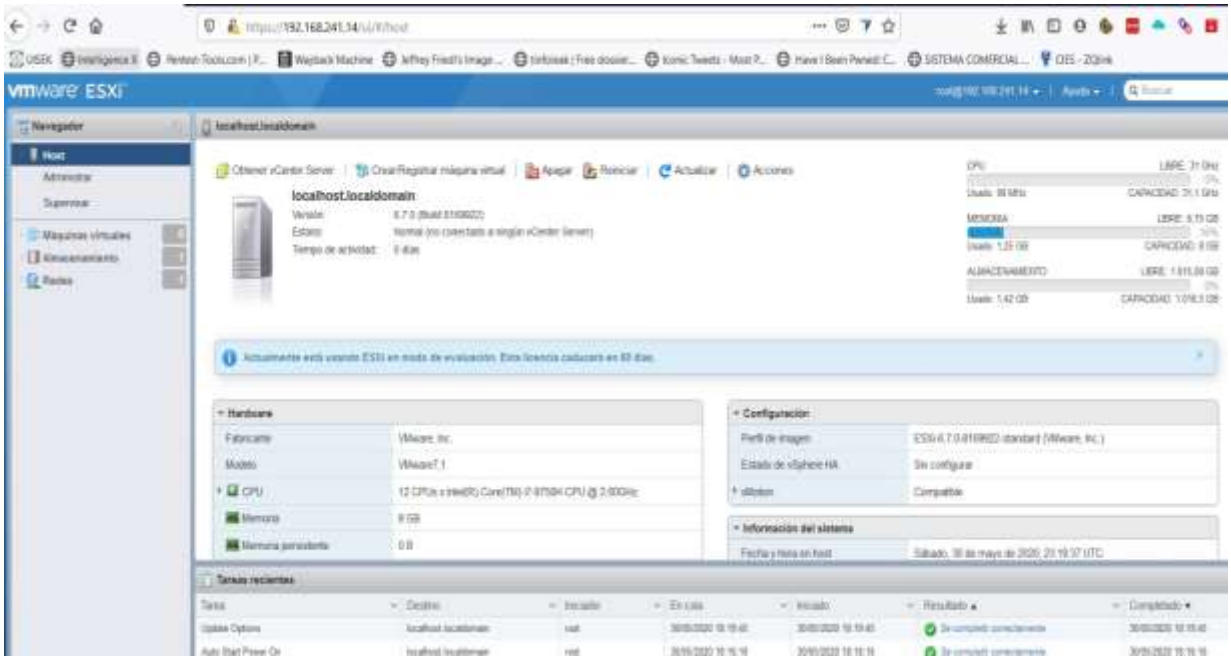


Figura 12: Interfaz Web de Administración VMware ESXi vSphere. Fuente: Elaboración propia.

5.4 Instalación y configuración del Servicio de VMware vCenter Server

El servidor vCenter fue implementado en un entorno Linux por su eficiencia y optimización de asignación de recursos, este servidor es distribuido en formato ova (Open Virtual Appliance).

El servidor de vCenter facilita la administración centralizada de varios host ESXi que se encuentran conectados a la red y permite la agrupación de varios hosts de ESXi vistos como un solo recurso informático de mayor capacidad de procesamiento, almacenamiento y memoria formando un clúster de host.

Mediante una interface web de manera centralizada se administran los hosts y máquinas virtuales, también se realiza el monitoreo y control de los recursos de procesamiento, almacenamiento y memoria del clúster de host de ESXi y de sus máquinas virtuales invitadas que se ejecutan en los equipos host físicos.

5.4.1 Requerimientos de Hardware

Los requerimientos para la implementación del servidor vCenter dependen de la cantidad de VMs y los hosts de ESXi que componen el clúster del centro de datos, en la siguiente tabla se especifica los requerimientos de hardware emitida por el fabricante VMware.

Tabla 13: Requerimientos de Hardware Servidor vCenter. Fuente: (VMware, 2020a)

Tamaño de Implementación	# CPU	RAM (GB)	Almacenamiento (GB)	# Host ESXi Máximo	# VM Máximo
Entornos Muy Pequeños	2	10	300	10	100
Entornos Pequeños	4	16	340	100	1000
Entornos Medianos	8	24	525	400	4000
Entornos Grandes	8	24	425	1000	10000
Entornos Extragrandes	8	24	425	2000	35000

La instalación y configuración del servidor virtual de vCenter se detalla en el ANEXO 2.

En la siguiente imagen se muestra la interface web de administración y control del servidor vCenter.

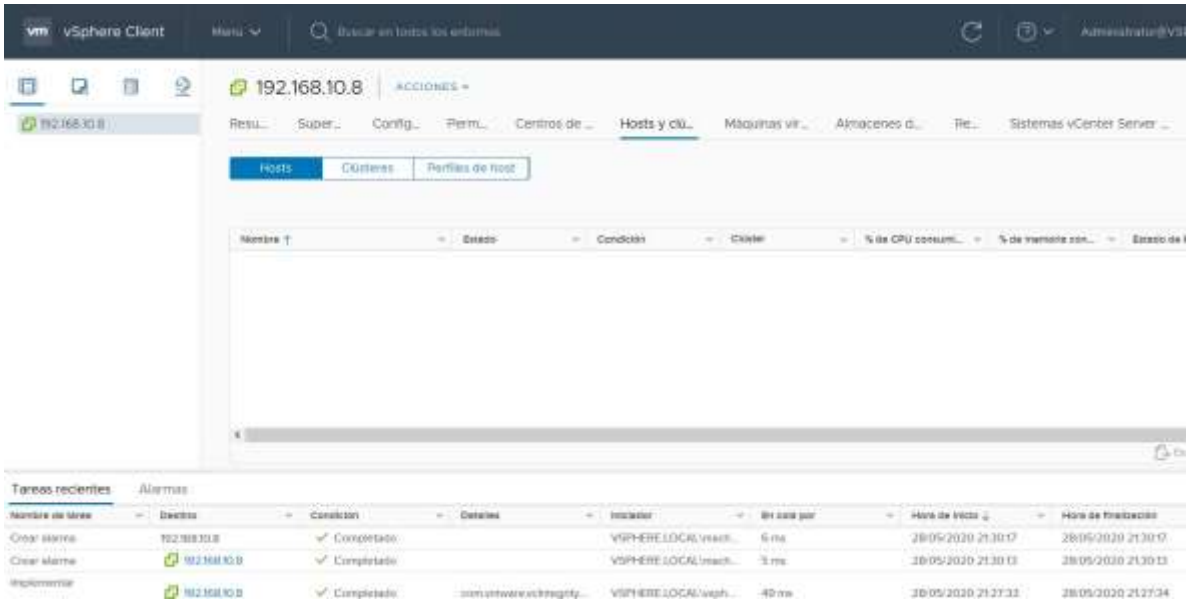


Figura 13: Interface Web de Administración del Servidor VMware vCenter. Fuente: Elaboración Propia.

5.4.2 Configuración del Clúster en el Servidor de vCenter.

Para la configuración del clúster de host ESXi desde la interface web de vCenter se identificaron los nodos ESXi, que proporcionan los recursos de hardware para la implementación y ejecución de las máquinas virtuales. Para las configuraciones del clúster de vSphere se asignó una interface de red física del servidor en un segmento de red completamente independiente, con una dirección ipv4. La siguiente tabla se especifica las direcciones IPv4 utilizadas segmento de red VLAN vMotion.

Tabla 14: Asignación de Direcciones IP VLAN vMotion. Fuente: Elaboración propia.

Descripción del Servidor	Interface de Red	Dirección IPv4	Mascara de Red	Puerta de Enlace
Servidor IBM 1	Ethernet 1	192.168.20.1	255.255.255.240	192.168.20.14
Servidor IBM 2	Ethernet 1	192.168.20.2	255.255.255.240	192.168.20.14
Servidor IBM 3	Ethernet 1	192.168.20.3	255.255.255.240	192.168.20.14
Servidor HP 3	Ethernet 1	192.168.20.4	255.255.255.240	192.168.20.14
Servidor HP 4	Ethernet 1	192.168.20.5	255.255.255.240	192.168.20.14

5.4.3 Diagrama de Red Lógico VLAN vMotion y VLAN vMkernel Clúster de vSphere

El siguiente diagrama de red se muestra las interfaces y las direcciones IPv4 asignadas en la configuración del segmento de red VLAN vMotion, para habilitar las características de clúster vSphere.

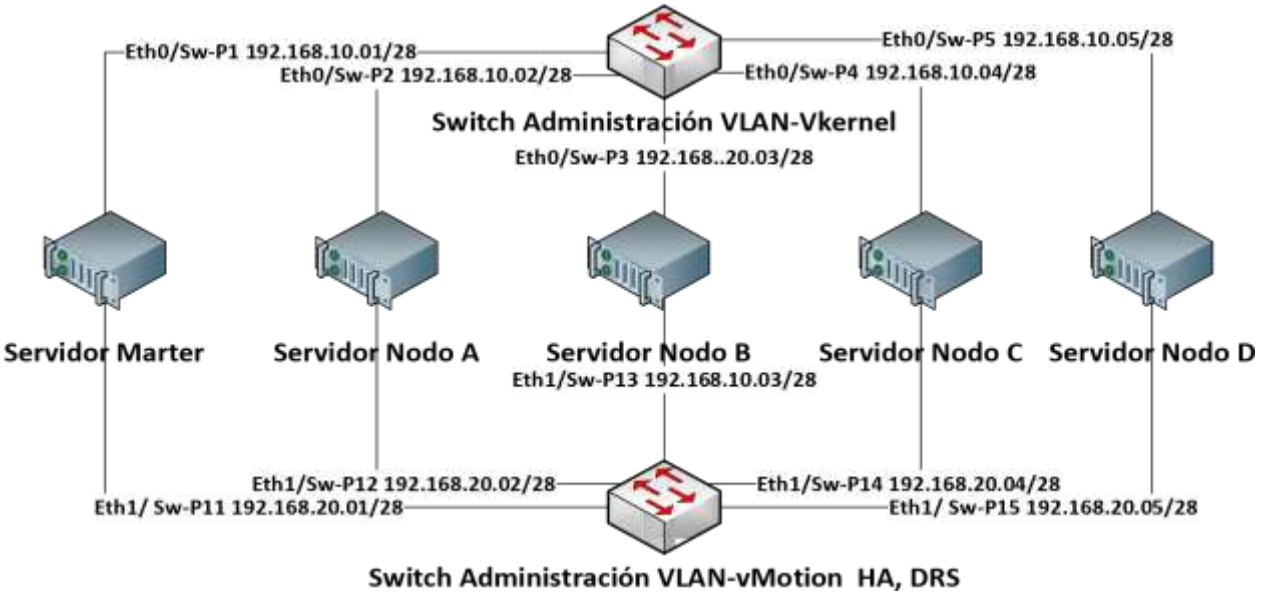


Figura 14: Diagrama de Red Lógico Clúster vSphere. Fuente: Elaboración propia.

La configuración del clúster de vSphere se detalla en el ANEXO 3.

En las siguientes imágenes se muestran las características de las capacidades del clúster de host ESXi.

Figura 15: Capacidad total del número de Cores. Fuente: Elaboración propia.

Figura 16: Capacidad de procesamiento, memoria y almacenamiento. Fuente: Elaboración propia.

5.5 Implementación y configuración VMware Integrated OpenStack

VMware Integrated OpenStack (VIO) fue implementado en el modo compacto, para lo cual fue necesario obtener el paquete OVA de VIO e instalarlo en el entorno vSphere y los componentes de OpenStack fueron configurados mediante OpenStack Manager.

5.5.1 Requerimientos de implementación

Para la implementación de VMware Integrated OpenStack en su modo compacto fue necesario basarse en los requerimientos de hardware emitida por el fabricante VMware, estos requisitos dependen de la cantidad de máquinas virtuales utilizadas para cada componente. El modo compacto consiste en la **"**configuración de 1 máquina virtual (sin incluir el controlador de proceso y el servidor de administración OpenStack - OMS)" (VMware, 2018). Los requerimientos de hardware se detallan en la siguiente tabla:

Tabla 15: Requerimientos Hardware modo compacto Fuente: (VMware, 2018)

Componente	VMs	CPU	RAM(GB)	Espacio en disco (GB)
Administrador de OpenStack integrado (OMS	1	2 (2 por VM)	4 (4 por VM)	25 (25 por VM)
Controladores	1	8 (8 por VM)	16 (16 por VM)	80 (80 por VM)
Servicio de cómputo (Nova CPU)	1	2 (2 por VM)	4 (4 por VM)	20 (20 por VM)
TOTAL (Sin incluir DHCP)	3	12	24	120

La instalación y configuración del VMware Integrated OpenStack se detalla en el ANEXO 4.

Capítulo VI

Implementación y configuración de las redes de comunicación

La red de comunicación de la infraestructura tecnológica que fue implementada y configurada en la organización se encuentra compuesta por Switches físicos y virtuales, los Switches virtuales son los encargados de la comunicación entre las máquinas virtuales, mientras los Switches físicos son los encargados de la comunicación de los equipos host de usuarios con los servicios tecnológicos dentro de la organización.

6.1 Implementación de la topología de red lógica de los servicios.

La infraestructura tecnológica de computación en la nube (IaaS) proporciona dispositivos virtuales para las comunicaciones entre las máquinas virtuales dentro de uno o varios host ESXi, existen dos tipos de dispositivos de Switches virtuales los cuales son: Switch estándar y Switch distribuido.

Switches virtuales estándar

El Switch estándar es configurado de manera virtual en un solo host de ESXi, al cual se le asigna un grupo de puertos para el tráfico de red también llamados portgroups, este tipo de dispositivos virtuales se configura de manera repetitiva en cada host ESXi.

Switches virtual distribuido

Se configura un Switch virtual para el centro de datos completo, la configuración se lo realiza por vCenter y no en el host ESXi.

En la siguiente tabla se especifica los tipos de Switches virtuales y los segmentos de red VLAN`s asignados para la configuración de las comunicaciones dentro de la infraestructura tecnológica virtual.

Tabla 16: Tabla descriptiva de Switches virtuales. Fuente: Elaboración propia.

Tipo Dispositivo Virtual	VLAN Asignada	NIC	Descripción
Switches Virtual Estándar	**VLAN vKernel**	**Ethernet 0**	Switch Virtual Estándar fue utilizado para la administración de un host ESXi vSphere, se configura de manera predeterminada cuando se realiza la instalación del hipervisor.
Switches Virtual Distribución	**VLAN vMotion**	**Ethernet 1**	Switch Virtual Distribución, este dispositivo fue utilizado para todos los host ESXi que conforman el clúster, para habilitar las funcionalidades de DRS, HA del clúster.
Switches Virtual Estándar	**VLAN ADMIN**	**Ethernet 1**	Switch Virtual Estándar, este dispositivo fue utilizado para las aplicaciones de administración de la Infraestructura Tecnológica de computación en la nube (IaaS).
Switches Virtual Distribución	**VLAN-DAI, VLAN-DGI, VLAN TIC, VLAN SERVICIOS**	**Ethernet 2**	Switch Virtual Distribución, este dispositivo fue utilizado para los servicios: Servicio de Directorio Activo, Servicio de Correo Electrónico, Aplicaciones de Administración TIC.
Switches Virtual Estándar	**VLAN DMZ**	**Ethernet 4**	Switch Virtual Estándar fue utilizado para el segmento de red DMZ, zona desmilitarizada utilizada para la publicación de servicio de correo electrónico al internet.

En el siguiente diagrama de topología de red lógica se especifica las conexiones de los servicios y los Switches virtuales que se ejecutan de manera virtual en la infraestructura tecnológica de computación en la nube (IaaS).

