Capítulo I

Presentación del Proyecto

1.- Capítulo 1: Presentación del Proyecto

IDENTIFICACIÓN DEL PROYECTO	
Título del Proyecto	Diseño de un Data Center bajo la Norma ISO/IEC 22237 y un Servidor de Monitoreo en Tiempo Real para la Optimización de la Infraestructura Tecnológica en la Fiscalía Departamental de Tarija
Nombre del Postulante	Vannesa Cañizares Vilte
Celular	78220150
Carrera/Unidad	Ingeniería Informática
Facultad	Ciencias y Tecnología
Correo Electrónico	vannec2398@gmail.com
Institución/Centro Cooperante	Fiscalía Departamental de Tarija
Duración del Proyecto	8 meses
Área/línea de investigación priorizada	Redes

1.1.- Perfil de Proyecto

1.1.1.- Introducción

En la era digital actual, los Data Centers se han convertido en el corazón de las organizaciones, proporcionando el almacenamiento, procesamiento y distribución de grandes cantidades de datos. Sin embargo, la gestión eficiente de estos centros de datos es un desafío constante debido a la creciente demanda de servicios digitales y la necesidad de garantizar la seguridad y disponibilidad de los datos.

Este proyecto se centra en el diseño de un Data Center bajo la Norma ISO/IEC 22237, un estándar internacional que establece los requisitos para la disponibilidad, calidad y seguridad de los Data Centers. La implementación de esta norma permitirá optimizar la infraestructura tecnológica de la Fiscalía Departamental de Tarija, mejorando su capacidad para manejar y proteger los datos críticos.

Además, este proyecto propone la configuración de un Servidor de Monitoreo en Tiempo Real. Este servidor permitirá supervisar continuamente el rendimiento y el estado de la infraestructura

tecnológica, proporcionando información en tiempo real que puede ser utilizada para detectar y resolver problemas rápidamente, optimizando así la eficiencia operativa.

La combinación de un Data Center diseñado según la Norma ISO/IEC 22237 y un Servidor de Monitoreo en Tiempo Real proporcionará a la Fiscalía Departamental de Tarija una infraestructura tecnológica robusta, segura y eficiente, capaz de satisfacer las crecientes demandas de la era digital.

1.2.- Descripción del Proyecto

1.2.1.- Antecedentes

En los últimos años, la digitalización ha transformado la forma en que las organizaciones operan y gestionan sus operaciones. Los Data Centers, como centros neurálgicos de almacenamiento y procesamiento de datos, han surgido como una infraestructura crítica en este paisaje digital. Sin embargo, el diseño y la gestión de estos centros de datos presentan desafíos significativos.

La Norma ISO/IEC 22237 surgió como respuesta a estos desafíos, proporcionando un marco para el diseño de Data Centers que garantiza altos niveles de disponibilidad, calidad y seguridad. A pesar de su importancia, la implementación de esta norma sigue siendo limitada, especialmente en las instituciones públicas de Bolivia.

Por otro lado, el monitoreo en tiempo real se ha convertido en una herramienta esencial para la gestión eficiente de la infraestructura tecnológica. A pesar de sus beneficios, muchas organizaciones aún no han implementado soluciones de monitoreo en tiempo real, lo que resulta en una gestión ineficiente y en la incapacidad para responder rápidamente a los problemas.

En el caso de la Fiscalía Departamental de Tarija, la falta de un Data Center y de un Servidor de Monitoreo en Tiempo Real ha limitado su capacidad para gestionar eficientemente su infraestructura tecnológica. Esto ha llevado a problemas de rendimiento, seguridad y disponibilidad, afectando la capacidad de la Fiscalía para llevar a cabo sus operaciones de manera eficiente.

Este proyecto surge como respuesta a estos desafíos, con el objetivo de diseñar un Data Center bajo la Norma ISO/IEC 22237 y configurar un Servidor de Monitoreo en Tiempo Real para la Fiscalía Departamental de Tarija. Con este proyecto, esperamos mejorar la eficiencia operativa de la Fiscalía y optimizar su infraestructura tecnológica.

1.2.2.- Antecedentes de investigación

1.- “Diseño De Un Data Center Con Arquitectura Convergente Para Optimizar Los Procesos Informáticos De La Municipalidad Distrital De José Leonardo Ortiz”

La tesis se centra en la problemática de la Municipalidad Distrital de José Leonardo Ortiz, que depende en gran medida de los sistemas informáticos para llevar a cabo sus operaciones diarias. Sin embargo, la infraestructura tecnológica actual puede no estar optimizada para manejar la creciente demanda de servicios digitales.

El objetivo principal de la tesis fue diseñar un Data Center con arquitectura convergente, que permita integrar los servicios de voz, datos y video sobre una misma infraestructura de cableado estructurado. Este diseño busca solucionar la problemática de la Municipalidad Distrital de José Leonardo Ortiz y servir como material de estudio para otros trabajos similares de investigación1.

Los resultados indicaron que el diseño óptimo de red lógica, el cálculo de la capacidad correcta de los equipos eléctricos y mecánicos, el cálculo del cableado estructurado, la simulación del funcionamiento de red en software Packet Tracer y la simulación en 3D en el programa Sketchup 2019 fueron factores que permitieron determinar el diseño adecuado. Esto permitirá a la municipalidad enfrentar los desafíos tecnológicos actuales y mejorar la calidad de los servicios ofrecidos a la comunidad. Montaño Guerrero, R. A., & Bustíos Arteaga, J. L. J. (2020).

2.- “Implementación de un Sistema de Monitoreo y Supervisión de la Infraestructura y Servicios de Red para Optimizar la Gestión de TI en la Universidad Nacional Pedro Ruiz Gallo”

En el entorno universitario moderno, la gestión eficiente de la infraestructura y los servicios de red es crucial para garantizar un entorno de aprendizaje y trabajo efectivo. La Universidad Nacional Pedro Ruiz Gallo enfrenta desafíos en este aspecto, con la necesidad de monitorear y supervisar de manera proactiva su infraestructura de TI para garantizar la disponibilidad, el rendimiento y la seguridad de los servicios digitales ofrecidos a estudiantes, profesores y personal administrativo. En respuesta a esta necesidad, se propone la implementación de un Sistema de Monitoreo y Supervisión de la Infraestructura y Servicios de Red, con el objetivo de mejorar la gestión de TI en la universidad y garantizar una experiencia de usuario óptima.

El objetivo central de esta tesis es diseñar e implementar un Sistema de Monitoreo y Supervisión de la Infraestructura y Servicios de Red en la Universidad Nacional Pedro Ruiz Gallo, con el fin de optimizar la gestión de TI y mejorar la calidad de los servicios digitales ofrecidos por la institución. El sistema propuesto permitirá monitorear en tiempo real el estado de la infraestructura

de red, identificar y resolver proactivamente problemas de rendimiento o seguridad, y proporcionar información valiosa para la toma de decisiones estratégicas en el ámbito de TI.

La implementación del Sistema de Monitoreo y Supervisión de la Infraestructura y Servicios de Red en la Universidad Nacional Pedro Ruiz Gallo representa un paso significativo hacia la mejora de la gestión de TI y la garantía de la disponibilidad y calidad de los servicios digitales en la institución. A través de la monitorización proactiva de la infraestructura de red y la supervisión continua de los servicios, se pueden identificar y abordar rápidamente los problemas potenciales, minimizando el impacto en los usuarios finales y mejorando la eficiencia operativa de la universidad. Casas Reque, R. M., & Sempértegui Tocto, M. L. (2018).

1.3.- Justificación del Proyecto

1.3.1.- Tecnológica

La implementación de un Data Center bajo la Norma ISO/IEC 22237 y la configuración de un servidor de monitoreo en tiempo real en la Fiscalía Departamental de Tarija representa una decisión tecnológica estratégica. Estas tecnologías permitirán una gestión más eficiente de la infraestructura tecnológica, garantizando la disponibilidad, confidencialidad e integridad de los datos. Además, facilitarán la detección temprana de posibles fallos o vulnerabilidades en la infraestructura, lo que contribuirá a minimizar los tiempos de inactividad y a mejorar la capacidad de respuesta ante incidentes de seguridad permitiendo mejorar su eficiencia operativa, garantizar la seguridad de los datos y mejorar la calidad de los servicios que ofrece.

1.3.2.- Económica

Desde una perspectiva económica, la modernización de la infraestructura tecnológica de la Fiscalía mediante la implementación de un Data Center y un servidor de monitoreo en tiempo real conlleva diversos beneficios financieros a largo plazo. Entre estos beneficios se incluyen la reducción de costos operativos derivados de la optimización de recursos, la disminución de los tiempos de inactividad y la mejora de la eficiencia en el uso de la energía. Asimismo, se espera un retorno de la inversión significativo debido a la mejora en la productividad y la calidad de los servicios ofrecidos por la institución.

1.3.3.- Social

La implementación de tecnologías modernas en la Fiscalía Departamental de Tarija tendrá un impacto positivo en la comunidad. La mejora en la eficiencia y la transparencia de los procesos judiciales contribuirá a fortalecer la confianza de los ciudadanos en las instituciones públicas y en

el sistema de justicia en general. Además, una infraestructura tecnológica robusta y segura garantizará el acceso oportuno a la información y los servicios ofrecidos por la Fiscalía, promoviendo así la igualdad de oportunidades y el cumplimiento de los derechos fundamentales de los ciudadanos.

1.3.4.- Desarrollo Sostenible

El diseño de un Data Center eficiente y un Servidor de Monitoreo en Tiempo Real pueden contribuir al desarrollo sostenible. Al optimizar el uso de recursos y reducir el consumo de energía, este proyecto puede ayudar a la Fiscalía a reducir su huella de carbono y contribuir a los esfuerzos de sostenibilidad.

1.3.5.- Medio Ambiental

Desde una perspectiva medioambiental, la implementación de un Data Center eficiente puede tener un impacto positivo. Los Data Centers son conocidos por su alto consumo de energía. Sin embargo, al diseñar el Data Center de acuerdo a una norma, se puede minimizar el consumo de energía y reducir el impacto medioambiental.

1.4.- Planteamiento del problema

La Fiscalía Departamental de Tarija, como muchas otras instituciones públicas en Bolivia, enfrenta desafíos significativos en la gestión de su infraestructura tecnológica. A pesar de la creciente dependencia de los servicios digitales, la Fiscalía aún no ha implementado un Data Center diseñado según una norma ni una configuración de Servidor de Monitoreo en Tiempo Real. Esto ha resultado en problemas de rendimiento, seguridad y disponibilidad, afectando la eficiencia operativa de la Fiscalía y la calidad de los servicios que ofrece a la población.

La falta de un Data Center adecuado y de un sistema de monitoreo en tiempo real dificulta la eficiencia, seguridad y disponibilidad de los datos críticos manejados por la institución. Esta situación se agrava por la ausencia de una normativa clara que regule la gestión y operación de los recursos tecnológicos, lo que puede resultar en riesgos de seguridad, tiempos de inactividad prolongados y pérdida de confianza por parte de los ciudadanos en los servicios ofrecidos por la Fiscalía.

1.5.- Cuadro de Involucrados

Grupos	Intereses	Problemas Percibidos	Recursos y Mandatos
Funcionarios Fiscales de Materia	Presentar y analizar el caso ante tribunal, investigar delitos y acusar al acusado en nombre del Estado con la presentación de documentos.	- Ineficiencia en la red y equipos, afectando la rapidez en la presentación de casos. - Fallos en la conexión a la red durante investigaciones críticas.	R: - Mejora en la infraestructura de red principal para mejorar la agilización en el procesamiento de casos.
Médicos Forenses	Determina el origen de las lesiones sufridas por una herida o la causa de la muerte mediante el examen de un cadáver para los casos que se presentan.	-Interrupciones de red lenta en afectando la comunicación de resultados y análisis forenses. - Problemas de lentitud en los equipos de red para el acceso a información médica digitalizada.	R: Informes de la funcionalidad de red en los equipos. R: Actualización y mantenimiento de equipos.
Conciliadores Legales	Ayudar a las apartes a llegar a un acuerdo mutuo para evitar que se generen discrepancias o conflictos, mediante la documentación de los casos presentados.	- Fallos en algunos equipos sin mantenimiento, generando demoras en la mediación. - Tiempos de espera por la lentitud de la red, afectando el proceso de conciliación.	R: Optimizar la red para evitar pérdida de información durante procesos de mediación R: Informe de los equipos y análisis del estado de la red.
Administrativos	Mantienen y gestionan toda la documentación de los casos, incluyendo informes, registros y archivos en su sistema.	- Equipos lentos y tiempo de espera prolongado para el acceso a documentos. - Fallos en scanners e impresoras sin mantenimiento.	R: Analizar y mejorar el rendimiento de equipos utilizados por administrativos. R: Mantenimiento preventivo de scanner e impresoras.

Funcionarios Informáticos	Son responsables de gestionar y mantener los sistemas y tecnologías de la información utilizadas por la fiscalía mejorando los sistemas y red y adaptándolas al crecimiento constante de información de la fiscalía.	- Dispositivos sin mantenimiento, generando fallos y tiempos de espera. - Rendimiento lento de dispositivos, afectando la eficiencia en la gestión de sistemas. -Largo tiempo de espera para cambio de dispositivos en mal funcionamiento - Problemas de seguridad por vulnerabilidades en dispositivos de red.	R: Mantenimiento regular de dispositivos. R: Monitoreo y gestión del ancho de banda. R: Reforzamiento de medidas de seguridad para proteger la información.
Atención de Servicios	Brindan información a las personas, asesoramiento sobre proceso judicial como los testigos y victimas, así como para canalizar sus quejas, denuncias y sugerencias - Mejorar la atención a la población.	- Pérdida de conexión a la red no planificados, - Red lenta debido al mal uso de ancho de banda, generando demoras en la asesoría. - Equipos lentos para la atención al cliente.	R: Optimizar el rendimiento de equipos utilizados en atención al cliente. R: Mantenimiento preventivo y reemplazo rápido de escáneres e impresoras en mal estado.
Cuarto Policial	Apoyar la investigación, el procesamiento de delitos y la seguridad de la institución. -Seguridad mediante las cámaras de seguridad.	- Fallas de la red en la carga y descarga de supervisión, afectando la eficacia en la seguridad.	R: - Mejorar la infraestructura de red principal para garantizar la transmisión eficiente de registros y datos de cámaras de seguridad.

1.6.- Árbol de Problemas

Figura 1. *Árbol de Problemas*

1.7.- Árbol de Objetivos

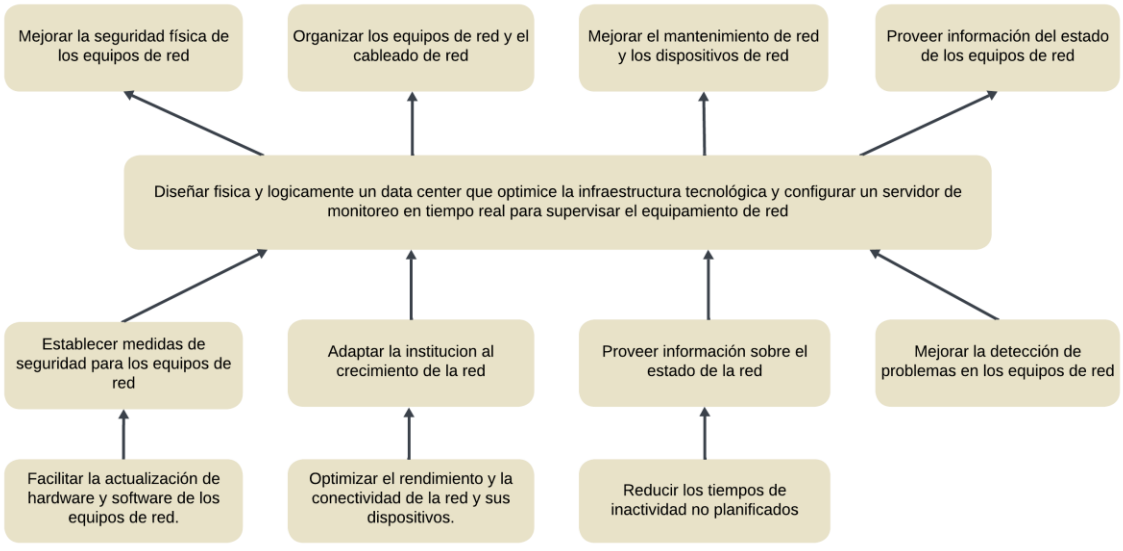


Figura 2*. Árbol de Objetivos*

1.8.- Objetivos

1.8.1.- Objetivo General

Optimizar la eficiencia operativa, la seguridad y la disponibilidad de la red de datos de la institución, garantizando un funcionamiento estable y eficiente, esencial para la mejora continua de los servicios que ofrece.

