
# ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

## ELABORACIÓN Y EVALUACIÓN DE UN SISTEMA QUE PERMITA MEJORAR LA DISPONIBILIDAD Y SEGURIDAD EN LOS SERVICIOS WEB DE LA UNIVERSIDAD TÉCNICA LUIS VARGAS TORRES, MEDIANTE EL USO DE HERRAMIENTAS DE SOFTWARE LIBRE

**JHONNY MAXIMILIANO QUIÑONEZ QUINTERO**

**Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:**

**MAGÍSTER EN SEGURIDAD TELEMÁTICA**

**RIOBAMBA - ECUADOR**

**Marzo 2022**

**ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**

# CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado ELABORACIÓN Y EVALUACIÓN DE UN SISTEMA QUE PERMITA MEJORAR LA DISPONIBILIDAD Y SEGURIDAD EN LOS SERVICIOS WEB DE LA UNIVERSIDAD TÉCNICA LUIS VARGAS TORRES, MEDIANTE EL USO DE HERRAMIENTAS DE SOFTWARE LIBRE, de responsabilidad del señor Jhonny Maximiliano Quiñonez Quintero ha sido prolijamente revisado y se autoriza su presentación.

Ing. Luis Eduardo Hidalgo Almeida; Ph. D.
**PRESIDENTE**

Firmado electrónicamente por:
LUIS EDUARDO HIDALGO ALMEIDA

Ing. Renny Geovanny Montalvo Armijos; Mag.
**DIRECTOR**

Firmado electrónicamente por:
RENNY GEOVANNY MONTALVO ARMIJOS

Ing. Jacqueline Elizabeth Ponce Pinos, Mag.
**MIEMBRO**

Firmado electrónicamente por:
JACQUELINE ELIZABETH PONCE PINOS

Ing. Cristian Geovanny Merino Sánchez; Mag.
**MIEMBRO**

CRISTIAN GEOVANNY MERINO SANCHEZ

Firmado digitalmente por CRISTIAN GEOVANNY MERINO SANCHEZ

Riobamba, marzo 2022

## DERECHOS INTELECTUALES

Yo, Jhonny Maximiliano Quiñonez Quintero, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.


Jhonny Maximiliano Quiñonez Quintero

CI: 0801901695

## DECLARACIÓN DE AUTENTICIDAD

Yo: Jhonny Maximiliano Quiñonez Quintero, declaro que el presente Trabajo de Titulación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados. Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Firmado electrónicamente por:
**JHONNY MAXIMILIANO QUINONEZ QUINTERO**

Jhonny Maximiliano Quiñonez Quintero

No. Cédula: 0801901695

## DEDICATORIA

Dedico esta tesis a DIOS por haberme dado el don de la vida, a mis padres quienes me dieron una gran crianza, educación, apoyo y consejos, a mi esposa e hijos quienes fueron un gran apoyo emocional e incondicional, que es lo que me motiva día a día a superarme, a todos ellos se los agradezco desde el fondo de mi alma.

Jhonny Maximiliano Quiñónez Quintero

## AGRADECIMIENTO

Le agradezco a Dios por haberme guiado y acompañado a lo largo de mi vida.

Le agradezco a mi madre, Evelina, por apoyarme en todo momento y haberme inculcado valores, por sacrificarse para brindarme una excelente educación y, por sobretodo, ser un ejemplo de vida para mí.

Agradezco a Erika, mi amada esposa, a mis queridos hijos Armando, Joel e Iliana, mis compañeros en las buenas y en las malas, y a que pesar de todo nunca pierden la fé en mí.

Gracias a la Escuela Politécnica del Chimborazo, y a mis Maestros, en especial a mi Sr. Asesor, Ing. Renny Montalvo Armijos y al Ing. Oswaldo Martínez, Coordinador de este Programa de Maestría, por su apoyo y por brindarme un espacio acogedor donde he vivido buenas experiencias de aprendizaje.

A mis amigos Jimmy Ramírez y David Romero, por confiar en mí y por hacer esta trayectoria universitaria más fácil y una vivencia que nunca olvidaré.

Jhonny

**CONTENIDO**

CAPÍTULO III

## ÍNDICE DE TABLAS

## ÍNDICE DE FIGURAS

## ÍNDICE DE ANEXOS

**RESUMEN**

Este trabajo de titulación tuvo como objetivo la elaboración y evaluación de un sistema que permita mejorar la disponibilidad y seguridad en los servicios web de la Universidad Técnica Luis Vargas Torres, mediante el uso de herramientas de software libre. La disponibilidad de los servicios y aplicaciones web es un factor preponderante de las operaciones administrativas y académicas diarias de cualquier institución que utiliza la tecnología como herramienta de trabajo. Para la mitigación de este problema y del impacto de eventos de seguridad y disponibilidad adversos que paralizan las actividades de manera frecuente y prolongada, se plantea la implementación de un sistema virtualizado, con una adecuada distribución del software sobre el hardware que garantice el aprovechamiento de recursos físicos y la continuidad de los procesos en la universidad. Todo este proceso de elaboración, pruebas y evaluación se ha realizado en un entorno virtual controlado. Los resultados alcanzados demuestran que es posible configurar un sistema seguro de alta disponibilidad que incluya todas los servicios y aplicaciones. Se concluye que las herramientas de software libre, en este caso Proxmox, cumple plenamente con las expectativas de uso para entornos virtualizados por sus herramientas de administración de contenedores, servidores virtuales, firewalls, backup, almacenamiento y alta disponibilidad.

**Palabras Clave:** <ALTA DISPONIBILIDAD>, <SEGURIDAD>, <MÁQUINAS VIRTUALES>, <CONTENEDORES>, <PROXMOX>, <SOFTWARE LIBRE>.

**SUMARY**

This degree project has the aim of building and evaluating a system that allows improving the availability and security of web services at Luis Vargas Torres Technical University, through the use of open source software tools. The availability of services and web applications is a key factor in administrative and academic daily operations of any institution that uses technology as a working tool. For the mitigation of this problem and security events impact and adverse availability that frequently stop activities in a prolonged way, a virtual system is been proposed. This, with an adequate software distribution over hardware that guarantees taking the advantage of physical resources and the continuity of the processes at the university. All this elaboration process, test and evaluations have been done on a virtual controlled environment. The findings show that is possible to configure a secure system of high availability that includes all the services and applications. As a conclusion, it has been recognised that all the open source software tools, in this case Proxmox, complies with the expectations for its use in virtual environments, with its administrative tools of containers, virtual servers, firewalls, backup storage and high availability.

Key words: <HIGH AVAILABILITY>, <SECURITY>, <VIRTUAL MACHINES>, <CONTAINERS>, <PROXMOX>, <OPEN SOFTWARE>.

# CAPÍTULO I

## 1. INTRODUCCIÓN

La búsqueda continua del mejoramiento del aprovechamiento y rendimiento de los recursos informáticos, ha sido un gestor del nacimiento de nuevas tecnologías en la gestión de procesos productivos en las instituciones como la virtualización y los Contenedores o Dockers en Ingles.

Los servicios informáticos se han convertidos en un elemento fundamental de las operaciones de una empresa, reflejándose directamente en su nivel de calidad del negocio y su productividad. Además, hoy en día los activos de información son recursos imprescindibles en cualquier organización moderna.

Un centro de datos consiste en uno o varios locales, una planta o un edificio completo que alberga el sistema principal de redes, ordenadores y recursos asociados para procesar toda la información de una empresa u organismo (López Aguilera, 2010).

Un centro de datos debe estar diseñado para proteger y garantizar los recursos informáticos de una organización, además de contar con la prevención para la mitigación de eventos adversos.

La explotación de esta tecnología combinada con estrategias y herramientas de Alta Disponibilidad, ofrece una alternativa más rápida y económica en la implementación de servicios y aplicaciones sobre servidores, además de la movilidad, ligereza y practicidad. Debido a las características antes mencionadas, se ha popularizado el uso de estas tecnologías (Andrade Pazmiño, 2014).

Por tal motivo, es necesario implementar soluciones informáticas que permitan mantener operativa toda la infraestructura, en otras palabras, tomar acciones que permitan un trabajo ininterrumpido de Servidores y servicios.

### 1.1. Problema de investigación

#### *1.1.1. Planteamiento del problema*

En la Universidad Técnica Luis Vagas Torres de Esmeraldas, el uso de esta tecnología ha traído consigo nuevos retos en el área de seguridad al personal del Departamento de Tecnologías, en su afán de obtener un buen performance de los servicios y aplicaciones que se ejecutan sobre servidores los servidores virtualizados.

Las aplicaciones más importantes en producción son: Sistema Administrativo, Sistema Académico, Sistema de Evaluación Docente, Sistema de Leccionario Docente, Portal Web.

La falta de gestión de la seguridad de los servidores ha provocado problemas de interacción de las aplicaciones y servicios implementados en diferentes servidores virtuales, debido a la falta de controles sobre el acceso a la información que se puede realizar entre aplicaciones y usuarios.

Además, la gobernabilidad de los servicios está comprometida por la inadecuada administración de los privilegios y roles de usuarios, lo cual permite realizar operaciones administrativas y configuraciones no controladas; presentándose situaciones de caídas de servicio y toma de tiempo para su respectiva recuperación.

Así mismo, las debilidades de la configuración de la seguridad de los sistemas operativos anfitriones de los contenedores ponen en riesgo el correcto funcionamiento de los sistemas y el óptimo consumo de recursos, ya que son vulnerables ante amenazas de ataques informáticos, virus, accesos no autorizados, etc.

Las frecuentes caídas de los servicios, con tiempos de recuperación altos, comprometen las operaciones normales de los usuarios de la comunidad universitaria, terminando en pérdidas de tiempo, retraso de trámites y nivel de satisfacción muy bajo.

Y por último, también hay que asegurar y calibrar los dispositivos de red que comunican los diferentes servicios y aplicaciones para su correcto consumo.

### *1.1.2. Formulación del problema*

¿Cómo debe ser el sistema de virtualización que se pueda aplicar para el fortalecimiento de la disponibilidad y seguridad en las aplicaciones y servicios web de la UTELVT?

### *1.1.3. Sistematización del problema*

¿Cuáles son las características de los equipos, máquinas físicas, virtuales y las aplicaciones explotadas en la UTELVT?

¿Cómo mejorara la administración de seguridad en sistemas operativos anfitriones de seguridad?

¿Cómo determinar vulnerabilidades en seguridad y rendimiento en infraestructuras virtualizadas?

¿Cómo mejorar la disponibilidad sin influir negativamente en el rendimiento e iteración de los contenedores y máquinas virtuales?

¿Cómo lograr un impacto positivo en la disponibilidad de los servicios virtualizados y su infraestructura?

## 1.2. Justificación de la investigación

El establecimiento de estrategias de seguridad para las virtualizaciones basadas en servidores y contenedores permitirá contar con servicios y aplicaciones confiables, con un sistema de seguridad organizado, que puede ser revisado mediante herramientas de monitorización.

Del mismo modo, se contará con un sistema de usuarios controlado con roles establecidos según sus funciones lo cual beneficia la seguridad informática de toda la organización; además que regulará el trafico libre de usuarios entre la red de los anfitriones y la de los servidores.

La "hardenización" de la seguridad a nivel de sistemas operativos anfitriones y de red, mitiga la exposición a vulnerabilidades de ataques, accesos no autorizados, control de tráfico, virus, etc., garantizando el normal funcionamiento de los aplicativos.

La utilización de sistemas que implementen estrategias de alta disponibilidad, e incluso permitan automatizar la detección y recuperación de servicios ante fallos; permitirá elevar el grado de confiabilidad de las operaciones diarias de la UTELVT.

También se dotará de una guía para la seguridad a implementar por parte del Personal de TIC's, lo que al final beneficia las actividades diarias basadas en sistemas de información de los usuarios de la Universidad Técnica de Esmeraldas Luis Vargas Torres.

La búsqueda de mejores prácticas a nivel de seguridad informática incrementa la fortaleza institucional frente a la vulneración del buen funcionamiento de sus sistemas y garantiza la continuidad de las operaciones Administrativas y Académicas de la Universidad.

## 1.3. Objetivos

### *1.3.1. Objetivo general*

Elaborar y evaluar un sistema que permita mejorar la disponibilidad y seguridad en los servicios web de la UNIVERSIDAD TÉCNICA LUIS VARGAS TORRES, mediante el uso de herramientas de software libre.

### *1.3.2. Objetivos específicos*

- Determinar las mejores prácticas de seguridad para incrementar la disponibilidad, que se pueden aplicar en servidores virtuales y / o contenedores.
- Diseñar en un ambiente controlado, las estrategias de seguridad seleccionadas a los sistemas de la UTE-LVT y comprobar los resultados.
- Implementar, en un ambiente de pruebas, un sistema de virtualización basado en servidores virtuales y / o contenedores, las aplicaciones y servicios de la UTE-LVT, en el cual determinar vulnerabilidades en seguridad y rendimiento.
- Evaluar mediante la comparación de métricas en términos de seguridad y rendimiento la aplicación de las estrategias de seguridad seleccionadas para las aplicaciones y servicios virtualizados en servidores virtuales y / o contenedores de la UTE-LVT.
- Documentar las estrategias de seguridad para infraestructuras de virtualización basados en servidores virtuales y / o contenedores de la UTE-LVT.

## 1.4. Hipótesis

La implementación de un sistema virtualizado de Alta Disponibilidad mediante el uso de software libre, mejorará la disponibilidad y seguridad en las aplicaciones y servicios web de la UTELVT.

# CAPÍTULO II

## 2. MARCO TEÓRICO

### 2.1. Antecedentes del problema

Una alternativa adecuada para resolver estos problemas de interrupción de servicios es implementar soluciones de alta disponibilidad y seguridad, utilizando ambientes virtualizados con servidores virtuales y / o contenedores; de tal manera que realice una activación automática de los servicios ante una caída de los servidores.

Tras la revisión de trabajos de investigación se han encontrado temas relacionados a la seguridad en infraestructuras de TI, que respaldan y sirven de referentes para el desarrollo de la investigación:

La investigación realizada por (Tapia, s. f.), con el tema: "Tecnología de Contenedores Docker", en la que se concluye lo siguiente:

- Los contenedores son mucho más ligeros que las máquinas virtuales ya que, mientras que las máquinas virtuales requieren de la instalación de un sistema operativo, asignación de disco, CPU y memoria RAM para funcionar, un contenedor de Docker sólo necesita el sistema operativo que corre en la máquina en la que está el contenedor. (Tapia, s. f.)

- Si hablamos de entornos de desarrollo, Docker es la herramienta ideal ya que es un sistema aislado que cuenta únicamente con librerías que utilizaremos para nuestro proyecto, por lo tanto, tendremos un entorno óptimo para desarrollar nuestra aplicación, que podremos ejecutar en cualquier máquina, independientemente del sistema operativo. (Tapia, s. f.)

- En cuanto a entornos de producción, y aunque se ha hablado mucho de que en un futuro los contenedores reemplazarán a las máquinas virtuales, yo creo que lo que realmente sucederá será la integración de esta tecnología con la tecnología de virtualización clásica, que aportará mejoras en el rendimiento de muchas aplicaciones. (Tapia, s. f.)

Se recomienda:

- Utilizar Docker Swarm o Kubernetes, ya que con estas herramientas podremos crear un clúster fácilmente escalable para ejecutar los diferentes servicios de los que esté compuesta nuestra aplicación.

Así mismo se muestra el estudio de (Hernández, s. f.), con el tema: “Seguridad en Docker”, en la que se concluye lo siguiente:

- Un contenedor requiere de múltiples planteamientos en la seguridad que se aplican en cada fase de su implementación, pero la información sobre esto y la concienciación de una implementación completa y correcta no han ido de la mano. (Hernández, s. f.)

- Al revisar en detalle los procesos de instalación de los Dockers o contenedores de manera segura, se han hallado marcadas diferencias de usabilidad y capacidad en las herramientas gratuitas disponibles para esta tarea. (Hernández, s. f.)

Se recomienda:

- Realizar un documento y guía de políticas y normas a seguir que recojan todas las fases de implantación de los Dockers, aportando recomendaciones de herramientas, configuraciones y consejos de seguridad. (Hernández, s. f.)

- Para realizar una buena configuración de una infraestructura de servicios virtualizados con contenedores o servidores virtuales, es necesario la configuración adecuada entre los perfiles de desarrollo y perfiles de sistemas. (Hernández, s. f.)

En cuanto a la virtualización, entre los estudios realizados tenemos a Espinoza & Lobatón (2014) quienes buscando estrategias mejorar la productividad del centro de datos del Ministerio de Transportes y Comunicaciones, determinaron que la alta disponibilidad y virtualización permite reducir los costos de hardware, los riegos de perdida de servicio, y por otro lado incrementar el nivel de convergencia de plataformas.

Continuando con este tema, (Moretta, 2017) implementó y evaluó una infraestructura para asegurar las aplicaciones de la carrera de licenciatura de sistemas de información de la universidad de Guayaquil, analizo varias alternativas de plataformas para ambientes virtualizados, además diseño una distribución de hardware para la residencia de los servidores; luego de su análisis, utilizó la aplicación de software libre Proxmox como plataforma de virtualización.

Por otro lado, (Espinoza R. M., 2019), en su Tesis de Maestría, en la ciudad de Riobamba. también analizó las características de varios hypervisores nativos propietarios y libres para el proceso de almacenamiento de datos y calificó el almacenamiento de datos en Proxmox como mejor opción de los hypervisores libre seleccionados, además obtuvo que al realizar el almacenamiento de datos virtualizado, Proxmox sobrepaso con más del 100% con respecto al valor comparativo del almacenamiento de datos, a las demás plataformas analizadas.