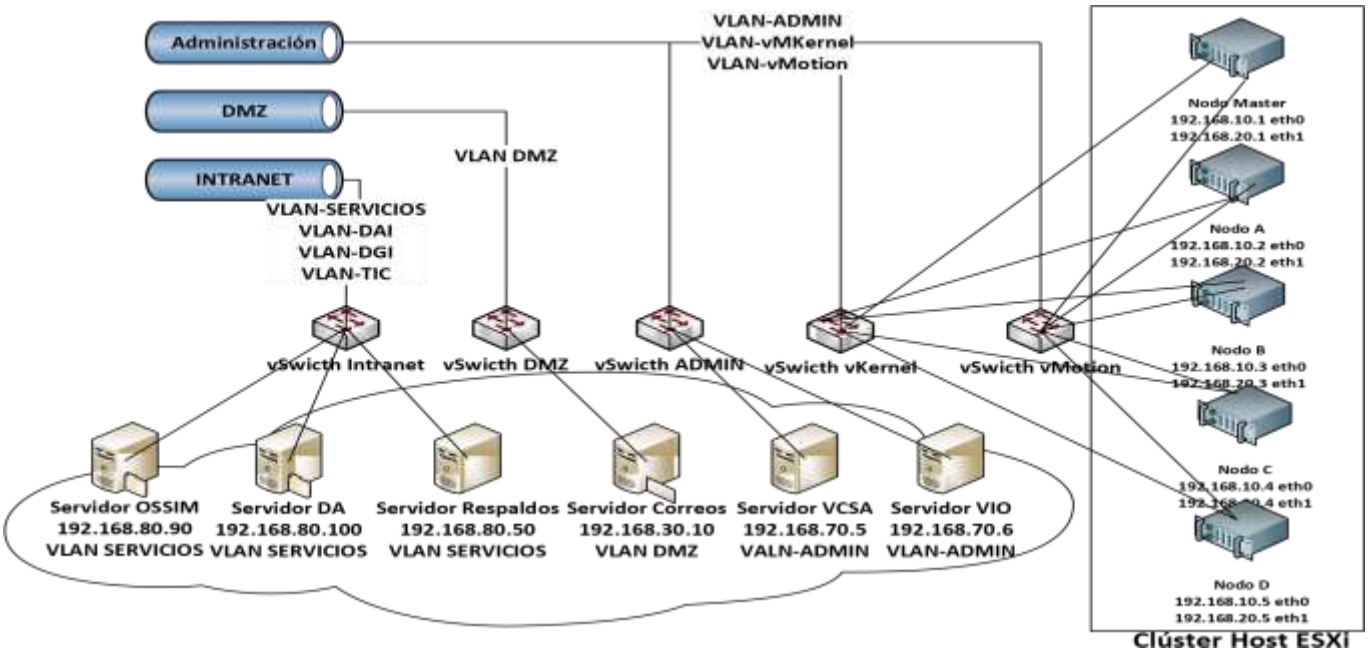


Figura 17: Diagrama de Topología de Red Lógica de Servicios. Fuente: Elaboración propia.

Nota: *Las direcciones IP's que se encuentran plasmadas en el diagrama de topología de red lógica de servicios, no pertenecen al ambiente de producción, solo fueron usadas para el desarrollo de este documento de tesis.*

6.2 Implementación de la topología de Red Lógica Jerárquica.

Esta topología de red está compuesta por Switches físicos encargados de la comunicación interna en la organización y permiten el acceso de los usuarios a los servicios que son publicados por la infraestructura tecnológica virtual (IaaS).

La topología de red jerárquica de 3 capas está compuesta por la capa de Core, capa de distribución y capa de acceso. Para mejorar la disponibilidad ante algún fallo en el enlace principal, fueron configurados enlaces redundantes entre los Switches. La implementación de la red jerárquica en la organización también permitió contar con escalabilidad horizontal al momento

de agregar nuevos dispositivos Switches, para el acceso de nuevos host o usuarios a la infraestructura tecnológica.

Capa de Núcleo: Está compuesto por un Switch de alta velocidad de datos y enlaces troncales, encargado de direccionar el tráfico interno y externo de la organización, los enlaces troncales se encuentran conectados a la capa de distribución, a la infraestructura tecnológica de computación en nube (IaaS) y al Firewall de seguridad perimetral.

Enlaces Troncales: En los dispositivos de redes de comunicación de la organización fueron configurados enlaces troncales, los cuales son conexiones físicas y lógicas de punto a punto entre dos Switches en la red, estos enlaces son los encargados de transportar tráfico entre las VLAN`s de la red.

Capa de Distribución: En esta capa fueron implementados 3 Switches cisco sg300 de capa 3, que cumplen con las siguientes funciones: proporcionan la comunicación entre la capa de acceso y la capa de núcleo, se encargan de la segmentación de tráfico de los departamentos de la Dirección General de Inteligencia y se encuentran configurados con enlaces redundantes para mantener la disponibilidad y balanceo de carga.

Segmentación de Red VLAN´s

La red LAN fue dividida en varios segmentos lógicos, se creó las VLAN´s para disminuir latencia en la red de datos de la organización, reduciendo el tráfico broadcast y mejorando la seguridad en la red con la separación del tráfico por departamentos, el estándar para la configuración de VLAN´s en los equipos cisco es IEEE 802.1 Q.

Enlaces Redundantes.

Fue configurado el protocolo Spanning Tree (STP) para evitar los bucles en los enlaces redundantes de la red y proporcionar un único camino entre dos Switches, el estándar de STP en los equipos cisco es IEEE 802.1 D.

Capa de Acceso: Es la encargada de la conectividad con los dispositivos o terminales de los usuarios en la red, fue implementada por Switches de capa dos y puntos de accesos con los computadores de los usuarios, que proporcionan la conectividad de los computadores y los servidores la organización.

Puntos de accesos en los computadores de los Usuarios: Para la implementación de esta capa en la Dirección General de Inteligencia, fueron reutilizaron los Switches de capa dos que ya se encontraban funcionando en la organización, también fue necesario verificar que los puntos de acceso a la red cumplan con las normativas TIA/EIA 568-B3 de cableado estructurado y enlaces de fibra óptica.

En el siguiente diagrama de topología de red jerárquica se especifica los enlaces troncales, los enlaces redundantes y la segmentación de red que fueron utilizados para la comunicación externa a la infraestructura tecnológica de computación en la nube (IaaS) en la organización.

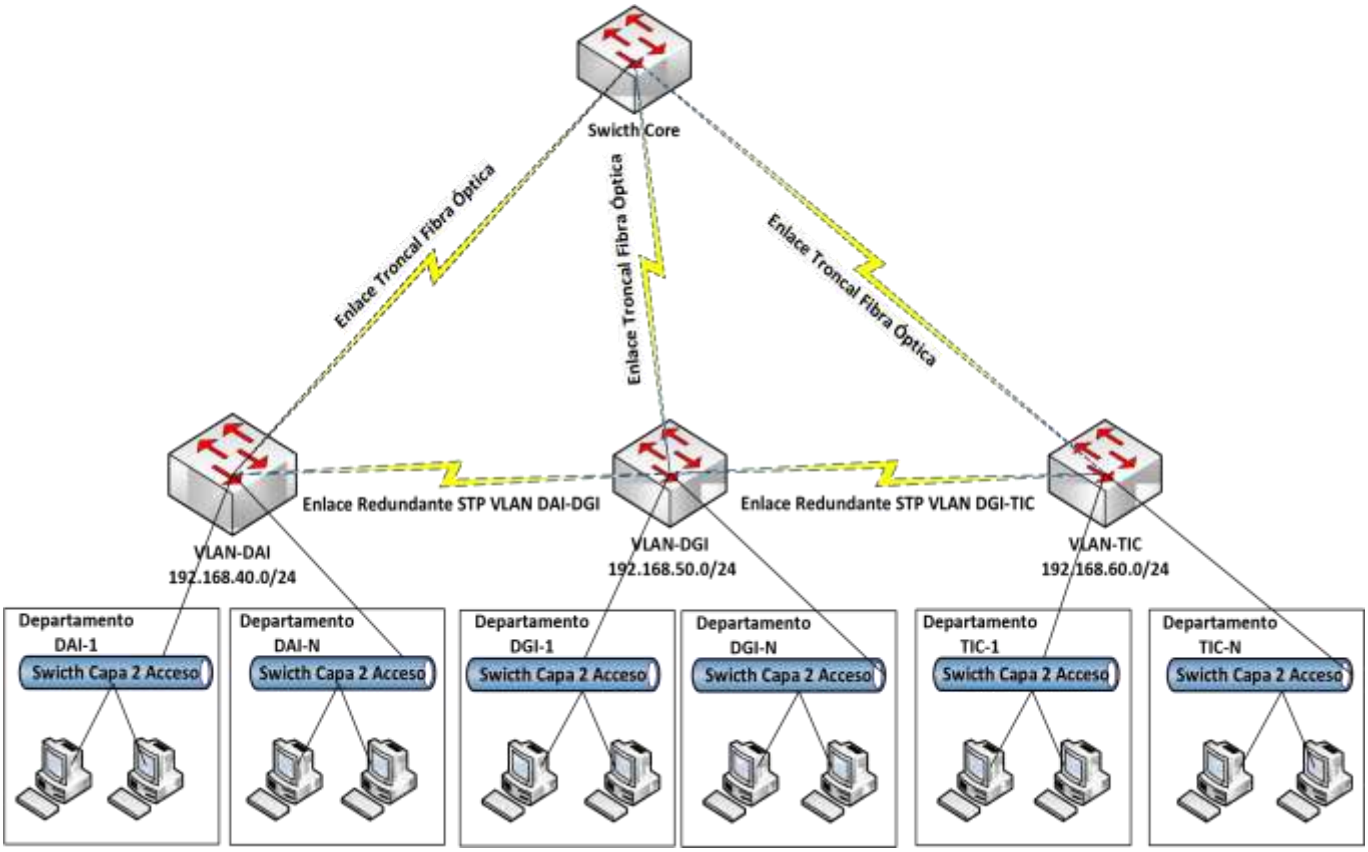


Figura 18: Diagrama de Topología de Red Jerárquica. Fuente: Elaboración propia.

Capitulo VII

Seguridades en la Infraestructura Tecnológica

7.1 Seguridad Perimetral de la Infraestructura Tecnológica

La seguridad perimetral es primordial para toda infraestructura tecnológica de una organización, los ataques realizados a una red pueden ocasionar perdidas a los activos de información digital, afectando a su confidencialidad e integridad, una plataforma robusta cuenta con dispositivos firewalls, que permitan el control y monitoreo del tráfico de datos que ingresan y salen de la infraestructura tecnológica, el firewall facilita a los administradores de la red configurar las reglas del tráfico permitido en la organización y mejorando la seguridad en la infraestructura tecnológica, preservando la confidencialidad e integridad de la información.

7.1.1 Implementación de Firewall

Para el control del tráfico que ingresa o sale de la organización, fue instalado y configurado el firewall de seguridad perimetral de código abierto pfsense, basado en FreeBSD, unos de los sistemas más seguros de Linux, dispone de una interface web para su configuración y administración.

Pfsense es un firewall que se puede implementar de manera virtual o ser instalarlo en cualquier computador como un sistema operativo propietario, en este proyecto de tesis fue instalado en un computador de manera de sistema propietario asignando todos los recursos de hardware al firewall.

Las principales funciones del firewall pfsense se describen a continuación:

- Limita las conexiones y filtra de paquetes por dirección IP, protocolos, puertos y enrutamiento por reglas.

- Multi-WAN, se puede configurar como un balanceador de carga, con varias conexiones WAN, realizando una distribución equilibrada del tráfico por cada enlace presentado al firewall, si se llegase a perder cualquiera de los servicios presentados por los ISP's, toma los enlaces disponibles como principales para la continuidad del servicio.
- Cuenta con tablero de monitoreo de las interfaces WAN y LAN, donde presenta graficas estadísticas del tráfico de red en tiempo real de las interfaces WAN y LAN, monitoreo del estado del dispositivo, consumo de memoria, procesador y almacenamiento.
- Servicio de DHCP, asignación de direcciones IP dinámicas para los segmentos de red LAN en la organización.
- Servidor DNS, servicio de resolución de nombres en la intranet.
- DMZ, zona desmilitarizada, interface de red independiente para la publicación de servicios al internet.
- Servidor de VPN, servicio de protocolo de red virtual, con OpenVPN, IPsec o PPTP.

El firewall también fue configurado como un IDS/IPS activo basado en red, creando reglas de manera automática y bloqueando las direcciones IP identificadas como maliciosas, este dispositivo al estar configurado de manera adecuada, facilita a los administradores de la infraestructura tecnológica contar con visibilidad de los posibles ataques cibernéticos realizados a la dirección IP publica, y de esta manera tomar las acciones correspondientes inmediatamente y minimizando los riesgos existentes en los principales activos tecnológicos de información.

En la siguiente imagen se muestra el tablero de monitoreo y control del firewall pfsense.

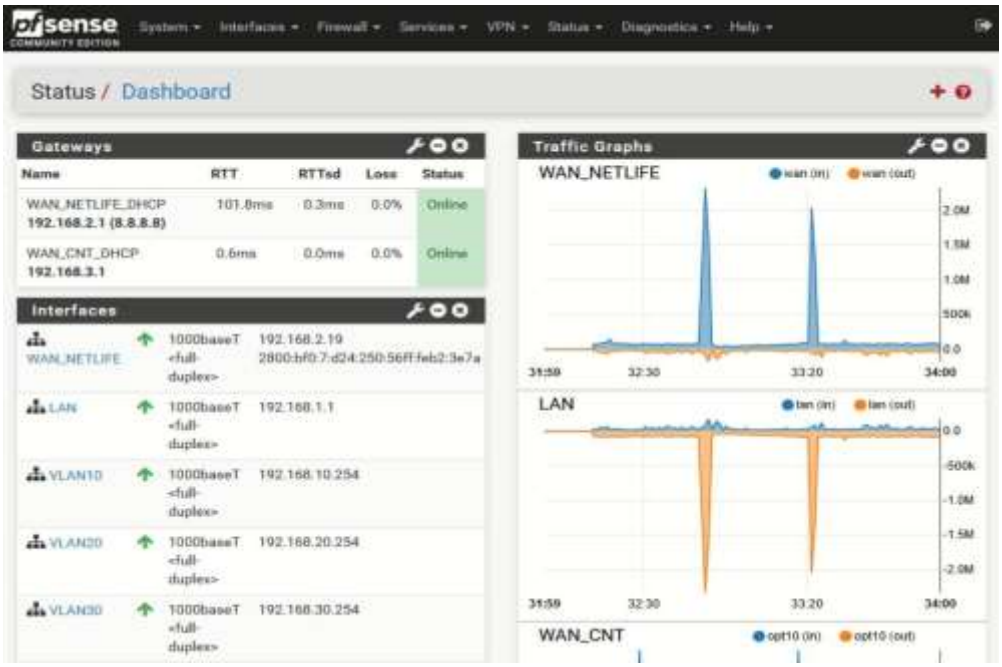


Figura 19: Tablero de monitoreo y control del firewall pfsense. Fuente: Elaboración propia.

7.2 Implementación de Directorio Activo

La gestión de acceso y control de identidad de usuarios de la organización es un tema fundamental en la seguridad, por lo tanto, fue necesario la implementación del servicio de Directorio Activo, el cual permite gestionar cuentas individuales de usuario y su asociación en grupos para facilitar la asignación de permisos. Esta plataforma almacena las contraseñas de usuarios en forma de hash, de tal manera, que si el registro de contraseñas de usuarios fuese robado la obtención de las mismas solo podría conseguirse mediante fuerza bruta, lo que sería muy ineficiente y altamente complicado si las contraseñas manejan una política de seguridad de contraseñas complejas.

Cuando un usuario acceda a un sistema podrá disponer de distintos permisos de acceso a directorios y archivos. Para cada árbol de directorios y para cada archivo el administrador puede establecer distintos privilegios para distintos usuarios o grupos.

7.2.1 Dominios y Unidades Organizativas

Se implementó un dominio principal xxx-xxx.int y como unidad organizativa (UO) xxx.int y a su vez la unidad organizativa xxx.int contiene las subunidades organizativas: Administradores, Equipos, Usuarios y grupos.

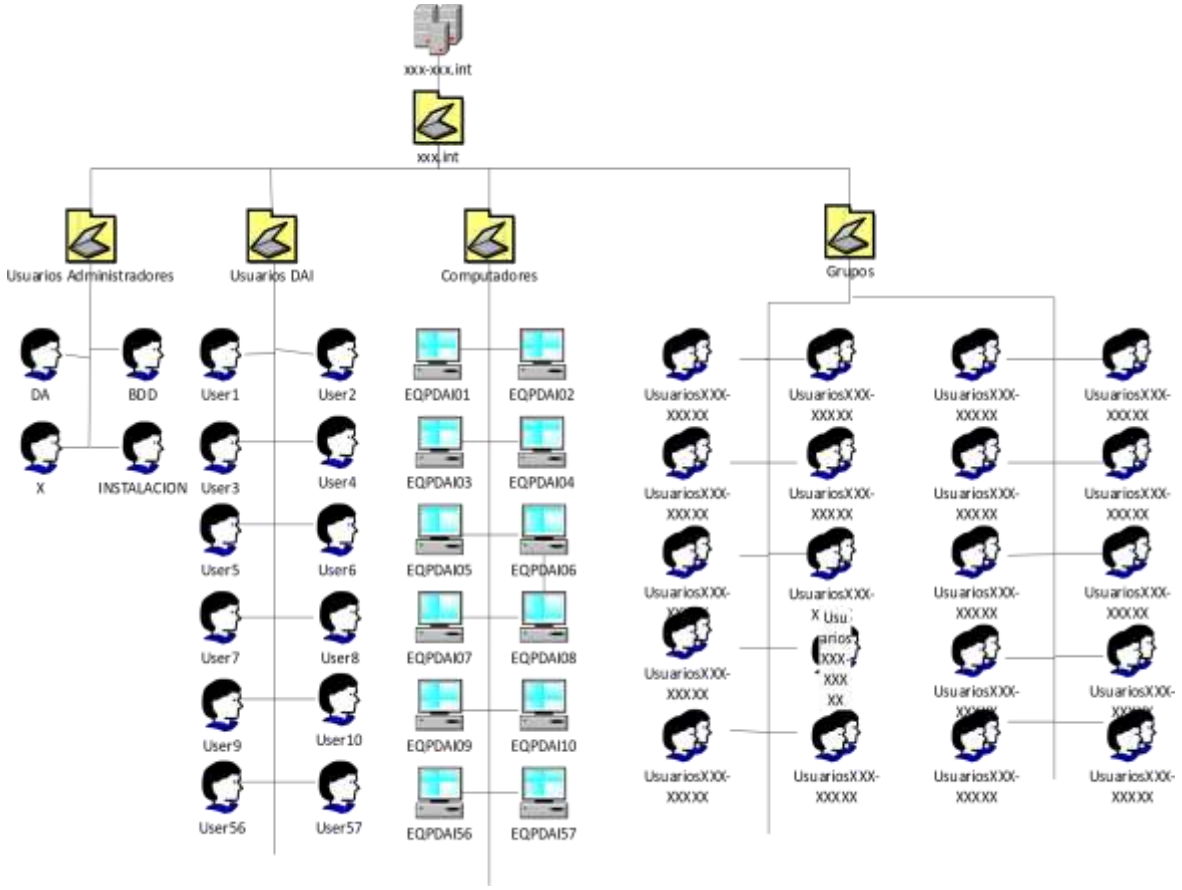


Figura 20: Diagrama General del Directorio Activo sin GPO. Fuente: Elaboración propia.