1.8.2.- Objetivos Específicos

- Diseñar un Data Center que cumpla con la Norma ISO/IEC 22237 y que satisfaga las necesidades de la Fiscalía Departamental de Tarija.
- Configurar un Servidor de Monitoreo en Tiempo Real que permita supervisar continuamente el rendimiento y el estado de la infraestructura tecnológica.

1.9.- Matriz del Marco Lógico (MML)

Resumen Narrativo del Proyecto	**Indicadores**	**Medios de Verificación**	**Supuestos**
Fin Contribuir a optimizar la infraestructura tecnológica de la Fiscalía con el objetivo de fortalecer la gestión operativa y garantizar la seguridad efectiva de la información.	Al cabo de un año de ejecutado el proyecto se obtiene un 70% de comparaciones de desempeño antes y después.	Informes de rendimiento del Data Center y de funcionalidad del Servidor de Monitoreo en Tiempo Real.	El diseño y la configuración del servidor se realiza correctamente.
Propósito Optimizar la eficiencia operativa, la seguridad y la disponibilidad de la red de datos de la institución, garantizando un funcionamiento estable y eficiente.	Al finalizar el proyecto, se espera lograr al menos un 80% de mejora sustancial en la disponibilidad y confiabilidad de los equipos tecnológicos con el Data Center, junto con una mayor eficacia en la detección y prevención de fallos en	Configuración y rendimiento del servidor, pruebas de red.	-Disponibilidad de recursos tecnológicos para el proyecto.

	la infraestructura tecnológica.		
Componentes C1: Diseñar un Data Center conforme a la Norma ISO/IEC 22237. C2: Configurar un servidor de monitoreo en tiempo real.	I. Elementos de diseño del Data Center alineados con las directrices de la Norma ISO/IEC 22237. II. Tiempo de respuesta promedio del servidor de monitoreo en tiempo real para la detección de eventos.	I. Documentación del diseño del Data Center y cómo cumple con los requisitos de la Norma ISO/IEC 22237. II. Registros de eventos generados por el servidor de monitoreo en tiempo real durante un período de tiempo determinado.	-Cumplimiento de la documentación con precisión del diseño del Data Center y su conformidad con los requisitos de la Norma ISO/IEC 22237. -El servidor de monitoreo en tiempo real funciona correctamente y registra eventos de manera confiable durante un período de observación.
Actividades **1.** Diseñar un Data Center conforme a la Norma ISO/IEC 22237. 1.1 Realizar un análisis de las necesidades específicas de la infraestructura tecnológica. 1.2. Estudiar los requisitos establecidos por la Norma ISO/IEC 22237 para un diseño óptimo adaptado a las necesidades de la infraestructura.	**Resumen presupuesto** -Componentes e equipamiento para el Data Center: **83.590Bs** -Equipo para servidor: **0.000 Bs** -Internet e investigación: **5.000 Bs** **Total 88.590Bs**	-Lista de costos del equipamiento para el diseño del Data Center y proceso de configuración del servidor.	La institución de la Fiscalía Departamental de Tarija colabore con el análisis y datos para el proyecto de grado propuesto.

1.3 Seleccionar la ubicación física del Data Center, considerando factores de seguridad, accesibilidad y capacidad de expansión. 1.4 Diseñar la distribución del espacio y la infraestructura eléctrica y de refrigeración. 1.5 Seleccionar los equipos necesarios para el diseño del Data Center. **2.** Configurar un servidor de monitoreo en tiempo real. 2.1 Analizar los equipos y sistemas existentes en la institución para determinar los requerimientos de monitoreo. 2.2 Seleccionar la plataforma de servidor de monitoreo adecuada. 2.3 Configurar el protocolo SNMP para los agentes de monitoreo. 2.4. Pruebas del servidor analizando los datos que recopila en un determinado tiempo.			

1.10.- Metodología de desarrollo del proyecto

La metodología "Top-Down" es un enfoque sistemático para el desarrollo de proyectos que se centra en comenzar con una visión general y luego descomponerla en componentes más pequeños y detallados. En este enfoque, comenzamos con una comprensión clara de los objetivos y requisitos generales del proyecto, y luego procedemos a identificar y abordar los detalles específicos a medida que avanzamos en las fases del proyecto.

Fase 1: Análisis de los Requerimientos

El proceso comienza con un diagnóstico exhaustivo de los objetivos y necesidades de la organización. En esta etapa, se evalúan las metas del negocio, como mejorar la productividad o la conectividad global, así como las metas técnicas relacionadas con el rendimiento, la escalabilidad, la seguridad y la disponibilidad de la red. También se estudia la infraestructura existente, identificando posibles limitaciones, y se realiza un análisis del tráfico actual para prever demandas futuras. Este paso establece una base sólida para garantizar que la red diseñada pueda cumplir con las expectativas de los usuarios y las capacidades de crecimiento.

Fase 2: Desarrollo del Diseño Lógico

En esta fase se construye un modelo abstracto que describe el comportamiento de la red sin entrar en los detalles físicos. Esto incluye la definición de la topología, que especifica cómo se interconectarán los dispositivos, y el esquema de direccionamiento, que organiza los rangos IP y subredes. Además, se seleccionan los protocolos que gestionarán las operaciones de la red, como protocolos de enrutamiento o de capa 2, y se diseñan estrategias para garantizar la seguridad y una administración eficaz. Este diseño lógico actúa como un mapa conceptual que guía el desarrollo posterior.

Fase 3: Desarrollo del Diseño Físico

Tras definir el diseño lógico, se pasa a la elección de componentes y tecnologías específicas que materialicen la red. Se seleccionan los dispositivos adecuados (como switches, routers y servidores), se decide el tipo de conexiones (alámbricas o inalámbricas) y se planifica la instalación física, considerando aspectos como el cableado, las distancias y la compatibilidad entre equipos. Esta etapa traduce las ideas conceptuales en una realidad tangible.

Fase 4: Implementación y Puesta en Marcha

Con los elementos físicos definidos, se inicia la instalación de la infraestructura y la configuración de los dispositivos según lo establecido en los diseños previos. Aquí, se elabora un cronograma para minimizar interrupciones en las operaciones existentes y se realizan pruebas preliminares que aseguren la conectividad y funcionalidad de la red. Este paso marca el inicio de la funcionalidad operativa de la red.

Fase 5: Pruebas del Diseño y Documentación

Una vez que la red está implementada, se realizan pruebas exhaustivas para validar su rendimiento. Estas pruebas simulan diferentes escenarios operativos con el fin de detectar posibles fallos o

ineficiencias. Además, se ajustan configuraciones y se elabora documentación técnica detallada, que incluye diagramas, manuales de configuración y protocolos de mantenimiento. Esto asegura que el conocimiento del diseño sea accesible para futuros ajustes o ampliaciones.

Fase 6: Monitoreo y Optimización

Finalmente, se establece un sistema de monitoreo continuo para garantizar la operatividad de la red. Este proceso permite identificar problemas de rendimiento, aplicar medidas correctivas y realizar ajustes para optimizar su funcionamiento. Además, se implementan rutinas de mantenimiento preventivo y correctivo, asegurando que la red pueda adaptarse a las demandas cambiantes de la organización.

1.11.- Resultados esperados

Se pretende lograr los siguientes resultados:

- Documentación detallada del diseño con la documentación exhaustiva que describa el diseño propuesto del Data Center y el servidor de monitoreo en tiempo real, incluyendo especificaciones técnicas, requisitos de hardware y software, y planos de diseño.
- Desarrollar prototipo del Data Center y configurar el sistema de monitoreo en tiempo real para demostrar la viabilidad técnica y validar los conceptos de diseño propuestos.
- Definir claramente las especificaciones de hardware y software necesarias para el diseño del Data Center y del servidor de monitoreo en tiempo real, teniendo en cuenta los requisitos de la Fiscalía Departamental de Tarija y las normativas pertinentes.
- Realizar pruebas del servidor de monitoreo en tiempo real, asegurando su funcionalidad, rendimiento y cumplimiento de los requisitos establecidos.

1.12.- Beneficiarios

1.12.1.- Beneficiarios Directos

Beneficiará directamente al personal de TI de la Fiscalía, brindándoles una infraestructura tecnológica mejorada que les permitirá gestionar de manera más eficiente los datos y servicios. Además, el personal se verá favorecido con medidas de seguridad física y lógica reforzadas en el Data Center, fortaleciendo así la protección de los datos y la infraestructura. Por otro lado, el personal administrativo y operativo de la Fiscalía experimentará una mejora en el acceso y la gestión de la información, lo que facilitará la realización de sus tareas cotidianas.

1.12.2.- Beneficiarios indirectos

A la comunidad en general, ciudadanos y residentes de Tarija se beneficiarán indirectamente de una administración más efectiva y transparente de la justicia, con la mejora en la eficiencia operativa y la seguridad de la información.

1.13.- Cronograma de Actividades

Nº	Actividad	Nº días	Fecha inicio	Fecha Finaliz.	M 1	M 2	M 3	M 4	M 5	M 6	M 7	M 8
1	Diseñar un Data Center conforme a la Norma ISO/IEC 22237.	**95**	**01/04/24**	**19/07/24**		**X**	**X**	**X**	**X**			
1.1	Realizar un análisis de las necesidades específicas de la infraestructura tecnológica.	**19**	**01/04/24**	**19/04/24**		**X**						
1.2	Estudiar los requisitos establecidos por la Norma ISO/IEC 22237 para un diseño óptimo adaptado a las necesidades de la infraestructura.	**12**	**22/04/24**	**03/05/24**		**X**	**X**					
1.3	Seleccionar la ubicación física del Data Center, considerando factores de seguridad, accesibilidad y capacidad de expansión	**12**	**06/05/24**	**17/05/24**			**X**					

1.4	Diseñar la distribución del espacio y la infraestructura eléctrica y de refrigeración.	**19**	**20/05/24**	**14/06/24**			**X**	**X**				
1.5	Seleccionar los equipos necesarios para el diseño del Data Center.	**33**	**17/06/24**	**19/07/24**				**X**	**X**			
2	Configurar un servidor de monitoreo en tiempo real.	**83**	**04/07/24**	**18/10/24**					**X**	**X**	**X**	**X**
2.1	Analizar los equipos y sistemas existentes en la institución para determinar los requerimientos de monitoreo.	**12**	**22/07/24**	**02/08/24**					**X**	**X**		
2.2	Seleccionar la plataforma de servidor de monitoreo adecuada.	**12**	**05/08/24**	**16/08/24**						**X**		
2.3	Configurar el protocolo SNMP para los agentes de monitoreo.	**26**	**19/08/24**	**13/09/24**						**X**	**X**	
2.4	Pruebas del servidor analizando los datos que recopila en un determinado tiempo.	**33**	**16/09/24**	**18/10/24**							**X**	**X**

Tabla 1. *Cuadro de Actividades*

1.14.- Presupuesto general

Nº	RUBROS	Aporte Universidad	Aporte Institucional	Cantidad	TOTAL (Bs)
	Componentes e equipamiento para el Data Center	0.00	0.00	1 (Anual)	83.590
	Sub total componente				83.590
	Computadora para Servidor	0.00	0.00	1	0.00
	Sub total componente		0.00		0.00
	Internet e Investigación	0.00	0.00	1(Anual)	5.000
	Sub total componente				5.000
	TOTAL				88.590

Tabla 2. *Presupuesto de Proyecto*

Condiciones

- El presupuesto tiene una duración de un año
- Sujeto a variación de precios por aumento en costos nivel nacional e internacional
- Equipos sujetos a Stock
- Cambio por actualización de modelos

Capítulo II

Marco Teórico

2.- Capitulo II: Marco Teórico

2.1.- Introducción

El diseño de un Data Center conforme a la Norma ISO/IEC 22237 es un proyecto que refleja la evolución y la adaptación de las instituciones públicas a las demandas tecnológicas contemporáneas. Esta normativa internacional proporciona un conjunto de especificaciones que abarcan desde la infraestructura física hasta la gestión operativa, asegurando así la resiliencia y la eficiencia de los servicios críticos. La configuración de un Servidor de Monitoreo en Tiempo Real Observium complementa esta iniciativa, ofreciendo una visión detallada del estado de la red y de los dispositivos conectados, lo que permite una respuesta rápida ante cualquier incidencia.

La integración de Observium en la Fiscalía Departamental de Tarija representa un avance significativo en la gestión proactiva de la infraestructura de red. Esta herramienta no solo facilita la detección de anomalías en tiempo real, sino que también promueve una cultura de mantenimiento preventivo, lo cual es esencial para la continuidad de los servicios judiciales. La capacidad de Observium para proporcionar informes detallados y personalizables sobre el rendimiento de la red es una ventaja invaluable para los administradores de sistemas, quienes pueden optimizar los recursos y planificar futuras expansiones con mayor precisión.

El compromiso con los estándares internacionales y la adopción de tecnologías de monitoreo avanzadas son pasos cruciales para garantizar la seguridad y la eficiencia de los Data Centers. En un mundo cada vez más digitalizado, donde la cantidad de datos generados y procesados crece exponencialmente, la relevancia de contar con centros de datos bien diseñados y gestionados adecuadamente es indiscutible. La Fiscalía Departamental de Tarija, al seguir estas directrices, no solo mejora su capacidad operativa, sino que también se posiciona como un referente en la implementación de mejores prácticas en el ámbito judicial y gubernamental.

Este estudio, por lo tanto, no solo tiene un impacto directo en la mejora de la infraestructura tecnológica de la Fiscalía, sino que también sirve como modelo para otras instituciones que buscan modernizar sus operaciones. La convergencia de la normativa ISO/IEC 22237 con las capacidades de Observium crea un ecosistema tecnológico robusto, capaz de soportar las demandas actuales y adaptarse a los desafíos futuros. La Fiscalía Departamental de Tarija, a través de este proyecto, demuestra su compromiso con la excelencia operativa y la seguridad de la información, aspectos fundamentales en la era de la transformación digital.

2.2.- Definición de Data Center

Los Data Centers son esenciales en la era digital, actuando como el corazón de la infraestructura de TI de las organizaciones. Con la creciente dependencia de los datos, su rol se ha vuelto aún más crítico, asegurando que la información esté disponible y protegida en todo momento. La evolución hacia Data Centers definidos por software y entornos de nube híbrida muestra una adaptación a las necesidades cambiantes de eficiencia, escalabilidad y agilidad. A medida que avanzamos, los Data Centers continuarán siendo un pilar fundamental en el soporte y desarrollo de nuevas tecnologías y servicios digitales, facilitando así la transformación digital global.

La arquitectura de un Data Center moderno es una maravilla de la tecnología, con sistemas avanzados de enfriamiento, alimentación ininterrumpida y redes de alta velocidad que trabajan en conjunto para mantener el flujo constante de datos.

La seguridad es una prioridad absoluta en los Data Centers, con múltiples capas de defensa que protegen contra una variedad de riesgos. Los sistemas de detección y supresión de incendios, las barreras físicas y los protocolos de seguridad cibernética son solo algunas de las medidas implementadas para salvaguardar la integridad de los datos.

La eficiencia energética es otro aspecto crítico, ya que los Data Centers consumen una cantidad significativa de electricidad.

2.3.- Beneficios de los Data Centers en Instituciones Gubernamentales

Los Data Centers son fundamentales para el funcionamiento eficiente y seguro de las instituciones gubernamentales. Proporcionan la infraestructura necesaria para una amplia variedad de servicios gubernamentales, desde la seguridad pública hasta la administración de la salud y la educación. La centralización de los recursos tecnológicos en Data Centers permite una gestión de datos más eficaz, facilitando el acceso y el análisis de grandes volúmenes de información.

La continuidad del negocio es otro aspecto importante. Los Data Centers están diseñados para ser resilientes y mantener operaciones ininterrumpidas incluso en el caso de desastres naturales o fallos técnicos. Esto asegura que los servicios esenciales que dependen de la tecnología, como los servicios de emergencia y las comunicaciones gubernamentales, permanezcan disponibles para los ciudadanos en todo momento.

