UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA TECNOLÓGICA DE SERVIDORES PARA MEJORAR LA SEGURIDAD Y DISPONIBILIDAD DE LOS SISTEMAS INFORMÁTICOS EN EL HOSPITAL REGIONAL HERMILIO VALDIZÁN MEDRANO (HRHVM) - 2020"

TESIS PARA OPTAR EL TÍTULO DE

INGENIERO DE SISTEMAS

TESISTAS:

Bach. DINA CABALLERO UGARTE

Bach. NELSON DRYER SALAZAR ARANDA

ASESOR:

Ing. LUIS MEZA ORDOÑEZ

HUÁNUCO – PERÚ

2021

DEDICATORIA

En primer lugar, el presente trabajo es dedicado a Dios por darnos la oportunidad de llegar hasta esta instancia y por brindarnos las fuerzas necesarias para desarrollar el proyecto de investigación. Y, en segundo lugar, el presente trabajo es dedicado a nuestros seres queridos ya que gracias a su apoyo se pudo realizar la presente investigación.

AGRADECIMIENTO

Agradecemos en primer lugar a Dios por no dejarnos caer en ningún momento, por darnos el pan de cada día, por darnos las fuerzas necesarias para poder superarnos en todos nuestros obstáculos y seguir creciendo profesionalmente.

A los familiares de Dina Caballero Ugarte, a su madre Edith Carmen Ugarte Jorge, a su padre Juan Caballero Gonzáles y a sus queridos hermanos Daniel Caballero Ugarte y Alfredo Caballero Ugarte por sus incentivaciones a seguir adelante con sus metas.

A los familiares de Dryer Salazar Aranda, a su madre María Aranda Retis, a su padre Cesar Salazar Zevallos y a sus queridos hermanos Cinthia Leyva Aranda, Irving Leyva Aranda y María Salazar Aranda por sus incentivaciones a seguir adelante con sus metas.

A mis asesores, Ing. Luis Meza Ordoñez, Ing. Milton Pérez Solís y Dr. Inés Eusebia Jesús Tolentino por asesorarnos y guiarnos para la realización de esta investigación.

RESUMEN

La presente investigación tiene como objetivo la implementación de una infraestructura tecnológica virtualizada de servidores para mejorar la seguridad y disponibilidad de los sistemas informáticos en el Hospital Regional Hermilio Valdizan Medrano. La investigación de esta problemática se realizó por el interés de disminuir el tiempo de indisponibilidad de los servicios informáticos, por los diversos problemas tales como lentitud o caídas de los sistemas, debido a conexiones concurrentes en los servicios web, disminuir también los ataques que comúnmente sufren los equipos informáticos como virus que pueden alterar información o datos importantes para la institución.

Se empezó por analizar el estado actual de la infraestructura de red física y lógica, así como también los servicios informáticos que brindan el Hospital Regional Hermilio Valdizan, a partir de esto se vio la manera de cómo solucionar los diversos problemas de la infraestructura tecnológica, dando, así como resultado el cambio de hipervisor, estructuramiento de la red e implementación de servidores virtualizados que brindan servicios de seguridad y de alta disponibilidad. Se implementó un servidor Firewall y Proxy que garantizo la seguridad informática, se implementó un servidor NGINX que garantizo el balanceo de carga de las peticiones de los usuarios y se realizó una configuración al hipervisor de alta disponibilidad mediante las interfaces de red.

Finalmente, se analizó el estado actual de los servidores y el estado posterior a la implementación mediante la realización de encuestas, entrevistas y observaciones en el área de informática del Hospital Regional, con lo cual se concluyó que el 66,6% del personal de informática aprueba con “muy buena” la implementación de la infraestructura tecnológica virtualizada de servidores para mejorar la seguridad y disponibilidad de los sistemas informáticos.

Palabras clave: Virtualización de servidores, infraestructura TI virtualizada, seguridad y disponibilidad a nivel de servidores.

SUMMARY

The present research aims to implement a virtualized technological infrastructure of servers to improve the security and availability of computer systems at the Hermilio Valdizan Medrano Regional Hospital. The investigation of this problem was carried out in the interest of reducing the time of unavailability of computer services, due to various problems such as slowness or crashes of the systems, due to concurrent connections in web services, also reducing the attacks that commonly suffer computer equipment such as viruses that can alter information or data important to the institution.

It began by analyzing the current state of the physical and logical network infrastructure, as well as the computer services provided by the Hermilio Valdizan Regional Hospital, from this it was seen how to solve the various problems of the technological infrastructure, giving as a result, the hypervisor change, network structuring and implementation of virtualized servers that provide security and high availability services. A Firewall and Proxy server was implemented that guaranteed computer security, an NGINX server was implemented that guaranteed the load balancing of user requests, and a high-availability hypervisor configuration was made through the network interfaces.

Finally, the current status of the servers and the status after implementation were analyzed by conducting surveys, interviews and observations in the IT area of the Regional Hospital, which concluded that 66.6% of IT staff approves with "very good" the implementation of the virtualized technological infrastructure of servers to improve the security and availability of computer systems.

Keywords: Server virtualization, virtualized IT infrastructure, security and availability at the server level.

INTRODUCCIÓN

Los servicios informáticos brindados por una institución de salud suelen realizar tareas fundamentales, en donde la falta de disponibilidad produce pérdidas de tiempo que no conviene a la institución debido a que los pacientes necesitan realizar cuanto antes sus consultas médicas, y no solo la disponibilidad sino también en cuanto a la seguridad informática en hospitales es cada vez más necesaria. Las instituciones para la salud se convierten en un punto crítico para la protección de datos, pues manejan información sensible sobre el estado de salud o condiciones de los pacientes. Sumado a esto, la cantidad de funcionarios de un hospital que pueden tener acceso a esta información es relativamente alta por lo que una fuga de información, especialmente en esta era digital, debe ser tratada con cuidado.

La presente investigación muestra una solución tecnológica de seguridad y alta disponibilidad para servidores. Investigación que nace de la necesidad de minimizar el tiempo muerto de los servicios ante las constantes caídas de los servidores, del Hospital Regional Hermilio Valdizán Medrano.

CAPITULO I: Se plantea la problemática, se establece el objetivo general y los objetivos específicos de la investigación, así como la hipótesis, justificación y los límites de la misma.

CAPITULO II: Se plantea el marco teórico, se realiza las leyes fundamentales y principios de servidores, en las cuales se basó para realizar esta investigación. Se presenta las definiciones y conceptos fundamentales relacionados a la investigación. Se realizar el marco situacional donde se hablará sobre la institución donde se realizará la investigación.

CAPITULO III: Se refiere al marco metodológico, donde se abarca el planteamiento metodológico, que incluye el nivel de investigación, el tipo de investigación, el diseño de la investigación, la población y muestra, instrumentos de recolección de datos y el procesamiento de datos.

CAPITULO IV: Se analiza el estado actual de la infraestructura de red a nivel físico, así como los equipos servidores y los servicios que brinda el Hospital

Regional a los usuarios, y a partir de ello se realiza un estudio detallado de soluciones tecnológicas a nivel de software, analizando y haciendo las comparaciones de las características que estos poseen; se cuantifican las ventajas y desventajas de los diferentes hipervisores y se eligió el hipervisor que garantiza alta disponibilidad y que funcionalmente minimice los tiempos de caídas de los servidores.

CAPITULO V: Se diseña una infraestructura tecnológica para mejorar la disponibilidad de los servicios como el servicio Web, el servicio de base de datos las 24/7 y la seguridad informática. Se explica el proceso de la implementación.

CAPITULO VI: Se analiza el estado actual de los servidores y el estado posterior a la implementación, mediante encuestas realizadas al personal del área de informática del Hospital Regional Hermilio Valdizán Medrano, de esta manera se garantiza la mejora en la disponibilidad de los servicios brindados y mejora en cuanto a la seguridad informática.

Y por último se realiza las conclusiones de cada objetivo presentado en la investigación y se da las recomendaciones respectivas al Hospital Regional Hermilio Valdizán.

INDICE

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

I. PLANTEAMIENTO DEL PROBLEMA

1.1. Antecedentes y fundamentación del problema

En la actualidad, la demanda en el uso de los sistemas informáticos en el sector de salud mundialmente ha venido en aumento, ya que el uso adecuado de estos sistemas contribuye al ahorro de recursos, procesamiento de información y permite ofrecer un servicio de forma más eficaz y eficiente, debido al aumento significativo en la demanda de servicios de internet y la cantidad de transferencia de todo tipo de información, los sistemas informáticos se ven en la necesidad de trabajar de manera ininterrumpida y sin fallos durante todo el año. Para que estos servicios informáticos puedan funcionar correctamente se necesita servidores gestionados en la parte de seguridad y disponibilidad informática que aloje todos estos servicios.

La problemática de esta investigación recae en los servidores que prestan servicios informáticos, entre los cuales encontramos: los servicios de acceso a la web, los servicios de almacenamiento de archivos, servidores de bases de datos, por mencionar algunos, dichos servicios no poseen una infraestructura tecnológica adecuada que ofrezca en primer lugar seguridad, ya que dichos sistemas manejan información confidencial y en segundo lugar la disponibilidad de los servicios informáticos las 24 horas del día. Poseer un apropiado soporte de hardware, sin que este sea respaldado con un adecuado soporte de software o una configuración propicia que asegure la disponibilidad y seguridad de los servicios que ofrece un servidor, podría ocasionar fallas y caídas en alguno de ellos, ocasionado interrupciones en los servicios que ofrecen, muchos de ellos críticos para la institución, generando de esta manera malestar al personal del Hospital como a los usuarios.

Actualmente el principal problema que existe en la unidad de informática del Hospital Regional Hermilio Valdizán Medrano, es el alto congestionamiento de la red de comunicación, lo cual causa que los sistemas de información que están albergados en los servidores

empiecen a colapsar, y esto trae el malestar o insatisfacción de los colaboradores del Hospital, debido a que no pueden acceder a dichos sistemas y no puedan atender a los pacientes de la mejor manera posible. Pero porque existe congestionamiento, existe porque tenemos una infraestructura tecnológica desfasada, incumplimiento de cableado estructurado, etc.

El Hospital Regional Hermilio Valdizan Medrano, que es una institución dedicada a la atención integral de salud, ofrece una serie de servicios de información que se encuentran alojado y soportados por sus servidores, sin embargo, conforme la cantidad de usuarios aumenta en el hospital, lo hacen también una serie de problemas, como la demora en las respuestas o caídas de los sistemas, ocasionado por conexiones concurrentes y falta de disponibilidad en los servicios web; dichos servidores no poseen una red de alta disponibilidad, tampoco cuentan con una buena configuración de los servidores físicos.

Es debido a esto que se usará y configurará un servidor como Hipervisor para poder albergar los servidores web, para los sistemas de información del Hospital, servidor firewall para asegurarse de la protección de los sistemas frente a cualquier amenaza que provenga del exterior (robo de datos confidenciales, virus, etc.), servidor proxy para filtrar el uso de páginas web prohibidas y páginas que no compete en nada con su trabajo (Facebook, YouTube, WhatsApp, etc.).

La implementación de estos servidores reducirá el tráfico o congestionamiento de la red de comunicación y por último haremos que estos servidores virtualizados brinden una alta disponibilidad y seguridad de los sistemas de información del Hospital Regional Hermilio Valdizan.

1.2. Formulación del problema

1.2.1. Formulación del problema general

¿De qué manera influirá la implementación de una infraestructura tecnológica de servidores para mejorar la seguridad y la

disponibilidad de los sistemas informáticos en el Hospital Regional Hermilio Valdizán Medrano (HRHVM)?

1.2.2. Formulación de los problemas específicos

- ¿De qué manera el análisis de la infraestructura tecnológica del Hospital Regional influirá en mejorar la seguridad y disponibilidad de los sistemas informáticos?
- ¿Cómo influye el realizar un diseño de una estructura de red más adecuada para mejorar la seguridad y disponibilidad de los sistemas informáticos?
- ¿En qué medida la comparación de los diversos tipos de Hipervisores influirá en mejorar la seguridad y disponibilidad de los sistemas informáticos?
- ¿De qué manera la implementación de un servidor Firewall, Proxy Squid y Squidguard mejorara la seguridad informática del Hospital Regional Hermilio Valdizan?
- ¿Cómo influye la configuración bonding e implementación del servidor NGINX para mejorar la disponibilidad de los sistemas informáticos?

1.3. Objetivos: generales y específicos

1.3.1. Objetivo general

Implementar la infraestructura tecnológica de servidores para mejorar la seguridad y la disponibilidad de los sistemas informáticos en el Hospital Regional Hermilio Valdizán Medrano (HRHVM).

1.3.2. Objetivos específicos

- Analizar la infraestructura tecnológica actual del Hospital Regional Hermilio Valdizán.

- Realizar un diseño de una estructura de red más adecuada para el Hospital Regional Hermilio Valdizan Medrano.
- Comparar los diversos tipos de Hipervisores que se encuentran en el mercado actualmente.
- Implementar un Servidor Firewall, Proxy Squid y Squidguard en el Hospital Regional Hermilio Valdizan.
- Implementar un servidor Nginx y realizar la configuración bonding en el Hospital Regional Hermilio Valdizan.

1.4. Hipótesis: General y Específicos

1.4.1. Hipótesis general

H1: La infraestructura tecnológica de servidores, mejorará la seguridad y la disponibilidad de los sistemas informáticos en el Hospital Regional Hermilio Valdizán Medrano (HRHVM).

H0: La infraestructura tecnológica de servidores, no mejorará la seguridad y la disponibilidad de los sistemas informáticos en el Hospital Regional Hermilio Valdizán Medrano (HRHVM).

1.4.2. Hipótesis específicos

Ha1: Él análisis de la infraestructura de TI actual del Hospital Regional, influirá en mejorar la seguridad y disponibilidad de los sistemas informáticos.

Ha0: Él análisis de la infraestructura de TI actual del Hospital Regional, no influirá en mejorar la seguridad y disponibilidad de los sistemas informáticos.

Hb1: Realizar el diseño de una estructura de red más adecuada para el Hospital Regional, mejorará la seguridad y disponibilidad de los sistemas informáticos.

Hb0: Realizar el diseño de una estructura de red más adecuada para el Hospital Regional, no mejorará la seguridad y disponibilidad de los sistemas informáticos.

Hc1: La comparación de los diversos tipos de Hipervisores, influirá en la mejora de la seguridad y disponibilidad de los sistemas informáticos.

Hc0: La comparación de los diversos tipos de Hipervisores, no influirá en la mejora de la seguridad y disponibilidad de los sistemas informáticos.

Hd1: La implementación de un servidor Firewall, Proxy Squid y Squidguard mejorará la seguridad informática en el HRHVM.

Hd0: La implementación de un servidor Firewall, Proxy Squid y Squidguard, no mejorará la seguridad informática en el HRHVM.

He1: La implementación de un servidor Nginx y configuración bonding, mejorará la seguridad y disponibilidad informática en el HRHVM.

He0: La implementación de un servidor Nginx y configuración bonding, no mejorará la seguridad y disponibilidad informática en el HRHVM.

1.5. Variables, dimensiones e indicadores

Tabla 1: Variables, Dimensiones e Indicadores

VARIABLES	DIMENSIONES	INDICADORES
La seguridad y disponibilidad de los sistemas informáticos	Confidencialidad	% usuarios desconocidos accediendo a los servidores.
	Irrefutable	% de visitas a páginas web que no compete con el trabajo.
	Integridad	% de usuarios no autorizados que realizan cambios en el sistema.
	Disponibilidad	% de caídas de los servidores.

		% de tiempo de respuesta del servidor.
Implementación de una infraestructura tecnológica de servidores	Almacenamiento	% de consumo del almacenamiento.
	Rendimiento	% de respuesta a las predicciones de los usuarios.
	Seguridad	% de respuesta a las peticiones de los usuarios.
	Accesibilidad	% de peticiones bloqueadas a los servidores.

Fuente: Elaboración propia

1.6. Operacionalización de las variables

1.6.1. Implementación de una infraestructura tecnológica de servidores

Definición conceptual

La virtualización de la red se encarga de relacionar el hardware de red (enrutadores y switches), lo configura y se encarga de su administración, dependiendo de la necesidad, a través del software. En otras palabras, la inteligencia de esta tecnología nace del software y no del hardware individual que lo compone**.**

Definición operacional

La virtualización es utilizada para establecer un conjunto de procesos y procedimiento (los cuales poseen recursos diferentes), entregados por medio de una capa de software ligera denominada como el “hipervisor”. Quien tiene la función de administrar la comunicación entre el software y el hardware en el cual se realizará:

1. Virtualización de la red

2. Virtualización del Almacenamiento

3. Virtualización de Aplicaciones

4. Virtualización de sistemas operativos

Dimensiones e indicadores

Almacenamiento - % de consumo del almacenamiento

Rendimiento - % de repuestas a las peticiones de los usuarios

Seguridad - % de peticiones bloqueadas a los servidores

Accesibilidad - % de disponibilidad de los servidores

1.6.2. La seguridad y disponibilidad de los sistemas informáticos

Definición conceptual

La seguridad informática se basa en cerciorarse de que los recursos que posee el sistema de información de una entidad sean utilizados de la forma en que se planificó y que el acceso a dicha información, así como su cambio o actualización, solo pueda ser realizado por personal acreditado de la institución y siguiendo los límites establecidos.

La alta disponibilidad hace referencia a que las aplicaciones y datos posean la capacidad de estar operativos para los usuarios acreditados de manera ininterrumpida y en cualquier momento, debido a su naturaleza crítica para la entidad.

Definición operacional

La seguridad Informática tiene la función de brindar la evaluación de riesgos y amenazas, definir el plan de acción y adecuación para disminuir los riesgos, basándose en la normativa o el conjunto de buenas prácticas que les permitan asegurar la confidencialidad, integridad y disponibilidad de la manipulación de la información de activos a través de la:

1. Configuración Segura

2. Técnicas de Protección

3. Auditorias

Dimensiones e indicadores

Confidencialidad - % usuarios desconocidos accediendo a los servidores

Irrefutable - % de visitas a páginas web que no compete con el trabajo

Integridad - % de usuarios no autorizados que realizan cambios en el sistema

Disponibilidad - % de caídas de los servidores - % de tiempo de respuesta del servidor

1.7. Justificación e importancia

En la actualidad las grandes empresas buscan seleccionar la opción más adecuada en lo que respecta a tecnología, esto quiere decir, analizar y hacer uso de distintas soluciones tecnológicas o diferentes alternativas que permitan reducir y anticiparse a los posibles riesgos, que puedan comprometer los servicios ofrecidos por el hospital. Por lo que es importante buscar que los servicios informáticos posean las características de alta disponibilidad frente a las diversas situaciones que puedan acontecer, ya que la información dentro de una institución es el activo más importante.

El presente proyecto hace hincapié en el estudio y análisis de la infraestructura de red, en una institución de gran tamaño como el hospital, para conseguir una disminución en las caídas de los servicios por medio de la implementación de una infraestructura tecnológica, de alta disponibilidad y seguridad informática dirigida a los servidores, para que esta cuento con la capacidad de ofrecer alta disponibilidad y seguridad a los servicios que brinda el hospital de tal manera que se pueda reducir, lo máximo posible, el tiempo muerto (time out) denominado también como tiempo de inactividad de un servidor.

Con la implementación de la solución propuesta se busca que el hospital pueda asegurar que sus servicios funcionen de manera normal, reduciendo de gran manera el riesgo tecnológico, enfocándose en conseguir alta disponibilidad y seguridad de aquellos servicios que requieren de los servidores, en los cuales estos se encuentran alojados.

Por otro lado, este proyecto permite generar conocimiento confiable y valido en el ámbito de las tecnologías de información y comunicación, con una proyección a investigaciones e implementaciones futuras, brindando de esta manera también, ayuda a otras entidades con problemas similares, sirviendo como marco de referencia para intentar resolver sus problemas y mejorar de esta manera sus servicios informáticos.

1.8. Limitaciones

Las principales limitaciones encontradas en la presente investigación son:

- Disponibilidad de tiempo para las configuraciones correspondiente, ya que el HRHVM es una entidad de salud, los trabajadores hacen uso de los sistemas las 24 horas del día, lo cual tuvimos que aprovechar los días de poca actividad de los usuarios.

II. MARCO TEÓRICO

2.1. Revisión de estudios realizados

- **Bibliografía internacional**

  IMPLEMENTACIÓN DE UN CLÚSTER EXPERIMENTAL BAJO TECNOLOGÍAS LIBRES PARA PROPORCIONAR ALTA DISPONIBILIDAD DE SERVICIOS WEB HTTP (CARO, 2014)

  ¿Cómo proporcionar alta disponibilidad para los servicios desarrollados en los proyectos web de los cursos del programa de Ingeniería de Sistemas de la Universidad de Cartagena, sin incurrir en altas inversiones en tecnología y altos costos asociados?

  Concluye en:

  Por medio de la implementación de un clúster HA, se logró brindar una alta disponibilidad para los servicios que fueron desarrollados en los proyectos web de los cursos del programa de Ingeniería de Sistemas de la Universidad de Cartagena, sin la necesidad de incurrir en inversiones altas en tecnología y altos costos relacionados, dando respuesta a la pregunta de investigación planteada. Dicha implementación del clúster implicó: definición de tecnologías a utilizar, plantear y estudiar un diseño, realizar una instalación y configuración de servicios y aplicaciones, y por ultimó realizar pruebas de funcionamiento para posterior análisis de resultados exitosos, de recomendación y/o mejoras. Por lo tanto, se cumplieron a cabalidad todos los objetivos planteados como se puede verificar detalladamente en el capítulo de resultados y como se resume a continuación.

- **Bibliografía nacional**

  DISEÑO E IMPLEMENTACION DE UN SISTEMA INTEGRADO DE GESTION DE EQUIPOS DE SEGURIDAD (MEJIA, 2015)

El objetivo de esta investigación es implementar el piloto de una herramienta desarrollada en software libre, partiendo de un diseño funcional que facilite el logro de la gestión integrada de diversos dispositivos de seguridad de la información distribuidos en una red en producción. Para conseguir tal fin, el desarrollo de este documento se centra en el uso de Cacti como una herramienta de acceso libre desarrollada en el lenguaje de programación PHP, que nos facilita la generación y presentación de graficas por medio del estándar RRDTool, que, haciendo uso de una interfaz web, consigue la interacción con la información recogida de equipos de seguridad heterogéneos por medio del protocolo SNMP.

Concluye en:

Se integró el monitoreo de equipos de seguridad heterogéneos en la red. Se logró implementar el monitoreo de 1 clúster compuesto por 2 firewalls Check Point, 1 clúster de 2 firewalls Juniper, 1 sensor IPS McAfee, 1 proxy web Bluecoat, 1 proxy antivirus Bluecoat. Se demostró que se puede atender los principales requerimientos de gestión de equipos de seguridad heterogéneos en una red mediante el uso de tecnologías disponibles y de libre acceso, sin implicar mayores costos de licenciamiento o adquisición.

- **Bibliografía nacional**

  IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA MEJORAR EL ACCESO Y LA SEGURIDAD LÓGICA DE LA RED EN LA OFICINA DEPARTAMENTAL DE ESTADÍSTICA E INFORMÁTICA DE JUNÍN (RIVEROS PARAGUAY, 2019)

  Implementar las políticas de seguridad informática para mejorar el acceso y seguridad lógica de la red en la Oficina Departamental de Estadística e Informática de Junín mediante la metodología Top Down.

Concluye en:

La implementación de políticas de seguridad informática en la Oficina Departamental de Estadística e Informática de Junín mejoró la seguridad lógica en la red teniendo menor tráfico con un 99% de acceso al código de estado 200 y el 1% completo en el código de estado 400, control sobre los puertos y el tráfico mediante reglas y perfiles,

2.2. Leyes fundamentales, Principios, Definiciones y Conceptos fundamentales

2.2.1. Estándar TIA-942

El TIA-942 "Norma de infraestructura de telecomunicaciones para centros de datos" fue elaborado por el Subcomité de cableado de edificios comerciales TIA TR-42.1 y fue publicado en agosto de 2012. Dicho estándar, que se originó basándose en un conjunto de especificaciones para las comunicaciones y cableado estructurado, avanza y abarca los subsistemas de infraestructura, dando origen a los lineamientos que sirven de guía para clasificar esos subsistemas con base en los distintos grados de disponibilidad que se desea alcanzar.

Por otra parte, la norma TIA-942 recomienda como rango aceptable de temperatura entre 20 °C y 25 °C.

2.2.2. ISO 27001

Esta norma internacional fue emitida por la Organización Internacional de Normalización (ISO) y detalla la manera en la que se debe gestionar la seguridad de la información en una entidad. La primera revisión se publicó en 2005 y fue elaborada teniendo como base la norma británica BS 7799-2.27001. La última revisión de esta norma fue publicada en 2013 y lleva el nombre de ISO/IEC 27001:2013.

2.2.3. Redes informáticas

Las redes informáticas también son denominadas redes de comunicaciones de datos o redes de computadoras, estas pueden ser entendidas como el número de sistemas informáticos que se encuentran conectado entre sí a través de un conjunto de dispositivos alámbricos o inalámbricos, gracias a esta comunicación, es posible compartir información por paquetes de datos, que se trasladan a través de impulsos eléctricos, ondas electromagnéticas u otro medio físico.

Contrario a lo que se piensa, la lógica de intercambio de las redes informáticas no difiere de otros procesos de comunicación conocidos, este proceso posee un emisor, un receptor y un mensaje, un medio que permita transmitirlo y un grupo de códigos o protocolos que permitan garantizar que este sea comprendido. La diferencia radica que, en este caso, los que envían y reciben los mensajes vienen a ser los sistemas computacionales automatizados.

Cuando contamos con una red de computadoras, tenemos la posibilidad de crear un sistema de comunicación interna, compartir un punto de acceso a internet, poder administrar periféricos como (impresoras, escáneres, entre otros), así mismo, es posible enviar de manera veloz los datos y archivos sin tener que utilizar algún dispositivo de almacenamiento secundario. Todo esto se puede lograr gracias a un grupo de estándares de comunicación, que se encargar de “traducir” a un mismo lenguaje los procesos que se realizan en distintas computadoras (siendo el más común de estos el TCP/IP)

Tipos de redes según su alcance

Tabla 2: Tipos de Redes según su alcance

ALCANCE O EXTENSIÓN	DESCRIPCIÓN
PAN (Red de Área Personal)	Este tipo de red abarca el entorno de una persona. Por ejemplo, en la actualidad es usual tener el teléfono móvil conectado a algún otro dispositivo, como una Tablet o smartwatch. El radio que abarca dicha red no posee muchos metros y es común que, para este tipo de casos, se haga uso del protocolo bluetooth para poder conectar los distintos dispositivos de manera inalámbrica (WPAN)
LAN (Red de Área Local)	Este tipo de red abarca una sola ubicación física, por ejemplo, puede ser un edificio completo o una casa. Usualmente en este tipo de red se posee un solo router, que cumple la función de separar las redes públicas o internet y la red LAN, logrando que los dispositivos ajenos a nuestra red se encuentren fuera de esta, además, cuando se configura de manera inalámbrica se la conoce como WLAN.
CAN (Red de Área de Campus)	Es tipo de red de computadoras se encarga de cconectar redes de área local en un área geográfica limitada, como lo pueden ser un campus universitario o una base naval. Esta

	puede también ser considera como una especie de red de área metropolitana que utiliza de manera específica a un ambiente universitario. Debido a estas características, una CAN es más grande que una LAN, pero es de menor tamaño que una WAN. La conexión entre la infraestructura de una universidad se hace usando el mismo tipo de equipos y tecnología de redes que se emplearían en una LAN, además, los componentes (conmutadores, enrutadores, cables, entre otros) de este sistema de redes le pertenecen a una misma organización. En un can, los edificios de una universidad están conectados usando el mismo tipo de equipos y tecnología de redes que se usaría en un LAN. Además, todos los componentes, incluyendo conmutadores, enrutadores, cableado, y otros, le pertenecen a la misma organización.
MAN (Red de Área Metropolitana)	Este tipo de res es de alta velocidad y brinda cobertura a un área geográfica extensa, permite la capacidad de integración de diversos servicios por medio de la transmisión de datos, voz y video, haciendo uso de medios de

	transmisión como la fibra óptica y el par trenzado. Una alternativa ideal para la implementación de este tipo de redes son la tecnología de pares de cobre, que brindan una baja latencia, adecuada estabilidad y la carencia de interferencias por ondas de radio eléctricas.
WAN (Red de Área Amplia)	Este tipo de redes abarcan áreas geográficas muy extensas, además de requerís de grandes infraestructuras que les permitan intercomunicarse, por ejemplo, cables interoceánicos o satélites. Por este motivo, este tipo de redes utilizan medios públicos de interconexión y se recomienda definir una serie de medidas de seguridad que permitan encapsular los datos que se envíen por dichos medios (esto quiere decir, que se cómo enviar información por internet, la cual se encontrará, sin embargo, esta solo puede ser vista por el emisor y receptos).

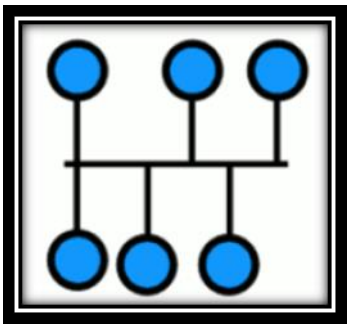
Fuente: Elaboración propia

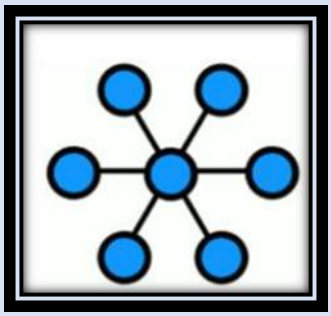
Topología de la red

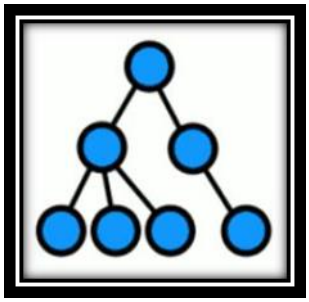
La topología de red es la manera en que se conectan las computadoras con el fin de intercambiar datos entre sí. Podría decirse que es como una familia de comunicación, que establece la manera en la que se diseñara la red tanto de manera física como lógica.

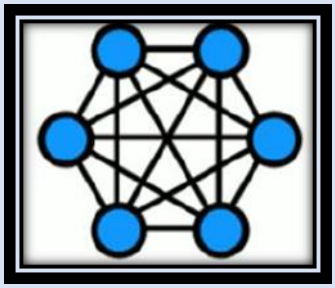
Dicho de otra manera, es la forma en la que se realizará el tendido del cableado que se encargará de conectar la computadora que forma parte de una red.

Tabla 3:Topología de Red

TOPOLOGIAS DE RED	DESCRIPCIÓN
PUNTO A PUNTO 	Esta topología es la más simple que existe, consta de un enlace permanente entre dos puntos finales (conocida también como point-to-point o PIP). Este tipo de topología es el modelo básico que se utiliza en la telefonía convencional. El valor que ofrece este tipo de red es la comunicación sin obstáculos entre los dos puntos finales definidos, además, su valor a demanda depende del número de pares posibles de abonados, expresado por la ley de Metcalfe.
TOPOLOGÍA EN BUS 	En este tipo de topología, todas las computadoras (nodos) se encuentran conectadas a un circuito común (bus). La información que se transfiere entre estos equipos viaja de manera directa o indirecta, siempre y cuando exista un controlador que enruta los datos al destino adecuado. La información se traslada por el

	cable en ambos sentidos, alcanzando aproximadamente una velocidad de 10/100 Mbps y ambos extremos poseen una resistencia (terminador). Es posible conectar un gran número de computadoras al bus, si una de ellas presenta alguna falla, la comunicación se mantiene, sin embargo, la comunicación se cae si el bus es el que falla.
TOPOLOGÍA ESTRELLA 	Este tipo de topología disminuye la posibilidad de fallo de red conectados todos los nodos que posee a un nodo central. Cuando se hace uso de esta tipología, el nodo central reenvía todas las transmisiones recibidas de cualquier uno de los nodos a todos los demás que lo componen, y en algunas ocasiones incluso al mismo nodo que lo envió. La comunicación entre todos los nodos es posible por medio de la transmisión o recepción del nodo central únicamente. De ocurrir un fallo en la línea de conexión de un nodo con el nodo central, ocasionaría el aislamiento de dicho nodo con

	respecto a sus pares, sin embargo, el resto del sistema estaría intacto.
TOPOLOGIA EN ARBOL 	Este tipo de topología también es denominada como topología jerárquica, esta puede ser entendida como una colección de redes de tipo estrella ordenadas jerárquicamente. Esta tipología consta de nodos periféricos individuales (hojas) que necesitan transmitir y recibir información únicamente de otro nodo y no necesitan cumplir la función de repetidores o regeneradores. A diferencia de las redes de tipo estrella, el rol que cumple el nodo central puede ser distribuido. Una característica que comparten con las redes de tipo estrella convencionales son que los nodos individuales podrían ser aislados de la red siempre y cuando se produzca un fallo puntual en la ruta de conexión de dicho nodo. Si ocurren fallas en un enlace que permite la conexión con un nodo hoja, dicho nodo queda asilado; por otro lado, si la falla se presenta en un enlace con

	un nodo que no sea hoja, toda esa sección se quedará asilada del resto.
TOPOLOGIA EN MALLA 	En este tipo de topología cada uno de los nodos se encuentra conectado con todos los demás. Debido a esta característica, es posible transmitir los mensajes de un nodo a otros por diferentes caminos. Si la red de malla esta adecuadamente conectada, la existencia de interrupciones en las comunicaciones es absolutamente imposible. Cada uno de estos nodos tiene sus propias conexiones con todas las demás. Este tipo de topología es auto ruteable. Además, indicar que, una red puede seguir funcionando incluso si uno de los nodos desaparece o la conexión presenta una falla, esto debido a que los demás nodos evitan el paso por ese punto. Considerando todo esto, la topología en malla, se convierte en una alternativa de red muy confiable.

Fuente: Elaboración propia

Arquitectura de red

La conexión entre equipos informáticos es posible por medio de los protocolos de comunicaciones. Un protocolo de comunicaciones consta de una serie de reglas perfectamente organizadas y aceptadas por mutuo acuerdo entre los involucrados en una comunicación, su finalidad es hacer posible el intercambio de información entre los dispositivos, ubicando los posibles fallos y errores que se puedan producir. El conjunto de protocolos que permiten que la comunicación entre dispositivos se haga de manera fácil es denominada la arquitectura de la red.

Existen un gran número de protocolos que contribuyeron con soluciones distintas a los problemas de red: Netbeui, AppleTalk, TCP/IP, etc. Entre estas destaca en la actualidad TCP/IP, que está por encima los otros convirtiéndose en el estándar de facto en todos los tipos de redes. Incluso hoy en día, los protocolos propietarios hacen uso de interfaces de TCP/IP

Arquitectura TCP/IP

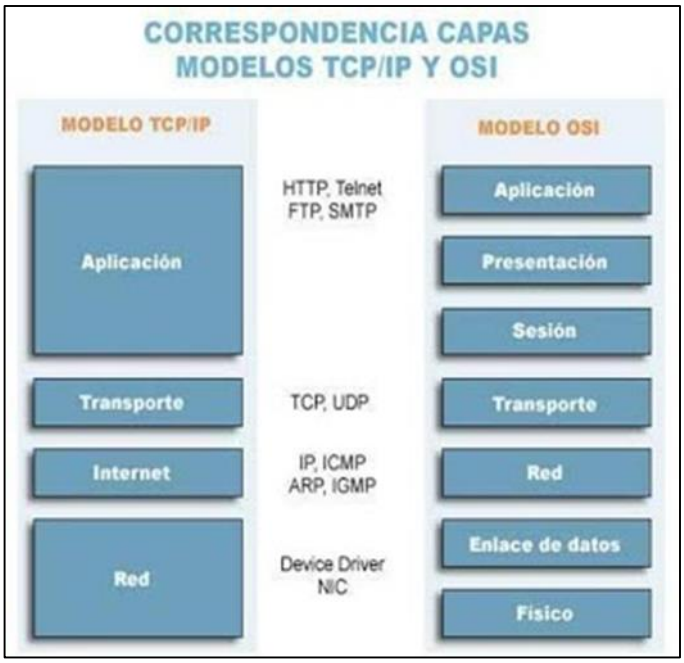
- **Funcionamiento de la Arquitectura TCP/IP**

  Consta de niveles superiores (capas de aplicación y transporte) que se implementan únicamente en los equipos finales (emisor y recepto), siendo los encargados de entregar a los niveles inferiores los bloques de datos y verificar que estos han llegado a su destino. Por otro lado, los niveles inferiores (capa de internet y acceso a red) son implementados a todas las computadoras y dispositivos de encaminamiento. Ambos niveles son los responsables de retransmitir datos que van de un ordenador a otro por medio de todos los dispositivos de encaminamiento necesarios.