Igualmente, (Acero Quilumbaquín, 2016), en su trabajo de Titulación, diseño e implementó un Clúster de Alta Disponibilidad para virtualizar los servidores de Adquisición y procesamiento de datos del Instituto Geofísico, concluyó que en un Clúster de Alta Disponibilidad en producción, en el que todos los servidores virtuales están activos, no existe desperdicio de recursos de hardware, más bien existe un balance de carga porque todos los servidores apoyan a la productividad como un conjunto.

Luego, (Flórez Hernández & Huertas Lucena, 2018) en Popayán, Colombia, virtualizaron los Servicios de Red de la Empresa HSE INGENIERÍA SA, y en su respectivo informe de investigación informaron haber alcanzado un nivel de disponibilidad del 99.6666%, y luego de su experiencia especificaron que a través de la virtualización evidenciaron las ventajas que ofrece esta tecnología como la reducción de costos, pronta recuperación ante fallos, ahorro de espacio físico y mejor administración de los servicios migrados, lo que se traduce en beneficios para la empresa.

Dentro de este mismo contexto, el estudio "Plataformas de software libre para la virtualización de servidores en pequeñas y medianas empresas cubanas" (Perdigon Llanes & Ramirez Alonso, 2020), determinaron que Proxmox 5.4 obtuvo los mejores valores en el diagnóstico de escalabilidad y de rendimiento con varias máquinas virtuales ejecutadas simultáneamente bajo estrés y constituye una opción libre y eficiente para la virtualización de servidores con uso eficiente de los recursos de hardware.

En el campo de la seguridad, expresamente en el control de tráfico y de acceso, el Ministerios del Interior y Seguridad Pública de Chile, a través de publicaciones del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), publico un artículo de Nilo Andrade (2020), en el que se recmiendan las mejores prácticas para la administración de firewalls, y hace énfasis en el modelo zero trust, con el objetivo de contribuir al endurecmiento de la ciberseguridad. Ademas destaca que, la seguridad no es solo administrar un firewall si no que es un conjunto de tecnologías y métodos; por esto motiva a tener controles, definicione y conocimiento del negocio para impementar capas de seguridad de forma efectiva y eficiente.

## 2.2. Bases teóricas

Para la revisión de literatura científica se aplicará la siguiente metodología: definir las preguntas sobre la cual se realizará la revisión de literatura, luego de eso se establecerán las palabras claves con las cuales se definen las cadenas de búsqueda que se ejecutaran en las bases de datos escogidas, para en base a los criterios de inclusión y exclusión facilitar la revisión de los artículos científicos seleccionados.

### *2.2.1. Seguridad informática*

Es la disciplina encargada de diseñar las normas procedimientos, métodos y técnicas para obtener un sistema de información seguro y confiable. La seguridad informática puede ser: activa es decir el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amanezcan al sistema o pasiva que son todas aquellas medidas que se implementan luego que la seguridad se ha incrementado, por ejemplo, realizar copias de seguridad a diario (Aguliera, 2010).

### *2.2.2. Normas ISO de Seguridad Informática*

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías. («Normas ISO sobre gestión de seguridad de la información | Seguridad Informática», s. f.)

En concreto la familia de normas ISO/IEC 27000 son un conjunto de estándares de seguridad (desarrollados o en fase de desarrollo) que proporciona un marco para la gestión de la seguridad. («Normas ISO sobre gestión de seguridad de la información | Seguridad Informática», s. f.)

Contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La seguridad de la información, según la ISO 27001, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento.

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requieran.

*2.2.2.1. ISO/IEC 27000:*

Publicada el 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012, una tercera edición de 14 de enero de 2014 y una cuarta en febrero de 2016. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua). Existen versiones traducidas al español, aunque hay que prestar atención a la versión descargada. El original en inglés y su traducción al francés en su versión de 2018 puede descargarse gratuitamente de standards.iso.org/ittf/PubliclyAvailableStandards. («Normas ISO sobre gestión de seguridad de la información | Seguridad Informática», s. f.)

*2.2.2.2. ISO/IEC 27001:*

Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI's de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. («ISO27000. "El portal de ISO 27001 en español. Gestión de Seguridad de la Información"», s. f.)

*2.2.2.3. ISO/IEC 27002:*

Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.

Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de diciembre de 2009 (a la venta en AENOR). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondonorma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh-ISO27002), Uruguay (UNIT-ISO/IEC 27002) o Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en iso.org. («ISO27000.esâ" El portal de ISO 27001 en español. Gestión de Seguridad de la Información», s. f.)

*2.2.2.4. ISO 17799*

Es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización. (ISO17799.pdf, s. f.)

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio. (ISO17799.pdf, s. f.)

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad. (ISO17799.pdf, s. f.)

Se trata de una norma NO CERTIFICABLE, pero que recoge la relación de controles a aplicar (o al menos, a evaluar) para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI) según la norma UNE 71502, CERTIFICABLE. (ISO17799.pdf, s. f.)

La norma UNE-ISO/IEC 17799 establece diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

1. Política de seguridad.
2. Aspectos organizativos para la seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Desarrollo y mantenimiento de sistemas.

9. Gestión de continuidad del negocio.
1. Conformidad con la legislación.

De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo). (ISO17799.pdf, s. f.)

### *2.2.3. Amenazas, riesgos y vulnerabilidades*

Según (Prandini & Pallero, 2013) amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre la confidencialidad, integridad, disponibilidad y autenticidad de los datos en un sistema informático. Además, se define riesgo como la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio. Mientras que vulnerabilidad es una debilidad en un sistema informático que puede ser el medio para causar un daño. Las debilidades pueden presentarse en el hardware o en el software de un sistema informático.

Según (Arias Buenaño, Merizalde Almedida, & Natasha, 2013), generalmente las vulnerabilidades informáticas se originan por lo siguiente:

- Fallas en el diseño o construcción del software; por ejemplo, sistemas operativos, programas de aplicación, el protocolo de comunicaciones TCP/IP.
- Uso de PC, programas y equipos de red de tipo genérico en aplicaciones críticas.
- Atención insuficiente al potencial error humano durante el diseño, implementación o explotación de sistemas.
- Confianza excesiva en algún único dispositivo u oficina de seguridad.
- Falta de seguimiento de las políticas, procedimientos e indicadores de seguridad.
- Pobre o nula gestión de activos informáticos.
- Modificaciones frecuentes de elementos de la plataforma informática.
- Planes de contingencia nulos o pobres, para incidentes de seguridad de la información.
- Ignorancia, negligencia o curiosidad por parte de usuarios en general de los sistemas.

- Equipos, programas y redes "heredados" de generaciones tecnológicas anteriores.
- Baja concientización del personal en general sobre la importancia de la seguridad y responsabilidades compartidas e integrales (Voutssas, 2010).

### *2.2.4. Alta disponibilidad*

(High availability) es la capacidad de garantizar que los datos y aplicaciones se encuentren disponibles para los usuarios autorizados en todo momento y sin interrupciones, debido principalmente a su carácter crítico. El objetivo es mantener los sistemas de TI funcionando 24 horas 7 días de la semana, durante todo el año, minimizando al máximo las interrupciones sea estas planeadas e imprevistas (Santos, 2014).

#### *2.2.4.1. Clúster*

Se denomina clúster a un sistema distribuido formado por un conjunto de computadoras autónomas interconectadas y fuertemente acopladas, que es utilizado como un recurso computacional unificado (Pfister, 1998). Los clústeres son utilizados principalmente para mejorar la disponibilidad y/o rendimiento de los datos y aplicaciones. Los Clúster pueden clasificarse en:

- High Performance Computing Clúster (HPCC), Clúster de Alto Rendimiento
- High Availability Computing Clúster (HA), Clúster de Alta Disponibilidad.
- High Throughput Computing Clusters (HT o HTCC), Clusters de Alta Eficiencia).

#### *2.2.4.2. Clúster de Alto Rendimiento*

Un clúster es un conjunto de computadoras de bajo costo conectados entre sí a través de una red de comunicaciones de alta velocidad, que operan bajo software que actúa como un sistema único de administración, responsable de distribuir las cargas de trabajo entre los nodos, de forma automática y transparente al usuario como si se tratara de un único ordenador (Perez, Mendez, Ayusa, Aucapiña, & Lopez, 2013).

Un clúster de alto rendimiento es usado fundamentalmente con fines académico - científicos, su objetivo principal es proporcionar altas prestaciones de capacidad de cómputo superior a los que pudiera ofrecer un ordenador común. Este modelo de arquitectura son una alternativa a la utilización de grandes y costosas supercomputadoras (Morros, 2013),

*2.2.4.3. Clúster de alta disponibilidad*

Un clúster de alta disponibilidad es un grupo de dos o más servidores, caracterizado por compartir el sistema de almacenamiento, se monitorean entre sí constantemente. Si se produce una falla de hardware o servicios de alguno de las máquinas que forman el clúster, el software de alta disponibilidad es capaz de reiniciar automáticamente los servicios que han fallado en cualquiera de los otros equipos del clúster. Y cuando el servidor que ha fallado se recupera, los servicios se migran de nuevo a la máquina original (Clavijo, 2010).

*2.2.4.4. Clúster de Alta Eficiencia*

Este tipo de clúster están diseñados con el objetivo ejecutar la mayor cantidad de tareas en el menor tiempo posible. Existe independencia de datos entre las tareas individuales. El retardo entre los nodos del clúster no es considerado un gran problema ( Montes de Oca, De Giusti, De Giusti, & Naiouf, 2012).

### *2.2.5. Virtualización*

La virtualización es una tecnología que simula la funcionalidad de hardware para crear servicios de TI basados en software como servidores de aplicaciones, almacenamiento y redes (Citrix, 2020). Es decir, la virtualización utiliza el software para reproducir las características del hardware y crear un sistema informático virtual. Lo cual permite a las organizaciones de TI ejecutar más de un sistema virtual, y múltiples sistemas operativos y aplicaciones, en un solo servidor físico. Obteniéndose ventajas económicas, mayor eficiencia, continuidad del negocio, disponibilidad de los servicios (vmware, 2020), tal como muestra en la Figura 1-2.

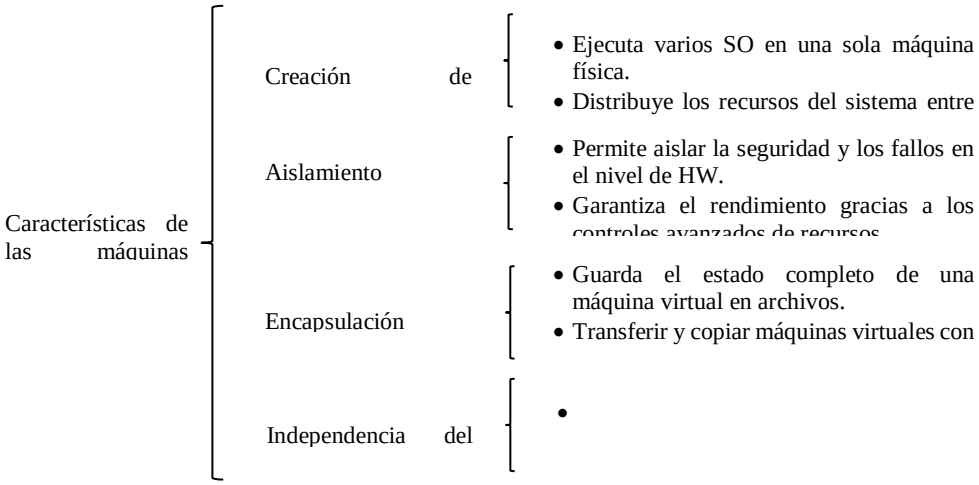



**Figura 1-2:** Características de las máquinas virtuales
**Fuente:** VMware, 2020.

*2.2.5.1. Tipos de virtualización*

En la Tabla 1-2 se explican los diferentes tipos de virtualización

**Tabla 1-2:** Tipos de virtualización

| Tipo de virtualización | Características |
|---|---|
| Virtualización de servidores | Permite ejecutar múltiples sistemas operativos en un solo servidor físico por medio de máquinas virtuales que ofrecen un elevado rendimiento. |
| Virtualización de aplicaciones y virtualización de escritorios | Virtualización de aplicaciones. - los usuarios pueden ejecutar aplicaciones independientemente del sistema operativo que se esté utilizando. Por ejemplo, ejecutar virtualmente una aplicación Windows en un sistema operativo Linux o Mac<br>Virtualización de escritorios. - permite a los usuarios simular la carga de una estación de trabajo para acceder a un escritorio de forma remota desde un dispositivo conectado, como un cliente ligero en un escritorio. |
| Virtualización de redes | Permite ejecutar las aplicaciones en una red virtual del mismo modo que en una red física. La virtualización de red muestra los dispositivos y servicios de red lógicos (puertos lógicos, conmutadores, enrutadores, cortafuegos, equilibradores de carga, VPN, etc.) a las cargas de trabajo vinculadas. |
| Virtualización de almacenamiento | Su objetivo es la representación virtual de los diversos recursos de almacenamiento de una organización, tales como discos duros, memorias flash o unidades de cinta, con la finalidad de hacerlos disponibles como un grupo de recursos interrelacionado. |
| Virtualización de datos | Permite que una aplicación acceda y aproveche los datos sin solicitar detalles como dónde se encuentran físicamente los datos ni el formato de dichos datos. |

***Fuente:*** *IONOS, 2020*
***Realizado por****: Quiñonez, J. 2021*

*2.2.5.2. Herramientas de virtualización*

En la Tabla 2-2 se describirán varias herramientas que permiten virtualizar equipos de computación.

**Tabla 2-2:** Herramientas de virtualización

| Herramienta de virtualización | Se puede instalar máquinas virtuales | Características |
|---|---|---|
| **VMware**. - Creado por Dell EMC para ordenadores compatibles X86 | Windows, Linux o NetWare | • Herramienta multiplataforma<br>• Clonación de máquina virtual<br>• Arranque de varias máquinas virtuales simultáneamente<br>• Encriptación de máquinas virtuales<br>• Soporta aceleración 3D<br>• Soporta USB 2.0 y 3.0 también es limitado |
| **Oracle VM VirtualBox**. - Desarrollado en Oracle para crear entornos virtuales | Linux, Mac y Windows | • Multiplataforma<br>• Puede virtualizar múltiples SO<br>• Software libre<br>• Portable<br>• Soporte 3D VirtualBox |

| | | |
|---|---|---|
| **Microsoft Hyper-v**.- Lanzado 2008 y se integra perfectamente con Microsoft, permitiendo un mejor aprovechamiento de los recursos | Windows como distintas versiones de Linux y FreeBSD | • Funcionalidad de redes SR-IOV<br>• Migración de maquias virtuales en caliente desde un servidor otro<br>• VHDX compartido |
| **Citrix XenServer**. - La compañía Citr-ix adquirió en 2007 el kernel del Hypervisor Xen para desarrollarlo de forma independiente. | Windows y Linux y entrega una plataforma extremadamente asequible para la consolidación de aplicaciones, escritorios y del servidor. | • Migraciones en caliente<br>• Virtualización por hardware<br>• Monitorización de rendimiento<br>• Capacidad para compartir archivos de forma directa |
| **Proxmox**. - Es un Hypervisor de código abierto GNU Linux | Linux en todas sus versiones, Microsoft Windows 10 / 2016 / 2012 / 7 / 8/ 2003 / XP, Solaris, AIX, entre otros | • Migración en caliente<br>• Optimización para puentes de red<br>• Herramientas en línea de comandos, como bueno software Linux<br>• Disponibilidad de copias de seguridad<br>• Preinstalación de plantillas de construcción de sistemas operativos |

***Realizado por:*** *Quiñonez, J. 2021*

### *2.2.6. Máquina virtual*

Una máquina virtual se define como un sistema informático virtual, es decir, un contenedor de software bien aislado que incluye un sistema operativo y una aplicación. Cada máquina virtual autónoma e independiente. Si se instalan varias máquinas virtuales en un mismo PC, se puede ejecutar varios sistemas operativos y aplicaciones en un solo servidor físico (vmware, 2020). En la fig. 1 se listan las características de las máquinas virtuales.

Un sistema informático virtual se denomina "máquina virtual" (Virtual Machine, VM): un contenedor de software muy aislado en el que se incluyen un sistema operativo y aplicaciones. Cada una de las VM autónomas es completamente independiente. Si se colocan varias VM en una misma computadora, se pueden ejecutar varios sistemas operativos y aplicaciones en un mismo servidor físico o "host". («Virtualization Technology & Virtual Machine Software», s. f.)

Una capa delgada de software, denominada "hypervisor", separa las máquinas virtuales del host y asigna de forma dinámica recursos de procesamiento a cada máquina virtual, según sea necesario. («Virtualization Technology & Virtual Machine Software», s. f.)

#### *2.2.6.1. Propiedades clave de las máquinas virtuales*

Las VM ofrecen varias ventajas, relacionadas con las siguientes características.

*Creación de particiones*

- Ejecuta múltiples sistemas operativos en una máquina física.

- Divide los recursos del sistema entre las máquinas virtuales.

*Aislamiento*

- Proporciona aislamiento por fallas y seguridad en el nivel del hardware.
- Conserva el rendimiento con controles de recursos avanzados.

*Encapsulamiento*

- Almacena el estado completo de una máquina virtual en archivos.
- Mueve y copia máquinas virtuales con la misma facilidad con la que mueve y copia archivos.

*Independencia de hardware*

- Aprovisiona o migra cualquier máquina virtual a cualquier servidor físico.