A continuación, se describe cada unidad organizativa con el conjunto de objetos que la componen:

UO Usuarios Administradores: Contiene todos los objetos usuario administradores del dominio, los cuales pueden realizar todo tipo de modificaciones en el servidor del dominio y en los equipos cliente. Se crearon varias cuentas de administrador: Una cuenta para el administrador del directorio Activo, una cuenta para el administrador de base de datos, una cuenta para

administrador un servicio X utilizado por la organización y una cuenta para el administrador de instalaciones de aplicaciones.

UO Usuarios DAI: En esta unidad organizativa se encuentran todos los usuarios de la red de la xxx.int, cada objeto usuario almacenara el nombre de usuario, contraseña y nombre completo.

UO Computadores: Conformada por los equipos que se encuentran dentro del dominio.

UO Grupos: Contiene la información referente a los grupos que están en el directorio activo. Para esta unidad organizativa se decidió que habrá un grupo por cada carpeta de ámbito compartida en la red, para restricción de acceso de usuarios a los ámbitos que no les correspondan.

7.2.2 Políticas de grupo (GPO)

Para la implementación de las GPO previamente se realizó un análisis de las políticas generales y las necesidades de administración de la red donde se propuso las siguientes políticas como medidas de seguridad:

Restricción de instalación de programas: Esto evita que los usuarios puedan instalar software innecesario para el desempeño de sus funciones o software sin licencia.

Restricción de ingreso al panel de control: Evita que se pueda realizar cambios en la configuración del equipo asignado.

Restricción a configuración avanzada de TCP/IP: Evita que los usuarios puedan abrir la página de propiedades de configuración avanzada de TCP/IP y modificar la configuración de IP, como la información del servidor DNS y WINS.

Cambio de contraseñas: Las contraseñas de los usuarios caducarán cada cierto tiempo y éstas deberán ser cambiadas. La creación de una nueva contraseña debe cumplir con los siguientes requisitos:

o No debe ser una contraseña utilizada anteriormente.

o Debe contener números. o Tener combinación de letras mayúsculas y minúsculas.

o Incluir caracteres especiales o La longitud debe ser mayor o igual a 8 caracteres.

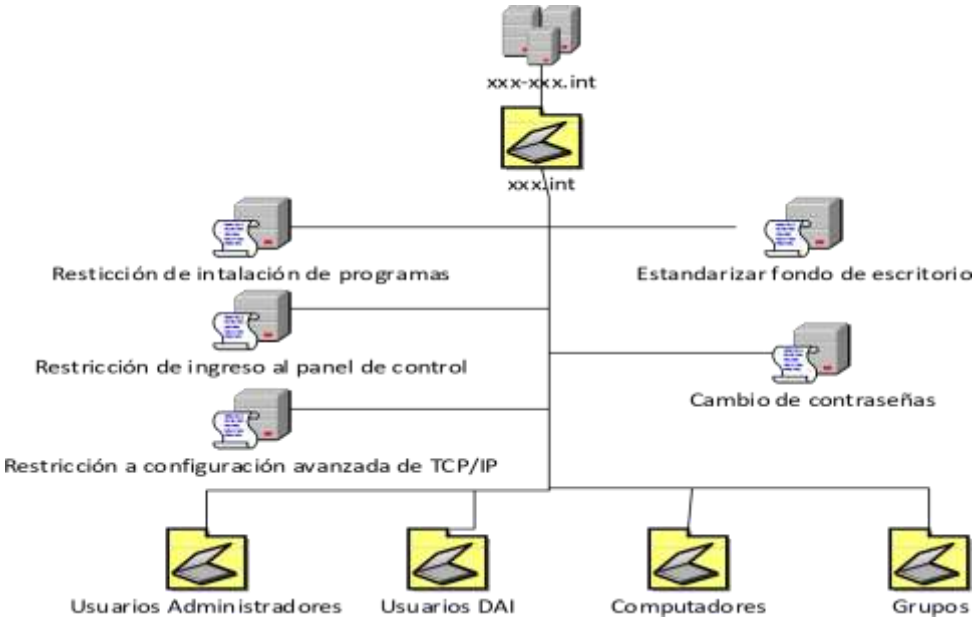


Figura 21: Diagrama de directorio activo de estructura lógica con GPO. Fuente: Elaboración propia.

7.3 Implementación de un SIEM

Fue implementado un SIEM (Gestión de información y eventos de seguridad) cuyo objetivo es proporcionar una visión global del estado de seguridad de una infraestructura tecnológica de información. Este sistema recolectará información de los distintos tipos de logs, dispositivos de seguridad y dispositivos de red y computadores de usuarios, normalizará la información para que esta tenga la misma fecha y hora permitiendo hacer búsquedas y análisis de información, correlacionará eventos y generará alertas de tal manera que se pueda tomar medidas frente a las posibles amenazas que estén pasando en la red.

La herramienta SIEM implementada en a la infraestructura tecnológica de la organización fue ALIEN VAULT OSSIM, por ser la herramienta de código abierto más utilizada y que cumple con las características necesarias para este proyecto. ALIEN VAULT OSSIM contiene de forma integrada y trabajando de manera conjunta, una serie de programas relacionados con la seguridad informática y redes, los cuales permiten labores de detección, monitoreo y correlación de eventos. Esta herramienta cuenta con una licencia OTX (Open Threat Exchange), lo cual significa que expertos en seguridad investigan de manera colaborativa nuevas amenazas, comparando datos de diversas fuentes y posteriormente integrando las nuevas firmas de amenazas a la herramienta para su monitoreo y control.

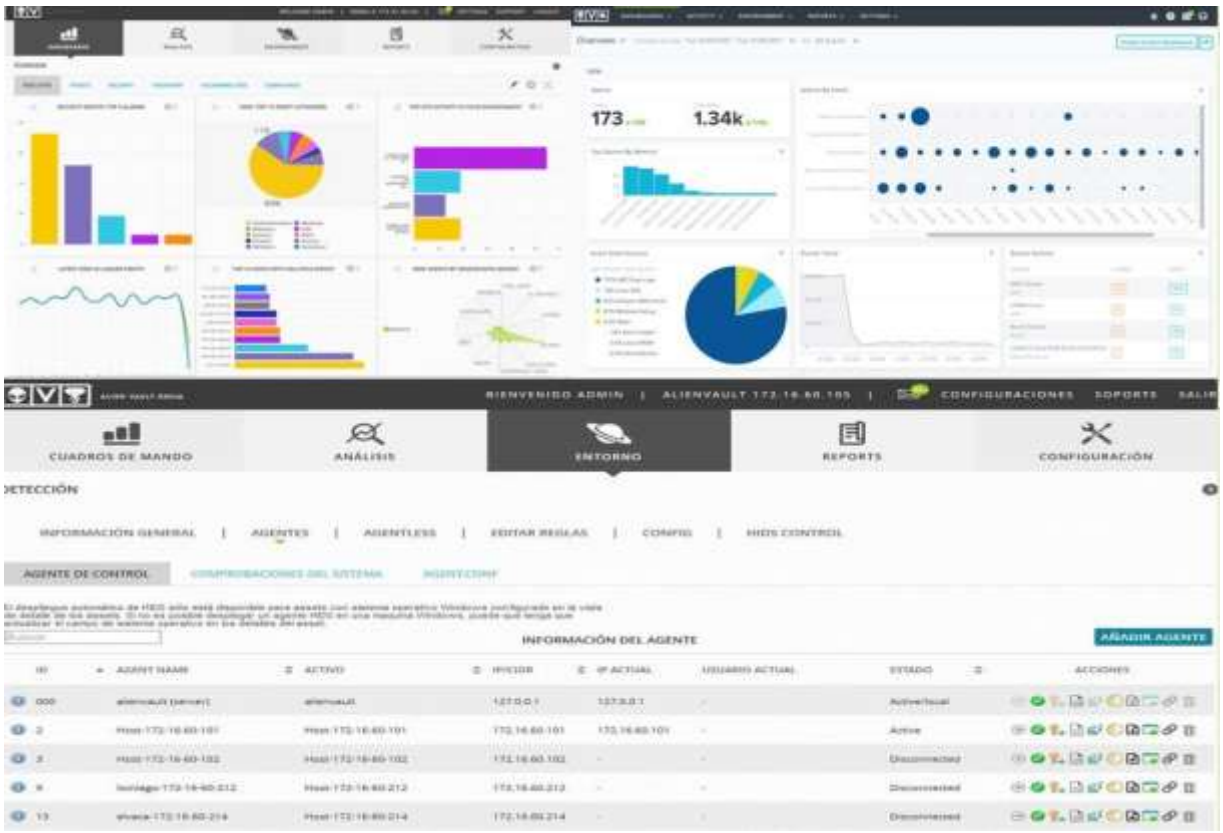


Figura 22: SIEM ALIEN VAULT OSSIM. Fuente: Elaboración propia.

Se implementaron sistemas de detección de intrusos (IDS) a nivel de Host (HIDS ALIEN VAULT) y a nivel de Red (HIDS ALIEN VAULT):

ALIEN VAULT HIDS: Se ejecutan individualmente en los sistemas host, encargándose de monitorear el tráfico proveniente desde y hacia el sistema host, así también como las actividades del mismo sistema. Utilizan una arquitectura de servidor-cliente, donde, el agente reside en el host que va a supervisar, todos los eventos son captados por el sensor donde los normaliza y posteriormente los envía al servidor HIDS para el análisis, correlación y almacenamiento.

Entre las características proporcionadas por los HIDS ALIEN VAULT se encuentran las siguientes: registro de monitoreo y recolección, detección de rootkits, monitoreo de integridad de archivos, monitoreo de integridad del registro de Windows y respuesta activa que puede ejecutar aplicaciones en un servidor en respuesta a ciertos desencadenantes, como alertas específicas o niveles de alerta.

ALIEN VAULT NIDS: Localizados en puntos estratégicos de la red, encargándose de monitorear el tráfico de la red y detectar eventos de red maliciosos, además proporcionando información vital para las directivas de correlación y las reglas de correlación cruzada. Al combinar esta información con los eventos recopilados de otros dispositivos, ALIEN VAULT OSSIM presenta una imagen completa de la actividad maliciosa.

El servidor de dispositivos consume las firmas NIDS a través de complementos, lo que genera los eventos ALIEN VAULT NIDS. El motor de correlación procesa y correlaciona los eventos normalizados, luego los almacena en la base de datos SIEM.

7.4 Seguridad en el entorno vSphere

Los componentes de la plataforma de virtualización vSphere se encuentran protegidos por varias características como la autenticación, autorización, un firewall en cada host ESXi, etc., pero además de esto, se puede realizar modificaciones a la configuración por defecto, entre

los cuales, se puede establecer permisos en objetos de vCenter, abrir puertos de firewall o cambiar los certificados predeterminados. También se puede tomar medidas de seguridad para los objetos en la jerarquía de vCenter, como lo son, sistemas de vCenter Server, hosts ESXi, máquinas virtuales y objetos de red y almacenamiento.

7.4.1 Asegurar el hipervisor ESXi

El hipervisor ESXi viene protegido por defecto, sin embargo, para contar con una mayor protección se realizaron las siguientes acciones:

7.4.1.1 Limitar el acceso a ESXi.

De forma predeterminada los servicios ESXi Shell y SSH no se ejecutan y solo el usuario raíz puede iniciar sesión en la Interfaz de usuario de la consola directa (DCUI). En la implementación de este proyecto se decidió habilitar el acceso ESXi o SSH, y se establecieron tiempos de espera para limitar el riesgo de acceso no autorizado.

Al host ESXi solo pueden acceder usuarios con permisos para administrar el host, los cuales se establecieron el objeto del sistema vCenter Server que administra el host.

7.4.1.2 Utilizar usuarios con nombre y privilegios mínimos

Por defecto, el usuario root puede realizar muchas tareas. Por ese motivo, se prohibió que administradores inicien sesión en el host ESXi mediante la cuenta root. En su lugar, se creó un usuario administrador, el cual fue designado desde vCenter Server y se le asignó el rol de Administrador.

7.4.1.3 Minimizar la cantidad de puertos de firewall ESXi abiertos

Los puertos del firewall se configuraron de manera predeterminada, para que se abran cuando inicie el servicio correspondiente. Por ejemplo, para el servicio de correo electrónico en

el firewall se abriría automáticamente el puerto 25 de smtp, para el servicio de Directorio Activo se abrirían los puertos 88 kerberos, 389 ldap, 53 dns, etc.

7.4.1.4 Aprovechar el modo de bloqueo

Se aumentó la protección de los hosts ESXi utilizando el modo de bloqueo normal. En este modo el servicio DCUI (interfaz de usuario de la consola directa) no se interrumpe, por lo tanto, si se llegase a perder la conexión con el sistema vCenter o el acceso desde el vSphere Web Client, sólo podrán acceder cuentas con privilegios mediante la DCUI del servidor y salir del modo bloqueo para administrar el servidor.

7.4.1.5 Administrar certificados ESXi.

Se utilizó VMware Certificate Authority (VCMCA) como autoridad de certificación raíz para aprovisionar a cada host ESXi un certificado firmado.

7.4.1.6 Bloqueo de cuenta de ESXi.

Se configuró para que se permita máximo 10 intentos fallidos de ingreso antes de que se bloquee la cuenta y se desbloqueará después de dos minutos de forma predeterminada.

7.4.2 Asegurar los sistemas vCenter Server y los servicios asociados

Su sistema vCenter Server y los servicios asociados están protegidos por autenticación a través de vCenter Single Sign-On y por autorización a través del modelo de permisos de vCenter Server. Las acciones tomadas fueron las siguientes:

7.4.2.1 Fortalecer todos los equipos host de vCenter.

Se instalaron los últimos parches seguridad para el sistema operativo de cada host y también se instaló software de antivirus y antimalware.

7.4.2.2 Configurar vCenter Single Sign-On.

Tanto el vCenter Server como todos los servicios asociados se protegieron mediante la autenticación de vCenter Single Sign-On, esto permite que los componentes de vSphere se comuniquen entre sí por medio de un token seguro en vez de solicitar a los usuarios que se autentiquen en cada componente por separado, también se agregó la fuente de identidad LDAP para que trabaje de forma simultánea ayudando a la seguridad organizacional.

7.4.3 Asegurar máquinas virtuales

Para mantener una buena protección de las máquinas virtuales es necesario tener todos los sistemas operativos parcheados y protegerlos de la misma manera como si fuesen equipos físicos, deshabilitando funcionalidades innecesarias, minimizando el uso de la consola VM y siguiendo buenas prácticas.

7.4.3.1 Proteger el sistema operativo invitado.

Para protección de un sistema operativo invitado, se aseguró la utilización de parches más actuales y aplicaciones antispyware y antimalware.

7.4.3.2 Deshabilitar funcionalidad innecesaria.

Se deshabilitaron funcionalidades innecesarias para minimizar posibles puntos de ataque, muchas de las funciones que se usan con poca frecuencia están deshabilitadas de forma predeterminada, debido a que cualquier función o servicio que encuentre ejecutando en una VM implica un potencial ataque.

