UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y SOCIALES

ANÁLISIS DE LA FACTIBILIDAD PARA LA TRANSFORMACIÓN DE UN CENTRO DE DATOS TRADICIONAL A UNO DEFINIDO POR SOFTWARE

TRABAJO TERMINAL QUE PARA OBTENER EL GRADO DE:
MAESTRA EN GESTIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

PRESENTA

VERÓNICA RICO RODRÍGUEZ

Ensenada, B. C. **Octubre de 2019**

CONSTANCIA DE APROBACIÓN

Director del trabajo terminal: _____

Dr. José Eleno Lozano Rizk

Co-director del trabajo terminal: _____

M.C. Evelio Martínez Martínez

Aprobado por los integrantes del Sínodo:

1.- _____

Sinodal M.C. Oscar Ricardo Osorio Cayetano

2.- _____

Sinodal M.I. Adrián Enciso Almanza

Agradecimientos

En estos párrafos deseo agradecer al Dr. José Eleno Lozano Rizk y al Mtro. Evelio Martínez Martínez que me apoyaron como directores, con paciencia y dedicación me brindaron la guía que necesitaba para la realización de este trabajo.

A la Universidad Autónoma de Baja California por mantener programas de maestría profesionalizantes y realizar convenios con instituciones como Centro de Investigación Científica y de Educación Superior de Ensenada a fin de promover la superación académica de sus empleados.

Al Centro de Investigación Científica y de Educación Superior de Ensenada por proporcionar las facilidades para que realizara mis estudios de maestría, a mis compañeros de trabajo que han sido amigos y colaboradores en el día a día.

A mis maestros por todas las aportaciones y conocimiento que contribuyeron al desarrollo del posgrado.

A Dios, por guiarme y darme las energías, la inteligencia, y todo lo que necesité.

A mi familia, por su apoyo incondicional.

Resumen

En el presente trabajo se aborda el tema de centro de datos en las organizaciones, su adaptación a las necesidades cambiantes de la tecnología a lo largo del tiempo y como se ha observado desde 2012 en adelante, una marcada tendencia la transformación a centros de datos definidos por software.

En este trabajo, se explicarán los conceptos básicos y requerimientos necesarios involucrados para contar con un centro de datos definidos por software.

En particular se realizará un análisis de factibilidad para que un centro de datos tradicional, como es el centro de datos del Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE), se transforme en un centro de datos definido por software (CDDS).

Para el desarrollo de este trabajo, se revisa el estado actual del centro de datos del CICESE y las tecnologías de vanguardia en CDDS, para determinar la posibilidad de que algunos de sus componentes sean utilizados en un CDDS y se propone un procedimiento de ruta de migración a seguir para implementarlo.

Adicionalmente, se propone un modelo de un CDDS basado en tecnologías de código abierto que contiene los elementos básicos de procesamiento, red, seguridad y almacenamientos definidos por software.

Palabras clave: Centro de datos, Virtualización, Tecnologías de la información, OpenStack.

TABLA DE CONTENIDO

Lista de Figuras

Lista de Tablas

1. Introducción.

Vivimos en la era de la información, la sociedad actual genera una gran cantidad de datos y en diversas ocasiones sin tener plena conciencia, estos datos son almacenados y procesados. Al utilizar servicios de internet básicos como el correo electrónico, redes sociales, transacciones bancarias, mediciones de datos meteorológicos, ambientales, sísmicos, de aerolíneas, compañías petroleras, etc., los datos son digitalizados, a través de medios de procesamiento, almacenamiento y comunicaciones.

Para la realización de las actividades fundamentales en las organizaciones es indispensable contar con la capacidad de acceder a este conjunto de datos y recursos de forma segura y eficiente. Algunas veces se reduce a contar con infraestructura de tecnologías de información esenciales, unos pocos servidores y equipos de comunicaciones, otras veces se opta por tener un centro de datos donde converjan todos estos recursos.

Un centro de datos tradicional es un espacio dedicado dentro de la organización que satisface ciertas necesidades físicas y de seguridad, donde se reúne infraestructura de hardware y software, equipos de procesamiento, medios de almacenamiento, redes de comunicaciones, en los que se almacena y procesa la información importante de la organización (Barroso & Hölzle, 2009).

Los centros de datos de vanguardia deben satisfacer determinadas condiciones de temperatura y humedad, contar con sistemas de energía eléctrica que permita operar continuamente, sistemas de seguridad que controlen el acceso, mecanismos de monitoreo del estado y funcionamiento de la instalación. Las características técnicas para la implementación de un centro de datos certificado están definidas en estándares como ANSI/TIA-942 diseñados para este fin (TIA, 2005).

De acuerdo a las necesidades de cada organización, se puede elegir un modelo de centro de datos ubicado en sus propias instalaciones (también llamado "en-sitio"), o en la nube, multiusuarios, por arrendamiento, etc.

Los modelos en-sitio suelen requerir una fuerte inversión en infraestructura, mantenimiento y administración, sin embargo se elige este modelo porque brinda eficiencia y confiabilidad, resulta ventajoso si la organización es mediana o grande y/o sus aplicaciones no cambian frecuentemente, también si requiere garantizar la confidencialidad de la información a sus clientes o la cantidad de datos que almacena es del orden de terabytes o mayor y sería mucho más costoso llevarlo a otro modelo de servicios de cómputo, por ejemplo, en una nube pública.

Para organizaciones pequeñas o medianas, es frecuente que decidan ir por la opción de un modelo de centro de datos rentando un espacio fuera de sus instalaciones, en un centro de datos multiusuario. Los proveedores de estos servicios ofrecen toda la infraestructura de un centro de datos tradicional, espacio, enfriamiento, conectividad y seguridad, bajo un esquema de arrendamiento. Al utilizar este modelo, la organización obtiene la tecnología e interconexión para realizar las funciones esenciales de su organización y se libera de la carga de administración y mantenimiento que conlleva un centro de datos en sitio.

Lo que las organizaciones buscan de un centro de datos es que sea eficiente para resolver sus necesidades de cómputo y comunicación, que le permita garantizar la continuidad de los servicios proporcionados a sus usuarios, clientes, colaboradores; que suministre facilidades para proteger físicamente los equipos de cómputo y de red, así como el activo más importante, la información contenida en ellos. Para las grandes compañías se vuelve más crítico el poder garantizar estas prestaciones, ya que, si las instalaciones esenciales sufren fallos, no podrán realizar las funciones para las que existen y repercutirá en pérdidas económicas considerables.

Aun cuando el concepto de centro de datos tiene décadas de existencia, es interesante notar que en México a partir de 2010-2012 de acuerdo con (Martínez, 2012) el uso y/o actualización de centros de datos se ha incrementado alrededor de 35% año con año, tanto en grandes empresas como en proveedores de servicio.

Los centros de datos han continuado transformándose, uno de los cambios trascendentales que han tenido, fue a partir del resurgimiento de la virtualización hacia finales de los 90's; compañías como *VMWare*[1]*, Citrix*[2]*, Microsoft*[3]*,* impulsaron el desarrollo de tecnologías para virtualizar los componentes esenciales del centro de datos, cómputo, memoria, redes y almacenamiento.

El software de virtualización hace posible que los recursos físicos de la infraestructuras del centro de datos sean desacoplados del hardware, tanto el poder de procesamiento, recursos de memoria, los medios físicos de conectividad y protocolo de la red, así como los recursos físicos y lógicos de los sistemas de almacenamiento, son abstraídos y presentados como recursos compartidos, de esta manera, en lugar de que las aplicaciones se ejecuten directamente sobre hardware*,* están contenidas en máquinas virtuales, redes virtuales y sistemas de almacenamiento virtuales.

La madurez en cuanto al uso de la virtualización en los centros de datos ha permitido proveer infraestructuras definidas por software que puedan presentarse como servicios, lo cual puso las bases para que, hacia finales de 2012(Fichera, Washburn, & Chi, 2012), surgiera el paradigma de centro de datos definidos por software (CDDS).

"Un CDDS es una capa de abstracción integrada que define un centro de datos completo por medio de una capa de software que presenta los recursos del centro

[1] https://www.vmware.com
[2] https://www.citrix.com
[3] https://www.microsoft.com

de datos como conjuntos de recursos virtuales y físicos, y les permite integrarse en servicios arbitrarios definidos por el usuario" (Fichera et al., 2012).

La implementación de CDDS aún no se adopta por la generalidad de las organizaciones, sin embargo, las grandes corporaciones como Amazon (AWS), Google (cloud.google.com), entre otras, ofrecen sus servicios en la nube basados en este tipo de infraestructura. Además, es importante considerar el impacto de los CDDS que se prevé a futuro cercano, ya que, según analistas de Gartner (Gartner, 2015) las tendencias para centros de datos indican que para 2020 el 75% de las empresas de Global 2000 requerirán de centros de datos definidos por software (CDDS).

Sin embargo, cada organización debe realizar un análisis a fin de determinar si es posible realizar una migración de su centro de datos tradicional a un CDDS. El personal de Tecnologías de la Información (TI), analizará los elementos con que cuenta su centro de datos; si es factible técnicamente su transformación hacia un CDDS, así como determinar los requerimientos, metodologías o acciones a seguir, y proponer posibles soluciones para su organización.

En este trabajo se presenta un análisis de la factibilidad de transformar un centro de datos tradicional del CICESE para llegar a ser un centro de datos definido por software y se propone una ruta migración a seguir para integrar la infraestructura existente a CDDS basado en tecnologías de código abierto.

1.1. Antecedentes.

Desde el inicio del Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE) en 1973, el establecimiento de un área computacional para el apoyo a las actividades sustantivas del centro, como son la investigación y los estudios de posgrado, ha sido una de sus características sobresalientes. Contar con

un centro de procesamiento electrónico en sitio se estableció como una de sus prioridades debido al manejo de información confidencial y proyectos estratégicos nacionales que así lo requieren.

El proceso para llegar a tener el centro de datos con el que actualmente cuenta el (CICESE) ha sido gradual, en la medida que sus necesidades en infraestructura de tecnologías de información han aumentado.

A mediados de la década del 2000 la mayor parte de los equipos que proporcionaban los servicios para el CICESE, como bases de datos, correo electrónico, portales web, sistemas de almacenamiento y compartición de datos, entre otros, estaban distribuidos en diferentes edificios del campus, incluso en espacios de uso común o bajo el resguardo del administrador, esta situación empezó a presentar inconvenientes sobre la seguridad de acceso físico a los equipos, en otros casos las condiciones ambientales de temperatura y humedad afectaron su funcionamiento, además su distribución dificultaba darles mantenimiento o no siempre era posible identificar situaciones de emergencia con prontitud y para resolverlas se necesitaba desplazarse al área requerida.

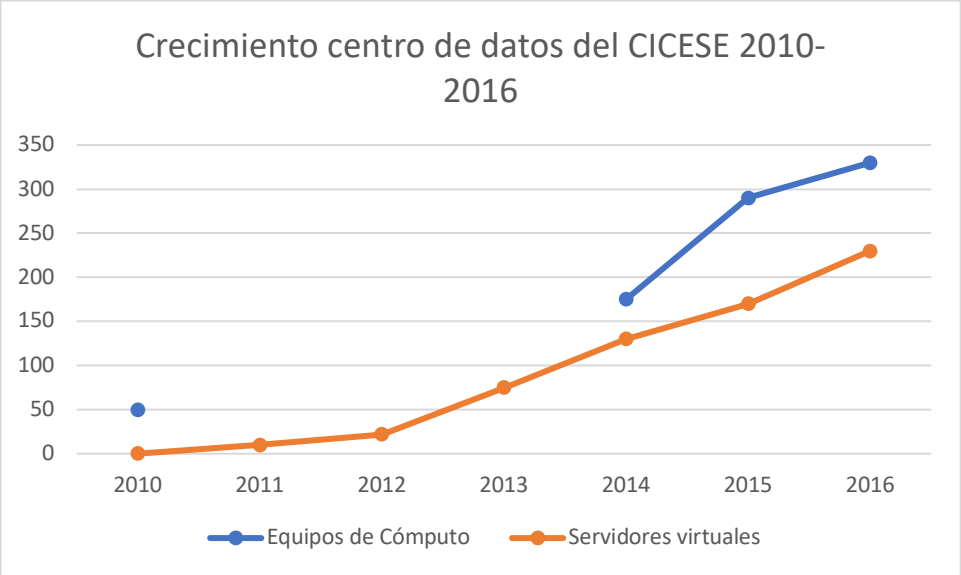
Para solucionar parte de la problemática, hacia finales del 2008 se aprovechó un espacio físico disponible, que en sus inicios solo tenía contemplado el hospedaje de los equipos de supercómputo existentes, sin embargo, contaba con la infraestructura física básica para iniciar un centro de datos, esta situación permitió centralizar los equipos que se encontraban dispersos. Alrededor del 2010 se adquirieron sistemas de virtualización, lo cual permitió consolidar la mayoría los servicios y servidores tipo estación de trabajo en máquinas virtuales.

Con el trascurso de los años, se han realizado adecuaciones al centro de datos con la finalidad de mejorar las condiciones de temperatura, humedad, energía y acceso físico a los equipos de cómputo esenciales para la operación del Centro. Se fortaleció infraestructura de soporte con la adquisición y/o renovación de equipos de aire

acondicionado de precisión, plantas de energía eléctricas de emergencia, actualización de equipos de red, sistemas de control de acceso, sistemas de monitoreo, actualización de infraestructura de virtualización, clúster de alto rendimiento, sistemas de almacenamiento, todos ellos de gran utilidad para garantizar la seguridad de la información y continuidad de los servicios de súper cómputo, virtualización, almacenamiento, web, cómputo científico, sistemas administrativos, entre otros servicios que son considerados estratégicos para la operación del Centro,

De la misma manera ha ido en aumento el número de aplicativos que solicitan ser hospedados en el centro de datos para brindar soporte tecnológico al desarrollo de proyectos de investigación, como se puede observar en la Figura 1.1 proporcionada por información pública del CICESE, donde es de notar que al 2016 se contaba con más de 300 equipos físicos y más de 200 sistemas virtualizados hospedados en su centro de datos.

Figura 1.1 Crecimiento del centro de datos del CICESE 2010-2016. Fuente propia con base en (Rivera Rodríguez & Lozano Rizk, 2017)



Todos estos cambios, sin duda han significado un avance tecnológico trascendental para la institución, sin embargo, también ha traído consigo problemáticas nuevas.

Precisamente generado por el crecimiento del centro de datos del CICESE en los últimos años, los administradores se enfrentan a la necesidad de integración de hardware de diferentes marcas y modelos, un considerable aumento de tráfico en la red, la necesidad de capacidades de almacenamiento mayores a las que se contaban, etc.

Adicionalmente, es notable el costo operativo que conlleva una administración cada vez más compleja, debido a que actualmente se requiere administrar de forma independiente los equipos de comunicaciones y red de datos, las infraestructuras de cómputo de alto desempeño y de virtualización, sistemas de almacenamiento independientes, etc., lo cual implica mayor cantidad personal involucrado, aumentando la generación de posibles errores, incremento en los tiempos de respuesta y del uso de recursos económicos.

1.2. Área de oportunidad.

Una situación particular que se presenta al evolucionar de los centros de datos tradicionales, como el del CICESE, es que a medida que van creciendo y se realizan actualizaciones, se adquiere infraestructura de hardware de diferentes modelos, marcas, sistemas operativos, que, si bien cuando se introducen tales equipos en el centro se busca que cumplan con estándares de comunicación, finalmente cuentan con especificaciones muy particulares que afectan la compatibilidad entre los equipos, lo cual impide aprovechar los recursos al máximo.

Por ejemplo, existen algunos sistemas de almacenamiento cuyo software de administración no son compatibles y por lo tanto no pueden compartir recursos entre sí para aprovechar el máximo su capacidad, también existen infraestructuras de virtualización que se administran de forma independiente, así otros casos que, por

limitaciones como estas, llegan a caer en desuso, además la acumulación de hardware antiguo genera un aumento de gasto económico y energético.

Por otra parte, debido a que el tráfico de red aumenta entre equipos que se encuentran en la misma capa es necesario la implementación de modelos de enrutamiento y políticas de seguridad para el tráfico este-oeste, esto también complementaría la seguridad tradicional o perimetral que existe.

Otro aspecto a considerar es que la administración de los centros de datos tradicionales se vuelve sumamente compleja, debido a que los profesionales a cargo deben tener conocimientos del hardware de los diferentes equipos que existen en el sitio, el software que tiene instalado cada uno de estos equipos, diferentes sistemas operativos y consolas de administración. Ahora bien, cuando surgen cambios no previstos dentro del centro de datos o se desea realizar actualizaciones, se enfrenta al desafío de cómo lograrlo de forma ágil y eficaz, como llegar a un mejor aprovechamiento de los recursos de tecnologías de información y reducir los tiempos de respuesta a incidentes y solicitudes.

De acuerdo con(Gartner, 2015), una de las tendencias que se proponen para solucionar esta problemática, son los Centros de Datos Definidos por Software (CDDS), con esta alternativa aseguran que se pueden lograr grandes niveles de eficiencia, rendimiento, seguridad y productividad englobados en una misma solución tecnológica.

Contar con una capa de infraestructura de software que nos permita administrar los recursos existentes dentro de nuestro centro de datos, un sistema que nos permita visualizar los recursos con que contamos en una sola interfaz administrativa, establecer políticas de uso de los recursos, resultará en el mejor aprovechamiento de los recursos de hardware y en la reducción de tiempos de respuesta a incidentes y solicitudes.

1.3. Preguntas de investigación.

- ¿Es factible migrar el centro de datos tradicional del CICESE a un centro de datos definido por software?
- ¿Qué requerimientos debería satisfacer los dispositivos de Cómputo, almacenamiento y redes, para lograr integrarse a un CDDS?
- ¿Es posible trazar un procedimiento de migración a seguir?

1.4. Hipótesis.

A través del uso de un centro de datos definido por software se obtendrá una administración centralizada y eficiente del centro de datos del CICESE, así como un mejor aprovechamiento de los recursos de la infraestructura con que cuenta.

1.5. Objetivos.

A continuación, mencionaremos los objetivos, tanto generales como específicos, que trazarán el curso de esta investigación.

1.5.1. Objetivo General.

Analizar la situación actual del centro de datos tradicional del CICESE para determinar la factibilidad de transformarlo a un centro de datos definido por software.

1.5.2. Objetivos específicos.

a) Analizar el estado actual del centro de datos del CICESE.
b) Estudiar el estado del arte de las tecnologías para centros de datos definidos por software.
c) Analizar la factibilidad técnica, operativa y económica para que el centro de datos del CICESE llegue a ser un CDDS.

d) Elaborar un procedimiento de ruta de migración para transformar el centro de datos del CICESE en un CDDS.
e) Presentar un modelo de un CDDS basado en tecnologías de código abierto.

1.6. Justificación.

Las organizaciones se enfrentan constantemente a la presión de adquirir nueva tecnología para no caer en la obsolescencia, sin embargo, es prioritario analizar si estas nuevas tecnologías son necesarias para la organización; si se requiere invertir, asegurarse de que tal inversión es realmente redituable, sobre todo en organizaciones donde debe justificarse el gasto ante organismos gubernamentales.

Al analizar los beneficios que se obtienen de la implementación de CDDS descritos por (Distributed Management Task Force (DMTF), 2014) se percibe la forma en que podrían mejorar el funcionamiento de un centro de datos tradicional como es el del CICESE.

Como en un CDDS la infraestructura puede llegar a estandarizarse, los centros de datos tradicionales podrían liberarse gradualmente de la dependencia a marcas, software propietario y pago de licenciamiento, esto representará a futuro una reducción en los costos en la adquisición de equipos, incluso puede reutilizarse la infraestructura existente que sea compatible con el software para CDDS.

Como el modelo de CDDS se basa en software inteligente que permite abstraerse del hardware, es posible compensar las fallas de hardware que se presenten, entregando una alta disponibilidad del servicio a un costo menor.

Además, debido a que el CDDS provee un software inteligente para gestionar la infraestructura sin tener que recurrir a la configuración manual de cada uno de los componentes, se aligera la carga administrativa del centro de datos.

Otra ventaja que ofrece un CDDS es el aprovisionamiento automatizado de los recursos, los cuales se pueden hacer disponibles de acuerdo a la demanda de aplicaciones.

1.7. Organización del trabajo terminal.

El presente trabajo de investigación está organizado de la siguiente manera: en el capítulo 3 Marco teórico se exponen los conceptos principales que sustentan el trabajo, presentamos las definiciones de virtualización, Cómputo, redes, almacenamiento definido por software, así como los aspectos de seguridad que son necesarios considerar para un centro de datos definido por software.

En el capítulo 4 se explica la Metodología a seguir para el desarrollo del trabajo. Se presentan cuatro fases principales, así como los instrumentos utilizados para obtener la información y llegar a los resultados.

A partir del capítulo 5 se inicia con la presentación de los resultados obtenidos; primeramente, una vista de su estado actual del centro de datos del CICESE, mediante la realización de inventario de hardware y software.

En el capítulo 6, se analizan tres soluciones para centro de datos definidos por software existentes en el mercado y se destaca el papel alternativas de código abierto que representan ahorros para entidades gubernamentales, como es la situación del CICESE.

En el capítulo 7 se exponen los resultados sobre el análisis de factibilidad de llevar el centro de datos del CICESE a un centro de datos definido por software, se consideran los aspectos técnicos, económicos y operacionales que están implicados.

En el capítulo 8 se propone un mapa o plan de migración que detalla las fases a seguir para lograr que los elementos del centro de datos tradicional del CICESE que sean compatibles puedan ser integrados a un centro de datos definido por software.

Y en el capítulo 9 se detalla la propuesta de un modelo de un centro de datos definido por software basado en tecnologías de código abierto con los elementos básicos que prueben su funcionalidad.

Finalmente, en el capítulo 10 se presentan las conclusiones sobre los resultados obtenidos del trabajo realizado, así como posibles oportunidades de trabajo a futuro relacionado.

2. Marco Teórico.

En este capítulo nos centraremos en definir conceptos básicos que facilitaran la comprensión del trabajo de investigación. Se divide en las siguientes secciones:

- Virtualización
- Centro de datos definido por software
- Redes definidas por software.
- Almacenamiento definido por software.
- Seguridad de la información en centros de datos definidos por software.