  Para que dicha comunicación sea posible, cada ordenador que forme parte de la red debe tener una única dirección IP, lo que

permitirá identificar ese equipo. Todo proceso o aplicación que se desarrolla dentro de un ordenador en red debe poseer una dirección única dentro del mismo, con el objetivo de que los protocolos del nivel de transporte puedan hacer entrega de los datos a la aplicación adecuada. Son estas direcciones los denominados puertos.

Ilustración 1:Puertos en los modelos OSI Y TCP/IP



Fuente: (sites.google)

- **Proceso de encapsulamiento de datos**

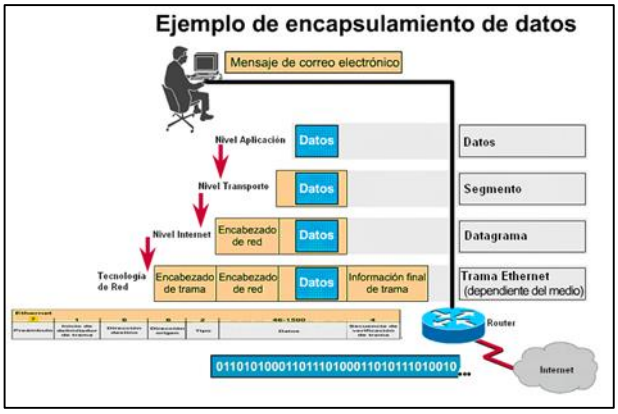
Cuando una aplicación envía información desde un ordenador a otro, los datos se encapsulan o integran unos dentro de otros. Proceso de encapsulamiento:

1. A los datos iniciales provenientes de una aplicación se les añade una cabecera de datos para el transporte (cabecera TCP). Este conjunto de datos recibe el nombre de segmento.

2. Al segmento anterior se le añade una cabecera de datos para su identificación por Internet (cabecera IP). Este conjunto de datos recibe el nombre de datagrama.

3. El datagrama anterior se integra dentro de una trama Ethernet.

Ilustración 2:Encapsulamiento de datos



Fuente: (sites.google)

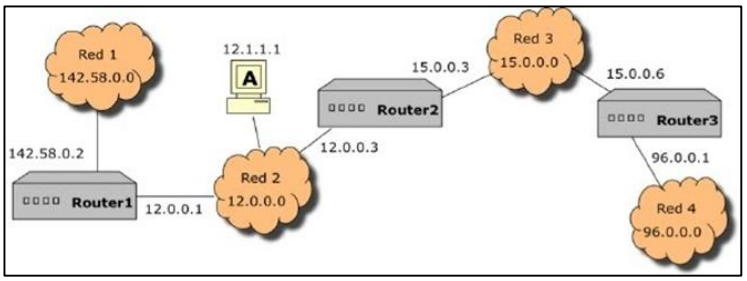
- **Encaminamiento IP**

Empezando con la dirección IP del destino de un paquete, todo dispositivo de la red (equipo o encaminador) debe definir el lugar hacia donde será encaminado. En el caso de que la dirección de la red destino sea la misma que la dirección de red actual (encaminamiento hacia un dipositivo que se encuentra en la propia red local o entrega inmediata), este paquete se trasladará a nivel de enlace de datos haciendo uso del protocolo ARP para poder traducir la dirección IP a dirección física. Por otro lado, cuando el destino se ubica en una red diferente, el paquete se direccionará por medio de la puerta de enlace (pasarela o gateway), para que pueda salir de la red loca. La puerta de enlace que se encarga de recibir los datos que se envían a otra red, se encargará de definir el encaminamiento que llevará a cabo, es decir, elige el próximo nodo que seguirán los datos teniendo en cuenta la dirección IP del destino y en una tabla interna que contiene la información del encaminamiento.

Al momento de definir la red a la que pertenece el destino del mensaje surgen dos posibilidades. En el primer caso, se

puede hacer uso de la máscara por defecto de la clase de la que forma parte la dirección de equipo destino; en el segundo, se podría hacer uso de una máscara diferente a la máscara de la clase. Considerando el tipo de opción que se elija, el encaminamiento será classfull (con clase) o classless (sin clase); en el primero no se admite el uso de máscaras diferentes a las de la propia clase, mientras que, en el otro, el uso de máscaras diferentes es posible.

Ilustración 3:Enrutamiento



Fuente: (sites.google)

- **Comandos y Utilidades de TCP/IP (sites.google)**

  - **HOSTNAME**

    Permite mostrar el nombre del equipo actual (host).

    C:\>hostname

    inf-unh21-profe

  - **PING**

    Este comando de utilidad de diagnóstico permite rastrear los paquetes de una red i verifica el estado de conexiones establecidas entre uno o varios hosts remotos. Algunas de las tareas que realiza son:

    - Verifica las conexiones de uno o varios equipos remotos; para conseguir eso, realiza el envío de paquetes de eco ICMP al equipo y recibe paquetes de respuesta eco.

- Posee un tiempo de espera máximo de un segundo por cada paquete enviado.
- Muestra la cantidad de paquetes transmitidos y recibidos.

- **ARP**

Permite mostrar y modificar las tablas de traducción de direcciones lógicas a dirección físicas, haciendo uso del protocolo de resolución de direcciones ARP (Address Resolution Protocol)

arp -a [dir_inet]

A través de este comando se muestran las entradas actuales en la tabla ARP por medio de una consulta de TCO/IP. Si se indica dir_inet, solamente se mostrarían las direcciones IP y físicas del equipo especificado.

- **IPCONFIG**

Este comando nos permite mostrar todos los valores actuales que posee la configuración de red TCP/IP. Es bastante útil especialmente en sistemas que hacen uso de DHCP, ya que facilita a los usuarios a determinar cuáles son los valores de configuración de TCP/P ha definido DHCP. El comando se escribe de la siguiente manera:

ipconfig [opciones]

Por medio del parámetro /all podemos ver una presentación completa. Sin este parámetro, el comando solo nos mostrará los valores de dirección IP, la máscara de subred y la puerta de enlace o gateway predefinida para cada tarjeta de red.

C:\>ipconfig /all

- **TRACERT**

Este comando traza la ruta seguida por los paquetes TCP/IP desde este equipo hasta otro equipo remoto. Él comando tracert hace uso de la petición de eco ICM y mensajes de respuesta (de manera similar al comando ping) para producir informes de líneas de comando acerca de cada encaminador o router que se cruza y del tiempo de ida y vuelta (RTT) de cada salto.

- **NETSTAT**

Este comando nos permite mostrar estadísticas del protocolo y el estado actual de las conexiones de la red TCP/IP. El formato es

netstat [-a] [-e] [-n] [-s] [-p protocolo] [-r]

Parámetros:

-a: Permite mostrar todas las conexiones y puertos de escucha. Usualmente no se visualizan las conexiones de servidor.

-e: Permite mostrar estadísticas relacionadas a Ethernet. Puede utilizarse en conjunto con la opción –s.

-n: Permite mostrar las direcciones y los números de cada puerto en formato numérico (para nos buscar nombres).

-s: Permite mostrar estadísticas de cada uno de los protocolos. De manera predefinida, se muestran las estadísticas referidas a TCP, UDP. ICMP e IP. Con la opción –p podemos especificar un subconjunto de los valores predefinidos.

-p protocolo: Permite mostrar conexiones correspondientes al protocolo que se ha especificado por medio de protocolo; este protocolo puede ser TCP o UDP. Si se combina con opción –s, se pueden ver las estadísticas de cada uno de los protocolos (que pueden ser TCP, UDP, ICMP o IP).

-r: Permite mostrar lo que contiene la tabla de enrutamiento. Es equivalente a route prunt:

C:\>netstat -s -p tcp

- **NSLOOKUP**

Por medio de esta herramienta de diagnóstico, podemos mostrar información de los servidores de nombres del Sistema de Nombres de Dominio, mejor conocido como DNS (Domain Name System).

Modo no interactivo: Si se necesita buscar sólo un dato, se suele utilizar el modo no interactivo. Para esto necesitamos argumentos adicionales para el comando, en el primero se escribe el nombre o la dirección del equipo que vamos a localizar. Para el segundo argumento, se escribe el nombre o la dirección IP de alguno de los servidores de nombres DNS. Si no colocamos el segundo argumento, se hará uso del servidor de nombres DNS predefinido.

C:\>nslookup www.elpais.es 212.166.64.2

Servidor: dns2.tiscalinet.es

Address: 212.166.64.2

Respuesta no autoritativa:

Nombre: www.elpais.es

Address: 212.80.177.133

Modo interactivo: Si se necesita buscar más de un dato, se puede utilizar el modo interactivo. Para hacer uso de este modo se escribe un guion (-) como primer argumento y el nombre o la dirección IP de uno de los servidores de nombres DNS para el segundo argumento. En caso de que se omitan ambos argumentos, se hará uso del servidor de nombres DNS predefinido.

Se escribe un guion (-) para el primer argumento y el nombre o la dirección IP de un servidor de nombres DNS para el segundo argumento. O bien, se omiten ambos argumentos y se utilizará el servidor de nombres DNS predeterminado.

C:\>nslookup

Servidor predeterminado: dns1.tiscalinet.es

address: 212.166.64.1

> www.google.com

Servidor: dns1.tiscalinet.es

Address: 212.166.64.1

Respuesta no autoritativa:

Nombre: www.google.com

Address: 216.239.39.101

- **ROUTE**

Nos permite controlar las tablas de enrutamiento de la red. La sintaxis es la siguiente:

route [-p] comando [destino]

Parámetros:

-p: Cuando lo utilizamos en conjunto con el comando add, establece una ruta de forma permanente para todos los

inicios del sistema. De manera predefinida, las rutas no se conservan al reiniciar el sistema. Cuando lo utilizamos con el comando print, se muestra una lista de rutas persistentes registradas. Este se omite con todos los demás comandos, que siempre hacen uso de las rutas permanentes adecuadas. Comandos disponibles:

- print: Imprime un camino
- add: Agrega un camino
- delete: Elimina un camino
- change: Modifica el camino existente

2.2.4. Infraestructura IT

Viene a ser el conjunto de dispositivos y aplicaciones que son necesarios para una empresa. Este sistema se gestiona por medio de la monitorización a través del despliegue de equipos suficientes, máquinas y software dirigidos al cliente.

Servidores

Desde el punto de vista de la informática, este término posee dos significados. El primer se refiere al ordenador que coloca recursos a disposición por medio de una red, el segundo hace referencia al programa que trabaja en dicho ordenador. Teniendo esto en consideración, nacen dos defunciones de servidor:

- Servidor (Hardware): Un servidor que se basa en hardware viene a ser una maquina física integrada en una red informática, en donde, aparte del sistema operativo, funcionan uno o varios servidores que se basan en software.
- Servidor (Software): Un servidor que se basa en software viene a ser un programa que brinda un servicio especial que otros programas (denominados clientes). Pueden utilizar a

nivel local o por medio de una red. El tipo de servicio dependerá del tipo de software que posee el servidor.

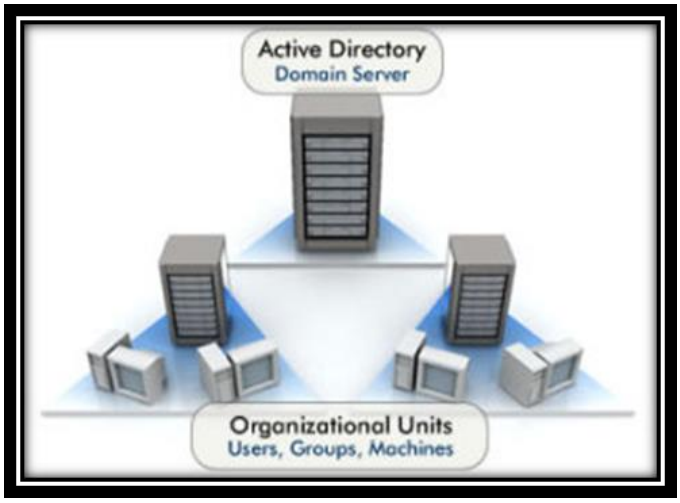
Tipos de servidores

La comunicación que se da entre cliente y servidor responde a cada servicio y se determin a través de un protocolo de trasmisión. Según (Digital Guide IONOS, 2018) para entender este principio, se deben entender los siguientes aspectos.

- **Servidor ADDS (Active Directory)**

  Es un término utilizado por Microsoft para hacer referencia a la implementación de su servicio de directorio en una red de computadoras. Hace uso de diversos protocolos, teniendo como principales LDAP, DNS, DHCP y Kerberos. En palabras más sencillas, podemos decir que es un servicio que se estableció en uno o varios servidores en donde hacen objetos tales como usuarios, equipos o grupos, con la finalidad de poder administrar el inicio de sesión de todos los equipos conectado a la red, así como la administración de políticas dentro de la misma.

Ilustración 4:Servidor Active Directory

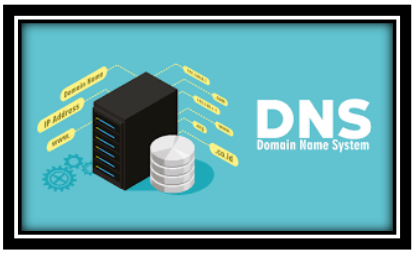


Fuente: (Multicomp S.A. de C.V., 2020)

- **Servidor DNS**

Este tipo de servidores nos permite la resolución de nombres en una red. El rol que cumplen este tipo de servidores es de crucial importancia para la red informática mundial (WWW), debido a que se encargar de traducir los nombres de host como www.ejemplo.com en la correspondiente dirección IP.

Ilustración 5:Servidor DNS

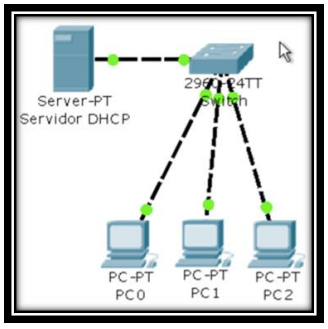


Fuente: (Fernandez, 2020)

- **Servidor DHCP**

Por medio de este protocolo un equipo que se encuentra conectado a una red puede obtener su configuración IP de manera dinámica. Para esto, solo se tiene que especificar al equipo, por medio DHCP, que busque una dirección IP de forma automática, realizando el envío de un mensaje broadcast a la red local en la que este se encuentre. Lo que se busca principalmente es simplificar el trabajo de administración de la red, algo bastante conveniente para redes grandes que abarcan n cantidad de host.

Ilustración 6: Servidor DHCP



Fuente: (David, 2011)

- **Servidor de archivos**

Los servidores de archivos son los responsables de almacenar los datos a los que los clientes acceden por medio de una red. Las entidades eligen esta opción para que aumentar el número de grupos de trabajo que accedan a los mismos datos. Un servidor de archivos impide los conflictos que se originan por las diferentes versiones de archivos locales y posibilita tanto la creación automática de las diversas versiones de datos como la posibilidad de realizar copias de seguridad central de la totalidad de datos de la entidad.

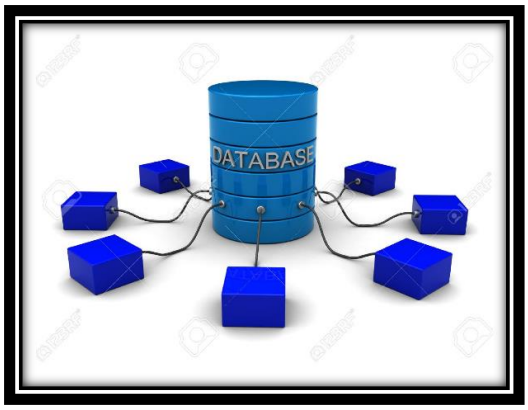
Ilustración 7:Servidor de Archivos

Fuente: (Tema Fantástico, S.A.., 2010)

- **Servidor de base de datos**

Al hablar de un servidor de base de datos nos referimos a un programa informático que brinda la posibilidad de que otros programas puedan tener acceso a uno o varios sistemas de bases de datos por medio de una red. Algunas de estas soluciones, que actualmente poseen una gran cuota del mercado de base de datos son Oracle, MySQL, Microsoft SQL Server, PostgreSQL y DB2. Este tipo de servidores brindan ayuda a los servidores web, por norma general, al momento de almacenar y entregar datos.

Ilustración 8:Servidor de Base de Datos



Fuente: (Azizi, s.f.)

- **Servidor Web**

La función principal que tiene un servidor web es la de almacenar y organizar páginas web y entregarlas a clientes (los que solicitan) como navegadores web o crawlers. La comunicación que se da entre el servidor (software) y el cliente se realiza por medio del HTTP, es decir, protocolo de transferencia de hipertexto o HTTPS, que es una variante codificada. Por lo general, se transfieren documento HTML y los elementos que lo integran, como lo son las imágenes, hojas de estilo o scripts.

Entre los servidores web que gozan de mayor popularidad encontramos al servidor HTTP Apache, los servicios de Internet Information Server de Microsoft (ISS) o el servidor Nginx.

Ilustración 9: Servidor Web

Fuente: (Raffino, 2020)

- **Servidor de correo electrónico**

Este tipo de servidores se compone por varios módulos de software que interactúan entre sí para hacer posible la recepción, envío y reenvío de los correos electrónicos, así como su disponibilidad al momento de ser consultados. Por lo general, trabajan por medio del protocolo de transferencia simple de correo (SMTP). Para que un usuario pueda acceder a un servidor de correo electrónico necesita de un cliente de correo electrónico, que se encargue de recoger los mensajes del servidor y haga la entrega de estos en la bandeja de entrada, todo este proceso se da por medio de los protocolos IMAP (Internet Message Access Protocol) o POP (Post Office Protocol).

Ilustración 10:Servidor Correo Electrónico

Fuente: (AprendiendoPC, s.f.)

Almacenamiento

- **SAN (Red de área de almacenamiento)**

Son un tipo de red dedicada de alta velocidad que ofrece acceso al almacenamiento a nivel de bloque. Las SAN se comenzaron a utilizar con el fin de mejorar la disponibilidad y el rendimiento de las aplicaciones al momento de segregar el tráfico de almacenamiento de las demás que conforman la LAN.

Las entidades que hacen uso de las SAN pueden asignar y administrar de manera sencilla los recursos de almacenamiento, consiguiendo de esta manera una mayor eficiencia. “En lugar de poseer capacidades de almacenamiento asiladas en distintos servidores, es posible compartir una serie de capacidades entre varias cargas de trabajo distintas y separarlas de acuerdo a la necesidad. Esto lo hace más fácil de proteger y de administrar” dice Scott Sinclair, analista senior de Enterprise Strategy Group. (Bednarz, 2018)

- **NAS**

Cuando hablamos de un sistema NAS nos referimos a un dispositivo de almacenamiento que se encuentra conectado a una red, que nos permite almacenar y recuperar los datos en un punto central solamente para usuarios autorizados de la red y multiplicidad de clientes. Este tipo de dispostivios se caracterizan por ser flexibles y expansibles, lo que significa que, conforme se necesite una mayor capacidad de almacenamiento, esta podrá ser añadida a lo que ya se posee. Un dispositivo NAS es muy parecido a contar con una nube privada en la oficina. Son más veloces, menos costos y ofrecen todas las facilidades de una nube pública dentro de los predios, lo que permite que se posea todo el control de la misma.

Este tipo de sistemas son perfectos para empresas pequeñas y medianas que son fáciles de operar, ya que usualmente no es necesaria la presencia de un especialista de informática, lo que reduce los costos de operación. Las copias de seguridad se ejecutan de manera sencilla, haciendo que estas sean accesibles cuando sean requeridas, también son excelentes para centralizar el almacenamiento de datos de manera segura y fiable. Cuando se trabaja con un sistema NAS, los

> datos se encuentran siempre accesible, faciltiando de esta manera la colaboración de los empleados, del mismo modo, permite responder a los clientes de forma oportuna y seguir de manera inmedita las situaciones de venta u otros aspectos, debido a que toda la información se encuentra en un solo lugar. Como estos dispositivos se asemejan a una nube privada, es posible acceder a los datos a distancia haciendo uso de una conexión de red; permitiendo de esta manera que los empleados trabajen desde cualquier parte del mundo y en todo momento. (SEAGATE, s.f.)

Datacenter

Un Datacenter o un centro de datos viene a ser una construcción en donde se almacenan los equipos electrónicos necesarios para que se pueda mantener una red de computadoras, es decir, cuenta con una infraestructura que posee la energía apropiada, una ventilación ideal y un adecuado sistema de seguridad. Este sistema trabajo bajo la modalidad de hosting, esto significa, que presta alojamiento web a entidades de mayor tamaño, asegurándose de resguardar y recopilar su información digital.

¿Cómo se clasifica?

Según (SOTO, 2015), los Datacenter cuentan con una clasificación denominada ANSI/TIA 942, que fue elaborada en abril de 2005 por las American National Standars Institute, tiene como finalidad certificar la disponibilidad que poseen los componentes que cuentan con estas especificaciones. Se encargan de ver, por ejemplo, el tamaño, los niveles de redundancia, la capacidad y tiempos de respuestas, entre otras variables. Lo anterior mencionado se puede medir en cuatro niveles, los cuales fueron denominados TIER y cuanto mayor sean estos, brindan una mayor confiabilidad.

- **TIER 1:** La creación de esta clase de Datacenter está dirigida para pequeñas y medianas empresas. Dentro de esta clasificación, el servicio puede mostrar interrupciones, debido a que no cuenta con un sistema de refrigeración ni de distribución eléctrica. Se estima que el tiempo para su implementación son alrededor de tres meses y para realizar trabajos de mantenimiento será necesario interrumpir el servicio, por último, poseen una disponibilidad del servicio de un 99.67%.

- **TIER 2:** Este tipo de Datacenter corresponde a uno redundante, lo que significa que, son menos propensos a interrupciones (planificadas o no), poseen una única línea de conexión de refrigeración y distribución eléctrica. Se estima que el tiempo para su implementación varía entre 3 a 6 meses y posee suelos elevados, generadores auxiliares o UPS. De llevarse a cabo labores de mantenimiento, el servicio aún debe interrumpirse, por último, poseen una disponibilidad del servicio de 99.74%.

- **TIER 3:** Este tipo de Datacenter, usualmente brindan servicios 24/7 y se encuentran conectadas a diversas líneas de distribución eléctrica y de refrigeración, aunque solamente cuentan con una activa. De llevarse a cabo labores de mantenimiento, no es necesario interrumpir el servicio, debido a que su capacidad es ideal para ofrecer el servicio por otras líneas.

- **TIER 4:** Este tipo de Datacenter, está dirigido a entidades de carácter internacional, como los bancos y multinacionales. Posee tolerancia a fallas, debido a que permite múltiples líneas de distribución de electricidad y refrigeración. Las labores de mantenimiento se pueden realizar sin verse afectado el servicio, además, puede hacer frente a eventos o planificados.

SAI (Sistema de Alimentación Ininterrumpida)

Conocidos también como UPS (Uninterruptable Power Supply), son artefactos que cuentan con la capacidad (por medio de baterías) de asegurar que los dispositivos que se encuentren conectados a él, reciban energía de manera continua para responder de manera adecuada a problemas de sobretensión de la red o cortes intempestivos.

Este tipo de dispositivos evitan daños mayores, porque la pérdida de electricidad de manera repetida puede provocar daños a los equipos, perdida de información o trabajos que se están realizando. Este tipo de sistemas son recomendados especialmente para equipos de sobremesa y portátiles que no posean baterías.

Ilustración 11: SAIs

Fuente: (Talius Technology S.L. , Cl. Atenas, 2019)

TIPOS DE SAIs

- **SAI Offline**

  Esta clase de SAI proporciona protección para tres anomalías: fallos, subidas y bajadas de tensión. Este tipo es bastante uil para ser usado en casa por sus usos domésticos: SAIs para PC, equipos de música, videoconsolas, electrodomésticos, monitores, etc.

- **SAI Inline**

  Esta clase de SAI proporciona protección a cinco de las anomalías eléctricas. Adicional a las tres mencionadas anteriormente, ofrece protección frente a tensiones bajas o altas que ocurren de forma continua. Es recomendable para la protección de dispositivos en hogares que presentan tensiones anómalas, negocios pequeños o empresas, ordenadores, cámaras de seguridad, router, switches, etc.

- **SAI Online.**

  Esta clase de SAI proporciona la máxima protección. Uno de los inconvenientes se presenta en las baterías, que se cambian con mayor frecuencia y poseen un precio mayor. Su uso es común en empresas que tienen que proteger cosas muy valiosas, como servidores, computadoras de monitorización, videograbadoras, cámaras de seguridad, etc. (Talius Technology S.L. , Cl. Atenas, 2019)

2.2.5. Virtualización

La virtualización consiste en la creación de una representación basada en software, o de manera virtual, de un ente físico como lo son, por ejemplo, las aplicaciones, servidores, redes y almacenamiento virtual. Es una opción bastante eficaz para disminuir los gastos de TI, y al mismo tiempo, permite mejorar la eficiencia y agilidad para todo tipo de empresas sin importar el tamaño.

Ventajas de la virtualización

Según (VMware, 2020), la virtualización permite la mejora de la agilidad, flexibilidad y la escalabilidad en la infraestructura de TI, al mismo tiempo que, brinda la posibilidad de conseguir ahorros significativos. Algunas de las ventajas que ofrece, como lo son la mayor movilidad de las cargas de trabajo, una mejora en el

rendimiento y en la disponibilidad de los recursos o la automatización de operaciones, permiten simplificar las labores de gestión de la infraestructura de TI, además permiten la reducción de los costes de propiedad y operativos. Otras de las ventajas que ofrecen son:

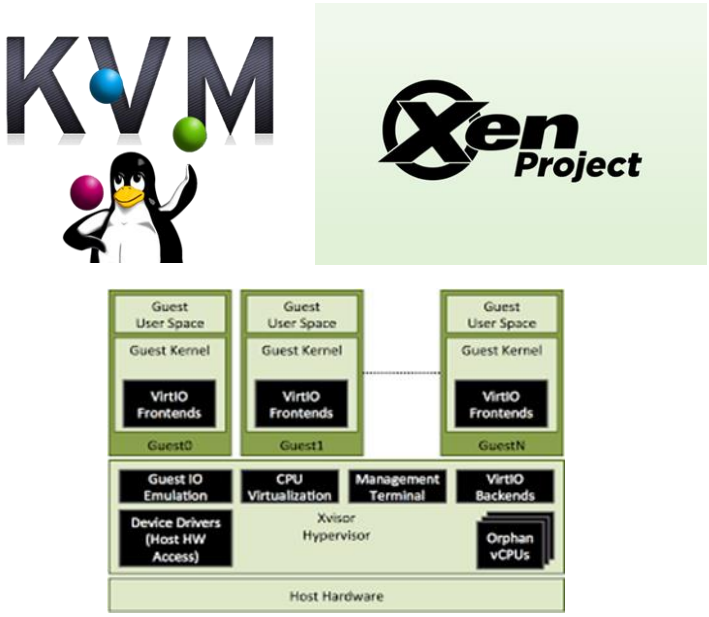
- Reducir la inversión en capital y los gastos operativos.
- Reducir o eliminar los tiempos de inactividad.
- Aumentar la productividad, la eficiencia, la agilidad y la mejora de la capacidad de respuesta del área de TI.
- Distribuir de manera más rápida las aplicaciones y recursos.
- Mejorar la continuidad del negocio, así como la capacidad de recuperarse frente a cualquier desastre que puede ocurrir.
- Gestionar de manera simplificada del centro de datos.
- Permitir la disponibilidad de un auténtico centro de datos basado en software.

Tipos de Hipervisores

- **Hipervisor de tipo I**

  El hipervisor tipo 1 es el más básico pero importante, así como el más utilizado. El hipervisor tipo 1 virtualiza directamente los recursos de hardware. Por ejemplo, el procesador, la memoria, el almacenamiento y la capa de red se pueden virtualizar. El hipervisor de tipo 1 también se conoce como el "hipervisor de metal desnudo" porque no requiere un sistema operativo.

Ilustración 12:Hipervisores

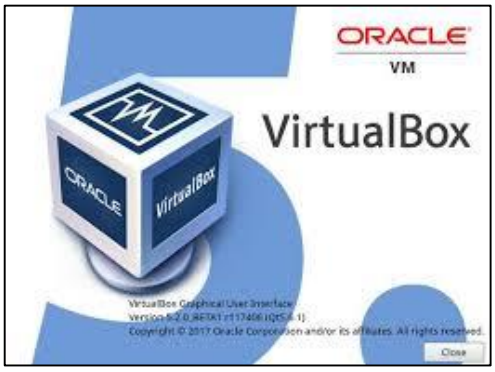


Fuente: (Total Publishing Network S.A., 2008)

- **Hipervisor tipo II**

El hipervisor tipo II administra los recursos de hardware indirectamente a través de un sistema operativo. Esto se logra virtualizando las instancias como procesos de software. El beneficio del Tipo II es que el hipervisor puede ejecutarse sin una implementación y administración demasiado compleja en comparación con el Hipervisor Tipo I. Sin embargo, la desventaja es que el hipervisor Tipo II está limitado a ejecutar una virtualización dinámica altamente escalable debido a la alta sobrecarga.

Ilustración 13:Hipervisores de tipo 2



Fuente: (UDS Enterprise Team, 2018)

Tipos de Virtualización

Virtualización de servidores

La virtualización de servidores nos da la capacidad de ejecutar múltiples sistemas operativos en un único servidor físico a través de máquinas virtuales que brindan un buen rendimiento. Dentro de las principales ventajas encontramos las siguientes:

- Mejora la eficiencia en el ambiente de TI.
- Reduce los costos operativos.
- Permite que la implementación de las cargas de trabajo se realice de manera más rápida.
- Mejora el rendimiento de las aplicaciones.
- Permite que la disponibilidad del servidor sea mayor.
- Facilita la eliminación de la complejidad y la propagación de los servidores.

Virtualización de red

Al replicar una red física de manera completa, la virtualización de red nos permite realiza la ejecución de aplicación en una red virtual de la misma manera que en una red física, pero con mayores ventajas en la parte operativa y contando con la independencia completa del hardware que brinda la virtualización. La virtualización de red tiene la capacidad de mostrar los dispositivos y servicios de red lógicos (puertos, conmutadores, VPN, firewall, entre otros) a las cargas de trabajo que están vinculadas.

Virtualización de escritorios

Al implementar los escritorios como un servicio gestionado las organizaciones de TI tienen la capacidad de responder más rápido a las necesidades tan cambiantes del entorno laboral y aprovechar las nuevas oportunidades que se presenten. Los escritorios y las aplicaciones virtualizadas también tienen la capacidad de ser distribuidas de manera rápida y sencilla a sucursales, trabajadores subcontratados o en que se encuentran en un país distinto, así como a trabajadores móviles que hacen uso de tabletas.

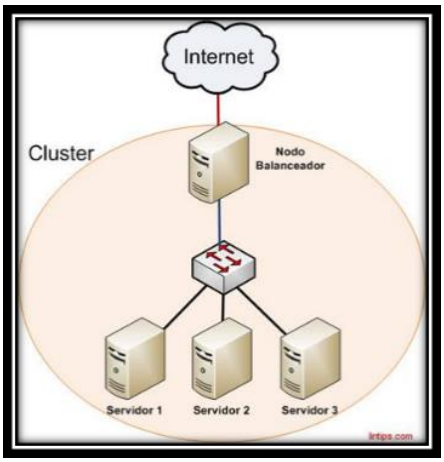
2.2.6. Clúster

Este tipo de sistemas consiste en la agrupación de distintos servidores que trabajan como si fuesen uno solo, un clúster es un conjunto de múltiples ordenadores que se encuentran unidos por una red de alta velocidad, de tal manera que este grupo es visto como un solo ordenador. Los clústeres pueden presentan combinaciones de los siguientes servicios

1. Alto rendimiento.
2. Alta disponibilidad.
3. Equilibrio en la carga.
4. Escalabilidad.

Algo que caracteriza el funcionamiento de un clúster, es que no necesitan que todas las maquinas que la conforman posean el mismo hardware y sistema operativo (clúster heterogéneo). Además, este tipo de sistema debe contar con una interfaz de manejo de clústeres, que tendrá la función de interactuar con el usuario y los proceso, distribuyendo la carga entre cada uno de los servidores.

Ilustración 14:Estructura de un Clúster



Fuente: (Pinterest, s.f.)

Clasificación del clúster

La clasificación de los clústeres se puede dar en función de diversos conceptos, siendo estos los relacionados a los servicios mencionados en los párrafos anteriores.

- **Clúster de alto rendimiento (HC o High Performance Clúster)**

  En este tipo de clúster se llevan a cabo las tareas que necesiten de una gran capacidad de cálculo o que requieran el uso de cantidades grandes de memoria. Este tipo de tareas, requiere que los recursos del clúster sean utilizados de manera exclusiva durante periodos de tiempo que usualmente son de larga duración.

- **Clúster de alta disponibilidad (HA o High Availability)**

  En este tipo de clúster lo que se pretende es proporcionar de disponibilidad y confiabilidad a los servicios ofrecidos. Para cumplir con este objetivo, se hace uso de hardware duplicado, de tal manera que al no contar con un único punto de fallos (de ocurrir algún fallo en uno de los componentes siempre existirá otro que pueda sustituirlo en su función), la disponibilidad del sistema está garantizada. Por otra parte, se añaden software

que permiten la detección y recuperación frente a fallos, con la finalidad de aumentar la confiabilidad del sistema para su uso.

- **Clúster de alta eficiencia (HT o High Throughput)**

  Este tipo de clúster tiene como finalidad brindar un entorno en donde sea posible la ejecución del mayor número de tareas en el menor tiempo posible. Las tareas a las que hacemos referencia, son individuales y no poseen dependencia entre ellas.

Clúster de Alta Disponibilidad

Conocida por sus siglas en ingles HA, la alta disponibilidad se considera un protocolo, su aplicación se da cuando tomamos la decisión de contar con un plan de contingencia para cualquiera de nuestros componentes que tengan alguna situación anómala, con el fin de poder seguir brindando el servicio del mismo. En este tipo de sistemas se tiene que contar con la capacidad de detectar fallos en el componente principal de la forma más eficaz y rápida posible, y al mismo tiempo, este de ser capaz de recuperarse del problema de manera eficiente y efectiva, haciendo uso de los componentes secundarios para que estos ofrezcan el mismo servicio y así la disponibilidad no sea afectada o lo haga durante el menor tiempo posible.

CONFIGURACION DE UN SISTEMA HA

En los sistemas HA, la configuración se conforma de dos componentes: el principal (que brinda el servicio de manera continua) y el secundario (que es un clon del principal utilizado para brindar el mismo servicio).

Ilustración 15:Ejemplo de Alta disponibilidad

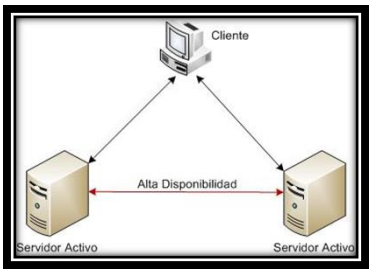
Fuente: (IMF Business School, s.f.)

- **Configuración Activo/Activo**

  En este tipo de configuración, todos los servidores que forman parte del clúster pueden hacer uso de los mismos recursos de manera simultánea. Esto quiere decir que, estos servidores cuentan con los mismos recursos y tienen acceso a estos de manera independiente. Si uno de los nodos del sistema presenta una falla o pasa a no estar disponible, los recursos con los que cuenta sigue siendo accesibles por medio de los otros servidores del clúster.

  Una de las principales ventajas de este tipo de configuración, es que los servidores dentro del clúster son más eficientes debido a que pueden realizar el trabajo de manera simultánea. Sin embargo, cuando uno de estos deja de ser accesible, la carga de sus operaciones de trabajo se transfiere a los nodos restantes, ocasionando de esta manera una degradación de manera global al servicio ofrecido a los usuarios.