7.4.3.3 Minimizar el uso de la consola de la máquina virtual.

Se creó una política de seguridad que consiste en reducir el uso de la consola de la máquina virtual y se configuró para que esté limitada a una sola conexión, debido a que esta consola tiene la misma función en una VM que proporciona un monitor en un servidor físico.

Los usuarios que cuentan con el acceso a la consola de la máquina virtual tienen la posibilidad de ingresar a la administración de energía de VM y a los controles de conectividad de dispositivos extraíbles, por lo tanto, el acceso a la consola de máquina virtual es peligroso, y podría permitir un ataque malicioso a una máquina virtual.

7.4.3.4 Arranque seguro UEFI.

Se configuró el arranque seguro UEFI en las VMs para mayor seguridad, debido a que esto impide la ejecución de software no firmado o certificado, evitando con esto la carga de malware o aplicaciones maliciosas cuando se inicia la VM.

La secuencia de arranque es la siguiente.

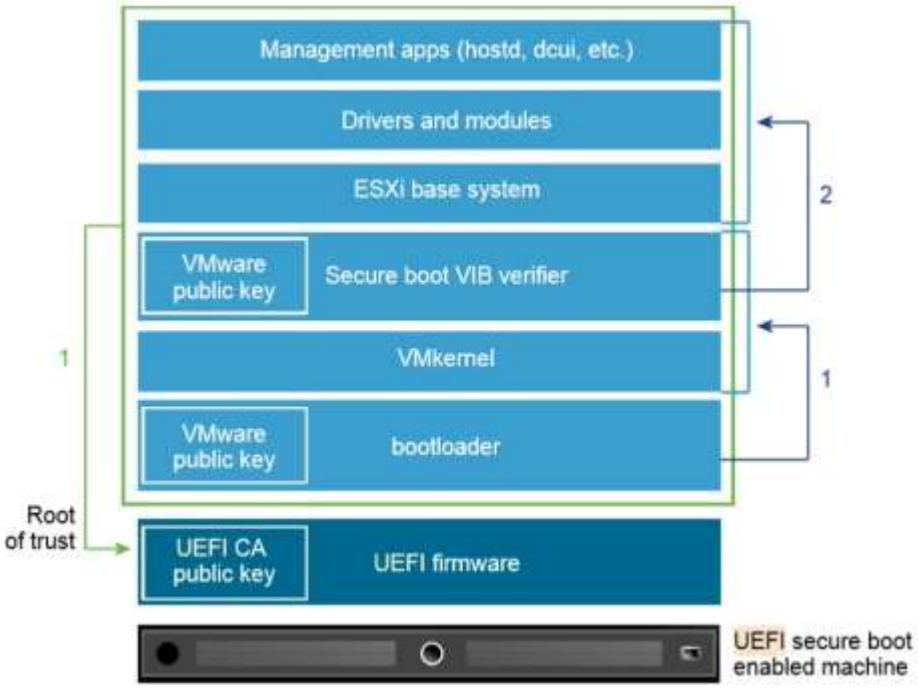


Figura 23: Arranque seguro UEFI. Fuente:(VMware, 2019)

1) El bootloader de ESXi contiene una clave pública de VMware, la cual se utilizará para verificar la firma del kernel y un pequeño subconjunto del sistema que incorpora un verificador VIB[4] (vSphere Installation Bundle) de arranque seguro.
2) El verificador VIB valida cada uno de los paquetes VIB que se instalan en el sistema.

7.4.4 Asegurar la capa de red virtual

La capa de red virtual contiene adaptadores de red virtual, virtual Switches, virtual Switches distribuidos, puertos y grupos de puertos. El entorno ESXi se basa en la capa de red virtual para admitir las comunicaciones entre las VMs y sus usuarios. Las acciones de seguridad que se tomaron fueron las siguientes:

7.4.4.1 Aislar el tráfico de red.

En un entorno ESXi el aislamiento del tráfico de red es esencial para su protección, las redes requieren distintos accesos y niveles de aislamiento. Se aisló la red de administración del tráfico del cliente, el tráfico API y el tráfico de software de terceros, asegurando que solo los usuarios administradores de los sistemas, redes y seguridad puedan acceder mediante la red de administración.

7.4.4.2 Considerar políticas de seguridad de red.

Se implementaron políticas de seguridad de red para la protección del tráfico contra la suplantación de direcciones MAC y el escaneo de puertos no deseado.

7.4.4.3 Considerar las VLAN para proteger su entorno.

Se consideraron las siguientes VLAN’s para poder segmentar la red: DAI, DIRECCION, TIC, ADMINISTRACIÓN, INTRANET, DMZ y SERVICIOS. El uso de las VLAN’s sirve para

[4] **VIB: “**Paquetes de software que incluyen una firma de VMware o un partner de VMware.” (VMware, 2019)

proteger más la red, ya que si dos máquinas no se encuentran en la misma VLAN no podrán enviar ni recibir paquetes entre sí.

Con la segmentación de la red se previenen diversas amenazas como la suplantación del protocolo ARP. Un atacante puede usar la técnica de suplantación de ARP para manipular la tabla de ARP y reasignar las direcciones MAC e IP, obteniendo de esta manera acceso al tráfico de red que va hacia el host y procede de él. Además, los atacantes usan la suplantación de protocolo ARP para realizar ataques de MITM ("Man in the middle"), DoS (denegación de servicio), secuestrar el sistema de destino y desestabilizar la red virtual de otras maneras.

7.4.5 Contraseñas en su entorno vSphere

Las restricciones de contraseña, la caducidad de la contraseña y el bloqueo de la cuenta en el entorno vSphere dependen del sistema al que se dirige el usuario, quién es el usuario y cómo se establecen las políticas.

7.4.5.1 Contraseñas de ESXi.

Las restricciones de contraseñas de ESXi fueron determinadas en el módulo PAM de Linux, para la creación de contraseñas se aplicaron los siguientes requisitos: La contraseña deberá conformarse por una combinación de letras en minúsculas, letras en mayúsculas, números y caracteres especiales; y la longitud no debe ser menor a 8 caracteres.

7.4.5.2 Contraseñas de vCenter Server y otros servicios de vCenter

La autenticación de los usuarios al vCenter y los servicios de vCenter es administrado por vCenter Single Sign-On. La restricción, expiración de contraseñas y el bloqueo de cuentas están sujetas al dominio del usuario y quién es el usuario.

Administrador de vCenter Single Sign-On

La contraseña del usuario administrador no caducará y no se encuentra subjeta a la directiva de bloqueo. Para los demás casos, la contraseña cumple con las restricciones definidas en la directiva de contraseñas de vCenter Single Sign-On.

Otros usuarios del dominio vCenter Single Sign-On

Las contraseñas de usuarios que no son administradores se configuraron para que cumplan las restricciones definidas en las directivas de contraseñas de vCenter Single Sign-On, donde las contraseñas caducarán cada 90 días, las contraseñas anteriores no pueden reutilizarse, la longitud mínima debe ser de 8 caracteres y contener al menos un meta carácter, al menos una letra mayúscula, contener al menos una letra minúscula y un número.

Capítulo VIII

Conclusiones y Recomendaciones

8.1 Conclusiones

- La implementación de la Infraestructura de computación en la nube privada IaaS permitió a la Dirección General de Inteligencia contar con escalabilidad horizontal y vertical, ya que los servicios informáticos son implementados de manera virtual independiente del hardware.

- La implementación de una nube privada IaaS en la Dirección General de Inteligencia facilita una administración centralizada de los servicios informáticos y de esta manera permitir el monitoreo y control de los recursos informáticos en tiempo real.

- La administración de la información y usuarios por Directorio Activo, permitió a los departamentos tener un mejor control de acceso a los repositorios y segmentación de la información.

- Se logró preservar las propiedades de la información: confidencialidad, integridad y disponibilidad de la siguiente manera: la confidencialidad, con la autenticación de usuarios, gestión de privilegios y el cifrado de información, la integridad, con el monitoreo del tráfico de la red, para detección oportuna de posibles incidentes de seguridad, políticas de auditoria y copias de seguridad, finalmente la disponibilidad, con la implementación de enlaces redundantes y balanceadores de carga de red para

minimizar el impacto de ataques de denegación de servicio; y copias de seguridad para la restauración de información perdida.

- Con la virtualización de los servidores informáticos, la asignación de los recursos de hardware a una máquina virtual se los puede realizar en caliente sin afectar la disponibilidad de un servicio.

8.2 Recomendaciones

- Se recomienda adecuar el centro de datos de la organización con certificación TIER I, donde se debe contar con un espacio dedicado para los servidores y equipos de redes de comunicación, un sistema de alimentación interrumpida para filtrar picos de energía, caídas y cortes momentáneos por un tiempo mínimo de 1 hora, un equipo adecuado de climatización seco dedicado conectado las 24hrs del día que no genere humedad, ya que los servidores son equipos electrónicos y con el tiempo la humedad se condensa formando gotas de agua, que pueden dañar los circuitos electrónicos de los dispositivos que son parte del centro datos; y contar con un generador con la carga necesaria en kVA para proporcionar energía ante cortes de suministro eléctrico prolongado.

- Se recomienda la adquisición e implementación de una SAN (Storage Area Network), equipo dedicado para la gestión de unidades de discos virtuales LUN (espacio de disco bruto sin formato), configurar la característica vSAN externo del clúster en la infraestructura de computación en nube (IaaS), encargado de proporcionar a las VMs unidades de discos lógicos, mejorando notablemente la velocidad y el tiempo de

respuesta, en la infraestructura tecnológica, eliminado la carga de trabajo de almacenamiento al clúster de servidores, dejándolo solo con procesamiento y ejecución.

- Se recomienda la contracción e implementación de un enlace redúndate para la conexión de internet, si el proveedor actual presenta algún tipo de problema con su servicio, la organización completa queda sin servicio de internet, la infraestructura tecnológica actual tiene los recursos necesarios para la implementación de un firewall virtual con un balanceador de cargar con dos interfaces WAN activas, disminuyendo la latencia del servicio de internet en el organización y reduciendo el riesgo por perdida del servicio de parte del ISP (Internet Service Provider).

BIBLIOGRAFIA

Alberto, U., Annie, F., David, B., & Elena, V. (2012). *Cloud Computing Retos y Oportunidades*.

Balu, V. (2015). A Model of Security Architecture on Private Cloud Using OpenStack. *International Journal on Recent and Innovation Trends in Computing and Communication*, *3*, 587–590. https://doi.org/10.17762/ijritcc2321-8169.150234

Buyya, R., & Ranjan, R. (2010). Federated resource management in grid and cloud computing systems. *Future Generation Computer Systems*.

Chase, J. S., Anderson, D. C., Thakar, P. N., & Vahdat, A. M. (2010). Managing Energy and Server Resources in Hosting Centers. *Proceedings of 11th IEEE/ACM International Conference on Grid Computing (GRID)*.

Cloud Standards Customer Council. (2017). *Cloud Standards Customer Council* (Vol. 3).

Galarza, B., Zaccardi, G., Belizán, M., Duarte, D., Morales, M., & Encinas, D. (2018). *Performance de Cloud Computing para HPC: Despliegue y Seguridad*.

Gleb, B. (2020). *Choosing the Right Cloud Service: IaaS, PaaS, or SaaS*. https://rubygarage.org/blog/iaas-vs-paas-vs-saas

Gonzales, D., & Rilo, J. (2012). Cloud Computing y Seguridad. *Reunión Española Sobre Criptología y Seguridad de La Información (RECSI 2012)*.

González, G., Vigil, P., Garcia, L., & Garófalo, A. (2012). PROPUESTA DE LAS ARQUITECTURAS DE SERVIDORES, RED Y VIRTUALIZACIÓN DE UNA NUBE PRIVADA QUE BRINDE INFRAESTRUCTURA COMO SERVICIO (IAAS1). *Revista Telem@tica*, *3*, 58–67.

Guerrero, J. (n.d.). Cloud Computing Open Source. *OPENSTACK ICEHOUSE*.

Hamouda, S. (2012). Security and privacy in cloud computing. *2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*, 241–245. https://doi.org/10.1109/ICCCTAM.2012.6488106

Hinojosa, H. A., & Ulloa, M. P. (2014). DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE NUBE COMPUTACIONAL BASADOS EN LA PLATAFORMA DE CÓDIGO ABIERTO OPENSTACK. *Escuela Politécnica de Las Fuerzas Armadas-ESPE*.

Infotecs. (2019). *Seguridad en la Nube*. https://infotecs.mx/blog/seguridad-en-la-nube.html

Kandpal, R., & Kumar, V. (2013). IaaS Implementation of a Private Cloud using Open Source Technology. *International Journal of Computer Applications*, *70*, 30–35. https://doi.org/10.5120/12186-8284

León, M. (2019). Escalado horizontal y vertical, dos opciones que garantizan el crecimiento de las aplicaciones. *Arsys*. https://www.arsys.es/blog/soluciones/escalado-horizontal-vs-vertical/

Malisow, B. (2020). *CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide* (I. John Wiley & Sons (ed.)).

Manvi, S. S., & Krishna Shyam, G. (2014). Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey. *Journal of Network and Computer Applications*, *41*, 424–440. https://doi.org/https://doi.org/10.1016/j.jnca.2013.10.004

Martín, M. J. (2018). *Servicios Cloud: ¿Qué es IaaS, SaaS y PaaS?* https://profile.es/blog/servicios-cloud-que-es-iaas-saas-y-paas/

Mell, P., Grance, T., & others. (2011). *The NIST definition of cloud computing*.

Ordoñez Pacheco, L. D. (2009). *La tecnologia de la virtualizacion en las computadoras*. *4*, 56–59. http://masterserver.f

Pangam, R. (2017). *7 mejores prácticas para asegurar su servicio en la nube*. CSO.

Policia Nacional del Ecuador. (n.d.). *Dirección General de Inteligencia*. Retrieved October 10, 2019, from https://www.policiaecuador.gob.ec/dgi/

Rouse, M. (2017). *Next-gen IT infrastructure strategy to guide digital transformation*. https://searchdatacenter.techtarget.com/definition/infrastructure

Rouse, M. (2018). Infrastructure management (IM). *Next-Gen IT Infrastructure Strategy to Guide Digital Transformation*.

Saavedra, A. (2018). *¿Qué es la Infraestructura Tecnólogica IT? Beneficios en la Transformación Digital*.

Sefraoui, O., Aissaoui, M., & Eleuldj, M. (2012). OpenStack: Toward an Open-Source Solution for Cloud Computing. *International Journal of Computer Applications*, *55*, 38–42. https://doi.org/10.5120/8738-2991

Serrano, M. (2018). *¿Qué es vRealize? Megaguía de VMware vRealize Suite*. https://virtualizadesdezero.com/que-es-vrealize-suite/

Shahzadi, S., Iqbal, M., Qayyum, Z. U., & Dagiuklas, T. (2017). Infrastructure as a service (IaaS): A comparative performance analysis of open-source cloud platforms. *2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 1–6. https://doi.org/10.1109/CAMAD.2017.8031522

Sushil, B., Leena, J., & Sandeep, J. (2010). CLOUD COMPUTING: A STUDY OF INFRASTRUCTURE AS A SERVICE (IAAS). *International Journal of Engineering and Information Technology*.

vmware. (2020). *VMware NSX : Network Virtualization and Security Platform*. https://www.vmware.com/latam/products/nsx.html

VMware. (2018). *VIO DESIGN GUIDE*.

VMware. (2019). *vSphere Security*.

VMware. (2020a). *vCenter Server Installation and Setup*.

VMware. (2020b). *VMware Integrated OpenStack Installation and Configuration Guide*.

VMware Docs. (2019). *Componentes del software de vSphere*. https://docs.vmware.com/es/VMwarevSphere/6.5/com.vmware.vsphere.vcenterhost.doc/GUID-B3A1A79B-EF9B-4C10-A053-D54D88254C52.html

Wang, L., Laszewski, G., Kunzeand, M., & Tao, J. (2010). Cloud computing: a perspective study. *J New Generation Computing*, 1–11.