2.4.- Norma ISO/IEC 22237

La Norma ISO/IEC 22237 representa un hito importante en la estandarización de los centros de datos, proporcionando un conjunto de prácticas que buscan optimizar su rendimiento y

confiabilidad. Al establecer criterios claros para el diseño y la operación, esta norma ayuda a las organizaciones a crear infraestructuras de TI resilientes y seguras.

Además, la norma enfatiza la importancia de considerar la sostenibilidad ambiental y la eficiencia energética, lo que es crucial en un mundo cada vez más consciente del impacto ecológico de la tecnología. En resumen, la ISO/IEC 22237 no solo mejora la gestión de los centros de datos, sino que también contribuye a la responsabilidad corporativa y al desarrollo sostenible.

2.4.1.- Principios Generales para Centros de Datos

- La norma describe los principios generales que sustentan los requisitos de la serie ISO/IEC 22237.
- Define aspectos comunes de los centros de datos, incluyendo terminología, parámetros y modelos de referencia (elementos funcionales y su alojamiento).
- Aborda tanto el tamaño como la complejidad prevista de los centros de datos.

2.4.2.- Facilidades e Infraestructuras para Centros de Datos

- Describe los aspectos generales de las instalaciones e infraestructuras necesarias para respaldar los centros de datos.
- Incluye temas como la gestión de la energía, la seguridad física y la distribución de cargas.

2.4.3.- Clasificación de Centros de Datos

- La norma específica un sistema de clasificación basado en los criterios clave de “disponibilidad”, “seguridad” y “eficiencia energética” a lo largo de la vida planificada del centro de datos.
- Permite la provisión efectiva de instalaciones e infraestructuras.

2.4.4.- Análisis de Riesgos y Costos Operativos

- Detalla los aspectos a considerar en un análisis de riesgos empresariales y costos operativos para aplicar la clasificación al centro de datos.

2.4.5.- Operación y Gestión de Centros de Datos

- Proporciona una referencia para la operación y administración de centros de datos.

2.5.- Data Center

Un Data Center, o centro de datos, es una infraestructura crítica para empresas e instituciones que dependen de la tecnología de la información. Estas instalaciones están diseñadas para albergar y proteger equipos de TI, como servidores, dispositivos de almacenamiento y componentes de red.

Además de proporcionar espacio físico, los Data Centers están equipados con sistemas de climatización para controlar la temperatura y la humedad, sistemas de alimentación ininterrumpida y generadores para garantizar la continuidad operativa ante cortes de energía, y sistemas de prevención y extinción de incendios para proteger el equipo de daños.

La seguridad física y cibernética también es primordial, con medidas que van desde el control de acceso hasta la vigilancia.

Componentes de un Data Center

Dentro de un Data Center se encuentra diferentes componentes:

- Equipos (Router, Switch, Servidores, Firewall)
- Rack: alojamiento de los equipos
- UPS: Sistema de alimentación ininterrumpida
- Conexiones Red (Internas, Externas)
- Bandejas – Organizadores
- Climatización

2.6.- Criterio para el diseño de un Data Center

La creación de un centro de datos es una tarea compleja que requiere una planificación meticulosa y un diseño cuidadoso para asegurar la continuidad y la alta disponibilidad de los servicios críticos. La protección del hardware es fundamental, ya que equipos como servidores de aplicaciones, de almacenamiento, web, de virtualización y bases de datos son el corazón de la operatividad de una organización.

Un análisis de riesgos exhaustivo es el primer paso en la planificación de una infraestructura de misión crítica, donde se deben identificar los requerimientos operativos y de disponibilidad, así como el impacto potencial de cualquier tiempo de inactividad. Esto permite determinar la clase de disponibilidad necesaria y diseñar un centro de datos que no solo cumpla con las necesidades actuales de la organización, sino que también sea escalable y flexible para adaptarse a los cambios futuros y a las nuevas tecnologías que puedan surgir.

2.7.- Clasificación y diseño de Data Center según la Norma ISO/IEC 22237

2.7.1.- Bases Teóricas.

Existen organismos que regulan las normas y estándares para el correcto diseño del Data Center, entre los cuales tenemos:

Figura 3. *Relación entre un Estándar y un Norma o Código*

Estándares. - El objetivo fundamental de un estándar es garantizar el mínimo nivel.

- **Normas o Códigos**. - Los códigos son lineamientos y procedimientos exclusivamente para la protección de la vida Humana y equipos de red.

2.7.2.- Aprobación y vigencia de la norma ISO/IEC 22237

La norma ISO/IEC 22237 es un conjunto de estándares internacionales que establece los requisitos y directrices para el diseño, construcción y operación de Data Centers. Este estándar se enfoca en aspectos clave como la infraestructura física, la eficiencia energética, la sostenibilidad y la seguridad de los centros de datos, con el objetivo de proporcionar una base sólida para su funcionamiento óptimo.

La primera parte de la norma, ISO/IEC 22237-1, fue aprobada y publicada en febrero de 2018 fue publicada oficialmente por ISO e IEC a través de sus respectivas oficinas centrales, que están ubicadas en Ginebra, Suiza. A partir de esa fecha, ha estado disponible para su implementación en organizaciones que desean garantizar que sus instalaciones de Data Centers cumplan con las mejores prácticas internacionales en términos de diseño y operación. Esta norma ha sido creada por el comité técnico conjunto ISO/IEC JTC 1, que trabaja en el desarrollo de estándares relacionados con tecnologías de la información, en colaboración con la Comisión Electrotécnica Internacional (IEC).

El conjunto de normas ISO/IEC 22237 reemplaza la norma EN 50600, utilizada principalmente en Europa, ampliando su alcance y alineando sus directrices con un estándar internacional que puede ser aplicado globalmente. Desde su entrada en vigor, ISO/IEC 22237 ha sido reconocida como un marco de referencia fundamental para la planificación y gestión de centros de datos, permitiendo a las organizaciones asegurar la eficiencia, seguridad y continuidad de sus operaciones.

Para las instituciones que deseen garantizar el cumplimiento de estándares de calidad internacional, la adopción de la ISO/IEC 22237 es una herramienta clave, ya que cubre áreas como la gestión del riesgo, la infraestructura energética, el control ambiental y la protección física de los equipos.

2.8.- La Norma ISO/IEC 22237 en Data Centers

Los centros de datos albergan y respaldan la tecnología de la información y los equipos de telecomunicaciones de red para el procesamiento, el almacenamiento y el transporte de datos. Los requieren tanto los operadores de red (que prestan esos servicios en las instalaciones del cliente) como las empresas dentro de las instalaciones de los clientes.

Los centros de datos deben proporcionar instalaciones e infraestructuras modulares, escalables y flexibles para adaptarse fácilmente a los requisitos del mercado que cambian rápidamente. Además, el consumo de energía de los centros de datos se ha vuelto crítico, tanto desde el punto de vista ambiental (reducción de la huella de carbono) como desde el punto de vista económico (coste de la energía) para el operador del centro de datos. La implementación de los centros de datos varía en términos de:

a) finalidad (empresa, co-ubicación, co-hospedaje o instalaciones del operador de la red);

b) nivel de seguridad;

c) tamaño físico;

d) alojamiento (construcciones móviles, temporales y permanentes).

La serie ISO/IEC 22237 especifica requisitos y recomendaciones para apoyar a las distintas partes involucradas en el diseño, planificación, adquisición, integración, instalación, operación y mantenimiento de instalaciones e infraestructuras dentro de los centros de datos.

Necesidades en los Centros de Datos según la Norma

- Alta Disponibilidad
- Modularidad
- Desempeño
- Gestión
- Seguridad
- Alta Densidad y Eficiencia Operacional

La serie ISO/IEC 22237 comprende los siguientes documentos que ayudan a la creación de los data center:

- ISO/IEC 22237-1 Parte 1: Conceptos generales;
- ISO/IEC 22237-2 Parte 2: Construcción de edificios;
- ISO/IEC 22237-3 Parte 3: Distribución de energía;
- ISO/IEC 22237-4 Parte 4: Control ambiental;
- ISO/IEC TS 22237-5 Parte 5: Infraestructura de cableado de telecomunicaciones;
- ISO/IEC TS 22237-6 Parte 6: Sistemas de seguridad;
- ISO/IEC TS 22237-7 Parte 7: Información operativa y de gestión.

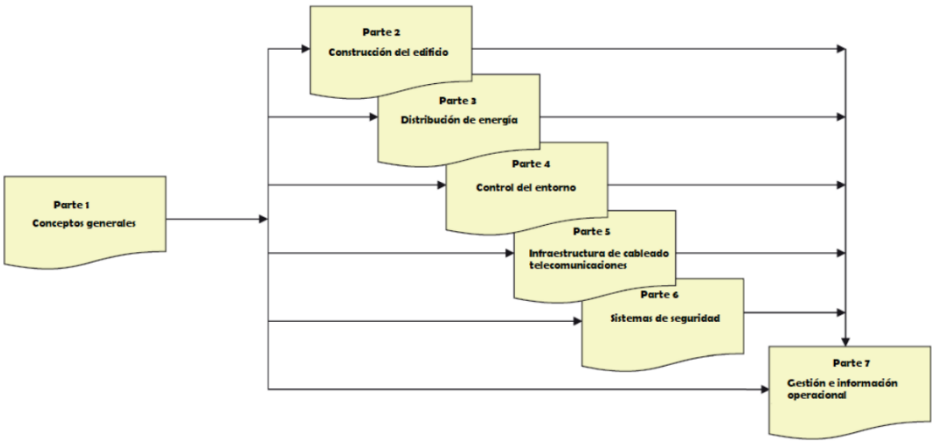


Figura 4. *Relación esquemática entre la serie de documentos ISO/IEC 22237*

2.9.- Clasificación de los Centro de Datos de Normas y Estándares

BICSI-002-2014	**ISO/IEC 22237-2018**	**UP TIME INS-TITUTE**	**ICREA-Std137.2017**	**TIA/EIA 942**	**NTP-ISO/IEC 22237:1-7**
CLASES	CLASES	TIER	NIVELES	RATING	TIPOS
4	4	4	5	4	4

Tabla 3. *Clasificación de Centro de Datos en Normas y Estándares*

2.10.- La ISO/IEC

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) son entidades fundamentales en el desarrollo de estándares internacionales, incluyendo aquellos para la tecnología de la información a través del comité técnico conjunto ISO/IEC JTC 1. Los miembros de estas organizaciones, que incluyen organismos nacionales, trabajan

colectivamente en comités técnicos para formular normas que faciliten el comercio internacional y promuevan la innovación y la seguridad. La colaboración con otras entidades gubernamentales y no gubernamentales asegura una amplia representación y relevancia en el proceso de estandarización. Además, las Directivas ISO/IEC proporcionan una guía esencial para la creación y mantenimiento de estos documentos normativos, asegurando que se sigan procedimientos rigurosos y transparentes.

2.11.- Norma ISO/IEC 22237-1- Conceptos Generales

2.11.1.- Análisis de riesgos al negocio

El análisis de riesgos se puede utilizar como una herramienta de gestión que permite la comparación con el riesgo total aceptable y muestra las tendencias resultantes de la actividad de mitigación. A los efectos de esta norma, el riesgo asociado con un evento relacionado con las instalaciones e infraestructuras del centro de datos que interrumpe la prestación del servicio del centro de datos se define como riesgo de evento que es una función del impacto y la probabilidad donde: El impacto se puede clasificar como:

a) Impacto es la magnitud o gravedad de los incidentes o impactos adversos, expresados numéricamente o duración nominalmente esperada de la pérdida de servicio (disponibilidad) del evento.

b) La probabilidad es la verosimilitud del evento.

El impacto del riesgo puede evaluarse utilizando diferentes unidades de medida, costo, seguridad, etc. La probabilidad de que ocurra un evento se puede definir de manera similar, es decir: muy bajo, bajo, medio o alto:

Ejemplo de medición de mapa de riesgo para el data center:

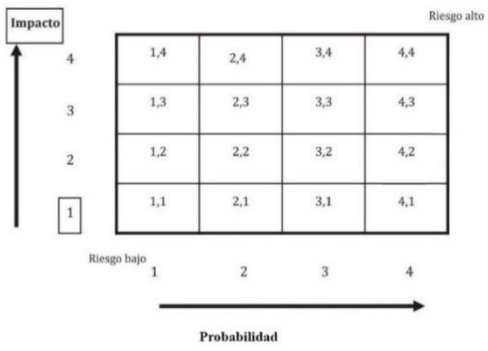


Figura 5. *Impacto y probabilidad de un evento según la norma*

Tratamiento del Riesgo. - Luego del resultado de la valoración del riesgo se debe dar tratamiento a los riesgos latentes que la empresa no acepta, haciendo uso de las estrategias ya conocidas: Reducir o mitigar, Asumir o retener, Evitar, Transferir

2.11.2.- Disponibilidad de Espacios e instalaciones

La disponibilidad de las instalaciones y la infraestructura es crucial para el funcionamiento óptimo de un data center. La determinación de la disponibilidad deseada debe basarse en un análisis de riesgo y un análisis de costos. Es importante reconocer que los requisitos de disponibilidad pueden fluctuar según el momento específico, ya sea diario, semanal o mensual.

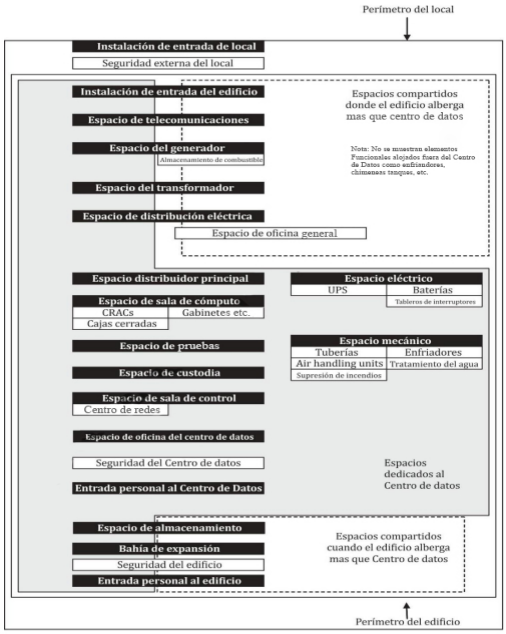


Figura 6. *Diagrama de instalaciones en Data Centers*

2.11.3.- Principios generales de diseño

La planificación estratégica para el desarrollo de un centro de datos es un proceso meticuloso que se divide en varias fases críticas. En la Fase 1, la Estrategia, se recopila información vital para definir los objetivos del proyecto. La Fase 2, Objetivos, es asegurando que cada aspecto del centro de datos esté alineado con las necesidades corporativas y los estándares de diseño. La Fase 3, Especificaciones del Sistema, establece los parámetros detallados para la infraestructura. Durante la Fase 4, el diseñador debe considerar cuidadosamente las especificaciones y objetivos para ofrecer. La Fase 5 implica una decisión crítica por parte del propietario, seleccionando la opción más viable basada en el diseño y los modelos de costos presentados. Posteriormente, en la Fase 6, el diseñador tiene la tarea de traducir esta elección en un diseño funcional detallado, asegurando

que todos los aspectos del centro de datos estén optimizados para la operación y administración eficientes. Finalmente, la Fase 7 sella el proceso con la aprobación del propietario. En la Fase 8 del diseño final y planificación del proyecto, el diseñador establece las dimensiones y componentes para todas las infraestructuras siguiendo las especificaciones. Posteriormente, en la fase 9, el propietario, con la asistencia del diseñador, selecciona al contratista adecuado. Durante la fase 10, la construcción es supervisada meticulosamente por el propietario y el diseñador, asegurando que todas las infraestructuras cumplan con los estándares de aceptación antes de que el centro de datos entre en funcionamiento. Finalmente, en la fase 11, el proyecto se entrega al propietario para su operación, marcando el comienzo de una nueva etapa en la vida del centro de datos. Este enfoque estructurado garantiza que todas las partes involucradas estén alineadas y comprometidas con el éxito del proyecto desde el inicio hasta la finalización.