Ilustración 16:HA activo/activo

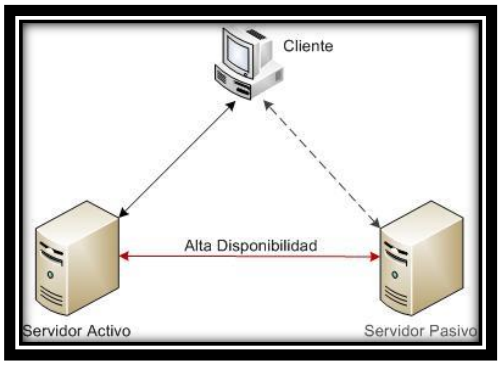


Fuente: (ECURED, s.f.)

- **Configuración Activo/Pasivo**

En este tipo de configuración, un servidor que tiene los recursos del clúster, mientras que los otros servidores que tienen la capacidad de utilizar estos recursos no lo pueden activar hasta que el usuario que esté haciendo uso de estos recursos no se encuentre disponible. Algunas de las ventajas que ofrece es que no existe la degradación de servicio, además que los servicios solamente se iniciando cuando el servidor activo no pueda responder. Por otro lado, algunas de las desventajas que se presentan es que los servidores pasivos no ofrecen ningún tipo de recurso mientras se encuentran en estado de espera, ocasionando que este tipo de configuración sea menos eficiente que la del tipo activo/activo. Otra desventaja que se presenta, es que los sistemas demoran un tiempo mayor al momento de migrar los recursos (failover) al nodo de espera.

Ilustración 17:HA activo/pasivo



Fuente: (ECURED, s.f.)

2.2.7. Seguridad informática

- **Respaldo y Backus**

En el ámbito de la informática, cuando hablamos de backup nos referimos a un respaldo, copia de seguridad o una copia de reserva a otra copia que contiene los datos originales de un sistema de información o de un grupo de software

(archivos, ejecutables, documentos, entre otros) que son almacenados en un lugar seguro o en una sección segura de la memoria del sistema, con la finalidad de que podamos volver a disponer de esta información en caso de presentarse alguna eventualidad, accidente o desastre que suceda y provoque la pérdida total o parcial del sistema. Dicho de otra manera, viene a ser una copia que se realiza por si sucediera cualquier cosa, que usualmente es actualizada en un periodo de tiempo como medida de seguridad.

En la actualidad, los sistemas informáticos pueden sufrir diversos tipos de siniestro, como lo son los ataques de manera remota por parte de hackers o virus informáticos, la destrucción física de los soportes de almacenamiento e incluso una eliminación accidental de la información de parte de algún usuario que cuenta con autorización. Para hacer frente a este tipo de casos, se recurre de manera manual o automática al backup del sistema para poder reestablecer la información perdida, disminuyendo de esta manera las perdidas en materia de datos o información.

- **Firewall**

  Un firewall, denominado también cortafuegos, es un sistema que permite la protección de computadoras (o una red de computadoras) frente a intrusiones que vengan de terceras personas (usualmente de internet). Este sistema hace posible el filtrado de los paquetes de datos que circulan por la red. Consiste de un “puente angosto” que cumple con filtrar el tráfico entre una red interna y externa. Estos pueden ser un programa (software) o un equipo físico (hardware) que cumplen el rol de intermediarios entre la red local (o la computadora local) y una o diversas redes externas.

Un firewall trabaja como una barrera entre nuestro computador y el internet u otras redes públicas. Si el tipo de tráfico que se realiza no se encuentra en la lista permitida por este, no entra ni sale del equipo.

Para cumplir con su función, un sistema de firewall posee una serie de reglas predefinidas que le permiten:

- La autorización de una conexión (Allow).
- El bloqueo una conexión (Deny).
- La redirección de un pedido de conexión sin emitir un aviso al emisor (Drop).

Por medio de esa serie de reglas es posible instalar un método de filtración que depende de la política de seguridad establecida por la organización. Usualmente se distingue dos tipos de políticas de seguridad:

- Aquellas que permiten únicamente las comunicaciones autorizadas de manera explícita: “Todo lo que no se autoriza de manera explícita está prohibido”.
- Aquella que impiden cualquier tipo de comunicación que fue explícitamente prohibida.

Tipos de firewall

Existen dos tipos de firewalls básicamente, que están orientados a distintos tipos de infraestructuras de datos y tamaños de red. Estos son:

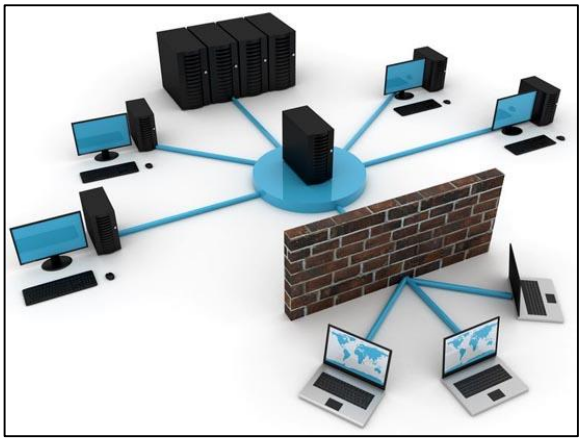
- Firewall por Software (que incluyen aplicaciones gratuitas y las de paga).
- Firewall por Hardware (las que se utilizan a través de dispositivos)

Firewall por software

También conocidos como “Desktop firewall” o “Software firewall”, es un programa que puede ser instalado y utilizado de maner libre, o no, en el equipo informático.

Este tipo de firewall son básicos y están dirigidos para instalaciones pequeñas como las del hogar o las de oficina, se encargan de monitorear y bloquear (de ser necesario) el tráfico de internet. Actualmente, casi todos los equipos de computadora poseen un firewall de manera predeterminada, independientemente del sistema operativo que se encuentre instalado en ellas.

Ilustración 18:Diseño de sistema con Firewall



Fuente: (tecnologia-informatica, 2020)

Firewall por Hardware

Este tipo de firewall usualmente está instalado en los routers que son utilizados para acceder a internet, lo que quiere decir que todos los dipostivos que se encuentren detrás de dicho router, se encuentran protegidos por el firewall que posee este dispositivo. En la actualidad, la mayoría de routers posee un firewall instalado de manera predeterminada.

La configuración de este tipo de firewall es mucho más complicada que la instalación de un firewall por software y esta tarea se realiza generalmente por medio del navegador que se usa para acceder a internet. Es importante señalar que la diferencia de precio entre un router con firewall y uno que no lo posee es bastante pequeña, por ese motivo es recomendable comprar uno que posea este tipo de protección.

Asimismo, es importante añadir que es posible contar con un firewall por hardware y uno por software que se encuentren activos de manera simultánea para conseguir una proyección aun mayor, sin embargo, es necesario contar con un mayor conocimiento en el aspecto de seguridad de red para que la configuración permita que estos cumplan con sus funciones de manera adecuada sin entorpecer sus actividades entre ellos.

2.3. Marco situacional

El Hospital Regional de Salud “Hermilio Valdizan Medrano” de Huánuco es una Unidad Ejecutora 402, establecimiento de salud II-2, del segundo nivel de atención de salud, órgano desconcentrado y referencial, responsable de brindar prestaciones asistenciales de prevención, recuperación y rehabilitación de las especialidades clínico – quirúrgicas de mediana complejidad, en concordancia con las normas y lineamientos emitidos por la Dirección Regional de salud Huánuco.

2.4. Definición de términos básicos

- **TCP/IP**

  Protocolo de comunicación para redes que facilita la comunicación de los equipos dentro de una red. Fue diseñado basándose en el modelo teórico OSI de capas (con la cual comparte cuatro de ellas),

sin embargo, este protocolo brinda una mayor cantidad de opciones y es un modelo práctico

Entender las principales características de la pila de protocolos de internet (conjunto ordenado de protocolos que se organizan por capas) que ofrece TCP/IP permite la configuración de redes básicas.

- **OSI**

  Este modelo fue desarrollado en el año 1984 por la ISO (International Organization for Standarization). Su finalidad era lograr interconectar sistemas de distintas procedencias para que tengan la capacidad de intercambiar información sin ningún tipo de obstáculo, sin importar los distintos protocolos de fábrica con los que estos trabajaban.

  Este modelo consta de 7 capas o niveles de abstracción. Dentro de cada uno de estos niveles se cumplen funciones propias para que luego de manera conjunta puedan conseguir su objetivo final. Es esta separación por niveles lo que posibilita la intercomunicación de distintos protocolos al momento de aglomerar funciones específicas en cada uno de los niveles de operación.

- **Protocolo ARP**

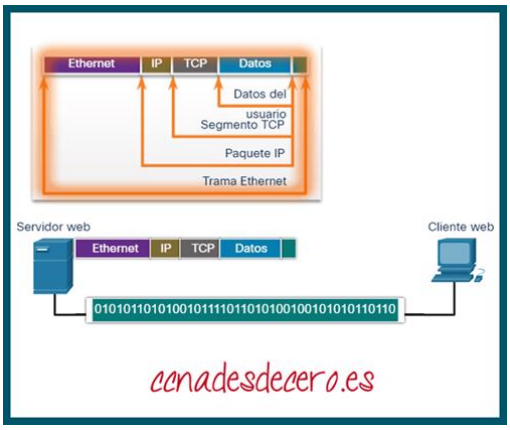
  El protocolo de resolución de direcciones forma parte de la capa de enlace de datos, es el encargado de ubicar la dirección de hardware que pertenece a una determinada dirección IP. Para cumplir con este trabajo, realiza el envío de un paquete a la dirección de difusión de la red en donde se encuentra la dirección IP por la que se hace la consulta, y se espera una respuesta del equipo en donde se envía la dirección Ethernet que le corresponde.

- **Encapsulamiento de datos**

  Al momento de realizar el envío de mensajes en una red, el proceso de encapsulamiento trabaja desde las capas superiores hacia las inferiores. En cada una de estas capas, la información de la capa

superior forma parte de los datos en el protocolo encapsulado. Por ejemplo, el segmento TCP es considerado como un dato dentro del paquete IP.

Ilustración 19:Encapsulamiento de Datos



Fuente: (Walton, s.f.)

- **IP**

  Vienen a ser las siglas de “Internet Protocol” o “Protocolo de internet” por su traducción. Este protocolo tiene la función de establecer las comunicaciones en la mayorá de las redes con las que trabajamos, al igual que otras como HTTP, TCP, UDP, entre otras. Para cumplir con ese objetivo, designa una dirección única e irrepetible a cada uno de los dispositivos (routers, servidores, teléfonos, electrodomésticos con conexión a internet, computadoras, etc.) que intentar comunicarse en Internet

  Un dispositivo no puede comunicarse sin poseer una dirección IP. Las direcciones IP vienen a ser los nombres numéricos que se establecen a un dispositivo a manera de “matricula” para que este pueda ser llamado por diferentes dispositivos. Dentro de su clasificación podemos encontrar a las direcciones IP públicas y a las direcciones IP privadas.

- **Máscara de red**

  La máscara de red cumple la función de separar e identificar la fija de la IP de la parte variable.

Para cumplir con esta función, la máscara establecer el numero 225 a la parte del IP que no varía y colocará un 0 a la parte variable. Esto quiere decir que, si contamos con una máscara de 255.255.255.0 significa que los tres primeros bloques de números de esa IP no varían, y solamente varia el último bloque.

Conocer las fijas de la IP es importante para poder conectarnos a internet. Además, la máscara de subred, que viene a ser la parte numérica que varía, es utilizada para que nuestros dispositivos puedan saber si las direcciones de los otros equipos con los que se desea establecer alguna conexión, se encuentran en nuestra red local o fuera de esta.

- **Puerta de Enlace**

Este dispositivo (usualmente un ordenador) permite la interconexión de redes con protocolos y arquitecuytras distintas a todos los niveles de comunicación. Su finalidad es transcribir la información del protocolo que es usado en una red al protocolo que está siendo utilizado en la red de destino.

El gateway o “puerta de enlace” usualmente es un equipo informático configurado para brindar a los dispositivos de una red local (LAN) una salida hacia una red exterior, para lo cual hace uso usualmente de operaciones de tradición de direcciones IP (NAT: Networl Address Translation). Esta capacidad de traducción de direcciones posibilita la aplicación de una técnica denomina IP Masquerading (enmascaramiento de IP), que es utilizada a menudo para bridar acceso a internet a los dispositivos de una red de área local compartiendo una sola conexión a internet y, en consecuencia, una única dirección IP externa.

- **HTTP (Hypertext Transfer Protocol)**

Viene a ser el protocolo de transmisión de información de la World Wide Web (WWW), esto significa, que se encarga de establecer los

aspectos que permiten la comunicación por la red entre el dispositivo que solicita y el que posee la información solicitada.

A través de este protocolo se definen los criterios de sintaxis y semántica informática (forma y significado) que permitan establecer la comunicación entre los diversos elementos que forman parte de la arquitectura web, entre los que podemos encontrar a los servidores, clientes, proxies, entre otros. Fue creado en 1999 por el World Wide Web Consortium y tuvo la colboración de la Internet Engineering Task Force.

- **HTTPS (Hypertext Transfer Protocol Secure)**

  Al igual que HTTP, este protocolo es utilizado para la transferencia de datos. Sin embargo, a diferencia de HTTP en donde la transferencia de datos se realiza de manera normal haciendo que estos datos sean accesibles para cualquier usuario externo que intercepte la información, el protocolo HTTPS permite una conexión segura haciendo uso de un cifrado SSL lo que genera que los datos viajen de manera segura desde un punto a otro.

- **Estándar ANSI/TIA**

  La ANSI (American National Standards Institute) es una organización sin fines de lucro que se encarga de la supervisión del desarrollo de estándares dirigidos a productos, serivicos, procesos y sistemas en los Estados Unidos. Además, forma parte de la Organización para la Estandarización (ISO) y de la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC).

  Por su parte, TIA (Telecommunications Industry Association) que nació en el año 1985 luego de que se desintegrara el monopolio de AT&T, en encarga de desarrollar las normas de cableado industrial voluntario para una gran cantidad de productos de las telecomunicaciones, actualmente posee alrededor de 70 normas definidas.

- **Puertos Lógicos**

  Viene a ser una zona o localización que forma parte de la memoria de un ordenador, la cual está asociada con un puerto físico o con un canal que permite la comunicación, estos puertos proporcionan un espacio para que la información que será transferida pueda ser almacenada de manera temporal entre la localización de memoria y el canal usado para la comunicación.

  La salida de información de los puertos lógicos se da en bits, que pueden ser 1 o 0, es decir, un puerto es el valor que se utiliza en el modelo de capa de transporte que nos permite diferenciar entre las distintas aplicaciones que se pueden conectar a un mismo host. Entonces podemos decir que, un puerto lógico de internet es una interfaz de software que permite el ingreso y salida de datos que se dan por el uso de aplicación que utilizan internet.

  Los puertos pueden ser identificados por números que van desde el 1 hasta el 65000 (e incluso pueden llegar a más). Entre los puertos más conocidos en el rango del 1 al 1024, encontramos los siguientes:

  - HTTP, utiliza el puerto 80 para la transferencia de hipertexto por Internet.
  - FTP, utiliza el puerto 20 para la transferencia de data (mp3, documentos, etc.).
  - HTTPS, utiliza el puerto 443 para la transferencia segura.
  - SMTP, utiliza el puerto 25 para el correo electrónico.

- **Equilibrio de Cargas**

  Es un sistema comúnmente utilizado cuando se requiere atender mucho tráfico en una aplicación o sitio web. El trabajo que realiza, consiste en crear un grupo de servidores que son los responsables de responder las solicitudes que recibe un servicio, como lo son una página web, un servidor de correo electrónico, entre otros.

A través de este, todo el conjunto de solicitudes al sistema de distribuyen entre los distintos servidores, generando de esta manera, un aumento en la cantidad de usuarios concurrentes que un proyecto pueda atender.

- **VPN**

  Es una tecnología de red la cual es utilizada para poder conectar uno a mas computadoras a una red privada por medio de internet. Las entidades suelen hacer uso de estas redes para que sus trabajadores, desde la cualquier parte del mundo, pueda tener acceso a los recursos que estas poseen que, de otra manera, no podrían. Sin embargo, es importante señalar que la conexión de un trabajador por medio de una computadora para hacer uso de los recursos corporativos, solamente es una de las múltiples funciones de una VPN. La correcta implementación de esta tecnología permite a la entidad asegurar la confidencialidad e integralidad de la información.

- **Alto Rendimiento**

  Son un tipo de clúster que están enfocados para brindar altas prestaciones en lo que respecta a la capacidad de cálculo. Algunas de las razones para hacer uso de este tipo de clúster son:

  La magnitud del problema a resolver.

  El precio de los equipos necesarios para poder resolverlo.

  A través de estos clústeres, es posible obtener capacidades de cálculo superiores a las de un ordenador mucho más caro en comparación al costo de todos los ordenadores que forman parte del mismo. Algunos ejemplos de clúster de bajo costo, son lo que se vienen desarrollando en diversas universidades haciendo uso de equipos personales desechados por ser considerados “anticuados”, los cuales consiguen competir de par a par con la capacidad de cálculo ofrecida por superordenadores de altos costos.

- **Escalabilidad**

  Viene a ser la capacidad que posee un sistema de adaptarse y responder, con respecto al rendimiento, que posee a medida que la cantidad de usuarios que posee el mismo incrementa de manera significativa. A pesar de verse como un concepto simple y claro, la escalabilidad de un sistema es un tema complejo e importante del diseño de un sistema.

  La escalabilidad se encuentra bastante relacionada al diseño del sistema, además, influye de manera significativa en su rendimiento. Cuando una aplicación se encuentra correctamente diseñada, la escalabilidad no significa un problema. La escalabilidad es considerada un factor crucial para el crecimiento de un sistema.

- **IPtables**

  Es una herramienta de filtrado de paquetes de Linux, la cual se encuentra bastante establecido debido al uso de muchos sitios a lo largo del mundo que trabajan y hacen uso de IPtables de manera continua.

  La función que cumple esta herramienta es la de analizar todos los paquetes del tráfico de red que ingresan a una máquina, es decir, teniendo como base una serie de reglas, deciden qué hacer con dicho paquete, sin embargo, existen muchas diferentes acciones que se pueden realizar con el tráfico de red a través de las IPtables.

- **Seguridad Informática**

  Esta disciplina tiene el objetivo de proteger la integridad y privacidad de la información que se encuentra alojada en un sistema informático. La seguridad informática, también hace referencia a la práctica de proteger los diferentes sistemas y dispositivos de ataques maliciosos.

  Para cumplir con esa finalidad, define normas que permitan minimizar los riesgos a los que se pueden ver expuestas la información o

infraestructura informática. Dentro de estas normas se pueden incluir los horarios de funcionamiento, las restricciones a zonas determinadas, autorizaciones, prohibiciones, planes y procedimientos de emergencia, protocolos, entre otros, que permitan brindar un nivel de seguridad informática optima, reduciendo de esta manera el impacto en el trabajo de los empleados y de la entidad en general

- **Pfsense**

  Es una distribución personalizada de FreeBSD que fue adaptada para ser utilizada como Firewall y Router. Tiene la característica de ser de código abierto, además de poder ser instalado en una gran diversidad de ordenadores, al mismo tiempo, pose una interfaz web sencilla para poder configurarlo. Este proyecto es mantenido comercialmente por la empresa Electri Sheep Fencing LLC.

- **Squid**

  Viene a ser un servidor de proxy para web con caché. Entre algunas de sus ventajas encontramos la mejora en el rendimiento de las conexiones dentro de la entidad (guardando en la memoria de la web las peticiones que se realizan de manera frecuente a los servidores web y DNS), la aceleración del acceso a un servidor web especifico o la adición de seguridad por medio de filtros al tráfico de internet.

- **Squidguard**

  Squidguard es un redirector de URL utilizado para usar listas negras con el software Proxys Squid. Squidguard tiene dos grandes ventajas: es rápido y es gratis. Squidguard se publica bajo licencia pública GNU.

  Características:

  - Registro configurable incluido.
  - Barra de progreso al compilar listas negras.

- Cumplimiento total de sed para reescribir declaraciones.
- Bloqueo de URL con nombres de host.

- **Blacklist**

  Puede elegir entre varias distribuciones gratuitas y comerciales de listas negras en la red o crear y usar la suya (o cualquier combinación de ellas). Squidguard viene con una pequeña lista negra básicamente para fines de prueba.

- **Logs**

  Viene a ser un historial que se utiliza para grabar de manera secuencial todas las acciones que afectan algún proceso en un archivo o en una base de datos. De esta manera, se cuenta con una evidencia de la manera en la que se comporta el sistema.

III. MARCO METODOLÓGICO

3.1. Nivel y Tipo de Investigación

La investigación tiene el nivel descriptivo explicativo

Según (ROBERTO, 2012), este tipo de investigación también es llamada como investigación estadística. En esta los datos y características que posee una población o fenómeno de estudio son descritas, respondiendo a preguntas sobre el quién, qué, dónde, cuándo y cómo.

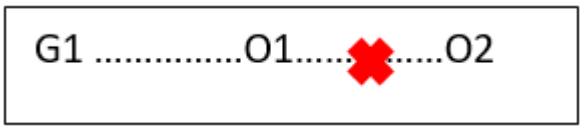
Tipo de Investigación

La presente investigación es considerada de tipo “aplicada”, ya que se hace uso de teorías específicas relacionadas al tema de investigación, dependiendo en gran medida de los descubrimientos y avances de la investigación básica, alimentándose de ellos. Al mismo tiempo este tipo de investigación se caracteriza por el enfoque hacia la aplicación, uso y consecuencias empíricas de estos saberes.

3.2. Diseño de la investigación

El diseño de la investigación es No experimental transversal-Descriptivos

- Método transversal: En este tipo de diseño, los datos se recogen en un solo momento del tiempo. La finalidad de este método es describir las variables y poder realizar su incidencia en un momento dado. (FERRER., 2010)
- Diseños transversales descriptivos: Tienen la finalidad de investigar la incidencia y valores que se muestran en una o más variables.



Donde:

G1: Grupo o muestra

O1: Observación pre implementación

X: Implementación de una infraestructura tecnológica de servidores

O2: Observación post implementación

3.3. Determinación del universo/población

El universo/población está constituido por los médicos, enfermeros y personal administrativo del Hospital Regional Hermilio Valdizan Medrano.

Tabla 4:Personal con acceso a los sistemas informáticos

Oficina/ unidad/ departamento/servicio	Personal
Unidad de estadística e informática	15
Consultorios Externos	19
Dpto. de Diagnóstico por Imágenes	2
Dpto. de Patología Clínica	3
Unidad de Seguros	20
Dpto. UCI y Emergencia	2
Unidad de Personal	10
Dirección Ejecutiva	6
Unidad de Logística	14
Unidad de Economía	17
Oficina de Planeamiento Estratégico	4
Dpto. de Enfermería	2
Unidad de Apoyo a la Docencia	1
Unidad de Gestión de la Calidad	2
Órgano de Control Interno	4
Unidad de Mantenimiento y Serv.	5
Dpto. de Medicina	3
Dpto. de Cirugía	2
Dpto. de Gineco-Obstetricia	6

Dpto. de Pediatría	4
Dpto. de Anestesiología	2
Unidad de Epidemiologia	2
COE	3
Dpto. de Farmacia	12
Dpto. de Servicio Social	3
Dpto. de Psicología	3
Dpto. de Nutrición	2
Dpto. de Odontología	2
	170

Fuente: Elaboración Propia

3.4. Selección de la muestra

La selección de la muestra se realizó por selección de muestreo no probabilístico intencional, ya que en este tipo de muestra el investigador escoge de forma voluntaria los elementos que conformaran la muestra, Se utiliza en escenarios en las que la población es muy variable y consiguientemente la muestra es muy pequeña.

La muestra de la presente investigación está determinada por el personal que labora en el Área de Informática del Hospital Regional Hermilio Valdizan Medran, que en su totalidad son 3 personas que forman parte del personal encargado del Área, y a quienes se les aplicará técnicas para poder recopilar información que sirva como base para sustentar la investigación, tal como es la encuesta.

El personal que integra el Área de Informática dentro del Hospital Regional Hermilio Valdizan Medrano. Tienen los siguientes cargos:

- jefe de Sistemas.
- jefe de redes y telecomunicaciones
- jefe de programación

3.5. Técnicas e instrumentos de recolección de datos

Las técnicas de recolección de datos vienen hacer los medios a través de las cuales el investigador se informa del estado de la población respecto al uso de los servicios en la corporación. A continuación, se mencionan las técnicas de recolección que usaremos según el caso en la investigación.

Recolección Primaria de datos

La observación

Se observaron diferentes modelos de la solución planteada y se eligió el modelo más estable que garantizaba un sistema más robusto con todas las características que se buscaba para satisfacer las necesidades de disponibilidad de los servidores del Hospital Regional Hermilio Valdizan Medrano.

La encuesta

Se elaborarán encuestas una para evaluar la situación actual y otra para evaluar la implementación realizada, estas serán aplicadas al personal del Área de Informática.

La entrevista

Se realizarán entrevistas una para evaluar la situación actual y otra para evaluar la implementación realizada, dichas entrevistas se realizarán al personal del Área de informática.

3.6. Procesamiento y presentación de datos

Para analizar el estado de la disponibilidad de los servicios que brinda el Hospital Regional Hermilio Valdizán Medrano previa implementación de la solución planteada, procedimos a realizar una encuesta al personal del área de Informática como se muestra en el anexo 8.

La encuesta que se formuló posee 10 preguntas relacionadas a la disponibilidad y seguridad de los servicios y servidores antes de la implementación de la solución tecnológica.

Para realizar la encuesta se utilizó la escala de Likert, que es un método de investigación de campo y de esta manera poder desarrollar el análisis estadístico.

Tabla 5:Tabla de valoración

○ Muy buena (4) ○ Buena (3) ○ Regular (2) ○ Mala (1) ○ Muy mala (0)	○ Muy frecuentemente (0) ○ Frecuentemente (1) ○ Ocasionalmente (2) ○ Raramente (3) ○ Nunca (4)
○ Extremadamente satisfechos (4) ○ Muy satisfechos (3) ○ Moderadamente satisfechos (2) ○ Poco satisfechos (1) ○ No satisfechos (0)	○ Totalmente de acuerdo (4) ○ De acuerdo (3) ○ Indeciso (2) ○ En desacuerdo (1) ○ Totalmente en desacuerdo (0)

Fuente: Elaboración Propia

A continuación, se muestran la tabla (escala de evaluación de Likert) de respuestas y el puntaje total que se obtiene por cada entrevistado, en donde la puntuación mínima es 0 y la máxima 40.

Tabla 6:Escala de Likert previa implementación

ÍTEMS / ENCUESTADOS	1	2	3	4	5	6	7	8	9	10	TOTAL POR ENCUESTADO
Sujeto 1	1	1	0	1	0	1	0	2	1	0	**7**
Sujeto 2	1	1	1	0	1	2	3	1	2	1	**13**
Sujeto 3	0	1	1	1	1	2	3	2	1	2	**14**
TOTAL POR ÍTEM	**2**	**3**	**2**	**2**	**2**	**5**	**6**	**5**	**4**	**3**	**34**

Fuente: Elaboración Propia

El nivel de la disponibilidad encontrada en el HRHVM está en un 33.3 % deficiente y un 66.6% regular. Siendo una entidad de salud, donde se requiere atender a los pacientes con suma urgencia, la disponibilidad no debe estar en estas condiciones; es por ello que se plantea la implementación tecnológica de los servidores para mejorar la seguridad y disponibilidad de los servicios informáticos.

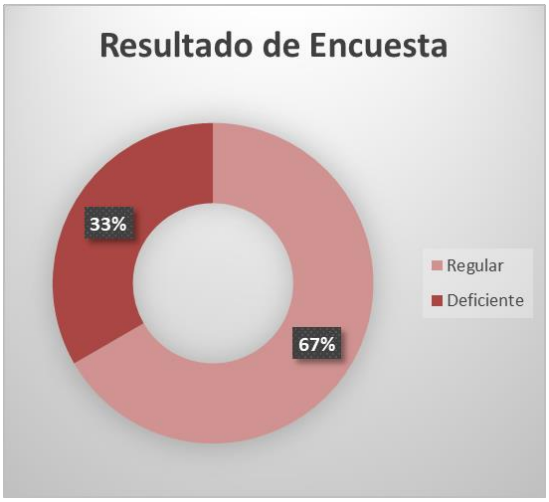
Tabla 7:Resultados obtenidos de las encuestas aplicadas previa implementación

Categorías	Rango calificativo	Frecuencia (fi)	Porcentaje (%)
Excelente	32 a 40	0	0 %
Muy buena	24 a 31	0	0 %
Buena	16 a 23	0	0 %
Regular	8 a 15	2	66.6 %
Deficiente	0 a 7	1	33.3 %
	Total	3	100 %

Fuente: Elaboración Propia

El nivel de la disponibilidad encontrada en el HRHVM está en un 33.3 % deficiente y un 66.6% regular. Siendo una entidad de salud, donde se requiere atender a los pacientes con suma urgencia, la disponibilidad no debe estar en estas condiciones; es por ello que se plantea la implementación tecnológica de los servidores para mejorar la seguridad y disponibilidad de los servicios informáticos.

Ilustración 20:Resultados de Encuesta



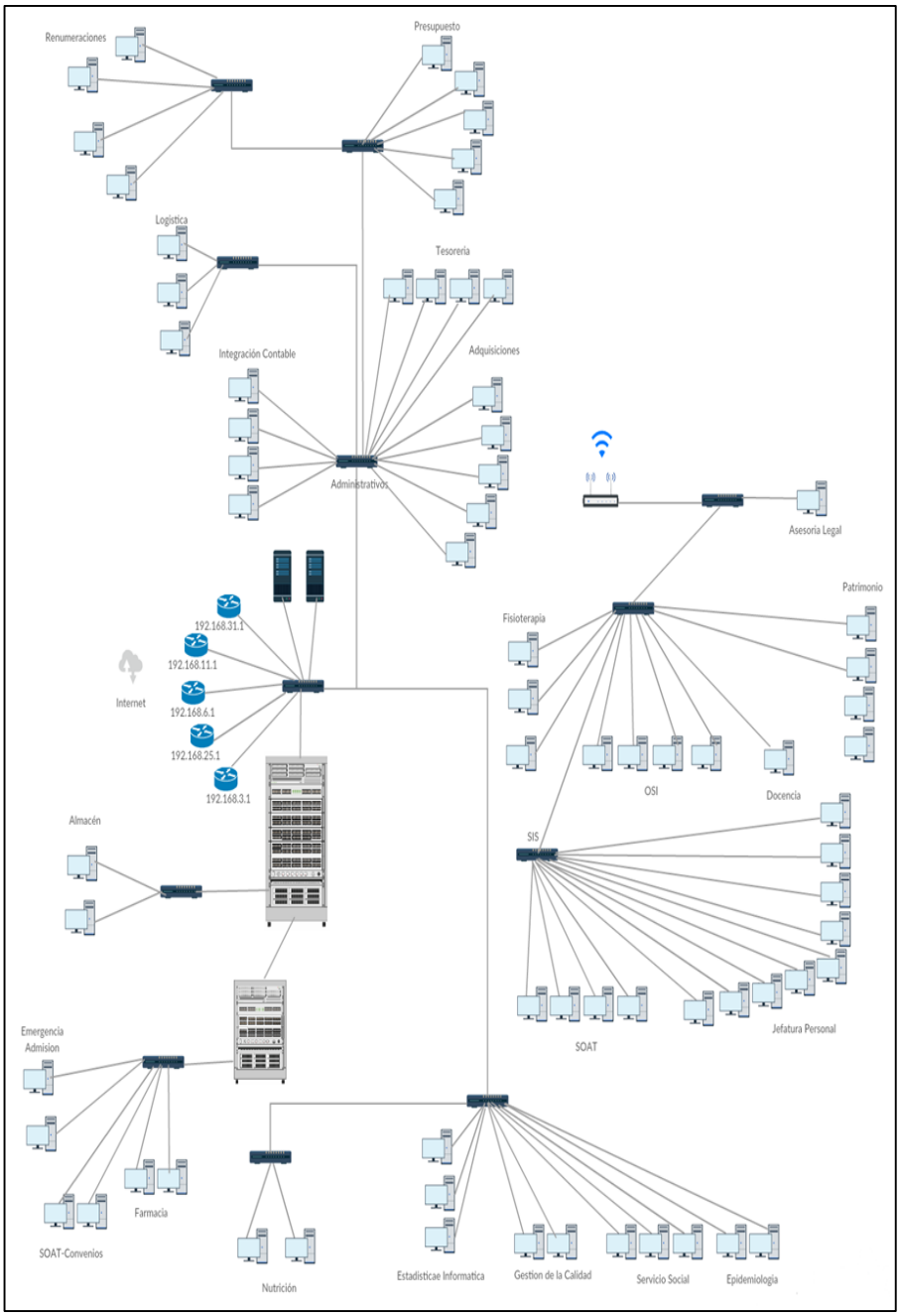
Fuente: Elaboración Propia

IV. ANÁLISIS DE LA SITUACIÓN ACTUAL Y COMPARATIVA DE HIPERVISORES PARA LA GESTION SERVIDORES

4.1. Análisis de la situación actual

4.1.1. Infraestructura de red actual del Hospital Regional Hermilio Valdizán.

Ilustración 21: Infraestructura de red actual



Fuente: Elaboración Propia

Los equipos que forman parte de la estructura de red serán mencionados continuación:

Tabla 8: Equipos de infraestructura de red

INFRAESTRUCTURA DE RED	
EQUIPO	**CANTIDAD**
Modem/Router ADSL Mitrastar	1
Router Movistar Nucom ADSL	3
Router Bitel (Línea Dedicada)	1
Switch Gigabit 24 puertos	6
Switch TP-LINK 8 puertos	3
Switch HPE 48 puertos	3
Servidores HP Proliant 380 G9	2
Antenas	2
Acces Point TP-LINK	1
Computadoras	170

Fuente: Elaboración Propia

De la imagen mostrada anteriormente podemos apreciar la topología de red del HRHVM, que es un modelo hibrido ya que podemos ver la topología estrella y topología en árbol. Actualmente la topología con la que cuenta no está gestionada ni tampoco cumple con los estándares de seguridad y cableado estructurado, pero esto es debido a que están en un local de contingencia; tuvieron que adquirir 2 locales separados para la parte de administración y SIS, dando como consecuencia la necesidad de implementar puntos de red en cada local y además el cableado de los 2 locales hacia el centro de datos.

En el centro de datos hay 2 servidores Hp proliant 380 g6 que están conectados al Switch, de la misma manera están conectados los routers y el gabinete para la distribución hacia todos los ambientes del HRHVM. Este tipo de conexión no brinda ninguna seguridad informática en toda la red ya que no cuentan con un firewall que restringa y bloquee acceso tanto externamente

como internamente, los servidores se encuentran expuestos a cualquier tipo de ataque (HACKEO, FILTRACION DE DATOS, PERDIDA DE DATOS) y es muy peligroso que estén accediendo a sistemas que son sector salud ya que estos son archivos confidenciales.

4.1.2. Descripción de Servidores Físicos del Hospital Regional Hermilio Valdizán Medrano.

Tabla 9:Equipos de servidores

LISTADO DE EQUIPOS SERVIDORES			
N°	**DESCRIPCIÓN**	**SISTEMA OPERATIVO**	**IP**
1	HP Proliant 380 G9	Windows Server 2012 R2	192.168.10.200
2	HP Proliant 380 G9	VMware EXSI	192.168.3.100

Fuente: Elaboración Propia

En el primer servidor Windows server 2012 aloja sistemas de gestión como el SIGA y SIAF, el cual solo debería brindar acceso a usuarios de área administrativa pero el acceso es para cualquiera que esté en la red LAN del HRHVM.

En el segundo servidor está instalado un hipervisor VMware EXSI en el cual gestionan máquinas virtuales para el servicio de página web del HRHVM.

4.1.3. Descripción de Servidores Lógicos del Hospital Regional Hermilio Valdizán Medrano

Tabla 10:Servidores Virtualizados

LISTADO DE EQUIPOS SERVIDORES			
N°	**DESCRIPCIÓN**	**SISTEMA OPERATIVO**	**IP**
1	Servidor Web	Ubuntu 16.04	**192.168.3.150**
2	Servidor Web	Ubuntu 16.04	**192.168.3.151**
3	Servidor BBDD	Ubuntu 16.04	**192.168.3.152**

Fuente: Elaboración Propia

Un servidor web gestiona la página del HRHVM y el otro gestiona el sistema de gestión hospitalario (SIGH), la cantidad de usuarios que usan los sistemas es un promedio de 160, esto quiere decir que el servidor web tiene que tener soporte para dar disponibilidad de los sistemas las 24 hrs del día, pero debido a que no se gestionó bien los adaptadores del hipervisor y de las máquinas virtuales existe un gran congestionamiento en la red haciendo que las paginas colapsen.