Wei, G., Vasilakos, A. V, Zheng, Y., & Xiong, N. (2010). A game-theoretic method of fair resource allocation for cloud computing services. *The Journal of Supercomputing*, *54*(2), 252–269. https://doi.org/10.1007/s11227-009-0318-1

Anexos

Anexo I: Instalación y Configuración de VMware ESXi 6.7

Para la instalación y configuración de VMware ESXi 6.7 se siguieron los siguientes pasos:

1. Se configuró una USB booteable con el sistema de VMware ESXi 6.7.

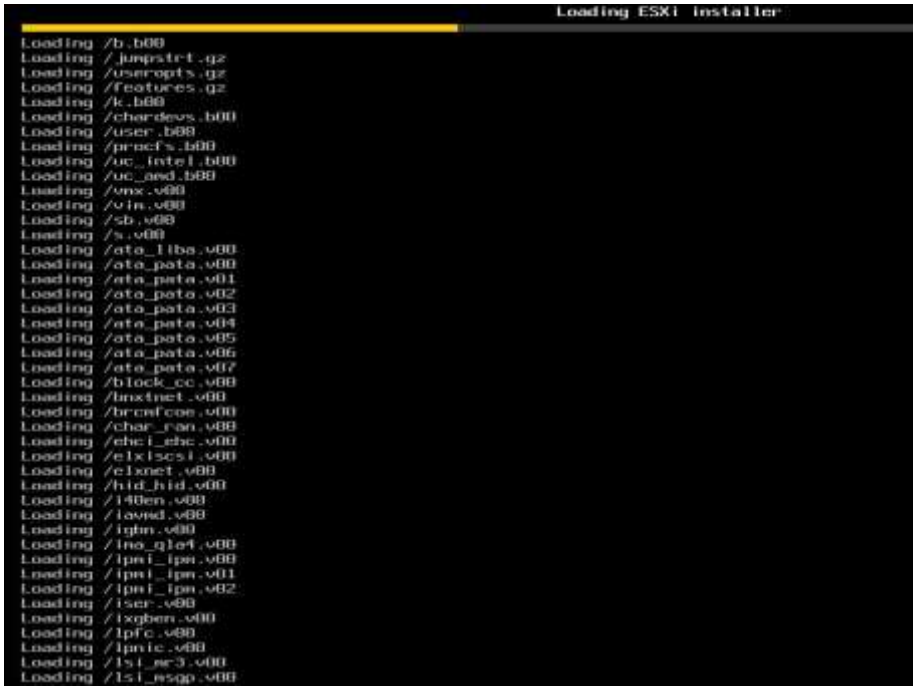


Figura 24: Proceso de carga del instalador ESXi. Fuente: Elaboración propia.

2. El proceso mostró un mensaje de bienvenida de la instalación del producto, donde se seleccionó la opción de continuar.

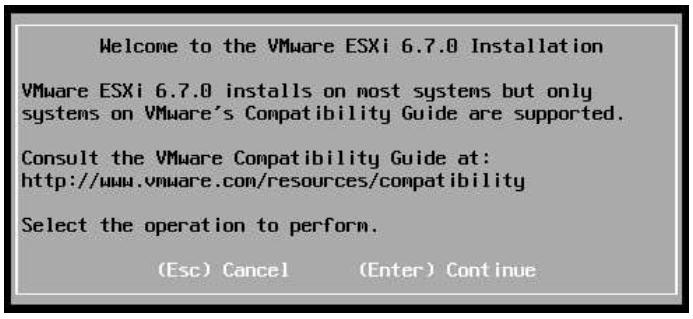


Figura 25: Mensaje de bienvenida a la instalación del ESXi. Fuente: Elaboración propia.

3. Se aceptó los términos y contratos del producto.

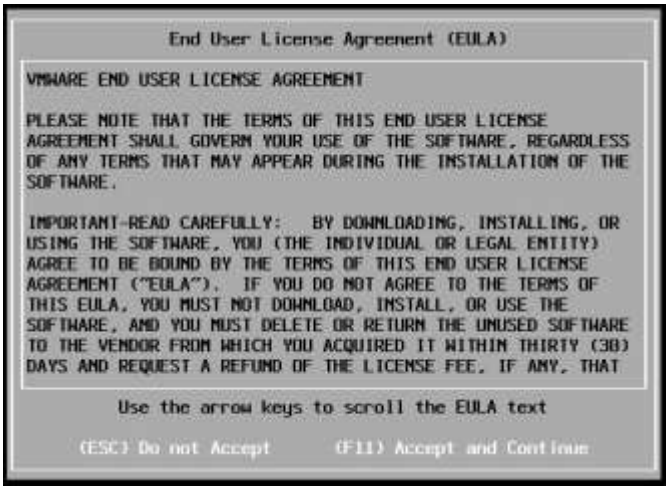


Figura 26: Mensaje de términos y contratos del producto ESXi. Fuente: Elaboración propia.

4. Se seleccionó la unidad de disco duro donde se instalará el hipervisor VMware vSphere 6.7.

Figura 27: Selección unidad de disco donde se instalará el hipervisor. Fuente: Elaboración propia.

5. Se seleccionó la distribución del idioma del teclado.

Figura

28: Selección distribución idioma del teclado. Fuente: Elaboración propia.

6. Se ingresó la contraseña del usuario root para la administración del servidor.

Figura 29: Ingreso de contraseña usuario root. Fuente: Elaboración propia.

7. Se confirmó el inicio de la instalación (F11).

Figura 30: Pantalla de confirmación inicio de instalación ESXi. Fuente: Elaboración propia.

8. El asistente mostró una barra con el porcentaje de progreso de la instalación.

Figura 31: Barra de progreso de la instalación. Fuente: Elaboración propia.

9. El asistente mostró un mensaje de finalización del proceso de instalación.

Figura

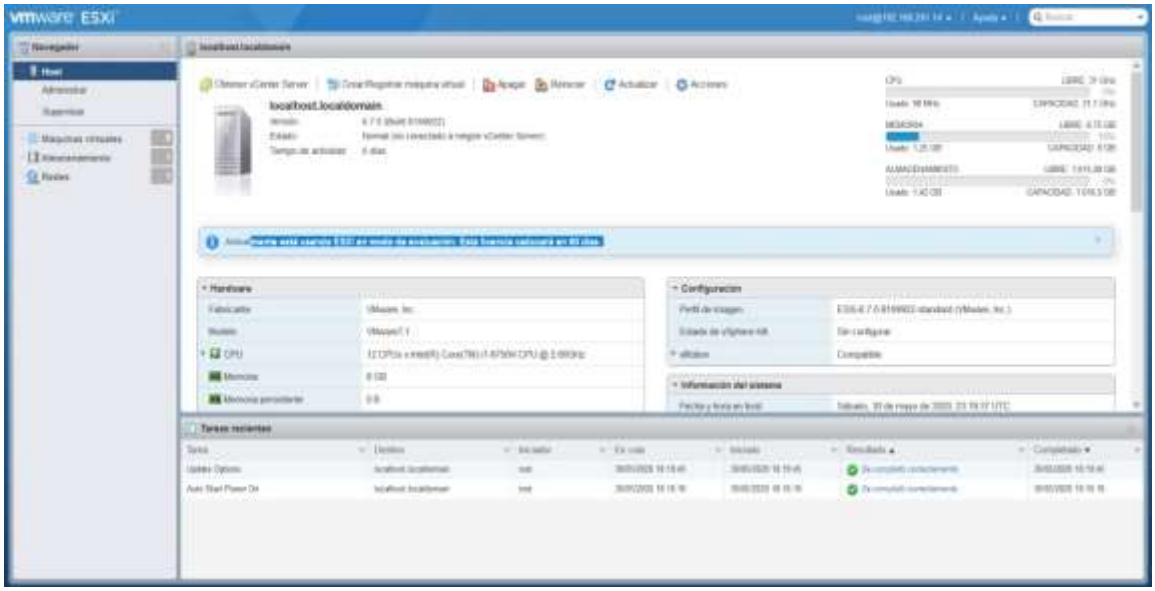
32: Mensaje de finalización del proceso de instalación. Fuente: Elaboración propia.

10. El servidor se reinició y cargó el sistema operativo de VMware vSphere ESXi 6.7.

Figura 33: Reinicio y carga del sistema operativo VMware vSphere ESXi 6.7. Fuente: Elaboración propia.

11. Para el ingreso a la consola de administración del servidor se lo realizó a través de un navegador web.

Figura



34: Consola de administración del servidor. Fuente Elaboración propia.

Anexo II: Instalación y configuración del servidor virtual de vCenter

Para la instalación y configuración del servidor virtual vCenter se siguieron los pasos del asistente de instalación VMware.

1. Para el inicio de la instalación se debió seleccionar la opción Instalar.

Figura 35: Pantalla de instalación vCenter. Fuente: Elaboración propia.

Figura

2. El asistente presentó una pantalla de introducción a la instalación del vCenter donde se seleccionó siguiente.

36: Pantalla de introducción a la instalación vCenter. Fuente: Elaboración propia.

Figura

3. El asistente mostró los términos de contrato de la licencia, donde se leyó y se aceptaron los mismos.

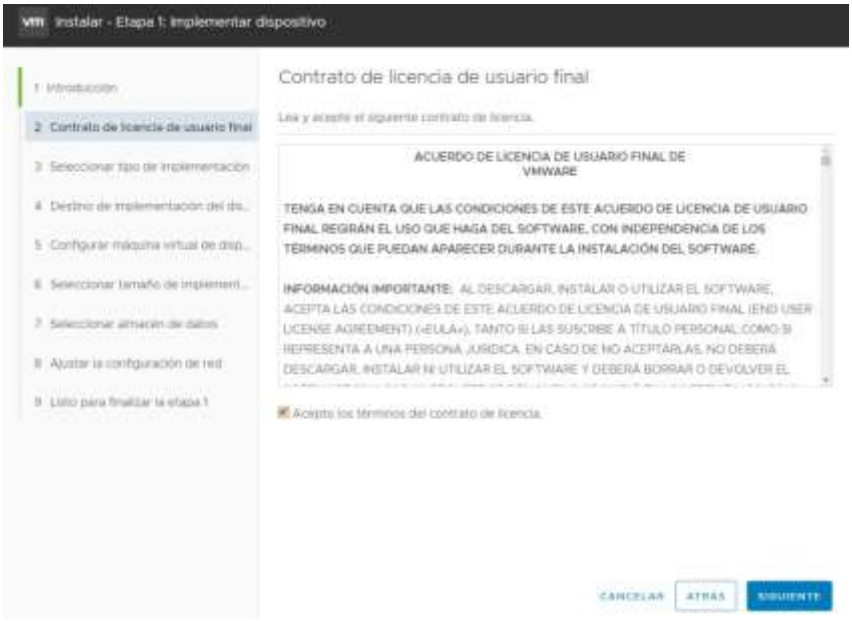


Figura 37: Términos de contrato licencia vCenter. Fuente: Elaboración propia.

4. Se seleccionó la opción vCenter con una instancia de Plataforma Servicios de Controlador Integrado.

Figura 38: Pantalla de selección tipo de implementación. Fuente: Elaboración propia.

5. Se ingresó la dirección IP del servidor para la implementación de la máquina virtual y las credenciales de administrador.

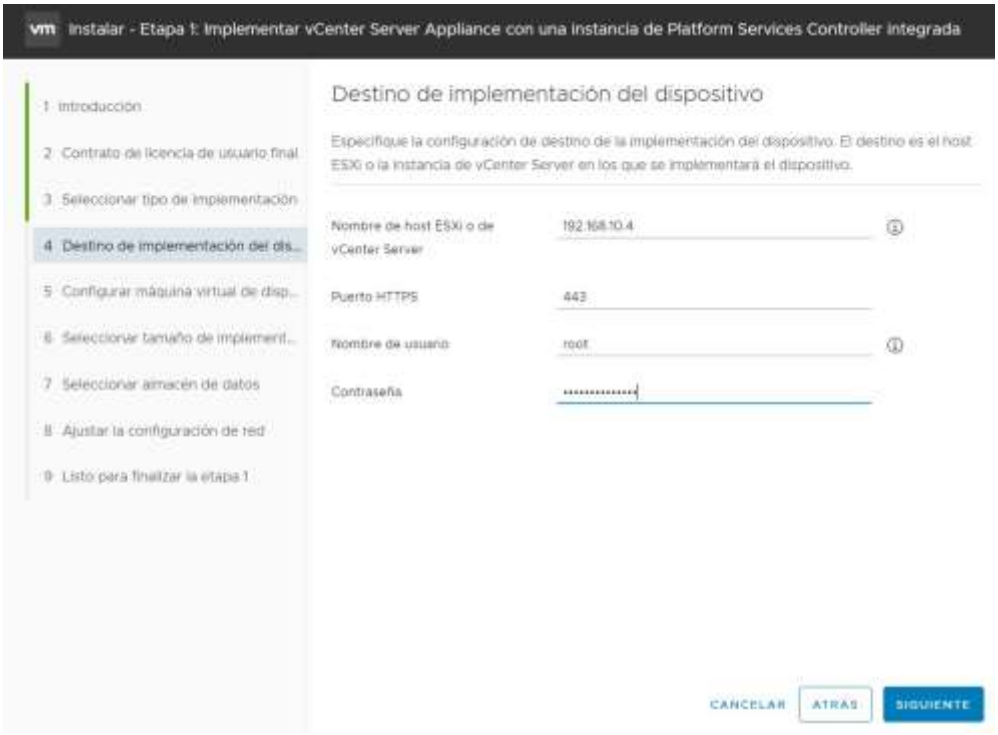


Figura 39: Pantalla de destino de implementación del dispositivo. Fuente: Elaboración propia.

6. El asistente de VMware presentó una advertencia del certificado del host ESXi, donde se procedió aceptar el Certificado por defecto del host ESXi.

Figura 40: Certificado por defecto del host ESXi. Fuente: Elaboración propia.

7. Se configuró el nombre del Servidor virtual y las credenciales de usuario root.

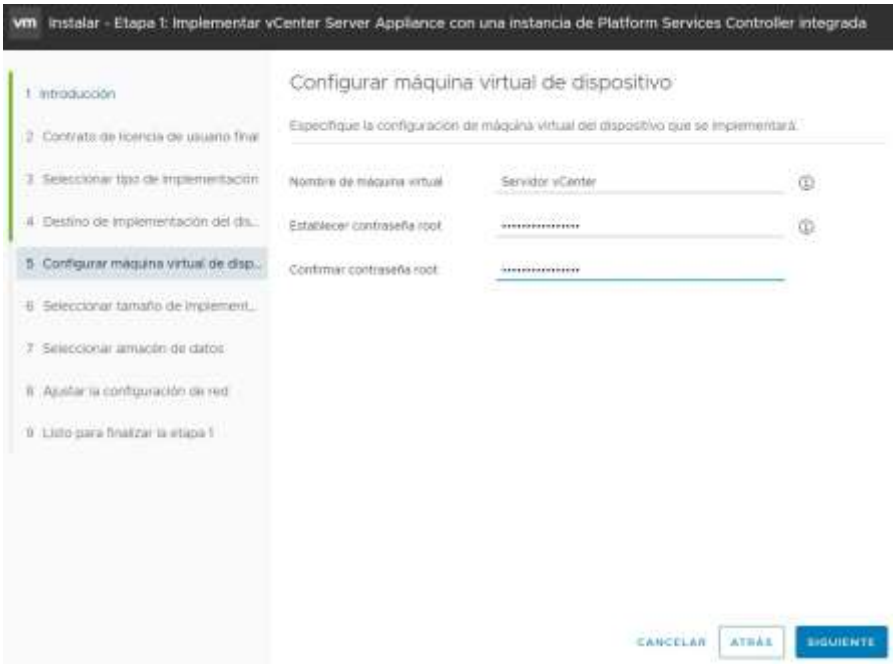
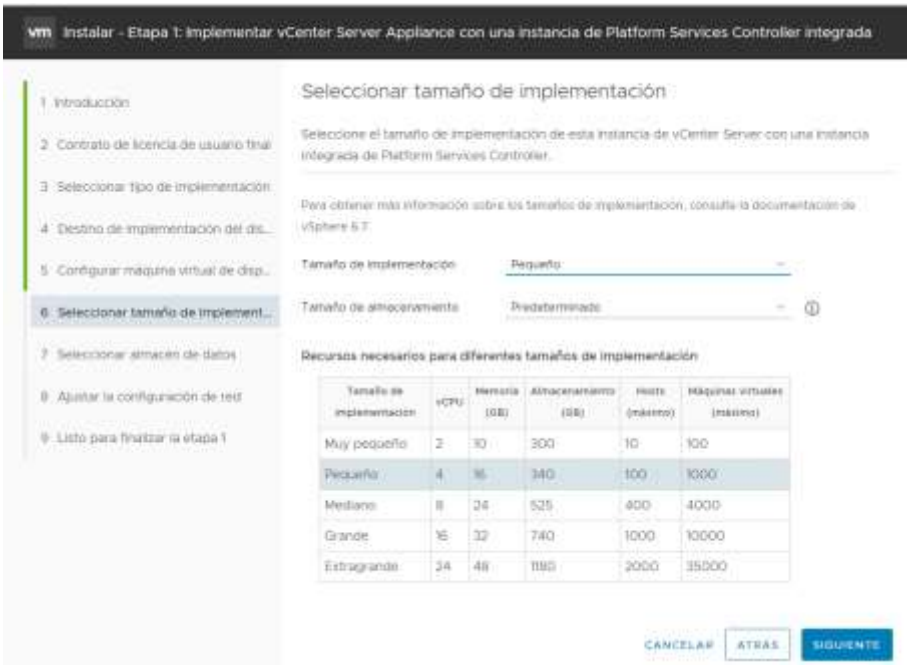


Figura 41: Pantalla de configuración de la máquina virtual del dispositivo. Fuente: Elaboración propia.