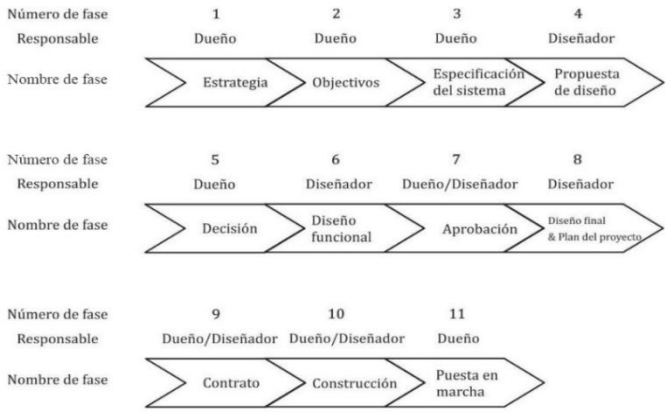


Figura 7. *Principios a seguir en el diseño de Data Centers*

2.11.4.- Factores Presupuestales

2.11.4.1.- Evaluación De Costos

El proceso de selección del sitio debiera incluir un análisis detallado de todos los costos relacionados con toda ubicación particular. A continuación, se indican los costos que debieran considerarse al comparar los sitios disponibles:

Los costos únicos que pueden ser significativos de tal manera que cualquiera pueda dirigir el proceso de selección del sitio son:

- Costos inmobiliarios: costos de demolición para cualquier estructura existente; costos de preparación del sitio.

2.11.4.2.- Evaluación del Sitio.

En una evaluación de riesgos debieran evaluarse los siguientes peligros:

- Peligros naturales (por ejemplo, geológicos, meteorológicos y biológicos)
- Eventos humanos (por ejemplo, accidentales e intencionales)
- Eventos tecnológicos (por ej., accidentales e intencionales)

2.11.5.- Conclusión

La normativa para la construcción de centros de datos enfatiza la importancia de una planificación detallada y una distribución eficiente de los espacios. Esto incluye áreas específicas para telecomunicaciones, electricidad, computación, y almacenamiento, así como la seguridad y la gestión de la energía. La evolución tecnológica ha permitido que los costos de implementación y operación de los centros de datos se reduzcan significativamente, lo que facilita la adopción de infraestructuras digitales avanzadas. Estos centros son vitales para la automatización y la transformación digital, actuando como el núcleo central de las organizaciones en la era de la información.

2.12.- ISO/IEC 22237-2 Construcción de edificios

2.12.1.- Ubicación

La selección de la ubicación para la construcción de edificios es un proceso que involucra múltiples consideraciones para asegurar la viabilidad y sostenibilidad del proyecto. Es fundamental elegir un sitio con bases sólidas para garantizar la estabilidad estructural y la seguridad a largo plazo. En cuanto al entorno, es imprescindible evaluar las condiciones climáticas, la humedad y los niveles de contaminación, ya que estos factores pueden afectar tanto a la integridad del edificio como al bienestar de sus ocupantes. Implementar medidas de control ambiental y utilizar materiales adecuados puede mitigar riesgos potenciales como incendios o deterioro por condiciones adversas. Por último, un análisis periódico del sitio y del edificio ayudará a mantener un ambiente seguro y funcional para todos los usuarios.

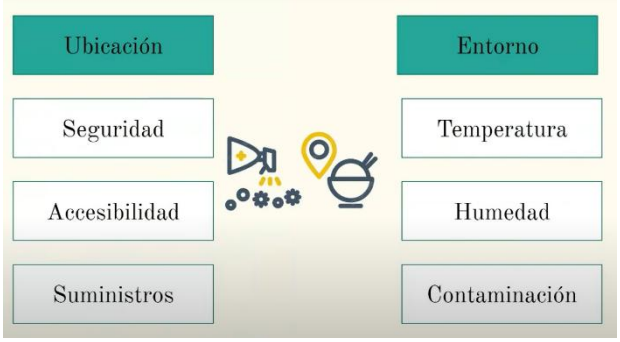


Figura 8. *Principios a seguir en la ubicación del edificio para Data Centers*

2.12.2.- Estructura del edificio

La normativa de construcción es fundamental para garantizar la seguridad y funcionalidad de los edificios, especialmente aquellos destinados a albergar centros de datos críticos. Los tres principios mencionados, resistencia, estabilidad y resistencia al fuego, son pilares esenciales en el diseño estructural. La resistencia se refiere a la capacidad del edificio para soportar cargas permanentes y temporales sin sufrir daños, incluyendo el peso de equipos y la tensión de cables y otros componentes. La estabilidad asegura que el edificio pueda resistir fuerzas externas como vientos fuertes y sismos, manteniendo su integridad estructural. Finalmente, la resistencia al fuego implica el uso de materiales y diseños que prevengan la propagación del fuego y permitan una evacuación segura. Además, la ubicación estratégica del edificio en zonas con menor riesgo de desastres naturales contribuye a la mitigación de posibles daños, complementando así las medidas de seguridad inherentes al diseño.

2.12.3.- Protección contra Incendios

La protección contra incendios es un aspecto crítico en la gestión de edificios y la seguridad de las personas. La detección temprana y precisa de incendios permite una respuesta rápida y efectiva, minimizando el riesgo para las personas y la infraestructura. Es esencial tener sistemas de detección y extinción de incendios bien ubicados y mantenidos, así como realizar evaluaciones periódicas de riesgos para identificar áreas vulnerables. Además, es fundamental contar con planes de evacuación claros y bien comunicados, que incluyan señalización adecuada y rutas de escape accesibles para todos los ocupantes del edificio. Estas medidas no solo cumplen con las normativas de seguridad, sino que también proporcionan tranquilidad a quienes trabajan y visitan estas instalaciones. La prevención y preparación son claves para garantizar la seguridad y protección tanto de las personas como de los datos críticos que se almacenan en los edificios.

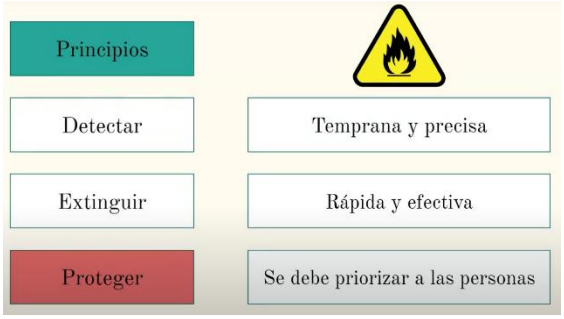


Figura 9. *Protección contra incendios en Data Centers*

2.12.4.- Protección contra Inundaciones

La protección contra inundaciones es un aspecto crítico en la planificación y construcción de edificios, especialmente en áreas propensas a este tipo de desastres naturales. Las estrategias efectivas incluyen la instalación de sistemas de drenaje adecuados que no solo manejen el agua que ingresa, sino que también la redirijan lejos de la estructura. La elevación de los edificios y la protección física mediante muros de contención son medidas preventivas esenciales. Además, es crucial la implementación de bombas de agua y la ubicación estratégica de equipos críticos por encima del nivel de inundación anticipado.

2.12.5.- Acumulación de electricidad Estática

La protección contra la electricidad estática es fundamental en entornos donde se manipulan componentes electrónicos sensibles. La acumulación de cargas electrostáticas puede causar daños irreparables en los circuitos y dispositivos. Sistemas de conexión a tierra para disipar estas cargas de manera segura. Estas medidas preventivas son esenciales para mantener la integridad de los equipos y garantizar la seguridad en el lugar de trabajo.

2.12.6.- Protección Contra Ruido

El propósito es reducir el ruido evitar su propagación con diferentes cosas con el uso de equipo informático silencioso.

2.12.7.- Seguridad Física

Los centros de datos comparten la prioridad de proteger activos valiosos. Ambos utilizan tecnologías avanzadas para salvaguardar estos activos contra amenazas como intrusiones, vandalismo y desastres naturales. La seguridad física y cibernética es esencial, implementando medidas como control de acceso y vigilancia constante. El objetivo final es asegurar la integridad y la disponibilidad de la información, garantizando que estén protegidos y accesibles solo para aquellos autorizados.

2.12.8.- Instalaciones

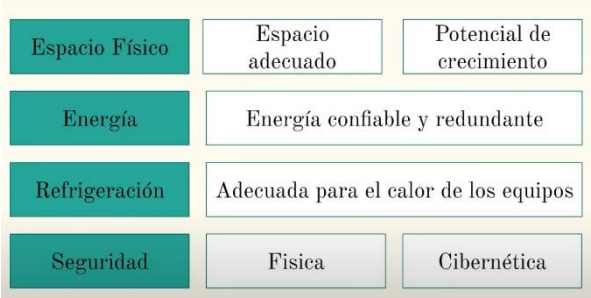


Figura 10. *Principios a seguir en instalaciones de Data Centers*

2.12.9.- Clasificación

La clasificación de las bases de datos en términos de su ubicación y gestión puede dividirse en tres categorías principales: on-premise, colocation y cloud. Las soluciones en instalaciones implican que las bases de datos están alojadas físicamente en las instalaciones de la empresa, ofreciendo control total, pero con mayores costos de inversión y mantenimiento. La colocación es un modelo híbrido donde las empresas alquilan espacio y servicios de un tercero, manteniendo la propiedad de su hardware. Finalmente, las soluciones en la nube representan la externalización completa, donde los recursos de almacenamiento y computación son proporcionados por un servicio en la nube, permitiendo escalabilidad y un modelo de pago según el uso que puede ayudar a reducir los gastos.

2.12.10.- Clasificación de equipos

La clasificación de equipos en un centro de datos es un proceso que considera varios factores críticos para garantizar la eficiencia y seguridad de las operaciones. Los servidores, el almacenamiento, las redes y la seguridad son los pilares fundamentales de esta clasificación. El hardware se refiere a los componentes físicos como servidores y dispositivos de almacenamiento, mientras que el software abarca los sistemas operativos y aplicaciones necesarias para la gestión de datos. La infraestructura, incluyendo la energía y refrigeración, es esencial para mantener el funcionamiento óptimo del hardware y software. Además, la seguridad, tanto física como de datos, es crucial para proteger contra amenazas externas e internas, asegurando la integridad y disponibilidad de la información.

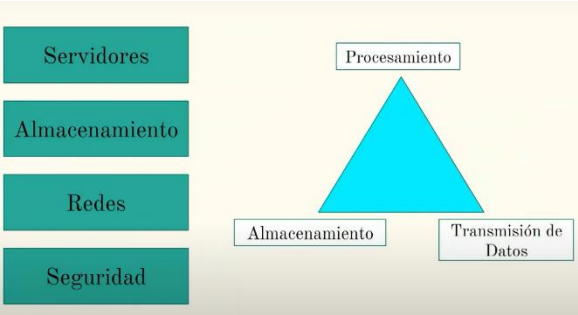


Figura 11. *Clasificación de equipos en Data Centers*

2.13.- ISO/IEC 22237-3 Distribución de Energía

2.13.1.- Objeto y campo de aplicación

Este punto nos proporciona directrices y especificaciones para el diseño e implementación y gestión de la distribución de la energía en centros de datos además busca garantizar un suministro eléctrico eficiente confiable y seguro para los equipos y sistemas críticos que operan en el centro de datos.

2.13.2.- Suministro y distribución de energía dentro de los data center

La distribución de energía eléctrica en los centros de datos es crucial para mantener la operatividad y la seguridad. Las fluctuaciones en la tensión, corriente y frecuencia pueden afectar significativamente el rendimiento y la disponibilidad de los servicios. Por ello, es esencial contar con sistemas de suministro primario y secundario robustos, que a menudo se conectan a través de transformadores ubicados dentro o fuera de las instalaciones. Estos sistemas deben ser diseñados para garantizar una entrega de energía constante y confiable, asegurando así la continuidad del negocio y la protección de los datos críticos.

2.13.3.- Elementos funcionales del suministro de energía

La distribución de energía eléctrica en los centros de datos es crucial para mantener la operatividad y la seguridad de las infraestructuras. Un diseño eléctrico eficiente y modular es esencial para soportar el crecimiento y la agilidad empresarial, permitiendo a los centros de datos adaptarse a las cambiantes demandas de energía y enfriamiento. Además, la implementación de sistemas de alimentación ininterrumpida (UPS) y la elección de componentes de alta eficiencia pueden aumentar la eficiencia del sistema sin comprometer la disponibilidad. La correcta distribución de energía no solo garantiza la continuidad operativa, sino que también apoya la sostenibilidad y la eficiencia energética del centro de datos.

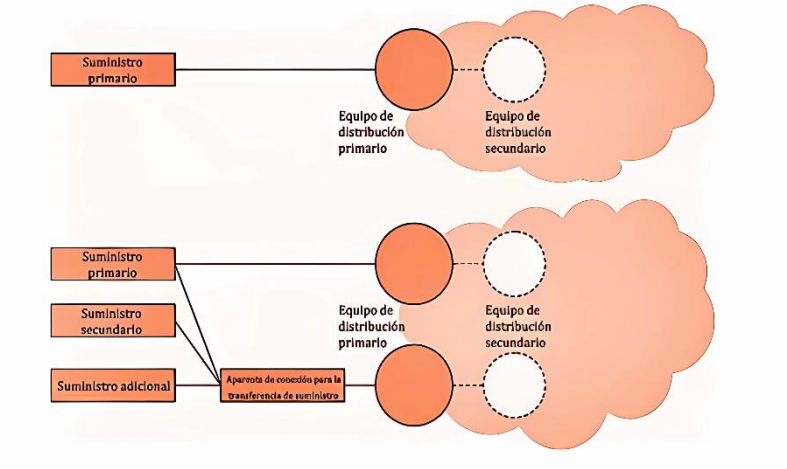


Figura 12. *Elementos funcionales de suministro de energía.*

2.13.4.- Disponibilidad y Distribución de energía

La disponibilidad y la optimización continua de los recursos son aspectos cruciales en la gestión de infraestructuras críticas, como los centros de datos. Un sistema de energía de respaldo robusto, que puede incluir bancos de condensadores o generadores eléctricos, es esencial para prevenir interrupciones en el servicio. Además, contar con una estación de transformadores adecuadamente dimensionada asegura que la corriente alterna se convierta en una forma utilizable para los dispositivos del centro de datos. La organización y etiquetado preciso de los equipos facilitan el mantenimiento y las reparaciones, mejorando la seguridad y el rendimiento del sistema.

La redundancia y la fiabilidad en la distribución de energía son fundamentales para garantizar la continuidad operativa. Un diseño redundante permite que el sistema siga funcionando incluso si una parte falla. Los circuitos eléctricos deben estar diseñados para manejar cargas variables y picos de demanda, proporcionando un suministro de energía estable y seguro. Por último, un sistema de monitoreo remoto avanzado es indispensable para supervisar la distribución de energía y actuar proactivamente ante cualquier anomalía, asegurando así la integridad y la eficiencia del centro de datos.

Especificación de Equipos	Considerar cargas capacitivas y distorsión armónica al seleccionar transformadores y controles.
Redundancia de Trayectorias de Distribución	Diseñar rutas de energía para soportar la carga máxima en caso de falla de la ruta redundante.
Interruptores de Transferencia Estática	Evaluar cuidadosamente debido a su "punto único de falla" y riesgo de corrientes de cortocircuito.
Estado de Tomacorrientes	Mantener y verificar el estado de los tomacorrientes que alimenten equipos para garantizar fiabilidad.
Modularidad y Fiabilidad	Equilibrar modularidad con fiabilidad, evitando aumentar componentes en detrimento de la confiabilidad.
Cableado de Suministros Múltiples	Usar cables separados para múltiples suministros de energía para minimizar riesgos y asegurar confiabilidad.
Entrada de Suministro de Energía	Garantizar la protección física y separación de las entradas de energía para mantener la seguridad.

Figura 13. *Disponibilidad de energía*

2.13.5.- Clasificacion de diseño de disponibilidad

En el diseño de centros de datos, las clases de disponibilidad son fundamentales para garantizar la eficiencia y la continuidad del servicio. La Clase 1, con una trayectoria única sin resiliencia, es adecuada para situaciones donde la tolerancia a fallos no es crítica. La Clase 2 añade redundancia de componentes, permitiendo operaciones de mantenimiento sin interrupción del servicio. La Clase 3 introduce trayectorias múltiples con soluciones de reparación operación concurrente, mejorando significativamente la resiliencia. Finalmente, la Clase 4 ofrece la máxima resiliencia con trayectorias múltiples, reparación operación concurrente y tolerancia a fallos, adecuada para entornos donde la disponibilidad es crítica.