*2.2.6.2. Virtualización de servidores*

La virtualización de servidores es una arquitectura de software que permite que más de un sistema operativo de servidor se ejecute como invitado en un host de servidor físico específico. Al abstraer el software de servidor de la máquina física de esta manera, el servidor se convierte en una "máquina virtual," separado de la superficie física, si bien el servidor "cree" que se está ejecutando exclusivamente en los recursos de memoria y de computación. Realmente se está ejecutando en una imitación virtual del hardware de servidor.(«¿Qué es la virtualización de servidores?», s. f.)

La virtualización de servidores permite ejecutar múltiples sistemas operativos como máquinas virtuales de gran eficiencia en un único servidor físico. Entre las ventajas clave, se incluyen las siguientes:

- Aumento de la eficiencia de TI
- Reducción de gastos operacionales
- Implementación de cargas de trabajo más rápida
- Aumento del rendimiento de las aplicaciones
- Mayor disponibilidad del servidor

- Eliminación de la complejidad y la expansión de servidores.(«Virtualization Technology & Virtual Machine Software», s. f.)

### *2.2.7. Contenedores*

Un contenedor o Docker, en inglés, es una unidad estándar de software que paquetes código y todas sus dependencias para la aplicación funciona rápida y confiable de un entorno a otro. Una imagen de envase de Docker es un peso ligero, independiente, es un paquete de software que tiene todo lo necesario para ejecutar una aplicación, incluye ejecutable de: código, tiempo de ejecución, herramientas del sistema, bibliotecas de sistema y configuraciones. («What is a Container?», s. f.)

Imágenes de contenedores se convierten en contenedores en tiempo de ejecución y en el caso de envases de cargadores - imágenes se convierten en contenedores cuando ejecuta en Dockers Engine. Disponible tanto para Linux y las aplicaciones basadas en Windows, software en contenedores voluntad siempre ejecutan el mismo, independientemente de la infraestructura. Contenedores aislar software de su entorno y asegurar que funcione uniformemente a pesar de las diferencias por ejemplo entre el desarrollo y puesta en escena.

Los Contenedores de cargadores que se ejecutan en Dockers Engine:

*Estándar:* Docker creó el estándar del sector de envases, pueden ser portátil en cualquier lugar

*Ligero:* Contenedores comparten el núcleo del sistema operativo de la máquina y por lo tanto no requieren de un sistema operativo por el uso, conduce a una mayor eficiencia del servidor y reduciendo el servidor y los costos de licencias

Seguro: Aplicaciones son más seguras en contenedores y Docker proporciona las capacidades de aislamiento por defecto más fuerte en la industria.

#### *2.2.7.1. Ventajas de los contenedores*

*Modularidad*

El enfoque contenedor o Docker para la creación de contenedores se centra en la capacidad de tomar una parte de una aplicación, para actualizarla o repararla, sin necesidad de tomar la aplicación completa. Además de este enfoque basado en los microservicios, puede compartir procesos entre varias aplicaciones de la misma forma que funciona la arquitectura orientada al servicio (SOA).(«¿Qué es Docker?», s. f.)

*Control de versiones de imágenes y capas*

Cada archivo de imagen de Docker se compone de una serie de capas. Estas capas se combinan en una sola imagen. Una capa se crea cuando la imagen cambia. Cada vez que un usuario especifica un comando, como ejecutar o copiar, se crea una nueva capa. («¿Qué es Docker?», s. f.)

Docker reutiliza estas capas para construir nuevos contenedores, lo cual hace mucho más rápido el proceso de construcción. Los cambios intermedios se comparten entre imágenes, mejorando aún más la velocidad, el tamaño y la eficiencia. El control de versiones es inherente a la creación de capas. Cada vez que se produce un cambio nuevo, básicamente, usted tiene un registro de cambios incorporado: control completo de sus imágenes de contenedor. («¿Qué es Docker?», s. f.)

*Restauración*

Probablemente la mejor parte de la creación de capas es la capacidad de restaurar. Toda imagen tiene capas. ¿No le gusta la iteración actual de una imagen? Restáurela a la versión anterior. Esto es compatible con un enfoque de desarrollo ágil y permite hacer realidad la integración e implementación continuas (CI/CD) desde una perspectiva de las herramientas. («¿Qué es Docker?», s. f.)

*Implementación rápida*

Solía demorar días desarrollar un nuevo hardware, ejecutarlo, proveerlo y facilitarlo. Y el nivel de esfuerzo y sobrecarga era extenuante. Los contenedores basados en Docker pueden reducir el tiempo de implementación a segundos. Al crear un contenedor para cada proceso, puede compartir rápidamente los procesos similares con nuevas aplicaciones. Y, debido a que un SO no necesita iniciarse para agregar o mover un contenedor, los tiempos de implementación son sustancialmente inferiores. Además, con la velocidad de implementación, puede crear y destruir la información creada por sus contenedores sin preocupación, de forma fácil y rentable. («¿Qué es Docker?», s. f.)

Por lo tanto, la tecnología Docker es un enfoque más granular y controlable, basado en microservicios, que prioriza la eficiencia.

# CAPÍTULO III

## 3. DISEÑO DE INVESTIGACIÓN

Este apartado muestra de manera detallada los pasos de la metodología utilizada para el desarrollo de esta investigación, esto es la descripción del tipo y diseño de la investigación, los materiales y métodos, las técnicas e instrumentos de recolección de datos que fueron los insumos para la comprobación de la respectiva hipótesis.

Esta investigación es de tipo cuasi-experimental, ya que se realizó las pruebas y mediciones del sistema con los servicios de la UTELVT, configurados en un entorno virtualizado, en donde se pueden caracterizar algunas variables. (Arias, 2012).

El método de investigación utilizado fue hipotético deductivo, debido a que se planteó una hipostasis que fue verificada mediante los resultados de la experimentación. (Sánchez, 2012)

Así mismo, el presente estudio tiene un enfoque cuantitativo, identificado en la medición que se realiza de las diferentes variables que caracterizan el fenómeno, estas mediciones nos permitieron contrastar los resultados con referencia a la hipótesis. (Hernández, Fernández, & Baptista, 2014).

Además, el alcance de este trabajo es de tipo descriptivo, porque se caracteriza la situación actual y la situación deseada en cuanto a la disponibilidad y seguridad del sistema objeto de estudio. (Ñaupas, Mejia, Novoa, & Villagomez, 2014).

### 3.1. Población de estudio

Debido a la caracterización del presente estudio, no se requiere población y muestra; ya que objeto de estudio es un sistema que está basado en componentes tecnológicos de número limitado.

### 3.2. Unidad de análisis

El estudio se realizó en la Universidad Técnica Luis Vargas Torres de Esmeraldas (UTELVT).

### 3.3. Identificación de las variables

**Variables independientes:** Infraestructura virtualizada de Alta Disponibilidad mediante el uso de software libre.

**Variables dependientes:** Disponibilidad y seguridad en las aplicaciones y servicios web de la UTELVT.

## 3.4. Operacionalización de las variables

**Tabla 1-3:** Operacionalización de variables

| Hipótesis | Variables | Indicadores |
|---|---|---|
| **La implementación de una infraestructura virtualizada de Alta Disponibilidad mediante el uso de software libre, mejorará la disponibilidad y seguridad en las aplicaciones y servicios web de la UTELVT.** | **Independiente:**<br>Infraestructura virtualizada de Alta Disponibilidad | • Porcentaje de disponibilidad del sitio web [A(t)]<br>• Tiempo de inactividad anual total [I(t)]<br>• Tiempo medio para que ocurra un fallo [MTTF]<br>• Tiempo medio entre fallos [MTBF]<br>• Tiempo medio para la transición. [MTTT]<br>• Tiempo medio para recuperarse. [MTTR] |
| | **Dependiente:**<br>Disponibilidad y seguridad en las aplicaciones y servicios web de la UTELVT. | • Número de incidentes de seguridad de la información<br>• Tratamiento que se le da a los incidentes de seguridad de la información<br>• Documentación institucional sobre seguridad<br>• Nivel de cultura de seguridad de los administradores de los sistemas de información. |

***Realizado por:*** *Quiñonez, J. 2021*

## 3.5. Matriz de consistencia

**Tabla 2-3:** Matriz de consistencias.

| Formulación del problema | Objetivo general | Hipótesis | Variables | Indicadores | Índice | Técnica | Instrumento |
|---|---|---|---|---|---|---|---|
| ¿Cómo debe ser el sistema de virtualización que se pueda aplicar para el fortalecimiento de la disponibilidad y seguridad en las aplicaciones y servicios web de la UTELVT? | Elaborar y evaluar un sistema que permita mejorar la disponibilidad y seguridad en los servicios web de la UNIVERSIDAD TÉCNICA LUIS VARGAS TORRES, mediante el uso de herramientas de software libre. | La implementación de un sistema de virtualizado de Alta Disponibilidad mediante el uso de software libre, mejorará la disponibilidad y seguridad en las aplicaciones y servicios web de la UTELVT. | **Independiente** Implementación de un sistema virtualizado de Alta Disponibilidad mediante el uso de software libre, | • Porcentaje de disponibilidad del sitio web<br>• Tiempo medio para que ocurra un fallo [MTTF]<br>• Tiempo medio entre fallos [MTBF]<br>• Tiempo medio para la transición. [MTTT]<br>• Tiempo medio para recuperarse. [MTTR] | • Tanto por ciento (%) | • Observación | A(t)= MTBF / MTBF+MTTR<br><br>MTBF=MTTF+MTTR |
| | | | **Dependiente:** Disponibilidad y seguridad en las aplicaciones y servicios web de la UTELVT. | • Número de incidentes de seguridad de la información | • Tanto por ciento (%) | • Observación | • Registro de incidentes<br>• Herramientas de monitoreo de incidentes de seguridad de la información |
| | | | | • Tratamiento que se le da a los incidentes de seguridad de la información | • Tanto por ciento (%) | • Observación | • Registro de incidentes<br>• Cuestionario |
| | | | | • Documentación institucional sobre seguridad de la información | • Tanto por ciento (%) | • Entrevista | • Cuestionario |
| | | | | • Nivel de cultura de seguridad de los administradores. | • Tanto por ciento (%) | • Entrevista | • Plan de capacitación sobre seguridad de la información |

***Realizado por:*** *Quiñonez, J. 2021*

## 3.6. Técnicas de recolección de datos primarios y secundarios

Las técnicas a utilizarse en la presente investigación son las siguientes:

**Primarias:**

- Entrevistas al personal de TIC's de la UTELVT, administradores de sistemas y aplicaciones.
- Observación directa para determinar la organización del hardware y software del Data Center.
- Experimentación para las pruebas en el ambiente controlado.

**Secundarias**:

- Análisis Documental, sitios web y textos referentes al tema de estudio.

## 3.7. Instrumentos de recolección de datos primarios y secundarios

- Cuestionario que consiste en una lista de preguntas escritas que se entregó a los entrevistados.
- Fichas de Observación para recolectar características importantes para la investigación.

### *3.7.1. Instrumentos de software*

**Tabla 3-3:** Instrumentos de software

| Nombre | Versión | Descripción | Funcionalidad |
|---|---|---|---|
| VMware® Workstation 16 Pro | 16.1.0 | Máquina virtual | Crear /ejecutar máquinas virtuales en PC |
| Proxmox Virtual Environment | proxmox-ve_6.3-1 | Entorno de virtualización de servidores de código abierto | Virtualizar servidores, configurar nodos, redundancia, Alta disponibilidad |

***Realizado por:*** *Quiñonez, J. 2021*

### *3.7.2. Instrumentos de Hardware*

**Tabla 4-3:** Instrumentos de Hardware

| Nombre | Descripción | Funcionalidad |
|---|---|---|
| Proxmox1 | Pc01 | Ejecutar la máquina virtual Proxmox1 |
| Proxmox2 | Pc02 | Ejecutar la máquina virtual Proxmox2 |
| Proxmox3 | Pc03 | Ejecutar la máquina virtual Proxmox3 |

***Realizado por:*** *Quiñonez, J. 2021*

### 3.8. Configuración actual, sin HA

En la actualidad la Universidad Técnica "Luis Vargas Torres" de Esmeraldas, cuenta con un equipo de bastidor compacto Marca HP tipo Blade, con 3 módulos físicos o servidores.

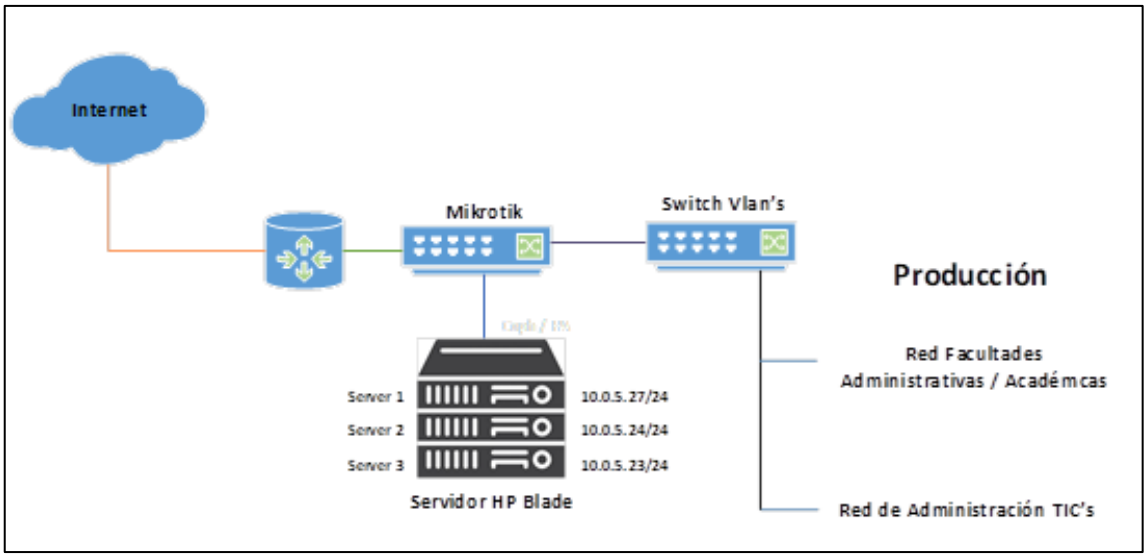



**Figura 1-3:** Diseño del sistema UTELVT
***Fuente:*** *Departamento de TIC's UTELVT*
***Realizado por:*** *Quiñonez, J. 2021*

Como muestra la Figura 1-3, los servidores están conectados directamente a la red Administrativa y Académica, sin discriminar la conexión a la red del Departamento de TIC's; lo cual no define una red autorizada para el acceso administrativo a los equipos.

A su vez, existe una segmentación lógica de la red a través de Vlan´s, para organizar el tráfico en grupos, evitar problemas de broadcast y darle algo de seguridad a la red.

El servidor físico contiene servidores virtuales administrados con VMWare, dichas máquinas virtuales tienen sistemas operativos como Windows Server y Linux Centos, utilizados para configurar ciertos servicios, los detalles más relevantes se muestran en la siguiente Tabla:

**Tabla 5-3**: Equipos Servidores UTELVT

| Servidor | Hardware | Software | Servicios | Sistema Operativo | Estado |
|---|---|---|---|---|---|
| **Server 1**<br>10.0.05.27 | Procesador de 6 Núcleos, 250GHz<br>128 GB Memoria RAM<br>1TB de HDD | VMWare | Eset<br>KOHA Biblioteca<br>SIAD APP WEB-BK<br>SIAD DB1<br>SIAD DB2<br>SIC DB | Windows Server<br>Linux Centos<br>Windows Server<br>Linux Centos<br>Linux Centos<br>Linux Centos | ok<br>ok<br>ok<br>ok<br>ok<br>ok |

| | | | | | |
|---|---|---|---|---|---|
| | | | SIC DB-BK | Linux Centos | ok |
| | | | VS APPs | Windows Server | ok |
| | | | Aula Virtual | Linux Centos | ok |
| | | | DomainController | Windows Server | off |
| | Procesador de 6 Núcleos, | | Moodle | Linux Centos | ok |
| **Server 2** | 250GHz | VMWare | SIAD APP WEB | Windows Server | off |
| 10.0.05.24 | 64 GB Memoria RAM | | SIC APP WEB | Windows Server | off |
| | 280 GB de HDD | | | | |
| | Procesador de 6 Núcleos, | | DSPACE | Linux Centos | ok |
| **Server 3** | 250GHz | VMWare | OTRS | Linux Centos | ok |
| 10.0.05.23 | 64 GB Memoria RAM | | SIC APP Local | Windows Server | off |
| | 280 GB de HDD | | DomainController2 | Windows Server | ok |

***Fuente:*** *Departamento de TIC's UTELVT*
***Realizado por:*** *Quiñonez, J. 2021*

Asimismo, se puede ver el comportamiento de los servidores en día promedio con cargas de trabajo medio, lo podemos observar en las Figuras 2-3 y 3-3:

Servidor 1

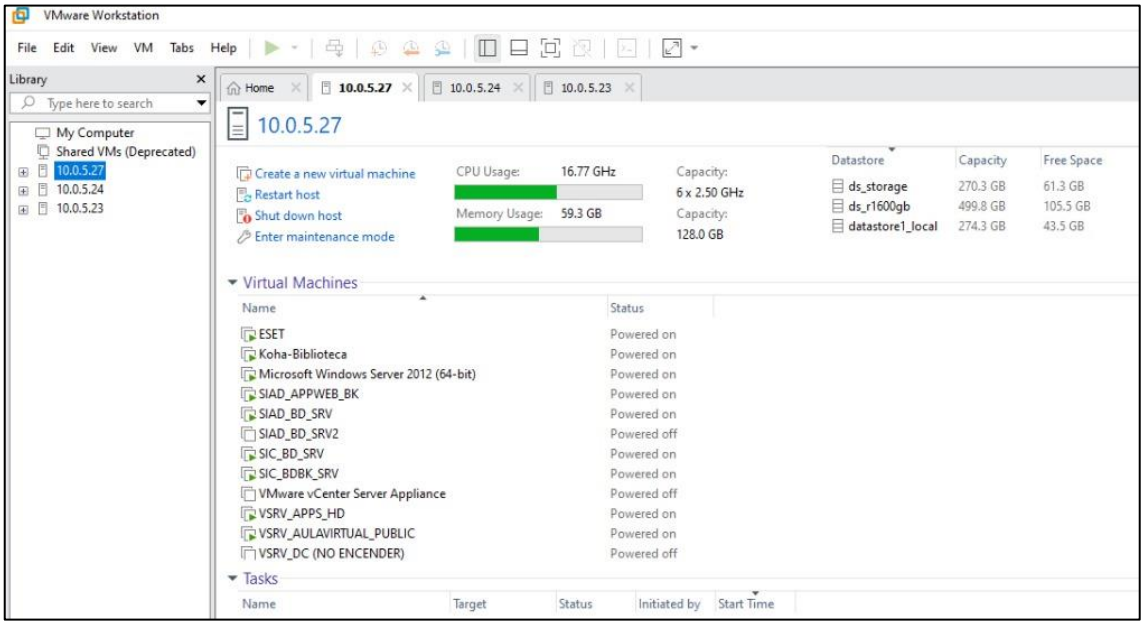



**Figura 2-3:** Desempeño Servidor 1
***Fuente:*** *Departamento de TIC's UTELVT, 2021.*

Servidor 2

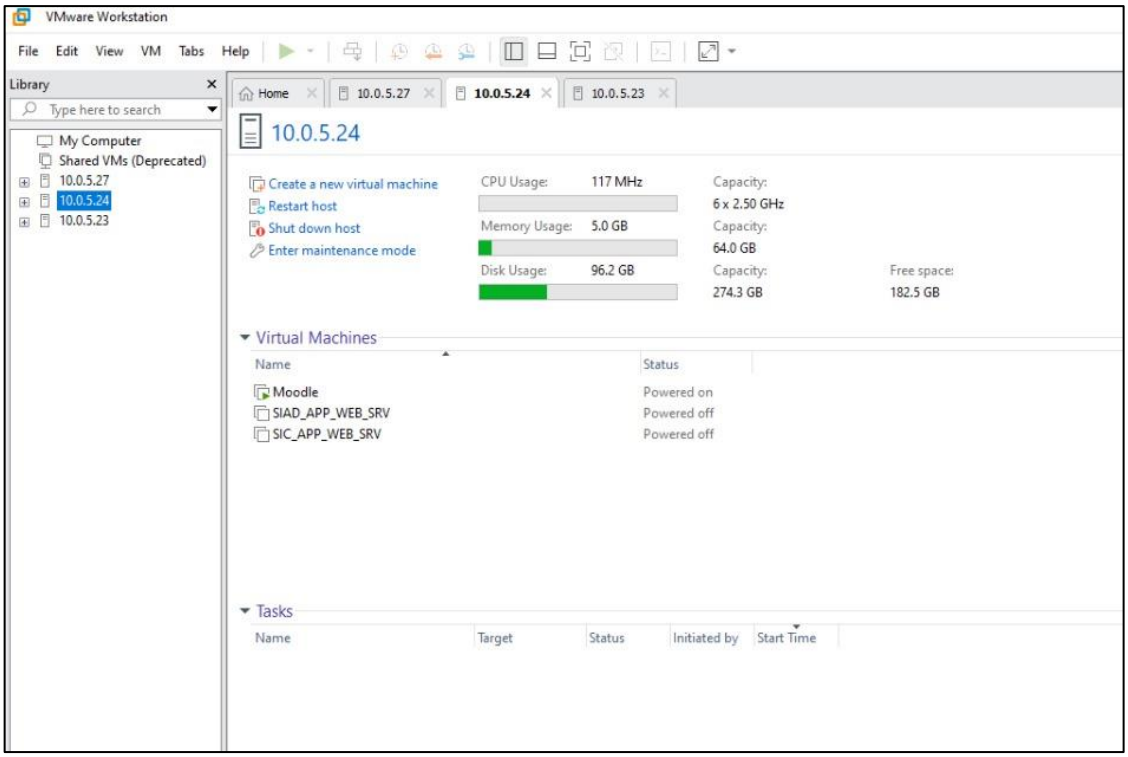



**Figura 3-3:** Desempeño Servidor 2
***Fuente:*** *Departamento de TIC's UTELVT, 2021.*

Servidor 3

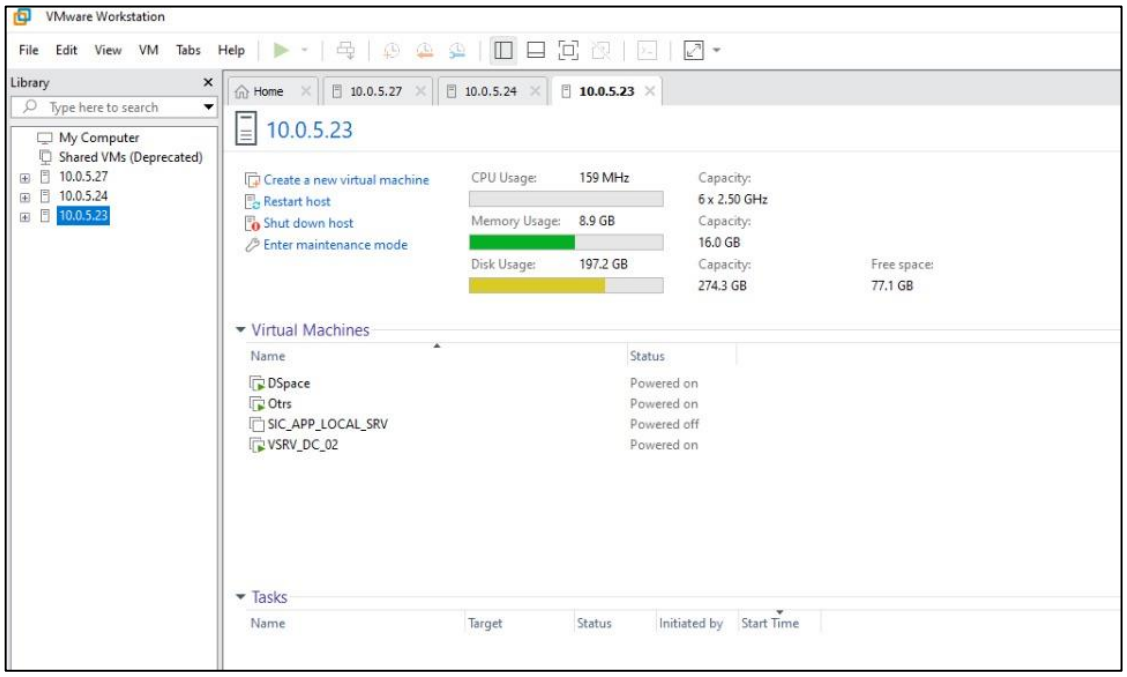



**Figura 4-3:** Desempeño Servidor 2
***Fuente:*** *Departamento de TIC's UTELVT, 2021.*

### 3.9. Cálculo de la disponibilidad del sistema actual, sin HA

Es importante aclarar que los parámetros utilizados para los cálculos de la disponibilidad o A(t) esta basados en el estándar internacional y adoptada por el Instituto Ecuatoriano de Normalización (INEN), NTE INEN-IEC 60300; en la cual se definen las mejores prácticas para mantener confiable a un sistema computacional.

Mediante la entrevista realizada al encargado de los servidores del datacenter de la UTELVT, se logró determinar valores para el cálculo estándar de la disponibilidad del sistema actual. Utilizamos como unidad de tiempo la hora y los valores promedios al año.

Las variables a utilizar son:

MTTF (**M**ean **T**ime **t**o **F**ailure) es el tiempo medio para un fallo.

MTBF (**M**ean **T**ime **B**etween **F**ailures) es el tiempo medio entre fallos.

MTTT (**M**ean **T**ime **t**o **T**ransition) es el tiempo medio para transición.

MTTR (**M**ean **T**ime **t**o **R**ecover) es el tiempo medio para recuperarse del fallo.

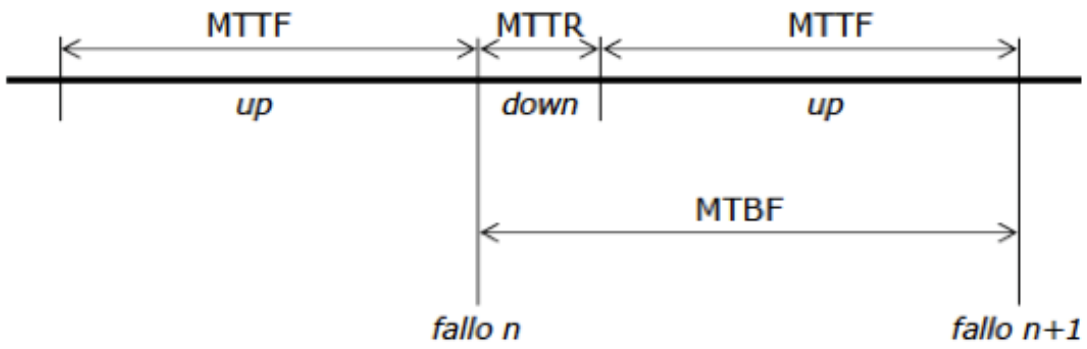



**Figura 5-3:** Variables del Cálculo de la Disponibilidad
***Fuente:*** *NTE INEN-IEC 60300.*

En la Figura 5-3, se define de manera gráfica y cronológica la conceptualización de las variables para el cálculo de la disponibilidad.

Las fórmulas para calcular la disponibilidad o A(t) son:

$$MTBF = MTTF + MTTR$$

$$A(t) = MTTF / (MTTF + MTTR) = MTTF / MTBF$$

Contabilizamos los fallos de los propios servidores, no de los otros componentes de toda la infraestructura, durante un año, aplicamos y obtenemos:

**Tabla 6-3:** Caídas de servicios y tiempos de recuperación al año

| No. | Eventos Fallos | Horas | Días |
|---|---|---|---|
| 1 | Caída Servidor MySQL | 48,00 | 2,00 |
| 2 | Caída del Servidor SIAD | 24,00 | 1,00 |
| 3 | Caída del Control Asistencia | 15,00 | 0,63 |
| 4 | Caída de la red interna | 6,00 | 0,25 |
| 5 | Caída del Servidor SIAD | 24,00 | 1,00 |
| 6 | Caída de Moodle | 48,00 | 2,00 |
| 7 | Caída del Portafolio Docente | 20,00 | 0,83 |
| 8 | Caída de servidor web local | 6,00 | 0,25 |
| | **Tiempo fallos al año** | **191,00** | **7,96** |
| | **Promedios tiempo al año** | **23,875** | **0,995** |

***Fuente:*** *Departamento de TIC's UTELVT*
***Realizado por:*** *Quiñonez, J. 2021*

MTTR = 0.995 días

MTBF = Tiempo / Total fallos = 365 / 8 = 45,625 días

MTTF = MTBF – MTTR = 45,625 – 0,995 = 44.630 días

**A(t)** = MTTF / MTBF = 44.630 / 45.625 = **97.820%**

Este valor de la disponibilidad o A(t) del 97,820% es lo que se mejoró con la implementación del Clúster de Alta Disponibilidad, propuesto.

### 3.10. Cálculo de la disponibilidad del sistema con HA

Continuando con la observación del basados del estándar internacional, NTE INEN-IEC 60300; en la cual se definen las mejores prácticas para mantener confiable a un sistema computacional; se calculó la disponibilidad contemplado la implementación del Clúster de Alta Disponibilidad.

En primera instancia la disponibilidad total de un sistema compuesto o As, está dado por el producto de la disponibilidad de sus componentes, esto es:

$$As = As_1 * As_2 * As_3 * \ldots As_n$$

Dónde $As_1$, $As_2$, $As_3$ hasta $As_n$, son los valores de la disponibilidad de N componentes del sistema, entendiéndose como componentes a los elementos que forman la infraestructura complete del datacenter como la red, equipos de trasmisión, servidores, UPS, etc.

La fórmula utilizada para calcular la disponibilidad en sistemas compuestos con redundancia o As es:

$$As = Ac_{n-1} + ((1 - Ac_n - 1) * Ac_n)$$

Dónde se determina la disponibilidad de un sistema compuesto como el producto de la disponibilidad de cada componente $C_n$ con su mejora; pero en esta investigación se ha tomado solo en cuenta la disponibilidad de los servidores y sus servicios, más no otros componentes como la infraestructura de red, suministro eléctrico, etc.

Por lo antes expuesto, en este caso utilizaremos la siguiente fórmula

$$As = Ac_1 + ( (1 - Ac_1 ) * Ac_2 )$$

Reemplazamos los valores, tomado en cuenta la implementación de la Alta Disponibilidad, dándole al sistema redundante el mismo valor de disponibilidad antes calculado:

Ac1= A(t) = 97, 820%; disponibilidad sin HA

Ac2= A(t) = 97.820%; disponibilidad del servidor redundante

**As** = 97,820 + ((1 – 97,820) * 97,820) = **99,952%**

Como podemos observar se ha mejorado significativamente la disponibilidad del sistema con la implementación del Clúster de Alta Disponibilidad.

# CAPÍTULO IV

## 4. RESULTADOS Y DISCUSIÓN

### 4.1. Presentación, análisis e interpretación de datos

En el presente capitulo se despliegan los resultados obtenidos mediante la aplicación del instrumento preparado para la entrevista y las diferentes fichas de observación para las visitas técnicas al Departamento de TIC's de la UTELVT, todo con el objetivo de caracterizar de cerca la problemática y proponer soluciones.

Inicialmente, una vez aplicado el instrumento de la entrevista, al Ing. Carlos Plata Cabrea, miembro del Departamento de Tics y Responsable del datacenter de la Universidad Técnica Luis Vargas Torres de Esmeraldas; se destacaron los siguientes resultados:

- El sistema de servidores actualmente instalado no tiene una configuración de alta disponibilidad.
- No cuentan con un sistema de backup automatizado de todos los sistemas, solo se realiza una copia de las bases de datos en diferentes servidores del Equipo Blade HP.
- No se cuenta con filtrado de tráfico o firewalls en cada servidor en producción.
- El sistema tiene un periodo de indisponibilidad de 191 horas/año, o 7.96 días/año; su disponibilidad es del 97.820%.
- La plataforma de virtualización utilizada es VMWARE SERVER.
- Sistemas operativos utilizados en los servidores virtuales son Windows Server 2016 y Linux Centos 7.
- El 58,82% de las aplicaciones o servicios virtualizados están residiendo en un solo servidor.
- Existe un equipo, el Server 2, está presentando problemas de funcionamiento, está casi fuera de servicio.
- Un servidor está funcionando solo como Almacenamiento.
- Para la administración de la red se cuenta con un equipo marca Mikrotik, donde se administran diferentes Vlan's para organizar las subredes,
- El problema más persistente del datacenter son las caídas de suministro eléctrico.
- No existe un plan de contingencias ante eventos de caída de los servicios, lo cual no permite realizar un adecuado tratamiento de las adversidades, ni planificar el uso de recursos humanos y tecnológicos para este fin.

- No existe un registro formal de incidentes y sus características, lo cual reduce la posibilidad de reducir significativamente la frecuencia y recuperación ágil de las adversidades.
- No existen políticas de Seguridad formalmente aprobadas y documentadas.
- El nivel de preparación del Personal del Departamento de TIC's de la UTELVT en al ámbito de la Seguridad de la Información, está determinado por su auto educación y experiencia.
- Dentro del POA del Departamento de TIC's de la UTELVT, no existe un plan de capacitación en temas de Seguridad de la Información.

Luego se elaboró y evaluó un sistema de Alta Disponibilidad que permitiera mejorar la disponibilidad y la seguridad, a través de la plataforma de virtualización Proxmox V6.3, que es una herramienta de software libre con soporte para entornos de HA. Se establecieron resultados como:

- Se pudo configurar un sistema Clúster de Alta Disponibilidad, de fácil gestión a través de consolas de administración seguras, a través de túneles SSH.
- La respuesta de respuesta de recuperación ante caídas o fallas de los servidores es automática.
- El tiempo de recuperación de un sistema caído es en promedio de 1min, esto dependerá de las prestaciones del hardware utilizado y la calidad de la red de comunicaciones.
- El almacenamiento compartido permitió configurar tareas y espacios de disco solo para Backups programados.
- Se controló el sistema de administración del Clúster y de sus servidores a través de un sistema de usuarios basado en roles y privilegios con contraseñas seguras.
- Asimismo, en los sistemas operativos de las máquinas virtuales se configuró un control de acceso de usuarios basado en roles y privilegios con contraseñas seguras.
- Se endureció la seguridad realizando configuración de firewalls con políticas restrictivas, en varios niveles: A nivel del Clúster, a nivel de los equipos miembros del Clúster, a nivel de las máquinas virtuales y contenedores.
- Una vez implementado el Sistema de Alta Disponibilidad se alcanzó un nivel de disponibilidad del 99.952%.

### 4.2. Discusión

La Tabla 1-4, expone el incremento de la disponibilidad alcanzada luego de la implementación del Sistema de Alta Disponibilidad utilizando la plataforma de software libre Proxmox.