2.1. Virtualización.

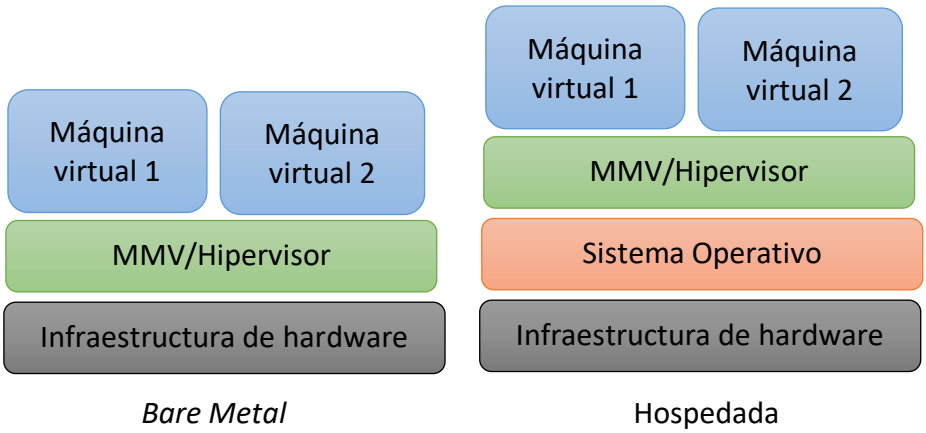
Desde mediados de la década de 1960 se establecieron las bases para lo que hoy se conoce como virtualización, cuando IBM desarrollo el programa de Control – Sistema de Monitoreo de Cambridge para la VM/370, el cual permitían al usuario ejecutar un sistema aislado en un entorno informático compartido. Sin embargo, fue probablemente hasta finales de 1990 cuando un proyecto de investigación de Stanford llamado 'Disco' que llegaron a implementarse lo que hoy conocemos como máquinas virtuales y se consolidó en la empresa VMWare. (Bazargan, Yeun, & Zemerly, 2016)(Douglis & Krieger, 2013).

De acuerdo con (Uhlig et al., 2014) la virtualización incluye una nueva capa de software llamada monitor de maquina virtual (MMV) cuya función es controlar el acceso a los recursos disponibles de la capa de física de la infraestructura anfitriona como CPU, memoria, red y almacenamiento, para presentarlos a cada sistema operativo invitado como un conjunto de interfaces virtuales que constituirán la máquina virtual.

El monitor de máquina virtual o hipervisor puede ser instalado como el mismo sistema operativo de la infraestructura anfitriona, conocido como *Bare Metal*. O bien,

el hipervisor puede instalarse sobre un sistema operativo nativo y ejecutarse como una aplicación más, como se aprecia en la Figura 2.1. (Bazargan et al., 2016)

Figura 2.1 Tipos de Virtualización.



El hipervisor cumple con la función de eliminar la dependencia existente de un sistema operativo con el hardware físico, así es como se pueden ejecutar múltiples sistemas operativos diferentes sobre un equipo físico clase x86 independientemente de la estructura o modelo de hardware. De acuerdo con (Bazargan et al., 2016; Uhlig et al., 2014) los atributos de la virtualización se pueden resumir en los tres siguientes aspectos:

- Aislamiento: cada máquina virtual esta aislada del resto de las máquinas que se están ejecutando en el mismo equipo virtualizado, el hipervisor impide que interactúen las aplicaciones que se ejecutan en cada una de ellas, incluso están aisladas del sistema operativo anfitrión.

- Interposición: el hipervisor administra todas las peticiones de E/S de los sistemas operativos de las maquinas virtuales huéspedes, que solicitan acceso a los dispositivos físicos.

- Inspección: el hipervisor es capaz de acceder a los estados de las máquinas virtuales, como son estado de memoria, CPU y cualquier otro dispositivo de E/S

que tenga asignado. Esta habilidad permite al hipervisor encapsular la máquina virtual y realizar operaciones sobre ella, como crear instantáneas del estado actual, reproducir un evento o revertirlo.

A continuación, se mencionan algunas de los beneficios de la virtualización como son la consolidación, migración, confiabilidad y seguridad. (Bazargan et al., 2016)

Con la virtualización se consolidan múltiples entornos virtuales en una única plataforma de hardware que satisface sus demandas de recursos de procesamiento, memoria, almacenamiento y red. Como resultado se obtiene una mejor utilización de los recursos.

Así mismo, facilita la migración de sistemas heredados al proporcionar una plataforma común y ampliamente compatible sobre la que se pueden ejecutar entornos de prueba o desarrollo y eliminar gradualmente plataformas más antiguas, con riesgos de seguridad a un hardware más nuevo, compatible y con un impacto mínimo.

La virtualización ofrece confiabilidad al mantener la funcionalidad y la disponibilidad de operación, debido a la capacidad de encapsulamiento y aislamiento de máquinas virtuales si su sistema operativo falla o alguna de sus particiones se corrompen, no tendrá efecto en el resto de las maquinas virtuales hospedadas.

Incluso desde el punto de vista de la seguridad de la información, si el sistema es comprometido, al estar encapsulada la máquina virtual, no afectará los servicios que ofrecen otros sistemas hospedados.

Entre otras ventajas de la virtualización, está que permite la asignación de recursos dinámicamente incluso en un tiempo de ejecución determinado, sin preocuparse por la adquisición, configuración o instalación del hardware.

La virtualización también facilita las operaciones de mantenimiento, gracias a la propiedad que tienen las máquinas virtuales de ser encapsuladas pueden desconectarse del hardware en el que se están ejecutando y migrarse a una plataforma diferente.(Uhlig et al., 2014)

Las características mencionadas hacen posible apoyar los sistemas de alta disponibilidad en los que utilizando un conjunto de al menos tres nodos que comparten recursos de red y almacenamiento virtualizados puedan mantener en ejecución las máquinas virtuales cuando uno de los nodos falla, el tema es ampliamente sustentado en (Gadir, Subbanna, & Vayyala, 2005)

2.2. Centro de datos definido por software.

El concepto 'definido por software' se basa en que interfaces de programación de aplicaciones *(APIs por sus siglas en inglés)* se utilicen para controlar y gestionar los recursos y dispositivos. Esencialmente 'definido por software' es la capacidad de la capa de control para controlar todos los recursos subyacentes, sin distinguir las variaciones de proveedores, aislándolos físicamente de los recursos de hardware en la capa de datos. (Ala Darabseh et al., 2015)

De manera, que la madurez en cuanto al uso de la virtualización y las infraestructuras definidas por software situaron las bases para que, hacia finales de 2012 surgiera el paradigma de centro de datos definidos por software (CDDS).

Aunque existen una gran cantidad de ideas que se manejan en torno a lo que es un CDDS, enseguida se mencionan algunas de definiciones formales,

"Un CDDS es una capa de abstracción integrada que define un centro de datos completo por medio de una capa de software que presenta los recursos del centro de datos como conjuntos de recursos virtuales y físicos, y les permite integrarse en servicios arbitrarios definidos por el usuario." (Fichera, Washburn , & Chi, 2012)

“Un CDDS es una instalación de almacenamiento de datos en la que todos los elementos de la infraestructura (redes, almacenamiento, CPU y seguridad) se virtualizan y se entregan como un servicio. La implementación, la operación, el aprovisionamiento y la configuración se abstraen del hardware. Esas tareas se implementan a través de la inteligencia del software. Steve Herrod, 2012.” (Rouse, 2017)

*“*CDDS: una abstracción programática de cálculo lógico, red, almacenamiento y otros recursos, representados como software. Estos recursos se descubren dinámicamente, se aprovisionan y se configuran en función de los requisitos de carga de trabajo. Por lo tanto, el CDDS permite la orquestación basada en políticas de cargas de trabajo, así como la medición y gestión de los recursos consumidos.”(Distributed Management Task Force (DMTF), 2014)

De estos conceptos se desprende que un CDDS depende en gran medida de recursos abstraídos a partir de elementos virtualizados y que gracias a las interfaces de programación de aplicaciones (*APIs*) es posible gestionarlas.

De acuerdo con (Distributed Management Task Force (DMTF), 2014) las funcionalidades que se lograran tener con un CDDS son:

- Acceso a la computación lógica, red, almacenamiento y otros recursos.
- Descubrimiento de recursos.
- Aprovisionamiento automatizado de recursos lógicos basados en requerimientos de cargas de trabajo.
- Medición y gestión de consumo de recursos.
- Orquestación basada en políticas definidas para asignación de recursos de acuerdo a las cargas de trabajo.
- Seguridad (autorización, autenticación, auditoria), Sistemas de detección y prevención de intrusos (IDS e IPS), firewalls.

Como resultado, el CDDS cuenta con las siguientes características (Ala Darabseh et al., 2015) (Distributed Management Task Force (DMTF), 2014):

- Estandarizado: al utilizar recursos de manera lógica la Infraestructura puede llegar a ser homogénea, provista incluso a través de un conjunto de hardware x86 standard y así es posible eliminar la complejidad innecesaria y el compromiso de usar marcas específicas.

- Homogéneo: Una plataforma unificada, optimizada para todo el centro de datos, para soportar de manera flexible cualquier carga de trabajo.

- Adaptativo: con el aprovisionamiento automatizado se logra que la infraestructura presentada sea auto-programable de acuerdo a la demanda cambiante de las aplicaciones, permitiendo el máximo nivel en cuanto a ejecución, agilidad y eficiencia.

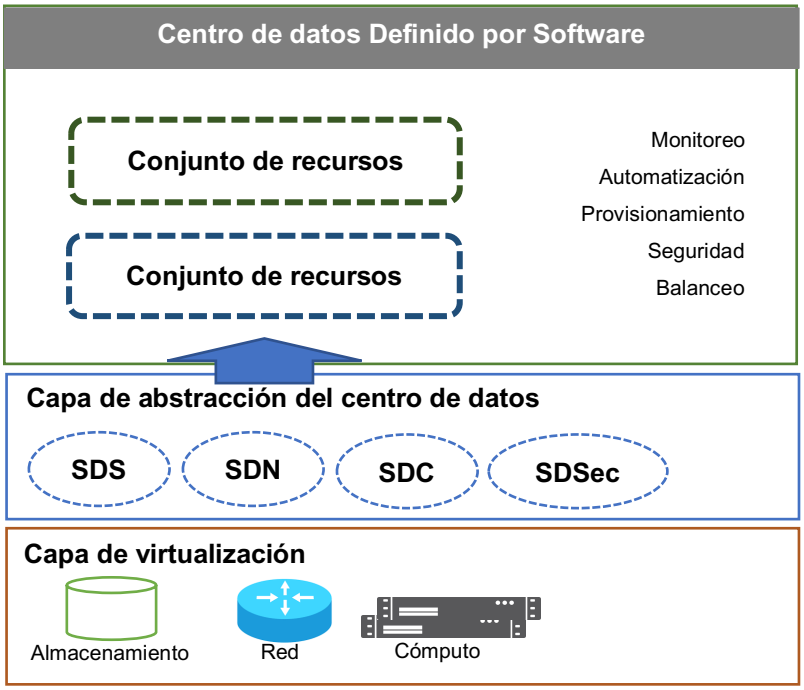
- Automatizado: Un orquestador de gestión con inteligencia incluida, para eliminar los complejos scripts de administración, para realizar operaciones con menos esfuerzo manual y para obtener un ahorro significativo en los costos.

- Resiliente: Como el modelo de CDDS se basa en software inteligente que permite abstraerse del hardware, es posible compensar las fallas de hardware que se presenten, entregando disponibilidad sin precedentes al mínimo costo.

Así con una capa de software, conocida como Capa de abstracción del centro de datos, se presentan recursos estandarizados de cómputo, almacenamiento, red y seguridad en elementos definidos por software; por sus siglas en inglés SDC, SDN, SDS, SDSec, los cuales detallaremos en los siguientes apartados.

Un CDDS permite configurar dinámicamente aplicaciones, infraestructura y recursos tecnológicos, este modelo ofrece administrar el centro de datos como un sistema unificado, es decir, visualizar y controlar los recursos con que contamos en una sola interfaz administrativa. Los administradores del centro de datos pueden construir sus topologías y escenarios adaptados a su entorno a fin de satisface los requisitos que demanden las organizaciones (Ala Darabseh et al., 2015). La Figura 2.2 ilustra los componentes que integraran in CDDS que presentar un conjunto de recursos como servicio.

Figura 2.2 Arquitectura de centro de datos definido por software.



La implementación de CDDS aún no se adopta por la generalidad de las organizaciones, sin embargo, las grandes corporaciones como AWS (Amazon Web Service, 2017), Google Cloud (Google, 2019), *RackSpace* (Rackspace, 2019), entre otras, ofrecen sus servicios en la nube basados en este tipo de infraestructura. Además, es importante considerar el impacto de los CDDS que se prevé a futuro cercano, ya que, según analistas de *Gartner* (Gartner, Inc. , 2015) las tendencias para centros de datos indican que para el 2020 el 75% de las empresas de Global 2000 requerirán de centros de datos definidos por software (CDDS).

2.2.1. Redes definidas por software (SDN).

Las redes de computadoras y los protocolos de comunicación, juegan un papel crucial para la conectividad en los centros de datos, para que esto pueda suceder es necesario un sofisticado proceso dentro de los equipos de conmutación de paquetes, *switches, routers*, etc.

El funcionamiento de las redes de computadoras tradicionales podemos verlas divididas en tres capas o planos (Gorannson P., Black C., 2015):

- Plano de datos, el cual se encarga de la recepción y transmisión de paquetes,
- Plano de control, aplica una serie de protocolos de control de acuerdo a la configuración y tipo de *switch* para determinar qué, cómo y cuándo, transmite los paquetes que ha recibido del plano de datos;
- Plano de gestión, donde el administrador de la red configura y monitorea lo que pasa en el switch.

Comúnmente los planos de control y datos están incrustados en los dispositivos de red, en los principios del internet se consideró importante para garantizar la resiliencia de la red y ha sido muy eficaz en términos de rendimiento de la red, sin embargo, reduce la flexibilidad y obstaculiza la innovación y evolución de la infraestructura de red (Kreutz et al., 2015)

Además, si se considera que la comunicación entre estos planos puede darse de forma horizontal, cuando elementos de la misma categoría se comunican entre sí o bien puede que se comuniquen con elementos de otras categorías, entonces se llama comunicación vertical; siendo en la mayoría de los casos de esta última forma.

De manera que cuando un administrador requiere configurar políticas en la red ya sea por cambios y actualizaciones planeadas o no, es necesario que configure individualmente cada dispositivo de red, si, además sumamos que cada uno puede

ser de diferente fabricante, el administrador debe especializarse en la codificación o comandos que cada fabricante requiera. De hecho, de acuerdo con (Kreutz et al., 2015) estos entornos de red, donde la comunicación se da de forma vertical, se dificulta adaptarse a fallas, cambios y aumento de cargas.

Considerando la situación descrita anteriormente, es que surge la necesidad de desarrollar una programación bien definida que permita romper con las limitaciones de las infraestructuras de red actuales y que mejore su velocidad, fiabilidad, seguridad, y eficiencia energética.

Sin embargo, por muchos años, estas ideas solo quedaron en laboratorios de investigación, no fue sino hasta 2009 cuando en la Universidad de Stanford, CA, USA, como parte del proyecto *OpenFlow*[4]*,* se generó el estándar abierto que lleva su nombre, si bien no es el único, se ha popularizado su uso.

La propuesta consiste en instalar pequeños fragmentos del firmware *OpenFlow* en los dispositivos de red y este brinda acceso a las tablas de flujo y reglas que indican a los switches y enrutadores como dirigir el tráfico de red, a la vez que protege las instrucciones de enrutamiento propietarias. Este acceso basado en software permite a los desarrolladores definir el diseño de la red, fue entonces cuando se mencionó por primera vez el término *Software Defined Network (SDN)* (Mckeown et al., 2008)

Desde entonces se han acuñado muchas definiciones para SDN, sin embargo, de acuerdo con (Kreutz et al., 2015) existen cuatro pilares fundamentales para el diseño de una SDN:

- Los planos de control y datos están desacoplados, las funcionalidades de control son removidas de los dispositivos de red, que se convertirán en retransmisores de paquetes.

[4] https://www.opennetworking.org

- Las decisiones de reenvió de los paquetes están dadas por el flujo, en lugar basarlas en el destino. Todos los paquetes de un flujo reciben políticas de servicio idénticas en los dispositivos de retransmisión. El flujo de abstracción permite unificar el comportamiento de diferentes dispositivos en la red.

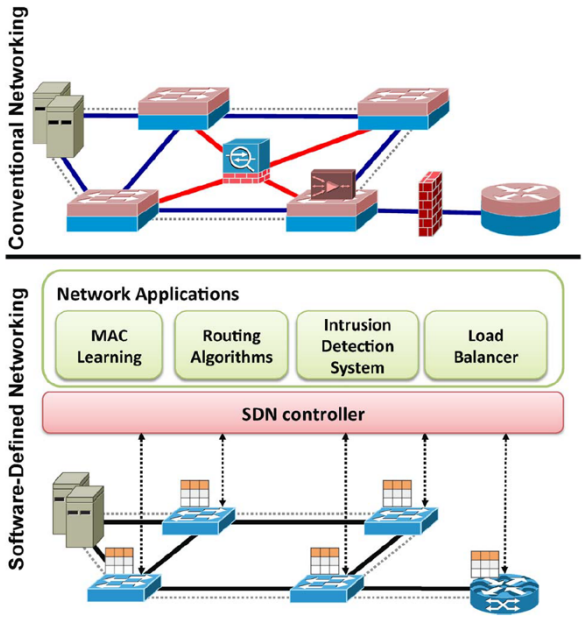
- La lógica de control se vuelve una entidad externa, denominada *Controlador SDN* o *NOS (Network Operating System),* NOS es una plataforma de software que se ejecuta en un servidor, provee los recursos esenciales y abstracciones para facilitar la programación de los dispositivos de reenvío basada en una lógica centralizada, como lo haría un sistema operativo tradicional.

- La red en programable a través de las aplicaciones de software que corren en el controlador SDN e interactúan con los dispositivos del plano de datos. Esta característica de las SDN, es considerada la más valiosa.

Las características anteriores plantean una serie de ventajas, por ejemplo, al tener la lógica de control de la red centralizada, será más simple y menos propensa a errores, al modificar políticas de red a través de lenguajes de alto nivel y componentes de software, en comparación con las configuraciones tradicionales que son especificas a cada dispositivo de bajo nivel.

En segundo lugar, un programa de control puede detectar cambios falsos del estado de la red y así mantener políticas de alto nivel intactas. En tercer lugar, la lógica de control en un controlador con conocimiento global del estado de la red simplifica la visión completa de la red, muy útil para los administradores. Por ejemplo, las políticas definidas podrían compartirse con múltiples dispositivos, posiblemente llevando la red a ser más consistente y eficaz. En la Figura 2.3 se puede observar la forma en la que se da la comunicación en una red tradicional y una red definida por software.

Figura 2.3 Red Tradicional y red definida por software.
Fuente: (Kreutz et al., 2015)



También se observa que existe gran interés por parte de organizaciones para impulsar la implementación de las SDN, ya que algunas organizaciones desarrolladoras de estándares como *OpenDayLigth, OpenStack, OPNFV, OFN*, por mencionar algunas, continúan trabajando en la realización de estándares de facto y por supuesto están presentes organizaciones como IETF, IEEE, IRTF, ITU-T, etc., para garantizar la compatibilidad con los estándares abiertos.

En los centros de datos cuyos escenarios cambian rápidamente, el valor tecnológico que representan las SDN es indispensable para resolver las problemáticas de escalabilidad, seguridad, movilidad, por mencionar algunas.

Los centros de datos tradicionales podrán adoptar gradualmente redes híbridas, combinando SDN y redes tradicionales a fin de aprovechar los dispositivos existentes en la red y mejorar la administración, incluso representará un ahorro de recursos en adquisición de hardware de marca.

2.2.2. Almacenamiento definido por software (SDS).

Como hemos comentado, en los sistemas definidos por software tienen como objetivo ocultar toda la complejidad de la gestión y control de los recursos de un sistema. En este caso nos referiremos a la abstracción de los componentes y dispositivos de almacenamiento. El almacenamiento definido por software (SDS) llega a facilitar y simplificar estos procesos y al mismo tiempo mantiene la calidad en el servicio. (Ala' Darabseh et al., 2015b)

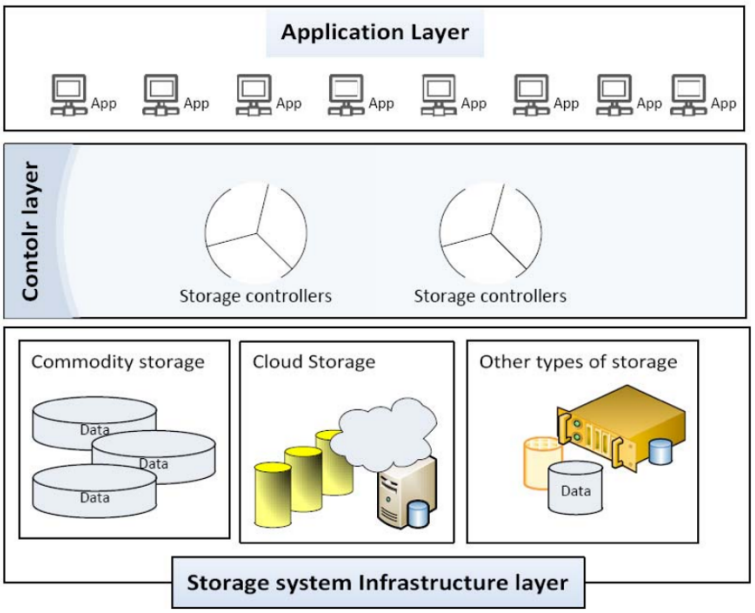
SDS separa el plano de datos y el plano de control. El plano de datos se refiere al aprovechamiento de la heterogeneidad de los dispositivos de almacenamiento, tanto físico como virtuales. Mientras que en el plano de control se definen diferentes políticas para proveer el aprovisionamiento automatizado para responder a una variedad de solicitudes del usuario final a través de las API (DMTF, 2014), (Ala' Darabseh et al., 2015b).