4.1.4. Servicios de TI/SI en el Hospital Regional Hermilio Valdizán Medrano.

Tabla 11:Sistemas de Información

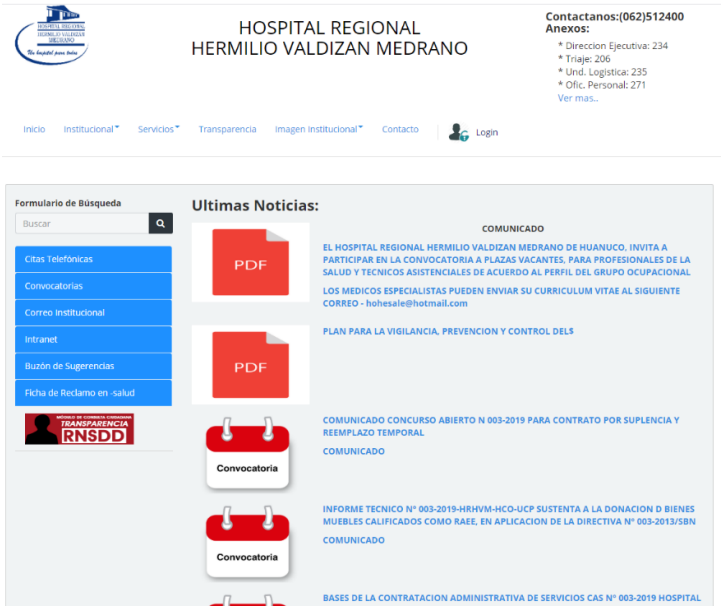
Manejo de Sistema de información
Página web del HRHVM
Sistema de Gestión Hospitalaria

Fuente: Elaboración Propia

Los sistemas mencionados anteriormente son los servicios alojados en los servidores web que se encuentran virtualizados.

1. **Página web del HRHVM**

Ilustración 22:Página web del HRHVM

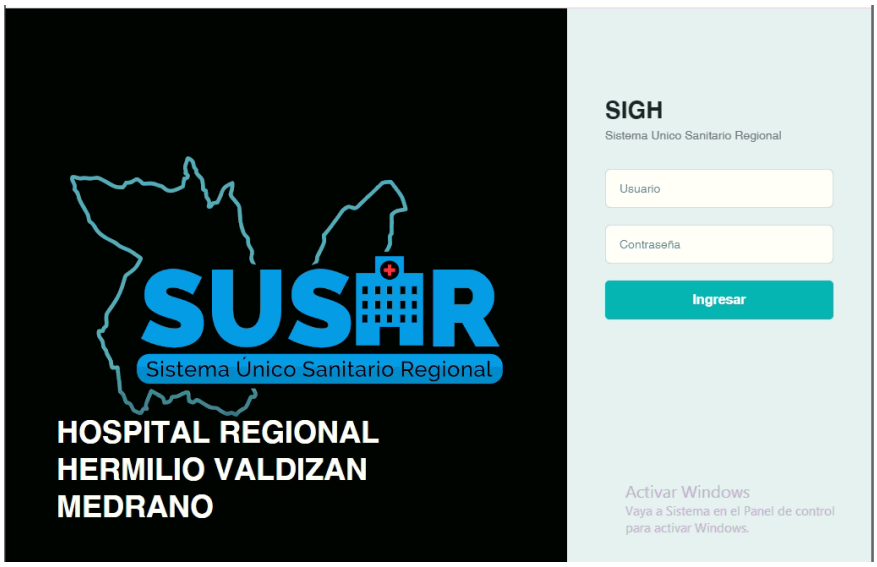


Fuente: Elaboración Propia

Esta página se encarga de gestionar la información actualizada del Hospital Regional Hermilio Valdizan Medrano. Como también las normas y convocatorias de trabajo.

2. Sistema de Gestión Hospitalaria

Ilustración 23:Sistema de gestión Hospitalaria



Fuente: Elaboración Propia

Ilustración 24:Sistema de gestión hospitalaria-Módulos

Fuente: Elaboración Propia

Este sistema gestiona todos los módulos que se encuentran en la imagen, cada módulo es un servicio que brinda el hospital a los empleados para la optimización de recursos y tiempo.

a) MODULO DE ADMISION

Es la atención que se da al paciente que ingresa a un servicio hospitalario enviado de consulta externa, urgencias o trasladado de otro servicio o entidad. Es la admisión del paciente quien requiere los servicios del hospital por diferentes situaciones de salud.

b) MODULO DE CAJA

Es la atención que se da al paciente que necesitara pagar por alguna consulta, atención médica o medicamentos recetados por los doctores.

c) MODULO DE RAYOS-X

Es la atención que se da al paciente para pueda trasladarse al servicio correspondiente de acuerdo al diagnóstico que le dieron.

d) MODULO DE RRHH

Este módulo se hizo para el uso de los doctores y enfermeros, en este módulo ellos podrán realizar su rol de turno de cada mes.

e) MODULO DE SERVICIO SOCIAL

Es la atención que se da al paciente cuando no cuenta con recursos económicos suficientes para pagar, dándole así al paciente una solución para que pueda ser atendido.

f) MODULO DE LABORATORIO

En este módulo ingresa y se recepciona el diagnóstico del paciente para que se le pueda dar los medicamentos correspondientes.

4.2. Estudio de los diferentes hipervisores para la gestión de servidores virtuales

4.2.1. Linux KVM

Esta tecnología de virtualización es open source, se encarga de convertir el kernel de Linux en un hipervisor que puede ser utilizado para la virtualización. Se muestra como una alternativa a tecnologías de virtualización propietarias, como las ofrecidas por VMware.

Elegir cambiar a una plataforma de este tipo nos brinda la posibilidad de inspeccionar, modificar y modificar el código fuente de su hipervisor. Tener una entrada libre al código fuente es un camino hacia la innovación, lo que le brinda la capacidad de virtual izar las cargas de trabajo y las aplicaciones tradicionales, al mismo tiempo, es posible crear una base para las cargas de trabajo nativas de la nube y que se basan en contenedores. Señalar también que, como la tecnología KVM se encuentra integrada al kernel de Linux, su uso e implementación es fácil.

Cambiar a una plataforma de virtualización basada en KVM permite inspeccionar, modificar y mejorar el código fuente de su hipervisor. El acceso al código fuente abre la puerta a la innovación, lo que le permite virtualizar las cargas de trabajo y las aplicaciones tradicionales, además de crear una base para las cargas de trabajo nativas de la nube y basadas en contenedores. Además, ya que la tecnología KVM está integrada en el kernel de Linux, es fácil de usar e implementar.

Ventajas:

- En lo que respecta a la velocidad, KMV permite ejecutar aplicaciones a velocidades optimas, siendo más rápido en comparación a otros hipervisores.

- Debido a su naturaleza open source esta no presenta restricciones, además, permite integrarse con infraestructura actual y distintas plataformas diferentes de Linux o Microsoft.

- En lo que respecta al costo, al formar parte de distintos sistemas operativos open source, KMV genera un cargo adicional.

- KVM es un hipervisor consolidado y estable, capaz de admitir cargas de trabajo empresarial.

- Debido a formar parte del kernel de Linux, KMV tiene la capacidad de expandirse para cumplir con la carga requerida su se presenta un aumenta en el número de máquinas guest y de solicitudes. Por medio de KMV, es posible virtual izar las cargas de trabajo de las aplicaciones que hacen uso de más recursos, siendo esta la base para muchas configuraciones de virtualización empresarial, como lo vemos en los centros de datos y las nubes privadas.

- Poseen un costo total de propiedad menor, significando una liberación de parte del presupuesto operativo destinado a analizar tecnologías innovadoras y modernas.

- Brinda la capacidad de interoperabilidad entre plataformas, debido a que puede ser ejecutada en plataformas de Linux y Windows, ofreciendo de esta manera un mayor provecho en la inversión de la infraestructura que posee actualmente.

- Ofrece la simplicidad de una sola plataforma de virtualización, permitiéndoos crear, iniciar, detener, pausar y trasladar un gran número de máquinas virtuales, así mismo, no permite crear plantillas, en una gran diversidad de sistemas de hardware y software.

4.2.2. VMware vSphere (ESXI)

Viene a ser un hipervisor que no posee sistema operativo y que es instalado directamente en un servidor físico, lo que permite consolidar sus sistemas de hardware. Las tecnologías de virtualización que posee VWware le brindan la capacidad de crear e implementar máquinas virtuales (VM), de manera que sea posible modernizar su infraestructura para brindar y gestionar aplicaciones nuevas y heredadas.

Ventajas:

- ESXI es un hipervisor consolidado y estable, capaz de admitir cargas de trabajo empresarial.
- En cuanto a la asistencia, VMware obtendrá asistencia de nivel empresarial de acuerdo con su ELA.
- Fácil administración.
- Mejora del 80% de utilización de los recursos del servidor.

Desventajas:

- El tiempo para crear e iniciar un servidor con ESXI usualmente requiere más tiempo.
- Los hipervisores hacen uso de diferentes métodos para poder comunicarse con el hardware físico del host. Al hacer uso de la plataforma de gestión de VMware, es necesario hacer uso de productos de la pila de control de esta compañía. Eso puede significar aumentos en los requisitos de hardware.
- Con respecto al costo, VMware necesariamente tendrá que adquirir licencias para ser utilizadas por varios productos y esta estará sujeta a un acuerdo de licencia empresarial (ELA). Si bien es cierto que un ELA ofrece ahorra parte del

presupuesto al inicio, sus costos pueden ir aumentando a medida que pase el tiempo, esto debido a los aumentos graduales en capacidad y funcionalidad.

- VMware nos brinda una plataforma de virtualización escalable. Sin embargo, es importante considerar como podría afectar a un ELA al momento de añadir host o máquinas virtuales adicionales, vSphere ofrece un máximo de 12 TB de RAM por cada host, con un límite de 64 host por clúster. Además, incluye varias interfaces de programación de aplicaciones (AOI), que pueden ser utilizadas para facilitar la gestión de las máquinas virtuales.

- VMware nos brinda un hipervisor escalable y que se encuentra consolidado, que cuenta con un rendimiento y característica excepcionales. Sin embargo, la virtualización propietario podría impedir que esta cuente con los recursos necesarios para invertir en nubes, contenedores y automatización.

4.2.3. Microsoft Hyper-V Server

Viene a ser un programa de virtualización ofrecido por Microsoft, que se base en un hipervisor dirigido a sistemas de 64 bits, posee procesadores basados en AMD-V o Tecnologia de Virtualización Intel. Es importante indiciar que el instrumental de gestión también puede ser instalado en sistemas de 32 bits.

Ventajas:

- Crea una copia de las máquinas virtuales para Recuperación de Desastres y lo almacena en cualquier otra ubicación física para que sea posible restaurarlo.

- Hay servicios de integración en cada sistema operativo invitado compatible. Posee controladores personalizados y varias funciones, lo que facilita el uso del sistema operativo en la máquina virtual.

- Hay características como la migración de almacenamiento, la importación / exportación y la migración en vivo, por lo que es fácil distribuir o mover cualquier máquina virtual, por lo que es portátil.

- Hay una herramienta de conexión remota que se incluye en la conexión de la máquina virtual en Linux y Windows. Esta herramienta le dará acceso a la consola, lo que le permitirá ver las cosas que están sucediendo en el invitado incluso antes de que se haya iniciado el sistema operativo. Esta es una característica única y mejor que el Escritorio remoto.

- Hyper-V tiene varias características avanzadas que están disponibles solo en las versiones superiores de VMware vSphere. El hipervisor de Windows es mejor que los otros hipervisores en todo, como las características ofrecidas, el ecosistema y el nivel de comodidad de las soluciones de la empresa.

- Define o amplia un entorno de nube privado.

- Ofrece un punto de automatización programable y centralizado para poder ser administrado, configurado, además que permite supervisar y solucionar problemas que se presenten en la infraestructura de red virtual o física en su centro de recursos.

4.2.4. Proxmox

Esta plataforma de virtualización se basa en sistemas de código open source, se encuentran disponibles bajo la licencia GLPv2, permiten la implementación de máquinas virtuales haciendo uso de tecnologías de virtualización OpenVZ y KVM.

Esta solución de software libre está basada en Debian, que se muestra como una alternativa a solcuiones comerciales brindadas por VMware o Citrix. Define una estructura completa de

virtualización que permite la gestión centralizada de máquinas virtuales, ofrece la característica de alta disponibilidad basada en clústeres, la posibilidad de conectarse con recursos de almacenamiento en red, entre otras.

Ventajas:

- Virtualización de servidores con soporte para KVM Y LXC
- Máquinas virtuales basadas en Kernel
- Virtualización basada en contenedores
- Migración en vivo
- Almacenamiento Flexible
- Copia de seguridad programada
- Almacenamiento de respaldo
- Cortafuegos a nivel de host
- Interfaz de gestión basada en web
- Sistema de archivos de clúster Proxmox
- Administrador de Proxmox VE HA
- Simulador Proxmox VE HA

4.3. Comparación entre las diferentes soluciones de hipervisores existentes frecuentemente usado

Tabla 12:Tabla de comparación de hipervisores

	PROXMOX VE	VMWARE ESXI	HYPER-V	LINUX KVM
Apoyo al sistema operativo invitado	Windows y Linux y otros sistemas operativos que son conocidos	Windows, Linux, Unix	Windows, algunas versiones soportadas de Linux	Windows y Linux
Open Source	✓	✓	✓	✓
Contenedores Linux	✓	-	-	✓
Alta Disponibilidad	✓	-	-	✓
Recuperación de desastres	-	✓	-	-
Migración en vivo	✓	-	✓	✓
Almacenamiento local	✓	✓	✓	✓
Almacenamiento compartido	✓	✓	✓	✓
Soporte Vlan (802.1q)	✓	✓	✓	✓
Modificaciones en caliente	✓	✓	-	✓
Firewall Interno	✓	-	-	-
Administración simple (Dashboard)	✓	✓	-	✓
Tecnología bonding	✓	✓	✓	✓
Puntuación	**11**	**8**	**6**	**10**

Fuente: Elaboración Propia

V. DISEÑO E IMPLEMENTACION DE LA SOLUCION PROPUESTA

5.1. Propuesta de solución para mejorar la seguridad informática y disponibilidad de los sistemas informáticos.

Luego de haberse realizado la comparativa de los hipervisores más usados actualmente, se llegó a la conclusión de que se usara el PROXMOX VE para la administración de servidores virtuales, debido a que este hipervisor cumple con casi todas las exigencias que necesita tener para la implementación de una infraestructura tecnológica de servidores.

Proxmox ve incluye una administración web, esto será muy útil al momento de querer administrar los servidores debido a que podremos acceder desde cualquier maquina con internet, no habrá necesidad de estar en el centro de datos. Y con lo que respecta a estar expuesto en el internet no se tendrá que preocupar debido a que cuenta con un firewall externo e interno para cada máquina virtual y además Proxmox ve cuenta con autenticación PAM, este tipo de autenticación se encripta en sha512 lo cual tiene una longitud de 64 bits.

Permite virtualizar maquinas Windows, Linux y otros sistemas debido a la tecnología KVM. También nos brinda la virtualización de contenedores, que aporta mayor rapidez de los procesos y no provoca sobrecarga al hardware.

Por el lado de la alta disponibilidad Proxmox ve nos permite crear clúster de múltiples nodos para que los servidores puedan migrar de un nodo a otro en caso de que el hardware colapse o se apague los servicios informáticos sigan brindándose. El otro tipo de alta disponibilidad que nos brinda Proxmox VE es la tecnología bonding que nos permite unir dos o más interfaces de red físicos.

5.2. Diseño de la solución tecnológica propuesta

Como se pudo ver en la imagen de infraestructura de red del hospital, no cuentan con equipos de seguridad ni tampoco con softwares que ayuden

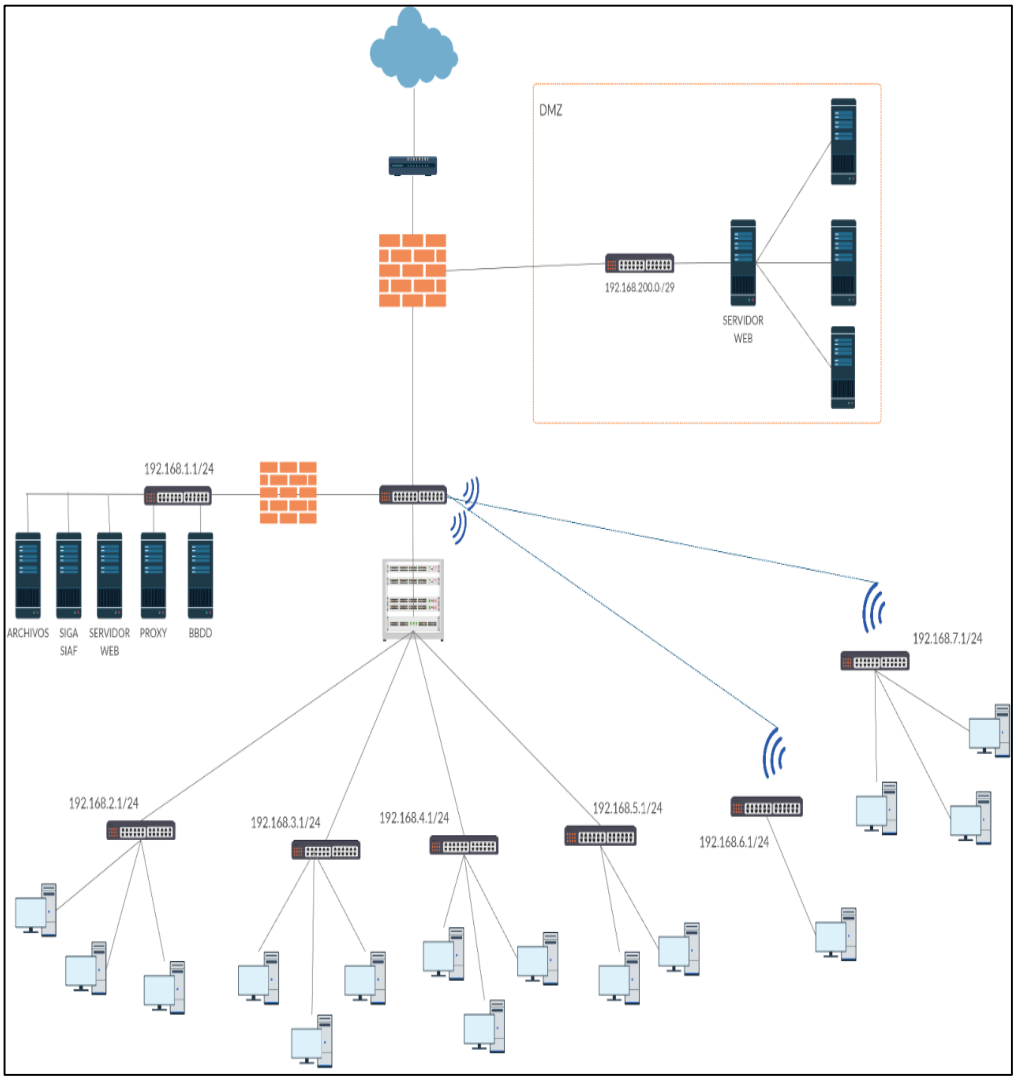
a restringir el acceso hacia los servidores, tampoco cuentan con softwares de recurso compartido por usuarios, tampoco con un bloqueo de páginas web que saturan la red del HRHVM, para todo esto se plantea una solución tecnológica de implementación de servidores virtuales para mejorar la seguridad informática y disponibilidad de los sistemas informáticos.

Se empezará implementando un firewall en el cual se configurará para el bloqueo y acceso al área DMZ y a la LAN, con las líneas de internet que se trabaja se darán de baja y se solicitara una sola línea de internet lo suficientemente buena para abastecer a toda la red del HRHVM.

De esta manera se tendrá control total del acceso a internet hacia los usuarios finales. El área DMZ es la que tendrá salida a internet ya que ahí se encuentra el servidor web, pero no podrá acceder a la red LAN por ningún motivo, de igual manera el firewall restringirá cualquier acceso desconocido que venga del exterior, evitándonos la filtración de datos o perdida de datos.

Se implementará un servidor Proxy para poder bloquear paginas prohibidas de acuerdo a las normas del HRHVM, así si cualquier usuario intente acceder a una página prohibida el proxy lo redireccionará hacia el servidor. Esto nos dará mayor seguridad ya que los usuarios no podrán descargar virus ni propagar un ransonware, mucho menos saturar la red del HRHVM. Para resolver el problema de caídas del servidor web se realizará configuraciones de alta disponibilidad tanto en el hipervisor como el servidor web. El hipervisor PROXMOX nos da una nueva tecnología de alta disponibilidad ya que nos permite unir 2 adaptadores puente dando así mayor estabilidad al momento de recibir y enviar datagramas, y el servidor web se usará NGINX el cual nos brindará balanceo de carga y el encubrimiento de la ip del servidor web (Proxy Inverso). A continuación, mostrare el diseño de red de la solución tecnológica.

Ilustración 25:Diseño de red de solución tecnológica



Fuente: Elaboración Propia

5.3. Implementación de la Infraestructura tecnológica de servidores

En este capítulo se explicará paso a paso de cómo se procedió con la implementación de los servidores virtualizados en el Hospital Regional Hermilio Valdizan, cabe recalcar que no se gastó recursos económicos debido a que tanto como el hipervisor y los servidores son open source.

5.3.1. Configuración del Hipervisor PROXMOX VE

1. Se empezará por descargar la imagen iso del Proxmox en la página oficial de PROXMOX y se puede grabar en un DVD o USB para luego bootear en el servidor físico. El Proxmox es un hipervisor de tipo 1 lo cual no será necesario entrar a la

interfaz gráfica del menú de booteo del servidor HP Proliant 380 gen9.

2. En el menú de booteo del servidor físico escogeremos a la unidad donde se encuentra la imagen iso del Proxmox.

3. Esperamos que cargue el menú del Proxmox VE y le daremos click en instalar Proxmox ve.

4. Aparecerá los términos y condiciones los cuales deveras leerlo y aceptarlo.

5. Dará a elegir el almacenamiento donde se instalará la raíz del Proxmox, el servidor cuenta con 2 TB de almacenamiento los cuales están divididos en 2 discos de 1 TB, escogeremos el primer almacenamiento.

6. Se escogerá el País, la zona horaria y el diseño del teclado para continuar con la instalación.

7. Se tendrá que escoger una interfaz de red, el nombre del usuario del Proxmox y la configuración de red con la cual podrá ser administrable mediante una página web.

8. Se tendrá que asignar una contraseña que sea mínima de ocho caracteres entre letras, números y símbolos; asignaremos un email donde les llegara cualquier aviso de Proxmox.

9. Al finalizar con todas estas configuraciones básicas nos mostrara un resumen de toda la configuración hecha, si está bien todo le daremos en instalar y esperaremos a que se instale.

10. Terminado la instalación nos mostrara en el monitor una bienvenida de Proxmox y la url a la cual tendremos que acceder para poder administrarlo.

11. Se coloca la url y el sitio web nos mostrara un mensaje de advertencia, hacemos click en configuración avanzada y luego hacemos click en la ip mostrada.

12. Para logearse se tiene que ingresar con root y la contraseña asignada anteriormente y ya podremos empezar con la administración de los servidores.

13. Se empezará habilitando todas las interfaces de red que tiene el servidor, una vez habilitada todas las interfaces se habilitara también los bridges (puentes) para cada interfaz de red, las cuales iremos configurando mientras vamos agregando los servidores.

14. Debido a que el Proxmox es una distribución GNU/Linux basada en Debian cualquier actualización o si se requiere instalar herramientas se realizará por la consola del Proxmox, para poder realizar las modificaciones en caliente de las interfaces de red se tendrá que instalar la herramienta ifupdown2.

5.3.2. Implementación del servidor Firewall

Para poder implementar un firewall se tiene que saber que, este debe contar con 3 interfaces de red para la conexión con la WAN, LAN y DMZ; esta es la estructura básica que debe tener para brindar seguridad y disponibilidad en el HRHVM.

1. Se descargar la imagen iso Debian 10 de la página oficial, no tomara mucho en descargar debido a que solo pesa 349MB a comparación con otros sistemas operativos que pesan más de 1GB.

2. El iso descargado se tiene que subir al servidor Proxmox para así poder consumir la imagen y crear los servidores virtuales.

3. Para poder cargar la imagen iso, se debe ir al almacenamiento local, luego a contenido y le damos en la opción a cargar. Escogemos la iso que descargamos y lo cargamos al Proxmox.

4. Creamos una Máquina Virtual y le asignaremos por nombre Firewall, tendrá la iso debían, crearemos 2 interfaces de red más, asignaremos 8 de memoria RAM, 100 GB de almacenamiento.

5. Empezara a cargar el sistema operativo debían, el particionamiento se realizará de 3, el primero será la raíz, el segundo será para el área de intercambio y el tercero será para el home. Se ingresará una clave para el super usuario y otra para el usuario por defecto.

6. Luego de haber finalizado la instalación, lo primero que se tendrá que hacer es configurar las interfaces de red.

7. Para realizar cualquier configuración en Linux se necesita un editor, para lo cual el editor por defecto es nano pero una vez que se configure para tener acceso a internet se descargara el vim.

8. Se ingresa a la ruta “/etc/network/interfaces” y se empieza a poner las 3 redes. La primera que es la WAN se debe poner la ip que tu proveedor de internet, la segunda será la red para la LAN y la tercera la red para el área DMZ.

9. Luego se ingresa a la ruta “/etc/resolv.conf” para configurar nuestros dns del proveedor de internet.

10. Se realiza la prueba de internet y se proseguí con la actualización del servidor con el comando “sudo apt update”, se continua con el comando “sudo apt upgrade” e instalaremos nuestro editor que nos facilite la configuración, en nuestro caso “sudo apt-get install vim”.

11. Se realiza la prueba de conexión de área local y dmz, para así empezar con la configuración del firewall.

12. Hay mucha herramientas y softwares que son de mucha ayuda para administrar el firewall. El sistema operativo Linux dispone de un firewall llamado Iptables, es un firewall que se gestionara mediante reglas.

13. Se instalará con el comando “sudo apt-get install Iptables-persistent”

14. Iptables funciona gracias a una serie de tipos de tablas que son la tabla mangle, nat y de filtrador.

15. Por defecto todas las tablas de Iptables vienen con políticas de aceptación, esto quiere decir que tenemos que asignar reglas para el filtrado de paquetes; o también podemos poner todas las tablas de filtrado en bloqueado, para así no tener que estar agregando reglas de filtrado lo cual consumirá mucho más recurso del sistema. En cambio, si se gestiona todas las tablas en bloqueado solo ingresaremos lo que se quiere aceptar.

16. Normalmente cuando se realiza una configuración de un servicio este se queda grabado en el sistema, ya no se tendrá que realizar la configuración de nuevo; pero en el caso del firewall Iptables si se llega a reiniciar el servidor o se apaga, las reglas que se configuro se borraran inmediatamente, teniendo así que configurar de nuevo a menos que se realice un backup y se vuelva a ejecutar el archivo guardado. Para evitarnos este problema, se tendrá que crear un script sh o bash para poder ejecutarlo de inmediato si en caso se llegase a apagar o reiniciar el servidor.

17. Se empezará ejecutando reglas en el script sh de limpiar tabla de filter.

18. Reglas para limpiar la tabla nat
19. Reglas para indicar a las tablas que estén por defecto en DROP.
20. Se activará el bit forwarding, este comando hará que nuestro firewall pueda funcionar como ruteador o como puerta de acceso hacia internet, a si es qué se tiene que activar.
21. Reglas para permitir el acceso Loopback.
22. Reglas para permitir el tráfico por SSH.
23. Reglas para permitir el tráfico HTTP
24. Reglas para permitir el tráfico HTTPS
25. Reglas para permitir el tráfico DNS
26. Reglas para permitir el tráfico ICMP
27. Reglas para permitir conexiones MYSQL.
28. Reglas para bloquear ataques DOS.
29. Reglas de POSTROUTING del nat para que nuestra red LAN y DMZ tengan acceso a internet.
30. Reglas de PREROUTING del nat para el servidor web.

5.3.3. Migración de los servidores web y Base de Datos al Proxmox VE

1. Primero se deberá crear los servidores virtualizados (WEB Y BBDD).
2. Como se explicó anteriormente, se hará uso de los contenedores y no de las máquinas virtuales, debido a que usan el kernel del sistema host en el que se ejecutan, en lugar

de emular un sistema operativo completo; en otras palabras, acceden a los recursos del sistema host directamente.

3. Se creará un contenedor para el servidor web en el cual usaremos como sistema operativo debían 10.
4. Se actualizar los repositorios del sistema e instalar el Vim.
5. Se instalará apache2, base de datos MySQL y Python.
6. Se instalará ssh para conectarnos al anterior servidor web y así poder migrar toda la data y base de datos.
7. Una vez conectado se usará el comando scp el cual nos permitirá copiar toda la información del antiguo servidor web.
8. Se realizará enlaces simbólicos para así culminar con las migraciones.
9. El segundo servidor web se realizará la misma configuración, pero se usará Nginx que es un servidor web/proxy inverso ligero de alto rendimiento.
10. Para este servidor no se realizará ninguna migración debido a que empezaran de cero. Se empezará a trabajar a nivel de microservicios lo cual hace que se trabaje a un nivel más detallado.
11. Debido a que trabajan a nivel de microservicio cada sistema se configurara para poder salir por un puerto distinto.
12. Por último, se creará un contenedor para la base de datos, como se hizo en el primer servidor se entrará por ssh al servidor y se migrará todas las tablas existentes en la base de datos

13. El servidor web estará en el área dmz así es que se le configurara su red de acuerdo con la red creada en el firewall para el área DMZ.

5.3.4. Configuración bonding en el PROXMOX VE

1. El hipervisor Proxmox tiene 3 tipos de integración de switches virtuales, el primero es Linux Bridge, Linux Bond y Linux Vlan.

2. La tecnología bonding de interfaces de red es la solución para tener alta disponibilidad y redundancia en los servidores donde la conectividad no debe fallar, como por ejemplo un servidor web.

3. Antes que de empezar a configurar se debe tener en cuenta que existe varios tipos de bonding, como se definió en el marco teórico el tipo de bonding que nos brindara alta disponibilidad y un aumento de velocidad es el bond 802.3ad.

4. Se ingresa al Proxmox y se dirigen a la configuración de red.

5. Crearemos el bonding en Linux Bond.

6. Se ingresará el nombre que se desee que tenga el bonding, una ip fija si también se quisiera, pero en nuestro caso solo agregaremos los nodos esclavos que queremos que estén en bonding.

7. Se escogerá el tipo de bonding y si se desea comentar algo también se puede hacer en la parte de comentario.

8. De esta manera nos aseguraremos la alta disponibilidad a nivel de red para los servidores web y BBDD.

5.3.5. Implementación del servidor NGINX

1. Nginx es un servidor que nos brindara rendimiento y un proxy inverso, el rendimiento nos lo brindara haciendo un balanceo de cargo del servidor web.

2. El balanceo de carga servirá para las solicitudes/acceso de clientes al mismo tiempo, el balanceo de carga mejora la distribución de carga de trabajo entre los diversos servidores de web. Optimiza el uso de recursos, maximiza el ancho de banda, minimiza los tiempos de respuesta y evita la sobrecarga de un recurso.

3. Se creará un contenedor y se instalar el Nginx, una vez instalada, en la ruta /etc/Nginx/conf.d/balanceador.conf se añadirá la configuración del balanceador.

4. La configuración se hará en 2 partes, la primera es el upstream donde se añadirá las ip's y los puertos en el cual está saliendo los servidores web.

5. La segunda configuración es para el servidor Nginx, donde se configurará el puerto y la ip por el cual saldrá el balanceador, se configurará por motivos de seguridad el proxy set header, en el sabremos las ip's que están enviando solicitudes.

6. Agregamos el proxy_pass para poder pasar las solicitudes a los servidores web agregados anteriormente.

7. Guardamos el fichero de configuración y reiniciamos el servicio.

8. Para brindarle seguridad al servidor web, realizaremos el proxy inverso, que se encargara básicamente de enmascarar la verdadera ip del servidor web.

9. Se entrará al fichero de configuración de por defecto del Nginx y también se configurará en 2 partes

10. La primera se indicará el puerto por donde saldrá el servidor que servirá como proxy inverso y la ip del servidor.

11. En la segunda se agregará el proxy set header y se agregara localizaciones donde se encuentra las ip's verdaderas de los microservicios que están alojados en el servidor web.

12. En las localizaciones si nos es más útil agregaremos un nombre para poder redirigir por nombre y ya no por un puerto, cosa contraria si en caso tengas 20 microservicios tendrás q acordarte de cada puerto por el que sale.

13. Es por esto que mejor se redijera por nombre ya que nos resultara más fácil de poder acordarse de los microservicios.

14. Guardamos el fichero de configuración y reiniciamos el servicio, y el proxy inverso ya estará funcionando como si fuera una máscara del servidor web.

5.3.6. Implementación del servidor Proxy Squid

1. Se creará un contenedor y se actualizará todos los paquetes necesarios para poder descargar el proxy Squid.

2. Se descargará editor vim y se realizará la configuración de red para poder gestionar el proxy.

3. Se descargará el Proxy Squid, el Squidguard y el blacklists que son el corazón de cada filtro de URL.

4. Luego de haber descargado todo, cada herramienta descargada tiene un fichero principal donde se realizará la configuración para poder hacer funcionar el proxy Squid.

5. Se empezará con el proxy Squid, iremos a su fichero de configuración que es el “Squid.conf”, nos dirigiremos a la sección de insertar las reglas de acceso para el cliente.

6. Se ingresará parámetros de configuración para que el nombre del servidor proxy sea detectado y en rango de ip’s que abarcara o se podrá usar el proxy.

7. Culminando la configuración de proxy Squid, se empezará con el Squidguard, pero el Squidguard se descargará junto con una lista negra.

8. La lista negra es un directorio que almacena ficheros donde se encuentra seccionado el tipo de contenido a querer bloquear.

9. Esa lista negra descargada lo moveremos al Squidguard que se encuentra en el estado de variable para preservar la condición del Squidguard y así exista un reinicio este no se vea modificado.

10. Realizaremos una búsqueda en /var/lib/Squidguard/, donde nos mostrara un archivo donde se encuentra la lista negra.

11. En los anexos verán los tipos de contenido que se puede bloquear o tener acceso desde el proxy.

12. Se ira al fichero de configuración del Squidguard para poder agregar los contenidos de la lista negra que se quiere bloquear.

13. El Squidguard tiene 3 secciones de configuración. La primera es la cabecera donde si no especificamos de donde se quiere tener la conexión para la lista negra este no funcionara. El segundo será la sección donde se agregará todos los contenidos que se bloquearan, se ingresara un bloqueo por dominio y por url haciendo más efectivo este bloqueo. El tercero se agrupará todos los contenidos que agregamos

anteriormente y se dará una orden la cual es pasar todo que no esté en el contenido bloqueado y si encuentra un contenido bloqueado que lo redireccione a un servidor web donde le aparecerá un mensaje de que dicha página se bloqueó por motivos de políticas de seguridad del HRHVM.

14. Para redireccionar al servidor web este se tiene q configurar previamente, se puede crear un HTML para poder mostrar el mensaje anterior.

15. Con esta configuración ya está casi completo el servidor proxy, pero aún nos falta configurar para sea transparente el proxy.

16. El proxy transparente redireccionara todo el tráfico http y https al proxy haciendo que las máquinas que no tengan el proxy se quedaran sin acceso a internet. Lo cual hará que las persona no puedan quitar el proxy.

17. Terminado la configuración se reiniciará el servicio de proxy Squid.

VI. ANALISIS E INTERPRETACION DE LOS RESULTADOS

6.1. Disponibilidad de los servidores del HRHVM antes de la implementación tecnológica

En este parte se realizará la medición de la disponibilidad de los servidores antes de implementar la propuesta tecnológica. Se tiene que saber que no todos los servidores tienen que estar activos las 24 horas del día, se debe diferenciar niveles de criticidad entre los servidores como es en el caso del Hospital Regional Hermilio Valdizan donde se tienen niveles de servicios informáticos que alcanzaran las 24 horas del día los 365 días del año.

$$\text{Disponibilidad} = \frac{(A-B)}{A} \times 100\ \%$$

Donde:

A: Horas comprometidas de disponibilidad.