8. Se seleccionó el tamaño de implementación dependiendo del número de host ESXi y Numero de Máquinas Virtuales.



Figura

42: Pantalla de selección del tamaño de implementación. Fuente: Elaboración propia.

9. Se seleccionó el disco donde se debe instalar el servidor virtual de vCenter.

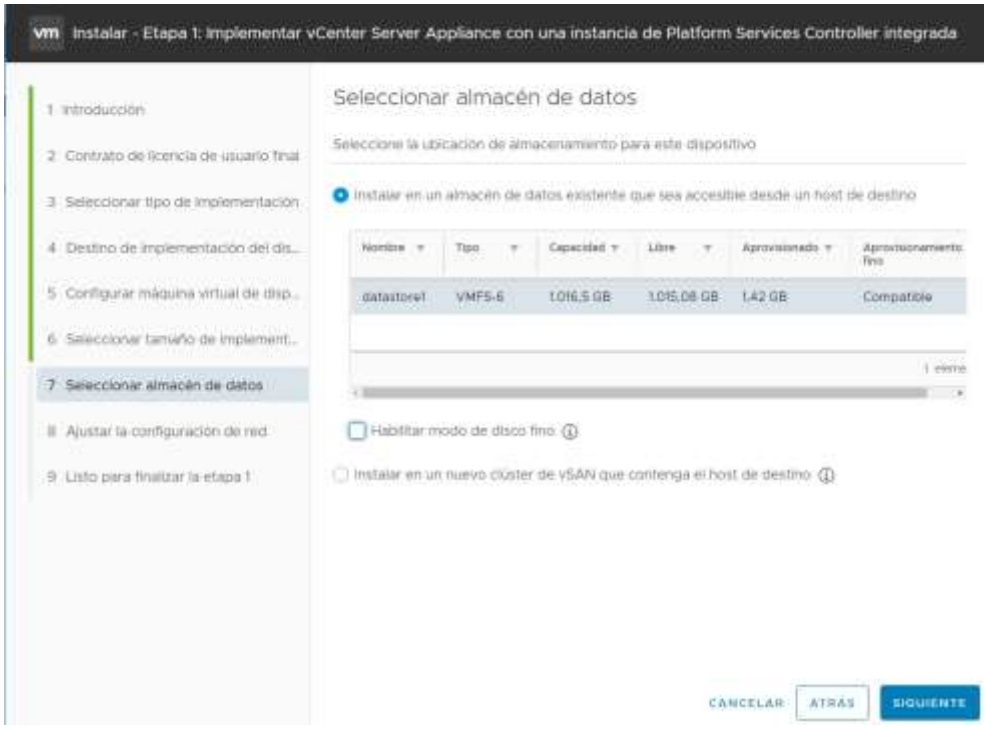
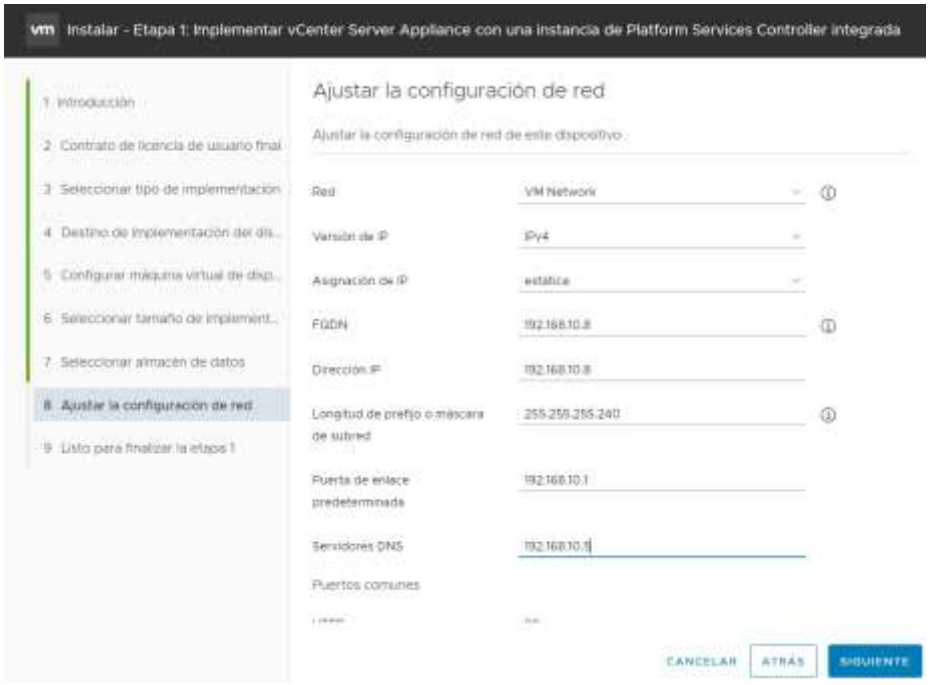


Figura 43: Pantalla de selección de almacén de datos. Fuente: Elaboración propia.

10. Se ingresó la dirección IP para el servidor virtual vCenter.



Figura

44: Pantalla para ajustar configuración de red. Fuente: Elaboración propia.

11. El asistente VMware presentó una tabla resumen de las configuraciones del Servidor Virtual.

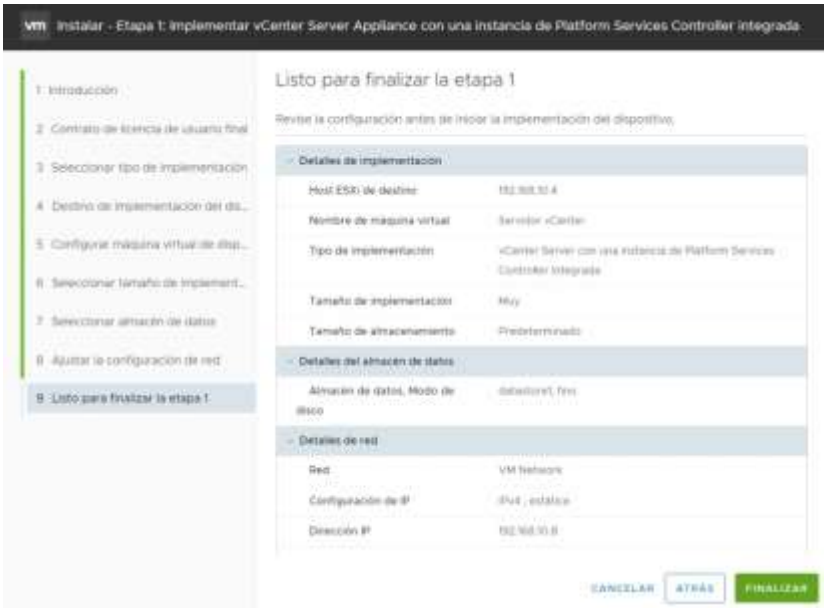


Figura 45: Tabla resumen de las configuraciones del servidor virtual. Fuente: elaboración propia.

12. Comenzó el proceso de instalación mostrando una barra de progreso.

Figura 46: Barra de progreso instalación vCenter. Fuente: Elaboración propia.

13. El asistente de la instalación del vCenter mostró un mensaje para el inicio de la Etapa2 para la implementación de Servidor Virtual de vCenter.

47: Mensaje inicio etapa2 de implementación vCenter. Fuente: Elaboración propia.

14. El asistente de instalación VMware presentó una introducción a la instalación de la segunda etapa del Servidor de vCenter.

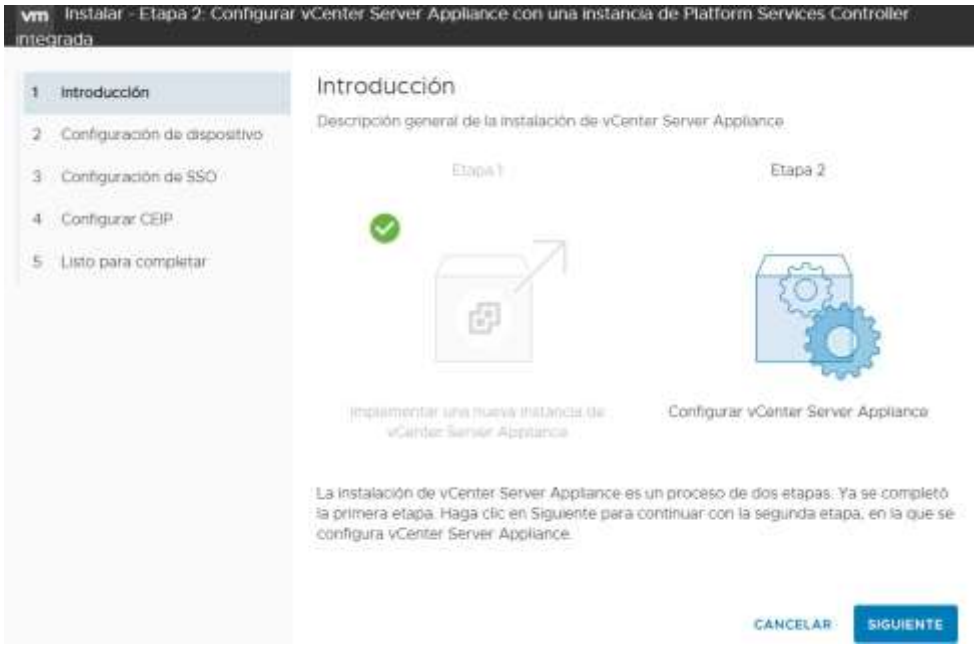


Figura 48: Introducción a la segunda etapa de instalación vCenter. Fuente: Elaboración propia.

15. Se configuró el modo de sincronización de la hora con un servidor de ntp.

Figura

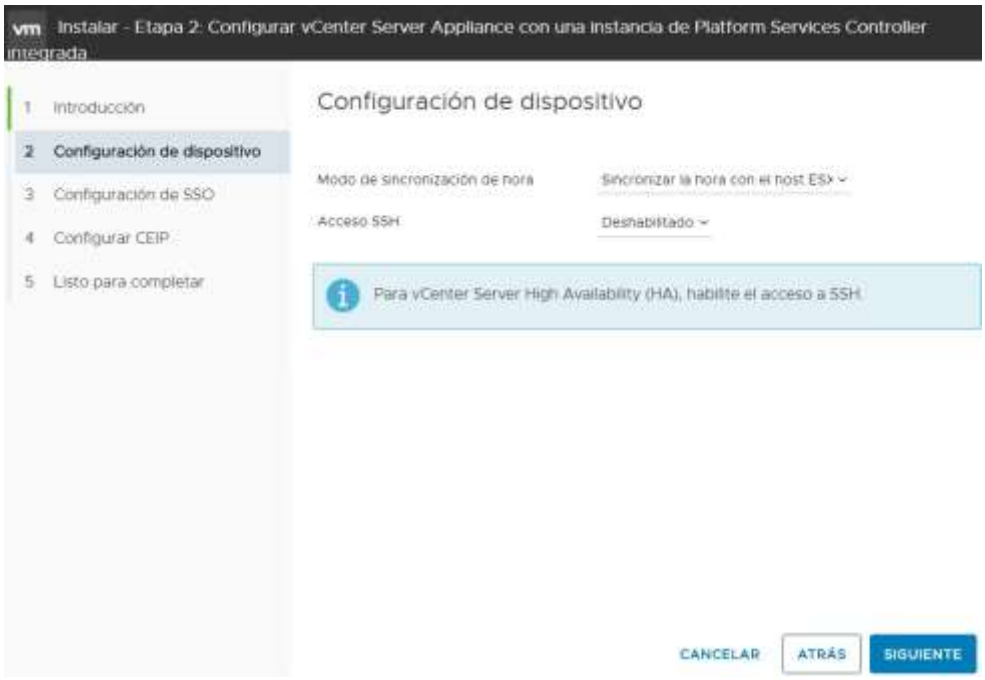


Figura 49: Pantalla de configuración de dispositivo. Fuente: Elaboración propia.

16. Se configuraron los accesos por Single Sign-On.

Figura 50. Configuración de SSO. Fuente: Elaboración propia.

17. Configuró el CEPI, aceptando unirse al programa de mejora de experiencia del cliente de VMware.

Figura 51: Configurar CEIP. Fuente: Elaboración propia.

18. El asistente presentó una tabla resumen con las configuraciones de la segunda etapa.

Figura 52: Tabla resumen de las configuraciones segunda etapa. Fuente: Elaboración propia.

19. Comenzó el proceso de instalación de la segunda etapa, mostrando la barra de progreso de la misma.

Figura 53: Barra de progreso instalación segunda etapa vCenter. Fuente: Elaboración propia.

20. El asistente de instalación VMware mostró una pantalla de finalización del proceso de instalación de vCenter.

Figura 54: Pantalla de finalización del proceso de instalación de vCenter. Fuente: Elaboración propia.

21. Para el acceso a la interfaz de administración y control de VMware vCenter se lo realizó mediante un navegador web, tal como se muestra en la siguiente imagen.

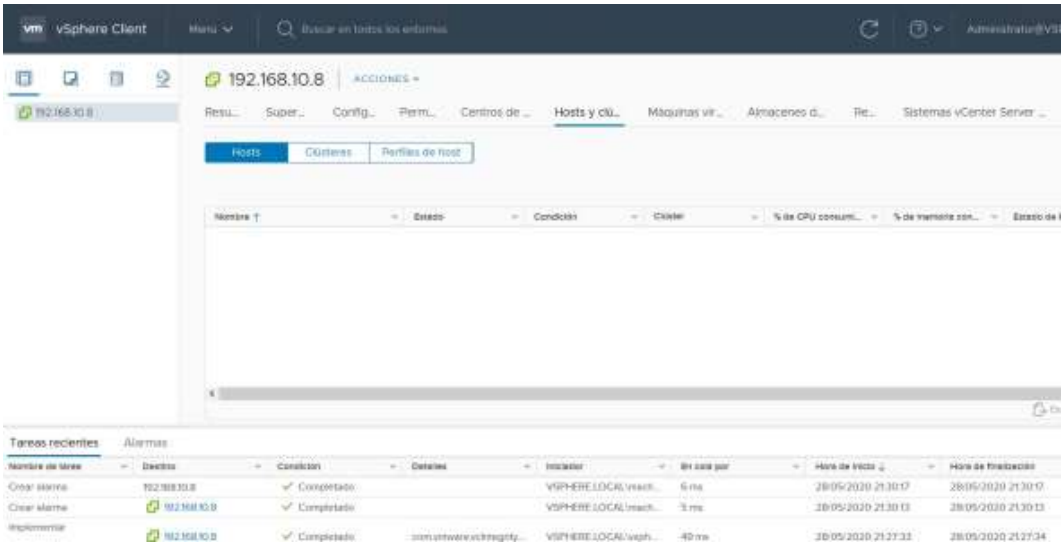


Figura 55: Interfaz de administración y control de VMware vCenter. Fuente: Elaboración propia.

Anexo III: Configuración del clúster de vSphere

Para la configuración de clúster Host ESXi se realizaron las siguientes acciones:

1. Se ingresó a la interface de vCenter.

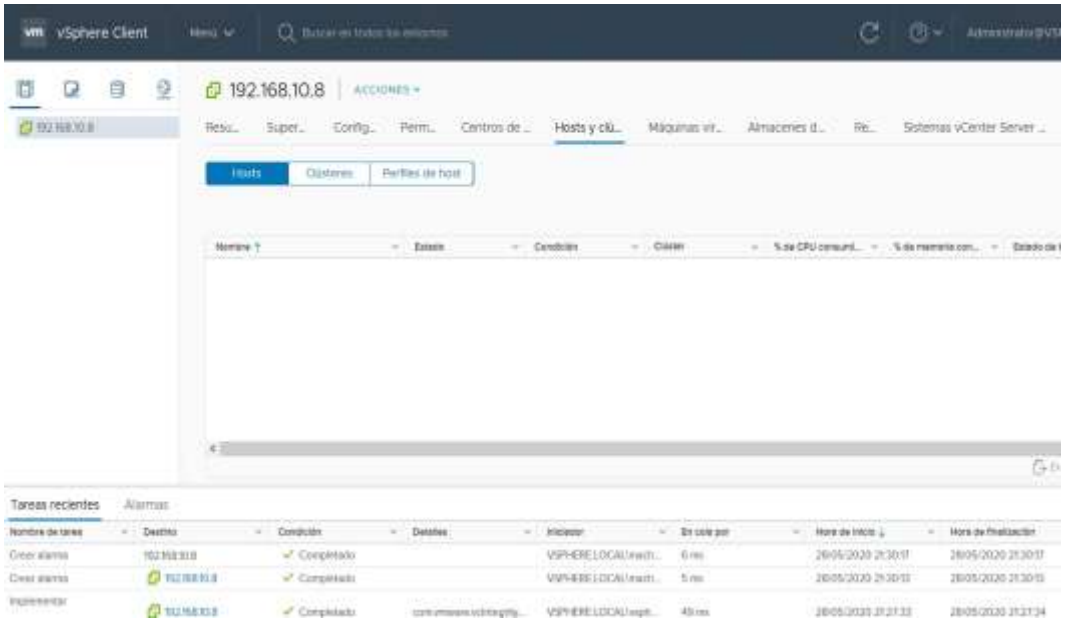


Figura 56: Interface de vCenter. Fuente: Elaboración propia.