En tanto que los medios de almacenamiento tradicionales se administran de mediante un controlador instalado individualmente, el SDS crea una unidad de control central única para administrar los diferentes elementos del sistema independientemente de cual sea su proveedor, en lugar de instalar un controlador en cada dispositivo. En la Figura 2.4 podemos observar los diferentes componentes de un SDS.(Ala' Darabseh et al., 2015a)

De acuerdo con *Storage Networking Industry Association* (SNIA) (Mark Carlson, Alan Yoder, Don Deel, Carlos Pratt, & Voigt, 2015) los SDS deben cumplir con las siguientes funcionalidades:

Automatización. Administración implícita que reduce el costo de mantenimiento de la infraestructura de almacenamiento, en respuesta a la solicitud de los usuarios en caso de que necesiten configurar el espacio de almacenamiento en el Sistema o verificar si se requiere alguna reconfiguración.

Figura 2.4 Arquitectura de Almacenamiento definido por software. Fuente: (Ala' Darabseh et al., 2015b)



Programabilidad. Interfaces estándar API para la administración, aprovisionamiento y mantenimiento de dispositivos y servicios de almacenamiento. Proporcionar un control visible de los recursos, que integran varios componentes del sistema para permitir la automatización del sistema.

Ruta de datos virtualizada. Interfaces de bloque, archivo y objeto que admiten aplicaciones escritas en estas interfaces.

Escalabilidad. Capacidad para escalar la infraestructura de almacenamiento sin interrumpir la disponibilidad o el rendimiento especificados (por ejemplo, la configuración de QoS y SLA).

Transparencia. La capacidad de los consumidores de almacenamiento para monitorear y administrar su propio consumo de almacenamiento en función de los recursos y costos disponibles.

(Ala' Darabseh et al., 2015a) agrega otras características que distinguen SDS:

Commodity HW. El sistema usa los recursos disponibles *commodity* o de red, para construir la infraestructura, lo que facilita la escalabilidad, resiliencia y performance.

Agrupación de recursos. Se refiere a la abstracción de todos los recursos del sistema en un solo lugar lógico y organizadas en agrupaciones controladas por la unidad de control centralizada. Representa una reducción de la sobrecarga de los administradores para asignar los recursos, ya que se realizan dinámicamente a pedido.

Dirigido por las políticas. Una de las características más importantes en SDS es la capacidad de controlar y manejar todas las políticas en el sistema. El control está separado en dos capas de control: usuario y almacenamiento. Donde la disponibilidad, confiabilidad, latencia y otros problemas especificados por la capa de usuario. Por otro lado, todos los problemas que se requieren para mantener un alto nivel de QoS son manejados por la capa de control de almacenamiento, como la recuperación de fallas, la migración de recursos y otros.

Los SDS son un componente esencial de los CDDS, sin embargo, tienen la capacidad de utilizarse independientemente. (Ala' Darabseh et al., 2015a; Mark Carlson, Alan Yoder et al., 2015). Existen diferentes compañías que ofrecen soluciones de acuerdo a su filosofía en el mercado, por ejemplo VxRail de DELL-EMC o *IBM Spectrum Storage* (Nadkarni, 2018).

2.2.3. Seguridad de la información definida por software. (SDSec).

De acuerdo con (Aguilera, 2010), la seguridad de la información se considera como la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. Un sistema de información se considera seguro si cumple con las propiedades de:

Integridad. Se garantiza la autenticidad de la información en el momento que se solicita y que los datos no han sido alterados ni destruidos sin autorización.

Confidencialidad. Se refiere al hecho de que los datos o la información sea accesible solo para las personas, entidades o mecanismos autorizados, en los tiempos autorizados y por el método autorizado.

Disponibilidad. Los datos deben estar disponibles en el lugar momento y forma en que es solicitado por un usuario autorizado. Este aspecto esta estrechamente relacionado con la fiabilidad técnica de los sistemas de información.

Sin embargo, la aplicación tradicional de la seguridad de la información no es suficiente para los nuevos retos que presenta el surgimiento de la virtualización y los sistemas definidos por software.

En el trabajo realizado por (Ala' Darabseh et al., 2015a) presenta mediante SDSec, una forma de diseñar, implementar y administrar mecanismos de seguridad al separar el plano de reenvío y procesamiento del plano de control de la seguridad. Esta separación proporciona una solución de seguridad escalable, que virtualiza las funciones de seguridad, pero sigue siendo administrable como un solo sistema lógico. Propone una arquitectura basada en tres capas de aplicación:

• **Capa física:** incluye todos los dispositivos de la infraestructura, desde bases de datos, conmutadores, enrutadores o cualquier otro activo. También es conocida como capa de datos, básicamente sigue las políticas creadas por la capa de control.

• **Capa de control** (*middleware*): Esta capa se considera la mente maestra de cualquier sistema definido por software, ya que maneja todas las operaciones de control del núcleo. Las operaciones de control y administración se extraen de los dispositivos existentes en la capa física.

• **Capa de aplicación**: Es la parte donde se implementan todas las aplicaciones que permitirán al usuario tener visibilidad. Se pueden crear varias aplicaciones en la parte superior de la capa de control que ayudarán a los usuarios a interactuar con los dispositivos y datos subyacentes.

Estas capas pueden interactuar por medio de un conjunto de APIs hacia el sur y hacia el norte. Un ejemplo muy conocido de estos, es el protocolo *OpenFlow* para SDN, utilizado por la capa física para comunicarse con la capa de control.

SDSec difiere de la seguridad tradicional al elimina los cuellos de botella que impiden que el sistema se expanda y explote los recursos virtuales, de acuerdo a los siguientes atributos identificados por (Ala' Darabseh et al., 2015a) al analizar una solución existente en el mercado llamada *Catbird*:

Abstracción: SDSec abstrae las políticas de seguridad de la capa de hardware y las ejecuta en una capa de software independiente.

Automatización: La detección de una violación de seguridad se realiza automáticamente cuando ocurre un evento y luego se activan las alertas apropiadas para resolver el problema. Representa un aumento la velocidad del sistema y mejora su eficiencia el hecho de pasar del proceso tradicional de seguridad, generalmente manual, a automático en SDsec.

Elasticidad: Al ser basado en software y no estar restringido al hardware, es fácil ampliarlo y adaptarlo a nuevos cambios.

Control de concurrencia: Los controles de seguridad de SDSec, como la detección de intrusiones, firewall, monitoreo de violaciones, etc., trabajan como un único sistema integral; lo cual representa una mejora de la seguridad y la precisión del sistema.

Visibilidad: Al virtualizar la seguridad, aumenta la capacidad de descubrir los problemas y acciones y actividades anormales.

Portabilidad: Facilita el proceso de implementación incluso si los dispositivos se mueven de una ubicación a otra.

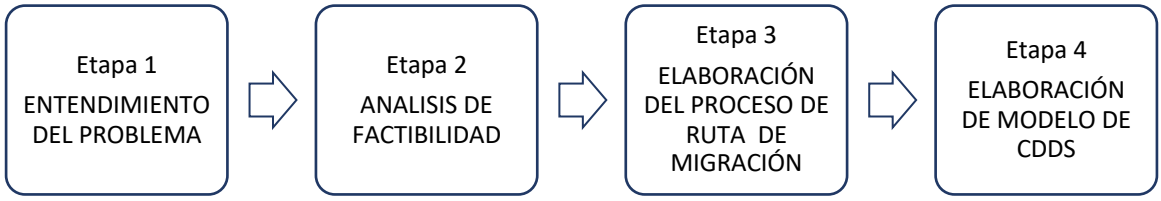
2.3. Conclusión.

En este capítulo se presentaron los conceptos que estaremos utilizando en el desarrollo de este trabajo. Estos conceptos son necesarios para comprender la interrelación y funcionamiento de los distintos componentes de un CDDS. El entendimiento de los mismos también permite apreciar el impacto que representa para una organización su implementación.

3. Metodología.

Para la realización del presente trabajo de investigación se utilizó una metodología con enfoque mixto, de cuatro etapas, las cuales se describen a continuación y se pueden visualizar en la Figura 3.1.

Figura 3.1 Etapas de la metodología de investigación utilizada.



Etapa 1. Entendimiento del Problema. En esta etapa, se lleva a cabo una revisión general del estado del arte de las tecnologías existentes para centros de datos definidos por software. Se abordan los temas de virtualización y componentes de centros de datos definidos por software. Las tendencias en los centros de datos tradicionales en instituciones académicas en México. La revisión se llevó a cabo realizando búsquedas en internet Google Académico, revistas de investigación, memorias de congresos, así como en herramientas para gestión y recopilación de bibliografía (Ej. *Mendeley*[5]).

Además, se hace una revisión de la infraestructura actual del centro de datos del CICESE, mediante consultas a los registros existentes de solicitudes de hospedaje del hardware que se haya alojado en el centro de datos del CICESE. También se consultó al personal del centro para corroborar datos de los equipos alojados y se hizo inspección directa del hardware en sitio, para obtener las características técnicas de los equipos que se encuentran físicamente en el centro de datos.

Para el inventario se registran los siguientes datos de los equipos:

[5] www.mendeley.com

- *Etiqueta del Rack.* Se refiere al identificador del rack que ubica su posición dentro del cuadrante del centro de datos.
- *Etiqueta del equipo*. Se refiere al identificador que ubica la posición del equipo dentro del rack.
- *Nombre registrado en el DNS.*
- *Dirección IP.*
- *Fecha de instalación.* Fecha en la que se alojó el equipo en el centro de datos.
- *Personal responsable del equipo.* Es el nombre de la persona que tiene asignado el equipo y/o el técnico responsable de su mantenimiento.
- *Sistema Operativo.*
- *Estado de la solicitud.* Si esta completa la solicitud de hospedaje, donde se registran el resto de las características del equipo.

La información obtenida del inventario se sintetizó en una tabla agrupando las características anteriores (Tabla 3.1).

Tabla 3.1 Formato para el registro de equipo hospedado en el centro de datos del CICESE.

INVENTARIO DEL CENTRO DE DATOS DEL SITE DE TELEMATICA marzo – mayo 2018								
Etiqueta RACK								
	ETIQUETA EQUIPO	NOMBRE DNS	DIRECCIÓN IP	DIRECCIÓN MACADDRESS	FECHA INSTALACIÓN	RESPONSABLE CONTACTO	SISTEMA	REG/SOL

Las actividades de la Etapa 1 inciden directamente en los objetivos específicos 1 y 2; se obtiene una radiografía cualitativa y cuantitativa de los equipos y sistemas operativos utilizados por los equipos hospedados en el centro de datos del CICESE y se tiene un panorama general de lo que son los centros de datos definidos por software.

Etapa 2. Análisis de factibilidad: Durante esta etapa se realiza una revisión de soluciones tecnológicas para CDDS seleccionadas a partir de un emparejamiento

con los resultados obtenidos en la Etapa 1 en cuanto a infraestructura, tecnologías y sistemas operativos identificados en los equipos alojados en el centro de datos del CICESE.

Además, se presentan elementos comparativos de las soluciones para CDDS seleccionadas, mostrando sus características principales, beneficios, desventajas, inversión económica implicada; estos factores sirven para determinar cual de estas soluciones es técnica, operativa y económicamente posible implementar en el centro de datos del CICESE de acuerdo a los recursos y la compatibilidad de la infraestructura con que cuenta.

Como resultado de la Etapa 2, se elige una de las soluciones para CDDS y se establecen las bases para determinar cuales elementos de hardware y software del centro de datos del CICESE son compatibles con las soluciones para CDDS analizadas. Las actividades realizadas en esta etapa, se relacionan directamente con el objetivo específico 3 del presente trabajo.

Etapa 3. Elaboración del proceso de ruta de migración. Esta etapa se lleva a cabo a partir de los resultados de las Etapas 1 y 2, donde se elabora la propuesta de un procedimiento de ruta de migración a seguir para que los elementos que componen el centro de datos tradicional del CICESE y que cumplen con requerimientos de compatibilidad, puedan ser integrados en un CDDS de forma gradual.

Además, esta etapa utiliza el inventario generado en la Etapa 1, se catalogan los equipos alojados en el centro de datos del CICESE de acuerdo a su compatibilidad con los requerimientos para CDDS, se identifica si existen equipos que son compatibles, cuáles podrían actualizarse para ser compatibles y cuáles no son compatibles debido a su arquitectura o bien, por el uso para los que están destinados, no se integrarían a un CDDS.

Finalmente, en esta Etapa 3 se describe una serie de pasos a seguir para que los equipos compatibles puedan ser migrados a un CDDS, de esta manera se elabora un procedimiento de ruta de migración que satisface el objetivo específico 4.

Etapa 4. Elaboración de modelo de CDDS. A partir de los resultados de la Etapas 2 y 3, se elabora un modelo de CDDS basado en tecnologías de código abierto que demuestre su funcionalidad. Este modelo de CDDS toma en cuenta los resultados del análisis de la factibilidad de la etapa 2 y las características definidas en el plan de migración de la etapa 3. Las actividades de esta etapa inciden directamente con el objetivo específico 5.

3.1. Conclusión.

Con las cuatro etapas de la metodología descritas en este capítulo, se abarcan los objetivos planteados para el presente trabajo terminal.

4. Análisis del estado actual del centro de datos del CICESE.

En este capítulo se describen los resultados pertinentes al análisis del estado actual del centro de datos del CICESE como parte de la etapa 1 del presente trabajo.

Mediante la realización de un inventario de hardware y software se hizo una revisión de la infraestructura que se encuentra alojada actualmente en centro de datos del CICESE, se consultaron los registros existentes de solicitudes de hospedaje del hardware que se encuentra alojado en el centro de datos (Formato de solicitudes de hospedaje del centro de datos del CICESE.).

También se consultó al personal de la Dirección de Telemática del CICESE para corroborar datos de los equipos alojados y se hizo inspección directa del hardware en sitio, para obtener las características técnicas de los equipos.

El compendio total de la información obtenida en el inventario se encuentra bajo resguardo de la institución, debido a que posee información sensible y se requiere autorización para publicarla, no es posible presentarla en el completo detalle. A continuación, se muestra como resultado del inventario, la identificación de las siguientes grandes áreas:

- Infraestructura de soporte.
- Infraestructura de comunicaciones.
- Infraestructura de virtualización.
- Infraestructura de cómputo de alto desempeño.
- Servidores de propósito general.

En la Tabla 4.1 se muestra un resumen del equipo de hardware encontrado catalogado de acuerdo a las áreas identificadas, haciendo un total de 302 equipos físicos. Cabe señalar el fuerte impulso de la virtualización debido a que en 7 infraestructuras se alojan un total de 204 máquinas virtuales, sumando un total de 506 activos.

Tabla 4.1 Resumen de inventario de equipo hospedado en el centro de datos del CICESE.

RESUMEN DE INVENTARIO DE EQUIPO		
Infraestructura	**Unidades**	Unidades virtuales
Cómputo de alto desempeño (9)	218	
Virtualización (7)	14	204
Servidores de propósito general	30	
Comunicaciones	36	
Almacenamiento independiente	4	
Total, equipos físicos	**302**	
Total, activos		**506**

En la Tabla 4.2, se presenta un resumen de los sistemas operativos identificados, para equipos de cómputo y procesamiento, equipos de almacenamiento y equipos de comunicaciones. Se destaca que predomina el uso de sistemas operativos Linux y en cuanto equipos de comunicaciones predominan los IOS de CISCO.

Tabla 4.2 Resumen de inventario de Software utilizado en el centro de datos del CICESE.

RESUMEN DE INVENTARIO DE SOFTWARE	
Sistemas Operativos en Equipos de Procesamiento	Cantidad
Linux	238
Windows	10
Solaris	1
VMware	14
Sistemas Operativos en Equipos de Almacenamiento	Cantidad
Series VNX celerra-clariion (EMC2)	2
HP Storage Utility	1
Lustre	4
Linux NFS	6
Windows Share	4
Sistemas Operativos en Equipos de Comunicaciones	Cantidad
Cisco IOS Internetwork Operating system	23
HP Switch OS	8
Otros	5

4.1. Infraestructura de soporte.

La infraestructura de soporte es requerida en los centros de datos para garantizar las condiciones de energía, temperatura, humedad y seguridad de acuerdo a los estándares provistos para centros de datos para garantizar la continuidad del servicio y la operación óptima de los equipos alojados. (TIA, 2005)

La infraestructura de soporte para el centro de datos del CICESE, incluye los equipos que a continuación se mencionan:

- *2 plantas de energía eléctrica de emergencia.* Estos equipos son los encargados de proveer energía eléctrica suficiente hasta por 12 horas continuas en caso de falla del suministro por parte de Comisión Federal de Electricidad (CFE).

- *4 UPS sistemas de fuerza no interrumpible* (2 de 100KVA y 2 de 50KVA). Estos equipos en conjunto forman un sistema batería que proporciona soporte en caso de interrupciones breves por parte de las plantas de emergencia.

- *2 sistemas de enfriamiento de precisión* (25 Toneladas y 20 Toneladas). Estos sistemas mantienen las condiciones de temperatura y humedad idóneas para el funcionamiento de los equipos alojados en el centro de datos del CICESE.

- *1 sistema de enfriamiento de confort redundante* (20T). Es un sistema alterno que provee solo de condiciones de temperatura y funciona solo en casos de contingencia por falla de los dos sistemas de precisión.

- *1 sistema contra incendios.* Es un sistema especial para ambientes con componentes electrónicos sensibles a polvos y humedad, está basado en agente FM200 que se caracteriza por suprimir el oxigeno en el área y así evitar la combustión sin afectar los electrónicos.

- *1 sistema de control de acceso biométrico.* A fin de proporcionar controles de seguridad se implementó el uso de un sistema computacional que contiene una base de datos de los empleados autorizados para acceder al centro de datos del CICESE, así como los lectores biométricos que validan los privilegios cada vez que se desea acceder al sitio.

- *Sistema de monitoreo.* Sistema de software disponible para administradores encargados de revisar diariamente el estado óptimo de la infraestructura de soporte y condiciones generales del centro de datos del CICESE.

4.2. Infraestructura de comunicaciones.

La infraestructura de redes y comunicaciones es la parte medular que soporta el flujo de información del centro de datos del CICESE. Proporciona conectividad entre todos los nodos y brinda soporte a los servicios de una manera segura y con calidad

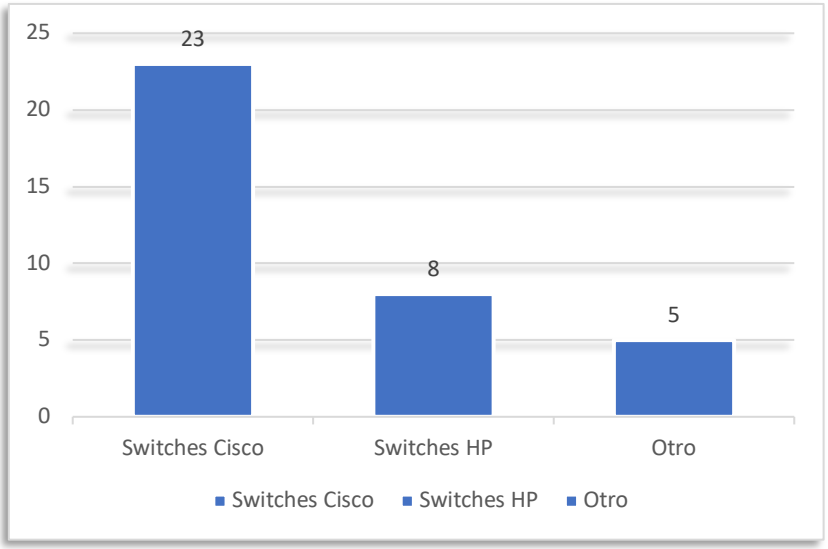
Esta conformada por treinta y seis conmutadores de paquetes (switch) que ofrecen conectividad de alta velocidad de hasta 1Gb/s al usuario y una comunicación entre edificios de hasta 10 Gb/s, el equipamiento utilizado permite manejar calidad de servicio, control de acceso y puede soportar las necesidades de comunicación de las nuevas tecnologías.

La conectividad en el centro de datos del CICESE son dos switch-core los que realizan el enlace hacia la red externa, a estos se conectan otros 7 switch-agregación están destinados a estructurar las subredes internas del centro de datos.

El resto de los equipos de comunicaciones corresponde a los switch-usuario donde están conectados los equipos directamente, están específicamente asignados a la comunicación interna de clústeres de cómputo de alto desempeño, virtualización, redes de almacenamiento y telefonía.

Las marcas que se utilizan son *Cisco, HP, Dell, Intel y Melanox* y en la Figura 4.1 se observan las proporciones identificadas.

Figura 4.1 Marcas de los switches utilizados.



4.3. Infraestructura de virtualización

La infraestructura de virtualización del centro de datos del CICESE proporciona un fuerte soporte para la consolidación de los servicios de tecnologías de la información que requiere la institución, proporcionando confiabilidad al mantener la funcionalidad y la disponibilidad de operación.

En el presente inventario se identificó la existencia de cuatro grandes sistemas de virtualización, son descritos a continuación de acuerdo a su uso principal:

- *Infraestructura de producción:* Servicios críticos que ofrece la Dirección de Telemática hacia la institución como sistemas administrativos, correo electrónico, DNS, portales web institucionales, entre otros.
- *Infraestructura de Zona Desmilitarizada:* (DMZ por sus siglas en inglés *Demilitarized Zone*) Hospeda máquinas virtuales para proyectos que por sus necesidades requieren estar en una zona de la red no restringida.

- *Infraestructura de contingencia:* Es utilizada para realizar respaldos de máquinas virtuales y/o réplicas de máquinas virtuales de los servicios críticos en producción.

- *Otros servidores virtualizados:* Estos servidores están destinados a proyectos específicos y ambientes de desarrollo y pruebas antes de ser integrados a la infraestructura de producción.