**Tabla 1-4:** Valores de comparación con y sin HA

| Variable | Sin HA | Con HA | Variación |
|---|---|---|---|
| Disponibilidad | 97,820% | 99,952% | 2,13% |
| indisponibilidad | 2,18% | 0,05% | -2,13% |
| indisponibilidad | 191 horas | 4,206 horas | -186,794 horas |
| Tiempo Promedio de recuperación | 24 horas | 1min | |
| Puntos de control de tráfico y acceso | 2 | 4+n VM | 2+n VM |

***Realizado por:*** *Quiñonez, J. 2021*

En esta implementación se demostró las utilidades que contiene la plataforma Proxmox para la configuración y administración la cual facilitó la elaboración y puesta en marcha del sistema de HA, este resultado concuerda con los resultados de la comparativa sobre entornos de virtualización realiza por Espinoza (2019) donde concluye que el Hypervisor libre Proxmox superó, con más de un 100%, a todos los demás sistemas objetos de estudio, incluido VMWare, al realizar almacenamiento de datos virtualizados.

Del mismo modo, según (Perdigon Llanes & Ramirez Alonso, 2020), en su estudio comparativo entre plataformas de virtualización definen que Proxmox obtuvo los mejores resultaos de funcionamiento en las pruebas de escalabilidad y rendimiento con sistemas en producción; y que además, tal como lo evidencia la presente investigación, es una opción eficiente para implementar sistemas virtualizados con el propósito de ahorrar recursos y utilizar de manera más eficiente las prestaciones del Hardware.

Continuando, en este estudio se logró una sustancial mejora de la disponibilidad a través de la puesta en marcha del Clúster de Alta Disponibilidad o HA, puntualmente se pasó de una disponibilidad del 97.820% a una disponibilidad del 99,952%; mejorando los tiempos de recuperación y tiempo de servicio activo sin interrupciones a la comunidad universitaria. Estos valores son semejantes a los alcanzados por (Flórez Hernández & Huertas Lucena, 2018), ya que luego de implementar un sistema de Virtualización con HA, en la empresa ISP HSE ingeniería SAS, alcanzaron un nivel de disponibilidad del 99.666%.; mejorando sus prestaciones frente a sus clientes.

Es también importante destacar que la implementación del Clúster de Alta disponibilidad permitió balancear la carga de trabajo de los servidores, debido a que ahora ya no es un solo servidor que ejecuta la mayoría de las aplicaciones, el sistema permitió distribuir de manera uniforme las aplicaciones entre los equipos del Clúster, dejan además la flexibilidad de crecimiento a futuro del sistema de HA con el aumento de nodos o servidores; objetivo que también fue obtenido por Acero (2021), luego de evaluar el Sistema de virtualización con HA, afirmo que fue posible balancear la carga de los servidores y lograr un nulo desperdicio de recursos de hardware.

Por otro lado, en cuanto a la mejora de la seguridad desde los ámbitos de Control de tráfico y control de acceso, se logró establecer un patrón para la implementación de las mejoras en los puntos, las reglas, la administración de usuarios y sus roles; coincidiendo con lo recomendado por Nilo (2020) en sus recomendaciones de las mejores prácticas para la administración de firewalls, originando un endurecimiento de la seguridad de los sistemas.

### 4.3. Verificación de la Hipótesis

Ho= Hipótesis nula

H1= Hipótesis alterna

Ho= La implementación de un sistema de virtualizado de Alta Disponibilidad mediante el uso de software libre, NO mejorará la disponibilidad y seguridad en las aplicaciones y servicios web de la UTELVT.

H1= La implementación de un sistema de virtualizado de Alta Disponibilidad mediante el uso de software libre, mejorará la disponibilidad y seguridad en las aplicaciones y servicios web de la UTELVT.

**Tabla 2-4:** Comparación de la Disponibilidad y Seguridad con y sin HA

| Variable | Sin HA | Con HA | Variación |
|---|---|---|---|
| Disponibilidad | 97,820% | 99,952% | 2,13% |
| Puntos de control de tráfico y acceso | 2 | 4 + nVM | 2 + nVM |

***nVm** = Numero de Máquinas Virtuales y/o contenedores*

***Realizado por: Quiñonez, J. 2021***

Como se pudo demostrar, en la Tabla 2-4, que la implementación de un sistema virtualizado de Alta Disponibilidad, mediante el uso de software libre mejoró la disponibilidad y seguridad en las aplicaciones y servicios web de la UTELVT, se acepta la Hipótesis alterna.

# CAPÍTULO V

## 5. PROPUESTA

### 5.1. Metodología para la implementación de un clúster de HA

Persiguiendo las metas de esta investigación, se diseñó un sistema de virtualización aplicando redundancia y alta disponibilidad (HA) para la mejora de la disponibilidad como elemento de seguridad en las operaciones de las aplicaciones de la Universidad Técnica Luis Vargas Torres de Esmeraldas (UTELVT). Para esto, se utilizaron tres equipos servidores, cuyas características están descritas en la tabla no. 9, interconectados entre sí, se utilizó como plataforma de software libre para virtualización en los tres servidores, Proxmox v. 6.3, creando un clúster de HA entre ellos, Uno de los tres servidores se configuro como master del Clúster.

Además, se configuró u sistema de almacenamiento distribuido entre los servidores físicos donde residirán los servidores virtuales y contenedores; aprovechando y organizando los recursos de almacenamiento masivo. Con esto se logra que, si un servidor que contiene la máquina virtual o contenedor, Windows o CentOS falla, automáticamente se inicie el proceso de recuperación, el cual consiste en que ésta migre hacia otro servidor y puedan seguir disponibles todos los servicios; este proceso es casi indetectable por los usuarios.

#### *5.1.1. Diseño del clúster de HA*

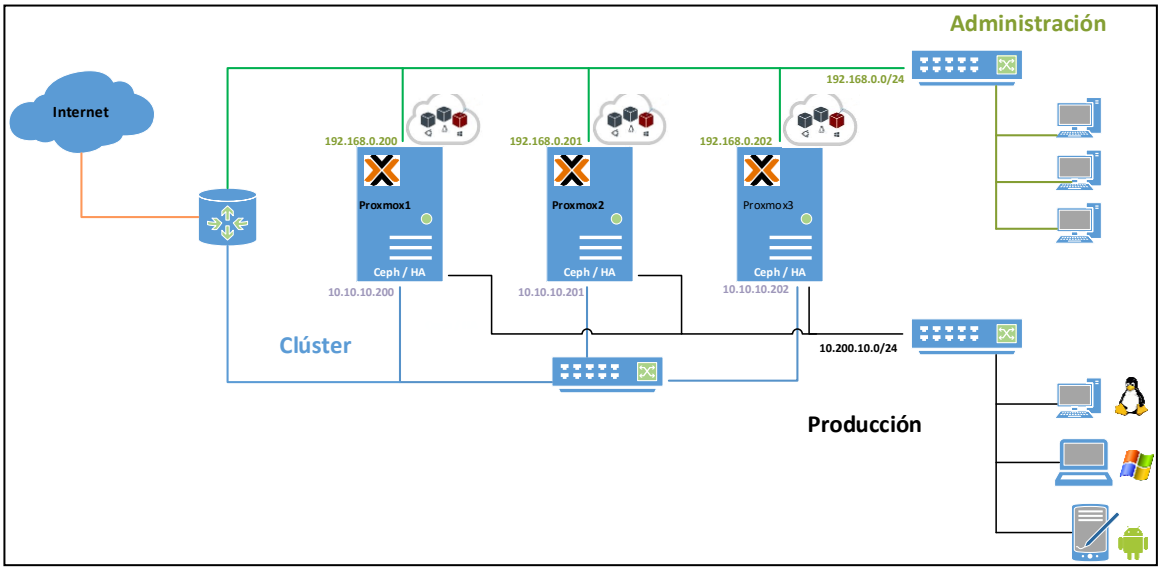



**Figura 1-5:** Diseño del clúster de HA UTELVT
***Realizado por:*** *Quiñonez, J. 2021*

Como indica la Figura 1.-5, el clúster de HA para el fortalecimiento de la seguridad, disponibilidad y prevención de tiempos prolongados de recuperación ante fallas, está conformado por tres servidores físicos, con Proxmox y se configura el servidor de almacenamiento compartido NFS aplicando CEPH. En la Tabla 1-5 se destalla la configuración de la estructura del clúster HA.

**Tabla 1-5:** Detalle de configuración de Servidores Proxmox

| | **MV Proxmox1** | **MV Proxmox2** | **MV Proxmox3** | **MV NFS** |
|---|---|---|---|---|
| **Nombre** | svr1.utelvt.edu.ec | svr2.utelvt.edu.ec | svr3.utelvt.edu.ec | CEPH_NAS |
| **Net Adapter** | 192.168.0.200/24 | 192.168.0.201/24 | 192.168.0.202/24 | |
| **Net Adapter 2** | 10.10.10.200/24 | 10.10.10.201/24 | 10.10.10.202/24 | |
| **Net Adapter 3** | 10.200.10.200/24 | 10.200.10.201/24 | 10.200.10.202/24 | |
| **RAM** | 8GB | 4GB | 8GB | |
| **HD** | 100GB<br>150GB(NAS) | 1000GB<br>150GB(NAS) | 100GB<br>150GB(NAS) | 450GB |
| **Interfaces de red** | 03 (adaptador puente) | 03 (adaptador puente) | 03 (adaptador puente) | |
| **Versión SO** | Proxmox 6.3-1 | Proxmox 6.3-1 | Proxmox 6.3-1 | |

***Realizado por:*** *Quiñonez, J. 2021*

### *5.1.2. Implementación del clúster de HA*

A continuación, se describen las fases de instalación del sistema Clúster de Alta Disponibilidad con Proxmox 6.3; se pretende guiar el proceso por eso solo se mostrarán las pantallas más relevantes.

**Fase 1.** Instalación de VMware® Workstation 16 Pro, ampliación que permite crear y ejecutar máquinas virtuales en PC, una vez instalada esta aplicación se crean las 03 máquinas virtuales Proxmox 6.3-1. En la Figura 2-5 se muestra las características de hardware que debe tener cada una de las 03 máquinas Proxmox.

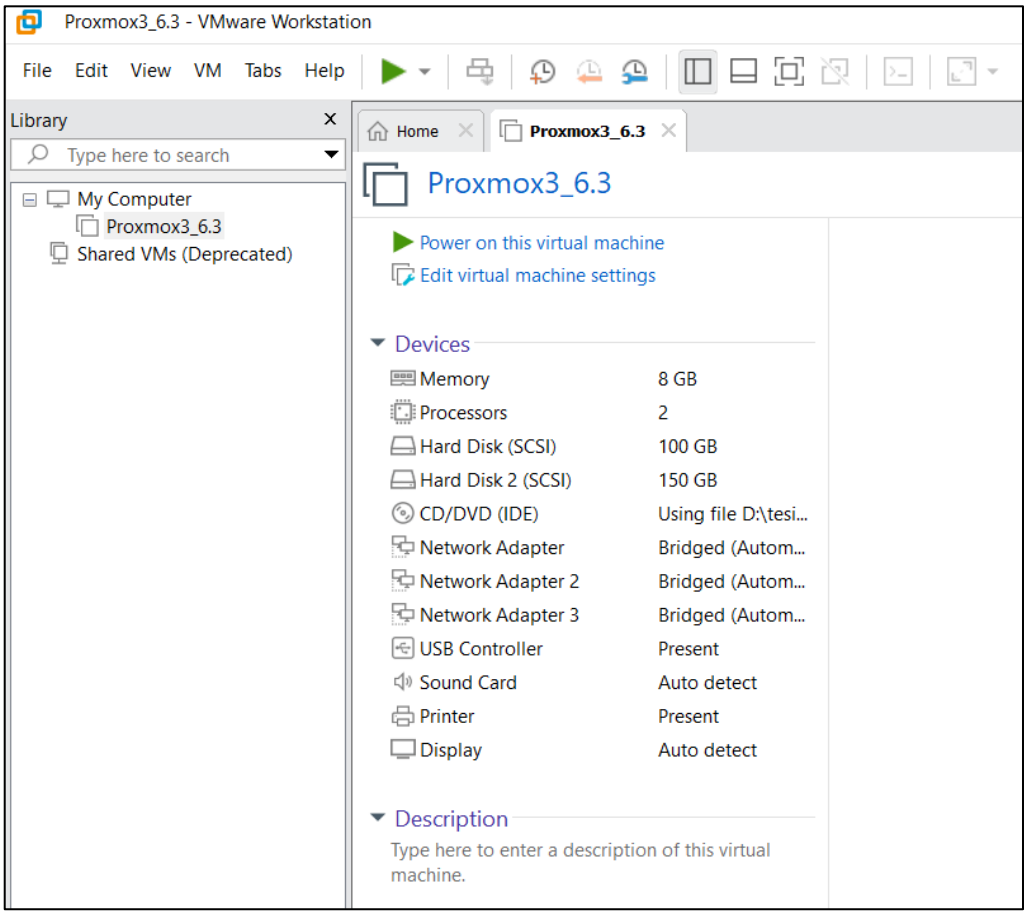



**Figura 2-5:** VMware y máquina virtual Proxmox
***Fuente:*** *Departamento de TIC's UTELVT, 2021.*

**Fase 2.** Se configura el clúster de máquinas Proxmox, para ello se debe primero configurar las tarjetas de red, como se muestra en las Figuras 3-5 y 4-5.

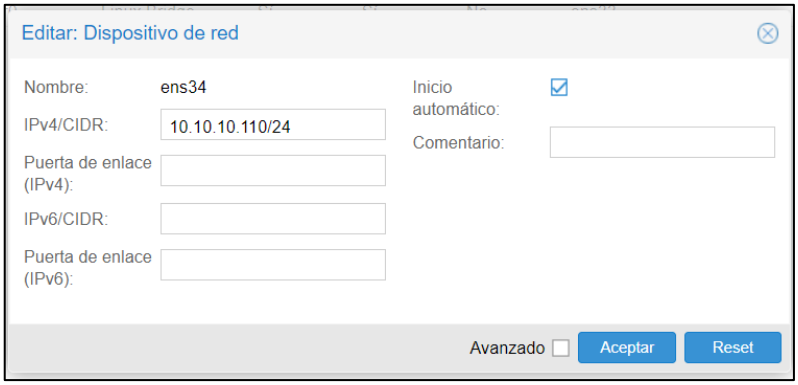



**Figura 3-5:** Configuración de la tarjeta de red ens34
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

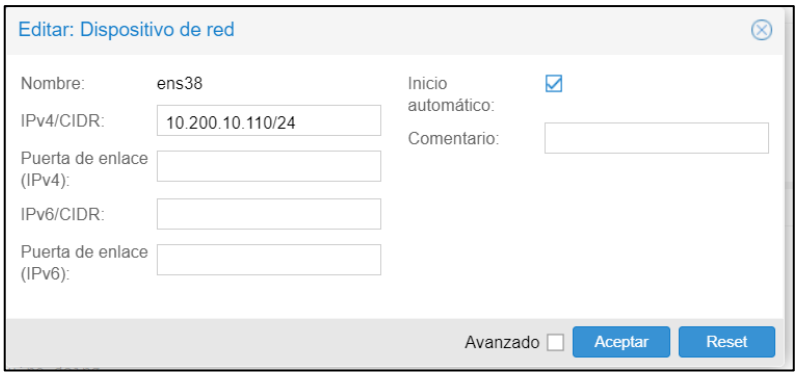



**Figura 4-5:** Configuración de la tarjeta de red ens36
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

A continuación, en la máquina virtual Proxmox1 se configura el clúster incluyendo a las máquinas virtuales Proxmox2 y Proxmox3, se genera una cadena de conexión, la cual se copia, luego en la máquina virtual Proxmox2 se realiza la operación unirse al clúster como se observa en la Figura 5-5, y se pega la cadena de conexión.


**Figura 5-5:** Unirse al clúster maquinas Proxmox2 y Proxmox3
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

En la Figura 6-5 se puede observar la creación del clúster con las maquinas Proxmox1 Proxmox2 y Proxmox3.

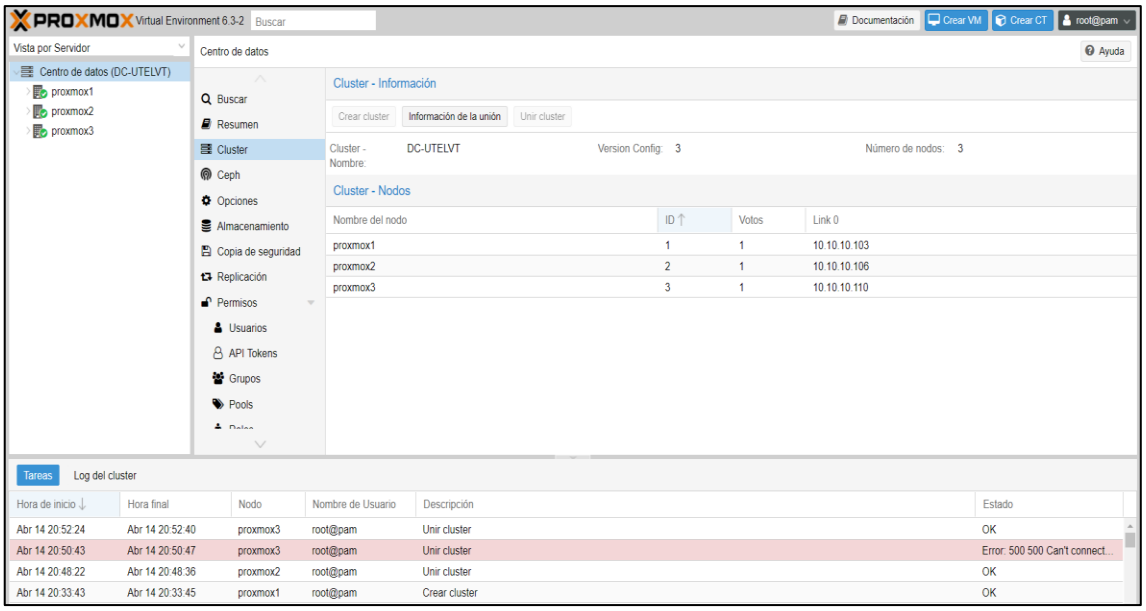



**Figura 6-5:** Clúster maquinas Proxmox1 Proxmox2 y Proxmox
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

**Fase 3.** Se instala y configurara el CEPH para el almacenamiento compartido en cada máquina Proxmox se creó un disco duro de 150GB para el NAS, lo que sumaría 450GB de almacenamiento total compartido entre las 03 máquinas Proxmox. En las figuras 7-5, 8-5 y 9-5 se puede observar cómo lleva a cabo el proceso de configuración del CEPH_NAS.