B: Número de horas fuera de línea (corresponde a las horas de “caída los servicios informáticos” durante el tiempo de disponibilidad comprometido)

Para nuestro caso las “horas comprometidas de disponibilidad” se calculan de la siguiente manera:

$$\boldsymbol{A = 24\frac{horas}{dia} \times 365\frac{dias}{año} = 8760\ horas/año}$$

Y para el cálculo de “número de horas fuera de línea”, en nuestro caso, teniendo en cuenta los factores que se muestran en la siguiente tabla (la fuente de estos factores fue proporcionada por el jefe del Área de Informática del Hospital Regional Hermilio Valdizan Medrano, así como sus respectivos valores):

Tabla 13:Tabla de factores de caídas antes de la implementación

ANTES DE LA IMPLEMENTACIÓN	
FACTORES DE HORAS FUERA DE LINEA	**HORAS POR 1 AÑO**
Caída de discos del servidor	20
caída por mantenimiento de servidor no planeado	28
Caída por sobrecarga	40
Caída de base de datos	28
Caída por motivos de seguridad (ataques)	6
Caída por virus	10
Caída de algún equipo de red	10
TOTAL	140

Fuente: Elaboración Propia

Ahora calculamos la disponibilidad reemplazando los valores en la formula mencionada anteriormente:

$$Disponibilidad = \frac{(8760 - 140)}{8760} \times 100\ \%$$

$$Disponibilidad = 98{,}40182\ \%$$

Es así como se obtiene el valor de la disponibilidad antes de la implementación de la solución propuesta.

Al comparar el valor de la disponibilidad antes de la implementación (98,40%), con la siguiente tabla podríamos obtener el tiempo de indisponibilidad permitidos por años, meses y días para un servidor.

Tabla 14:Tabla de tiempo permitido de indisponibilidad.

Disponibilidad (%)	Tiempo offline/año	Tiempo offline/mes	Tiempo offline/día
90%	36.5 días	73 hrs	2.4 hrs
95%	18.3 días	36.5 hrs	1.2 hrs
98%	7.3 días	14.6 hrs	28.8 min
99%	3.7 días	7.3 hrs	14.4 min
99.5%	1.8 días	3.66 hrs	7.22 min
99.9%	8.8 hrs	43.8 min	1.46 min
99.95%	4.4 hrs	21.9 min	43.8 s
99.99%	52.6 min	4.4 min	8.6 s

99.999%	5.26 min	26.3 s	0.86 s
99.9999%	31.5 s	2.62 s	0.08 s

Fuente: Elaboración Propia

El Hospital Regional Hermilio Valdizan Medrano, antes de la implementación tiene una disponibilidad del 98,40%, por lo tanto, se permite un tiempo de indisponibilidad para sus servidores de 7 días al año, 14 horas al mes y 28 minutos al día aproximadamente.

Con el resultado obtenido se podrá comparar y hacer un análisis con el estándar TIA-942, dicho estándar se clasifica en cuatro niveles de disponibilidad, TIER I, TIER II, TIER III Y TIER IV. Estos niveles de tier clasificara al centro datos con un nivel de porcentaje aceptable y confiable para la entidad.

El nivel de porcentaje de cada TIER se verá en el siguiente cuadro:

Tabla 15:Tabla Tiers, Estándar ANSI/TIA-942

TIER	% DE DISPONIBILIDAD	% DE INSDIPONBILIDAD	TIEMPO DE INDISPONIBILIDAD
TIER I	99.67%	0.329%	28.82 H
TIER II	99.74%	0.251%	22.68 H
TIER III	99.98%	0.018%	1.57 H
TIER IV	99.99%	0.005%	52.56 min

Fuente: Elaboración Propia

De acuerdo con el siguiente cuadro, nuestro resultado obtenido de disponibilidad no entra en ninguna de los cuatro niveles de tier, esto quiere decir que es urgente implementar una solución.

6.2. Disponibilidad de los servidores del HRHVM luego de la implementación tecnológica

Luego de la implementación se dejó 3 meses funcionando los servidores y se volvió a tomar la misma encuesta al personal del área de informática para poder sacar los resultados obtenidos de dicha implementación.

A continuación, se muestra la tabla de (escala de evaluación de Likert), donde se digitará los puntos obtenidos de la encuesta. La puntuación mínima es 0 y máxima 40.

Tabla 16:Escala de Likert post implementación

ÍTEMS / ENCUESTADOS	1	2	3	4	5	6	7	8	9	10	TOTAL POR ENCUESTADO
Sujeto 1	3	3	3	3	4	4	4	3	4	3	**34**
Sujeto 2	4	3	3	3	3	4	2	3	4	2	**31**
Sujeto 3	3	3	2	3	3	4	2	3	4	3	**30**
TOTAL POR ÍTEM	**10**	**9**	**8**	**9**	**10**	**12**	**8**	**9**	**12**	**8**	**95**

Fuente: Elaboración Propia

Se presenta la siguiente tabla de resultados obtenidos en las encuestas mostrando la frecuencia distribuida por categoría y su porcentaje, después de la implementación de la solución propuesta:

Tabla 17:Resultados obtenidos de las encuestas aplicadas post implementación

Categorías	Rango calificativo	Frecuencia (fi)	Porcentaje (%)
Excelente	32 a 40	1	33.3 %
Muy buena	24 a 31	2	66.6 %
Buena	16 a 23	0	0 %
Regular	8 a 15	0	0 %
Deficiente	0 a 7	0	0 %
	Total	3	100 %

Fuente: Elaboración Propia

Procederemos a realizar el cálculo de la disponibilidad de los servicios informáticos después de la implementación, para calcular el “número de horas fuera de línea”, tomando los datos que se muestra en la siguiente tabla (la fuente de estos datos fue proporcionada por el jefe del área de Informática del Hospital Regional Hermilio Valdizán).

Tabla 18:Tabla de factores de caídas post implementación

ANTES DE LA IMPLEMENTACIÓN	
FACTORES DE HORAS FUERA DE LINEA (CAIDAS NO PLANEADAS)	**HORAS POR 3 MESES**
Caída de discos del servidor	0
caída por mantenimiento de servidor no planeado	3
Caída por sobrecarga	1
Caída de base de datos	1
Caída por motivos de seguridad (ataques)	0
Caída por virus	2
Caída de algún equipo de red	0
TOTAL	7

Fuente: Elaboración Propia

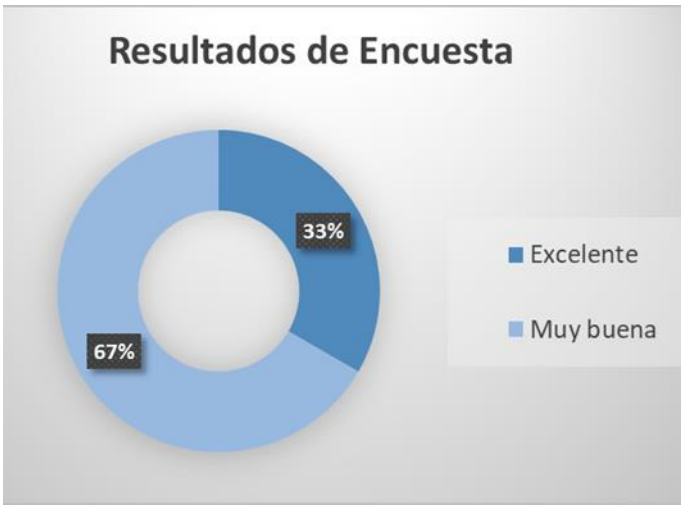
Luego calculamos la disponibilidad después de la implementación:

$$Disponibilidad = \frac{(2160 - 7)}{2160} \times 100\ \%$$

$$Disponibilidad = 99{,}67592\%$$

El resultado de la disponibilidad después de la implementación de la solución propuesta es 99,67592%. Comparando el resultado obtenido con un referente al cuadro estándar ANSI/TIA-942, vemos que la disponibilidad se posiciona en el nivel de Tier I con una disponibilidad de 99,67592%.

Ilustración 26:Resultados de Encuesta Post-Implementación



Fuente: Elaboración Propia

CONCLUSIONES

El presente trabajo después de finalizar con la implementación se llegó a las siguientes conclusiones:

- Con el análisis de la infraestructura de la red actual del Hospital Regional Hermilio Valdizan Medrano, se determinó que tiene una topología hibrida, pero esta no tiene servidores físicos ni lógicos que garanticen seguridad y disponibilidad.

- Con el diseño de una estructura de red para el Hospital Regional Hermilio Valdizan, se determinó una estructura lógica para mejorar la seguridad y disponibilidad informática, para evitar la indisponibilidad de los servicios informáticos.

- Con la comparación de los diversos tipos de hipervisores virtuales, se determinó que, él Proxmox VE es la elección perfecta para virtualizar la infraestructura TI del Hospital Regional Hermilio Valdizan, debido a que cumplía con casi todas las especificaciones que necesitaríamos para mejorar la seguridad y disponibilidad de la información.

- Con la implementación del Firewall, Proxy Squid y Squidguard se determinó que la gran mayoría de caídas de los servidores se debía a la falta de seguridad y de control de acceso del personal a sitios web que no compete con la institución, dé esta manera se pudo reducir en gran parte los ataques de virus, spam, intromisiones y otros en el Hospital Regional Hermilio Valdizan.

- Con la implementación del Servidor Nginx y bonding, se determinó que las interrupciones de los servicios informáticos disminuyeron, dando así una disponibilidad del 99,67592% e ingresando a los estándares del ANSI/TIA 942 en TIER I.

- Con la implementación de la infraestructura tecnológica de servidores, se mejoró la seguridad y disponibilidad de los servicios informáticos. Según la encuesta realizada después de la implementación tecnológica el 66.6% del personal de informática opina que la seguridad y disponibilidad informática es muy buena.

RECOMENDACIONES

El presente trabajo después de finalizar con la implementación se llegó a las siguientes recomendaciones:

- Se recomienda al Hospital Regional Hermilio Valdizan la adquisición de equipos físicos que brinden Alta gama seguridad informática.

- Se recomienda a las entidades pequeñas y medianas a la migración de servidores físicos a servidores lógicos, para optimizar los recursos de hardware y minimizar los gastos económicos.

- Se recomienda la adquisición de un servidor físico nuevo al Hospital Regional Hermilio Valdizan para la configuración en clúster de los 2 servidores físicos, brindando así una alta disponibilidad de los servicios informáticos.

- Se sugiera capacitaciones al personal del área de informática del Hospital Regional Hermilio Valdizan en temas de disponibilidad y seguridad informática; y realizar mantenimiento y actualizaciones programadas (PRVENTIVAS Y CORRECTIVAS) de los equipos informáticos, infraestructura tecnológica y servidores implementados en el HRHVM.

- Se sugiere al Hospital Regional Hermilio Valdizan a la utilización de sistemas operativos open source e invertir más en la virtualización de servidores open source.

BIBLIÓGRAFA

tecnologia-informatica. (2020). *QUE ES UN FIREWALL Y COMO FUNCIONA*. Obtenido de QUE ES UN FIREWALL Y COMO FUNCIONA: https://www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/

AprendiendoPC. (s.f.). *QUE ES UN SERVIDOR DE CORREO ELECTRONICO*. Obtenido de QUE ES UN SERVIDOR DE CORREO ELECTRONICO: http://www.aprendiendopc.com/que-es-un-servidor-de-correo-electronico

Azizi, Y. E. (s.f.). *QUE ES UN SERVIDOR DE BASE DE DATOS*. Obtenido de QUE ES UN SERVIDOR DE BASE DE DATOS: https://www.youngeek.com/servidor-base-datos/

Bednarz, A. (05 de MARZO de 2018). *NETWORKWORLD*. Obtenido de NETWORKWORLD: https://www.networkworld.es/networking/que-es-una-san

CARO, R. S. (2014). *IMPLEMENTACIÓN DE UN CLÚSTER EXPERIMENTAL BAJO TECNOLOGIAS LIBRES PARA PROPORCIONAR ALTA DISPONIBILIDAD DE SERVICIOS WEB HTTP.* CARTAGENA.

Castillero. (s.f.). *Psicología y Mente.* Obtenido de Psicología y Mente: https://psicologiaymente.net/miscelanea/tipos-de-investigacion

Catoira, F. (13 de Enero de 2014). *Primeros pasos para implementar un IDS con Snort*. Obtenido de Primeros pasos para implementar un IDS con Snort: https://www.welivesecurity.com/la-es/2014/01/13/primeros-pasos-implementacion-ids-snort/

David. (10 de Octubre de 2011). *SERVIDOR DHCP Windows 2008*. Obtenido de SERVIDOR DHCP Windows 2008: https://www.hostdown.es/minimanual/servidor-dhcp-windows-2008/

Digital Guide IONOS. (2018). *¿Que es un servidor informatico?* Obtenido de ¿Que es un servidor informatico?: https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-un-concepto-dos-definiciones/

ECURED. (s.f.). *Cluster de alta disponibilidad*. Obtenido de Cluster de alta disponibilidad: https://www.ecured.cu/Cluster_de_alta_disponibilidad

ESPINO, L. R. (2013). *Diseño e Implementacion de un sistema de cluster de alta disponibilidad para mejorar el desempeño de los servidores Web.* Trujillo.

Fernandez, L. (22 de Febrero de 2020). *Servidores DNS mas rapidos*. Obtenido de Servidores DNS mas rapidos: https://www.redeszone.net/tutoriales/redes-cable/servidores-dns-mas-rapidos/

FERRER., J. (2010). *TIPOS DE INVESTIGACION Y DISEÑO DE INVESTIGACION*. Obtenido de TIPOS DE INVESTIGACION Y DISEÑO DE INVESTIGACION: http://metodologia02.blogspot.com/p/operacionalizacion-de-variables.html

IMF Business School. (s.f.). *ALTA DISPONIBILIDAD, DEFINICIONES Y FUNCIONAMIENTO INFORMATICO*. Obtenido de ALTA DISPONIBILIDAD, DEFINICIONES Y

FUNCIONAMIENTO INFORMATICO: https://blogs.imf-formacion.com/blog/tecnologia/alta-disponibilidad-funcionamiento-201806/

Mejia, R. E. (2015). *DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA INTEGRADO.* Lima.

Multicomp S.A. de C.V. (2020). *IMPLEMENTAR ACTIVE DIRECTORY EN UNA EMPRESA*. Obtenido de IMPLEMENTAR ACTIVE DIRECTORY EN UNA EMPRESA: http://multicomp.com.mx/seguridad-informatica/seguridad-de-acceso/active-directory/

Pinterest. (s.f.). *SERVIDOR CLUSTER*. Obtenido de SERVIDOR CLUSTER: https://www.pinterest.com.mx/pin/513340057499056491/

Raffino, M. E. (14 de febrero de 2020). *Concepto.de*. Obtenido de Concepto.de: https://concepto.de/redes-informaticas/

RIVEROS PARAGUAY, J. K. (2019). *IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD INFORMATICA PARA MEJORAR EL ACCESO Y LA SEGURIDAD LOGICA DE LARED EN LA OFICINA DEPARTAMENTAL DE ESTADÍSTICA E INFOMÁTICA DE JUNIN.* HUANCAYO.

ROBERTO, M. P. (2012). *EL PROYECTO EDUCATIVO.* Obtenido de EL PROYECTO EDUCATIVO: http://www.une.edu.pe/Sesion04-Metodologia_de_la_investigacion.pdf

SEAGATE. (s.f.). *QUE ES NAS Y PORQUE ES IMPORTANTE*. Obtenido de QUE ES NAS Y PORQUE ES IMPORTANTE: https://www.seagate.com/la/es/tech-insights/what-is-nas-master-ti/

sites.google. (s.f.). *REDES LOCALES Y GLOBALES.* Obtenido de REDES LOCALES Y GLOBALES: https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes

SOTO, J. (19 de ABRIL de 2015). *HOSTNAME*. Obtenido de HOSTNAME: https://www.hn.pe/blog/que-es-un-datacenter

Systems, L. (17 de Noviembre de 2016). *TRAFFIC ANALYSIS Y COLLECTION*. Obtenido de TRAFFIC ANALYSIS Y COLLECTION: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DuGN6NYFkrh4&psig=AOvVaw1Z120zQ06Hqz6vHN-4jD0P&ust=1589824616978000&source=images&cd=vfe&ved=0CA0QjhxqFwoTCIjqrq-8u-kCFQAAAAAdAAAAABAD

Talius Technology S.L. , Cl. Atenas. (17 de JUNIO de 2019). *Talius Technology*. Obtenido de Talius Technology: https://talius.es/blog/21/sistemas-de-alimentaci%C3%B3n-ininterrumpida-sais.html

Tema Fantástico, S.A.. (9 de Julio de 2010). *ARQUITECTURA DE TELEPROCESO*. Obtenido de ARQUITECTURA DE TELEPROCESO: http://mauroed.blogspot.com/p/arquitectura-de-teleproceso.html

Total Publishing Network S.A. (2008). *El hipervisor Xen mejora la seguridad y reforma su código*. Obtenido de El hipervisor Xen mejora la seguridad y reforma su código: https://www.muylinux.com/2018/07/17/xen-4-11/

UDS Enterprise Team. (9 de NOVIEMBRE de 2018). *OPEN VIRTUALIZATION BLOG*. Obtenido de OPEN VIRTUALIZATION BLOG: https://www.udsenterprise.com/es/blog/2018/11/09/vulnerabilidad-dia-cero-en-virtual-box/

VMware. (2020). *Virtualización*. Obtenido de Virtualización: https://www.vmware.com/latam/solutions/virtualization.html

Walton, A. (s.f.). *ENCAPSULAMIENTO DE DATOS*. Obtenido de ENCAPSULAMIENTO DE DATOS: https://ccnadesdecero.es/encapsulamiento-de-datos-redes/

ZAMORRA, L. J. (2014). *CLUSTER DE SERVIDORES LINUX PARA ALTA DISPONIBILIDAD DE LA INFORMACION.* Cajamarca.

ANEXOS

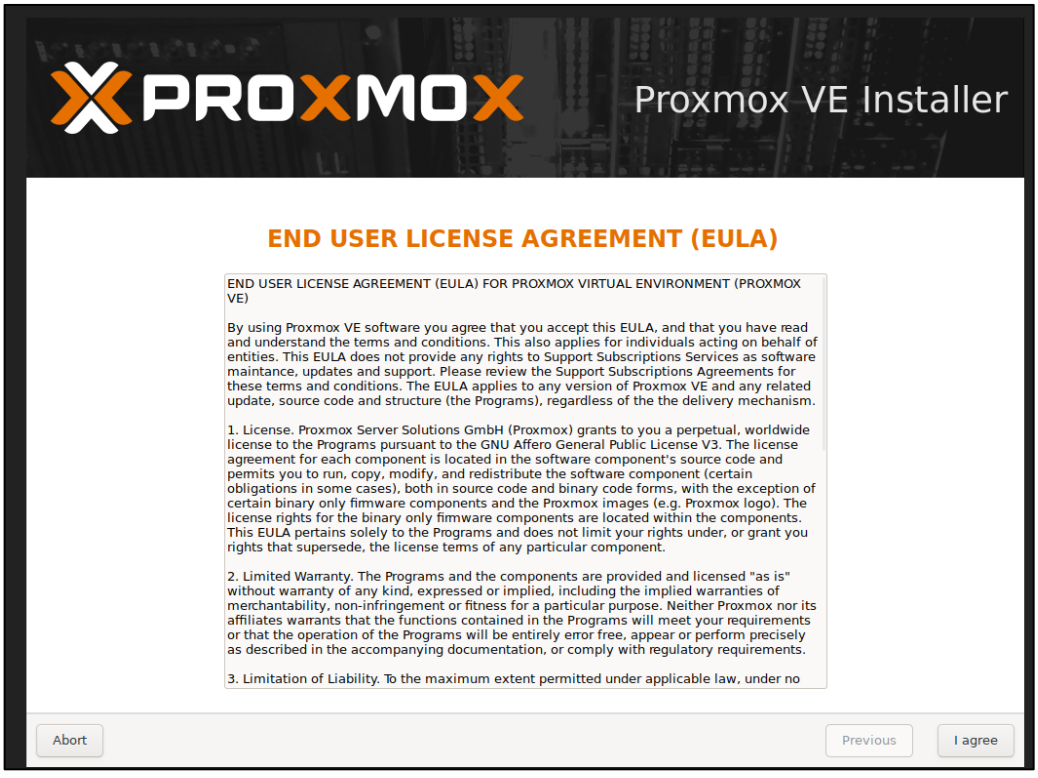
ANEXO 01: MATRIZ DE CONSISTENCIA

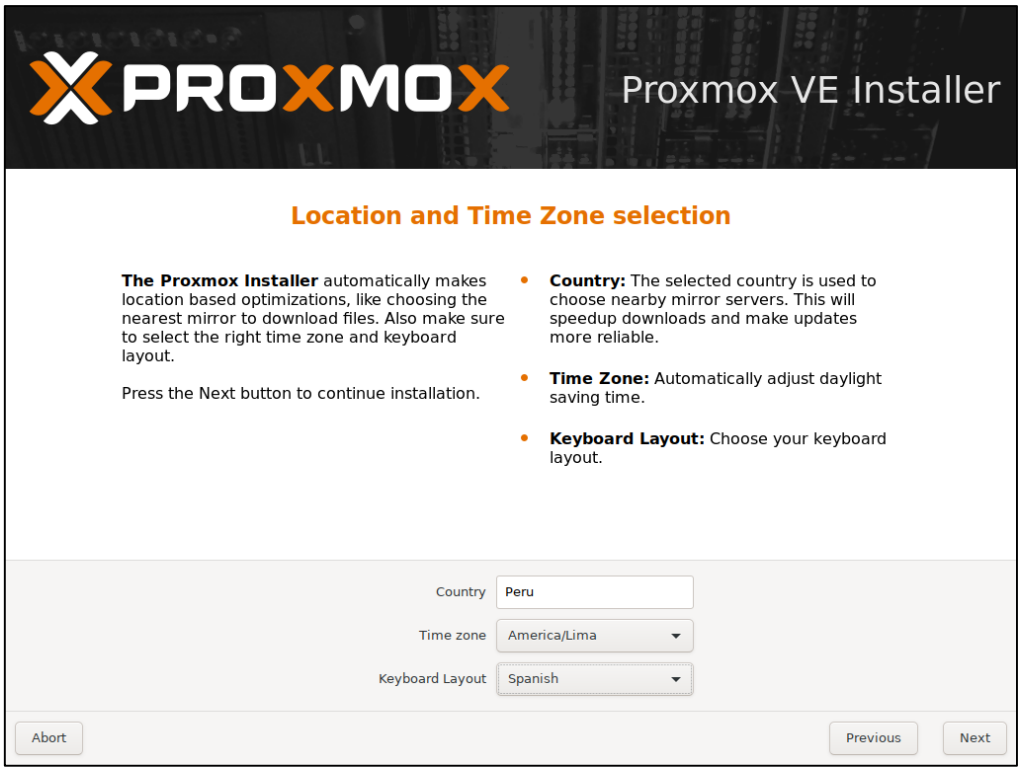
Tabla 19:Matriz de Consistencia

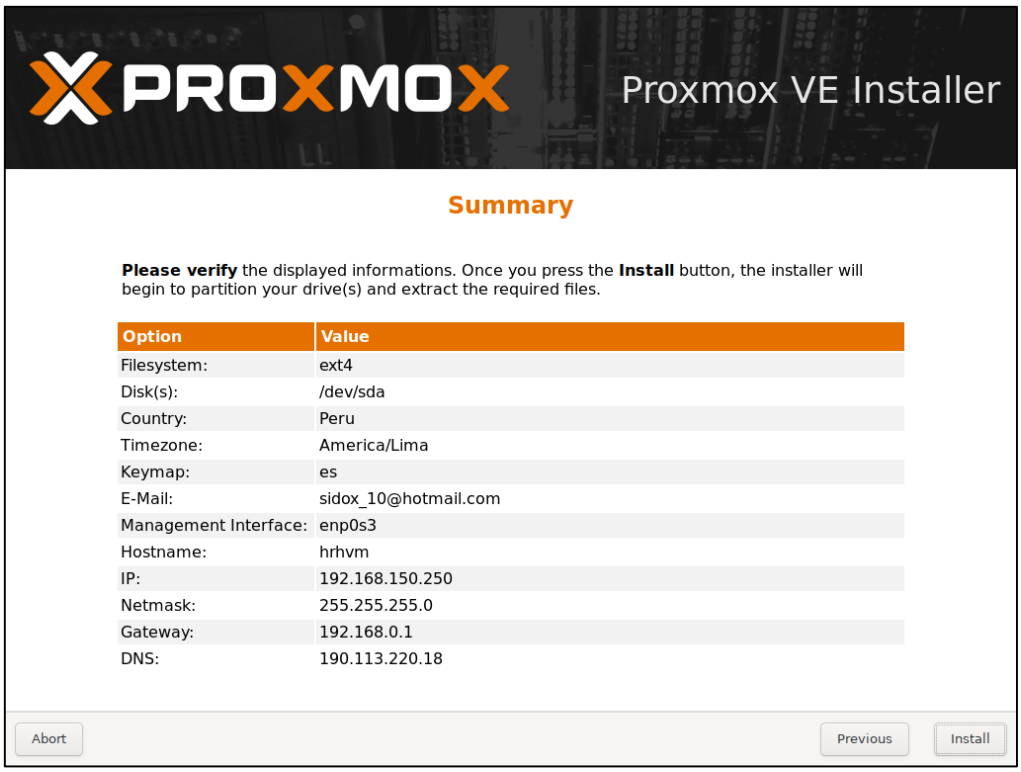
<table>
<tr><th>TITULO</th><th>FORMULACIÓN DEL PROBLEMA</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th>VARIABLES
y = f(x)</th><th>DIMENSIONES</th><th>INDICADORES</th><th>DISEÑO DE LA INVESTIGACIÓN</th></tr>
<tr><td rowspan="2">"Implementacion de una infraestructura tecnologica de servidores para mejorar la seguridad y disponibilidad de los sistemas informaticos en el Hospital Regional Hermilio Valdizan Medrano (HRHVM)"</td><td rowspan="2">¿De que manera influira la implementacion de una infraestructura tecnologica de servidores para mejorar la seguridad y la disponibilidad de los sistemas informaticos en el Hospital Regional Hermilio Valdizan Medrano (HRHVM)?</td><td>OBJETIVO GENERAL:</td><td>HIPOTESIS PRINCIPAL:</td><td colspan="3">VARIABLE DEPENDIENTE (y):</td><td rowspan="15">El diseño de la investigacion es No experimental transversal-descriptivo</td></tr>
<tr><td>Implementar la infraestructura tecnologica de servidores para mejorar la seguridad y la disponibilidad de los sistemas informaticos en el Hospital Regional Hermilio Valdizan Medrano (HRHVM)</td><td>La infraestructura tecnologica de servidores, mejorará la seguridad y la disponibilidad de los sistemas informaticos en el Hospital Regional Hermilio Valdizan Medrano (HRHVM)</td><td rowspan="5">Mejorar la seguridad y la disponibilidad de los sistemas informaticos</td><td>Confidencialidad</td><td>% usuarios desconocidos accediendo a los servidores</td></tr>
<tr><td>Irrefutable</td><td>% de de visitas a paginas web que no compete con el trabajo</td></tr>
<tr><td>Integridad</td><td>% de usuarios no autorizados que realizan cambios en el sistema</td></tr>
<tr><td rowspan="2">Disponibilidad</td><td>% de caidas de los servidores</td></tr>
<tr><td>% de tiempo de respuestas del servidor</td></tr>
<tr><td colspan="2">FORMULACION DE LOS PROBLEMAS ESPECIFICOS</td><td>OBJETIVOS ESPECÍFICOS:</td><td>HIPOTESIS ESPECÍFICAS:</td><td colspan="3">VARIABLE INDEPENDIENTE (x):</td></tr>
<tr><td colspan="2">a) ¿De que manera el analisis de la infraestructura TI del Hospital Regional influira en mejorar la seguridad y disponibilidad de los sistemas informaticos ?</td><td>Analizar la infraestructura TI actual del Hospital Regional Hermilio Valdizan</td><td>El analisis de la infraestructura TI actual del Hospital Regional, influirá en mejorar la seguridad y disponibilidad de los sistemas informaticos</td><td rowspan="4">Implementacion de una infraestructura tecnologica de servidores</td><td>Almacenamiento</td><td>% de consumo del almacenamiento</td></tr>
<tr><td colspan="2">b) ¿Cómo influye el realizar un diseño de una estructura de red mas adecuada para mejorar la seguridad y disponibilidad de los sistemas informaticos ?</td><td>Realizar un diseño de una estructura de red mas adecuada para el Hospital Regional Hermilio Valdizan Medrano</td><td>Realizar el diseño de una estructura de red mas adecuada para el Hospital Regional, mejorará la seguridad y disponiblidad de los sistemas informaticos</td><td>Rendimiento</td><td>% de respuesta a las peticiones de los usuarios</td></tr>
<tr><td colspan="2">c) ¿En que medida la comparacion de los diversos tipos de Hypervisores influira en mejorar la seguridad y disponiblidad de los sistemas informaticos ?</td><td>Comparar los diversos tipos de Hipervisores que se encuentran en el mercado actualmente.</td><td>La comparacion de los diversos tipos de Hipervisores, influirá en mejorar la seguridad y disponibilidad de los sistemas informaticos</td><td>Seguridad</td><td>% de peticiones bloqueadas a los servidores</td></tr>
<tr><td colspan="2">d) ¿De qué manera la implementación de un servidor Firewall, Proxy Squid y Squidguard mejorara la seguridad informática del Hospital Regional Hermilio Valdizan?</td><td>Implementar un Servidor Firewall, Proxy Squid y Squidguard en el Hospital Regional Hermilio Valdizan.</td><td>La implementación de un servidor Firewall, Proxy Squid y Squidguard mejorará la seguridad informática en el HRHVM.</td><td>Accecibilidad</td><td>% de disponibilidad de los servidores</td></tr>
<tr><td colspan="2">e) ¿ Como influye la configuracion bonding e implementacion del servidor NGINX para mejorar la disponibilidad de los sistemas informaticos?</td><td>Implementar un servidor Nginx y realizar la configuracion bonding en el Hospital Regional Hermilio Valdizan</td><td>La implementacion de un servidor Nginx y configuracion bonding, mejorara la seguridad y disponibilidad informatica en el HRHVM</td><td colspan="3">VARIABLE INTERVINIENTE:
Hospital Regional Hermilio Valdizan Medrano (HRHVM)</td></tr>
</table>

Fuente: Elaboración Propia

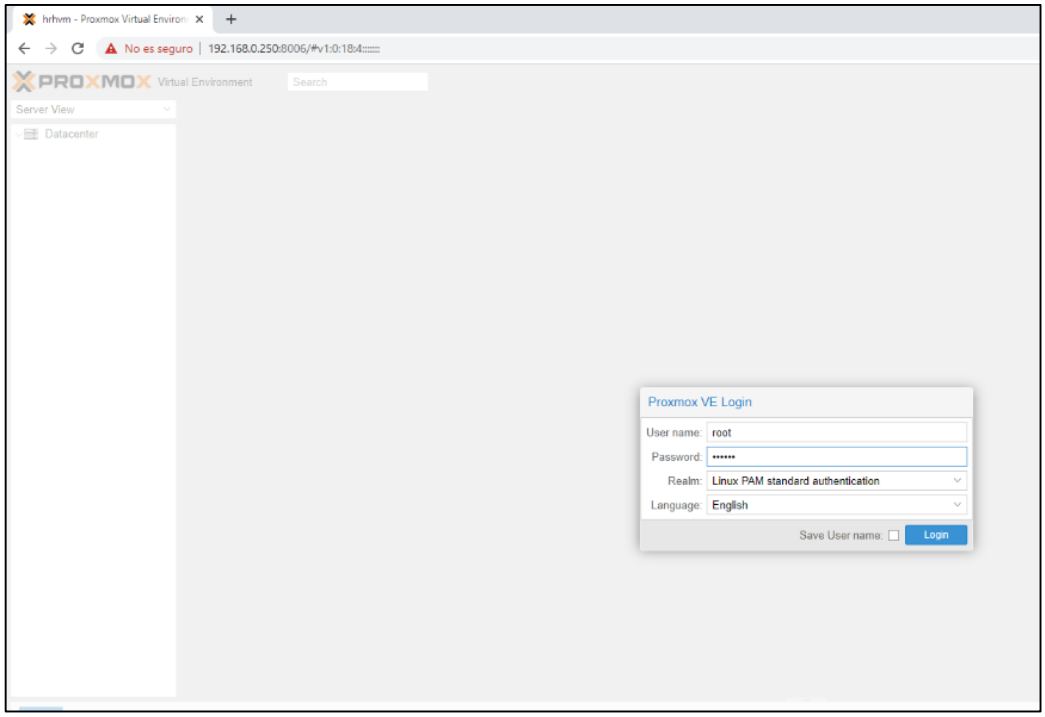
ANEXO 2: INSTALACION DEL PROXMOX VE

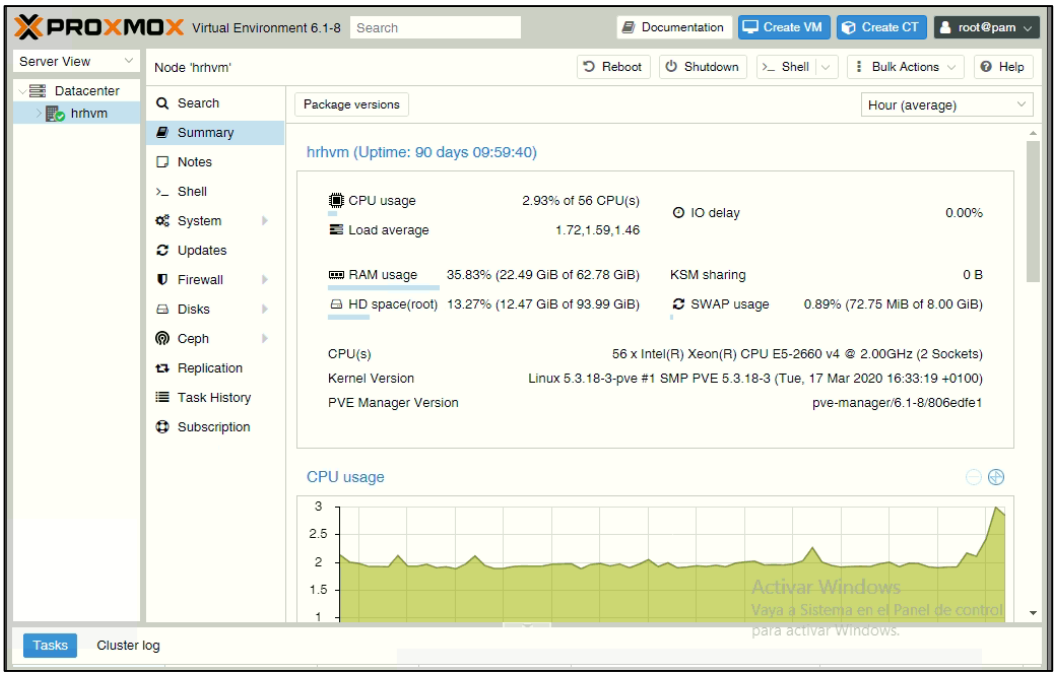


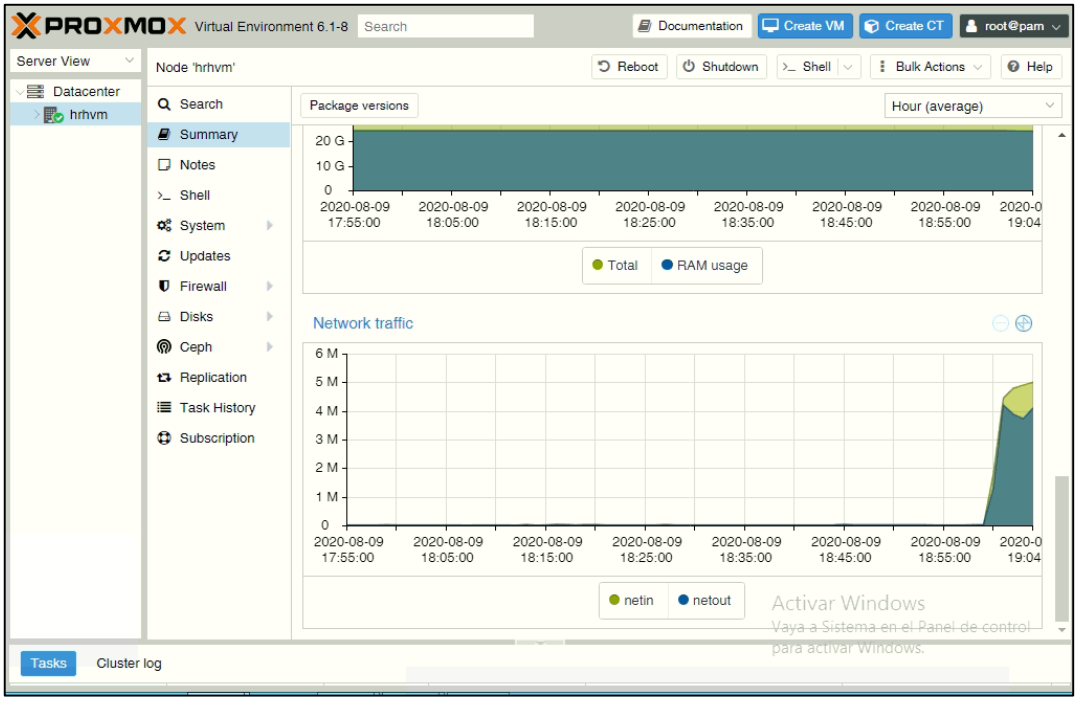

PROXMOX
Proxmox VE Installer
Location and Time Zone selection
The Proxmox Installer automatically makes location based optimizations, like choosing the nearest mirror to download files. Also make sure to select the right time zone and keyboard layout.
Press the Next button to continue installation.
Country: The selected country is used to choose nearby mirror servers. This will speedup downloads and make updates more reliable.
Time Zone: Automatically adjust daylight saving time.
Keyboard Layout: Choose your keyboard layout.
Country
Peru
Time zone
America/Lima
Keyboard Layout
Spanish
Abort
Previous
Next