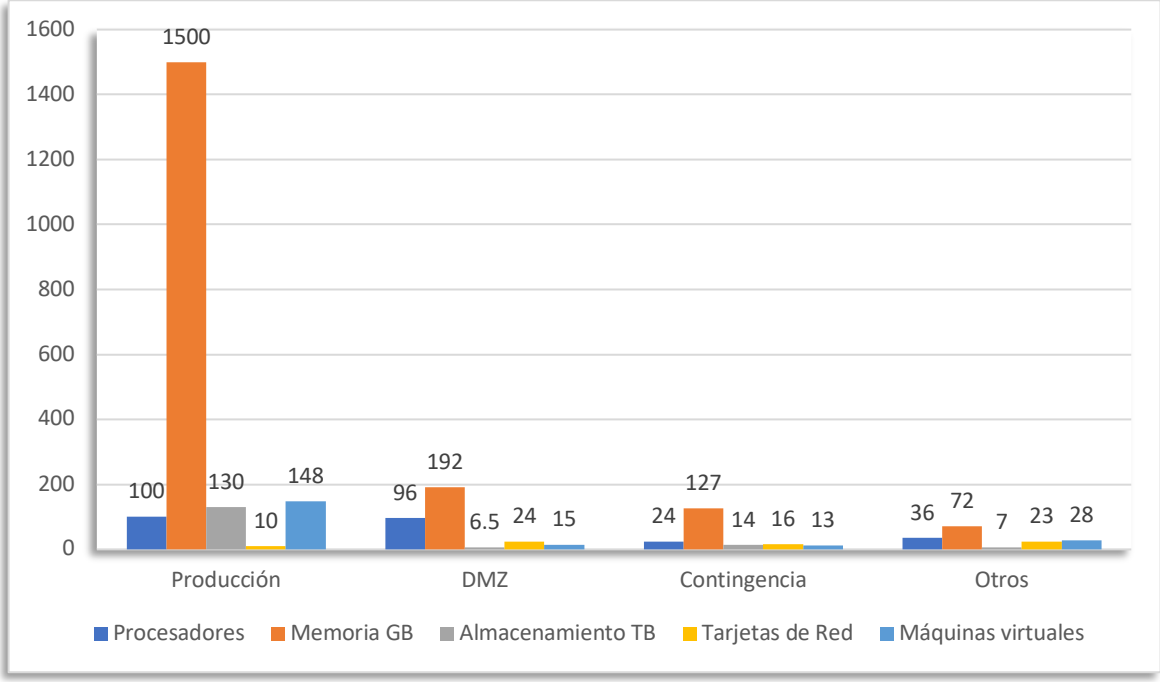
En la Tabla 4.3 se especifican las características de las infraestructuras de virtualización identificadas.

Tabla 4.3 Características de infraestructuras de virtualización.

Infraestructura de Virtualización	**Características**
Infraestructura de producción	Sistema con licenciamiento *VMware* Estándar, Clúster de 5 *blades* o navajas de procesamiento Cisco UCS, 100 CPUs, 1.5TB RAM, 10 interfaces de red. 2 switches Cisco UCS Series Fabric Interconnect, 2 switches Nexus Series 5000 1 sistema de almacenamiento EMC2 con capacidad de 130 TB
Infraestructura DMZ	Sistema con licenciamiento *VMware Essential kit*, Clúster de 3 hosts de procesamiento *HP Proliant*, 96 CPUs,192 GB de RAM, 24 interfaces de red de 1GB. 2 Switches HP 1 sistema de almacenamiento HP P2000 con capacidad de 6TB
Infraestructura de contingencia	Sistema con licenciamiento *VMware Estándar*, Clúster de 2 hosts de procesamiento *HP Proliant*, 24 CPUs, 72GB RAM, 16 tarjetas de red. 1 sistema de almacenamiento EMC2 con capacidad de 7TB. 2 switches Cisco.
Otros servidores virtualizados	licencia gratuita de *VMWare* 4 hosts independientes *HP Proliant,* Server 1: 8 CPU, 16GB RAM, 2TB disco, 8 tarjetas de red. Server 2: 12 CPU, 24GB RAM, 1.7TB disco, 6 tarjetas de red. Server 3: 8 CPU, 16GB RAM, 2TB disco, 4 tarjetas de red. Server 4: 8 CPU, 16GB RAM, 1.25TB disco, 4 tarjetas de red.

En la Figura 4.2 se resumen las capacidades de las infraestructuras de virtualización en cuanto a procesamiento, memoria, almacenamiento, interfaces de red y número de máquinas virtuales alojadas.

Figura 4.2 Infraestructuras de Virtualización



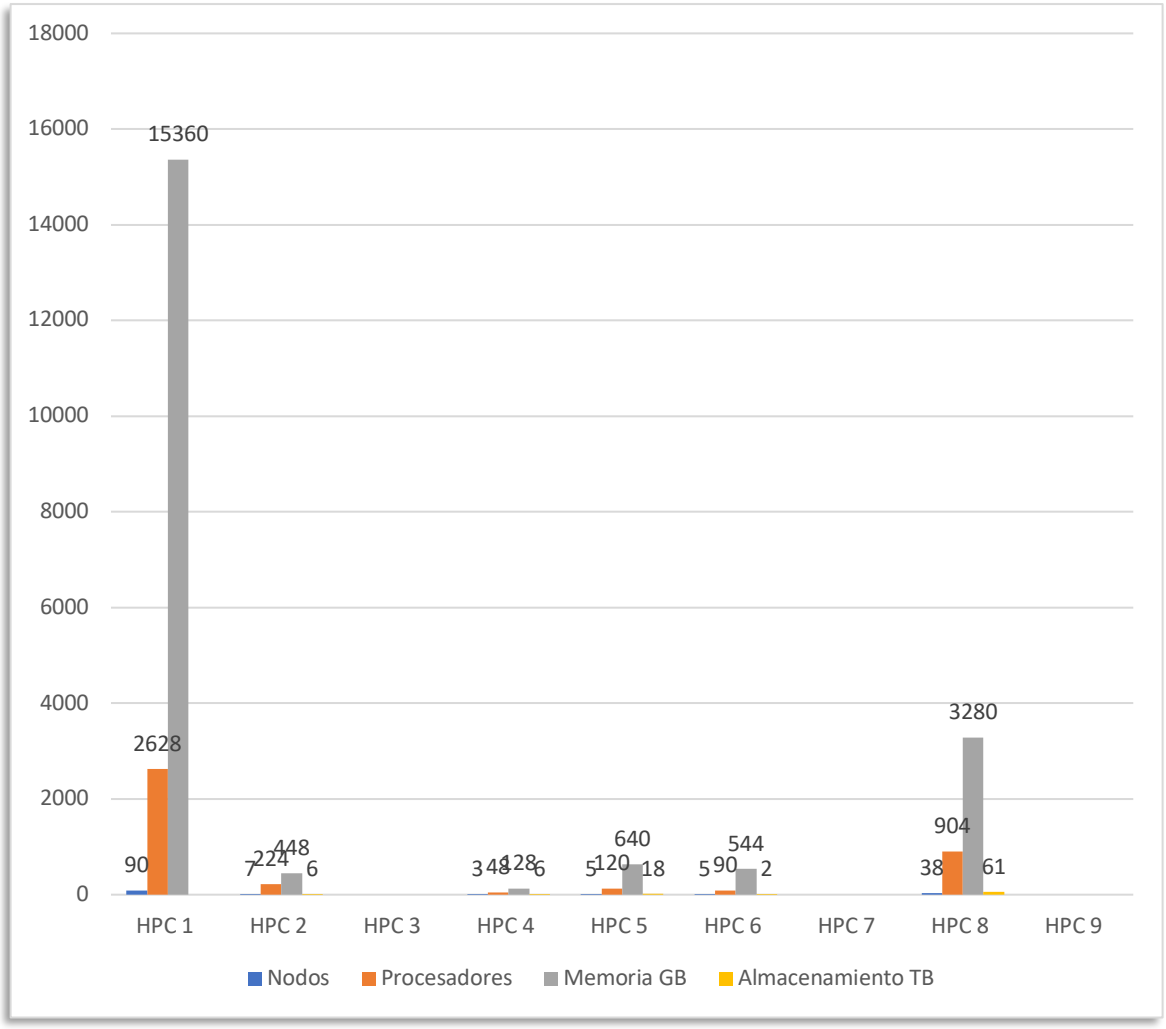
4.4. Infraestructura de cómputo de alto desempeño.

En el inventario realizado se detectó la existencia de nueve clústeres de Cómputo de alto desempeño (HPC por sus siglas en inglés para *High Performance Computing*).

Estos equipos son adquiridos principalmente por grupos de investigación de la institución y asignados específicamente al desarrollo sus proyectos académicos y de investigación; son alojados en el centro de datos del CICESE a solicitud de los investigadores para proveerles las condiciones ambientales y de energía para su óptimo desempeño, así como facilitar el acceso al personal técnico de la Dirección de Telemática que brinda soporte a la administración de los mismos.

En la Figura 4.3 se resumen las características los clústeres de HPC en cuanto a número de nodos, procesadores, memoria y almacenamiento

Figura 4.3 Clústeres de cómputo de alto desempeño.



Estos clústeres de HPC son equipos de diversas marcas como *DELL, HP, Supermicro o PCS Labs* que utilizan sistemas operativos de versiones de Linux *CentOS* o *RedHat*.

4 de estos clústeres configuran su almacenamiento usando el propio sistema Linux y compartiéndolo por *NFS (Por sus siglas en inglés Network File System)* y el resto de los clústeres tiene sistemas de almacenamiento distribuido configurado con Lustre. Para la eficiencia misma que requieren los servicios de HPC en la configuración de los clústeres se utilizan switches que proporcionan comunicación interna de alta velocidad.

4.5. Servidores de propósito general.

Entre los equipos que se encuentran alojados en el centro de datos del CICESE se identificaron 30 servidores de propósito general, cuyo hospedaje fue requerido por el personal que es responsable de los mismos para garantizar su funcionamiento continuo y seguridad de acceso físico.

Estos servidores son utilizados para proyectos académicos, sistemas de video vigilancia, sistemas de telefonía, sistemas de control de acceso al campus, sistemas contables y administrativos, sistemas de almacenamiento para proyectos específicos de investigación, sistemas de almacenamiento para uso de servicios de Telemática, entre otros. Los servidores de propósito general utilizan sistemas operativos Windows, Linux y Solaris.

4.6. Conclusiones.

Con los resultados del inventario de hardware y software expuestos en este capítulo, se obtuvo una radiografía del estado actual del centro de datos del CICESE que permitió identificar la Infraestructura de soporte, de comunicaciones, de virtualización, de Cómputo de alto desempeño y Servidores de propósito general, así como características especificas, datos que serán base para el desarrollo de los capítulos siguientes.

5. Revisión de soluciones para centros de datos definidos por software.

En este capítulo se presentan los resultados que se obtuvieron de la revisión realizada de tecnologías factibles a implementar en el centro de datos del CICESE como parte de la etapa 1 del presente trabajo.

De acuerdo con el estudio de Tecnologías de la Información y Comunicación (TIC) realizado por la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) en México en 2017; 89% de las Instituciones de Educación Superior (IES) cuentan con un espacio físico dedicado totalmente como centro de cómputo, como podemos observar en la Tabla 5.1.

Tabla 5.1 Comparación bianual de porcentaje de IES que cuentan con un centro de datos propio. Fuente (ANUIES, 2017).

	2016	2017	Variación
Sí	91%	89%	-2%
No	5%	5%	0%
Parcialmente	4%	6%	2%
No Contestó	0%	0%	0%

El estudio revela que las IES han conservado en sus instalaciones los centros de datos, como se observa en la Tabla *5.2*, con una ligera disminución probablemente originada por el incremento de participantes en la encuesta en 2017, así como en el incremento en la adopción de servicios de nube. En la Figura siguiente se aprecia un ligero crecimiento respecto al 2016 que demuestra que las IES en México han empezado a utilizar algunos servicios en la nube.

Tabla 5.2 Indicadores de uso de servicios en la nube de IES. Fuente (ANUIES, 2017).

	2016	2017	Variación
Sí	47%	71%	24%
No	35%	28%	-7%
Parcialmente	16%	0%	-16%
No Contestó	2%	1%	-2%

De lo anterior se deduce que en las IES se esta dando la adopción de centros de datos híbridos con el fin de satisfacer las necesidades de servicios requeridos, parte de ellos ofrecidos en sus instalaciones y otros en las nubes públicas.

De hecho, el CICESE como miembro de la ANUIES es considerado en esta estadística debido a que cuenta con una infraestructura local para su centro de datos, sin embargo, algunos de los servicios para estudiantes, como correo electrónico, ya se ofrecen en la nube pública de Google académico.

En este punto, es importante mencionar que para instituciones como el CICESE, en los que se cuenta con una gran cantidad de equipos y un cúmulo de terabytes de datos almacenados alojados en su centro de datos, no es viable realizar una migración de todos sus activos y los servicios implicados a soluciones ofrecidas en las nubes públicas, pues representaría una inversión sumamente costosa en tiempo y recursos financieros.

Las nubes públicas tampoco serian una opción para proyectos específicos con los que CICESE ha firmado acuerdos de confidencialidad de la información que exigen la garantía de que esté almacenada en equipos resguardados en instalaciones del centro.

Por lo tanto, es imprescindible determinar que soluciones tecnológicas para CDDS permitan una implementación en sitio, a la vez que sirvan de base ante la posibilidad de integrar servicios a la nube pública de acuerdo a las necesidades que surjan.

Por ello, a partir del inventario de software realizado en este trabajo, se observa que actualmente se encuentra instalado en los equipos del CICESE licenciamiento de VMWare para virtualización, licenciamiento de Microsoft bajo convenio *Campus Agreement* con centros CONACyT, así como un fuerte impulso por tecnologías de código abierto en sistemas operativos para servicios de TI y supercómputo, por estas razones se eligió analizar las siguientes opciones:

- ***VMware** Cloud Foundation*
- *Microsoft Windows Server Software-Defined Datacenter*
- *OpenStack*

A continuación, describiremos en que consisten estas soluciones y como sus principales características satisfacen las demandas establecidas para CDDS.

5.1. VMware Cloud Foundation.

La compañía VMWare es líder en el desarrollo de la virtualización, desde 2014 ha ofrecido soluciones para CDDS, como VMWare EVO, reemplazado en 2016 por *VMWare Cloud Foundation,* que actualmente es su opción como plataforma unificada del CDDS para nubes públicas y privadas. (VMware Inc, 2015, 2018).

VMWare Cloud Foundation provee una vista convergente de recursos físicos (por ejemplo, CPU, memoria, almacenamiento y red) a una abstracción lógica. Superpone un paquete de software sobre el hardware físico para la administración de operaciones, informes de eventos y auditoría. Esto le permite proporcionar una administración de hardware consistente a través de switches, servidores y almacenamiento, así como una solución de administración consolidada en su CDDS.

5.1.1. Características.

VMware Cloud Foundation se basa en dos componentes (VMware Inc, 2017) esenciales:

- VIA, es '*Virtual Appliance'*, un dispositivo virtual que se utiliza para crear imágenes del primer bastidor, bastidores adicionales y servidores individuales. Durante la creación de imágenes, VIA configura previamente la pila de software SDDC en el bastidor.

- *SDDC Manager*, una aplicación que automatiza todo el ciclo de vida de CDDS (desde el inicio inicial hasta la configuración y el aprovisionamiento, las actualizaciones y los parches), y simplifica la administración y las operaciones diarias. También supervisa los recursos lógicos y físicos de *Cloud Foundation. SDDC Manager* ofrece una interfaz basada en web.

Componentes de *SDDC Manager* (VMware Inc, 2017):

ESXi es un hipervisor utilizado para implementar la virtualización sobre los hosts fisicos. ESXi proporciona virtualización cómputo en el CDDS. Es la base para crear dominios de carga de trabajo. El administrador del CDDS agrupa los hosts en clústeres de *vSphere* administrados por *vCenter Server*. *vSphere HA* proporciona una alta disponibilidad para proteger contra fallas del servidor ESXi.

vCenter Server proporciona la administración de un entorno virtualizado de VMware con uno o más hosts ESXi. *SDDC Manager* requiere un servidor vCenter por dominio de carga de trabajo.

Controladores de servicios de plataforma. Son implementados durante la instalación en el dominio de administración, estos instancian un dominio SSO. Todos

los servidores vCenter (dominio de administración y dominios de carga de trabajo de cómputo) se registran con el dominio SSO.

vSAN proporciona sistemas de almacenamiento para el CDDS. Reúne dispositivos flash y / o discos duros para proporcionar un almacén de datos compartido altamente resistente adecuado para una variedad de dominios de carga de trabajo que incluyen aplicaciones críticas para el negocio, escritorios virtuales, TI remota, recuperación de desastres y la infraestructura de desarrollo de aplicaciones.

NSX es la plataforma de virtualización de red para el SDDC, que ofrece el modelo operativo de una máquina virtual para redes completas. Con *NSX*, las funciones de red que incluyen conmutación, enrutamiento y cortafuegos están integradas en el hipervisor y se distribuyen en todo el entorno.

vRealize Log Insight ofrece una gestión de registros heterogénea y altamente escalable con paneles de control intuitivos y procesables, análisis sofisticados y amplia extensibilidad de terceros, que proporciona una visibilidad operativa profunda y una resolución de problemas más rápida. Los administradores pueden monitorear los registros de los componentes físicos y virtuales a través de una sola interfaz.

VMware Cloud Foundation, cuenta con una serie de características propias de las funcionalidades de las nubes, descritas ampliamente en (VMware Inc, 2016, 2018), de las que mencionaremos solo algunas, como la integración nativa de la pila de software que proporciona un conjunto completo de servicios definidos por software para recursos informáticos, de almacenamiento, de redes, de seguridad y de gestión de la nube.

En conjunto, *VMware Cloud Foundation,* permite la automatización del entorno de TI, al crear una pila de infraestructura completa en forma de modelos (plantillas) que incluyen recursos informáticos, de almacenamiento, de red y de seguridad, además de todas las relaciones que los unen.

Además, ofrece seguridad integral para todas las aplicaciones gracias a la micro segmentación de nivel de red, cortafuegos distribuidos y VPN, el cifrado de nivel de capa informática para máquinas virtuales, hipervisor, y cifrado de nivel de almacenamiento y vMotion para los datos en reposo y los clústeres.

La implementación rápida: al automatiza el proceso de puesta en marcha de toda la plataforma de software, incluida la implementación de las máquinas virtuales de la infraestructura, la creación del clúster de gestión, la configuración de las VLAN, el almacenamiento, la red física y la creación y el aprovisionamiento de clústeres.

La aplicación simplificada de parches y actualizaciones: al realizar un proceso simplificado de actualización/aplicación de parches a la plataforma de software. Los administradores del centro de datos pueden calendarizar el momento y el alcance de las actualizaciones.

El aprovisionamiento basado en políticas: permite automatizar la creación de clústeres mediante políticas para simplificar la asignación de recursos a las cargas de trabajo individuales.

Entre los casos de uso en los que se aplica *VMware Cloud Foundation,* (VMware Inc, 2018) están:

- Proveer infraestructura de nube, al aprovechar el alto rendimiento, la disponibilidad y la escalabilidad del CDDS de *VMware* para ejecutar cualquier aplicación esencial, como bases de datos, aplicaciones web, VDI (*Virtual Desktop Enviroment*), etc.

- Automatización del entorno de TI: al automatizar la infraestructura y la distribución de aplicaciones con funciones de autoservicio.

- Nube híbrida: permite crear una nube híbrida con una infraestructura común y un modelo operativo coherente, que conecta el centro de datos dentro y fuera de las instalaciones, y que es compatible, extendido y distribuido.

Como opciones de implementación, *VMware Cloud Foundation*, puede utilizarse de tres formas(VMware Inc, 2018):

- Implementación del software en conmutadores de red y sistemas de almacenamiento virtualizados que estén certificados. Para lo cual debe asegurarse su compatibilidad con *VMware*.

- Mediante un sistema integrado, es decir el software de *VMware Cloud Foundation* se proporciona de forma preinstalada de fábrica a través de los proveedores certificados: *Dell EMC, Fujitsu, Hitachi Vantara, HPE y QCT.*

- También, *VMware Cloud Foundation*, se puede adquirir como un servicio de la nube pública: *VMware Cloud on AWS* o proveedores distinguidos como *VMware Cloud Provider: IBM Cloud, OVH, Rackspace y CenturyLink.*

Un aspecto importante a considerar es el modelo de licenciamiento de *VMware Cloud Foundation* (VMware Inc, 2016) Los componentes básicos para *SDDC Manager* se adquieren con licencia por CPU y son los siguientes:

- *VMware vSphere*
- *VMware Virtual SAN*
- *VMware NSX for vSphere*

Los componentes de software, que a continuación se listan, son adicionales y tienen licencias individuales:

- *VMware vCenter Server*

- *VMware vRealize Log Insight*
- *VMware vRealize Operations*
- *Content packs for Log Insight*
- *Management packs for vRealize Operations*
- *VMware Horizon 6*.
- *VMware App Volumes*

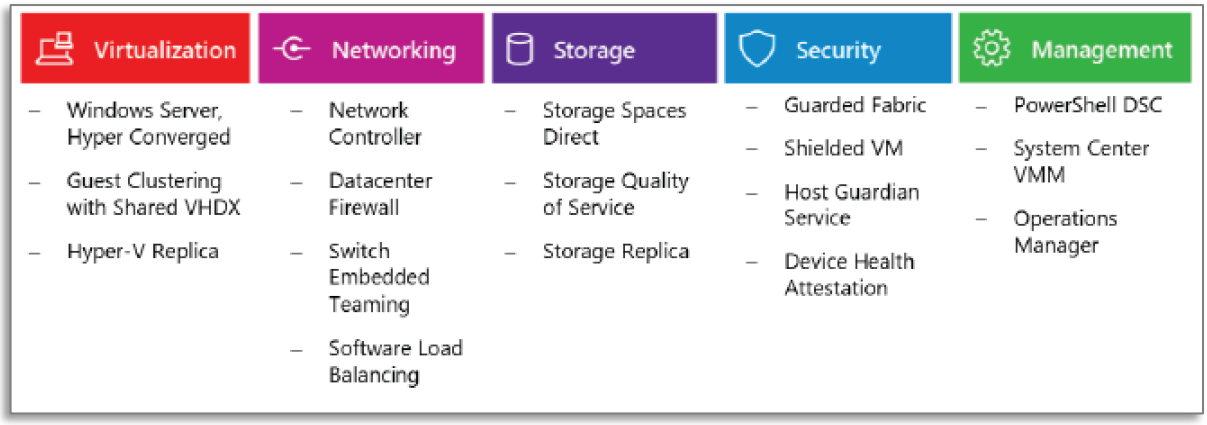
5.2. Microsoft Windows Server Software-Defined-Datacenter.