2. Se creó un nuevo centro de datos llamado “Centro Datos DGI”.

Figura 57: Nuevo centro de datos. Fuente: Elaboración propia.

3. En el Centro de datos DGI Clic se procedió hacer clic derecho y seleccionar la opción Nuevo clúster.

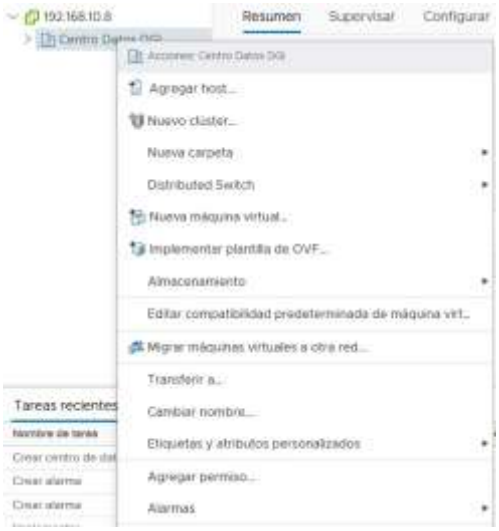


Figura 58: Opción nuevo clúster. Fuente: Elaboración propia.

4. Se habilitó el VMware DRS y vSphere HA.

Figura

59: Configuración del Centro de datos DGI. Fuente: Elaboración propia.

5. Para agregar un host de ESXi al clúster DGI, se realizó clic derecho en el clúster y se seleccionó la opción agregar hosts.

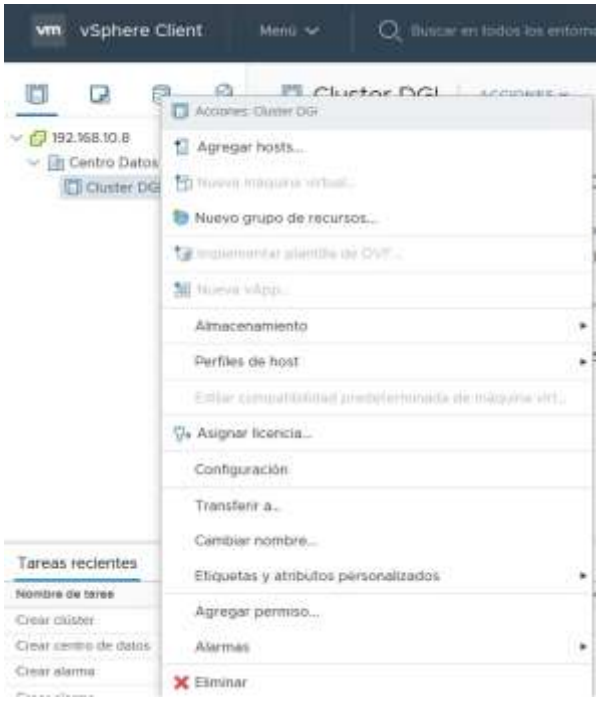
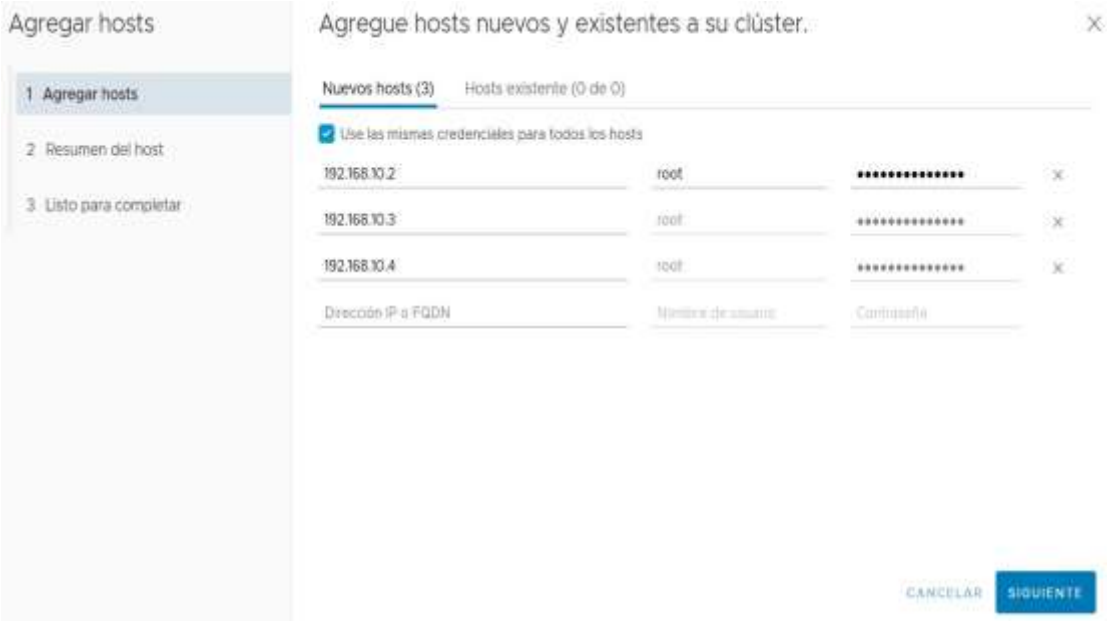


Figura 60: Opción Agregar hosts al clúster. Fuente: Elaboración propia.

6. Se ingresaron las direcciones ip de los hosts y las credenciales.

Figura



61: Agregar nuevos hosts al clúster. Fuente: Elaboración propia.

7. Se verificaron los certificados utilizados por cada servidor.

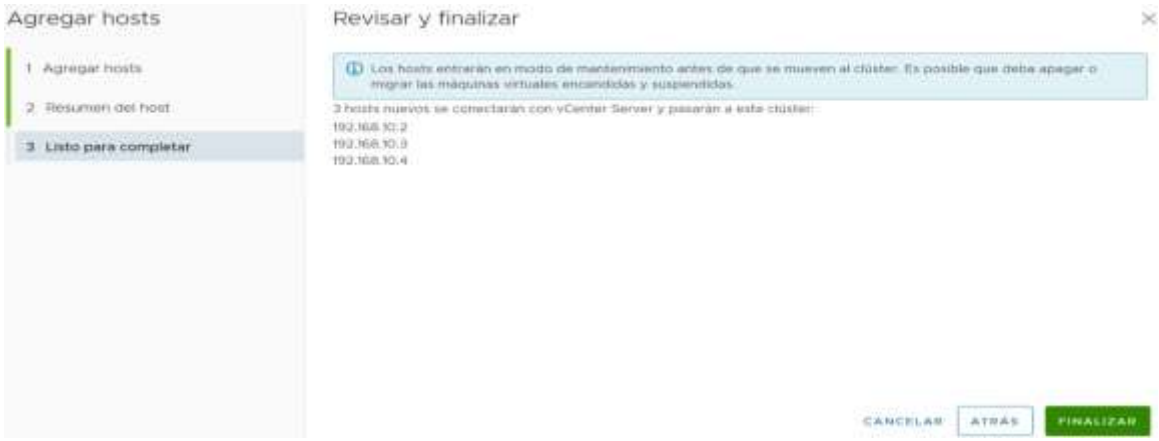
Figura 62: Alerta de seguridad certificados de servidores. Fuente: Elaboración propia.

8. El asistente de VMware mostró un resumen de los host ESXi que forman parte del clúster.

Figura

Figura 63: Resumen de host ESXi que forman parte del clúster. Fuente: Elaboración propia.

9. Para finalizar el proceso de configuración del clúster el asistente de VMware muestra una tabla resumen de los nuevos hosts agregados al clúster.



64: Tabla resumen de los nuevos hosts agregados al clúster. Fuente: Elaboración propia.

Anexo IV: Instalación y Configuración de VIO VMware Integrated OpenStack (VIO)

Para instalar y configurara el servicio virtual integrado de OpenStack, fue necesario descargar el paquete OVA de VIO, que se encuentra disponible de manera gratuita en la página oficial del fabricante VMware.

1. Se seleccionó el archivo .ova de VIO previamente descargado.

Figura

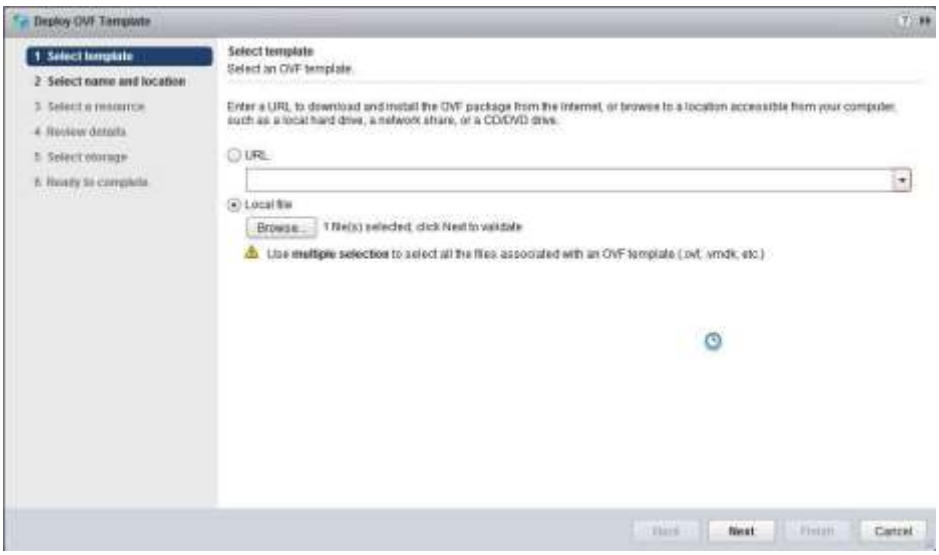
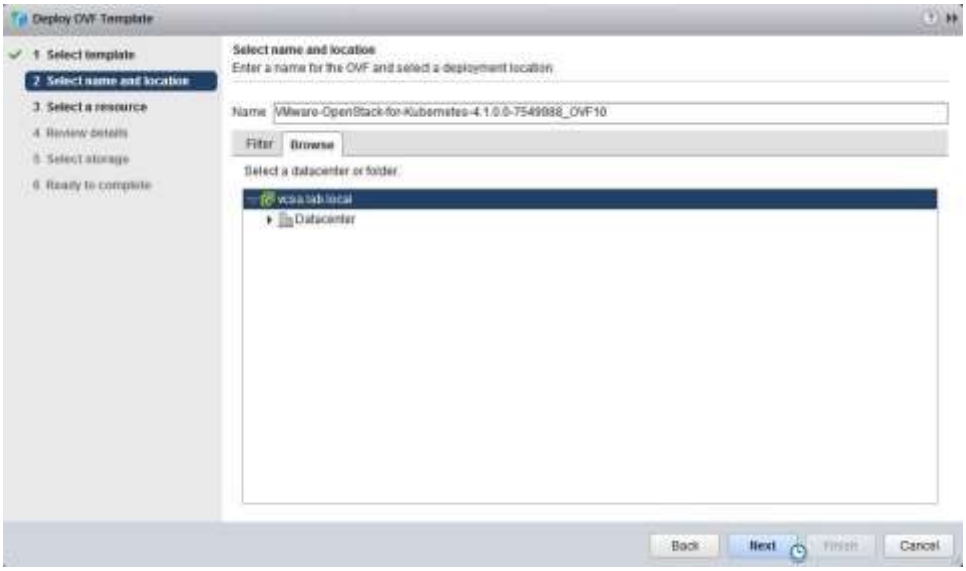


Figura 65: Selección archivo .ova VIO. Fuente: Elaboración propia.

2. Se seleccionó el nombre y la ubicación del servicio virtual.



66: Selección de nombre y ubicación del servicio virtual. Fuente: Elaboración propia.

3. Se seleccionó el clúster del centro de datos.

Figura

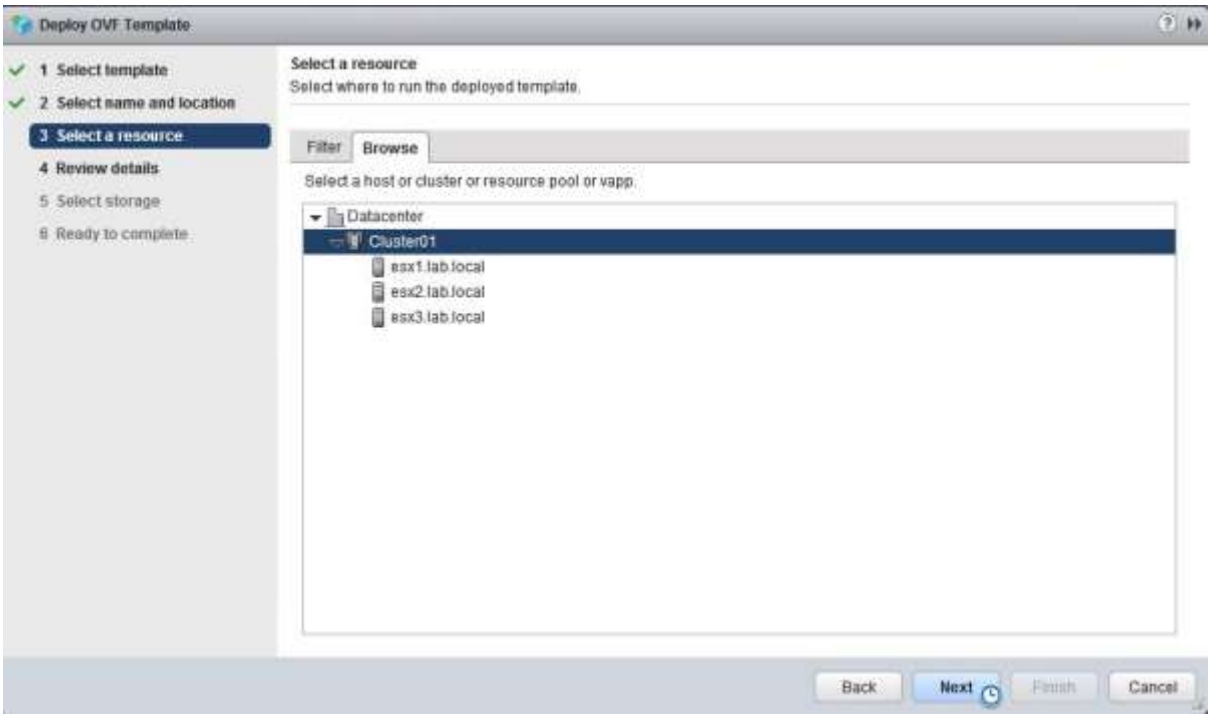
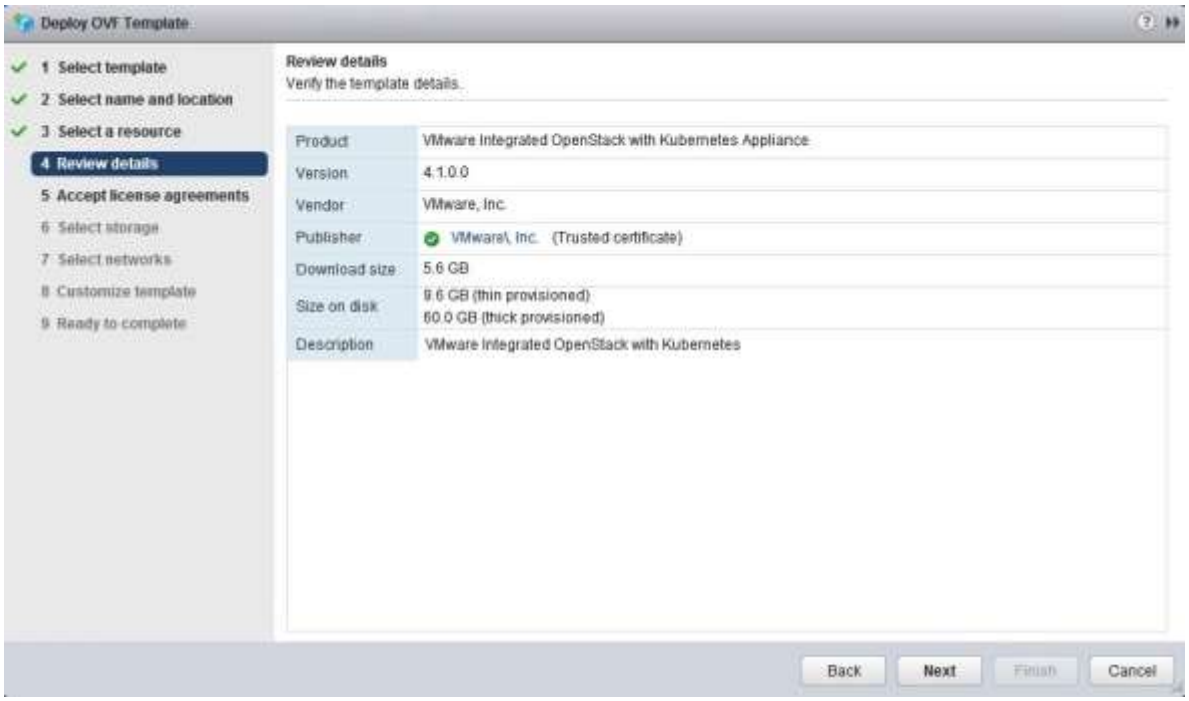


Figura 67: Selección del clúster del centro de datos. Fuente: Elaboración propia.