2.13.6.- Distribución de LVDC

A menor pérdida de energía hay mayor eficiencia en la distribución de energía en comparación con el sistema convencional. Lo que puede resultar en una reducción significativa de los costos operativos a lo largo del tiempo. Además, la integración de nuevas tecnologías en las redes de baja tensión es crucial para maximizar los beneficios a largo plazo, incluyendo mejoras en la eficiencia energética y la sostenibilidad operativa de los centros de datos modernos.

- Doble fuente, doble ruta de alimentación
- La calidad de la energía suministrada por los equipos UPS estáticos debe estar conforme con la clase apropiada
- SPD (Sistema de Protección contra Sobretensiones) en entradas, salidas y bypass
- EPO (Apagado de emergencia)

2.14.- ISO/IEC 22237-4 Control ambiental

La Parte cuatro de la normativa se enfoca en el control ambiental dentro de las instalaciones e infraestructuras de centros de datos. El objetivo es garantizar la regulación óptima de factores como la temperatura, la humedad relativa, el movimiento de fluidos, la presencia de partículas y vibraciones, así como la disposición del suelo y la ubicación del equipo. Estos controles son cruciales para mantener la integridad y eficiencia operativa de los centros de datos. Además, se promueven prácticas de ahorro de energía y se asegura la seguridad física de los sistemas de control ambiental. Esta sección de la norma también hace referencia a conceptos generales y sistemas de seguridad, alineándose con otras partes de la normativa ISO para una comprensión holística y coherente de las mejores prácticas en la gestión de infraestructuras de centros de datos. Los términos clave incluyen la refrigeración adiabática, que aprovecha la evaporación para enfriar el aire; el piso de acceso, que permite un fácil acceso a servicios subterráneos; y los controles ambientales de confort, que ajustan las condiciones para el bienestar del personal. Además, se definen términos técnicos como la carga de calor y la temperatura del aire exterior, fundamentales para el diseño y operación de sistemas eficientes. El termino CRAC (aire acondicionado de sala de cómputo) son también parte integral de la terminología estándar en la industria.

2.14.1.- Requisitos

Al diseñar un sistema de control ambiental para un centro de datos, es crucial considerar la tecnología actual, la seguridad física y la disponibilidad del centro. Los factores como la vibración, la fricción y la obstrucción en las vías de fluidos de temperatura controlada deben ser evaluados cuidadosamente. Es vital mantener la integridad del flujo de aire y fluidos. Además, la gestión de la humedad y el punto de condensación son esenciales para proteger equipos sensibles a la estática, asegurando así la continuidad y eficiencia operativa del centro de datos.

Se recomienda utilizar unidades de refrigeración con desacoplamiento de vibraciones integrado por todas las piezas giratorias.

2.14.2.- Distribución Eléctrica y Telecomunicación

Para los espacios de distribución eléctrica y centros de datos, es crucial mantener condiciones ambientales óptimas para asegurar el funcionamiento adecuado del equipo. La Sociedad Americana de Aire Acondicionado, Refrigeración y Calefacción (ASHRAE) recomienda mantener la temperatura operativa entre 18 °C y 27 °C. Además, se aconseja una humedad relativa entre el 20% y el 70% para prevenir problemas de condensación y garantizar la longevidad del equipo.

Estas recomendaciones son un punto de partida y deben ajustarse según las especificaciones de cada proveedor y las características únicas de cada instalación.

2.14.3.- Espacio eléctrico

- La temperatura debe mantenerse en concordancia con las instrucciones del proveedor del equipo cuando no exista esta información la temperatura debe mantenerse por encima de los 0 grados centígrados.
- Se debe proveer ventilación natural.
- Se debe proporcionar calefacción anti condensación.
- Se debe monitorear la temperatura y la humedad relativa.

2.14.4.- Colocación de Equipos de UPS

La normativa recomienda tomar en cuenta lo que recomienda el fabricante de estos equipos, estos equipos deben estar adicionados con un aire acondicionado ya que muchas veces estos equipos se calientan y entonces necesitan buenas condiciones ambientales.

- Ups estático o rotativo entonces la temperatura debe mantenerse entre 15 y 35 °C.
- El calor residual que se genera puede ayudar también a precalentar la planta generadora de reserva entonces de esta manera también se ahorra un poco de energía.
- La batería su temperatura debe mantenerse en (20+-2) °C.

2.14.5.- Disponibilidad

La "n" en la planificación de carga y redundancia en data centers es un concepto fundamental para garantizar la continuidad y la fiabilidad del servicio. Representa la cantidad mínima de componentes necesarios para que un sistema funcione correctamente. Por ejemplo, una configuración "n" tendría exactamente los componentes necesarios, mientras que "n+1" indica un componente adicional para mayor seguridad. "2n" duplica los componentes necesarios, y "2n+1" añade otra unidad más, ofreciendo aún más redundancia y robustez al sistema.

2.14.6.- Requisitos por Nivel de Granularidad

- Temperatura de aire de suministro
- Temperatura de aire de entorno
- Humedad Relativa
- Humedad relativa externa y temperatura
- Presión de aire y remoción de calor

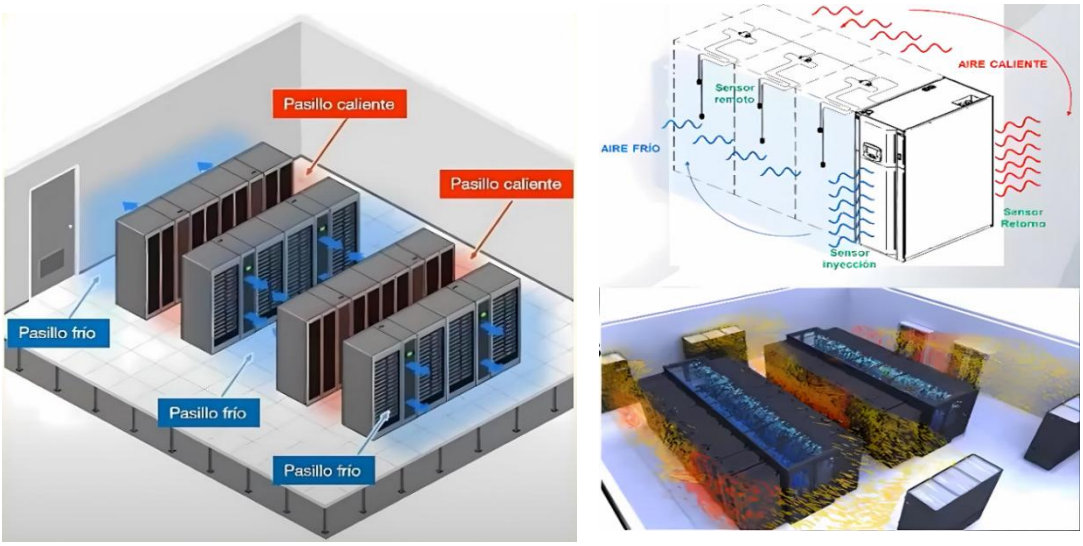


Figura 14. *Manejo de aire en los data centers*

2.14.7.- Distribución de temperatura para aire controlado

Los requisitos de temperatura y humedad para los equipos son cruciales para garantizar el funcionamiento óptimo y la longevidad del hardware. Las mejores prácticas sugieren mantener la temperatura del aire de suministro en un data center entre 18 °C y 27 °C, con un rango óptimo de 21 °C a 23 °C. La humedad relativa debe estar entre el 20% y el 80%, asegurando así un ambiente controlado que previene daños por condensación o electricidad estática. Además, la presión del aire y la refrigeración eficiente son esenciales para disipar el calor generado por los equipos, especialmente en los racks y contenedores de servidores. Estos parámetros deben ser monitoreados y ajustados cuidadosamente para mantener las condiciones ambientales dentro de los límites seguros y eficientes. La granularidad en la distribución de estos contenedores permite un control más detallado de las condiciones ambientales, como la temperatura y la humedad. Además, los sistemas de contención de aire son esenciales para separar los pasillos calientes y fríos, optimizando así el flujo de aire y mejorando la eficiencia de la refrigeración. Estos ajustes no solo mejoran la eficiencia energética, sino que también contribuyen a una mayor disponibilidad de

refrigeración libre, lo que a su vez puede reducir los costos operativos y aumentar la potencia eléctrica disponible para el centro de datos.

Figura 15. *Estructuración de equipos de refrigeración en data centers*

2.15.- ISO/IEC 22237-5 Infraestructura de Cableado de Telecomunicaciones

2.15.1.- Especificaciones y Recomendaciones

La infraestructura de cableado en los centros de datos es fundamental para garantizar la operatividad y eficiencia de estos complejos sistemas. La normativa sobre cableado no solo proporciona una guía detallada para la instalación y gestión de los cables, sino que también establece estándares de disponibilidad para asegurar que los sistemas estén operativos y accesibles cuando se requieran. Es esencial considerar varios tipos de cableado, como el general para TI y el de monitoreo y control, que supervisan aspectos críticos como la distribución de energía, el control ambiental y la seguridad física. La planificación y diseño cuidadosos del cableado son cruciales desde las primeras etapas de diseño o renovación de un centro de datos, integrándose con sistemas de energía, control ambiental, seguridad y sistemas de iluminación. Una planificación inadecuada puede llevar a interrupciones del servicio, afectando la continuidad y la eficiencia del centro de datos.

2.15.2.- Cableado de Telecomunicaciones en Sala de Computo

El cableado de comunicaciones en una sala de cómputo es fundamental para el funcionamiento eficiente de los sistemas de tecnología de la información. La norma ISO/IEC 11801 establece los estándares para el cableado estructurado, que incluye tanto cableado de cobre como de fibra óptica, y es aplicable a una variedad de entornos, incluidos los centros de datos. Este estándar internacional especifica los requisitos para sistemas de cableado que son utilizables para un amplio rango de aplicaciones, asegurando así la calidad y el rendimiento de las redes de comunicación.

La escalabilidad y flexibilidad son aspectos clave del cableado genérico, permitiendo adaptarse a las necesidades cambiantes y soportar el desarrollo de aplicaciones de alta velocidad de datos. Se puede tomar una o una combinación de las siguientes formas:

- Punto a Punto
- Fijo

2.15.3.- Clasificación de disponibilidad para la infraestructura de cableado

La infraestructura de cableado actúa como el sistema circulatorio que permite el flujo de información y comunicación. La clasificación de disponibilidad es crucial, no solo para la eficiencia operativa sino también para la seguridad de la información. En la próxima sección, exploraremos cómo diferentes clases de disponibilidad se aplican en entornos de computación y otros espacios, destacando la importancia de una infraestructura robusta y segura. La simplicidad de una conexión directa puede ser atractiva, pero también debemos ser conscientes de las vulnerabilidades que puede presentar.

2.15.3.1.- Cableado para disponibilidad de clase 1

Esta es en esencia de la clase un simple directa, pero con una vulnerabilidad inherente que viene a ser la falta de redundancia se adopta para pequeñas empresas donde el riesgo es bajo y la simplicidad reina.

- Conexión punto a punto
- Cables predeterminados
- Conexiones locales limitadas
- Un solo path

2.15.3.2.- Cableado para disponibilidad de clase 2

Es donde la redundancia entra en escena con un solo path, aquí una interrupción no significa el fin, es como tener un camino alternativo en una ruta crítica esta capa adicional de seguridad se combina con una gestión de cables más estratégico vital para entornos de tamaño mediano donde la flexibilidad es clave.

- Cableado fijo con arquitectura de un solo Path y redundancia
- Adecuada gestión de cables y de fácil expansión
- Conexiones cruzadas y centrales y locales
- Considerar el número de contactos y longitud total de canales

2.15.3.3.- Cableado para disponibilidad de clase 3

Piensa en rutas múltiples en una red de caminos entrelazados cada uno capaz de sostener la carga si uno otro falla la gestión posterior.

- Considera el radio de curvatura y almacenamiento para futuras expansiones
- Gestión de cables posterior y lateral
- Flexibilidad y escalabilidad
- Redundancia Multi-Path

2.15.3.4.- Cableado para disponibilidad de clase 4

Es la fortaleza de la disponibilidad con multi-Path en todas las esquinas aquí cada cable cada conexión cuenta y se gestiona con una precisión quirúrgica el radio de curvatura eh la predeterminación de cables se diseña pensando en la misión crítica es el nivel de infraestructura donde el tiempo de inactividad es un concepto desconocido.

- Diseño que permita traslados adiciones y cambios eficientes
- Control del radio de curvatura para la gestión de cables
- Cableado predeterminado
- Cableado Multi-Path y redundancia

2.15.4.- Sistemas de Rutas

Los sistemas de cableado en los centros de datos deben cumplir con normativas específicas que garantizan la seguridad y eficiencia de las infraestructuras. La norma ISO/IEC 22237-1:2021 establece conceptos generales para las instalaciones y estructuras de centros de datos, incluyendo aspectos como la disponibilidad, la seguridad física y la eficiencia energética. Además, es fundamental que los sistemas de vías no interfieran con otros sistemas como los de tuberías, para evitar daños y asegurar un acceso fácil para mantenimiento. Estos estándares son esenciales para el diseño y operación efectiva de los centros de datos modernos.

2.15.5.- Apertura de baldosas de piso

Los sistemas de piso no deben ser accesibles, son pisos que no permiten el acceso de los servicios públicos como subterráneos tuberías, cables y conductos. Solo son para el acceso de los cables que van a ser instalados y también se debe aplicar los requisitos de la ISO/IEC 22237-2.

2.15.6.- Sistema de Gestión de Cable

La gestión de cables en centros de datos es una tarea crítica que asegura el funcionamiento eficiente y la escalabilidad de estas instalaciones. Los sistemas de gestión de cables deben cumplir con

ciertos requisitos para garantizar la eficacia y la seguridad. Primero, deben ofrecer la capacidad necesaria para soportar el máximo nivel de carga definido. Segundo, es esencial que dispongan de espacio suficiente para almacenar cualquier exceso de material. Tercero, deben mantener un control adecuado sobre el radio de curvatura de los cables, evitando daños por doblado o flexión debido a condiciones ambientales. Por último, en el caso de sistemas que no proporcionan soporte continuo, como mallas o canastas, su uso debe limitarse a rutas verticales donde el soporte discontinuo sea adecuado. Además, se debe proporcionar una lista de combinaciones aceptables de sistemas de vías y cables al operador del centro de datos para mantener un equilibrio y asegurar una correcta mitigación de riesgos.

2.15.7.- Administración y Operación de la infraestructura de cableado

El sistema de gestión de la infraestructura automatizada

Esta nos dice que es una documentación en tiempo real y administración eficiente, administra eficientemente la capa física o sea la capa encargada de la transmisión de datos y dice que debería integrarse en herramientas de administración de centro de datos existentes.

Cables de fibra óptica

Al momento de realizar la instalación nos dice que se debe revisar las caras finales de la fibra óptica ya que debe haber contaminantes y para realizar esa inspección y procedimiento de limpieza se van a guiar ese proceso, para que no se dañe tanto el cableado como el equipo.

2.16.- ISO/IEC 22237-6 Sistemas de Seguridad

2.16.1.- Campo de Aplicación

El campo de aplicación de esta Norma aborda la seguridad física dentro de centros de datos basándose en los criterios de disponibilidad, seguridad y está más que todo centrado en la 22237-1, sin embargo, esta norma específica los requisitos y recomendaciones para las instalaciones de sistemas de centros de datos utilizados con respecto a la protección contra el:

- Acceso no autorizado soluciones de diseño organizativas y tecnológicas.
- Incendios en las instalaciones de centro de datos
- Otros eventos dentro o fuera de las instalaciones de centro de datos que puedan afectar el nivel de protección establecido.

2.16.2.- Cumplimiento

Para que un centro de datos cumpla con los requisitos de este documento como tal se debe primero:

- Aplicar la clase de protección requerida del apartado de protección física protección física a cada una de las instalaciones del centro de datos.
- Aplicar los requisitos de la clase de protección correspondiente a las secciones de clase de protección de acceso no autorizado y la aplicación de las mismas.
- Los sistemas para soportar los requisitos de la sección de la aplicación de protección deben cumplir con la sección de sistemas para evitar el acceso no autorizado.