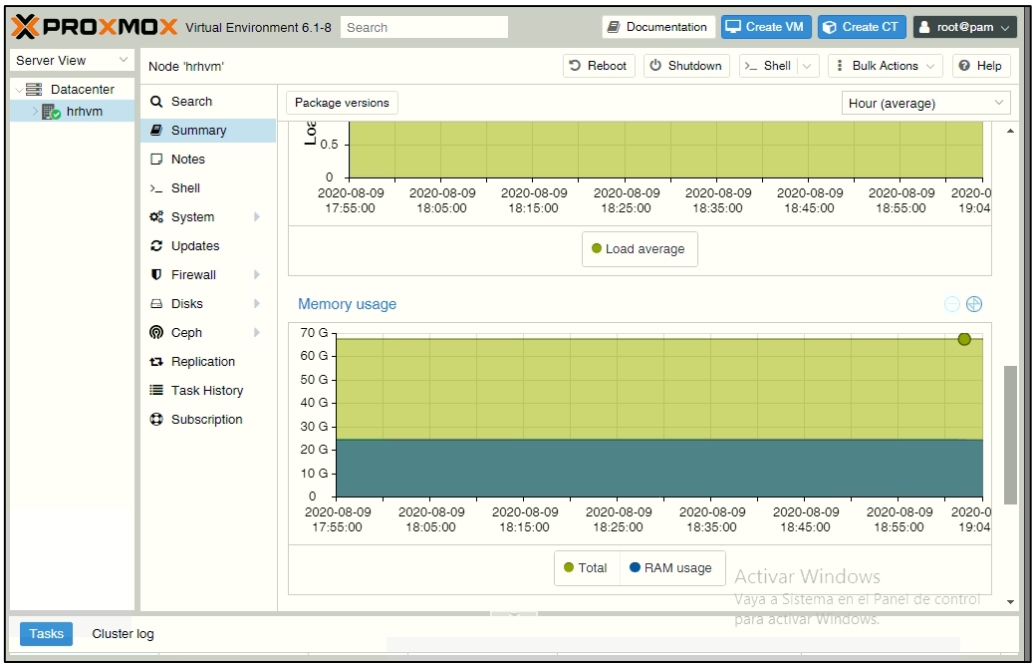

PROXMOX
Proxmox VE Installer
Summary
Please verify the displayed informations. Once you press the Install button, the installer will begin to partition your drive(s) and extract the required files.
Option
Value
Filesystem:
ext4
Disk(s):
/dev/sda
Country:
Peru
Timezone:
America/Lima
Keymap:
es
E-Mail:
sidox_10@hotmail.com
Management Interface:
enp0s3
Hostname:
hrhvm
IP:
192.168.150.250
Netmask:
255.255.255.0
Gateway:
192.168.0.1
DNS:
190.113.220.18
Abort
Previous
Install

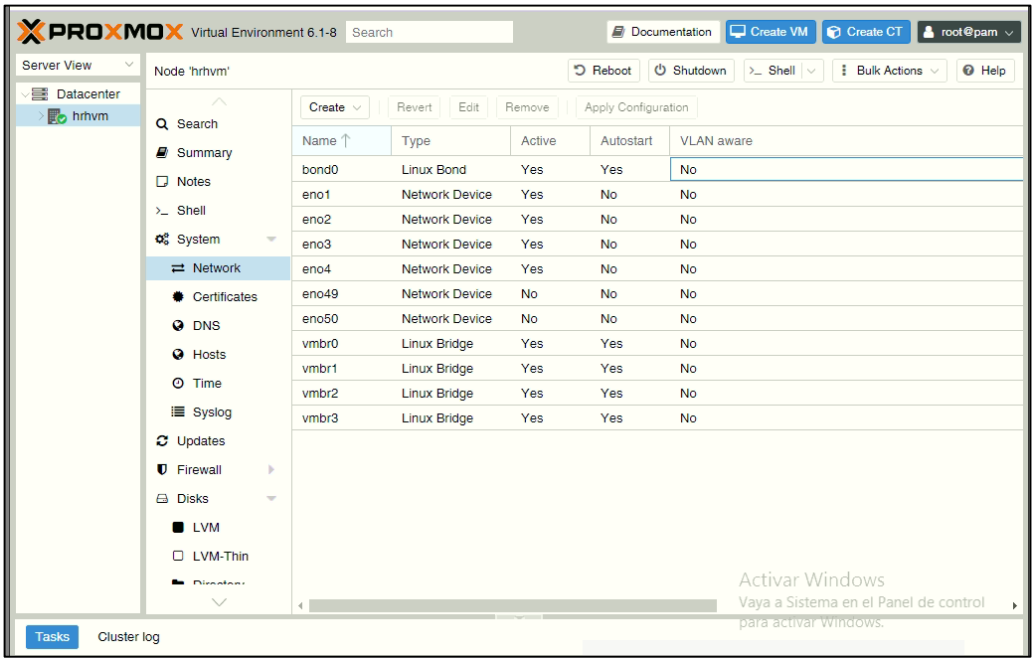
```
--------------------------------------------------------------------------------

Welcome to the Proxmox Virtual Environment. Please use your web browser to
configure this server - connect to:

  https://192.168.150.250:8006/

--------------------------------------------------------------------------------

hrhvm login: root
Password:
Linux hrhvm 5.4.34-1-pve #1 SMP PVE 5.4.34-2 (Thu, 07 May 2020 10:02:02 +0200) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@hrhvm:~# _
```

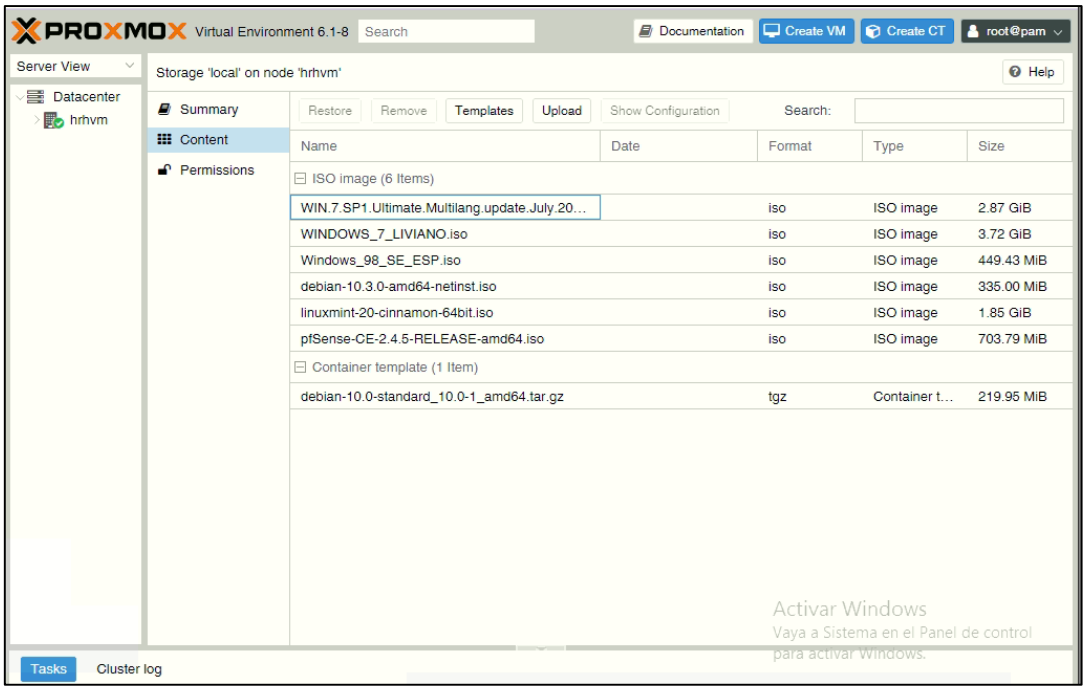



PROXMOX Virtual Environment 6.1-8
Search
Documentation
Create VM
Create CT
root@pam
Server View
Datacenter
hrhvm
Node 'hrhvm'
Reboot
Shutdown
Shell
Bulk Actions
Help
Search
Summary
Notes
Shell
System
Updates
Firewall
Disks
Ceph
Replication
Task History
Subscription
Package versions
Hour (average)
hrhvm (Uptime: 90 days 09:59:40)
CPU usage 2.93% of 56 CPU(s)
Load average 1.72,1.59,1.46
IO delay 0.00%
RAM usage 35.83% (22.49 GiB of 62.78 GiB)
HD space(root) 13.27% (12.47 GiB of 93.99 GiB)
KSM sharing 0 B
SWAP usage 0.89% (72.75 MiB of 8.00 GiB)
CPU(s) 56 x Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz (2 Sockets)
Kernel Version Linux 5.3.18-3-pve #1 SMP PVE 5.3.18-3 (Tue, 17 Mar 2020 16:33:19 +0100)
PVE Manager Version pve-manager/6.1-8/806edfe1
CPU usage
3
2.5
2
1.5
1
Activar Windows
Vaya a Sistema en el Panel de control para activar Windows.
Tasks
Cluster log

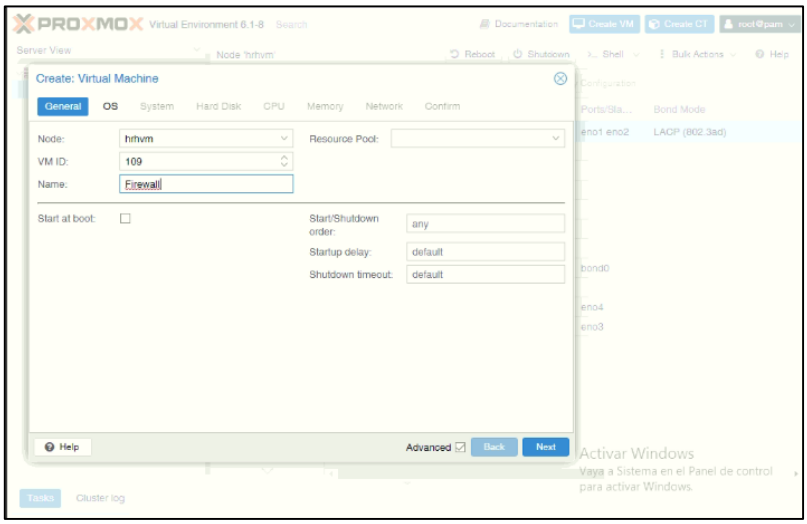

PROXMOX Virtual Environment 6.1-8
Search
Documentation
Create VM
Create CT
root@pam
Server View
Datacenter
hrhvm
Node 'hrhvm'
Reboot
Shutdown
Shell
Bulk Actions
Help
Search
Summary
Notes
Shell
System
Updates
Firewall
Disks
Ceph
Replication
Task History
Subscription
Package versions
Hour (average)
20 G
10 G
0
2020-08-09 17:55:00
2020-08-09 18:05:00
2020-08-09 18:15:00
2020-08-09 18:25:00
2020-08-09 18:35:00
2020-08-09 18:45:00
2020-08-09 18:55:00
2020-0 19:04
Total
RAM usage
Network traffic
6 M
5 M
4 M
3 M
2 M
1 M
0
netin
netout
Activar Windows
Vaya a Sistema en el Panel de control para activar Windows.
Tasks
Cluster log

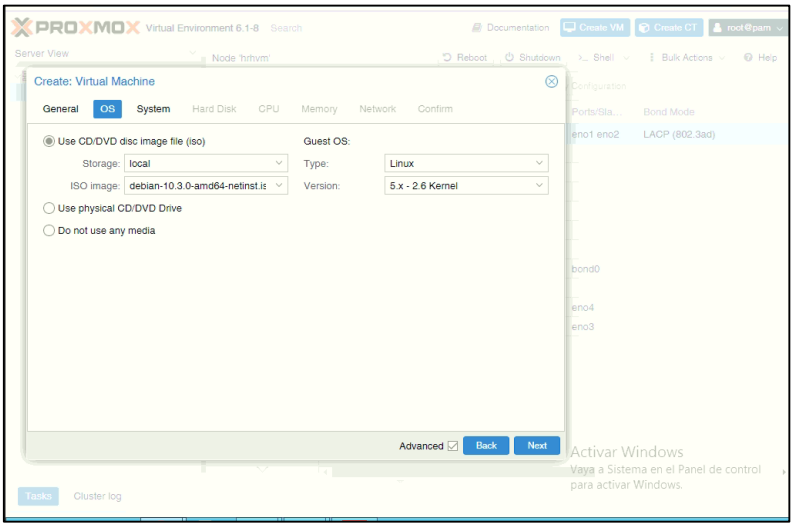

PROXMOX Virtual Environment 6.1-8
Search
Documentation
Create VM
Create CT
root@pam
Server View
Datacenter
hrhvm
Node 'hrhvm'
Reboot
Shutdown
Shell
Bulk Actions
Help
Search
Summary
Notes
Shell
System
Updates
Firewall
Disks
Ceph
Replication
Task History
Subscription
Package versions
Hour (average)
Load average
Memory usage
70 G
60 G
50 G
40 G
30 G
20 G
10 G
0
2020-08-09 17:55:00
2020-08-09 18:05:00
2020-08-09 18:15:00
2020-08-09 18:25:00
2020-08-09 18:35:00
2020-08-09 18:45:00
2020-08-09 18:55:00
Total
RAM usage
Activar Windows
Vaya a Sistema en el Panel de control para activar Windows.
Tasks
Cluster log

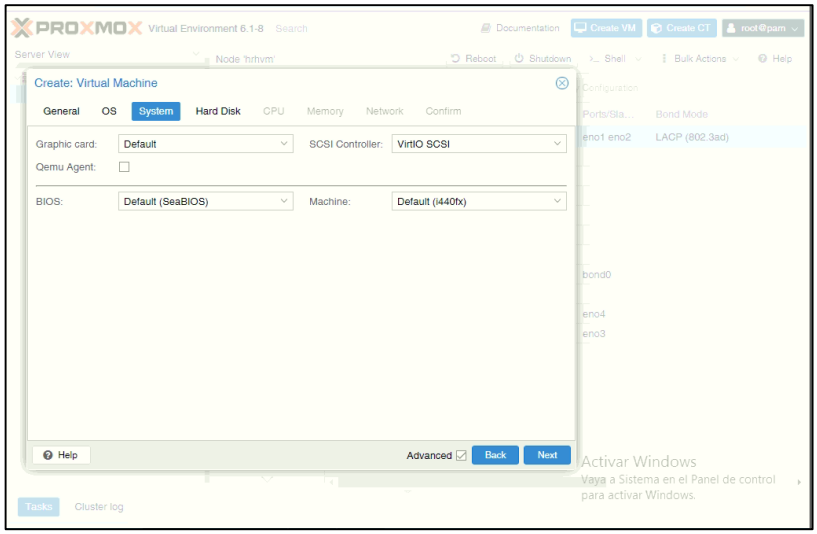

PROXMOX Virtual Environment 6.1-8
Search
Documentation
Create VM
Create CT
root@pam
Server View
Datacenter
hrhvm
Node 'hrhvm'
Reboot
Shutdown
Shell
Bulk Actions
Help
Search
Summary
Notes
Shell
System
Network
Certificates
DNS
Hosts
Time
Syslog
Updates
Firewall
Disks
LVM
LVM-Thin
Create
Revert
Edit
Remove
Apply Configuration
Name
Type
Active
Autostart
VLAN aware
bond0 Linux Bond Yes Yes No
eno1 Network Device Yes No No
eno2 Network Device Yes No No
eno3 Network Device Yes No No
eno4 Network Device Yes No No
eno49 Network Device No No No
eno50 Network Device No No No
vmbr0 Linux Bridge Yes Yes No
vmbr1 Linux Bridge Yes Yes No
vmbr2 Linux Bridge Yes Yes No
vmbr3 Linux Bridge Yes Yes No
Activar Windows
Vaya a Sistema en el Panel de control para activar Windows.
Tasks
Cluster log

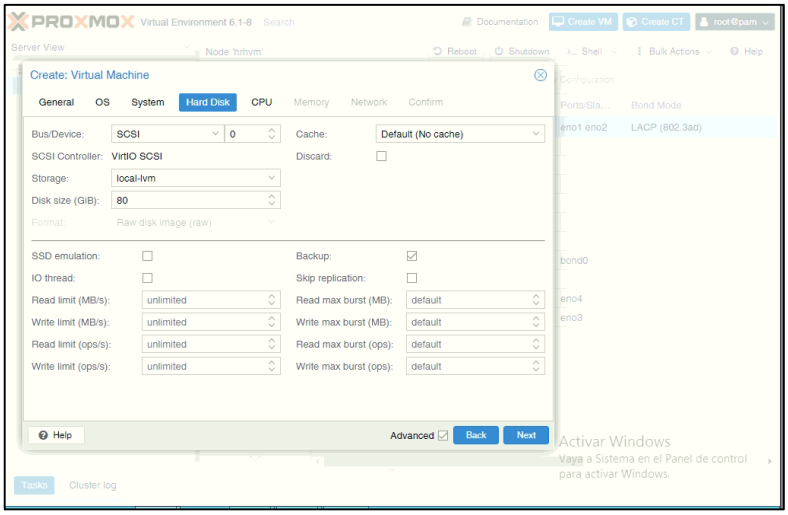

PROXMOX Virtual Environment 6.1-8
Search
Documentation
Create VM
Create CT
root@pam
Server View
Datacenter
hrhvm
Storage 'local' on node 'hrhvm'
Help
Summary
Content
Permissions
Restore
Remove
Templates
Upload
Show Configuration
Search:
Name
Date
Format
Type
Size
ISO image (6 Items)
WIN.7.SP1.Ultimate.Multilang.update.July.20…
iso
ISO image
2.87 GiB
WINDOWS_7_LIVIANO.iso
iso
ISO image
3.72 GiB
Windows_98_SE_ESP.iso
iso
ISO image
449.43 MiB
debian-10.3.0-amd64-netinst.iso
iso
ISO image
335.00 MiB
linuxmint-20-cinnamon-64bit.iso
iso
ISO image
1.85 GiB
pfSense-CE-2.4.5-RELEASE-amd64.iso
iso
ISO image
703.79 MiB
Container template (1 Item)
debian-10.0-standard_10.0-1_amd64.tar.gz
tgz
Container t…
219.95 MiB
Activar Windows
Vaya a Sistema en el Panel de control
para activar Windows.
Tasks
Cluster log

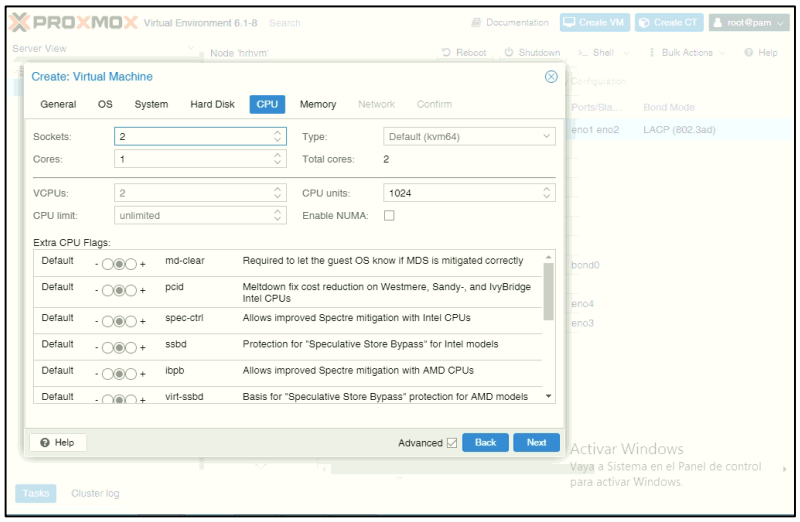
ANEXO 3: IMPLEMENTACION DEL SERVIDOR FIREWALL

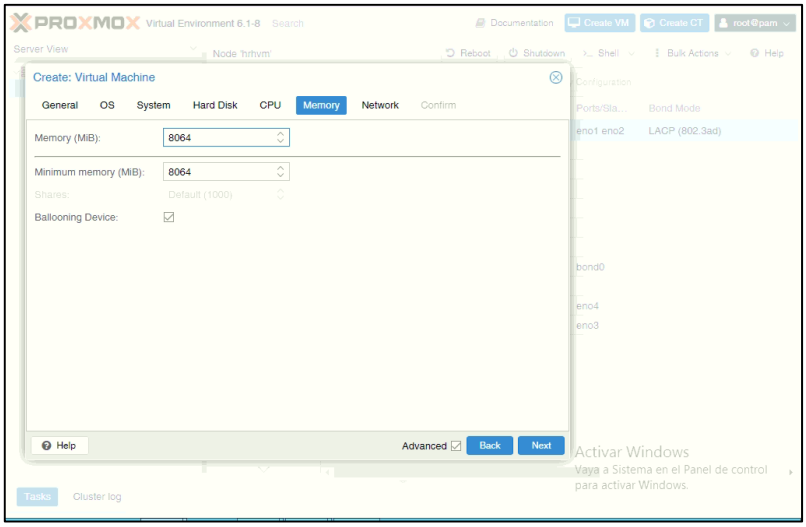


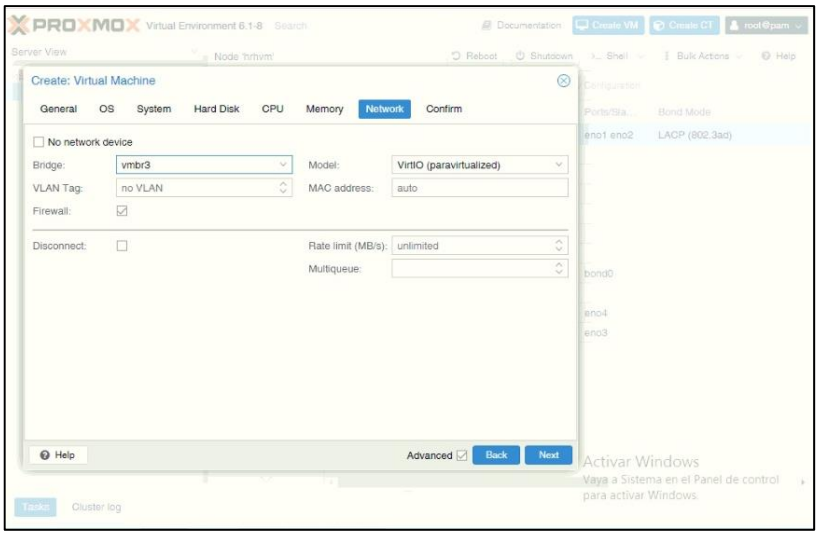


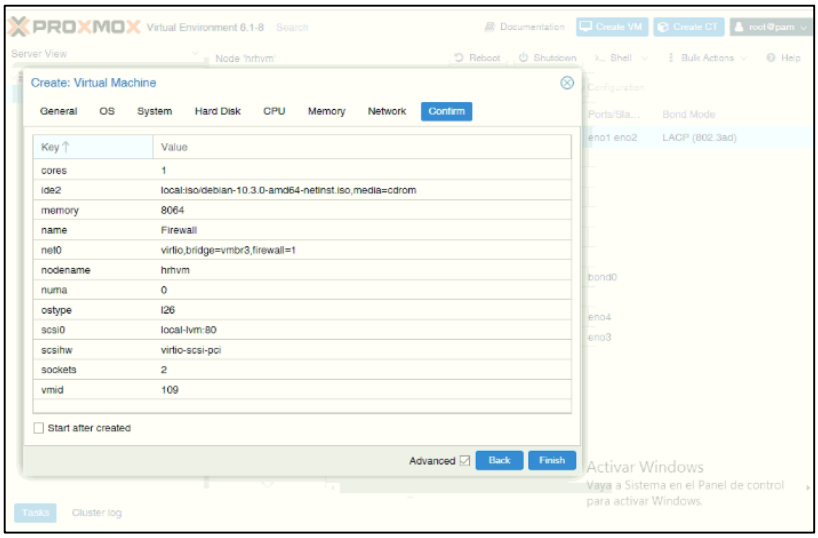


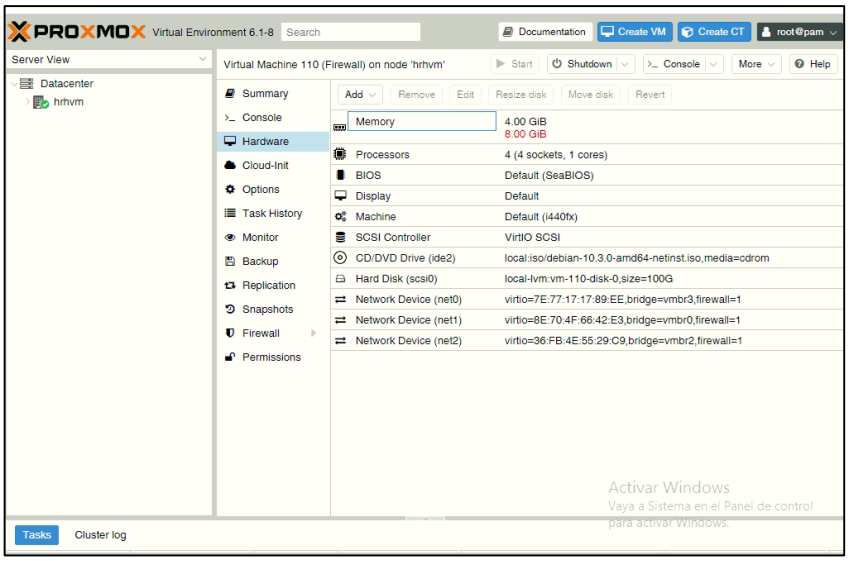

PROXMOX Virtual Environment 6.1-8
Create: Virtual Machine
General OS System Hard Disk CPU Memory Network Confirm
Bus/Device: SCSI 0
SCSI Controller: VirtIO SCSI
Storage: local-lvm
Disk size (GiB): 80
Format: Raw disk image (raw)
Cache: Default (No cache)
Discard:
SSD emulation:
IO thread:
Backup:
Skip replication:
Read limit (MB/s): unlimited
Write limit (MB/s): unlimited
Read limit (ops/s): unlimited
Write limit (ops/s): unlimited
Read max burst (MB): default
Write max burst (MB): default
Read max burst (ops): default
Write max burst (ops): default
Help
Advanced
Back
Next
Activar Windows

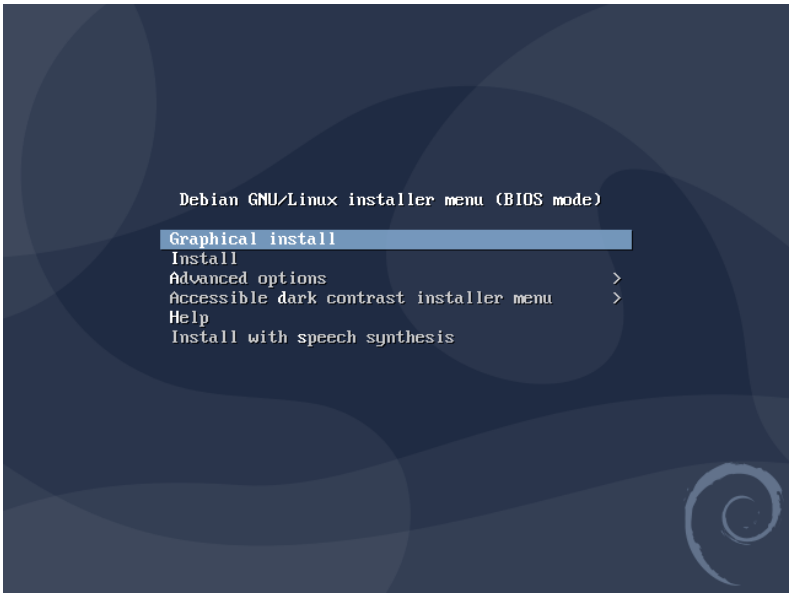

PROXMOX Virtual Environment 6.1-8
Create: Virtual Machine
General OS System Hard Disk CPU Memory Network Confirm
Sockets: 2
Cores: 1
Type: Default (kvm64)
Total cores: 2
VCPUs: 2
CPU limit: unlimited
CPU units: 1024
Enable NUMA:
Extra CPU Flags:
Default md-clear Required to let the guest OS know if MDS is mitigated correctly
Default pcid Meltdown fix cost reduction on Westmere, Sandy-, and IvyBridge Intel CPUs
Default spec-ctrl Allows improved Spectre mitigation with Intel CPUs
Default ssbd Protection for "Speculative Store Bypass" for Intel models
Default ibpb Allows improved Spectre mitigation with AMD CPUs
Default virt-ssbd Basis for "Speculative Store Bypass" protection for AMD models
Help
Advanced
Back
Next
Activar Windows

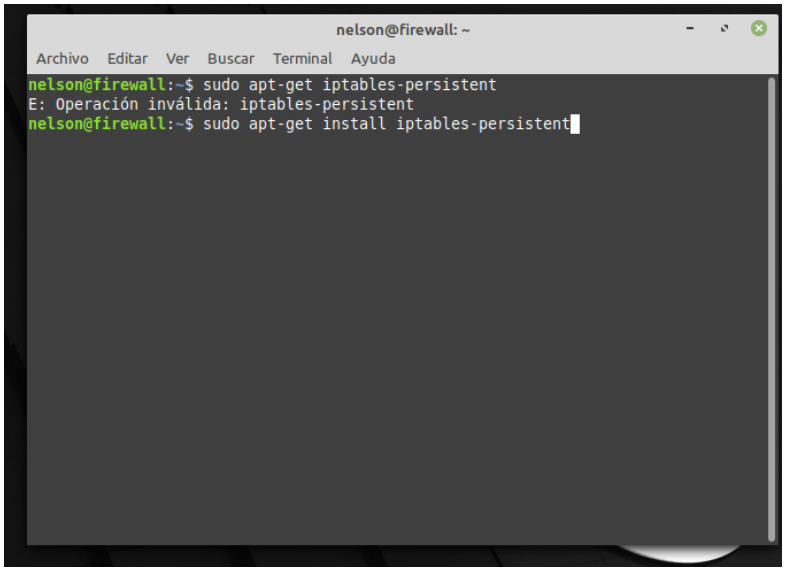

PROXMOX Virtual Environment 6.1-8
Create: Virtual Machine
General OS System Hard Disk CPU Memory Network Confirm
Memory (MiB): 8064
Minimum memory (MiB): 8064
Shares: Default (1000)
Ballooning Device:
Help
Advanced
Back
Next
Activar Windows

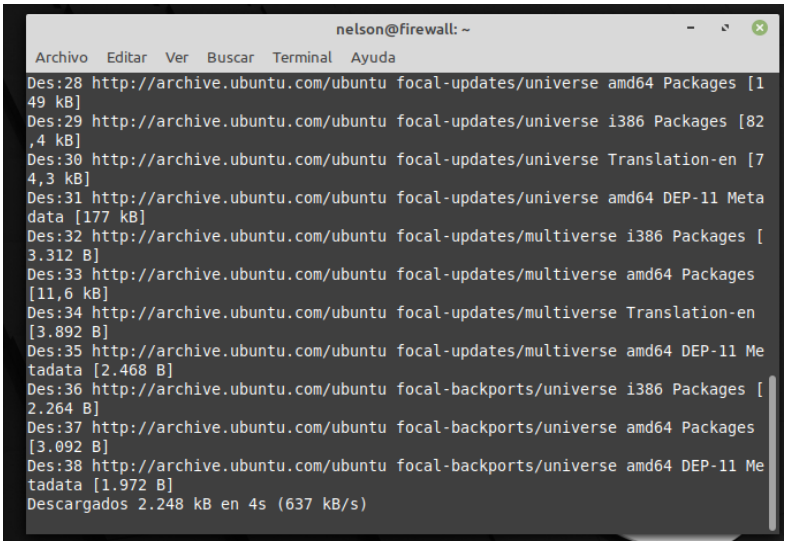

PROXMOX Virtual Environment 6.1-8
Create: Virtual Machine
General OS System Hard Disk CPU Memory Network Confirm
No network device
Bridge: vmbr3
Model: VirtIO (paravirtualized)
VLAN Tag: no VLAN
MAC address: auto
Firewall:
Disconnect:
Rate limit (MB/s): unlimited
Multiqueue:
Help
Advanced
Back
Next
Activar Windows

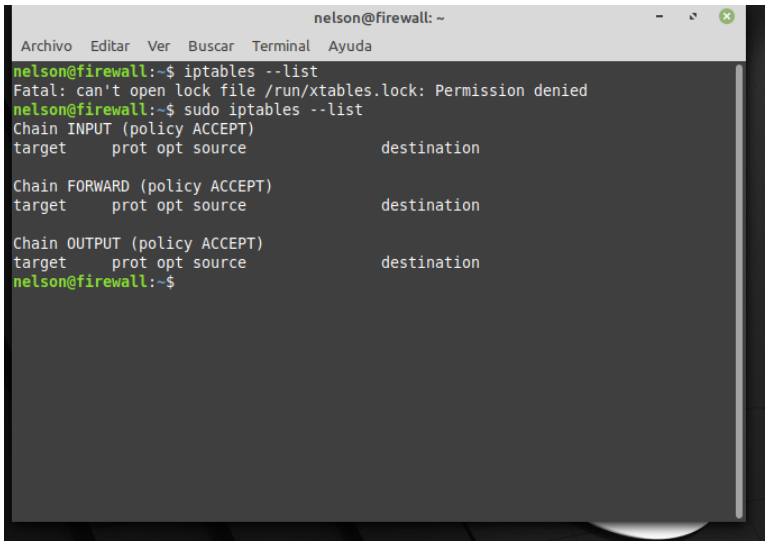

PROXMOX Virtual Environment 6.1-8
Create: Virtual Machine
General OS System Hard Disk CPU Memory Network Confirm
Key
Value
cores 1
ide2 local:iso/debian-10.3.0-amd64-netinst.iso,media=cdrom
memory 8064
name Firewall
net0 virtio,bridge=vmbr3,firewall=1
nodename hrhvm
numa 0
ostype l26
scsi0 local-lvm:80
scsihw virtio-scsi-pci
sockets 2
vmid 109
Start after created
Advanced
Back
Finish
Activar Windows