La implementación de *Windows Server Software-Defined-Datacenter* (WSSD) se refiere al uso de las tecnologías integradas en *Windows Server* y *System Center*. WSSD toma como base la virtualización, mediante el hipervisor *Hyper-V* que proporciona la plataforma de virtualización sobre la que se crean las redes y el almacenamiento. Las tecnologías de seguridad, desarrolladas para los desafíos únicos de la infraestructura virtualizada, mitigan los problemas internos y amenazas externas. Con *PowerShell* integrado en *Windows Server*, y la adición de *System Center* y / o *Operations Management Suite*, puede programar y automatizar el aprovisionamiento, la implementación, la configuración y administración. (Microsoft, 2018)

5.2.1. Características.

De acuerdo con la documentación del portal de Microsoft para Windows Server Software-Defined-Datacenter (Microsoft, 2018) cataloga sus componentes en cinco grandes categorías mostradas en la Figura 5.1. A continuación, describiremos cada uno de ellos:

Figura 5.1 Tecnologías utilizadas en *Windows Server Software-Defined-Datacenter.* (Microsoft, 2018).



- **Virtualización:** Es el hipervisor, *Hyper-V,* es el núcleo de la virtualización informática desarrollado por Microsoft, sin embargo, desde la introducción de Windows Server 2016 se actualizó el conjunto de tecnologías de virtualización como, Hyper-V, Hyper-V Virtual Switch, Hyper-V Replica, y de las máquinas virtuales mismas que mejoran la seguridad, la escalabilidad y la confiabilidad.

- **Red:** El controlador de red ofrece un punto centralizado para la programación, administración, configuración, monitoreo y manejo de errores de la red virtual y física del centro de datos. Se integra la creación de contrafuegos que permiten programar políticas para proteger las redes virtuales del tráfico no deseado de la red interna o desde internet. El controlador de red presenta la opción de crear *Switch Enbedded Teaming* como alternativa para redes definidas por software. Adicionalmente se proporcionan balanceadores de carga para mejorar la eficiencia y disponibilidad de los servicios.

- **Almacenamiento:** *Storage Spaces Direct* ofrece almacenamiento altamente escalable, definido por software y altamente disponible a una fracción del costo de los arreglos SAN o NAS tradicionales. Su arquitectura simplifica radicalmente la adquisición y el despliegue. Incluye funcionalidades de calidad de servicio y replicación del almacenamiento con la capacidad de proteger sincrónicamente

datos en diferentes ubicaciones en caso de contingencia o recuperación de desastres.

- **Seguridad:** Mediante la funcionalidad *Guarded Fabric* provee un entorno más seguro para las máquinas virtuales. Consiste en un servicio de "Guardianes de Host", generalmente, un grupo de tres nodos, más uno o más hosts protegidos y un conjunto de máquinas virtuales blindadas. La máquina virtual blindada estará protegida contra inspección, robo y manipulación. El servicio *Guardian Host* tiene las claves, así como las máquinas virtuales encriptadas.

- **Gestión:** Dependiendo del tipo de estructura que se desee implementar en el centro de datos, la administración de los recursos puede proveerse mediante tres mecanismos:

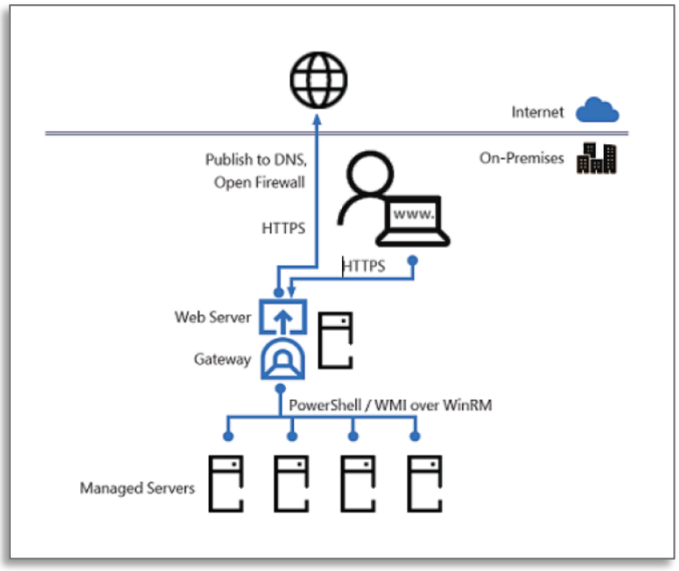
  - PowerShell DSC (por sus siglas en inglés Desired State Configuration): es una plataforma basada en estándares abiertos, lo suficientemente flexible para funcionar de forma confiable y consistente en cada etapa del ciclo de vida de la implementación (desarrollo, prueba, preproducción, producción), así como durante la ampliación. Se puede utilizar en las instalaciones del centro de datos, en un entorno privado o público en la nube.

  - *Virtual Machine Manager* (VMM) se utiliza para configurar, administrar y transformar los centros de datos tradicionales y brindar una experiencia de administración unificada en las instalaciones, el proveedor de servicios y la nube de Azure. VMM está estrechamente relacionado con *Cloud Management*.

  - *Windows Admin Center* es un conjunto de herramientas de administración implementado localmente, como se observa en la Figura 5.2. Es accesible mediante un navegador, que permite la administración local de servidores Windows sin *Azure* o la dependencia de la nube. Provee a los administradores

control total sobre todos los aspectos de la infraestructura de su centro de datos, y es particularmente útil para la administración en redes privadas que no están conectadas a Internet.

Figura 5.2 Funcionamiento de Windows Admin Center en sitio. (Microsoft, 2018)

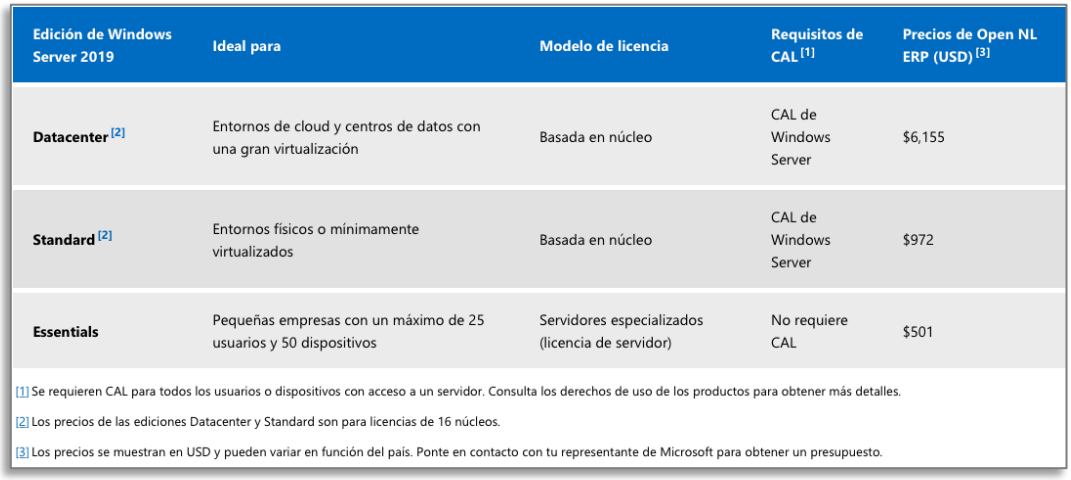


La construcción del CDDS mediante WSSD toma como premisa la selección correcta de la infraestructura de hardware, por eso *Microsoft* se ha asociado con compañías como *DataON, Fujitsu, Lenovo, QCT, SuperMicro, Hewlett Packard Enterprise y Dell EMC*, para crear diseños CDDS validados por Microsoft. Con el objetivo es ofrecer una solución hiperconvergente, al proveer una abstracción del cómputo, el almacenamiento y las redes en servidores y componentes estándar de la industria para mejorar la inteligencia y el control del centro de datos en hardware certificado.

Existen tres modelos de licenciamiento por los cuales se puede adquirir *Windows Server Software-Defined-Datacenter,* mediante *Windows Server*: *Datacenter*, *Standard* o *Essentials*. El modelo de licenciamiento *Datacenter* es la opción más adecuada para centros de datos con una gran virtualización y entornos de nube. Ver Figura 5.3.

De la misma manera que compañías como VMware, los costos de licenciamiento son basados en la cantidad de núcleos de procesamiento con que cuenta la infraestructura de hardware donde se implementará.

Figura 5.3 Modelos de licenciamiento para Windows Server 2019. Fuente Microsoft



Edición de Windows Server 2019	Ideal para	Modelo de licencia	Requisitos de CAL [1]	Precios de Open NL ERP (USD) [3]
Datacenter [2]	Entornos de cloud y centros de datos con una gran virtualización	Basada en núcleo	CAL de Windows Server	$6,155
Standard [2]	Entornos físicos o mínimamente virtualizados	Basada en núcleo	CAL de Windows Server	$972
Essentials	Pequeñas empresas con un máximo de 25 usuarios y 50 dispositivos	Servidores especializados (licencia de servidor)	No requiere CAL	$501

[1] Se requieren CAL para todos los usuarios o dispositivos con acceso a un servidor. Consulta los derechos de uso de los productos para obtener más detalles.

[2] Los precios de las ediciones Datacenter y Standard son para licencias de 16 núcleos.

[3] Los precios se muestran en USD y pueden variar en función del país. Ponte en contacto con tu representante de Microsoft para obtener un presupuesto.

5.3. OpenStack.

OpenStack es una plataforma de código abierto para la creación de nubes privadas, inició como proyecto de la NASA y *Rackspace* en 2010 y fue liberado en 2012 para la fundación que lleva su nombre, actualmente reúne una colaboración global de desarrolladores y tecnólogos de computación en la nube (OpenStack, 2019),(Corradi, Fanelli, & Foschini, 2014)

OpenStack es utilizado para la presentación de infraestructura como servicio (IaaS) que se ejecuta sobre hardware básico, controlando grandes grupos de recursos de computación, almacenamiento y redes de los centros de datos.

Uno de sus valores fundamentales de *OpenStack,* radica en la aceptación de estándares abiertos, así como código abierto, los cuales promueve a través de API's de *OpenStack.*(Pepple, 2011). Mediante las API's de *Openstack* es posible administrar estos grupos de recursos desde una interfaz web centralizada, un cliente

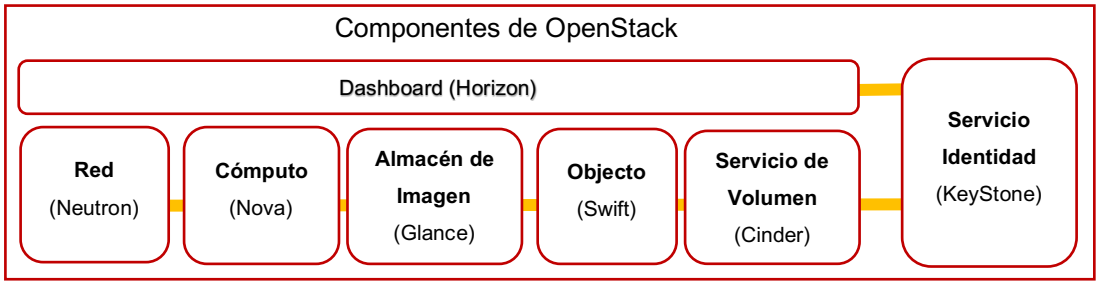
de línea de comandos o kits de desarrollo de software compatibles con la API. *OpenStack* está diseñado para la escalabilidad horizontal, por lo que puede agregar fácilmente nuevos recursos de cómputo, red y almacenamiento para hacer crecer su nube con el tiempo (OpenStack Community Project, 2018).

5.3.1. Características.

OpenStack a su vez está conformado por una gran cantidad de proyectos que se relacionan entre si, cada uno de ellos enfocado a controlar los diferentes componentes del centro de datos; y se gestionan desde una interfaz web. El desarrollo dinámico *OpenStack* tiene como objetivo presentar actualizaciones cada seis meses del desarrollo de sus proyectos.

Inicialmente los proyectos desarrollados fueron dos, el primero para los recursos de computación y red; y el segundo para el almacenamiento distribuido. Sin embargo, actualmente existen 31 proyectos activos (OpenStack, 2019), de los que solo describiremos los esenciales (Litvinski & Gherbi, 2013) para abarcar los componentes básicos del CDDS que se aprecian en la Figura 5.4:

Figura 5.4 Componentes básicos de OpenStack.



OpenStack Nova- Es el componente de *OpenStack* encargado de proveer el cómputo como servicio. Se conforma de seis APIs principales: *nova-api, queue, nova-db, nova-conductor, nova-scheduler y nova-compute,* estos interactúan entre si para facilitar los procesos de virtualización. *Nova-api* es el punto de interacción con el usuario, proporciona soporte para OpenStack Compute API, Amazon API de

EC2. *Queue* provee la comunicación central para todos los componentes de nova, utiliza el estándar de mensajes *RabbitQM. Nova-db* es una base de datos SQL que almacena el estado de las instancias. *Nova-conductor es un módulo que actúa como mediador y facilita la interacción entre nova-compute y la base de datos. Nova-compute* es el responsable de la creación de instancias de máquinas virtuales a través de hipervisor (XenAPI, libvirt, VMwareAPI). (Datt, Goel, & Gupta, 2015)

OpenStack Nova también utiliza middleware para propósitos de aprovisionamiento de máquinas virtuales y administración de recursos. Por medio de API recopila información de la infraestructura del sistema subyacente con fines de monitoreo y análisis de infraestructura. El middleware de código abierto estándar asociado con Nova es *libvirt*, proporciona soporte de API para hipervisores como, KVM y QEMU, y XenAPI que proporciona soporte de API para XenServer y XCP. (Datt et al., 2015)

OpenStack Neutron: Es la parte del proyecto *OpenStack* dedicado al manejo de las redes definidas por software (SDN), presenta la red como un servicio (NaaS), cubre todos los aspectos relacionados con la configuración de la red y comunicaciones. (OpenStack, 2019). *Neutron* funciona mediante la interacción de componentes como *neutrón-api, neutron-plugin, neutron-dhcp, neutron-l3, neutron-lbass y neutrón-metadata.*

A través de estos, provee servicios de red como conmutación o switching, enrutamiento, balanceo de cargas, contrafuegos, redes privadas virtuales (VPN), entre otras. La conmutación la realiza mediante soporte de switches virtuales de capa 2 de múltiples plataformas incluso Linux brigging y OpenvSwitch, estándares como Netflow, SPAN, RSPAN, LACP, y 802.1q; etiquetado VLAN, protocolos GRE o VXLAN. Provee enrutamiento, direccionamiento NAT a través del uso de IP forwarding, iptables. Proporciona balanceadores de cargas (lbass), para distribuir las peticiones de los clientes a través de múltiples instancias de servidores. Incluye mecanismos de seguridad mediante configuración de contrafuegos y tablas de filtrado a nivel de red. Mediante el uso de VPN proporciona el acceso a recursos

disponibles para la red privada a través de redes públicas como Internet. (Denton, 2014)

OpenStack Glance, Swift y Cinder: Son los componentes encargados de proporcionar diferentes tipos de almacenamiento y hacerlo accesibles.

Glance es el encargado de administrar almacenamiento de imágenes. Es el primer recurso que se instala ya que se requiere un espacio donde almacenar las imágenes de los sistemas operativos que pueden ser instalados en las instancias de las máquinas virtuales, pueden ser plantillas predefinidas que se utilizarán repetidas veces, incluso pueden descargarse de repositorios existentes en las nubes públicas.

Cinder administra el almacenamiento tipo block. Volúmenes pueden ser creados y agregados a instancias para después ser particionados, formateados y montados en los sistemas. *Cinder* tiene la capacidad de tomar '*Snapshots*' o instantáneas de los bloques o de las instancias. Por omisión Cinder usa LVM (*Logical Volume Manager*). ClusterFS y Ceph son dos soluciones comúnmente utilizadas. (Radez, 2016)

Swift es el encargado del almacenamiento tipo objeto. Está compuesto de dos elementos un proxy y el motor del almacenamiento. El proxy es un API que interactúa con el usuario y el motor de almacenamiento que hace la distribución y replicación de almacenamiento basada en software. GlusterFS y Ceph también son medios de almacenamiento populares para Swift.

OpenStack Keystone: Es el componente de gestión de identidades. Proporciona mecanismos de identificación y autenticación. Maneja '*tenants'* o proyectos, usuarios, roles y cataloga los servicios y los puntos de acceso de todos los componentes que se están ejecutando en el clúster. Todos los objetos dentro del clúster deben pertenecer a un proyecto, sea un usuario, una red, una instancia, etc. *Keystone* también almacena un catálogo de los servicios y los puntos de acceso de

todo el clúster. Para que un usuario acceda a los recursos del clúster, debe estar registrado en un proyecto y tener un rol definido. (Radez, 2016)

OpenStack Horizon: Es el componente de que proporciona una interfaz web para el usuario final. Esta interfaz no puede realizar ninguna acción que el API no pueda. Todas las acciones que efectuadas a través de *Horizon* son el resultado de llamadas hechas al API para completar las peticiones realizadas por el usuario. (OpenStack, 2019), (Radez, 2016).

OpenStack, puede implementarse de al menos tres formas distintas:

- Una solución hiperconvergente, es probablemente la opción más simplificada, se adquiere un dispositivo todo-en-uno, con un proveedor certificado, el dispositivo se desempaqueta, se conecta a la alimentación eléctrica adecuada y a su red local; con una configuración mínima adicional logra tener una nube privada de OpenStack.

- Otra alternativa, es adquirir una solución de software con soporte empresarial de OpenStack, como *Canonical* (con OpenStack desde 2011), *RedHat y SUSE*; estas pueden ejecutarse en servidores, almacenamiento y productos de red que la organización ha seleccionado debido a necesidades de hardware especificas para las aplicaciones que utiliza. Otras distribuciones especializadas, como las de *Rackspace, Piston, SwiftStack o Cloudscaling* también pueden ser de interés en estos casos.

  Incluso es posible contactar integradores de sistemas con la experiencia OpenStack, como *Mirantis* o *Metacloud* para apoyo en las decisiones sobre el hardware subyacente o sus aplicaciones, o a la integración de componentes adicionales según surjan nuevas necesidades en la organización.

- Otra opción es realizar la implementación con los recursos humanos y de hardware existentes en la organización, para lo cual la *OpenStack Foundation* tiene un mercado de capacitación donde puede buscar eventos cercanos y/o acceder a los materiales de capacitación de código abierto que tiene disponibles.

5.4. Conclusiones.

En este capítulo se ha revisado el estado del arte de soluciones tecnológicas de vanguardia para CDDS como *VMWare Cloud Foundation,* Microsoft *Windows Server Software-Defined Datacenter y* OpenStack*,* sus características más destacadas, así como modelos de implementación que proponen cada una de ellas. La información recabada será de utilidad en el próximo capítulo para determinar si estas soluciones son factibles a implementar en el centro de datos del CICESE.

6. Análisis de Factibilidad.

En este capítulo se describen los resultados del análisis de factibilidad de transformar un centro de datos tradicional a uno definido por software, tomando como caso de estudio al centro de datos del CICESE. Este análisis es realizado como parte de la etapa 2 del presente trabajo.

De acuerdo con (Burneo Valarezo, Delgado Víctore, & Vérez, 2016), los directivos y encargados de la gestión de proyectos de tecnologías de la información requieren contar con mecanismos que les permitan evaluar de forma efectiva si un proyecto es viable y en base a indicadores resultantes establecer prioridades de los proyectos demandantes en función de la disponibilidad real de recursos, ya sean financieros o tecnológicos El análisis de factibilidad es la base para la toma de decisiones de los directivos que tienen la responsabilidad de aprobar las inversiones y cumplir con indicadores, que, en el caso del centro de datos, implican el cumplimiento de acuerdos de servicio (*Service Level Agreement* SLA por sus siglas en inglés).

Dentro de las fases de un proyecto, es posible incluir el análisis de factibilidad como un trabajo de rutina previo al proyecto, o bien ser la primera fase de un proyecto, incluso podría tratarse como un proyecto independiente y separado. Mucho depende de la naturaleza del proyecto específico y del estilo del equipo u organización del proyecto.(PMI, 2008).

De acuerdo con (Dubs de Moya, 2006), el análisis de factibilidad se desarrolla mediante la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, satisfacer requerimientos o necesidades de organizaciones.

En el presente trabajo, el análisis de factibilidad se enfocó principalmente a revisar los aspectos técnicos, económicos y operacionales implicados para seleccionar una

solución que puede ser implementada como opción para CDDS en las instalaciones del centro de datos del CICESE.

6.1. Factibilidad Técnica.

En la Capítulo 5 se realizó una revisión de las tecnologías para CDDS que pudieran ser implementadas en el centro de datos del CICESE: *VMware Cloud Foundation, Microsoft Windows Server Software Defined Datacenter* y *OpenStack,* cada una de ellas satisface los requerimientos técnicos esenciales para un CDDS. En la Tabla 6.1 se resumen los componentes equivalentes en cada solución correspondientes al cómputo, almacenamiento, red y seguridad, definidos por software, así como gestión centralizada de los recursos y compatibilidad con las nubes públicas.

Tabla 6.1 Comparación de Soluciones para CDDS.

	VMware Cloud Foundation	**Microsoft Windows Server Software Defined Datacenter**	**OpenStack**
Cómputo	*VMware vSphere ESXi*	Windows Server Hyper Converged, Hyper-V	OpenStack Nova
Almacenamiento	*VMware Virtual SAN*	Storage Spaces Direct, Storage Replica, Storage Quality of Service	OpenStack Glance, Swift, Cinder
Red y Seguridad	*VMware NSX for vSphere*	Network Controller Firewall	OpenStack Identity OpenStack Neutron
Gestión Centralizada	*VMware vRealize, vCenter, SDDC Manager*	Power Shell DSC System Center Operations Manager	OpenStack Horizon

De acuerdo a los hallazgos en el estado actual del centro de datos del CICESE, registrado en el Capítulo 4.3 donde se detallan los componentes de las

infraestructuras de virtualización con que se cuentan, se detecta que los elementos de hardware deben ser actualizados o reemplazados para que puedan ser integrados a dos de las soluciones para CDDS aquí analizadas, tanto *VMware Cloud Foundation como Microsoft Windows Server Software Defined Datacenter*, su implementación implica la adquisición de nueva infraestructura.

Respecto al software de virtualización que actualmente utilizado, se detectó que las versiones de VMware ocupan ser actualizados para ser compatibles con *VMware Cloud Foundation*.

Si se opta por utilizar la solución de CDDS de Microsoft deben adquirirse como compra inicial pues el convenio de los centros CONACyT no incluye a *Microsoft Windows Server Software Defined Datacenter*. Como se puede apreciar, en ambos casos se requiere una fuerte inversión en el licenciamiento y soporte correspondiente.