2.16.3.- Protección Física

La disposición general para entender un poco el contexto el grado de seguridad física aplicado a las instalaciones infraestructura de centro de datos afecta tanto la disponibilidad como de las funciones de integridad/seguridad de los datos almacenados y se procesan en los centros de datos por lo que los requisitos y recomendaciones para las instalaciones de estos centros de datos se relacionan a la protección tenemos tres puntos:

- el acceso no autorizado
- incendio ocurrido en instalaciones dentro del procesamiento de datos
- otros eventos dentro o fuera de las instalaciones

2.16.4.- Evaluación de Riesgos

Los requisitos de seguridad operativa de determinarse después de una evaluación de riegos basada en las amenazas a las que están expuestos los datos y una clasificación de estos datos. Se debe tener en cuenta:

- **Valor activo. -** La clasificación del material debe determinarse en una fase temprana para poder implementar las contramedidas de protección adecuadas.
- **Probabilidad. -** La probabilidad de que se produzca algún tipo de ataque al bien protegido
- **Análisis de amenazas. -** Por ejemplo, la amenaza de acceso no autorizado a la propiedad
- **Análisis de Vulnerabilidad. -** Nivel suficiente de seguridad física o control técnico de los datos alojados.

Finalmente, una vez que se hayan implementado las contramedidas básicas, se deben tomar las siguientes decisiones con respecto a los riesgos residuales en función de la aceptación del riesgo.

- **Desviación tolerable. -** Se aceptan los riegos residuales y no se implementan contramedidas adicionales.
- **Tratamiento. -** Se toman medidas adicionales para contrarrestar los riesgos restantes.

- **Transferencia. -** El riesgo se transfiere a otra parte por ejemplo obteniendo cobertura de seguro adicional reducir el riesgo.
- **Terminación. -** Se detiene la actividad que representa un riesgo.

2.16.5.- Clases de Protección

2.16.5.1.- Clase de Protección contra acceso no autorizado

La disposición general que tiene esta clase es de cuatro clases:

- La primera es la zona de su público esto generalmente son visitantes o entregas que serán muy exceptuadas.
- La clase dos sería los empleados visitantes área personal autorizado.
- La clase tres sería áreas regidas para ciertos empleados.
- La clase cuatro sería más que todo administrativos o partes importantes de la empresa que no puede acceder a muchas personas, ni el personal autorizado.

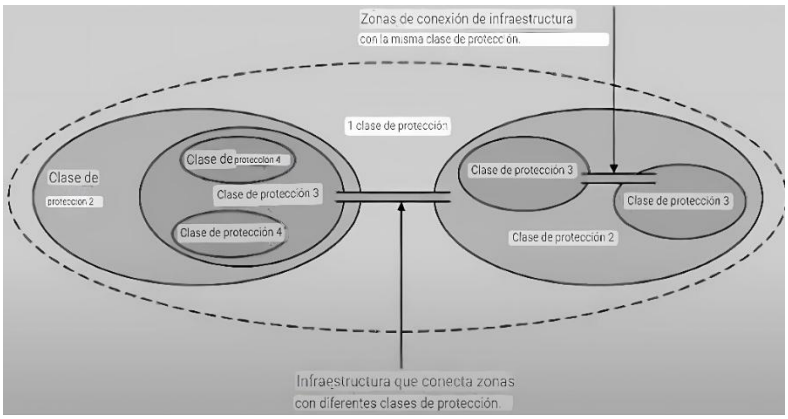


Figura 16. *Clases de protección en Data Centers*

2.16.5.2.- Acceso a las instalaciones del centro de datos

- **Generalidades. -**Todas las rutas y señalizaciones deben estar claramente marcadas para cada clase de protección de acceso. Además de una iluminación y administración correcta en ellas.
- **Estacionamiento. -** Debe existir cierta seguridad y distancia respecto a otras zonas, ya sea a través de videovigilancia, iluminación, etc.
- **Visitantes. -** Debe ser un espacio adecuado para atender a los visitantes, además de brindar mecanismos de puerta adecuados para el personal y visitantes autorizados.

- **Entregas. -** El muelle de carga debe estar controlado mediante mecanismos de seguridad para el área de centro de datos, ya sea como enclavamientos o videovigilancia.

2.16.6.- Clase de Protección contra incendios en instalaciones de data centers

2.16.6.1.- Disposición General

Tipo de protección	**Clase 1**	**Clase 2**	**Clase 3**	**Clase 4**
Protección interior contra incendios	No se aplica ninguna protección especial	El área debe de estar protegida contra incendios mediante un sistema de detección y extinción de incendios que pueda garantizar la seguridad de las funciones críticas del centro de datos durante un incendio en esta área de zona de clase 1.	El área debe de estar protegida contra incendios mediante un sistema de detección y extinción de incendios que pueda garantizar la seguridad de las funciones críticas del centro de datos durante un incendio en esta área de zona de clase 1 y 2.	El área debe de estar protegida contra incendios mediante un sistema de detección y extinción de incendios que pueda garantizar la seguridad de las funciones críticas del centro de datos durante un incendio en esta área o en otra área del centro de datos

Tabla 4. *Tabla de Clase de Protección Contra Incendios*

2.16.6.2.- Protección contra incendios

- **Zonas de incendio y barreras:** Los muros y barreras deben tener la resistencia mínima al fuego requerida dependiendo de la clase de protección. Además de tener tecnologías cortafuegos.
- **Sistemas de alarma y detección de incendios:** Las alarmas deben estar instaladas correctamente y no interrumpir directamente la funcionalidad del centro de datos. Debe estar señaladas correctamente.
- **Sistemas fijos de extinción de incendios:** Debe haber un sistema fijo para minimizar el riesgo de personal y equipo dentro de las locaciones, ya sea un incendio incipiente o de menor escalabilidad.

2.16.6.3.- Sistemas Fijos de extinción de incendios

- **Sistemas de recuperación de oxígeno:** Los sistemas de extinción de incendios con oxígeno reducido mantienen el oxígeno en una concentración reducida para evitar ignición o propagación del fuego.
- **Sistemas de extinción por agua:** Utilizando rociadores y agua nebulizada, buscando proteger el edificio y las instalaciones,
- **Sistemas de aerosol condensado:** Estos no se deben utilizar en áreas residenciales o áreas con equipos electrónicos.
- **Sistemas de extinción con espuma:** Debe haber un sistema fijo para minimizar el riesgo de personal y equipo dentro de las locaciones, ya sea un incendio incipiente o de menor escalabilidad.

2.16.6.4.- Clase de Protección contra efectos fuera de las instalaciones de data centers

La "Clase de Protección contra Efectos Fuera de las Instalaciones de los Centros de Procesamiento de Datos" establece niveles específicos de resistencia y mitigación contra influencias ambientales externas que podrían afectar las instalaciones que albergan elementos críticos, como equipos y sistemas de procesamiento de datos.

La clasificación se basa en la exposición a eventos ambientales como incendios, interferencias electromagnéticas, vibraciones (incluidos terremotos), inundaciones, gases y polvo.

2.16.6.5.- Clase de Protección contra influencias ambientales

Tipo de Protección	**1Clase**	**2do. grado**	**3er grado**	**4to. grado**
Protección contra incidentes ambientales	No se aplica ninguna protección especial	Mitigación aplicada	Mitigación aplicada	Mitigación aplicada

Tabla 5. *Clase de protección contra incidentes ambientales*

2.16.6.6.- Implementación

Disposiciones generales:

- Los límites de cada clase de protección deben garantizar el nivel necesario de protección física contra influencias externas del entorno.

- Evaluación de interferencias electromagnéticas externas para determinar la necesidad de medidas de mitigación específicas.
- Posibilidad de prohibir teléfonos móviles en fronteras de protección o instalar estaciones base para mitigar interferencias.

Clase de protección 1

- No existen requisitos ni recomendaciones.

Clase de protección 2

- Protección física necesaria en cualquier camino abierto que atraviese los límites de esta clase y superiores.
- Importancia de garantizar el funcionamiento normal o de emergencia de las infraestructuras del centro de procesamiento de datos.
- Evitar entrada de objetos que puedan dañar o limitar los servicios.

2.16.6.7.- Elementos de los sistemas de protección no autorizado

Objeto	Elemento
Personal	- Garantizar disponibilidad y formación del personal calificado. - Verificaciones de antecedentes para gestionar amenazas internas. - Controles adicionales en casos de mayor seguridad.
Procesos	- Desarrollar y operar procesos operativos para el funcionamiento continuo del sitio. - Ejemplos: gestión y procesamiento de visitantes, recepción y procesamiento de entregas.
Físico	- Desarrollar y operar controles físicos en el sitio para garantizar niveles adecuados de protección. - Determinado por evaluaciones de riesgos o requisitos operativos de las organizaciones anfitrionas.
Tecnológico	- Utilizar sistemas tecnológicos para apoyar el funcionamiento del sitio. - Ejemplos: sistemas automáticos de control de acceso, sistemas de Videovigilancia (VSS).

Figura 17. *Elementos de protección no autorizado en los data centers*

2.16.6.8.- Tecnología

Iluminación del área de seguridad

- La ubicación estratégica de la iluminación proporciona prevención de intrusiones y apoyo al sistema de monitoreo VSS.
- La iluminación debe tener al menos 5 lux y evitar sombras profundas alrededor del centro de datos.
- Posibilidad de iluminación adicional fuera de la valla fronteriza para crear una pantalla de luz efectiva.

2.17.- ISO/IEC 22237-7 Gestión e Información Operacional

La gestión de un data center implica una serie de normativas y estándares que aseguran su correcta operación y sostenibilidad. Entre los aspectos más críticos se encuentran el mantenimiento y el proceso de decomiso, ambos esenciales para la continuidad y actualización tecnológica. El mantenimiento preventivo y correctivo es vital para prevenir fallos y garantizar la operatividad. Por otro lado, el decomiso de equipos por obsolescencia o recambio tecnológico debe realizarse considerando las implicaciones ambientales y de sostenibilidad. Estas prácticas son fundamentales para mantener la eficiencia y la competitividad en el ámbito de los data centers.

2.17.1.- Mantenimiento

La implementación de un plan de mantenimiento integral para un centro de datos es crucial para garantizar su operatividad y eficiencia a largo plazo. Este plan debe abarcar no solo la infraestructura física, como el ambiente y la climatización, sino también los sistemas eléctricos, incluyendo el mantenimiento de pozos a tierra y la revisión de las baterías de UPS, las cuales son esenciales para la continuidad del servicio en caso de cortes de energía. Es importante considerar la vida útil promedio de las baterías, que suele ser de tres años, y planificar su reemplazo oportuno para evitar fallos.

Además, se debe evaluar la relación costo-beneficio entre el mantenimiento de equipos antiguos versus la adquisición de nuevos. A veces, resulta más conveniente reemplazar completamente un equipo obsoleto que invertir en su mantenimiento.

El plan debe ser dinámico, adaptándose a las necesidades cambiantes del centro de datos y a la evolución tecnológica. Debe contemplar revisiones periódicas y ajustes basados en el desempeño y la vida útil de cada equipo. Algunos equipos requerirán mantenimiento en intervalos más cortos, mientras que otros podrán esperar. La clave es mantener una visión a futuro, programando y presupuestando las actividades de mantenimiento para asegurar la operatividad continua y eficiente del centro de datos.

El mantenimiento preventivo es esencial para garantizar la operatividad y eficiencia de los equipos. Un plan de mantenimiento bien estructurado debe incluir inspecciones regulares, limpieza y reemplazo de partes según sea necesario, basándose en las recomendaciones del fabricante y la frecuencia de uso del equipo. La implementación de un programa de mantenimiento preventivo puede reducir significativamente la necesidad de reparaciones correctivas, lo que a su vez puede minimizar el tiempo de inactividad y los costos asociados. Además, mantener un registro detallado

de todas las actividades de mantenimiento ayuda a tomar decisiones informadas sobre actualizaciones tecnológicas y reemplazos de equipos a largo plazo.

2.17.2.- Desmantelar Equipos

El proceso de desmantelamiento y actualización de equipos en un centro de datos es una tarea crítica que requiere una planificación meticulosa y una ejecución cuidadosa. La obsolescencia tecnológica y el recambio de equipos son factores inevitables en la gestión de infraestructuras tecnológicas. Es esencial comprender que retirar un equipo no es simplemente desconectarlo y removerlo; implica una serie de pasos que aseguran que la integridad de la red y los sistemas permanezcan intactos. Los cables internos, por ejemplo, deben ser etiquetados y rastreados para evitar confusiones y desorden posterior.

Un plan detallado para desmantelar debe incluir la documentación de cada equipo, la evaluación de los impactos en la red y los procedimientos para la eliminación segura de datos. Además, es importante considerar la disposición final del hardware, que puede incluir reciclaje o reutilización de acuerdo con las políticas de sostenibilidad de la empresa. La continuidad de los datos y la operatividad del centro de datos no deben verse comprometidas durante este proceso.

2.18.- Servidor de Monitoreo en Tiempo Real

2.18.1.- Definición del monitoreo en tiempo real

El monitoreo en tiempo real se define como un proceso continuo y automatizado que permite la recolección, análisis y presentación de datos en tiempo real, con el objetivo de obtener información actualizada y precisa sobre un sistema, proceso o actividad en particular.

Este enfoque de monitoreo se basa en la captura y procesamiento de datos en tiempo real, lo que permite una vigilancia constante y una respuesta rápida a eventos o condiciones detectadas. Se utiliza en diversos ámbitos, como la gestión de redes, la supervisión de sistemas industriales y la seguridad informática.

La implementación del monitoreo en tiempo real implica el uso de sensores, instrumentos de medición y sistemas de adquisición de datos para capturar y transmitir información de manera continua. Un sistema de procesamiento y visualización analiza los datos recibidos, generando alertas, reportes y visualizaciones en tiempo real.

El monitoreo en tiempo real tiene como objetivo mejorar la eficiencia, la seguridad y la calidad de los procesos, facilitando la toma de decisiones oportunas y la optimización de recursos. Además,

proporciona la detección temprana de problemas, la identificación de patrones y tendencias, y la generación de informes para el análisis posterior.

2.18.2.- Importancia del monitoreo en tiempo real en entornos críticos

La importancia del monitoreo en tiempo real en entornos críticos radica en su capacidad para proporcionar una vigilancia constante y actualizada de los sistemas y procesos vitales de una organización. En estos entornos, donde cada segundo cuenta y cualquier interrupción o fallo puede tener consecuencias graves, el monitoreo en tiempo real se convierte en una herramienta esencial para garantizar la seguridad, la eficiencia y la continuidad de las operaciones.

El monitoreo en tiempo real es crucial en entornos críticos para identificar de manera proactiva cualquier anomalía o desviación del funcionamiento normal, permitiendo una rápida respuesta y mitigación de riesgos.

El monitoreo en tiempo real brinda una visibilidad constante de los sistemas y procesos, lo que permite la detección temprana de problemas y la toma de decisiones informadas para evitar daños mayores. En entornos críticos, el monitoreo en tiempo real garantiza la monitorización continua de variables esenciales, como temperatura, presión, flujo de datos o rendimiento del sistema, lo que contribuye a la prevención de fallos y a la optimización de los recursos.

2.18.3.- Beneficios del monitoreo en tiempo real en instituciones gubernamentales

El monitoreo en tiempo real en instituciones gubernamentales se refiere al proceso de supervisar y controlar de forma continua y en tiempo real los sistemas y procesos operativos que son críticos para el funcionamiento del gobierno. Este enfoque permite a las instituciones gubernamentales tener una visión actualizada de su rendimiento y tomar decisiones informadas para mejorar la eficiencia, la transparencia y la toma de decisiones en beneficio de la sociedad.

El monitoreo en tiempo real en instituciones gubernamentales permite la identificación inmediata de problemas y el análisis en tiempo real de datos, lo que mejora la capacidad de respuesta y ayuda a evitar retrasos y errores en la toma de decisiones.

También facilita la transparencia y la rendición de cuentas al proporcionar información actualizada sobre el rendimiento de los programas y servicios gubernamentales, lo que permite a los ciudadanos y a los responsables de la toma de decisiones evaluar y mejorar la eficacia de las políticas públicas.