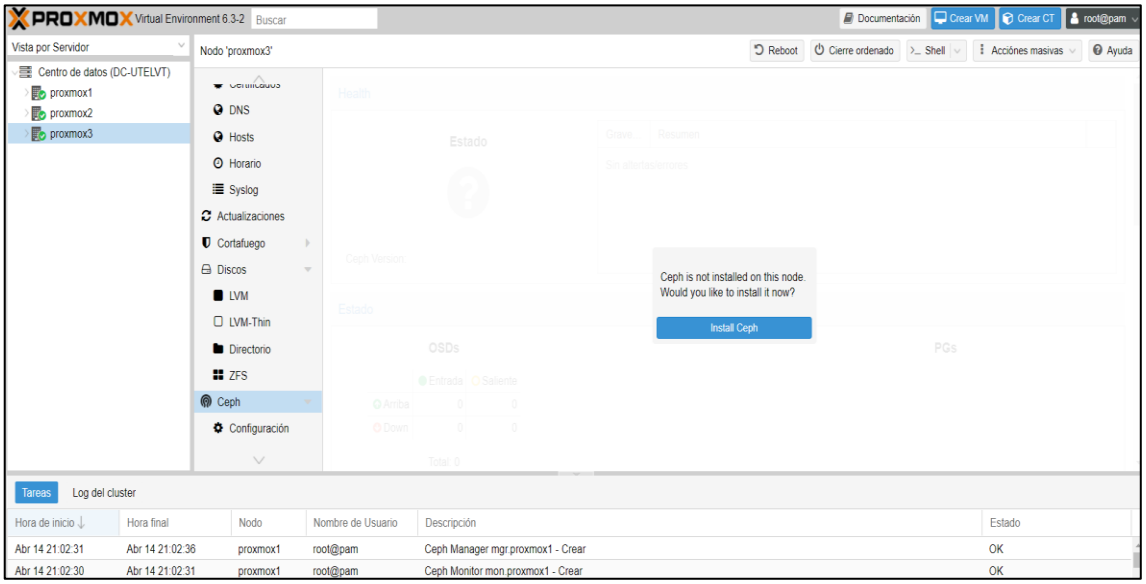



**Figura 7-5:** Configuración del OSD
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

### *5.1.3. CEPH monitor*

En la Figura 8-5 se puede observar la configuración del CEPH con los servidores Proxmox1, Proxmox2 y Proxmox3.

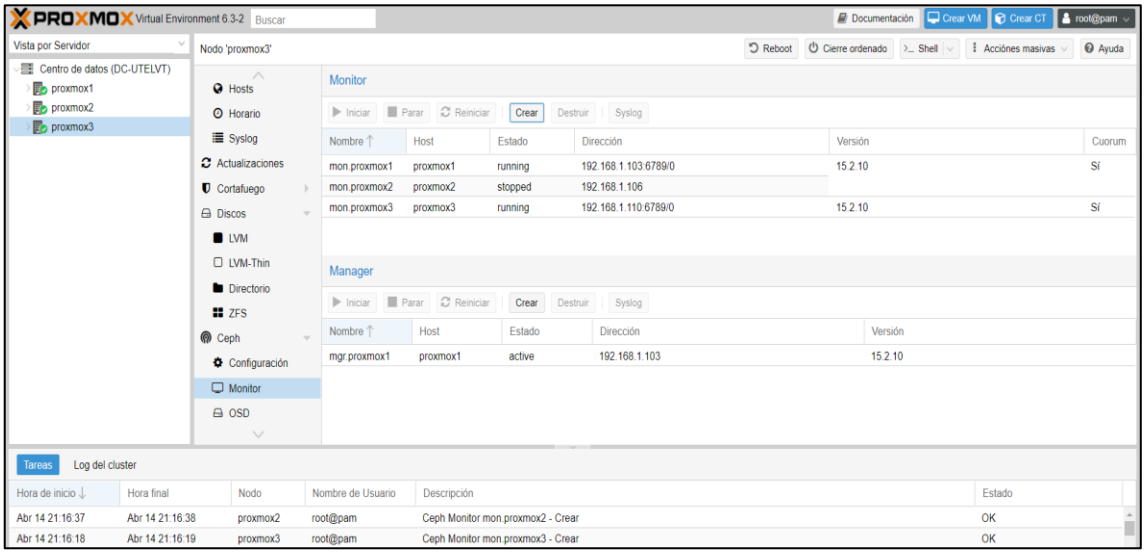



**Figura 8-5:** CEPH monitor
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

### *5.1.4. CEPH OSD*

Configuración del OSD (Object Storage Daemon) es decir los servicios asociados a las Unidades de Almacenamiento Extra como indica en la Figura 9-5.

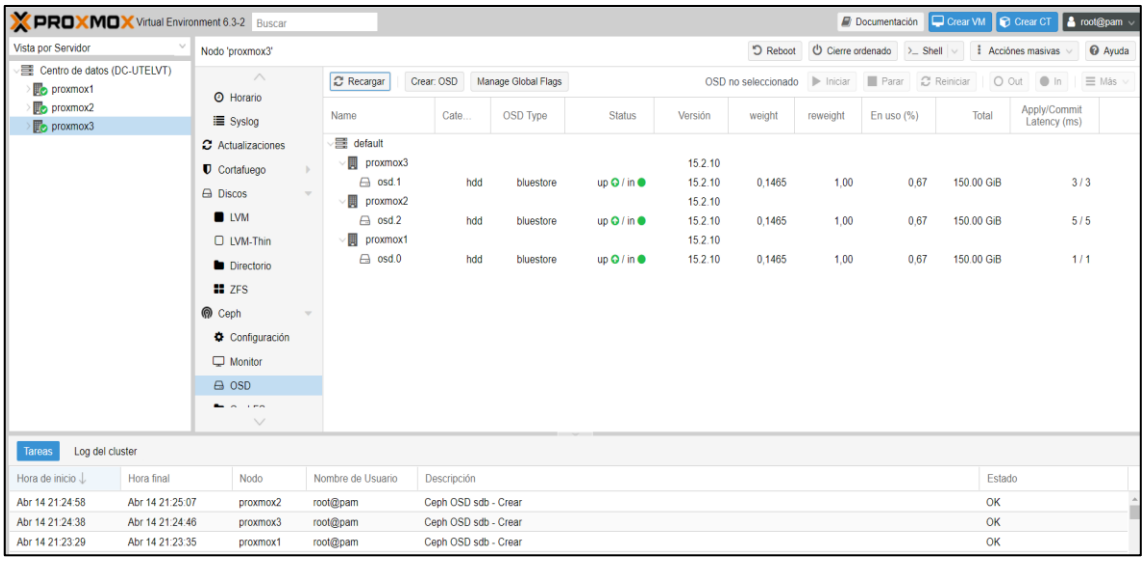



**Figura 9-5:** CEPH OSD
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

**Fase 4.** Se crea un Pool en el Promox1. Los pools son particiones lógicas para almacenar objetos. Contiene grupos de ubicación (PG, pg_num), una colección de objetos. Como se muestra en la Figura 10-5.

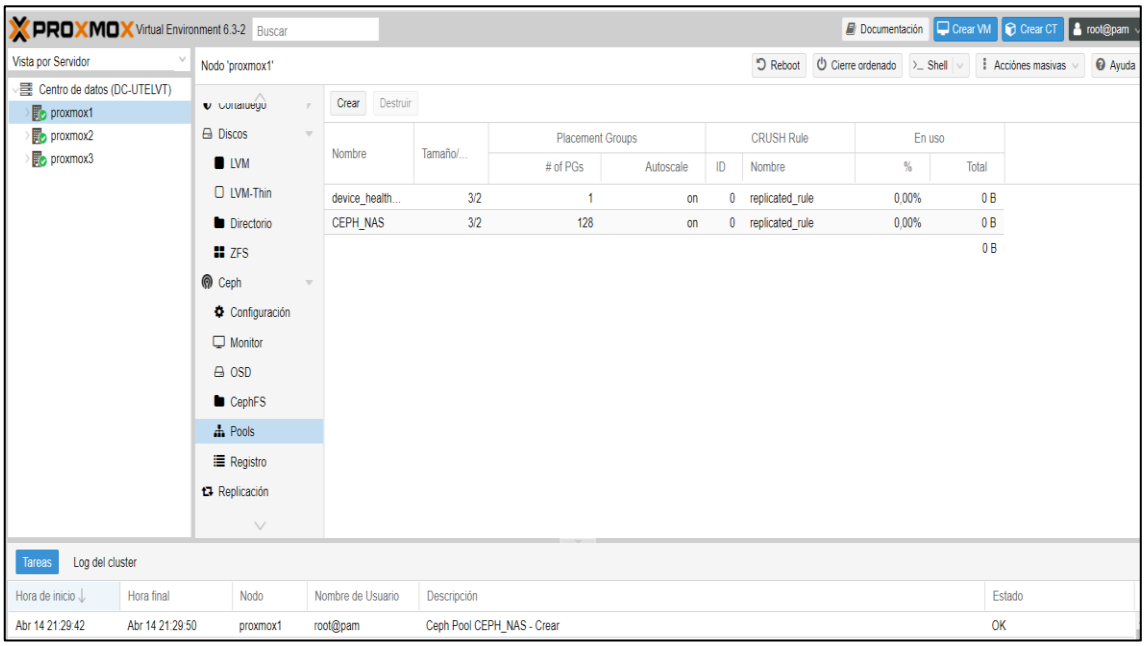



**Figura 10-5:** Creación del Pools
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

**Fase 5.** Se crea el recurso compartido (Máquina virtual o contenedor). En el CEPH_NAS del Proxmox1, como se grafica en la figura 11-5.

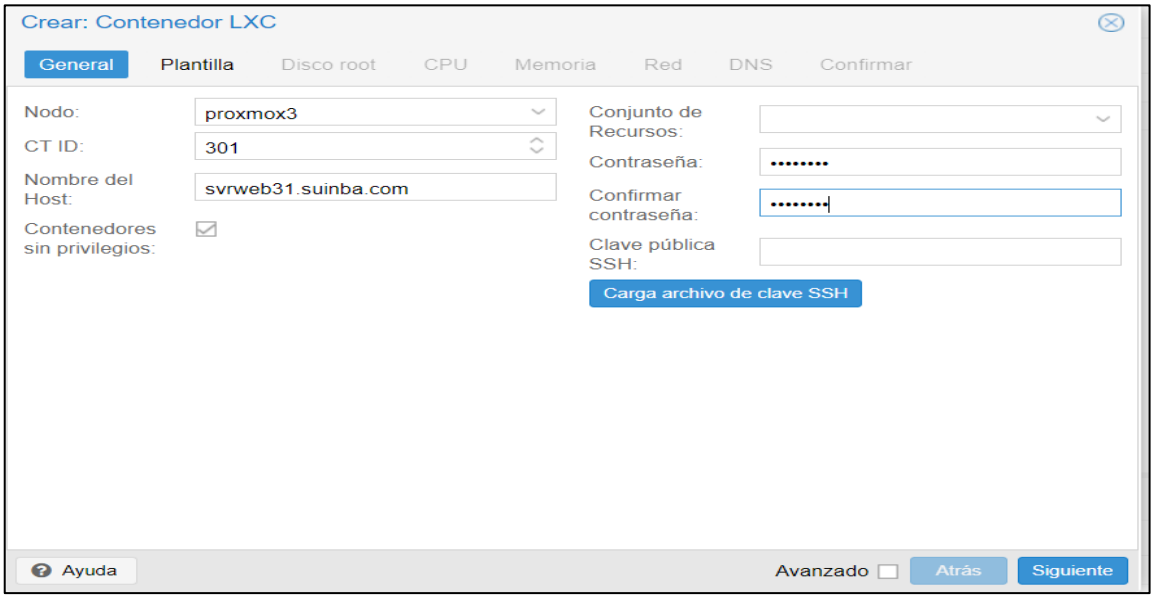



**Figura 11-5:** Creación de un recurso compartido (Contenedor)
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

**Fase 6.** Se configura la HA dándole prioridad al servidor que tiene mejores recursos, presentado en la Figura 12-5.

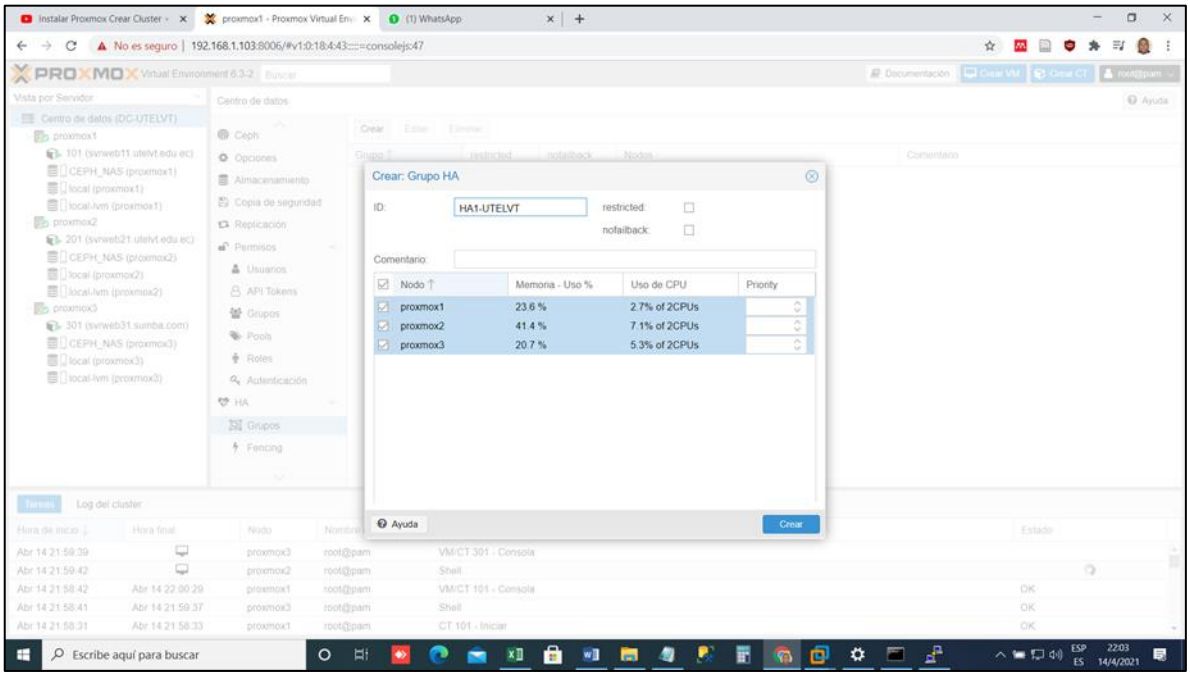



**Figura 12-5:** Creación y configuración de la HA
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

**Fase 7.** Se instala CentOS-8.3.2011 con los servicios de servidor web, como muestra la Figura 18-3. Una vez instalado el servidor se configuran los accesos y la aplicación web requerida. Luego se realizan las pruebas, ocasionando intencionalmente la desconexión de un equipo y verificando la migración de sus recursos virtuales a otros equipos del clúster, como se muestra en la Figura 13-5.