Por otra parte, *OpenStack*, al ser una opción de código abierto, es flexible y permite la implementación en una gama más amplia de hardware[6], lo cual hace posible su instalación en infraestructura de hardware selecta que existe en el inventario del centro de datos del CICESE, esta se especificará en el capítulo 7.

A su vez, se encontró que *OpenStack* es compatible con el software utilizado para virtualización en el Centro como *VMware,* sin embargo, algunos de los componentes que se requieren para realizar el enlace, como *VMware NSX* para Redes definidas por software, no está disponible para licencias fuera de soporte como es el caso de las que actualmente cuenta la institución. Cabe señalar que existen soluciones que realizan la integración entre *OpenStack* y *VMware*, como *VIO (VMware Integrated OpenStack)* (VMware Inc, 2019)

[6] https://docs.openstack.org/arch-design/design-compute/design-compute-hardware.html

Como hemos mencionado anteriormente, el proyecto *OpenStack* es respaldado por una comunidad mundial de compañías y desarrolladores, lo cual hace posible disponer de un soporte para la implementación y resolución de problemáticas, así como la actualización del software mismo de forma dinámica y gratuita.

Sin embargo, se debe considerar que al implementar soluciones de código abierto como *OpenStack* existen riesgos como posibles incompatibilidades de controladores que requieran actualización, los tiempos de aprendizaje y capacitación por parte del personal técnico, los tiempos de implementación y de seguimiento de un procedimiento de ruta de integración de infraestructuras que se hayan en producción, que puede impactar en la calidad del servicio que se ofrece a los usuarios.

6.2. Factibilidad Económica.

El análisis de factibilidad económica es crucial para la toma de decisiones por parte de los directivos encargados del manejo de proyectos, en las instituciones como el CICESE, donde la asignación presupuestal proviene del Gobierno Federal, es crucial sustentar el mayor éxito posible de los proyectos a fin de que se asignen los recursos financieros necesarios.

Debe considerarse además que el Gobierno Federal, en particular la administración presente, está impulsando la reducción del gasto público e impulsando fuertemente el uso de tecnologías de código abierto que promuevan ahorros sustanciales a la economía del país.

Por esta razón, en el presente se ha visto disminuida la posibilidad de que el Centro adquiera infraestructura de hardware y renovación o adquisición de licenciamientos de software. Debido a ello, para el presente trabajo, no fue posible obtener cotizaciones reales de las tecnologías para CDDS analizados: *VMware Cloud Foundation, Microsoft Windows Server Software Defined Datacenter.*

Sin embargo, en la Tabla 6.2 se muestran los beneficios de cada una de las soluciones para CDDS analizadas y se señalan los costos implicados que deberán solicitarse a los proveedores si se desea adquirir en el futuro alguna de estas soluciones.

Tabla 6.2 Relación costo-beneficio de soluciones analizadas para CDDS.

	Beneficios	Costos
VMware Cloud Foundation	• Instalación rápida • Administración en sitio • Soporte para atención a incidentes y actualizaciones • Extensamente soportado por proveedores certificados. • Compatibilidad con nube pública	• Costo por Adquisición de nuevo hardware • Costo de Licenciamiento de aplicaciones individuales y por núcleo de procesamiento. • Costos de Soporte
Microsoft Windows Server Software Defined Datacenter	• Instalación rápida • Administración en sitio • Soporte para atención a incidentes y actualizaciones • Compatibilidad con nube pública	• Costo por Adquisición de nuevo hardware • Costo de Licenciamiento de aplicaciones individuales y por núcleo de procesamiento. • Costos de Soporte
OpenStack	• Código abierto • Conjunto de APIs estandarizados y bien aceptadas • Soporte de la comunidad • Interoperabilidad con múltiples componentes • Re-utilización de infraestructura • Compatibilidad con nube pública	• Software de uso gratuito. • Costos de Soporte (opcional)

6.3. Factibilidad Operacional.

El análisis de factibilidad operacional nos permite explicar como la implementación de un CDDS puede impactar la operación del centro de datos del CICESE y los beneficios que puede representar desde el nivel de usuario hasta nivel de organización.

Haciendo referencia a los objetivos estratégicos de la Dirección de Telemática, publicados en su página oficial[7], se destaca que es la entidad responsable de gestionar los recursos de las Tecnologías de la Información y Comunicaciones en beneficio de las actividades sustantivas y administrativas del Centro. Y a lo largo de los años, se ha caracterizado por el impulso a la implementación de tecnologías de código abierto, ha destinado recursos para explorar opciones de implementación de CDDS basado en tecnologías de código abierto.

Al proponer, en el presente trabajo el uso de *OpenStack* como opción para CDDS, se proveen soluciones que representan ahorros de recursos para la organización, como resultado del soporte y compatibilidad de *OpenStack* con múltiples compañías y desarrolladores, se logra gran flexibilidad para utilizar hardware básico, de tal manera que el centro de datos del CICESE, podría liberarse gradualmente de la dependencia a marcas, software propietario y pago de licenciamientos.

También, con la implementación de *OpenStack* se logra una gestión unificada de los recursos existentes en el centro de datos, lo cual representa una mejora a los procesos de administración de la infraestructura de cómputo, red y almacenamiento sin tener que recurrir a la configuración manual de cada uno de los dispositivos; así como, proveer un punto central para el establecimiento de medidas de seguridad, detección de incidentes o fallas en los componentes.

[7] https://telematica.cicese.mx

Además, considerando que una de las características de los CDDS es el aprovisionamiento automatizado de los recursos, el hacer disponible el acceso a recursos de red, cómputo y almacenamiento de acuerdo a la demanda de las aplicaciones, esto representa una mejora de los niveles de servicio perceptibles para el usuario final del centro de datos.

6.4. Conclusiones.

Del análisis de factibilidad realizado en el presente capítulo, se llegó a la conclusión de que cualquiera de las soluciones revisadas en este trabajo para CDDS, *VMWare Cloud Foundation,* Microsoft *Windows Server Software-Defined Datacenter y* OpenStack*,* poseen ventajas y desventajas que deben considerarse para su implementación en la infraestructura del centro de datos del CICESE.

Sin embargo, la opción de código abierto *OpenStack* destaca porque permitirá integrar gradualmente un mayor número de elementos de hardware existente en un modelo de CDDS sin necesidad de realizar fuertes inversiones económicas. Aunque es necesario señalar que para lograr la integración de VMware con OpenStack se requiere invertir en soporte para poder actualizar el software existente.

7. Procedimiento de ruta de migración.

En este capítulo se propone un procedimiento de ruta de migración a seguir para que los componentes de hardware y software del centro de datos del CICESE puedan integrarse gradualmente a un CDDS, estos resultados forman parte de la etapa 3 del presente trabajo.

Como se describió en el Capítulo 5 las compañías encargadas del diseño CDDS, generalmente ofrecen a las organizaciones sus soluciones integrales como parte de un portafolio de servicios en los que incluyen sus productos de hardware, software de licenciamiento, soporte para la implementación y mantenimiento.

Estas soluciones pueden presentarse de forma preinstalada de fábrica a través de los proveedores certificados en soluciones hiperconvengentes o realizar la implementación de la solución en sistemas virtualizados existentes que cuenten con certificación. Si bien estas opciones son relativamente simples de instaurar, como se analizó en la sección 6.2, se requiere de una fuerte inversión inicial, así como planeación de los costos de prolongación de servicios de soporte y actualización de licenciamiento.

En el Capítulo 0 se expuso como variante a considerar OpenStack, opción de código abierto que permiten mayor flexibilidad en la integración de diferentes tipos de hardware y software de virtualización, aunque si requiere una inversión en capacitación y tiempos de implementación, a mediano plazo puede representar la liberación de las organizaciones de dependencia a marcas y licencias costosas.

7.1. Descripción de fases.

A continuación, se explican las fases que se han identificado en el presente trabajo son necesarias llevar a cabo en implementaciones basadas en soluciones de código abierto como *OpenStack* y que pueden ser adoptadas por las organizaciones como

el CICESE, utilizando recursos propios de hardware y aprovechar el personal de TI calificado con el que cuenta.

Fase 1: En esta fase se realiza una selección de recursos existentes en el inventario de hardware cuyos recursos de cómputo, red y almacenamiento están disponibles para integrarse a un CDDS

Fase 2: En esta segunda fase, los elementos seleccionados en la Fase 1, se realiza una verificación de compatibilidad de acuerdo a los requerimientos de hardware y software que soporta la solución de código abierto para CDDS. Si se determina que son compatibles, continuamos en la Fase 4, en caso contrario se procede con la Fase 3.

Fase 3: Esta tercera fase se aplica a los elementos que en la Fase 2 se identificó que requieren actualizar sistema operativo, librerías y/o controladores para hacerlos compatibles con la solución de código abierto para CDDS. Es importante considerar posibles ventanas de mantenimiento, periodos de tiempo en los que estos equipos estarán fuera de servicio.

Fase 4: La fase 4 se enfocará a realizar la configuración de los elementos compatibles en base a mejores prácticas para la solución de código abierto para CDDS, a fin de lograr disponibilidad de los recursos de cómputo, red y almacenamiento. Requiere programar ventana de mantenimiento.

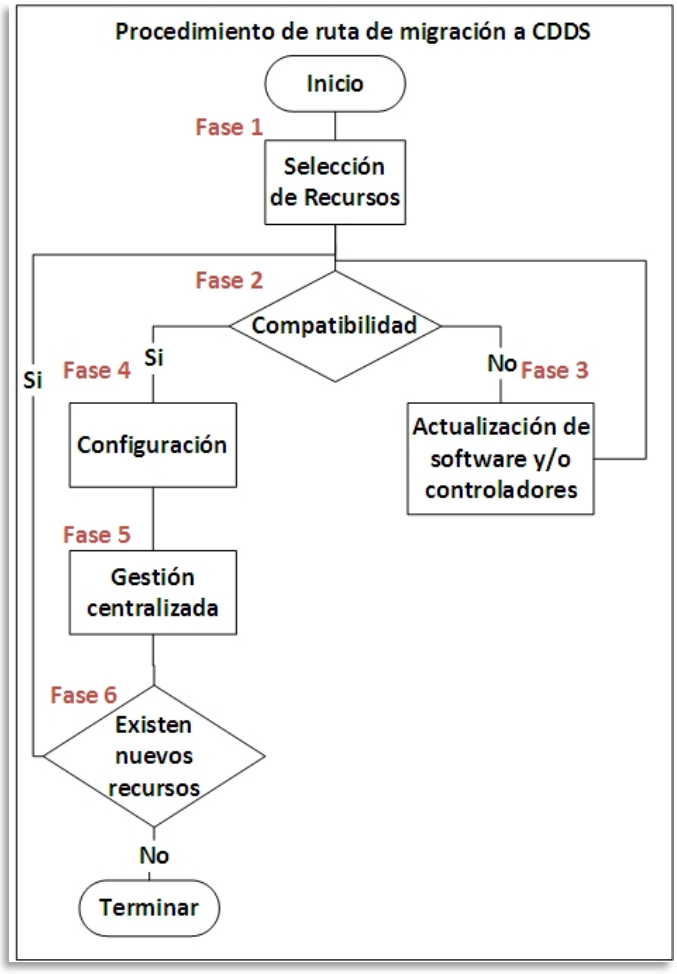
Fase 5: En esta quinta fase, se establece el enlace de los elementos configurados en la fase 4 con la interfaz de gestión unificada de la solución de código abierto para CDDS. Representa una reducción

de los tiempos de respuesta administrativa de los recursos y se fortalecen las medidas la seguridad de la información.

Fase 6: La sexta fase permite agregar nuevos grupos de recursos al CDDS, los cuales contribuirán a ofrecer características de alta disponibilidad y cumplir con los requisitos de rendimiento para sistemas en producción. Estos nuevos grupos de recursos se agregan a la Fase 1 para reiniciar el proceso de integración al CDDS.

En la Figura 7.1 se representan las fases del procedimiento de ruta de migración en un diagrama de flujo.

Figura 7.1 Diagrama de flujo para fases del procedimiento de ruta de migración.



Es importante mencionar que, para iniciar el proceso de la ruta de migración a un CDDS, la Fase 1 requiere utilizar los resultados del inventario mostrados en el Capítulo 4 para determinar cuáles elementos se podrían integrar.

En el inventario del centro de datos del CICESE, se identificó la existencia de infraestructuras como los clústeres de HPC, los servidores de propósito general y sistemas de almacenamiento que están dedicados a propósitos específicos, proyectos académicos y de investigación, de hecho, el 95% de ellos no han sido virtualizados lo cual es un requisito esencial para integrarse a un modelo de CDDS, por tales razones estos componentes no se considerarían en primera instancia como candidatos a integrarse a un CDDS.

Por otra parte, las infraestructuras de virtualización, serían el primer activo a considerar evaluar, si de acuerdo con sus características de hardware y software es posible integrarlas a un modelo de CDDS basado en *OpenStack.*

7.2. Clasificación de equipos.

Para facilitar la selección de componentes de la Fase 1 del procedimiento de ruta de migración, proponemos catalogar los elementos existentes de acuerdo a su nivel de compatibilidad con una solución para CDDS de código abierto como *OpenStack* en las siguientes clases:

Clase 1: Elementos que son compatibles con *OpenStack* y se pueden integrar en un CDDS.

Clase 2: Elementos que es necesario actualizar alguno de sus componentes o controladores para asegurar su compatibilidad con *OpenStack* y puedan ser integrados en un CDDS.

Clase 3: Elementos que no son compatibles con *OpenStack*, no es posible su integración. En esta categoría caben infraestructuras que por su estructura o propósito no se planea incluir en un CDDS.

En la Tabla 7.1 se muestran las infraestructuras identificadas en el inventario del centro de datos del CICESE de acuerdo a su compatibilidad con CDDS basado en *OpenStack.*

Tabla 7.1 Infraestructuras catalogadas de acuerdo a su compatibilidad con OpenStack.

INFRAESTRUCTURA	CLASE 1	CLASE 2	CLASE 3
Virtualización – Producción[8]		✓	
Requiere actualización de controladores de Red de *VMware* NSX, implica adquisición de soporte de licencia.			
Virtualización - DMZ		✓	
Requiere actualización de controladores de Red de *VMware* NSX implica adquisición de soporte de licencia.			
Virtualización - Contingencia		✓	
Requiere actualización de controladores de Red de *VMware* NSX implica adquisición de soporte de licencia.			
Virtualización – Otros		✓	
Requiere actualización de hipervisor, se propone KVM compatible con *OpenStack*			
Comunicaciones - Cisco		✓	
Requiere actualización de controladores de Red			
Comunicaciones - HP Switch OS		✓	
Comunicaciones - Otros			✓
Almacenamiento - Linux NFS		✓	
Almacenamiento - Windows Share Asignado a proyectos académicos			✓

[8] Ver detalles en Tabla 4.3 Características de infraestructuras de virtualización.

7.3. Conclusiones.

En el desarrollo de este capítulo se explicaron 6 fases identificadas en el presente trabajo como esenciales para la migración de un centro de datos tradicional a una implementación de CDDS basada en soluciones de código abierto como *OpenStack.*

Adicionalmente, proponemos una clasificación de los elementos existentes de en el inventario del centro de datos del CICESE, de acuerdo a su nivel de compatibilidad con una solución para CDDS de código abierto como *OpenStack*.

Las fases y clasificaciones expuestas, pueden servir de guía a otras IES, que deseen utilizar los recursos propios de hardware y aprovechar la experiencia del personal de TI calificado con el que cuenta en centros de datos tradicionales.

Los resultados obtenidos en este capítulo serán de utilidad para el desarrollo del modelo de CDDS basado en OpenStack planteado a continuación.

8. Modelo para CDDS basado en tecnologías de código abierto.

En este capítulo se presenta la propuesta de un modelo para CDDS basado en la tecnología de código abierto *OpenStack*, estos resultados forman parte de la etapa 4 del presente trabajo.

De acuerdo con el capítulo 5 donde se revisaron tres diferentes soluciones para CDDS que pudieran ser implementadas en las instalaciones del CICESE y considerando los resultados del Análisis de la Factibilidad presentado en el capítulo 0, se llegó a la conclusión que *OpenStack* es una opción viable a instalar a un bajo costo y utilizando elementos existentes en el inventario del Centro.

Además, se explicó que en el caso de integración de las infraestructuras de VMware a un CDDS basado en OpenStack es necesario adquirir soporte mínimo para realizar las actualizaciones pertinentes de versiones.

El modelo de CDDS basado en *OpenStack*, representará en pequeña escala la gestión de los componentes definidos por software de cómputo, red, seguridad y almacenamiento. Este modelo puede servir de punto de referencia para la realización de una implementación real que sea utilizada para servicios en producción.

En la Figura 8.1 se muestra el modelo de CDDS propuesto, donde se pueden apreciar los componentes básicos de *OpenStack* descritos en la sección 5.3, Se distinguen principalmente los siguientes elementos:

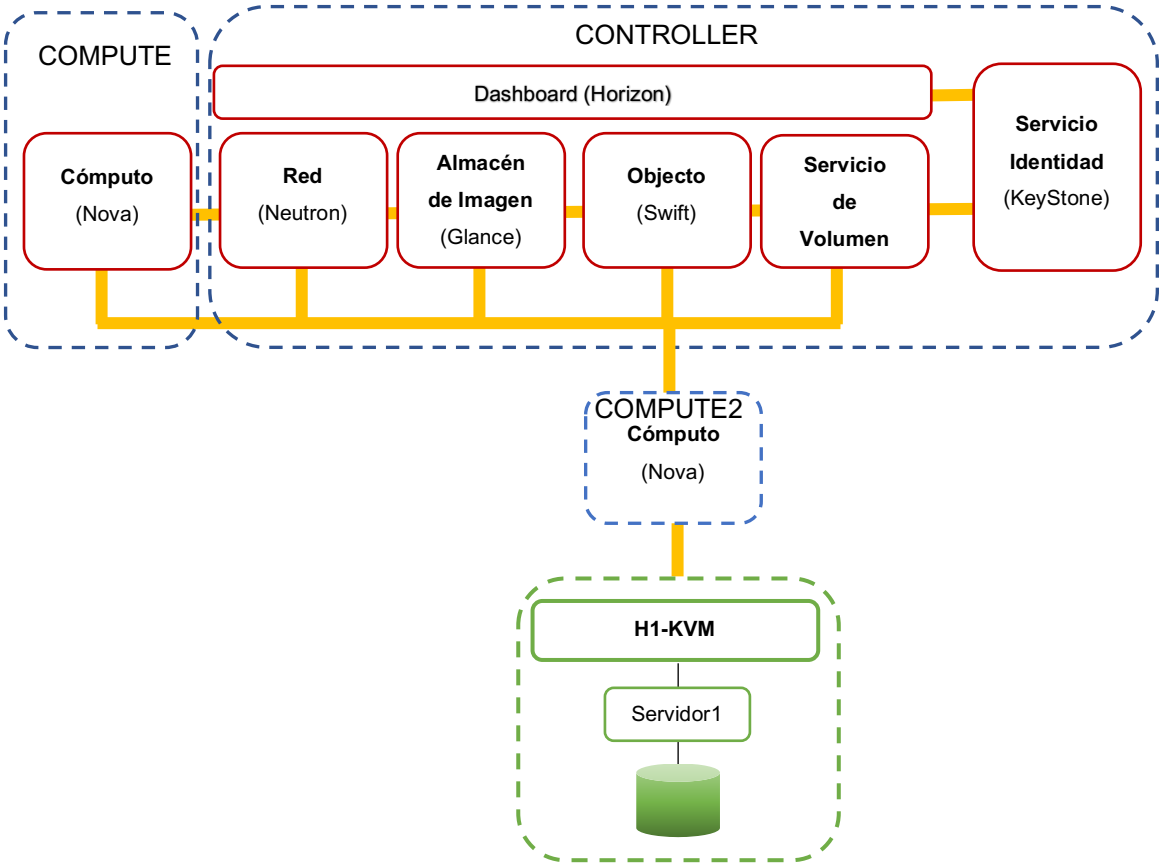
CONTROLLER, Es el entorno que reúne los componentes de OpenStack encargados de la administración y configuración de la Red definida por software (Neutron), diferentes tipos de almacenamiento definidos por software (Cinder, Glance, Swift), Servicios de identificación y políticas de seguridad (Keystone) así como el Centro de gestión unificada (Horizon).

COMPUTE, Es el ambiente que contiene el componente de OpenStack encargado de la administración global del procesamiento definido por software (Nova).

COMPUTE2, Es el ambiente que contiene el componente de OpenStack encargado de la administración y configuración del procesamiento definido por software (Nova) y facilitará el enlace de un hipervisor independiente.

H1-KVM, Es el componente que servirá para ejemplificar la integración de un equipo independiente virtualizado, en este caso por motivos de compatibilidad se eligió KVM que es el estándar manejado por OpenStack.

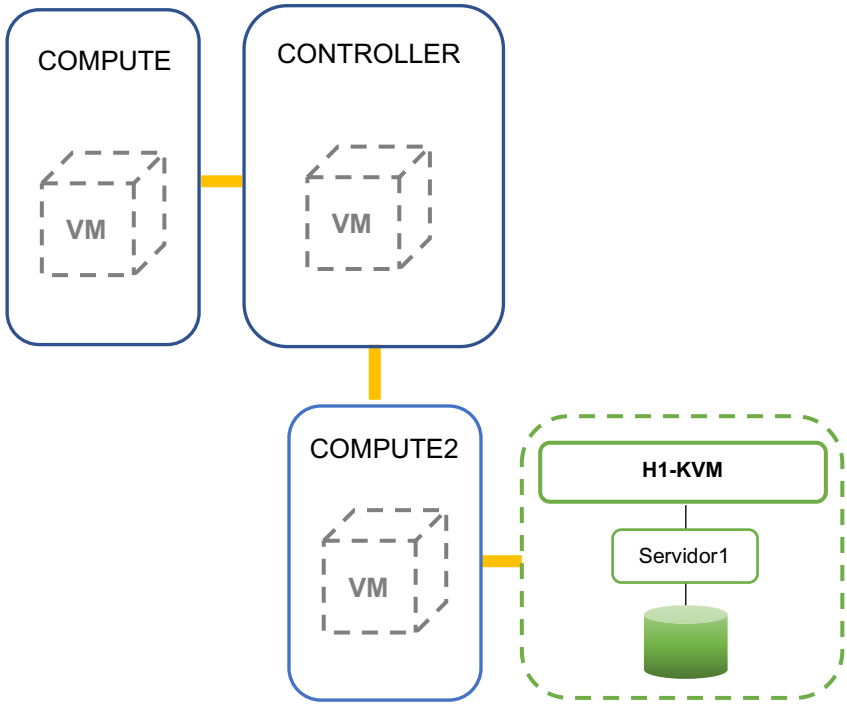
Figura 8.1 Modelo de CDDS basado en OpenStack.