2.18.4.- Fundamentos de SNMP (Simple Network Management Protocol)

2.18.4.1.- Descripción del protocolo SNMP y su propósito

La descripción del protocolo SNMP (Simple Network Management Protocol) y su propósito se refiere a la explicación de los fundamentos de este protocolo de gestión de red ampliamente utilizado. SNMP es un protocolo de comunicación que permite a los administradores de red supervisar, controlar y gestionar dispositivos de red de manera eficiente. Su objetivo principal es facilitar la gestión de redes, proporcionando un conjunto estandarizado de comandos y procedimientos para la recopilación de información y el control de dispositivos en una red. El protocolo SNMP se basa en una arquitectura cliente-servidor.

La MIB (Management Information Base), juega un papel fundamental en SNMP, ya que define los objetos gestionados que pueden ser monitoreados y controlados mediante este protocolo. La MIB establece una estructura jerárquica de datos que permite a los administradores acceder a información relevante de los dispositivos de red.

El propósito del protocolo SNMP, es proporcionar un estándar de gestión de red que permita a los administradores supervisar y controlar eficientemente los dispositivos de red en un entorno heterogéneo. SNMP facilita la monitorización en tiempo real, la detección de problemas, la configuración remota y la recopilación de datos estadísticos, lo que contribuye a la eficiencia operativa y a la toma de decisiones informadas en la administración de redes.

2.18.4.2.- Componentes y arquitectura del protocolo SNMP

Los componentes y la arquitectura del protocolo SNMP (Simple Network Management Protocol) se refieren a los elementos fundamentales y la estructura de este protocolo de gestión de red ampliamente utilizado. SNMP se basa en una arquitectura cliente-servidor y consta de varios componentes clave que permiten la supervisión y control de dispositivos de red.

El protocolo SNMP, consta de tres componentes principales: el administrador SNMP, el agente SNMP y la base de información de administración (MIB). El administrador SNMP es el encargado de enviar comandos y solicitudes de información al agente SNMP, que se encuentra en los dispositivos de red. El agente SNMP recopila y almacena información sobre el estado y rendimiento de los dispositivos, y responde a las solicitudes del administrador. La MIB define la estructura jerárquica de los objetos gestionados que pueden ser supervisados y controlados mediante SNMP.

La arquitectura de SNMP, sigue un modelo cliente-servidor. El administrador SNMP actúa como el cliente, mientras que el agente SNMP actúa como el servidor. El administrador envía solicitudes al agente para obtener información o realizar acciones, y el agente responde con la información solicitada o lleva a cabo las acciones requeridas. Esta comunicación se realiza a través de mensajes SNMP, que se transmiten mediante el protocolo de transporte UDP (User Datagram Protocol).

En cuanto a la arquitectura de la red, SNMP se puede implementar en una estructura de red distribuida, donde múltiples agentes SNMP están presentes en diferentes dispositivos de red y se comunican con un administrador centralizado. Además, SNMP es compatible con el modelo de gestión de red OSI (Open Systems Interconnection), que consta de cinco capas: física, enlace de datos, red, transporte y aplicación.

2.18.4.3.- Funcionamiento del protocolo SNMP para la gestión de dispositivos de red

El funcionamiento del protocolo SNMP (Simple Network Management Protocol) para la gestión de dispositivos de red se basa en un conjunto de operaciones y procedimientos diseñados para supervisar y controlar de manera eficiente los dispositivos de una red.

El funcionamiento de SNMP implica la interacción entre dos entidades principales: el administrador SNMP y el agente SNMP. El administrador SNMP es el encargado de realizar solicitudes al agente SNMP para obtener información específica del dispositivo, como el estado, rendimiento, configuración y eventos. Estas solicitudes se envían mediante mensajes SNMP, utilizando el protocolo de transporte UDP (User Datagram Protocol).

Por su parte, el agente SNMP se encuentra en los dispositivos de red y responde a las solicitudes del administrador. El agente recopila y almacena información sobre los parámetros y variables de gestión en su Base de Información de Administración (MIB). Cuando recibe una solicitud del administrador, el agente busca la información solicitada en la MIB y la envía de vuelta al administrador en forma de respuestas SNMP.

2.18.4.4.- Importancia de SNMP en la administración y monitoreo de redes

La importancia del protocolo SNMP (Simple Network Management Protocol) en la administración y monitoreo de redes radica en su capacidad para proporcionar un marco estándar y eficiente para la supervisión y control de dispositivos de red. SNMP se ha convertido en un componente fundamental en las operaciones de administración de redes debido a sus aspectos.

SNMP permite a los administradores de red obtener una visión completa y detallada del estado y rendimiento de los dispositivos de red. A través de consultas SNMP, los administradores pueden monitorear parámetros como el ancho de banda, la utilización de recursos, los errores de transmisión, entre otros. Esta información es esencial para identificar problemas, diagnosticar fallas y tomar decisiones informadas para optimizar el rendimiento de la red.

Además, SNMP es altamente escalable y puede gestionar redes de cualquier tamaño, desde redes pequeñas hasta entornos empresariales complejos. SNMP proporciona capacidades de notificación y alerta, permitiendo a los administradores recibir notificaciones instantáneas cuando se producen eventos importantes o anormales en la red.

Finalmente, SNMP es un estándar ampliamente aceptado en la industria de redes y es compatible con una amplia gama de dispositivos y sistemas de gestión.

2.18.5.- Herramienta de monitoreo Observium

2.18.5.1.- Introducción a la herramienta de monitoreo Observium

Observium es una herramienta de monitoreo de red de código abierto diseñada para brindar una visión integral y en tiempo real del rendimiento y la salud de los dispositivos de red. Se trata de una solución completa de monitoreo basada en el protocolo SNMP (Simple Network Management Protocol) que ofrece una amplia gama de funcionalidades para supervisar y analizar redes de cualquier tamaño.

Observium permite la monitorización de dispositivos de red, como enrutadores, conmutadores, servidores, dispositivos de almacenamiento y más. Proporciona una interfaz intuitiva y personalizable que muestra información detallada sobre el estado de los dispositivos, el tráfico de red, las interfaces, los servicios y otros parámetros relevantes. Entre las características principales de Observium se encuentran:

- Descubrimiento automático: Observium realiza un descubrimiento automático de los dispositivos de red presentes en la infraestructura y los agrega a la herramienta de monitoreo de forma automática. Esto simplifica el proceso de configuración y permite una rápida puesta en marcha.

- ❖ Monitorización en tiempo real: La herramienta proporciona datos actualizados en tiempo real sobre el rendimiento y la disponibilidad de los dispositivos de red. Esto permite detectar y resolver problemas de manera proactiva, evitando interrupciones en la red.
- ❖ Alertas y notificaciones: Observium permite configurar alertas y notificaciones personalizadas para informar sobre eventos importantes, como caídas de conexión, sobrecargas de tráfico, cambios en el estado de los dispositivos, entre otros.
- ❖ Generación de informes: La herramienta ofrece la posibilidad de generar informes detallados sobre el rendimiento de la red, el uso de ancho de banda, la disponibilidad de los dispositivos y otros parámetros relevantes. Estos informes son útiles para el análisis, la planificación y la toma de decisiones informadas.

2.18.5.2.- Características y funcionalidades de Observium

Observium es una herramienta de monitoreo de red de código abierto que ofrece una amplia gama de características y funcionalidades para supervisar y analizar redes de cualquier tamaño, estas son algunas de las principales características y funcionalidades de la herramienta:

- ❖ Descubrimiento automático: Observium realiza un descubrimiento automático de los dispositivos de red presentes en la infraestructura y los agrega a la herramienta de monitoreo de forma automática.
- ❖ Monitorización en tiempo real: Observium proporciona datos actualizados en tiempo real sobre el rendimiento y la disponibilidad de los dispositivos de red.
- ❖ Alertas y notificaciones: La herramienta permite configurar alertas y notificaciones personalizadas para informar sobre eventos importantes en la red.
- ❖ Generación de informes: Observium ofrece capacidades de generación de informes que permiten obtener información detallada sobre el rendimiento de la red, el uso de ancho de banda, la disponibilidad de los dispositivos y otros parámetros relevantes.
- ❖ Interfaz intuitiva: La herramienta cuenta con una interfaz intuitiva y fácil de usar que muestra la información de manera clara y organizada.
- ❖ Soporte SNMP: Observium se basa en el protocolo SNMP (Simple Network Management Protocol) para adquirir datos de los dispositivos de red. Esto le permite monitorear una amplia variedad de dispositivos compatibles con SNMP, como enrutadores, conmutadores, servidores, dispositivos de almacenamiento, entre otros.

2.18.5.3.- Importancia de Observium en la monitorización de dispositivos de red.

Observium desempeña un papel crucial en la monitorización de dispositivos de red al proporcionar una solución integral y eficiente para supervisar y gestionar la infraestructura de red. Se destacan las siguientes razones que resaltan la importancia de esta herramienta:

- Supervisión proactiva: Observium permite supervisar los dispositivos de red de manera continua y proactiva.
- Identificación de cuellos de botella: Con Observium, es posible identificar cuellos de botella en la red y analizar el rendimiento de los dispositivos y las interfaces.
- Generación de informes y análisis: Observium ofrece funcionalidades avanzadas de generación de informes y análisis de datos. Esto permite obtener una visión completa del estado de la red, el comportamiento del tráfico y el rendimiento de los dispositivos a lo largo del tiempo. Los informes generados por Observium son valiosos para realizar análisis comparativos, evaluar tendencias y tomar decisiones estratégicas para mejorar la gestión de la red.
- Detección de fallas y resolución de problemas: Observium ayuda a detectar fallas en la red y simplifica la resolución de problemas. Con sus alertas y notificaciones personalizables, la herramienta alerta sobre eventos críticos y permite a los administradores de red tomar medidas rápidas para solucionar problemas.
- Soporte multiplataforma: Observium es compatible con una amplia gama de dispositivos y tecnologías de red, lo que lo convierte en una solución versátil para entornos heterogéneos.

2.19.- Modelo OSI

El modelo OSI es una estructura conceptual diseñada para estandarizar las funciones de un sistema de comunicación en redes informáticas, dividida en siete capas jerárquicas. Cada capa tiene una función específica y se comunica únicamente con la capa adyacente. Su objetivo principal es facilitar la interoperabilidad y el desarrollo de aplicaciones y protocolos. A continuación, se describen sus capas:

Capa Física: Responsable de la transmisión de bits a través del medio físico, incluye aspectos como voltajes, cables, conectores y la modulación de señales. Establece las bases de la conectividad física y define estándares como Ethernet y Wi-Fi para la comunicación básica.

Capa de Enlace de Datos: Garantiza una transferencia confiable de datos entre nodos conectados directamente, organizándolos en tramas y gestionando direcciones físicas (MAC). También detecta y corrige errores básicos en la transmisión.

Capa de Red: Se encarga de dirigir los paquetes a través de distintas redes, utilizando direcciones lógicas como las del protocolo IP. Su función incluye el enrutamiento, fragmentación y reensamblaje de datos.

Capa de Transporte: Proporciona transmisión confiable y controla el flujo de datos entre sistemas finales. Protocolos como TCP aseguran la entrega ordenada y sin pérdidas, mientras que UDP prioriza la velocidad sobre la fiabilidad.

Capa de Sesión: Maneja el inicio, mantenimiento y finalización de sesiones entre aplicaciones en dispositivos diferentes. Sincroniza datos y restablece conexiones interrumpidas.

Capa de Presentación: Traduce los datos al formato comprensible por la aplicación, asegurando compatibilidad entre diferentes sistemas. Además, realiza compresión y encriptación para proteger los datos.

Capa de Aplicación: Permite la interacción directa con el usuario a través de aplicaciones específicas como navegadores, clientes de correo y servicios de transferencia de archivos.

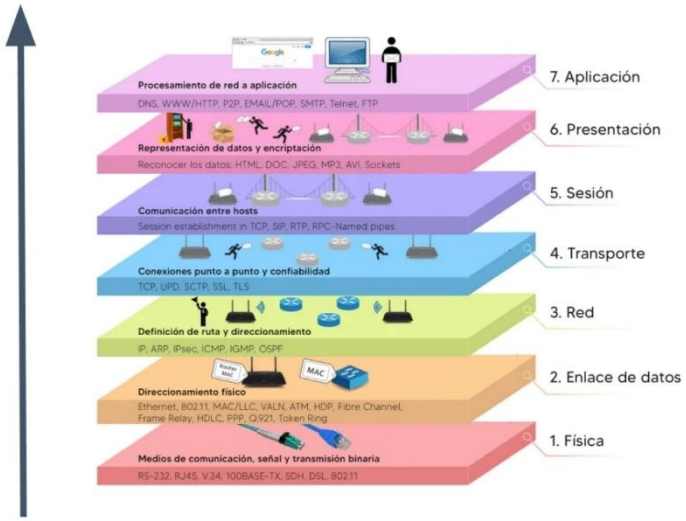


Figura 18. *Modelo OSI*

2.20.- Modelo TCP/IP

La arquitectura TCP/IP (Transmission Control Protocol/Internet Protocol) es el delo de referencia de comunicación en redes que define cómo se estructuran y transfieren los datos a través de distintas redes. Consta de cuatro capas: Aplicación, Transporte, Internet y Acceso a la Red, cada una de las cuales tiene responsabilidades específicas para el procesamiento y la transmisión de datos. TCP/IP es el estándar fundamental de las redes de datos y permite la interoperabilidad entre diferentes sistemas y redes, desde pequeñas redes locales hasta Internet a nivel global.

Capa de Aplicación: Reúne las funciones de las capas superiores del OSI. Incluye protocolos como HTTP, FTP y DNS para la interacción entre aplicaciones.

Capa de Transporte: Proporciona mecanismos para la transmisión de datos confiable o rápida, dependiendo del protocolo utilizado: TCP para comunicaciones robustas y UDP para aplicaciones en tiempo real como videollamadas.

Capa de Internet: Equivalente a la capa de red del modelo OSI, maneja el direccionamiento y enrutamiento de paquetes mediante el protocolo IP.

Capa de Acceso a la Red: Combina las funciones de las capas física y de enlace del modelo OSI, definiendo cómo los datos se envían y reciben en el medio físico. Incluye tecnologías como Ethernet, Wi-Fi y DSL. Integra funciones de las capas superiores del modelo OSI y permite que las aplicaciones interactúen con la red, utilizando protocolos como HTTP, FTP y SMTP.

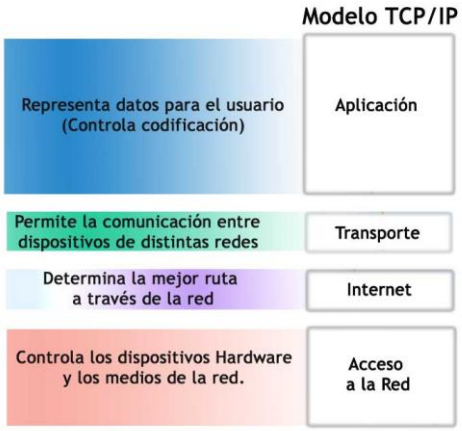


Figura 19. *Modelo TCP/IP*

2.21.- Estándar ANSI/TIA-568-B para cableado estructurado

La norma ANSI/TIA-568-B es un estándar de la Telecommunications Industry Association (TIA) y el American National Standards Institute (ANSI) para el diseño y la instalación de sistemas de cableado estructurado en edificios comerciales. Publicada originalmente en 2001, la serie 568-B proporciona directrices detalladas para la configuración de cables de par trenzado y fibra óptica, utilizados ampliamente en redes de área local (LAN). Esta norma incluye especificaciones para la disposición de cables en conectores RJ45, asegurando compatibilidad entre dispositivos y un rendimiento confiable en redes de datos. La serie 568-B también se subdivide en secciones como TIA-568-B.1, B.2 y B.3, las cuales abordan diferentes aspectos del cableado estructurado, como la infraestructura general, los requisitos para cables de cobre y fibra óptica, respectivamente. Esta serie ha sido clave para la estandarización y la interoperabilidad en redes de telecomunicaciones, y sigue siendo relevante en muchos entornos empresariales y tecnológicos.

2.22.- Aplicación de las Capas del Modelo OSI y TCP/IP

Ambos modelos son fundamentales para entender y estructurar las funciones del proyecto. El modelo OSI sirve como marco teórico para segmentar y optimizar funciones específicas de la red, mientras que el modelo TCP/IP proporciona un enfoque práctico para implementar dichas funciones en un entorno real.