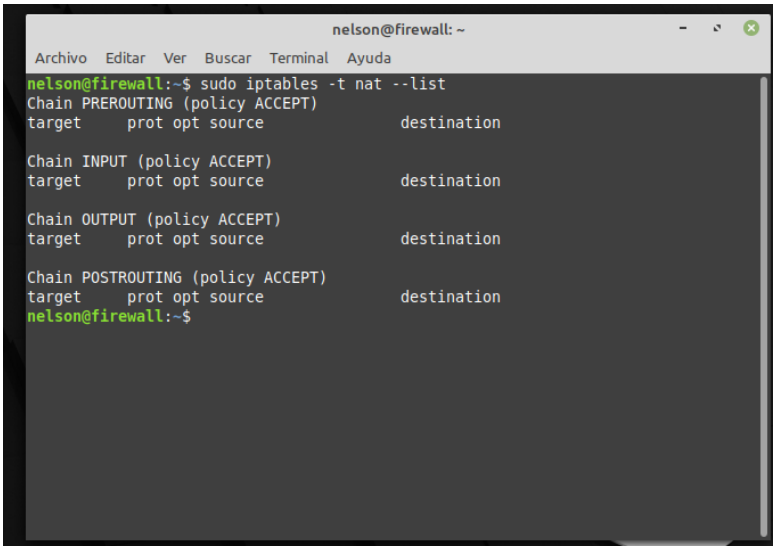

PROXMOX Virtual Environment 6.1-8
Server View
Datacenter
hrhvm
Virtual Machine 110 (Firewall) on node 'hrhvm'
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Backup
Replication
Snapshots
Firewall
Permissions
Memory 4.00 GiB 8.00 GiB
Processors 4 (4 sockets, 1 cores)
BIOS Default (SeaBIOS)
Display Default
Machine Default (i440fx)
SCSI Controller VirtIO SCSI
CD/DVD Drive (ide2) local:iso/debian-10.3.0-amd64-netinst.iso,media=cdrom
Hard Disk (scsi0) local-lvm:vm-110-disk-0,size=100G
Network Device (net0) virtio=7E:77:17:17:89:EE,bridge=vmbr3,firewall=1
Network Device (net1) virtio=8E:70:4F:66:42:E3,bridge=vmbr0,firewall=1
Network Device (net2) virtio=36:FB:4E:55:29:C9,bridge=vmbr2,firewall=1
Tasks
Cluster log
Activar Windows

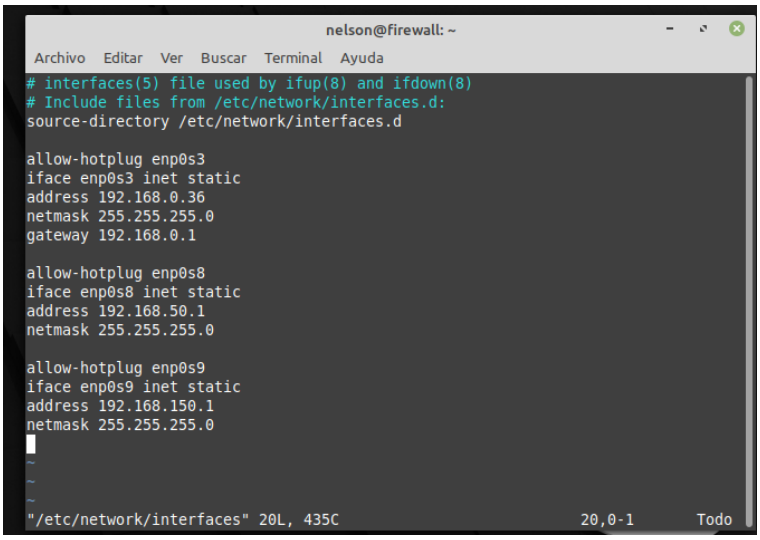

Debian GNU/Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options >
Accessible dark contrast installer menu >
Help
Install with speech synthesis


nelson@firewall: ~
Archivo Editar Ver Buscar Terminal Ayuda
nelson@firewall:~$ sudo apt-get iptables-persistent
E: Operación inválida: iptables-persistent
nelson@firewall:~$ sudo apt-get install iptables-persistent


nelson@firewall: ~
Archivo Editar Ver Buscar Terminal Ayuda
Des:28 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [1
49 kB]
Des:29 http://archive.ubuntu.com/ubuntu focal-updates/universe i386 Packages [82
,4 kB]
Des:30 http://archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [7
4,3 kB]
Des:31 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Meta
data [177 kB]
Des:32 http://archive.ubuntu.com/ubuntu focal-updates/multiverse i386 Packages [
3.312 B]
Des:33 http://archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages
[11,6 kB]
Des:34 http://archive.ubuntu.com/ubuntu focal-updates/multiverse Translation-en
[3.892 B]
Des:35 http://archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 Me
tadata [2.468 B]
Des:36 http://archive.ubuntu.com/ubuntu focal-backports/universe i386 Packages [
2.264 B]
Des:37 http://archive.ubuntu.com/ubuntu focal-backports/universe amd64 Packages
[3.092 B]
Des:38 http://archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11 Me
tadata [1.972 B]
Descargados 2.248 kB en 4s (637 kB/s)


nelson@firewall: ~
Archivo Editar Ver Buscar Terminal Ayuda
nelson@firewall:~$ iptables --list
Fatal: can't open lock file /run/xtables.lock: Permission denied
nelson@firewall:~$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
nelson@firewall:~$


nelson@firewall: ~
Archivo Editar Ver Buscar Terminal Ayuda
nelson@firewall:~$ sudo iptables -t nat --list
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
nelson@firewall:~$

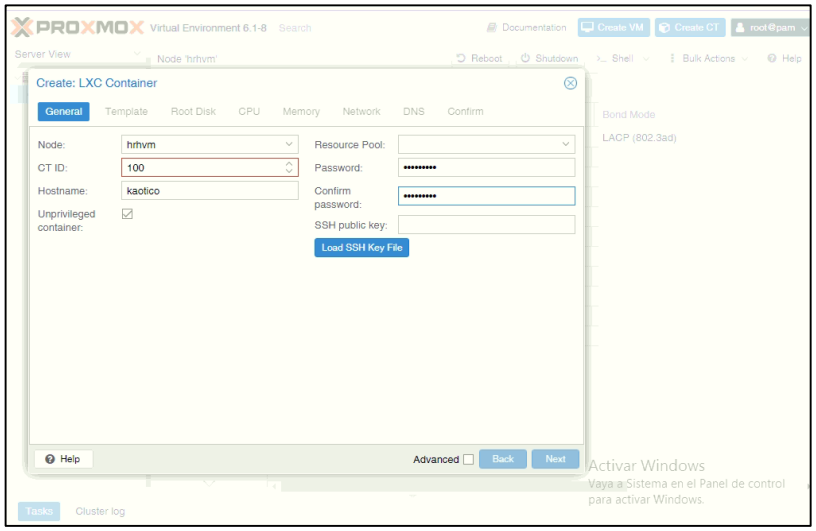

nelson@firewall: ~
Archivo Editar Ver Buscar Terminal Ayuda
interfaces(5) file used by ifup(8) and ifdown(8)
Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.0.36
netmask 255.255.255.0
gateway 192.168.0.1
allow-hotplug enp0s8
iface enp0s8 inet static
address 192.168.50.1
netmask 255.255.255.0
allow-hotplug enp0s9
iface enp0s9 inet static
address 192.168.150.1
netmask 255.255.255.0
"/etc/network/interfaces" 20L, 435C 20,0-1 Todo

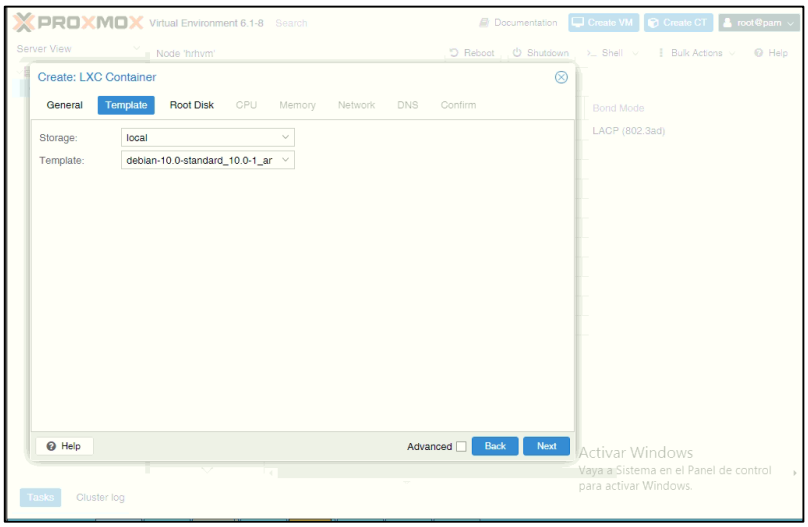
root@firewall: /

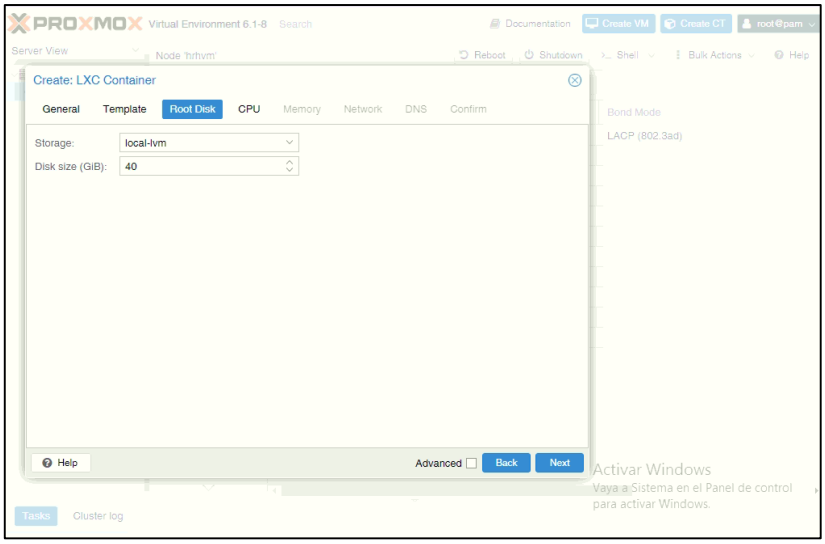
Archivo Editar Ver Buscar Terminal Ayuda

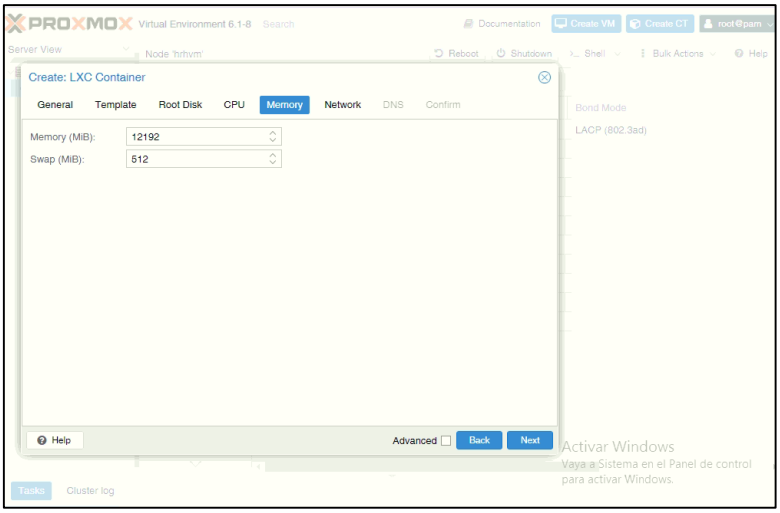
```
#!/bin/sh

#Limpia tabla
iptables -F
iptables -X
iptables -Z

#limpiamos tabla nat
iptables -t nat -F
iptables -t nat -X

#DROP OR ACCEPT
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

#BIT FORWARDING
echo 1 > /proc/sys/net/ipv4/ip_forward

#PERMITIR TRAFICO POR SSH
iptables -A INPUT -i enp0s3 -p tcp -s 192.168.0.3/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o enp0s3 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

#PERMITIR TRAFICO ENTRANTE HTTP Y HTTPS
iptables -A INPUT -i enp0s3 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o enp0s3 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -i enp0s3 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o enp0s3 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT

#PERMITIR SALIDA DE TRAFICO HTTP Y HTTPS
iptables -A OUTPUT -o enp0s3 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i enp0s3 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o enp0s3 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i enp0s3 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT


#PERMITIR PING DESDE EL EXTERIOR
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
                                                                                1,1           Comienzo
```

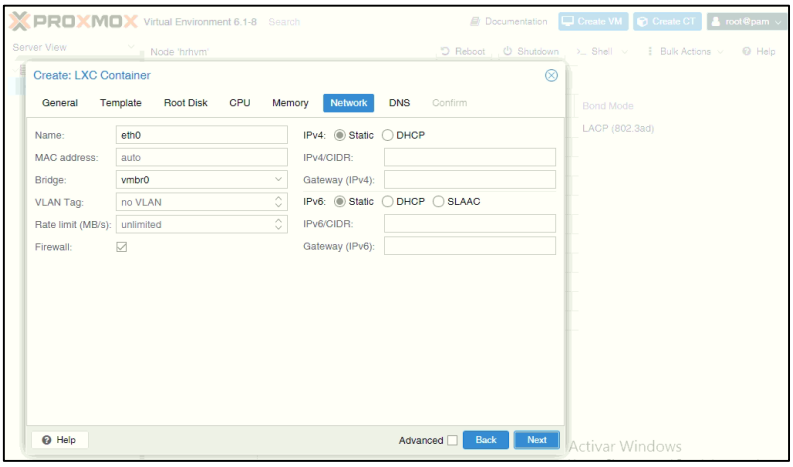
ANEXO 4: IMPLEMENTACION DE LOS SERVIDORES WEB Y BBDD

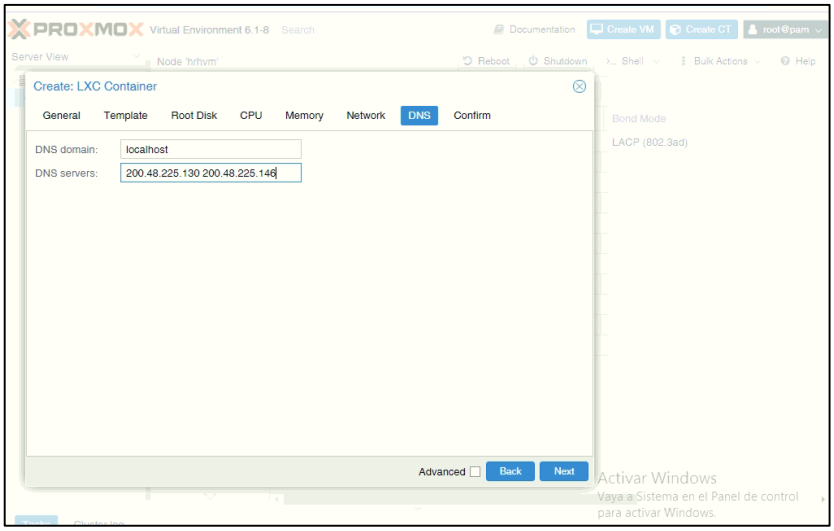


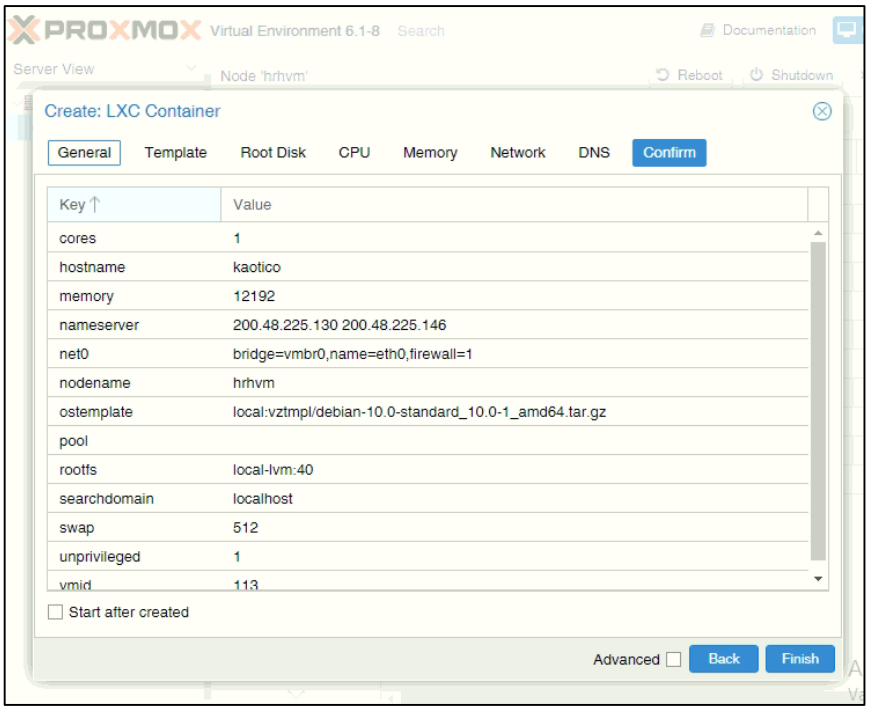


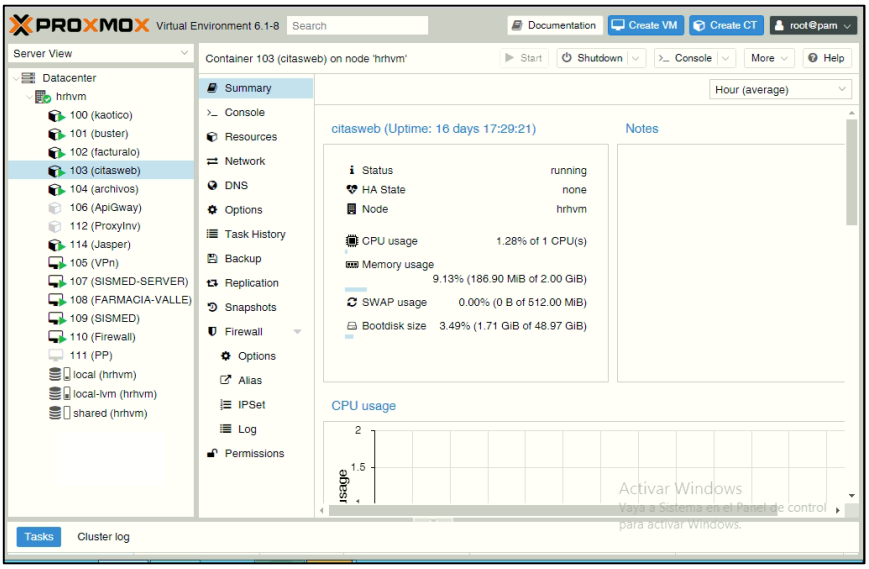


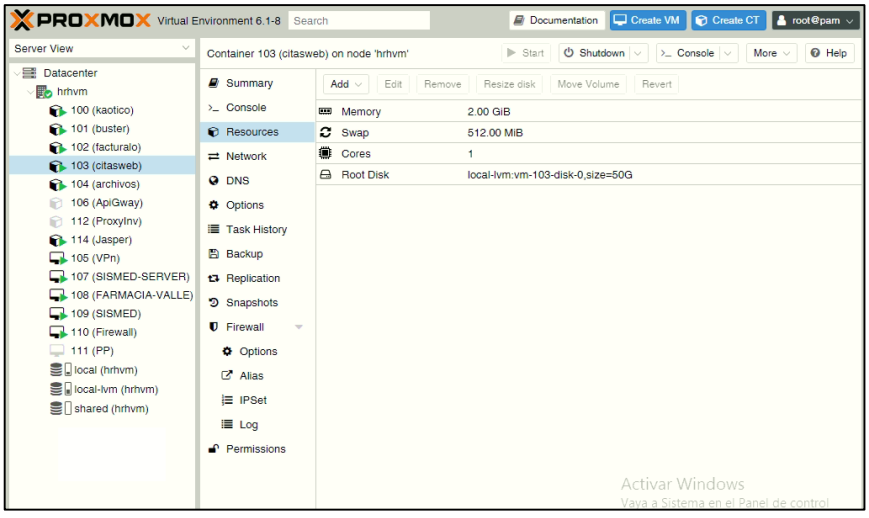

PROXMOX Virtual Environment 6.1-8
Create: LXC Container
General
Template
Root Disk
CPU
Memory
Network
DNS
Confirm
Memory (MiB): 12192
Swap (MiB): 512
Help
Advanced
Back
Next
Activar Windows

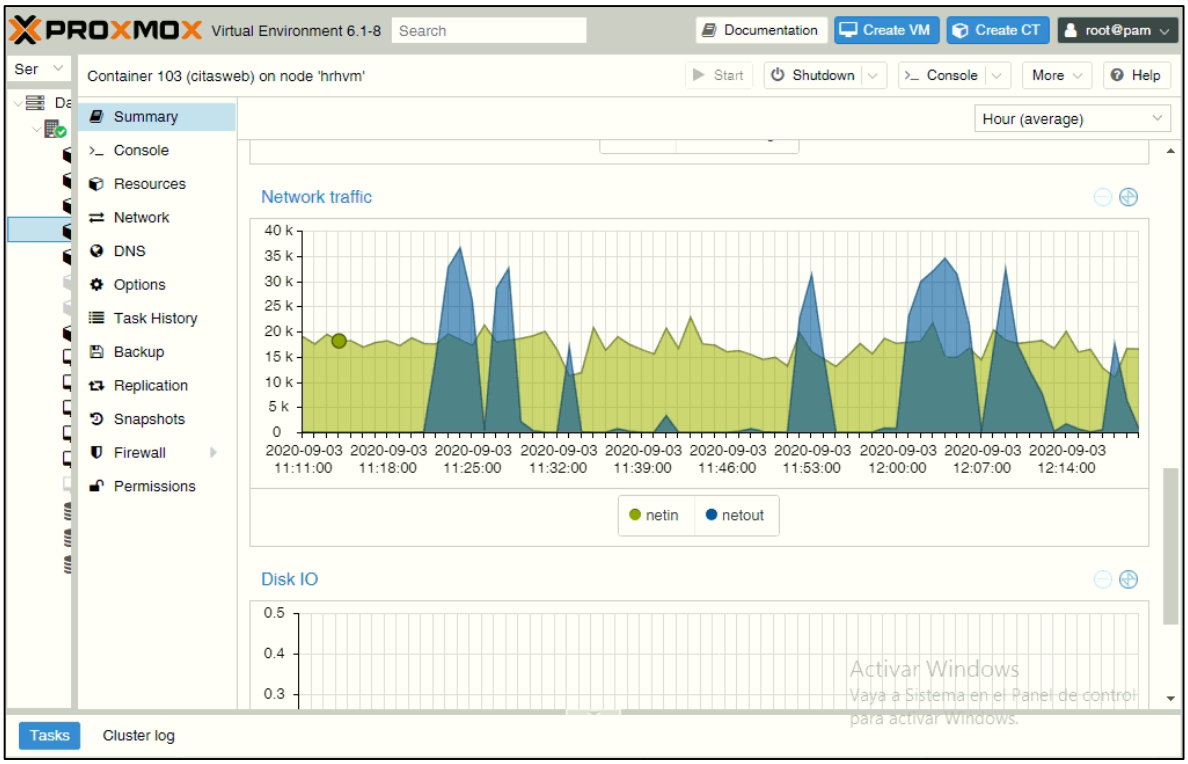

PROXMOX Virtual Environment 6.1-8
Create: LXC Container
General
Template
Root Disk
CPU
Memory
Network
DNS
Confirm
Name: eth0
MAC address: auto
Bridge: vmbr0
VLAN Tag: no VLAN
Rate limit (MB/s): unlimited
Firewall:
IPv4: Static DHCP
IPv4/CIDR:
Gateway (IPv4):
IPv6: Static DHCP SLAAC
IPv6/CIDR:
Gateway (IPv6):
Help
Advanced
Back
Next
Activar Windows


PROXMOX Virtual Environment 6.1-8
Create: LXC Container
General
Template
Root Disk
CPU
Memory
Network
DNS
Confirm
DNS domain: localhost
DNS servers: 200.48.225.130 200.48.225.146
Advanced
Back
Next
Activar Windows

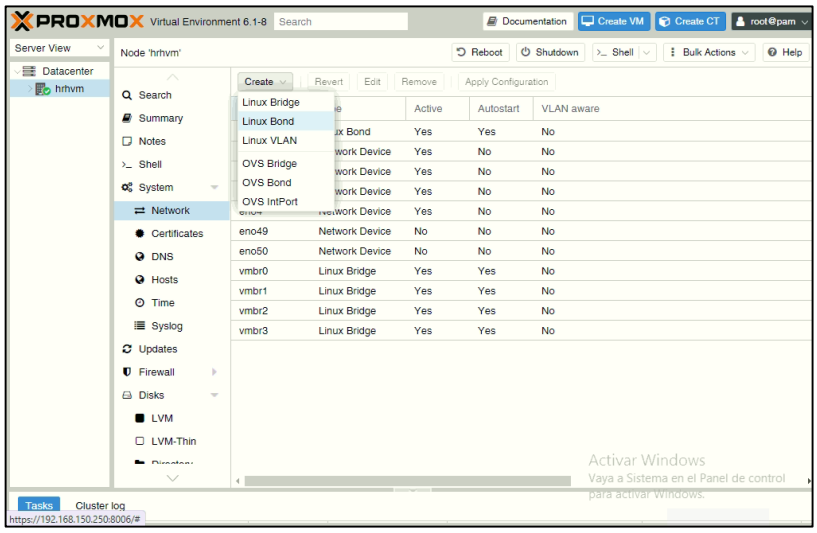

PROXMOX Virtual Environment 6.1-8
Search
Documentation
Server View
Node 'hrhvm'
Reboot
Shutdown
Create: LXC Container
General
Template
Root Disk
CPU
Memory
Network
DNS
Confirm
Key
Value
cores 1
hostname kaotico
memory 12192
nameserver 200.48.225.130 200.48.225.146
net0 bridge=vmbr0,name=eth0,firewall=1
nodename hrhvm
ostemplate local:vztmpl/debian-10.0-standard_10.0-1_amd64.tar.gz
pool
rootfs local-lvm:40
searchdomain localhost
swap 512
unprivileged 1
vmid 113
Start after created
Advanced
Back
Finish

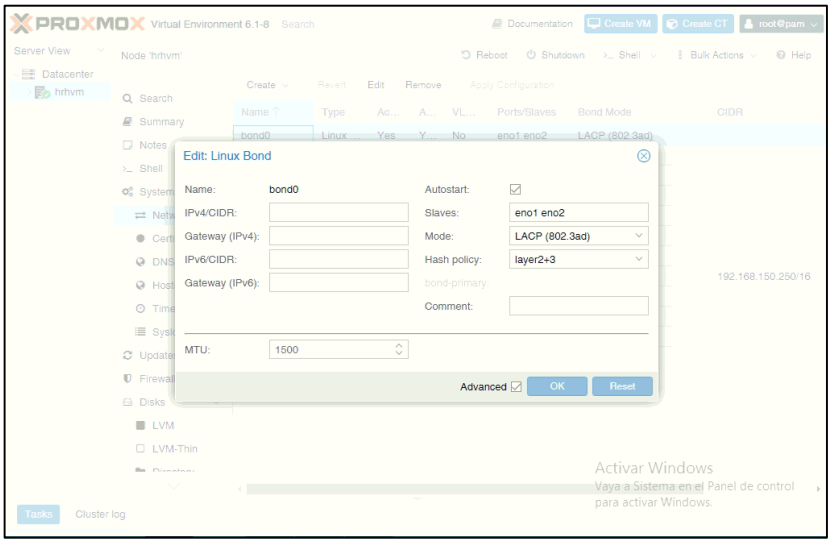

PROXMOX Virtual Environment 6.1-8
Search
Documentation
Create VM
Create CT
root@pam
Server View
Container 103 (citasweb) on node 'hrhvm'
Start
Shutdown
Console
More
Help
Datacenter
hrhvm
100 (kaotico)
101 (buster)
102 (facturalo)
103 (citasweb)
104 (archivos)
106 (ApiGway)
112 (ProxyInv)
114 (Jasper)
105 (VPn)
107 (SISMED-SERVER)
108 (FARMACIA-VALLE)
109 (SISMED)
110 (Firewall)
111 (PP)
local (hrhvm)
local-lvm (hrhvm)
shared (hrhvm)
Summary
Console
Resources
Network
DNS
Options
Task History
Backup
Replication
Snapshots
Firewall
Options
Alias
IPSet
Log
Permissions
Hour (average)
citasweb (Uptime: 16 days 17:29:21)
Notes
Status running
HA State none
Node hrhvm
CPU usage 1.28% of 1 CPU(s)
Memory usage 9.13% (186.90 MiB of 2.00 GiB)
SWAP usage 0.00% (0 B of 512.00 MiB)
Bootdisk size 3.49% (1.71 GiB of 48.97 GiB)
CPU usage
Activar Windows
Tasks
Cluster log

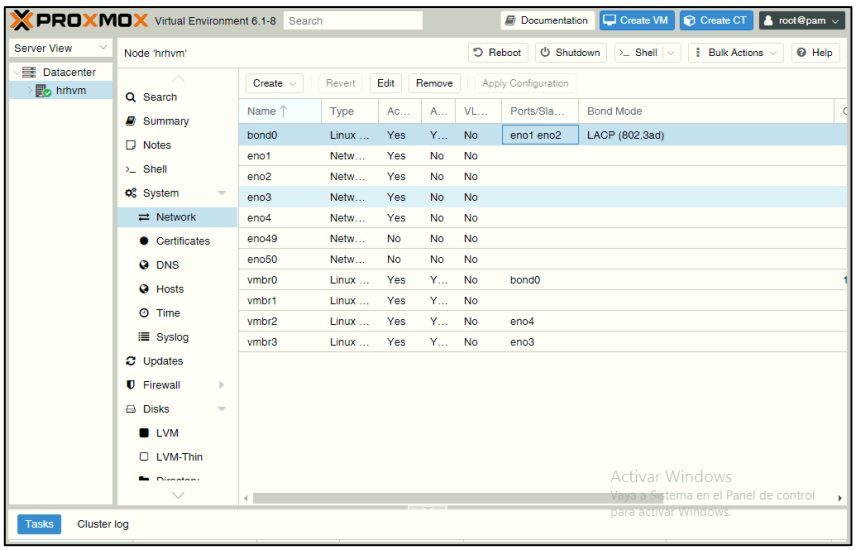

PROXMOX Virtual Environment 6.1-8
Search
Documentation
Create VM
Create CT
root@pam
Server View
Container 103 (citasweb) on node 'hrhvm'
Start
Shutdown
Console
More
Help
Datacenter
hrhvm
100 (kaotico)
101 (buster)
102 (facturalo)
103 (citasweb)
104 (archivos)
106 (ApiGway)
112 (ProxyInv)
114 (Jasper)
105 (VPn)
107 (SISMED-SERVER)
108 (FARMACIA-VALLE)
109 (SISMED)
110 (Firewall)
111 (PP)
local (hrhvm)
local-lvm (hrhvm)
shared (hrhvm)
Summary
Console
Resources
Network
DNS
Options
Task History
Backup
Replication
Snapshots
Firewall
Options
Alias
IPSet
Log
Permissions
Add
Edit
Remove
Resize disk
Move Volume
Revert
Memory 2.00 GiB
Swap 512.00 MiB
Cores 1
Root Disk local-lvm:vm-103-disk-0,size=50G
Activar Windows


PROXMOX Virtual Environment 6.1-8
Search
Documentation
Create VM
Create CT
root@pam
Container 103 (citasweb) on node 'hrhvm'
Start
Shutdown
Console
More
Help
Summary
Console
Resources
Network
DNS
Options
Task History
Backup
Replication
Snapshots
Firewall
Permissions
Hour (average)
Network traffic
40 k
35 k
30 k
25 k
20 k
15 k
10 k
5 k
0
2020-09-03 11:11:00
2020-09-03 11:18:00
2020-09-03 11:25:00
2020-09-03 11:32:00
2020-09-03 11:39:00
2020-09-03 11:46:00
2020-09-03 11:53:00
2020-09-03 12:00:00
2020-09-03 12:07:00
2020-09-03 12:14:00
netin
netout
Disk IO
0.5
0.4
0.3
Activar Windows
Vaya a Sistema en el Panel de control para activar Windows.
Tasks
Cluster log

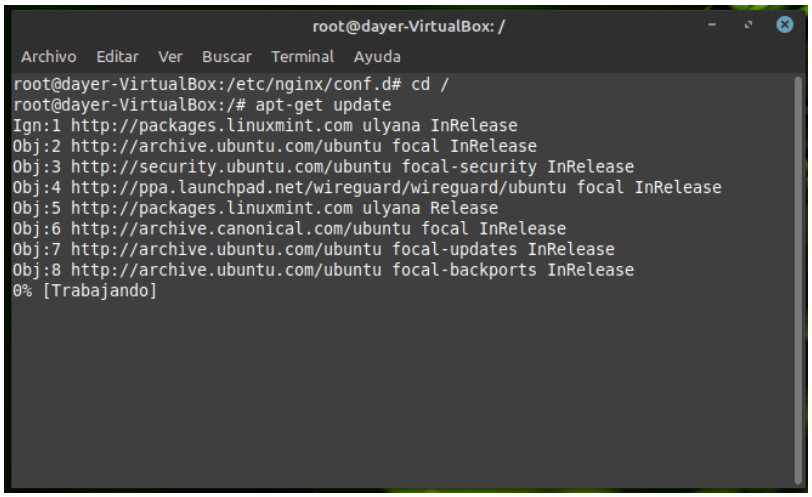
ANEXO 5: CONFIGURACION DEL BONDING

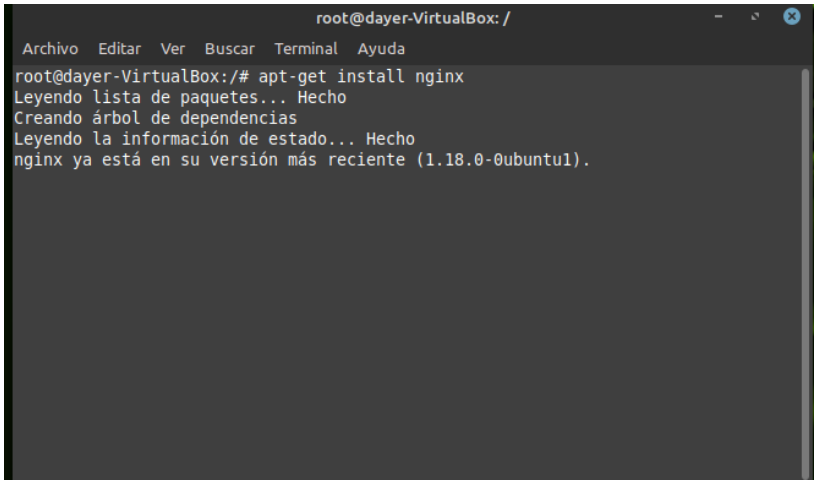


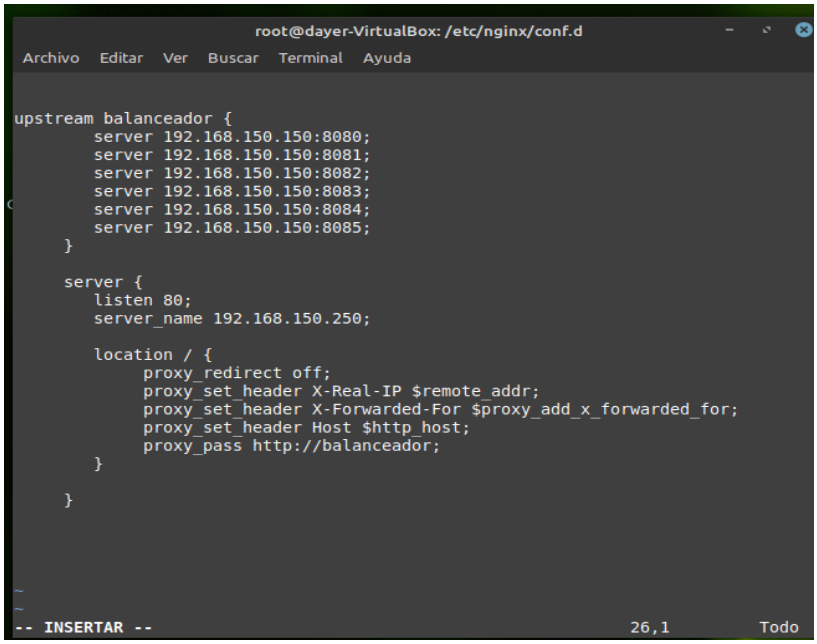


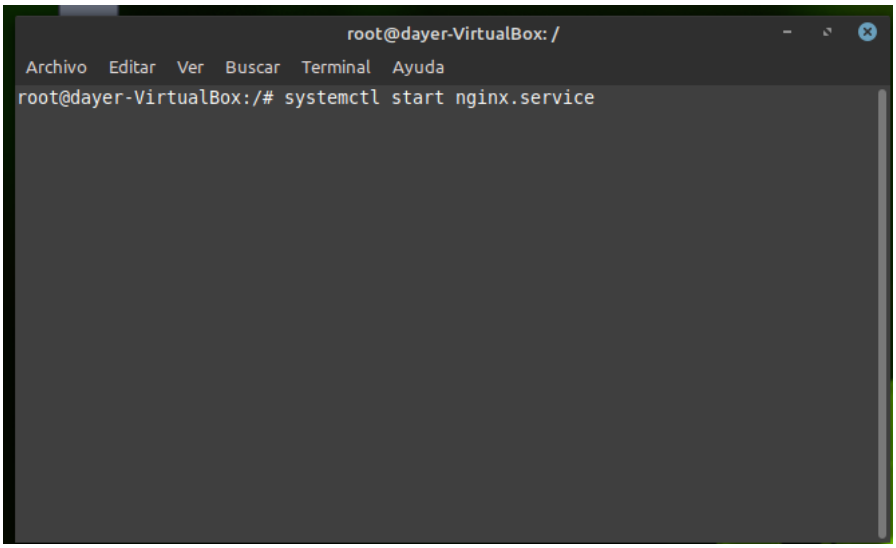


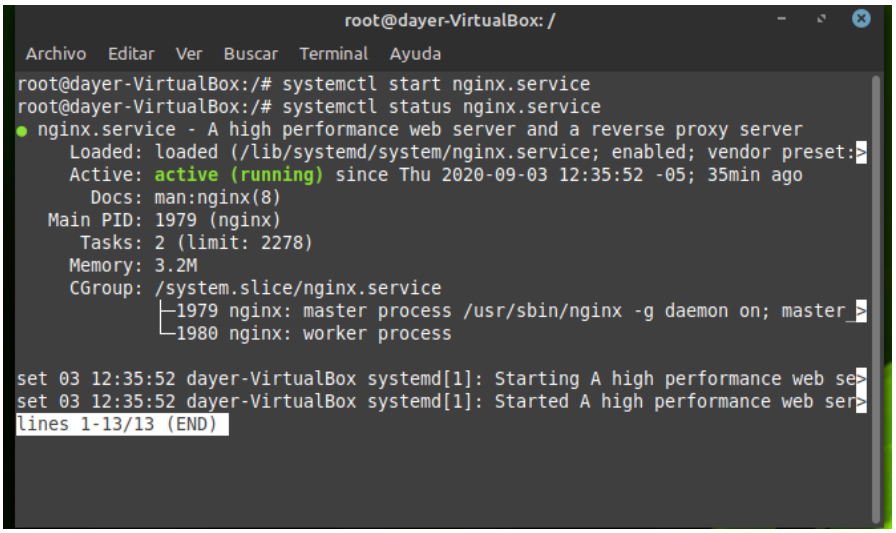
ANEXO 6: IMPLEMENTACION DEL SERVIDOR NGINX