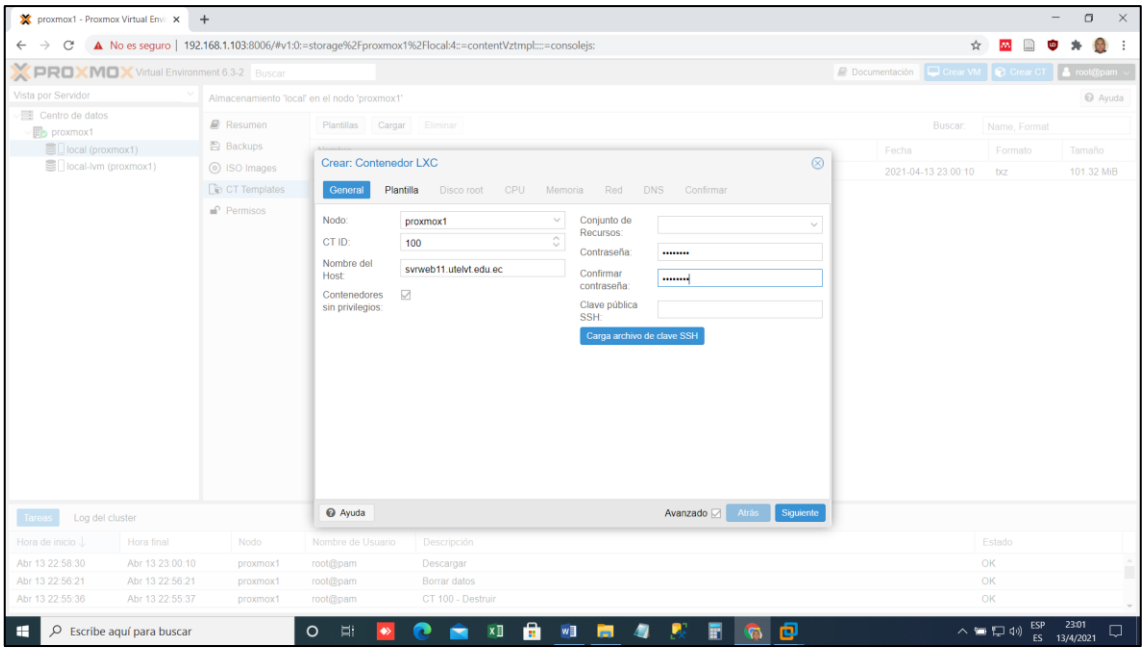



**Figura 13-5:** Creación y configuración de la Servidor web virtual con Centos8
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

**Fase 8.** Luego se realizan las pruebas, ocasionando intencionalmente la desconexión de un equipo y verificando la migración de sus recursos virtuales a otros equipos del clúster, como se muestra en la Figura 14-5.

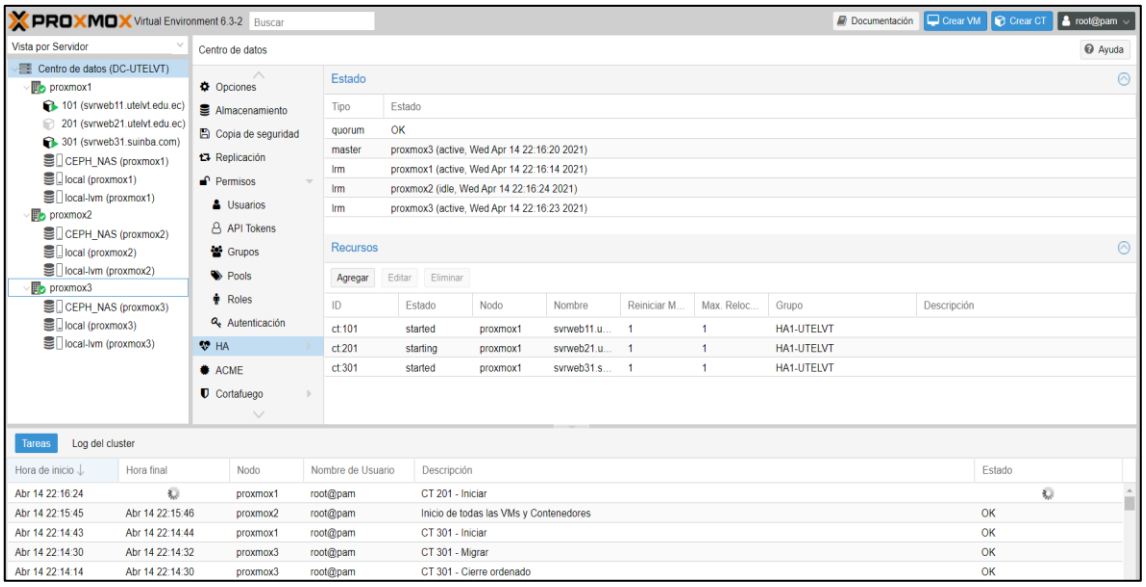



**Figura 14-5:** Pruebas HA
***Fuente:*** *Configuración de Proxmox 6.3, 2021.*

## 5.2. Metodología para la implementación de la seguridad del Clúster de HA

Para dotar de seguridad al Clúster de Alta Disponibilidad, este estudio abordó esta característica desde los siguientes puntos de vista:

a) El control del tráfico a través de la configuración de Firewalls.
b) El control de acceso a los servidores mediante la Administración de Usuarios.

### *5.2.1. Control del tráfico a través de la configuración de Firewalls*

En la implementación de los Firewalls se tomó como referencia las mejores prácticas y consideraciones propuesta en la publicación No. 24 del Equipo de Respuesta ante incidentes de Seguridad Informática de Chile, en diciembre del 2020.

Para la implementación de los firewalls, se recomienda tener una política general de tipo restrictiva, en otras palabras, todo tráfico que no tenga permiso explícito en las reglas será bloqueado; esto debido a la cantidad limitada de aplicaciones residentes en los servidores.

Los firewalls bien configurados y documentados permitirán a los administradores realizar controles periódicos, verificaciones, actualizaciones y monitoreo de sus eventos de seguridad relacionados al tráfico.

Este estudio, propone implementar firewalls en diferentes puntos y niveles.

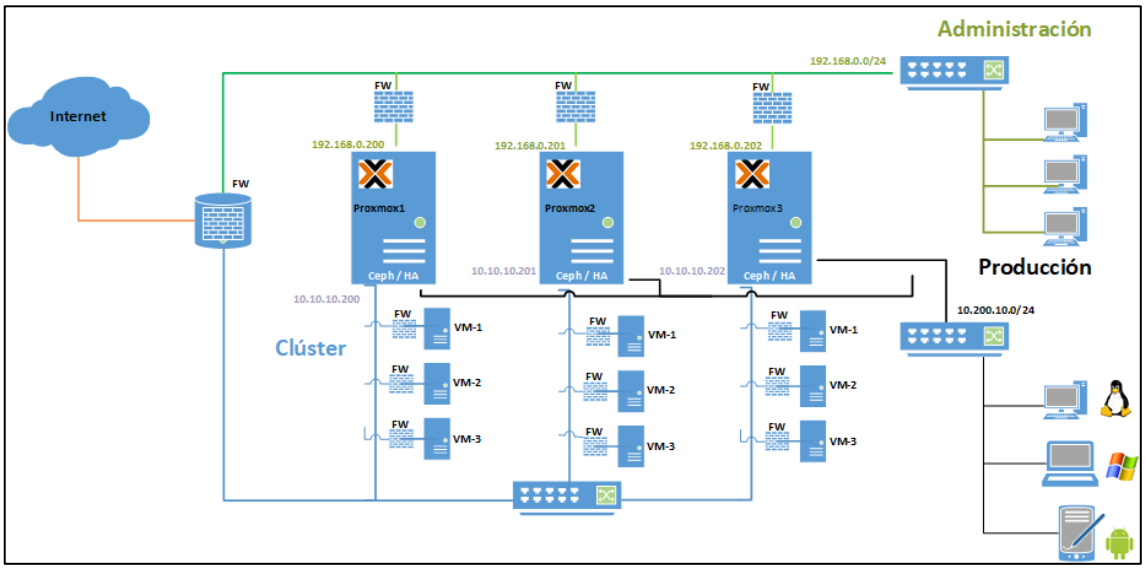



**Figura 15-5:** Firewalls del clúster de HA UTELVT
***Realizado por:*** *Quiñonez, J. 2021*

.

Como indica la Figura 15-5, se configuró un firewall para proteger el Clúster de Alta Disponibilidad y sus servidores, o sea a un firewall a nivel del Clúster, el cual contiene reglas de acceso basadas en las redes de origen.

Así mismo, se configuró un firewall para cada servidor, parte del clúster, abriendo los puertos / servicios permitidos en cada equipo y sus máquinas virtuales o contenedores.

Del mismo modo. Se configuró el firewall de cada máquina virtual o contenedor según sea el caso; permitiendo solo el acceso a servicios configurados en el servidor virtual. Cabe destacar que esta configuración dependerá de las características de los servicios de configurados en cada servidor virtual.

También es importante mencionar que la administración de reglas de cada firewall se realizó previo a el análisis de la necesidad de protección de cada servicio o equipo y se implementó usando la consola de Administración del Clúster de Alta Disponibilidad creado con Proxmox.

Además, según Andrade (2020), otras recomendaciones generales a seguir son:

- Aplicar modelo zero trust tanto para acceder a administrar los equipos como para el tráfico de usuarios a través del cortafuego.
- No utilizar políticas con “any” o “all” en los objetos de red, servicios o aplicación en políticas con tráfico permitido.
- Respaldar la configuración de los equipos permanentemente.
- Bloquear categorías de aplicaciones o filtros web catalogadas como maliciosas (hacking, pornografía, gambling y phishing, por ejemplo).
- Administrar los equipos a través de una interfaz fuera de banda, no se recomienda administrar desde una red LAN a través de la red productiva o desde la IP Publica del firewall.
- Acotar los accesos a administradores con IP de confianza, así se permite el servicio de administración solo a IP permitidas.
- No habilitar protocolos inseguros como TELNET o HTTP para la administración de los dispositivos.
- Realizar cada cierto tiempo auditoria de configuración, mantener un orden en la creación de políticas de seguridad, otorgar permisos granulares y solo en caso de ser necesario otorgar permisos al segmento de red.
- Nombrar las políticas para identificarlas fácilmente.
- Es responsabilidad del administrador estar alineado e informado sobre los boletines de seguridad entregados por los fabricantes y mantener actualizados los firmwares con el

objetivo de corregir bugs (errores de software) y vulnerabilidades presentadas en las diferentes versiones.

A continuación las Figura 16-5, muestra el resultado de realizar un test NMAP con la herramienta Zenmap 7.92; luego de poner en práctica las politicas de firewall sugeridas.

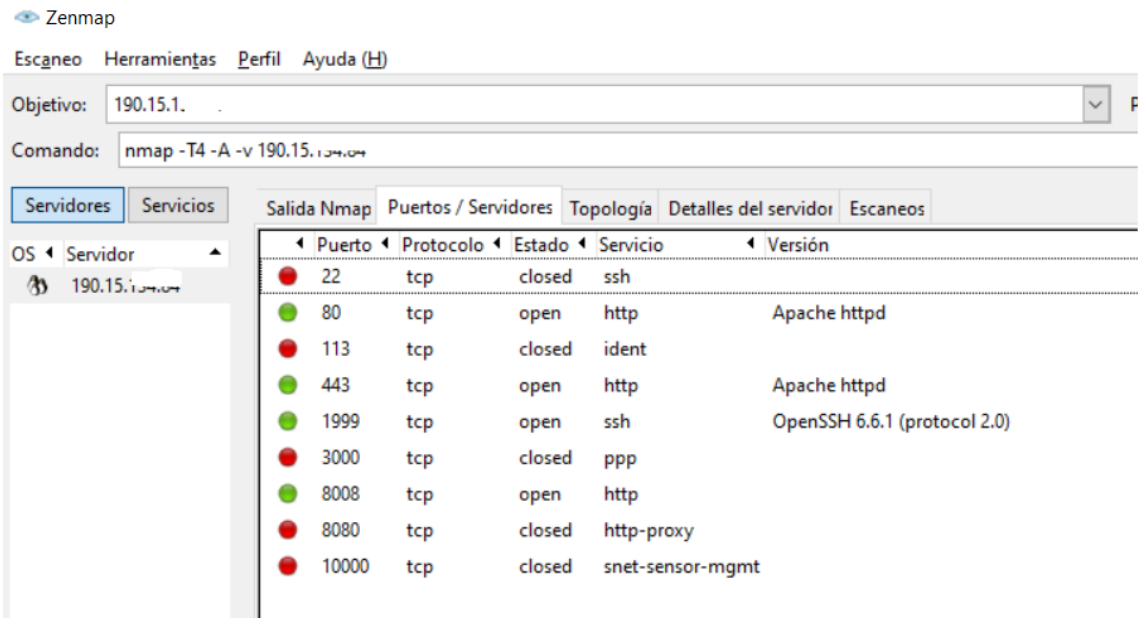



**Figura 16-5:** Resultados Test Nmap Servidor 2 UTELVT
***Fuente:*** *Test Zanmap 7.92, 2021.*
***Realizado por:*** *Quiñonez, J. 2021*

### *5.2.2. Control de Acceso mediante la Administración de Usuarios*

El control de acceso se implementó siguiendo lo sugerido en la norma Gestión de los controles de acceso según ISO 27001 en la Sección A9 del Anexo A, donde se determina que: *"Los usuarios sólo deben tener acceso a la red y a los servicios para los que se les ha autorizado específicamente para usar. El acceso debe ser controlado por un procedimiento de inicio seguro y restringido, de acuerdo con la política de control de acceso".*

Para controlar el acceso administrativo a la configuración de los equipos servidores y al Clúster de Alta Disponibilidad, se configuró un esquema basado en grupos de perfiles y roles de las personas que laboran en el Departamento de Tecnologías de la Información y Comunicación de la UTELVT y de los usuarios en general.

La organización del control de acceso quedo de la siguiente manera:

**Tabla 2-5:** Organización de Control de Usuarios

| COMPONENTE | GRUPO | ROL | PRIVILEGIO |
|---|---|---|---|
| Clúster de Alta Disponibilidad | TIC's | Administrador | Súper Usuario |
| | | Operador | Instalador, Editor |
| | | Monitor | Solo Lectura |
| Servicios Aplicaciones | Usuarios Intranet | Usuario | Crear, Editar, Leer, Eliminar Registros |
| | Publico General | Invitado | Leer |

***Realizado por:*** *Quiñonez, J. 2021*

De la misma manera, se recomienda utilizar políticas de contraseña, estableciendo caracteristicas como: un mínimo de caracteres, exigiendo, mezclando y posicionando letras, números y caracteres especiales y que se caduquen ambio cada cierto tiempo. Ademas, llevar un registro de todos los usuarios internos, sus respectivos contactos, puestos de trabajo y estar atentos a sus cambios de roles o salida de la Universidad para desactivarlos.

### *5.2.3. Otras Medidas de seguridad sugeridas*

Para endurecer aún más la seguridad del Clúster de Alta Disponibilidad, se recomienda, si es necesario implementar TCP estrategias en los servidores:

- TCP WRAPPERS, que son un tipo de ACL (Access Control List) que nos permiten filtrar conexiones entrantes en servicio basados en Linux. Trabajan en la capa y su actuación se puede monitorear en los logs del sistema.
- Buscar herramientas para encriptar el tráfico de la red, lo cual puede implicar inversión de tiempo y recursos económicos.

## CONCLUSIONES

- Para el diseño de las estrategias de seguridad y alta disponibilidad es práctico tomar en cuenta las normas de seguridad basadas en los modelos estándares como ISO, NIST, IEEE, etc., Y utilizar métricas basadas en hechos reales.

- Para mejorar la seguridad de los servicios y servidores es necesario realizar un análisis de usuarios, privilegios y de los recursos que se van a compartir tener una administración controlada del acceso a los sistemas.

- Los ambientes de pruebas virtualizados permiten diseñar, organizar y experimentar las ventajas e inconvenientes que se pueden presentar en una infraestructura antes de ponerla en equipos físicos y ocasionar eventos adversos como altos tiempos de recuperación, paralización de servicios y pérdida de recursos económicos.

- La herramienta de software libre Proxmox, satisface los requerimientos para una adecuada y aceptable administración de infraestructuras virtualizadas, ya que contiene un excelente grupo de utilidades para implementar configuraciones de seguridad en varios niveles, alta disponibilidad, almacenamiento, backup y acceso compartido.

- Un detalle muy importante en un ambiente virtualizados es organizar los servicios y servidores de aplicaciones con el objetivo de realizar la mejor distribución posible para aprovechar los recursos de hardware disponible, también teniendo en cuenta tareas como el backup y el mantenimiento periódico.

## RECOMENDACIONES

- Mantener actualizada la documentación detalla con características relevantes de los diagramas de conexión, censo de servidores físicos y virtuales, contenedores, aplicaciones, usuarios y su respectiva distribución.

- Actualizar de manera programada y periódica el software base de las plataformas de virtualización para garantizar las mejoras seguridad y alta disponibilidad de todo el sistema.

- En sistemas virtualizados, se recomienda mantener separadas de manera lógicas las redes de acceso para mejorar el control de acceso a los dispositivos virtuales y físicos.

- Es recomendable utilizar sistemas de almacenamiento de red NAS, ya que dichos sistemas cuentan con herramientas propias de administración de raid de discos, backup y optimización de uso.

## BIBLIOGRAFÍA


**Montes de Oca, E., De Giusti, L. C., De Giusti, A. E., & Naiouf, M.** (2012). Comparación del uso de GPU y cluster de multicore en problemas con alta demanda computacional. *XVIII Congreso Argentino de Ciencias de la Computación.* Buenos Aires, Argentina.

**Acero Quilumbaquín, W. A.** (2016). *Diseño e implementación de in Cluster de ALta Disponibilidad para virtualizar los servidores de adquisición y procesamiento de datos del Instituto Geofñisico.* Quito: EPN. Recuperado el 10 de 07 de 2021

**Aguliera, L.** (2010). *Seguridad informatica*. Editex.

**Arias, F.** (2012). *el proyecto de la investigacion cientiífica, introducción a la metodología cientifica*. Caracas: Episteme.