Para el desarrollo del presente modelo de CDDS se toma en consideración que las infraestructuras de virtualización identificadas en el inventario del centro de datos del CICESE actualmente está en producción y no es posible utilizarlas con fines de prueba, por lo tanto, se realizará una representación mediante máquinas virtuales.

En la Figura 8.2 se observan los ambientes del modelo de CDDS representados de acuerdo con las máquinas virtuales que se utilizarán para el modelado. En la sección 8.1 se describirán sus características de acuerdo a los requerimientos específicos.

Figura 8.2 Máquinas virtuales requeridas para el Modelo cd CDDS basado en OpenStack.



8.1. Requerimientos.

El modelo de CDDS implantado utiliza la última versión estable de *OpenStack*, conocida con el nombre de *Stein* [9]. A continuación, se mencionan los requerimientos de software y hardware que necesita para ser instalado:

[9] https://docs.openstack.org/devstack/latest/

Requerimientos del Sistema[10]:

- Sistemas operativos soportados (64-bits):
  - openSUSE Leap 42.3, openSUSE Leap 15, SUSE Linux Enterprise Server 12 SP4, SUSE Linux Enterprise Server 15.
  - Red Hat Enterprise Linux 7 and CentOS 7
  - Ubuntu 16.04 (LTS).

- Otras librerías:
  - Python 2.7 o 3.5, (3.6 soporte experimental).
  - Django 1.11 o 2.0
  - Chrony implementación de NTP *(Network Protocol Time),* sincronización de tiempo entre servidores de *OpenStack*
  - SQL database, MariaDB, MySQL, algunas versiones de OpenStack soportan PostgreSQL.
  - DNS (*Domain Name Service*) para configuración de red.

Requerimientos de hardware:

Para la instalación de *OpenStack* en este modelo de CDDS, se requieren dos tipos de nodos, Controller y Compute, con las siguientes características mínimas de hardware[11],

- Nodo Controller: 1 procesador, 4 GB memoria, y 5 GB almacenamiento.
- Nodo Compute: 1 procesador, 2 GB memoria, y 10 GB almacenamiento.

[10] https://docs.openstack.org/horizon/stein/install/system-requirements.html

[11] https://docs.openstack.org/newton/install-guide-rdo/environment.html

Para propósitos de la implementación del modelo de CDDS se eligió construir cada nodo como una máquina virtual (VM). Adicionalmente se requiere un nodo Compute por cada hipervisor que se agregue al ambiente de OpenStack y las máquinas virtuales que representarán los hipervisores. Las características de cada una de estas máquinas virtuales están descritas en la Tabla 8.1,

Tabla 8.1 Características de las máquinas virtuales requeridas para modelo de CDDS.

Nombre VM	**Características**	**Propósito**
Controller/ Stack-begin	Ubuntu 16 64bits 8vCPU 16GB RAM 40 GB HDD IP 158.97.243.63	Horizon -Interfaz administrativa (dashboard) Neutron – Servicio de Red Keystone - Servicio de identificación Swif, Glance - Servicio de almacenamiento básico
Compute/ stack-01	Ubuntu 16 64bits 2vCPU 4GB RAM 20GB HDD IP 158.97.243.64	Nova - Servicio de cómputo de OpenStack
Compute2/ Stack-02	Ubuntu 16 64bits 2vCPU 4GB RAM 20GB HDD IP 158.97.243.51	Módulo NOVA de cómputo de OpenStack para enlace con hipervisor KVM
H1-KVM	Ubuntu 16 64bits 8vCPU 16GB RAM 40 GB HDD IP 158.97.243.200	Hipervisor KVM

En este punto es importante señalar que para implementaciones reales es obligatorio dimensionar[12] los requerimientos de la infraestructura que se utilizará de acuerdo a las necesidades que se demanden en el proyecto de CDDS.

8.2. Instalación y configuración.

Los procesos de instalación y configuración descritos en esta sección están de acuerdo con la documentación oficial publicada por OpenStack.

Los pasos para la instalación y configuración del nodo Controller en la máquina virtual controller, con la última versión de *OpenStack Stein,* fueron los siguientes*,*

i. Debido a que es muy importante la sincronización de tiempos entre los diferentes nodos que se utilizaran, en una consola se debe verificar el tiempo con el mando:
   timedatectl
ii. Es necesario agregar el usuario stack, con el mando:
   sudo useradd -s /bin/bash -d /opt/stack -m stack
iii. Editar el archvio /etc/sudoers.d/stack y agregar la línea
   stack ALL=(ALL) NOPASSWD: ALL
iv. En adelante debe de efectuar los mandos como usuario stack
v. Se clona el repositorio:
   git clone https://git.openstack.org/openstack-dev/devstack
vi. Acceder a la carpeta devstack
vii. Generar el fichero de configuración local, local.conf y escribir la configuración:

```
[[local|localrc]]
ADMIN_PASSWORD=stack
DATABASE_PASSWORD=$ADMIN_PASSWORD
RABBIT_PASSWORD=$ADMIN_PASSWORD
```

[12] https://www.stratoscale.com/blog/openstack/openstack-hardware-requirements-and-capacity-planning-servers-cpu-and-ram-part-1/

SERVICE_PASSWORD=$ADMIN_PASSWORD

HOST_IP=158.97.243.63

viii. Editar el archivo /etc/hosts y escribir la dirección de pruebas asignada:

127.0.0.1 localhost

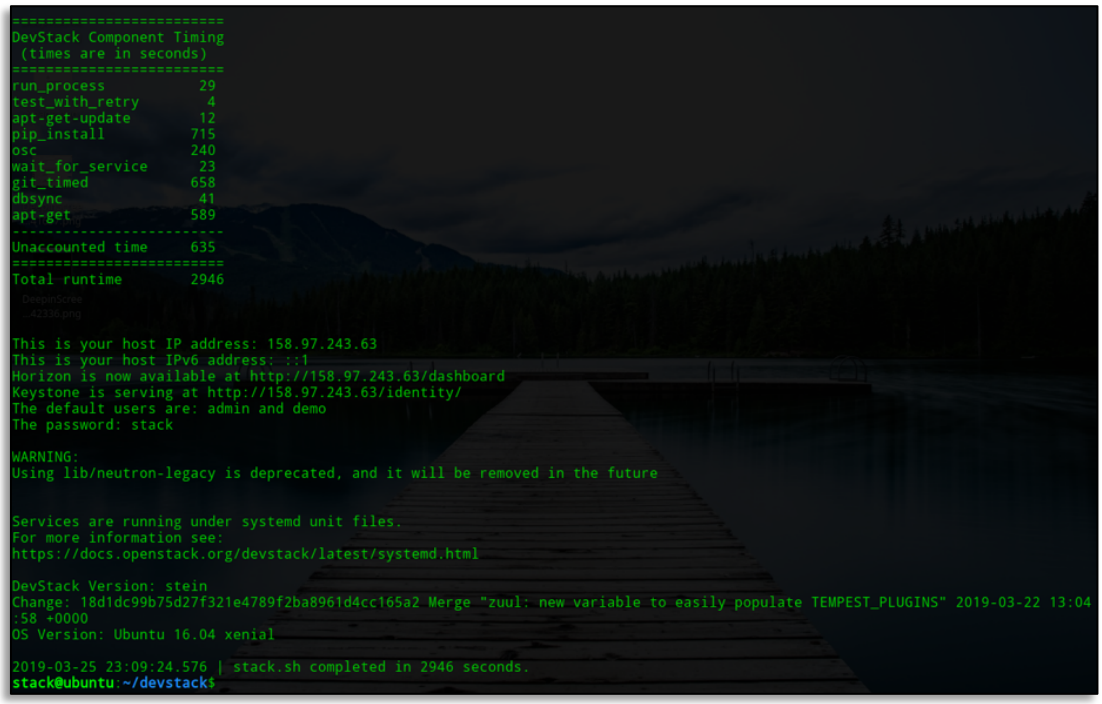
158.97.243.63 devstack

ix. Ejecutar el script de instalación

./stack.sh

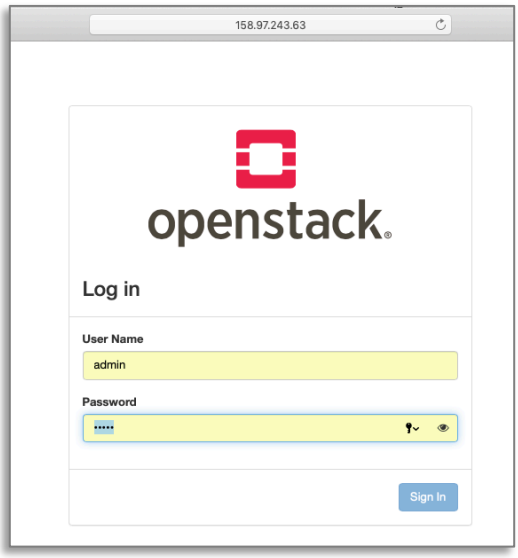
En la Figura 8.3 se observa la consola donde se completa la instalación del software con éxito.

Figura 8.3 Pantalla de instalación de Controller para OpenStack.



Como resultado de la instalación del nodo controller se obtiene la dirección de acceso a la interfaz de administración https://158.97.243.63/dashboard, que se muestra en la Figura 8.4.

Figura 8.4 Acceso a Dashboard del modelo de CDDS con OpenStack.



La instalación del módulo nova-compute se realizó a través de una consola en la maquina virtual compute, usando el siguiente comando:

"Apt-get install nova-compute nova-compute-vmware python-suds”

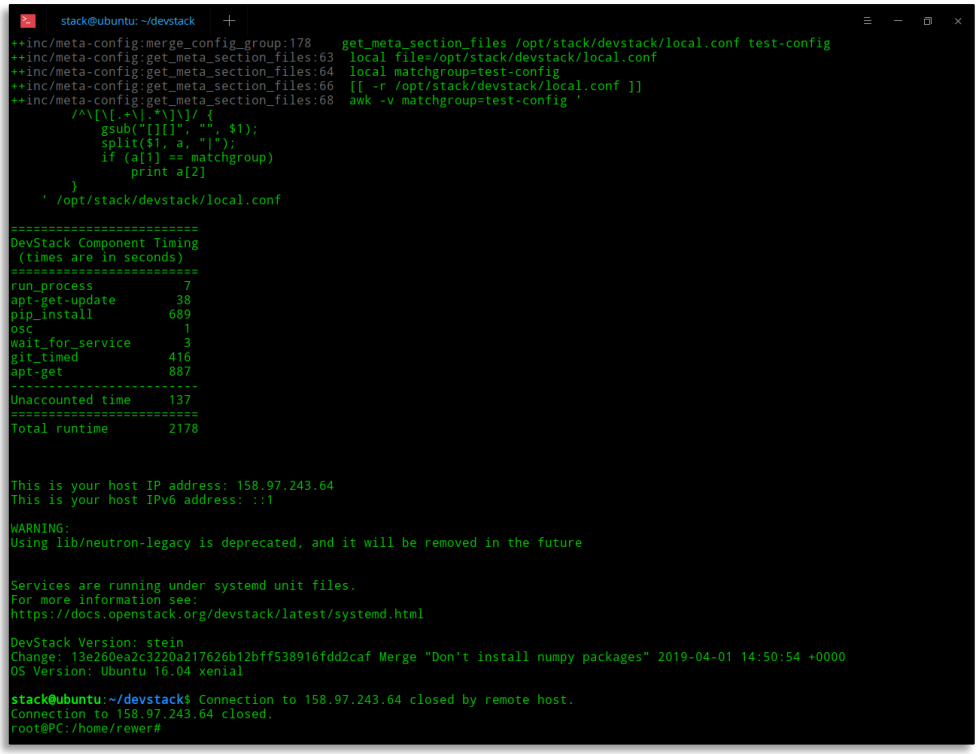
En la Figura 8.5 se presenta la consola de la maquina virtual compute donde se realizó la instalación completa del módulo nova-compute.

La configuración del nodo compute se especifica en el archivo /etc/nova/nova.conf, este contiene secciones predefinidas donde se agregaron la dirección IP del nodo controller al que estará conectado, la dirección IP asignada al nodo compute y los siguientes parámetros:

[DEFAULT]

transport_url =
rabbit://openstack:RABBIT_PASS@158.97.243.63
my_ip = 158.97.243.64
use_neutron = true
firewall_driver = nova.virt.firewall.NoopFirewallDriver

Figura 8.5 Pantalla de instalación de Nova-Compute de OpenStack.



[api]

auth_strategy = keystone

[keystone_authtoken]

www_authenticate_uri = http:// 158.97.243.63:5000/

auth_url = http:// 158.97.243.63:5000/

memcached_servers = 158.97.243.63:11211

auth_type = password

project_domain_name = Default

user_domain_name = Default

project_name = service

username = nova

password = NOVA_PASS

[oslo_concurrency]

```
lock_path = /var/lib/nova/tmp

[placement]
region_name = RegionOne
project_domain_name = Default
project_name = service
auth_type = password
user_domain_name = Default
auth_url = http:// 158.97.243.63:5000/v3
username = placement
password = PLACEMENT_PASS
```

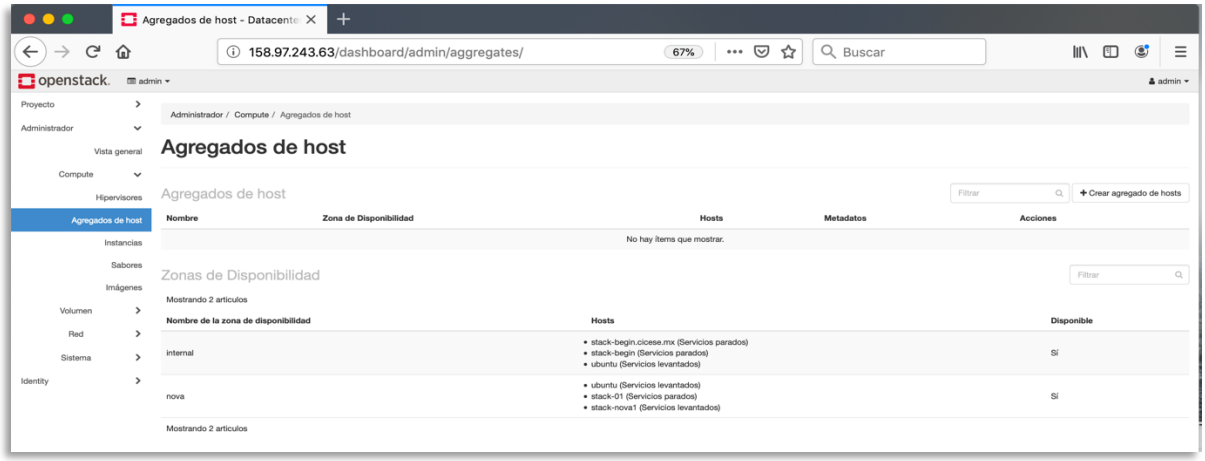
Enseguida, se realizó un clon de la maquina virtual compute para general la máquina compute2, que se encarga de establecer la conexión entre el hipervisor KVM con el nodo Controller de *OpenStack.* Se modificaron los siguientes parámetros de configuración en el archivo /etc/nova/nova.conf:

```
[DEFAULT]
my_ip = 158.97.243.64

[vnc]
enabled = true
server_listen = 0.0.0.0
server_proxyclient_address = $my_ip
novncproxy_base_url =
        http:// 158.97.243.63:6080/vnc_auto.html
```

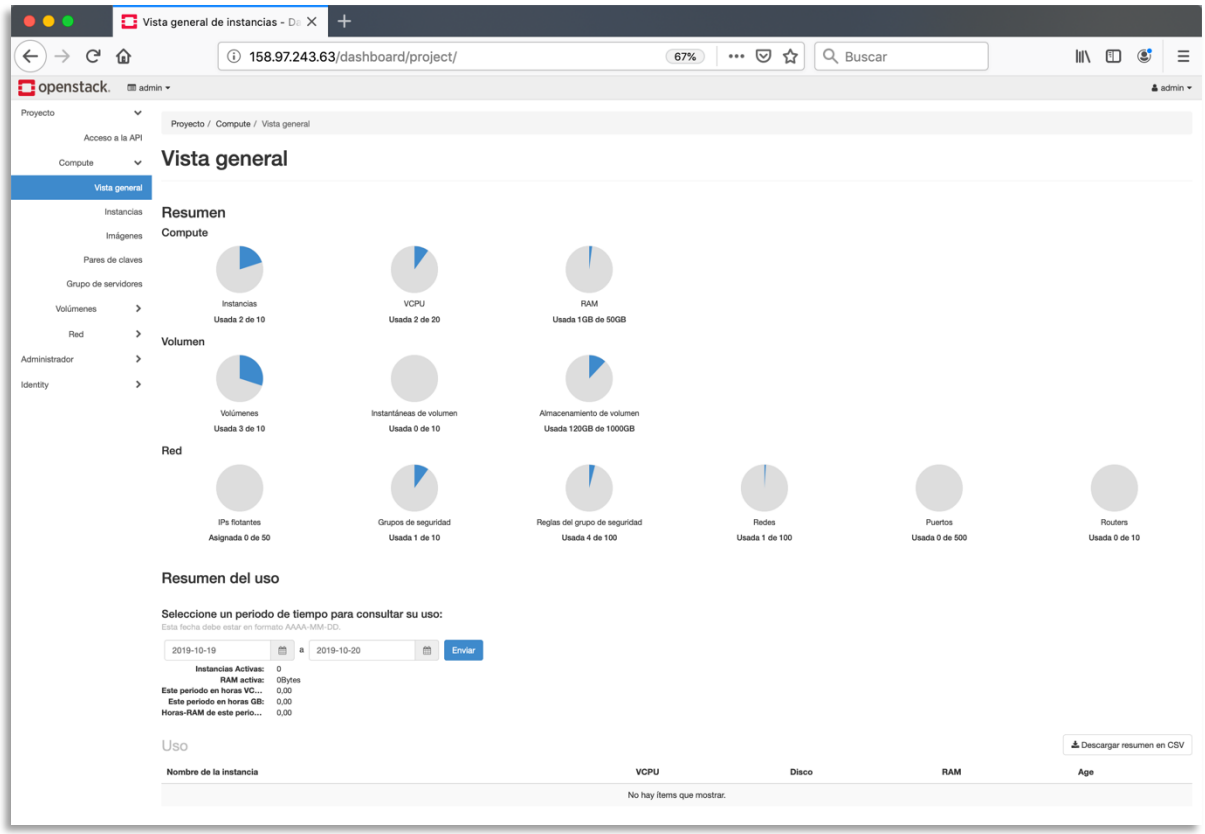
Como resultado se obtiene la integración de los nodos controller y compute como se aprecia en la Figura 8.6, en la sección Admin | Compute | Agregados de host

Figura 8.6 Visualización de nodos controller y compute generados en Dashboard de OpenStack.



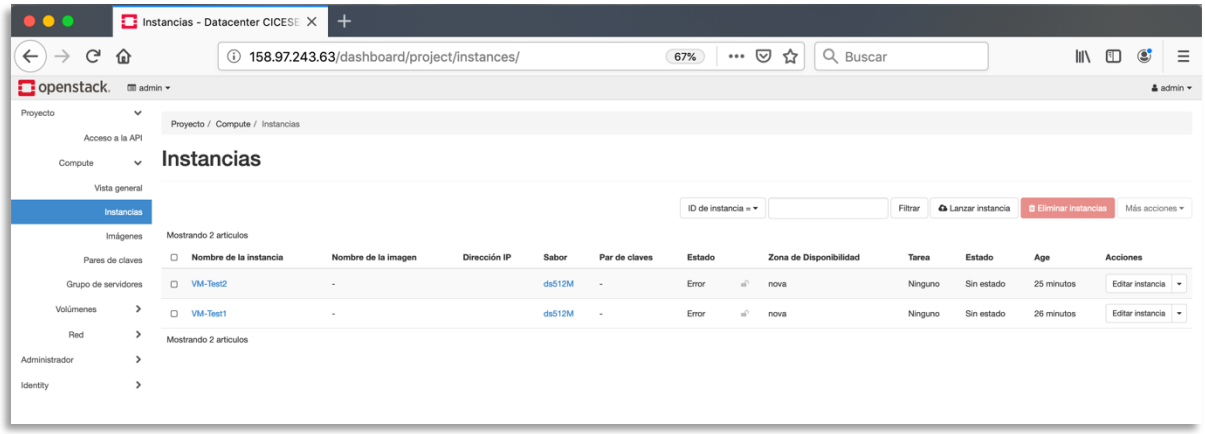
En la Figura 8.7 se presenta una vista general de Dashboard de OpenStack, donde se observa el resumen general de los recursos utilizados.

Figura 8.7 Vista general del Dashboard de OpenStack.



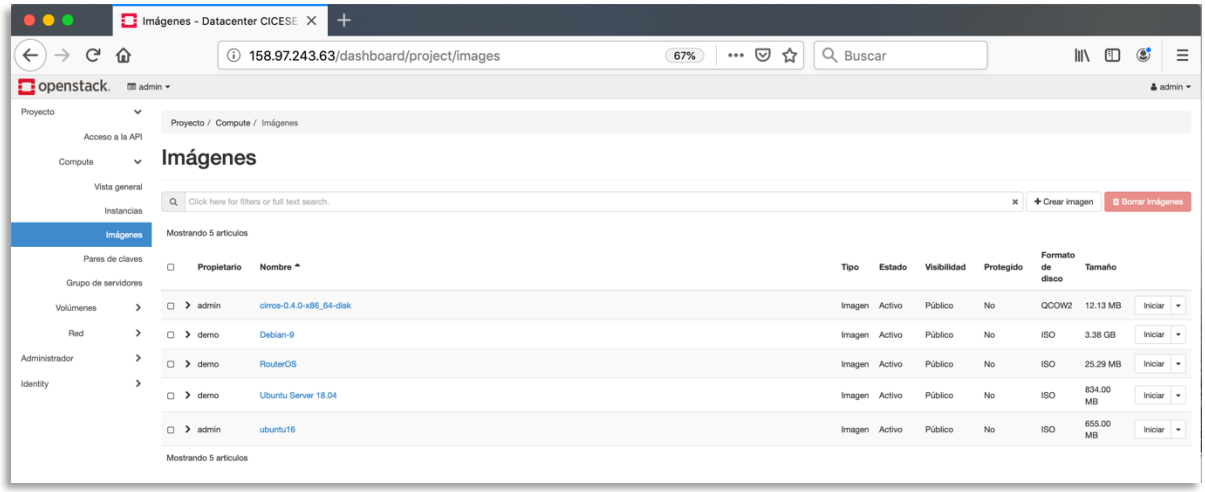
En la Figura 8.8 se listan dos instancias de máquinas virtuales levantadas a modo de ejemplo.