4. El asistente de VMware mostró un mensaje para verificación de los detalles.



68: Mensaje de verificación de detalles VIO. Fuente: Elaboración propia.

Figura

5. Se aceptó los términos de contrato de la licencia.

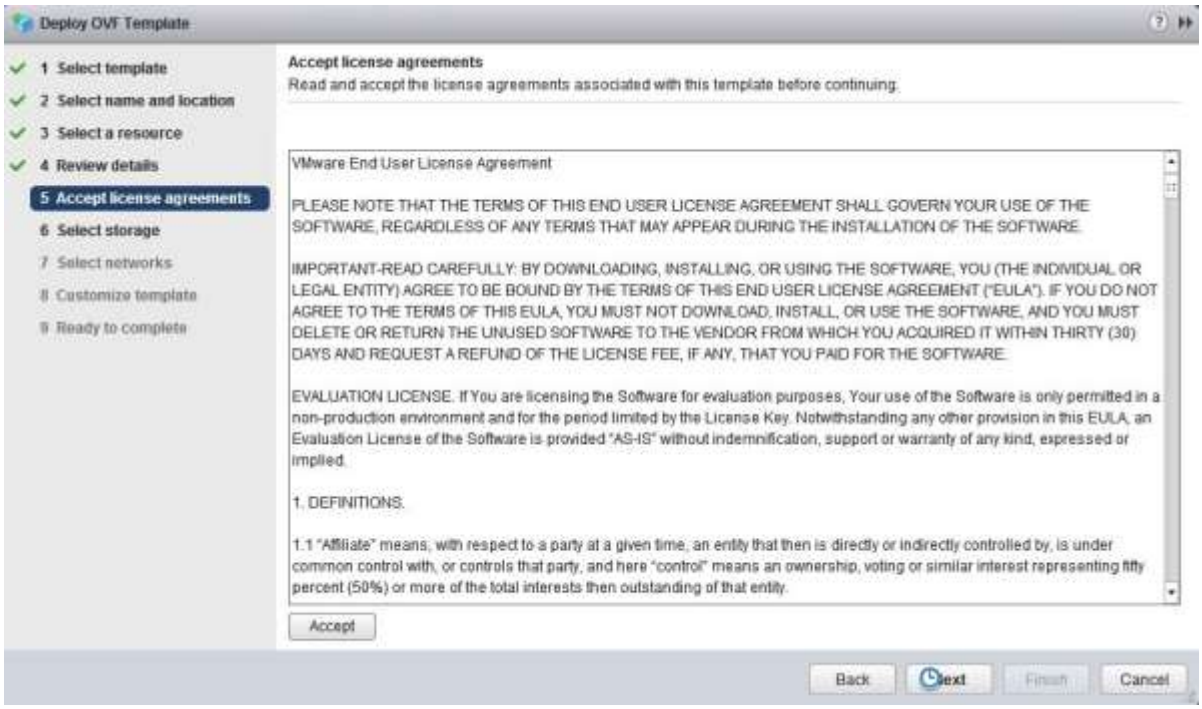
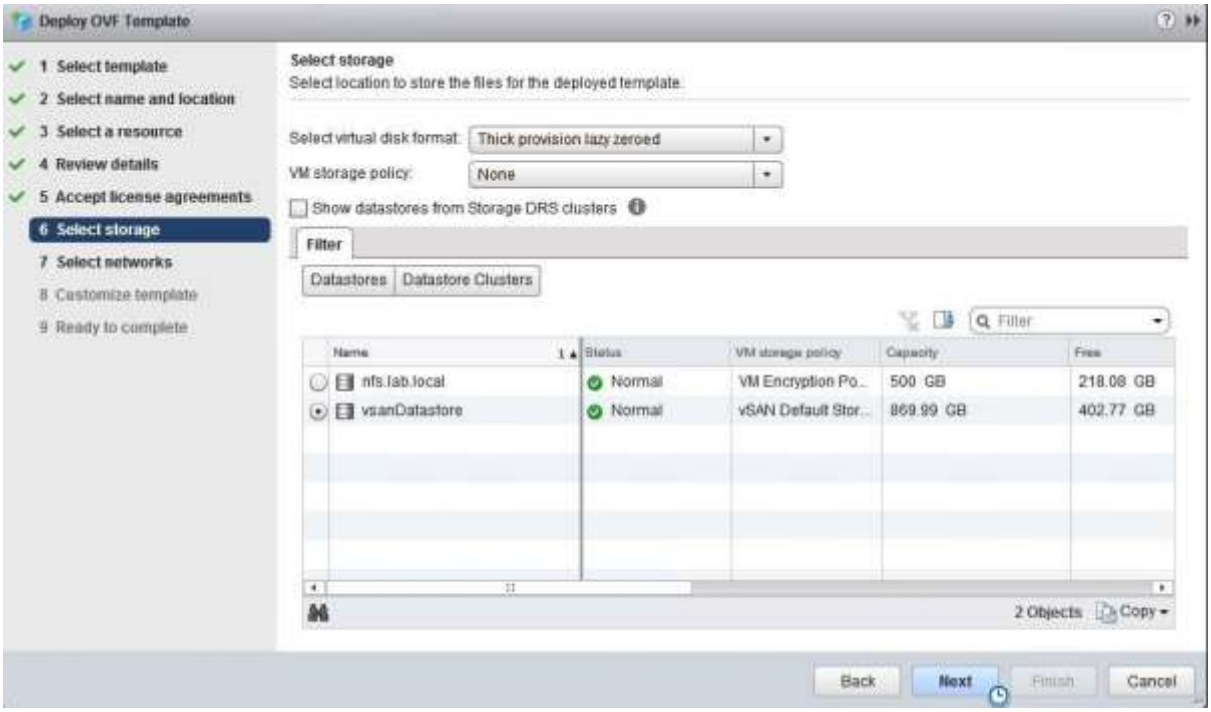


Figura 69: Términos y condiciones VIO. Fuente: Elaboración propia.

6. Se seleccionó la locación del para el almacenamiento.



Figura

70: Selección Almacenamiento VIO. Fuente: Elaboración propia.

7. Se seleccionó la interface de red donde se publicará el aplicativo de administración.

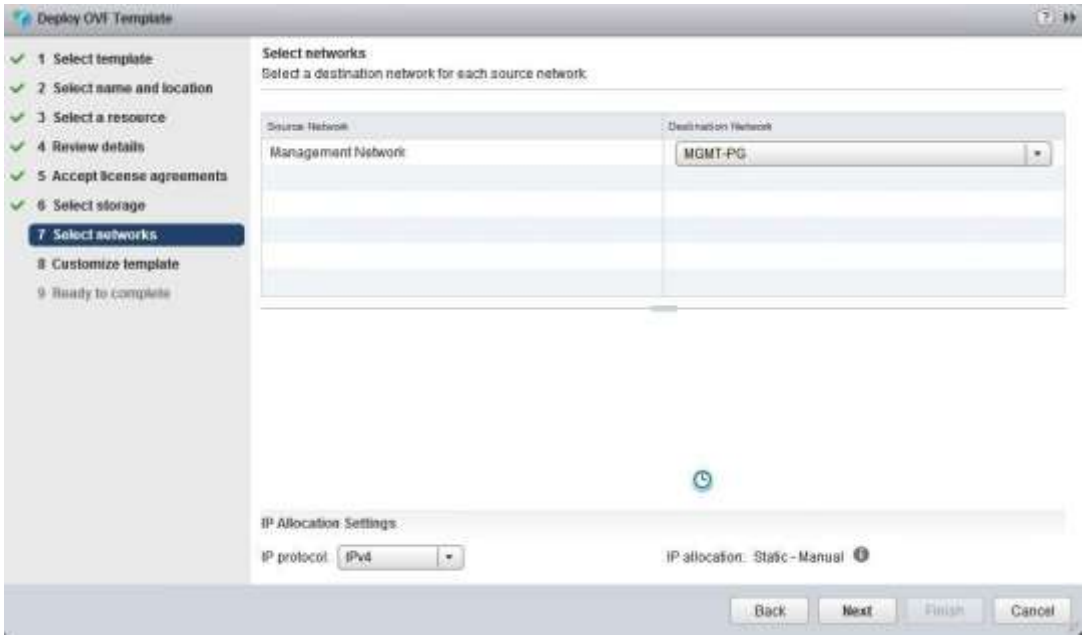
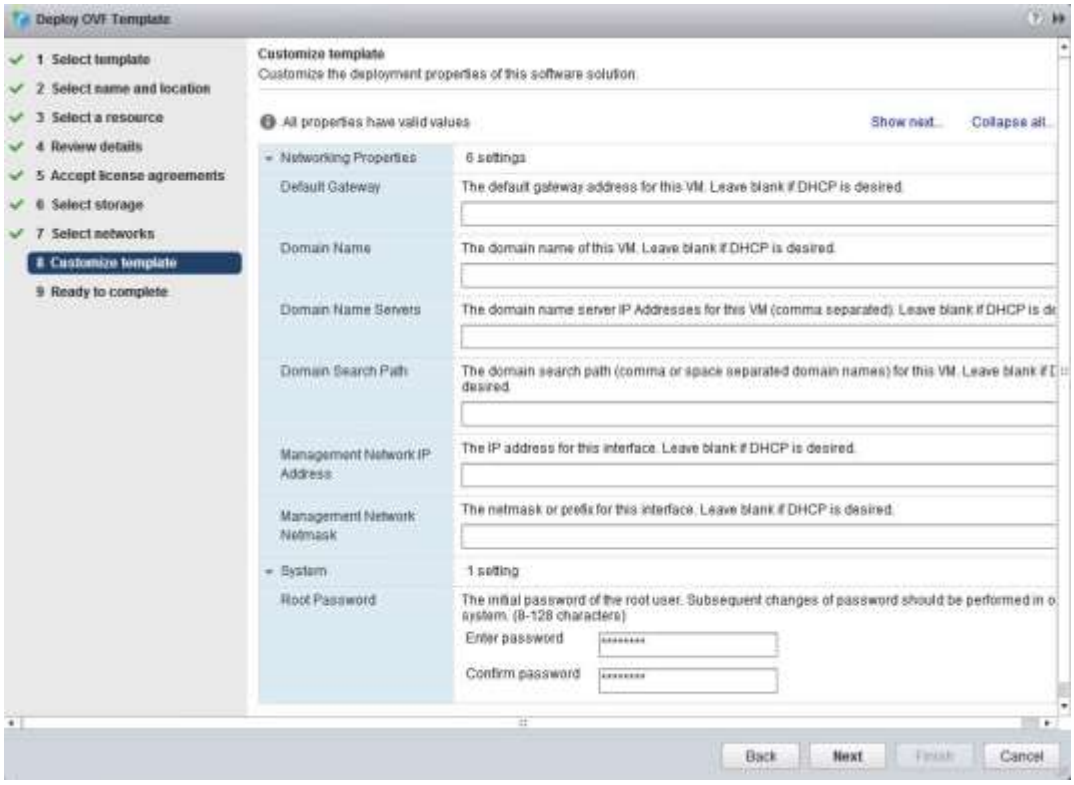


Figura 71: Selección interface de red. Fuente: Elaboración propia.

8. Se realizó configuraciones personalizadas de las propiedades del software.

Figura



72. Configuraciones personalizadas de propiedades del software. Fuente: Elaboración propia.

Figura

9. Se realizó una revisión de las configuraciones para iniciar la instalación.

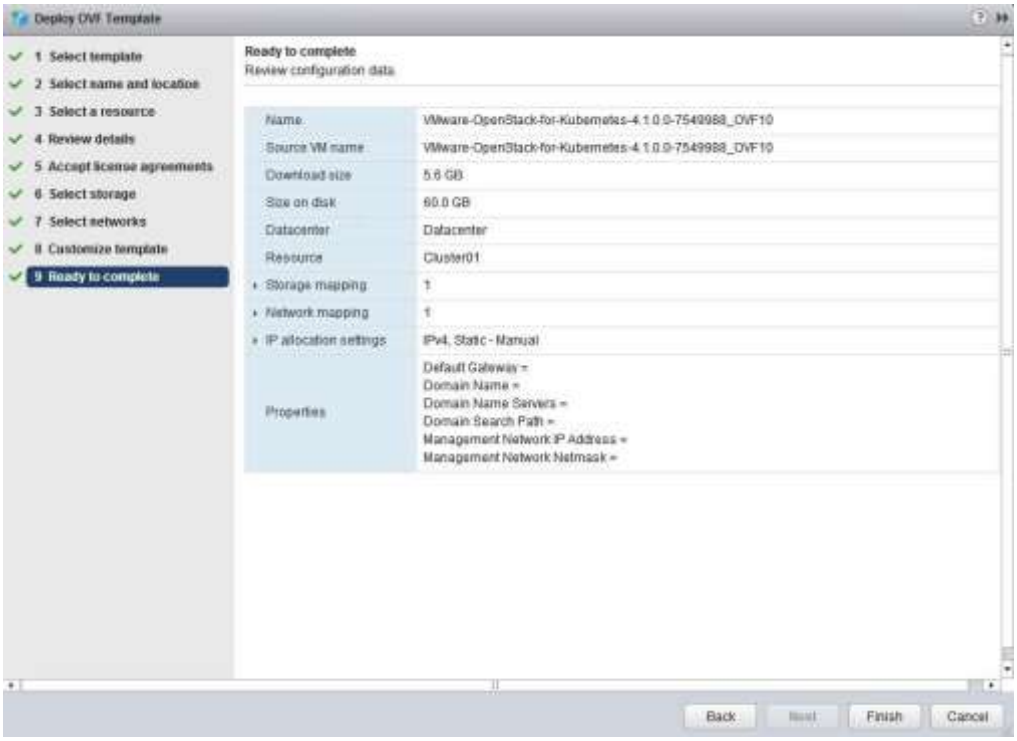


Figura 73: Revisión de configuraciones VIO. Fuente: Elaboración propia.

10. Finalmente, a través del navegador se ingresó a la pantalla de inicio de sesión del aplicativo.

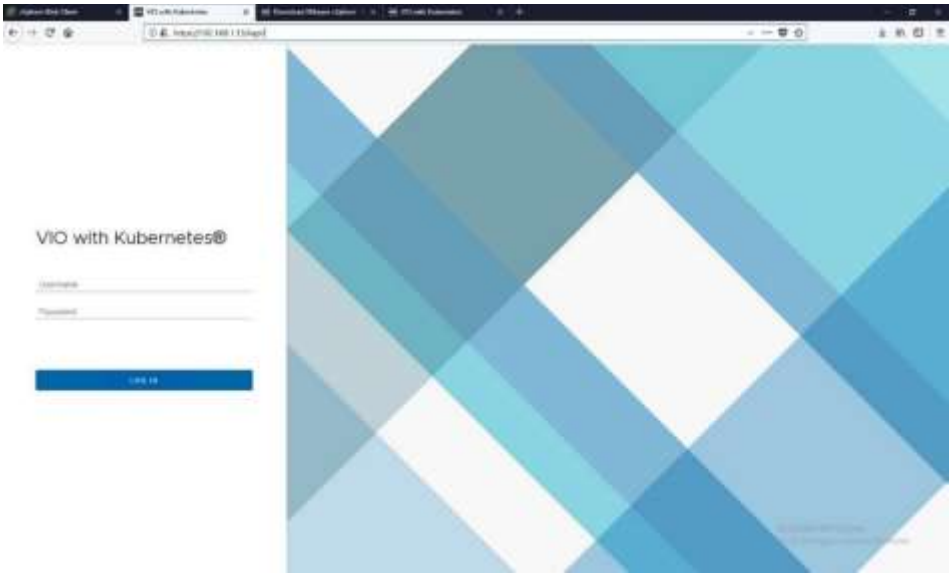


Figura 74: Pantalla de inicio de sesión aplicativo VIO. Fuente: Elaboración propia.