**C3NTRO Telecom.** (2020). *¿Qué es la alta disponibilidad y redundancia en la conectividad a la nube?* Obtenido de https://blog.c3ntro.mx/que-es-alta-disponibilidad-y-redundancia-en-conectividad-a-la-nube

**Castro, I.** (Julio de 2016). *¿Qué es un Análisis de Vulnerabilidades Informáticas?* Recuperado el Abril de 2018, de http://blog.cerounosoftware.com.mx/que-es-un-analisis-de-vulnerabilidades-inform%C3%A1ticas

**Citrix.** (2020). *¿Qué es la virtualización?* Obtenido de https://www.citrix.com/es-mx/glossary/what-is-virtualization.html

**Clavijo, P.** (2010). *Clusters de Alta Disponibilidad (HA)*. Obtenido de https://paucls.wordpress.com/2010/02/13/clusters-de-alta-disponibilidad-ha/

**Dussan, C.** (2015). Políticas de Seguridad Informatica. *Universidad Automnma del estado de Mexico Redaly*.

**eldiario.es.** (junio de 2017). *Un nuevo ciberataque con 'ransomware' afecta a empresas de todo el mundo*. Obtenido de https://www.eldiario.es/tecnologia/nuevo-ciberataque-ransomware-afecta-empresas_0_658984860.html

**Espinoza , R., & Lobatón, L.** (2014). *Implementación de Virtualización en el Centro de Cómputo del Ministerio De Transportes Y Comunicaciones*. Lim - Perú.

**Espinoza, R. M.** (2019). *Análisi comparativo de un Hypervisor Nativo Propietario y Libre como alternativa de solución para el proceso de datos.* Riobamba: ESPOCH. Recuperado el 01 de 10 de 2021

**Flórez Hernández, C. M., & Huertas Lucena, C. M.** (2018). *Virtualización de Servicios en Red de la empresa HSE INGENIERÍA SA.* Universidad del Cauca, Facultad de Ingenieria Electrónica y Telecomunicaciones. Popayán: Universidad del Cauca. Recuperado el 03 **de 08 de 2021**

**Hernández, R., Fernández, C., & Baptista, M.** (2014). *Metodología de la Investigación.* Mexico: McGraw Hill.

**IONOS.** (2020). *Virtualización: el alma de la nube*. Obtenido de https://www.ionos.es/digitalguide/servidores/configuracion/virtualizacion/

**Moretta, G**. (2017). *Estudio e implementación de una solución de virtualización de servidores de aplicaciones para la carrera de licenciatura de sistemas de información.* Guayaquil.

**Morros, R. S.** (2013). *Big Data: análisis de herramientas y soluciones.* Barcelona.

**Nilo Andrade, J.** (12 de 2020). Consejos y buenas prácticas de administración de firewalls. (K. C. M., Ed.) *Análisis de Amenazas Cibernéticas*, *24*, 18. Recuperado el 11 de 10 de 2021, de https://www.csirt.gob.cl/media/2020/12/AN2-2020-24-.pdf

**Ñaupas, H., Mejia, E., Novoa, E., & Villagomez, A.** (2014). *Metodologia de la inestigación científica cualitativa . cuantitataiva y redacción de tesis.* Bogota: Ediciones de la U.

**Organización Marítima Internacional.** (2017). *Riesgo cibernético marítimo*. Obtenido de OMI: http://www.imo.org/es/ourwork/security/guide_to_maritime_security/paginas/cyber-security.aspx

**Perdigon Llanes, R., & Ramirez Alonso, R.** (03 de 2020). Plataformas de software libre para la virtualización de servidores en pequeñas y medianas empresas cubanas. (R. C. Informáticas, Ed.) *Revista Cubana de Ciencias Informáticas*, *14*(1), 19. Recuperado el 01 de 10 de 2021, de http://rcci.uci.cu

**Perez, N., Mendez, S., Ayusa, V., Aucapiña, I., & Lopez, J.** (2013). Aplicaciones del cómputo de altas prestaciones. *XI Workshop de Investigadores en Ciencias de la Computación*.

**Pfister, G.** (1998). *In Search of Clusters.* Prentice Hall PTR.

**Prandini, P., & Pallero, M.** (25 de 05 de 2013). *Vulnerabilidades, amenazas y riesgo en "texto claro".* Recuperado el 04 de 04 de 2018, de http://www.magazcitum.com.mx/?p=2193#.WsWmeS7wbIU

**Ramos, J.** (2013). PRUEBAS DE PENETRACIÓN O PENT TEST. *Revista de Información, Tecnología y Sociedad*.

**Ruiz, T. C.** (2016). *Sistema portuario Ecuatoriano.* Obtenido de http://www.sela.org/media/2303887/15-sistema-portuario-ecuatoriano.pdf

**Sánchez, L. C.** (2012). *Los metodos de investigación.* Madrid: Diaz de Santos.

**Santos, J. C.** (2014). *Seguridad y alta disponibilidad.* Madrid: RA-MA.

**SUINBA**. (2017). *Suinba.* Obtenido de https://www.suinba.com/

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

**Voutssas, J.** (abril de 2010). *Preservación documental digital y seguridad informática.* Recuperado el 5 de abril de 2018, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

# ANEXOS

## Anexo A. Autorización para la Investigación UTELVT

UNIVERSIDAD TÉCNICA
"LUIS VARGAS TORRES"
DE ESMERALDAS

*Dirección de Tecnologías de la Información y Comunicación*

**Oficio Nro. UTLVTE-TICS-2020-0078-O**

**Esmeraldas, 17 de marzo de 2020**

Señor Ingeniero
Quiñonez Quintero Jhonny Maximiliano
**Docente FACI UTLVTE**

Ciudad. -

**ASUNTO: AUTORIZACIÓN DE REALIZACIÓN DE ESTUDIO.**

En respuesta al oficio S/N, de fecha 11 de marzo de 2020, en el cual usted expresa "Yo, Quiñonez Quintero Jhonny Maximiliano, con CI. 0801901695, docente de la carrera de Ingeniería de Tecnologías de la Información de la UTE-LVT, solicito muy respetuosamente, acepte y autorice la realización en el Departamento de TIC's el estudio ELABORACIÓN Y EVALUACIÓN DE UN SISTEMA QUE PERMITA MEJORAR LA DISPONIBILIDAD Y SEGURIDAD EN LOS SERVICIOS WEB DE LA UNIVERSIDAD TECNICA LUIS VARGAS TORRES, MEDIANTE EL USO DE HERRAMIENTAS DE SOFTWARE LIBRE, proyecto de investigación (...)"; al respecto otorgo a usted, **VISTO BUENO** para la ejecución del estudio propuesto como parte de su proyecto de investigación, bajo el compromiso de entregar a ésta Dirección los resultados obtenidos a manera de informe, incluyendo sugerencias o recomendaciones de mejoras bajo un criterio de carácter técnico, de así ameritarse.

Las fechas de realización de las pruebas técnicas a efectuarse, serán acordadas con anticipación mediante comunicado por vía electrónica a la dirección leonardo.reyes@utelvt.edu.ec, o llamada telefónica al número de contacto +593 993160691.

Atentamente,

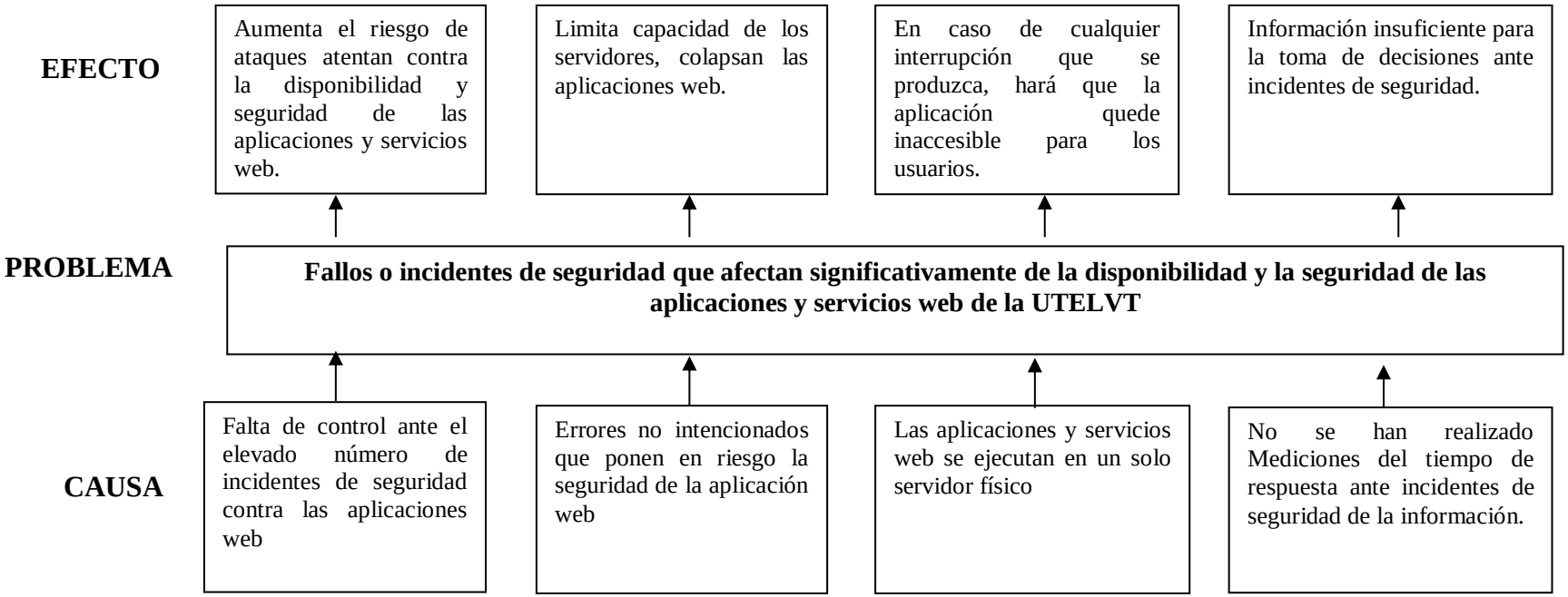
Ing. Leonardo Gabriel Reyes Vélez. Msc.
**DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN UTLVTE**

**Cc..**

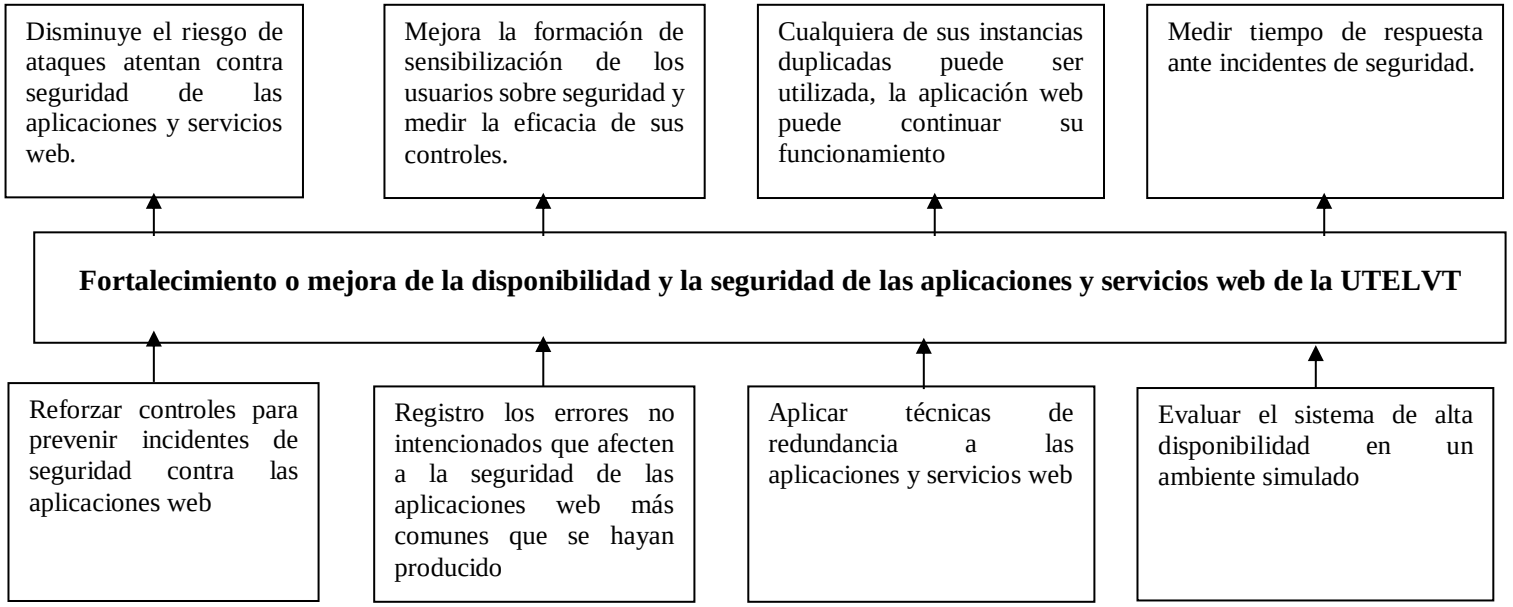
Señor Magister
Plata Cabrera Carlos Simón
**Analista Programador de la UTLVTE**

Cc. Archivo...

**Anexo B. Árbol de problema**



**Anexo C. Árbol de objetivos**



**Anexo D. Cuestionario para entrevista al Administrador de TIC's de la UTELVT**

1. **¿Existen Políticas de Seguridad debidamente aprobadas?**
   a) Si
   b) No
   c) Están en proceso de aprobación

2. **¿Existen algún manual o plan de contingencia para solventar los eventos adversos?**
   a) Si
   b) No
   c) Hay un proceso, pero no está escrito.

3. **¿Cómo se enteran de la ocurrencia de una caída de servicio?**
   a) Los usuarios alertan
   b) Algún sistema de alerta automática
   c) Realizan monitoreo permanente

4. **¿Cómo proceden ante eventos adversos?**
   a) Todos ayudan a revisar y a solucionar
   b) Hay alguien responsable de revisar y solucionar
   c) Una vez ocurrido y caracterizado el evento, se responsabiliza a alguien del personal.

5. **¿Qué tiempo promedio se demoran en reanudar los servicios?**
   a) 1 hora
   b) Entre 1 y 3 Horas
   c) Entre 3 y 6 Horas
   d) 1 días
   e) 2 días
   f) Más de 2 días.

6. **¿Registran las características y soluciones dadas a los eventos adversos de seguridad?**
   a) Si
   b) No
   c) Se registran algunos datos, pero incompletos.

7. **¿Realizan evaluaciones periódicas de las seguridades de sus sistemas?**
   a) Si
   b) No
   c) Solo cuando existe algún evento.

8. **¿Qué sucede cuando los eventos críticos se producen fuera del horario de trabajo?**
   a) Se inicia el tratamiento del incidente al retornar al trabajo
   b) Se inicia el tratamiento del incidente de manera remota.
   c) Alguien del personal atiende inmediatamente el evento.

d) Se pide paciencia a los usuarios hasta solucionar el problema.

**9. ¿Han realizado algún análisis para instalar los servicios y distribuir el nivel de carga de cada servidor?**

a) Si.
b) No
c) Está planificado.
d) No se pretende modificar la distribución por ahora

**10. ¿Han recibido capacitación formal sobre temas de Seguridad de la Información?**

a) Si, Básica.
b) Si, Intermedia.
c) Si, Avanzada.
d) No.

**11. ¿Tienen planificado realizar capacitación formal sobre temas de Seguridad de la Información?**

a) Si.
b) No.
c) Lo tomaran en cuenta para el futuro.

**12. ¿Utilizan alguna herramienta o sistema basado en software libre para implementar seguridades o aprovechar de mejor manera los recursos de hardware disponibles?**

a) Si.
b) No.
c) Ya estamos en eso.
d) Lo tomaran en cuenta para el futuro.

**Anexo E. Fichas de Observación**

***Infraestructura Hardware***

| **Equipos/ Características** | **Servidor 1** | **Servidor 2** | **Servidor 3** |
|---|---|---|---|
| **Marca / Modelo** | | | |
| **Procesador** | | | |
| **RAM** | | | |
| **Disco duro total** | | | |
| **Disco duro disponible** | | | |
| **Tecnologías** | | | |
| **Redundancia/ HA** | | | |
| **Mantenimientos al Año** | | | |
| **Sistema Operativo** | | | |
| **Herramientas** | | | |
| **Software / Aplicaciones** | | | |

***Infraestructura Red***

| **Equipos** | **Marca Modelo** | **Puertos** | **Velocidad** | **Capa** | **Conectividad** | **Mantenimientos** | **Redundancia** |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

*Aplicaciones*

| **Nombre** | **Área** | **Lenguaje** | **SGBD** | **Versión** | **Niveles** | **Adm. Roles** | **Backup** |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

*Eventos*

| **Evento** | | | | | | |
|---|---|---|---|---|---|---|
| **Frecuencia** | | | | | | |
| **Hard Comp.** | | | | | | |
| **Software Comp.** | | | | | | |
| **Criticidad** | | | | | | |
| **Complejidad** | | | | | | |
| **Solución** | | | | | | |
| **Tiempo de Recuperación** | | | | | | |
| **Contramedidas** | | | | | | |
| **Documentación** | | | | | | |

espoch | Dirección de Bibliotecas y Recursos del Aprendizaje

**UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL**

**REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA**

**Fecha de entrega:** 11 / 03 / 2022

| **INFORMACIÓN DEL AUTOR/A (S)** |
|---|
| **Nombres – Apellidos:** Jhonny Maximiliano Quiñonez Quintero |
| **INFORMACIÓN INSTITUCIONAL** |
| Instituto de Posgrado y Educación Continua |
| **Título a optar:** Magíster en Seguridad Telemática |
| **f. Analista de Biblioteca responsable:** Lic. Luis Caminos Vargas Mgs. |

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS
Nombre de reconocimiento (DN): c=EC, l=RIOBAMBA, serialNumber=0602766974, cn=LUIS ALBERTO CAMINOS VARGAS
Fecha: 2022.03.11 14:50:31 -05'00'

UNIDAD DE PROCESOS TÉCNICOS DBRA DIRECCION DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE ESPOCH