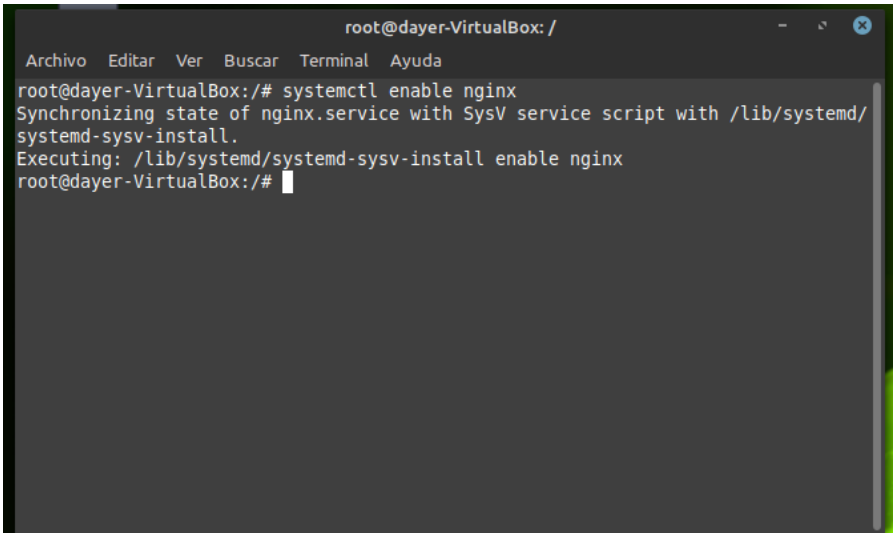


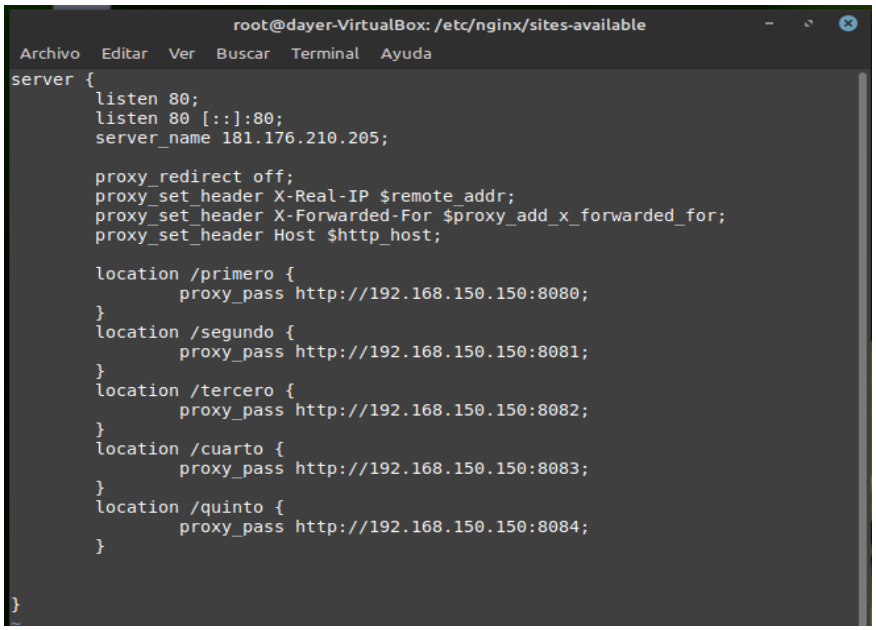


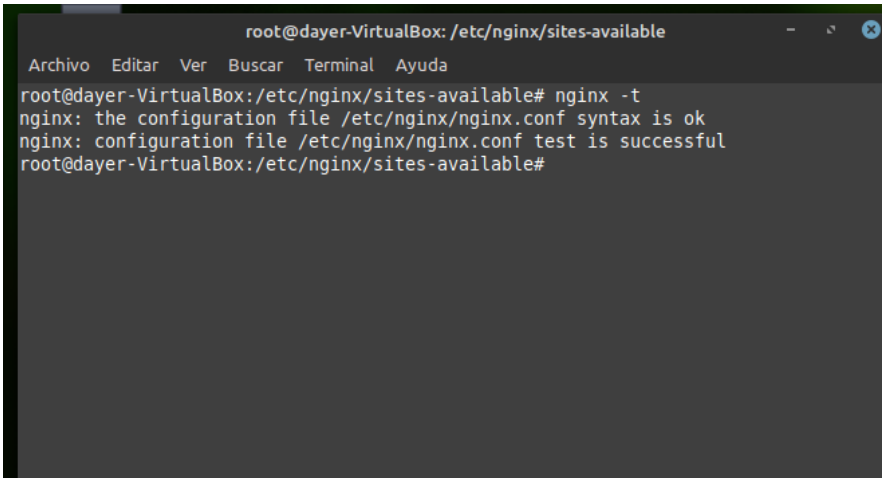


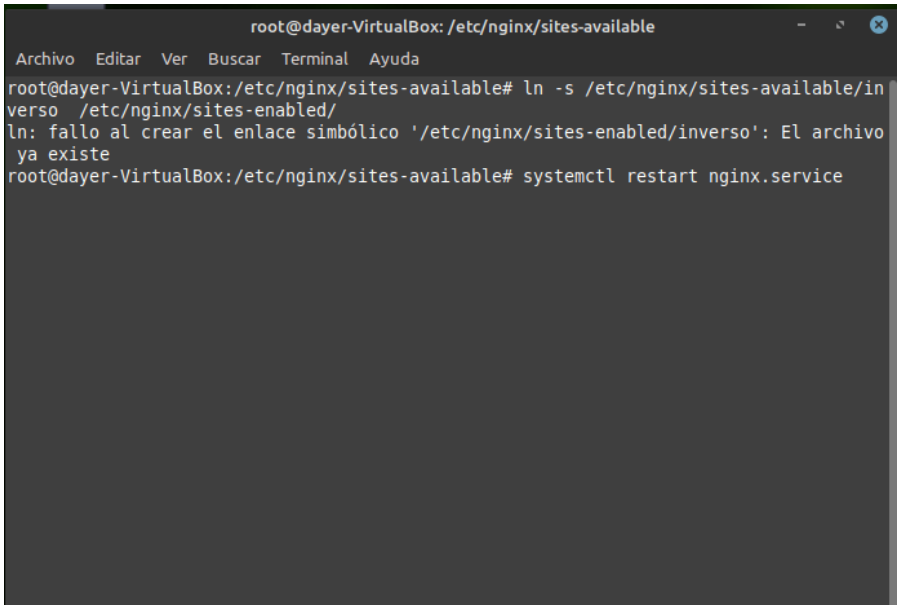

root@dayer-VirtualBox: /
Archivo Editar Ver Buscar Terminal Ayuda
root@dayer-VirtualBox:/# systemctl start nginx.service


root@dayer-VirtualBox: /
Archivo Editar Ver Buscar Terminal Ayuda
root@dayer-VirtualBox:/# systemctl start nginx.service
root@dayer-VirtualBox:/# systemctl status nginx.service
● nginx.service - A high performance web server and a reverse proxy server
Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset:
Active: active (running) since Thu 2020-09-03 12:35:52 -05; 35min ago
Docs: man:nginx(8)
Main PID: 1979 (nginx)
Tasks: 2 (limit: 2278)
Memory: 3.2M
CGroup: /system.slice/nginx.service
├─1979 nginx: master process /usr/sbin/nginx -g daemon on; master_
└─1980 nginx: worker process
set 03 12:35:52 dayer-VirtualBox systemd[1]: Starting A high performance web se
set 03 12:35:52 dayer-VirtualBox systemd[1]: Started A high performance web ser
lines 1-13/13 (END)


root@dayer-VirtualBox: /
Archivo Editar Ver Buscar Terminal Ayuda
root@dayer-VirtualBox:/# systemctl enable nginx
Synchronizing state of nginx.service with SysV service script with /lib/systemd/
systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nginx
root@dayer-VirtualBox:/#


root@dayer-VirtualBox: /etc/nginx/sites-available
Archivo Editar Ver Buscar Terminal Ayuda
server {
listen 80;
listen 80 [::]:80;
server_name 181.176.210.205;
proxy_redirect off;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header Host $http_host;
location /primero {
proxy_pass http://192.168.150.150:8080;
}
location /segundo {
proxy_pass http://192.168.150.150:8081;
}
location /tercero {
proxy_pass http://192.168.150.150:8082;
}
location /cuarto {
proxy_pass http://192.168.150.150:8083;
}
location /quinto {
proxy_pass http://192.168.150.150:8084;
}
}


root@dayer-VirtualBox: /etc/nginx/sites-available
Archivo Editar Ver Buscar Terminal Ayuda
root@dayer-VirtualBox:/etc/nginx/sites-available# nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
root@dayer-VirtualBox:/etc/nginx/sites-available#


root@dayer-VirtualBox: /etc/nginx/sites-available
Archivo Editar Ver Buscar Terminal Ayuda
root@dayer-VirtualBox:/etc/nginx/sites-available# ln -s /etc/nginx/sites-available/inverso /etc/nginx/sites-enabled/
ln: fallo al crear el enlace simbólico '/etc/nginx/sites-enabled/inverso': El archivo ya existe
root@dayer-VirtualBox:/etc/nginx/sites-available# systemctl restart nginx.service

ANEXO 7: IMPLEMENTACION DEL SERVIDOR PROXY

```
deb10u3 [1.538 kB]
Des:7 http://security.debian.org/debian-security buster/updates/main amd64 libldap-common all 2.4.47
+dfsg-3+deb10u2 [89,7 kB]
Des:8 http://security.debian.org/debian-security buster/updates/main amd64 libldap-2.4-2 amd64 2.4.4
7+dfsg-3+deb10u2 [224 kB]
Des:9 http://security.debian.org/debian-security buster/updates/main amd64 grub-pc amd64 2.02+dfsg1-
20+deb10u2 [131 kB]
Des:10 http://security.debian.org/debian-security buster/updates/main amd64 grub2-common amd64 2.02+
dfsg1-20+deb10u2 [538 kB]
Des:11 http://security.debian.org/debian-security buster/updates/main amd64 grub-pc-bin amd64 2.02+d
fsg1-20+deb10u2 [903 kB]
Des:12 http://security.debian.org/debian-security buster/updates/main amd64 grub-common amd64 2.02+d
fsg1-20+deb10u2 [2.477 kB]
Des:13 http://security.debian.org/debian-security buster/updates/main amd64 libcurl3-gnutls amd64 7.
64.0-4+deb10u1 [330 kB]
Des:14 http://security.debian.org/debian-security buster/updates/main amd64 libisc-export1100 amd64
1:9.11.5.P4+dfsg-5.1+deb10u2 [380 kB]
Des:15 http://security.debian.org/debian-security buster/updates/main amd64 libdns-export1104 amd64
1:9.11.5.P4+dfsg-5.1+deb10u2 [972 kB]
Des:16 http://security.debian.org/debian-security buster/updates/main amd64 linux-image-4.19.0-8-amd
64 amd64 4.19.98-1+deb10u1 [48,1 MB]
Des:17 http://security.debian.org/debian-security buster/updates/main amd64 openssl amd64 1.1.1d-0+d
eb10u3 [844 kB]
Des:18 http://security.debian.org/debian-security buster/updates/main amd64 libjson-c3 amd64 0.12.1+
ds-2+deb10u1 [27,3 kB]
Descargados 60,7 MB en 18s (3.440 kB/s)
Preconfigurando paquetes ...
(Leyendo la base de datos ... 22311 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../libapt-pkg5.0_1.8.2.1_amd64.deb ...
Desempaquetando libapt-pkg5.0:amd64 (1.8.2.1) sobre (1.8.2) ...
Configurando libapt-pkg5.0:amd64 (1.8.2.1) ...
(Leyendo la base de datos ... 22311 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../libapt-inst2.0_1.8.2.1_amd64.deb ...
Desempaquetando libapt-inst2.0:amd64 (1.8.2.1) sobre (1.8.2) ...
Preparando para desempaquetar .../archives/apt_1.8.2.1_amd64.deb ...
Desempaquetando apt (1.8.2.1) sobre (1.8.2) ...
```

```
root@debian:~# apt-get install squid3
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
squid3 ya está en su versión más reciente (4.6-1+deb10u4).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 1 no actualizados.
root@debian:~# _
```

```
root@debian:~# apt-get install squid3
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
squid3 ya está en su versión más reciente (4.6-1+deb10u4).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 1 no actualizados.
root@debian:~# systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-09-08 19:19:57 -05; 7min ago
     Docs: man:squid(8)
  Process: 384 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
  Process: 388 ExecStart=/usr/sbin/squid -sYC (code=exited, status=0/SUCCESS)
 Main PID: 389 (squid)
    Tasks: 4 (limit: 2198)
   Memory: 33.1M
   CGroup: /system.slice/squid.service
           ├─389 /usr/sbin/squid -sYC
           ├─391 (squid-1) --kid squid-1 -sYC
           ├─393 (logfile-daemon) /var/log/squid/access.log
           └─394 (pinger)

set 08 19:19:58 debian squid[391]: Max Swap size: 0 KB
set 08 19:19:58 debian squid[391]: Using Least Load store dir selection
set 08 19:19:58 debian squid[391]: Set Current Directory to /var/spool/squid
set 08 19:19:58 debian squid[391]: Finished loading MIME types and icons.
set 08 19:19:58 debian squid[391]: HTCP Disabled.
set 08 19:19:58 debian squid[391]: Pinger socket opened on FD 14
set 08 19:19:58 debian squid[391]: Squid plugin modules loaded: 0
set 08 19:19:58 debian squid[391]: Adaptation support is off.
set 08 19:19:58 debian squid[391]: Accepting HTTP Socket connections at local=[::]:3128 remote=[::]
set 08 19:19:59 debian squid[391]: storeLateRelease: released 0 objects
lines 1-25/25 (END)_
```

```
#       WELCOME TO SQUID 4.6
#       ----------------------------
#
#       This is the documentation for the Squid configuration file.
#       This documentation can also be found online at:
#               http://www.squid-cache.org/Doc/config/
#
#       You may wish to look at the Squid home page and wiki for the
#       FAQ and other documentation:
#               http://www.squid-cache.org/
#               http://wiki.squid-cache.org/SquidFaq
#               http://wiki.squid-cache.org/ConfigExamples
#
#       This documentation shows what the defaults for various directives
#       happen to be.  If you don't need to change the default, you should
#       leave the line out of your squid.conf in most cases.
#
#       In some cases "none" refers to no default setting at all,
#       while in other cases it refers to the value of the option
#       - the comments for that keyword indicate if this is the case.
#

#  Configuration options can be included using the "include" directive.
#  Include takes a list of files to include. Quoting and wildcards are
#  supported.
#
#  For example,
#
#  include /path/to/included/file/squid.acl.config
#
#  Includes can be nested up to a hard-coded depth of 16 levels.
#  This arbitrary restriction is to prevent recursive include references
#  from causing Squid entering an infinite loop whilst trying to load
#  configuration files.
#
#  Values with byte units
"/etc/squid/squid.conf" 8563L, 316146C                                1,1       Comienzo
```

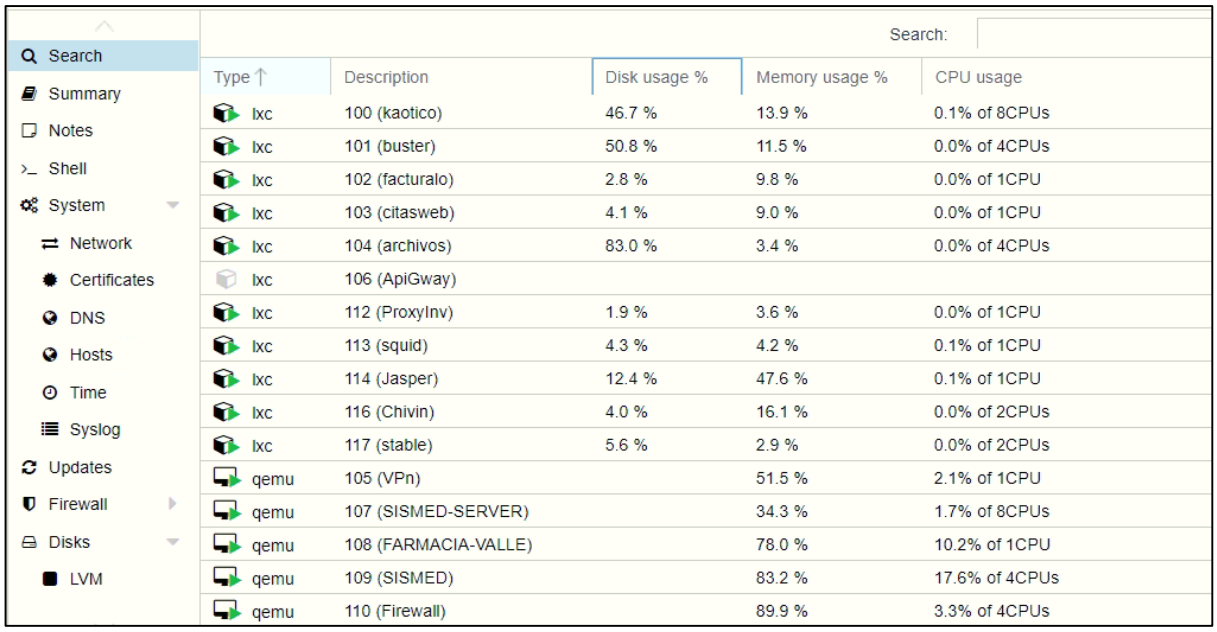
```
root@firewall: /
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
#
# CONFIG FILE FOR SQUIDGUARD
#
# Caution: do NOT use comments inside { }
#

dbhome /var/lib/squidguard/db
logdir /var/log/squidguard

#
# TIME RULES:
# abbrev for weekdays:
# s = sun, m = mon, t =tue, w = wed, h = thu, f = fri, a = sat

time workhours {
        weekly mtwhf 08:00 - 16:30
        date *-*-01  08:00 - 16:30
}


#
# SOURCE ADDRESSES:
#

src admin {
        ip              1.2.3.4  1.2.3.5
        user            root foo bar
        within          workhours
}

src foo-clients {
        ip              172.16.2.32-172.16.2.100 172.16.2.100 172.16.2.200
}

src bar-clients {
        ip              172.16.4.0/26
}

#
# DESTINATION CLASSES:
#
"squidGuard.conf" 82L, 1237C                                          1,1       Comienzo
```

```
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
visible_hostname Firewall
acl paginas url_regex "/etc/squid/paginas"
http_access deny paginas




# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny paginas

#  TAG: adapted_http_access
#       Allowing or Denying access based on defined access lists
#
#       Essentially identical to http_access, but runs after redirectors
#       and ICAP/eCAP adaptation. Allowing access control based on their
#       output.
#
#       If not set then only http_access is used.
#Default:
# Allow, unless rules exist in squid.conf.

#  TAG: http_reply_access
#       Allow replies to client requests. This is complementary to http_access.
#
#       http_reply_access allow|deny [!] aclname ...
#
#       NOTE: if there are no access lines present, the default is to allow
#       all replies.
#
#       If none of the access lines cause a match the opposite of the
#       last line will apply. Thus it is good practice to end the rules
#       with an "allow all" or "deny all" entry.
"/etc/squid/squid.conf" 8570L, 316220C
```

```
root@Firewall:/var/lib/squidguard# ls
db
root@Firewall:/var/lib/squidguard# cd db
root@Firewall:/var/lib/squidguard/db# ls
BL
root@Firewall:/var/lib/squidguard/db# cd BL
root@Firewall:/var/lib/squidguard/db/BL# ls
adv          drugs           hobby          music          ringtones      violence
aggressive   dynamic         homestyle      news           science        warez
alcohol      education       hospitals      podcasts       searchengines  weapons
anonvpn      finance         imagehosting   politics       sex            webmail
automobile   fortunetelling  isp            porn           shopping       webphone
chat         forum           jobsearch      radiotv        socialnet      webradio
COPYRIGHT    gamble          library        recreation     spyware        webtv
costtraps    global_usage    military       redirector     tracker
dating       government      models         religion       updatesites
downloads    hacking         movies         remotecontrol  urlshortener
root@Firewall:/var/lib/squidguard/db/BL#
root@Firewall:/var/lib/squidguard/db/BL# cd ..
root@Firewall:/var/lib/squidguard/db# ls -l
total 4
drwxr-xr-x 57 dayer dayer 4096 mar  4 20:17 BL
root@Firewall:/var/lib/squidguard/db#
```

```
#
# CONFIG FILE FOR SQUIDGUARD
#
# Caution: do NOT use comments inside { }
#

dbhome /var/lib/squidguard/db
logdir /var/log/squid

dest porn{

        domainlist BL/porn/domains
        urllist    BL/porn/urls

}

acl {

        default {
               pass !porn all
               redirect http://192.168.0.16/block.html

         }

}
```

```
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
# Deny requests to certain unsafe ports

visible_hostname squid
acl red_local src 192.168.50.0/16
http_port 192.168.50.1:3128
http_port 192.168.50.1:3129 intercept
acl pag_block_domains url_regex "/etc/squid/socialnet/domains"
acl pag_block dstdomain "/etc/squid/socialnet/urls"
#http_access allow red_local
# And finally deny all other access to this proxy
http_access allow red_local
redirect_program /usr/bin/squidGuard -c /etc/squidguard/squidGuard.conf
```


Search
Summary
Notes
Shell
System
Network
Certificates
DNS
Hosts
Time
Syslog
Updates
Firewall
Disks
LVM
Search:
Type
Description
Disk usage %
Memory usage %
CPU usage
lxc 100 (kaotico) 46.7 % 13.9 % 0.1% of 8CPUs
lxc 101 (buster) 50.8 % 11.5 % 0.0% of 4CPUs
lxc 102 (facturalo) 2.8 % 9.8 % 0.0% of 1CPU
lxc 103 (citasweb) 4.1 % 9.0 % 0.0% of 1CPU
lxc 104 (archivos) 83.0 % 3.4 % 0.0% of 4CPUs
lxc 106 (ApiGway)
lxc 112 (ProxyInv) 1.9 % 3.6 % 0.0% of 1CPU
lxc 113 (squid) 4.3 % 4.2 % 0.1% of 1CPU
lxc 114 (Jasper) 12.4 % 47.6 % 0.1% of 1CPU
lxc 116 (Chivin) 4.0 % 16.1 % 0.0% of 2CPUs
lxc 117 (stable) 5.6 % 2.9 % 0.0% of 2CPUs
qemu 105 (VPn) 51.5 % 2.1% of 1CPU
qemu 107 (SISMED-SERVER) 34.3 % 1.7% of 8CPUs
qemu 108 (FARMACIA-VALLE) 78.0 % 10.2% of 1CPU
qemu 109 (SISMED) 83.2 % 17.6% of 4CPUs
qemu 110 (Firewall) 89.9 % 3.3% of 4CPUs

ANEXO 8: ENCUESTA

ENCUESTA APLICADA AL PERSONAL DEL ÁREA DE INFORMÁTICA DEL HOSPITAL REGIONAL HERMILIO VALDIZÁN MEDRANO

1. ¿Cómo calificaría la disponibilidad de los servidores del Hospital Regional Hermilio Valdizán Medrano?

- ○ Muy buena (4)
- ○ Buena (3)
- ○ Regular (2)
- ○ Mala (1)
- ○ Muy mala (0)

2. ¿Con que frecuencia ocurre la caída de los servidores? *

- ○ Muy frecuentemente (0)
- ○ Frecuentemente (1)
- ○ Ocasionalmente (2)
- ○ Raramente (3)
- ○ Nunca (4)

3. ¿Qué tan satisfecho está el personal con los servicios informáticos que brinda el Hospital Regional Hermilio Valdizán Medrano? *

- ○ Extremadamente satisfechos (4)
- ○ Muy satisfechos (3)
- ○ Moderadamente satisfechos (2)
- ○ Poco satisfechos (1)
- ○ No satisfechos (0)

4. ¿Cómo calificaría el nivel de seguridad informática que tiene el Hospital Regional Hermilio Valdizán Medrano? *

- ○ Muy buena (4)
- ○ Buena (3)
- ○ Regular (2)
- ○ Mala (1)
- ○ Muy mala (0)

5. ¿Usted cree que el Hospital Regional Hermilio Valdizán Medrano desde el punto de vista tecnológico está preparado para brindar servicios que impliquen gran soporte tecnológico y de alta disponibilidad?

- ○ Totalmente de acuerdo (4)
- ○ De acuerdo (3)
- ○ Indeciso (2)
- ○ En desacuerdo (1)
- ○ Totalmente en desacuerdo (0)

6. ¿Cree Ud. que el tiempo fuera de línea que se pierde con las caídas de los servidores generan pérdidas en producción?

- ○ Totalmente de acuerdo (4)
- ○ De acuerdo (3)
- ○ Indeciso (2)
- ○ En desacuerdo (1)
- ○ Totalmente en desacuerdo (0)

7. ¿Con que frecuencia el personal del Hospital Regional Hermilio Valdizán Medrano hace mal uso del Internet?

- ○ Muy frecuentemente (0)
- ○ Frecuentemente (1)
- ○ Ocasionalmente (2)
- ○ Raramente (3)
- ○ Nunca (4)

8. ¿Con que frecuencia las solicitudes a los servicios informáticos no son devueltas?

- ○ Muy frecuentemente (0)
- ○ Frecuentemente (1)
- ○ Ocasionalmente (2)
- ○ Raramente (3)
- ○ Nunca (4)

9. ¿Cree Ud. que la implementación de la propuesta beneficia a todo el personal del Hospital Regional Hermilio Valdizán Medrano?

- ○ Totalmente de acuerdo (4)
- ○ De acuerdo (3)
- ○ Indeciso (2)
- ○ En desacuerdo (1)
- ○ Totalmente de acuerdo (0)

10. ¿Con que frecuencia los equipos informáticos sufren ataques de virus?

- ○ Muy frecuentemente (0)
- ○ Frecuentemente (1)
- ○ Ocasionalmente (2)
- ○ Raramente (3)
- ○ Nunca (4)

ANEXO 9: FOTO CON EL PERSONAL DE INFORMATICA

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" HUÁNUCO – PERÚ
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS - PROFI

En Huánuco, a los 09 días del mes de julio de 2021, siendo las 11:00 am horas de acuerdo al Reglamento del Programa de Fortalecimiento en Investigación PROFI de la Universidad Nacional Hermilio Valdizán, Capítulo XII DE LA SUSTENTACIÓN DE LA TESIS, Art. 48º al 52º, se procedió a la evaluación de la sustentación de la tesis virtual, titulado: **"IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA TECNOLÓGICA DE SERVIDORES PARA MEJORAR LA SEGURIDAD Y DISPONIBILIDAD DE LOS SISTEMAS INFORMÁTICOS EN EL HOSPITAL REGIONAL HERMILIO VALDIZÁN MEDRANO (HRHVM) - 2020"**, presentado por la Bachiller en Ingeniería de Sistemas: **DINA CABALLERO UGARTE.** Este evento se realizó vía Cisco Webex de la Facultad de Ingeniería Industrial y de Sistemas de la UNHEVAL, ante los miembros del Jurado Calificador, integrado por los siguientes catedráticos:

PRESIDENTE: Dra. INÉS EUSEBIA JESÚS TOLENTINO
SECRETARIO: Mg. JIMMY GROVER FLORES VIDAL
VOCAL: Mg. HEIDY VELSY RIVERA VIDAL

Finalizado el acto de sustentación, se procedió a la calificación conforme al Artículo 51º y 52º del Reglamento del Programa de Fortalecimiento en Investigación PROFI, obteniéndose el siguiente resultado: **Nota: DIECISEIS** equivalente a la calificación de BUENO Quedando la Bachiller en Ingeniería de Sistemas: **DINA CABALLERO UGARTE: APROBADO**

Con lo que se dio por concluido el acto y en fe de la cual firman los miembros del jurado Calificador.

.....
PRESIDENTE

.....
SECRETARIO

.....
VOCAL

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" HUÁNUCO – PERÚ
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

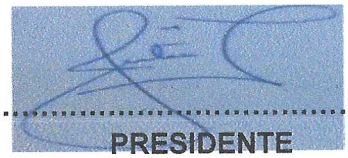
ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS - PROFI

En Huánuco, a los 09 días del mes de julio de 2021, siendo las 11:00 am horas de acuerdo al Reglamento del Programa de Fortalecimiento en Investigación PROFI de la Universidad Nacional Hermilio Valdizán, Capítulo XII DE LA SUSTENTACIÓN DE LA TESIS, Art. 48º al 52º, se procedió a la evaluación de la sustentación de la tesis virtual, titulado: **"IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA TECNOLÓGICA DE SERVIDORES PARA MEJORAR LA SEGURIDAD Y DISPONIBILIDAD DE LOS SISTEMAS INFORMÁTICOS EN EL HOSPITAL REGIONAL HERMILIO VALDIZÁN MEDRANO (HRHVM) - 2020",** presentado por el Bachiller en Ingeniería de Sistemas: **NELSON DRYER SALAZAR ARANDA.** Este evento se realizó vía Cisco Webex de la Facultad de Ingeniería Industrial y de Sistemas de la UNHEVAL, ante los miembros del Jurado Calificador, integrado por los siguientes catedráticos:

PRESIDENTE: Dra. INÉS EUSEBIA JESÚS TOLENTINO
SECRETARIO: Mg. JIMMY GROVER FLORES VIDAL
VOCAL: Mg. HEIDY VELSY RIVERA VIDAL

Finalizado el acto de sustentación, se procedió a la calificación conforme al Artículo 51º y 52º del Reglamento del Programa de Fortalecimiento en Investigación PROFI, obteniéndose el siguiente resultado: **Nota: DIECISEIS** equivalente a la calificación de BUENO Quedando el Bachiller en Ingeniería de Sistemas: **NELSON DRYER SALAZAR ARANDA: APROBADO**

Con lo que se dio por concluido el acto y en fe de la cual firman los miembros del jurado Calificador.



.....
PRESIDENTE

.....
SECRETARIO

.....
VOCAL

<UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" DE HUÁNUCO
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS
CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

CONSTANCIA DE APTO

De acuerdo al Reglamento General de Grados y Títulos Modificado de la Universidad Nacional Hermilio Valdizán de Huánuco aprobado con Resolución del Consejo Universitario N° 1893-2021-UNHEVAL, de fecha 17 de agosto de 2021 y en atención a la Tercera Disposición Complementaria, donde estipula que los trabajos de investigación y tesis de pregrado deberán tener una similitud máxima del 30%.

Después de aplicado el Software Turnitin, se evidencia una similitud del 23% encontrándose bajo los parámetros reglamentados.

Tesis para optar el Título Profesional de Ingeniero de Sistemas:

"Implementación de una infraestructura tecnológica de servidores para mejorar la seguridad y disponibilidad de los sistemas informáticos en el Hospital Regional Hermilio Valdizán Medrano (HRHVM) - 2020".

Tesistas

Bach. Ingeniería de Sistemas DINA CABALLERO UGARTE
Bach. Ingeniería de Sistemas NELSON DRYER SALAZAR ARANDA

Huánuco, 18 de febrero de 2022

Nérida del Carmen Pastrana Díaz
Directora de Investigación - FIIS

AUTORIZACION PARA PUBLICACION DE TESIS ELECTRONICA DE PREGRADO

IDENTIFICACION PERSONAL (especificar los datos de los autores de la tesis).

Apellidos y Nombres: Caballero Ugarte, Dina

DNI: 71912865 Correo Electrónico: dinabu@gmail.com

Teléfono Casa: _____ Celular: 914629769 Oficina: _____

Apellidos y Nombres: Salazar Aranda, Nelson Dryer

DNI: 75990752 Correo Electrónico: sidox_10@hotmail.com

Teléfono Casa: _____ Celular: 942423924 Oficina: _____

Apellidos y Nombres: _____

DNI: _____ Correo Electrónico: _____

Teléfono Casa: _____ Celular: _____ Oficina: _____

IDENTIFICACION DE LA TESIS

Pregrado
Facultad de: Ingeniería Industrial y de Sistemas
E.P.: de Ingeniería de Sistemas

Título Profesional obtenido:

Ingeniero de Sistemas

Título de la Tesis:

"Implementación de una infraestructura tecnológica de servidores para mejorar la seguridad y disponibilidad de los sistemas informáticos en el HRHVM-2020"

Tipo de acceso que autoriza (n) el (los) autor (es):

Marca "x"	Categoría de Acceso	Descripción de Acceso
X	**PUBLICO**	Es público y accesible al documento a texto completo por cualquier tipo de usuario que consulta al repositorio
	RESTRINGIDO	Solo permite el acceso al registro del metadato con información básica mas no al texto completo.

Al elegir la opción "Público" a través de la presente autorizo o autorizamos de manera gratuita al Repositorio Institucional – UNHEVAL, a publicar la versión electrónica de esta tesis en el Portal Web repositorio.unheval.edu.pe, por un plazo indefinido, consintiendo que dicha autorización cualquier tercero podrá acceder a dichas páginas de manera gratuita, pudiendo revisarla, imprimirla o grabarla, siempre y cuando se respete la autoría y sea citada correctamente.

En caso haya (n) marcado la opción "Restringido", por favor detallar las razones por las que se eligió este tipo de acceso:

Asimismo, pedimos indicar el periodo de tiempo en que la tesis tendría el tipo de acceso restringido:

( ) 1 año

( ) 2 años

( ) 3 años

( ) 4 años

Luego del periodo señalado por usted (es), automáticamente la tesis pasara a ser de acceso público.

Fecha Firma: 25 - 02 - 2022

Firma del Autor y/o autores:

Dina Caballero Ugarte

Nelson Dryer Salazar Aranda