Figura 8.8 Menú de Instancias.



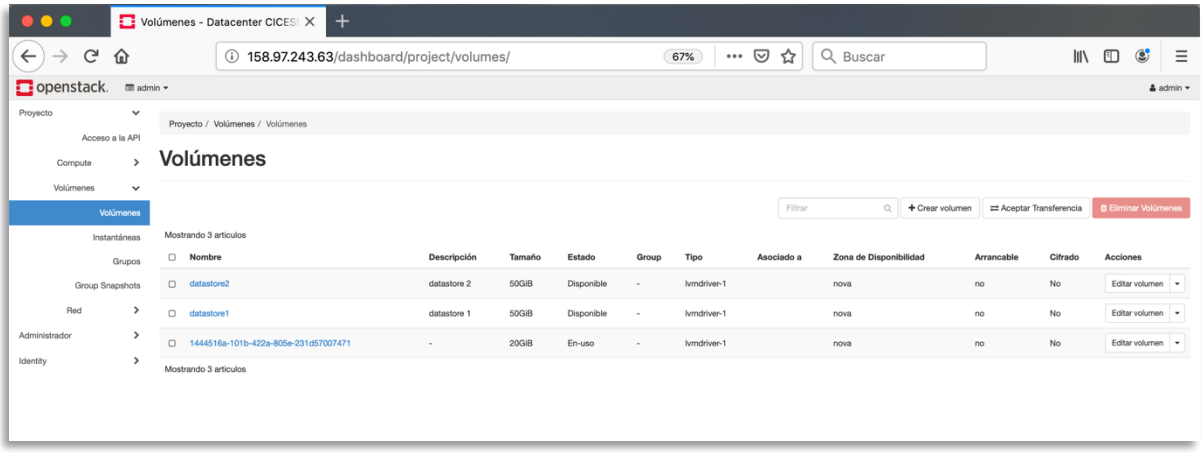
En la Figura 8.9 se presenta el menú de imágenes, donde se listan ejemplos de sistemas operativos, máquinas virtuales o contenedores disponibles para levantar instancias.

Figura 8.9 Menú de Imágenes.



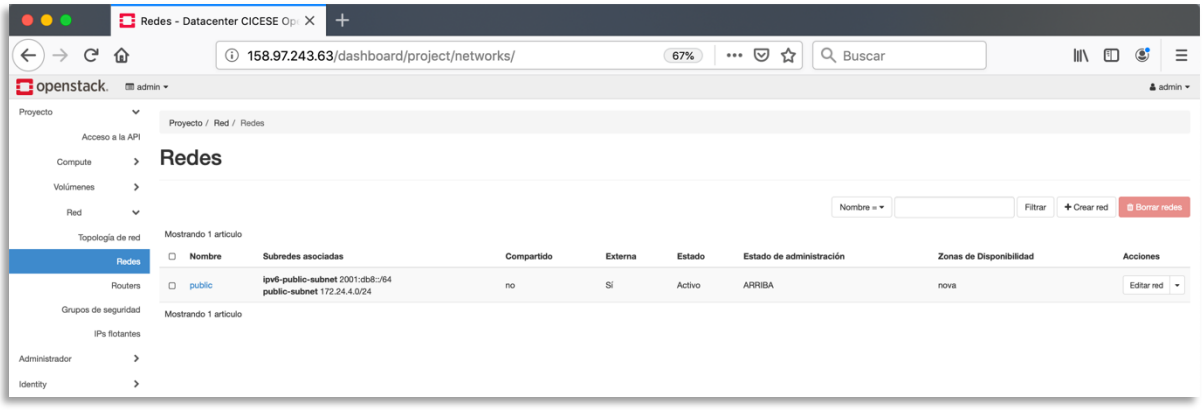
En la Figura 8.10 se muestra el menú de volúmenes, donde se pueden crear los diferentes tipos de almacenamiento definido por software que se utilizarán.

Figura 8.10 Menú de Volúmenes.



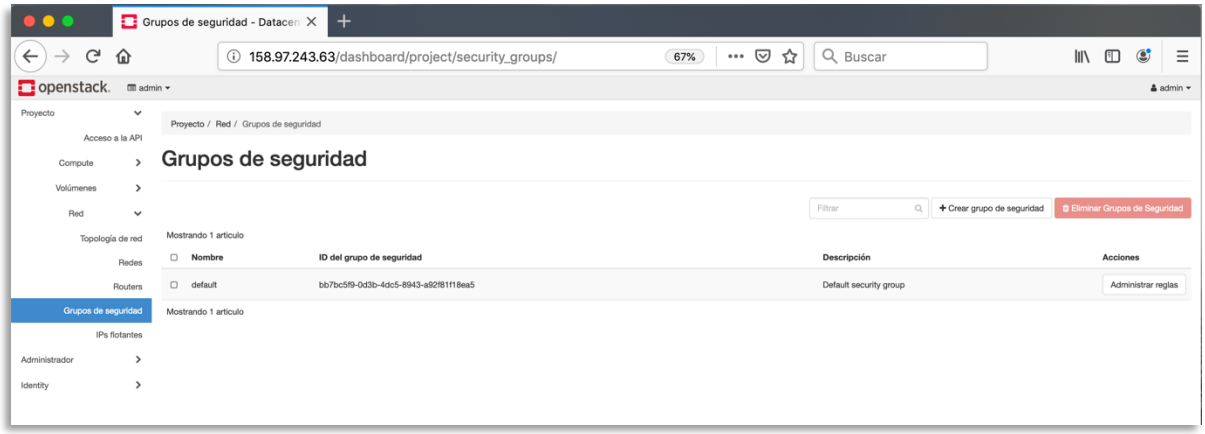
En la Figura 8.11 se muestran el menú de Red, donde se despliegan las redes definidas por software existentes, así como la topología de red, direcciones IP's flotantes y grupos de seguridad.

Figura 8.11 Menú de Red.



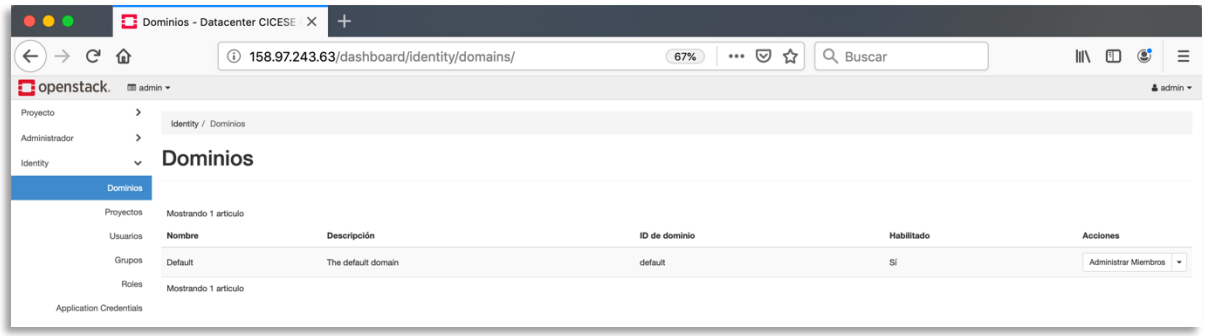
En la Figura 8.12 se observa como dentro del menú de red, es posible aplicar la seguridad definida por software mediante grupos de seguridad.

Figura 8.12 Seguridad definida por software creada para grupos.



En la Figura 8.13 se muestran el menú Identity donde es posible aplicar la seguridad definida por software mediante grupos de seguridad y gestión de identidades por dominios, proyectos, usuarios, roles.

Figura 8.13 Seguridad aplicada mediante control de acceso por identidades.



8.3. Conclusiones.

En el desarrollo de este capítulo se presentó la propuesta de un modelo de CDDS basado en OpenStack con los elementos básicos para la gestión del cómputo, red, almacenamiento y seguridad definidos por software, que permiten una visión general del funcionamiento de un CDDS.

Se realizó la implantación del modelo de CDDS utilizando máquinas virtuales lo cual proporciona un escenario de experimentación de la plataforma de OpenStack, que permitirá al personal de tecnologías de la información familiarizarse con ella.

Este modelo de CDDS permite percatarse de la opción real de utilizar los diferentes recursos existentes en un centro de datos convencional con tecnología de código abierto, incluso sustituir los hipervisores de licencia como VMWare por hipervisores de código abierto como KVM y otros.

9. Conclusiones.

En el presente trabajo se identificó la existencia de un área de oportunidad de implementación de CDDS en IES en México, en el estudio caso CICESE se obtuvo una radiografía de su centro de datos tradicional mediante el levantamiento de un inventario.

Al revisar la factibilidad técnica, operativa y económica se determinó que es posible su transformación gradual a un CDDS, utilizando recursos del inventario con que cuenta y soluciones existentes en el mercado, incluso ahorros al optar por soluciones de código abierto como *OpenStack.*

Las etapas propuestas en el procedimiento de ruta de migración facilitarán la migración de los recursos existentes y la integración de nuevos elementos al modelo de CDDS.

Además, el modelo de CDDS basado en OpenStack prueba la usabilidad e integración de elementos existentes con nuevas tecnologías que permitirán mantenerse a la vanguardia tecnológica en el ámbito de los centros de datos y proveer servicios de calidad.

10. Trabajo Futuro

Al realizar este estudio se observaron los siguientes aspectos que pueden ser considerados para continuar con la transformación a CDDS en las instalaciones del Centro:

- Actualizar equipos que pueden ser integrados a un CDDS.
- Reemplazar los equipos y sistemas más antiguos por implementaciones virtualizadas de código abierto.
- Para adquisiciones de nuevos equipos, asegurarse de su compatibilidad con los requerimientos de CDDS.
- Capacitación en CDDS para el personal tecnológico.

Adicionalmente, en este trabajo se identificó que los centros de datos también comprenden infraestructuras de soporte como plantas de energía, sistemas de enfriamiento, sistemas de control de incendio, sistemas de acceso, entre otros, los cuales podrían también ser gestionados por sistemas definidos por software para una detección oportuna de incidentes y fallas, así como un uso más eficiente de los mismos.

Anexo 1. Formato de solicitudes de hospedaje del centro de datos del CICESE.

CICESE	CENTRO DE INVESTIGACIÓN CIENTÍFICA Y DE EDUCACIÓN SUPERIOR DE ENSENADA, B. C. Dirección de Telemática	HOJA	2 DE 2
		FORMATO	DT- GCD-2016-01
		VERSIÓN	2.0
		FECHA	26-ABR-2016
	Solicitud de Hospedaje de Equipo de Cómputo en Centro de Datos		

Información adicional

1) **Responsable del equipo:**
2) **Contacto técnico:**
3) **Número de inventario (control patrimonial):** *Si no tiene, incluir número de contrato de servicio, arrendamiento, convenio con CICESE o especificar el proyecto de investigación donde proviene el equipo.*

Vigencia del servicio

1) **Fecha de inicio del servicio:**
2) **Fecha de finalización del servicio:**

Condiciones de uso del servicio

1) **Leer el documento "Condiciones de Uso del Servicio de Hospedaje de Equipo en el Centro de Datos".**

NOTA: Al firmar la solicitud, está enterado y acepta las condiciones de uso del servicio que solicita.

Fecha de la solicitud
dd/mm/aaaa

Sección de firmas

Nombre/ cargo y Rol	**Firma**
Nombre del responsable del equipo	

IMPORTANTE: El servicio de hospedaje de equipo es sólo para la realización de las actividades sustantivas del Centro por lo que no se permitirá su uso para actividades personales o con fines de lucro, a menos que sea parte de un convenio institucional o las autoridades competentes del Centro otorguen su autorización.

Requerimientos técnicos

1) **Número de unidades de racks (Us) o gabinetes:**
2) **Marca del equipo:**
3) **Modelo del equipo:**
4) **No. Serie:**
5) **Requerimientos de energía eléctrica (120V, 220V):**
6) **Consumo máximo de energía del equipo (watts):**
7) **Conectividad (1Gbps, 10Gbps):**
8) **Número de tarjetas de red:**
9) **Nombre(s) tentativo para registro en DNS:**

Requerimientos en software

En el caso de requerir apoyo/soporte para la instalación de software en el equipo, describir las necesidades en este rubro.

Servicios que ofrecerá el equipo

Describir detalladamente los servicios que estarán habilitados en el equipo, el uso que se le va a dar al equipo, que tipo de acceso remoto utilizará.

Describir los usuarios potenciales del servicio que ofrecerá el equipo (investigadores, comunidad en general, etc).

Anexo 2. Glosario

ANIUES: Asociación Nacional de Universidades e Instituciones de Educación Superior

API: por sus siglas en inglés *Application Programming Interface*, Interfaz de programación de aplicaciones.

CICESE: Centro de Investigación Científica y de Educación Superior de Ensenada.

CDDS. Centro de datos definido por software.

Hipervisor: software que controla el acceso a los recursos disponibles de la capa de física de la infraestructura anfitriona como CPU, memoria, red y almacenamiento, y los presenta a cada sistema operativo invitado como un conjunto de interfaces virtuales**.**

Hiperconvergente: Se refiere a las infraestructuras físicas que permiten la integración o combinación de los diferentes recursos de procesamiento, almacenamiento y red en un solo sistema.

IES: Instituciones de Educación Superior.

SDN. Por sus siglas en inglés *Software Defined Network*. Red definida por software.

SDSec. Por sus siglas en inglés *Software Defined Security*. Seguridad definida por software.

SLA. Por sus siglas en inglés *Service Level Agreement*, Acuerdo de nivel de servicio.
TIC: Tecnologías de la Información y Comunicación

Virtualización: Tecnología computacional que mediante el uso de software permite la ejecución de distintos sistemas operativos a la vez en un mismo servidor físico.

Anexo 3. Referencias

Aguilera, P. (2010). *Seguridad informática*. (G. Morlanes, Ed.). Madrid, España: Editorial Editex.

Amazon Web Service, I. (2017). Amazon Web Services Site. Retrieved from https://aws.amazon.com/

ANUIES. (2017). *Estado Actual De Las Tecnologías De La Información Y Las Comunicaciones En Las Instituciones De Educación Superior En México*. Retrieved from http://estudio-tic.anuies.mx/ESTUDIO_2017_ANUIES-TIC_v2_2.pdf

Barroso, L. A., & Hölzle, U. (2009). *The Datacenter as a Computer An Introduction to the Design of Warehouse-Scale Machines*. Madison: Morgan & Claypool.

Bazargan, F., Yeun, C. Y., & Zemerly, M. J. (2016). State-of-the-Art of Virtualization, its Security Threats and Deployment Models. *International Journal for Information Security Research*, *3*(3), 335–343. https://doi.org/10.20533/ijisr.2042.4639.2013.0039

Burneo Valarezo, S., Delgado Víctore, R., & Vérez, M. A. (2016). Estudio de factibilidad en el sistema de dirección por proyectos de inversión. *Ingeniería Industrial*, *XXXVII*(3), 305–312. Retrieved from http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59362016000300009

Corradi, A., Fanelli, M., & Foschini, L. (2014). VM consolidation: A real case based on OpenStack Cloud. *Future Generation Computer Systems*, *32*(1), 118–127. https://doi.org/10.1016/j.future.2012.05.012

Darabseh, Ala', Al-Ayyoub, M., Jararweh, Y., Benkhelifa, E., Vouk, M., & Rindos, A. (2015a). SDSecurity: A Software Defined Security experimental framework. In *2015 IEEE International Conference on Communication Workshop, ICCW 2015*. https://doi.org/10.1109/ICCW.2015.7247453

Darabseh, Ala', Al-Ayyoub, M., Jararweh, Y., Benkhelifa, E., Vouk, M., & Rindos, A. (2015b). SDStorage: A software defined storage experimental framework. In *Proceedings - 2015 IEEE International Conference on Cloud Engineering, IC2E 2015*. https://doi.org/10.1109/IC2E.2015.60

Darabseh, Ala, Al-Ayyoub, M., Jararweh, Y., Benkhelifa, E., Vouk, M., & Rindos, A. (2015). SDDC: A Software Defined Datacenter Experimental Framework. In *Proceedings - 2015 International Conference on Future Internet of Things and Cloud, FiCloud 2015 and 2015 International Conference on Open and Big Data, OBD 2015*. https://doi.org/10.1109/FiCloud.2015.127

Datt, A., Goel, A., & Gupta, S. C. (2015). Analysis of Infrastructure Monitoring Requirements for OpenStack Nova. *Procedia Computer Science*, *54*, 127–136. https://doi.org/10.1016/j.procs.2015.06.015

Denton, J. (2014). *Learning OpenStack Networking (Neutron)*. Packt Publishing Ltd. Retrieved from https://books.google.com.mx/books?hl=es&lr=&id=iXrKBAAAQBAJ&oi=fnd&pg=PT14&dq=openstack+Neutron+&ots=lH5ovEhZ1q&sig=fgSalF2y7VH9idQe08fuVll84As#v=onepage&q=openstack Neutron&f=false

Distributed Management Task Force (DMTF). (2014). *Software Defined Data Center (SDDC) Definition*.

DMTF. (2014). Software Defined Data Center (SDDC) Definition A White Paper from the OSDDC Incubator, 1–22. Retrieved from https://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0501_1.0.1a.pdf

Douglis, F., & Krieger, O. (2013). Virtualization. *IEEE Internet Computing*. https://doi.org/10.1109/MIC.2013.42

Dubs de Moya, R. (2006). El Proyecto Factible: una modalidad de investigación. *Sapiens. Revista Universitaria de Investigación*, *1*(1), 37–48. Retrieved from http://www.redalyc.org/articulo.oa?id=349832311003

Fichera, R., Washburn, D., & Chi, E. (2012). *The Software-Defined Data Center Is The Future Of Infrastructure Architecture*.

Gadir, O., Subbanna, K., & Vayyala, A. (2005). HIGH-AVAILIABILITY CLUSTER VIRTUAL SERVER SYSTEM. United States Patent.

Gartner. (2015). *Gartner Says the Future of the Data Center Is Software-Defined*. Retrieved from https://www.gartner.com/newsroom/id/3136417

Google, I. (2019). Google Cloud. Retrieved from https://cloud.google.com/

Gorannson P., Black C., & C. T. (2015). *Software Defined Network: A Comprensive Approach*. (M. Kaufmann, Ed.) (2da ed.).

Kreutz, D., Rothenberg, C. E., Azodolmolky, S., Uhlig, S., Verissimo, P., & Ramos, F. (2015). Software-Defined Networking : A Comprehensive Survey. *Proceedings of the IEEE*, *103*(1), 14–76. https://doi.org/10.1109/JPROC.2014.2371999

Litvinski, O., & Gherbi, A. (2013). Experimental evaluation of OpenStack compute scheduler. *Procedia Computer Science*, *19*(Ant), 116–123. https://doi.org/10.1016/j.procs.2013.06.020

Mark Carlson, Alan Yoder, L. S., Don Deel, Carlos Pratt, C. L., & Voigt, D. (2015). *SNIA Software Defined STirage White Paper v1*.

Mckeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Larry, P., Rexford, J., … Jonathan, T. (2008). OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM Newsletter Computer Communication Review*. https://doi.org/10.1145/1355734.1355746

Microsoft. (2018). Windows Server Software-Defined Datacenter. Retrieved from https://docs.microsoft.com/en-us/windows-server/sddc

Nadkarni, A. (2018). *White Paper Software-Defined Storage — Opportunities for the Enterprise*.

OpenStack. (2019). OpenStack Documentation. Retrieved from http://openstack.org

OpenStack Community Project. (2018). *OpenStack Operation Guide*.

Pepple, K. (2011). *Deploying OpenStack*. (O'Really, Ed.). https://doi.org/10.1017/CBO9781107415324.004

PMI. (2008). *A GUIDE TO THE PROJECT MANAGEMENT BODY OF KNOWLEDGE*. Project Management Institute.

Rackspace, I. (2019). Rackspace Home Page. Retrieved from https://www.rackspace.com/

Radez, D. (2016). *OpenStack Essentials* (Second). Packt Publishing Ltd.

Rivera Rodríguez, R., & Lozano Rizk, J. (2017). *La Importancia de las TICs como Apoyo a la Investigación Científica*. Ensenada.

TIA. (2005). TIA Standard ANSI/TIA-942-2005, (April), 148.

Uhlig, R., Neiger, G., Rodgers, D., L., A., Santoni, Fernando, … Smith, L. (2014). Intel Virtualization Technology List. *I E E E C o m p u t e r S o c i e t Y*, *2014*, 48–56. Retrieved from https://ieeexplore.ieee.org/abstract/document/1430631

VMware Inc. (2015). *VMware Software-Defined Data Center: Capabilities and Outcomes*. Retrieved from http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/technical-whitepaper-sddc-capabilities-itoutcomes-white-paper.pdf

VMware Inc. (2016). VMWARE CLOUD FOUNDATION: FAQ. Retrieved from www.vmware.com

VMware Inc. (2017). Cloud Foundation 2.2. Architecture. Retrieved from https://docs.vmware.com/en/VMware-Cloud-Foundation/2.2/com.vmware.vcf.ovdeploy.doc_22/GUID-C6AF75AE-569C-49F8-A15E-E9A6EF9549DA.html

VMware Inc. (2018). *VMWARE CLOUD FOUNDATION : THE SIMPLEST PATH TO THE HYBRID CLOUD*. Retrieved from https://www.vmware.com/mx/products/cloud-foundation.html

VMware Inc. (2019). VIO VMware Integrated OpenStack.