2.22.1.- Modelo OSI

Capa Física: Diseño e implementación de la infraestructura física, como el cableado estructurado bajo el estándar ANSI/TIA 568-B y los medios de transmisión. Elección de dispositivos como switches y routers para la conectividad física.

Capa de Enlace de Datos: Configuración de switchs y gestión de direcciones MAC para una red local eficiente.

Capa de Red: Configuración de direcciones IP y enrutamiento dentro del data center y hacia redes externas. Implementación de protocolos como ICMP para supervisión y diagnóstico de la red.

Capa de Transporte: Uso de protocolos como TCP para asegurar la transmisión confiable de datos entre el servidor de monitoreo y los dispositivos supervisados. Configuración de puertos y control de flujo para las comunicaciones.

Capa de Aplicación

Implementación de aplicaciones como Observium, que utiliza protocolos de monitoreo como SNMP y HTTP para recopilar y presentar datos en tiempo real.

2.22.2.- Modelo TCP/IP

Capa de Acceso a la Red: Manejo de interfaces físicas y tecnologías de transmisión, como Ethernet, para conectar equipos del data center.

Capa de Internet: Asignación de direcciones IP para dispositivos y configuraciones de subredes. Uso de enrutadores para gestionar el tráfico entre redes y garantizar el acceso remoto.

Capa de Transporte: Configuración de protocolos como TCP para comunicación confiable y UDP para transmisiones rápidas, si aplica en el monitoreo.

Capa de Aplicación: Observium para el monitoreo operan en esta capa, utilizando protocolos como HTTP, SNMP, y SSH para interactuar con la red.

2.23.- Virtual Box

VirtualBox es una herramienta de virtualización de código abierto desarrollada por Oracle que permite a los usuarios ejecutar múltiples sistemas operativos simultáneamente en una misma máquina física. Con VirtualBox, es posible crear y gestionar máquinas virtuales que operan de manera independiente, permitiendo, por ejemplo, correr Linux en un entorno Windows o viceversa. Esta plataforma es ampliamente utilizada en entornos de prueba y desarrollo, ya que facilita la experimentación sin riesgo para el sistema operativo principal, y soporta una amplia gama de sistemas operativos invitados, como Windows, macOS, Linux y Solaris.

VirtualBox ofrece varias características avanzadas, como la posibilidad de configurar redes virtuales, compartir carpetas entre el sistema anfitrión e invitado, y la opción de realizar "snapshots" (instantáneas) de las máquinas virtuales, permitiendo al usuario restaurar el sistema a un estado previo en caso de fallos. Además, cuenta con una interfaz intuitiva y opciones de configuración flexibles, lo que lo convierte en una herramienta popular tanto en entornos educativos como profesionales.

Capitulo III

COMPONENTE I

Diseñar un Data Center conforme a la Norma ISO/IEC 22237.

3.- Componente I: Diseñar un Data Center conforme a la Norma ISO/IEC 22237.

3.1.- Metodología de desarrollo del proyecto top-Down

La metodología de desarrollo Top-Down aplicada al diseño de un Data Center y configuración de servidor de monitoreo en tiempo real para la Fiscalía Departamental de Tarija, se fundamenta en un enfoque sistemático que comienza con una visión holística de los requerimientos y objetivos del proyecto, para luego descomponerlos en componentes más pequeños y manejables. Este enfoque permite una planificación estructurada y una implementación eficiente, asegurando la coherencia y la integración de cada fase del proyecto con la normativa ISO/IEC 22237. Además, facilita la identificación temprana de posibles riesgos y la adaptación ágil a los cambios, garantizando la entrega de una solución robusta y optimizada que cumpla con las necesidades tecnológicas de la Fiscalía Departamental de Tarija.

Las etapas a realizar de la metodología en el proyecto son:

- Fase 1: Análisis de Requerimientos
- Fase 2: Desarrollo del diseño lógico
- Fase 3: Desarrollo de diseño Físico
- Fase 4: Pruebas de Diseño y documentación

3.2.- Fase 1: Análisis de Requerimientos

3.2.1.- Analizar metas del negocio

3.2.1.1.- Misión

Es una institución constitucional, encargada de defender la legalidad y los intereses generales de la sociedad boliviana, con transparencia y autonomía, ejerciendo la acción penal pública, con oportunidad, objetividad y los demás principios que rigen la labor fiscal, con perspectiva de género y justicia restaurativa, protegiendo a la víctima, en resguardo de las garantías constitucionales y el respeto firme de los derechos humanos.

3.2.1.2.- Visión

Ser una institución sólida, con credibilidad y altos estándares de transparencia, reconocida por su efectividad y capacidad de respuesta técnico - científica, en el ejercicio de la acción penal publica, con calidad y modernidad tecnológica, con recursos humanos altamente calificados, responsables y comprometidos, siendo el referente del sistema de justicia penal, bajo el enfoque de una gestión fiscal por resultados, al servicio de la sociedad.

3.2.1.3.- Organigrama de la Institución

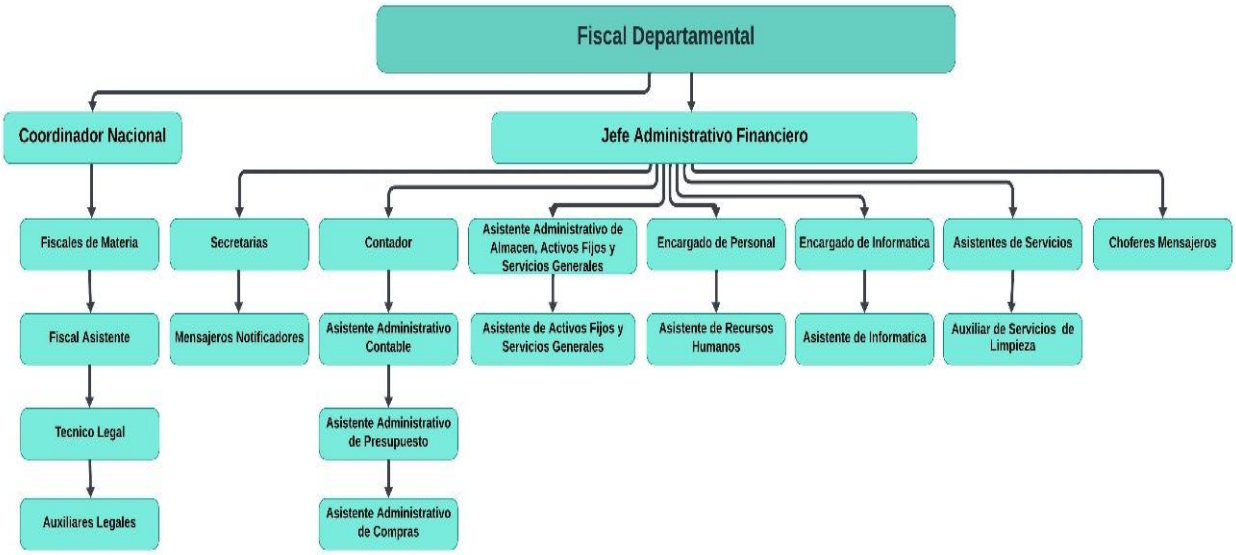


Figura 20. *Organigrama de la institución.*

3.2.1.4.- Casos de Uso de Negocio

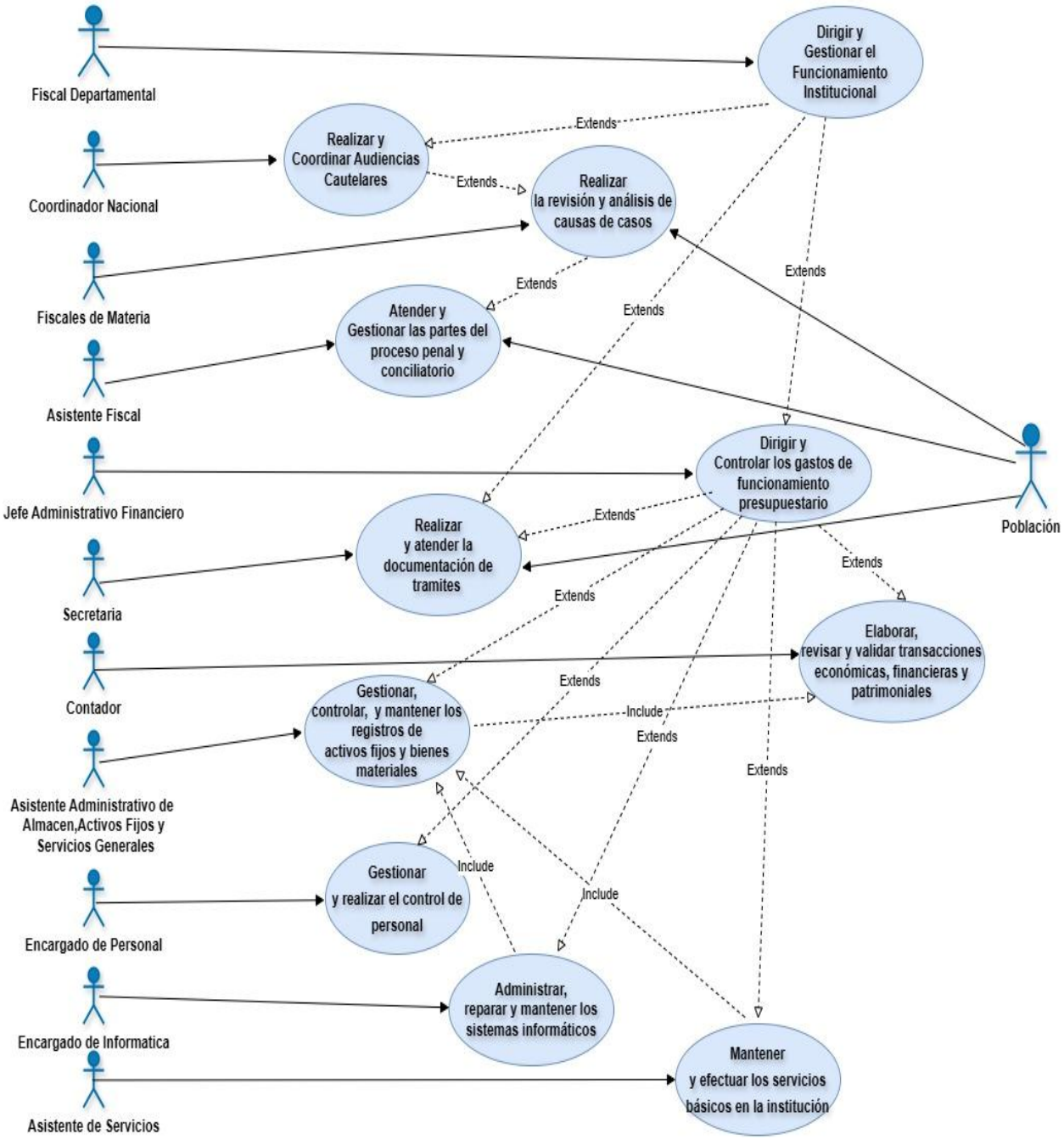


Figura 21. *Casos de uso de Negocio*

3.2.1.5.- Descripción de los casos de uso

3.2.1.5.1.- Casos de Uso de Negocio de la Fiscalía Departamental de Tarija

Caso de Uso	Dirigir y Gestionar el Funcionamiento Institucional
Actor	Fiscal Departamental
Descripción	Realizar el control y revisión del trabajo de las y los Fiscales y personal dependiente de la Fiscalía Departamental.

Caso de Uso	Realizar y Coordinar Audiencias Cautelares
Actor	Coordinador Nacional
Descripción	Coordinar el trabajo con los Fiscales de Materia, Asistentes Legales y Auxiliares Legales, procurando la eficacia y efectividad del trámite de los procesos penales.

Caso de Uso	Realizar la revisión y análisis de causas.
Actor	Fiscales de Materia
Descripción	Ejercer la acción penal pública, según las atribuciones que la Constitución Política del Estado y las leyes que le otorgan al Ministerio Público, asegurando su intervención en las diferentes etapas del proceso penal, desarrollando su trabajo de manera efectiva, para encontrar la verdad histórica y material de los hechos, así como dar con los responsables del delito.

Caso de Uso	Atender y Gestionar las partes del proceso penal y conciliatorio
Actor	Asistente Fiscal
Descripción	Brindar apoyo a las y los fiscales en el cumplimiento de sus funciones, en el avance de los procesos penales y el control de plazos, realizando la recepción, ingreso al sistema, así como, la recepción, registro y distribución de memoriales y otros a la unidad que corresponde.

Caso de Uso	Dirigir y Controlar los gastos de funcionamiento presupuestario
Actor	Jefe Administrativo Financiero
Descripción	Administrar eficaz y eficientemente los recursos humanos, financieros, bienes muebles, inmuebles, patrimonio y materiales de la Fiscalía Departamental, mediante la planificación, consolidación y ejecución de la gestión administrativa y financiera, con el propósito de garantizar los recursos materiales y financieros necesarios para el buen desempeño de la gestión.

Caso de Uso	Realizar y Atender la documentación de tramites
Actor	Secretarias
Descripción	Recepcionar la documentación que ingresa a la unidad, notificar a las y los servidores, elaborar comisiones para viajes, atender la central telefónica, elaborar notas e informar al público en general.

Caso de Uso	Elaborar, revisar y validar transacciones económicas, financieras y patrimoniales
Actor	Contador
Descripción	Realizar el registro ordenado de los ingresos y gastos de la entidad, en el marco del Sistema de Contabilidad Integrada y principios de contabilidad generalmente aceptados, proporcionando información oportuna, confiable y útil para la toma de decisiones.

Caso de Uso	Gestionar, controlar, y mantener los registros de activos fijos y bienes materiales
Actor	Asistente Administrativo de Almacenes, Activos Fijos y Servicios Generales
Descripción	Organizar, clasificar y custodiar los activos fijos, así como la provisión oportuna de servicios básicos.

	Registrar y participar en la recepción y entrega de bienes y materiales adquiridos, velando por la custodia de bienes e infraestructura y supervisión de la limpieza de ambientes de la Fiscalía Departamental.

Caso de Uso	Gestionar y realizar el control del personal
Actor	Encargado de Personal
Descripción	Realizar el control permanente de las y los servidores, velando por el cumplimiento estricto del Reglamento Interno de Control de personal, en cuanto a derechos, obligaciones, sanciones, vacaciones y control de asistencia de las y los servidores dependientes de la Fiscalía Departamental.

Caso de Uso	Administrar, reparar y mantener los sistemas informáticos
Actor	Encargado de Informática
Descripción	Realizar la administración de redes de comunicación, dar sostenibilidad al hardware y software a través del mantenimiento preventivo y correctivo a los equipos de computación, precautelando la seguridad de los mismos, a través de la actualización periódica del software; así mismo, coordinando constantemente con la Unidad de Informática de la fiscalía general del Estado.

Caso de Uso	Mantener y efectuar los servicios básicos en la institución
Actor	Asistente de Servicios
Descripción	Realizar y verificar la limpieza de las diferentes oficinas, coordinar la dotación de refrigerios para reuniones y otros eventos oficiales; así como, el apoyo efectivo en las diferentes actividades encomendadas.

Tabla 6. *Descripción de Casos de Uso de Negocio*

3.2.2.- Analizar metas técnicas

Este proyecto se iniciará con proveer la información necesaria para realizar el análisis inicial del estado de la red, esto incluirá la estructura de la red de datos, es decir, como están ubicados cada uno de los equipos en las diferentes áreas de la institución. Se procederá a analizar el diseño inicial de la red, posteriormente se empezará a obtener todos los requerimientos y restricciones de la red y determinar soluciones viables.

La Fiscalía Departamental de Tarija cuenta con un total 59 trabajadores los que se distribuyen de la siguiente manera:

Espacios	**Computadoras de Escritorio**	**N de Scanner**	**N de Impresoras**
Planta Baja	13	10	5
Primer Planta	20	18	10
Segunda Planta	7	5	3
Tercer Planta	12	11	8
Cuarta Planta	7	7	5

Tabla 7. *Número de equipos para trabajadores en la Institución*

3.2.2.1.- Analizar red e infraestructura tecnológica

Los equipos y red existente en la Fiscalía cuentan con los siguientes planos de distribución:

3.2.2.1.1.- Plano de la Infraestructura General de Planta Baja

Figura 22. *Plano de Planta baja*

3.2.2.1.2.- Plano de la Infraestructura General de Primer Planta

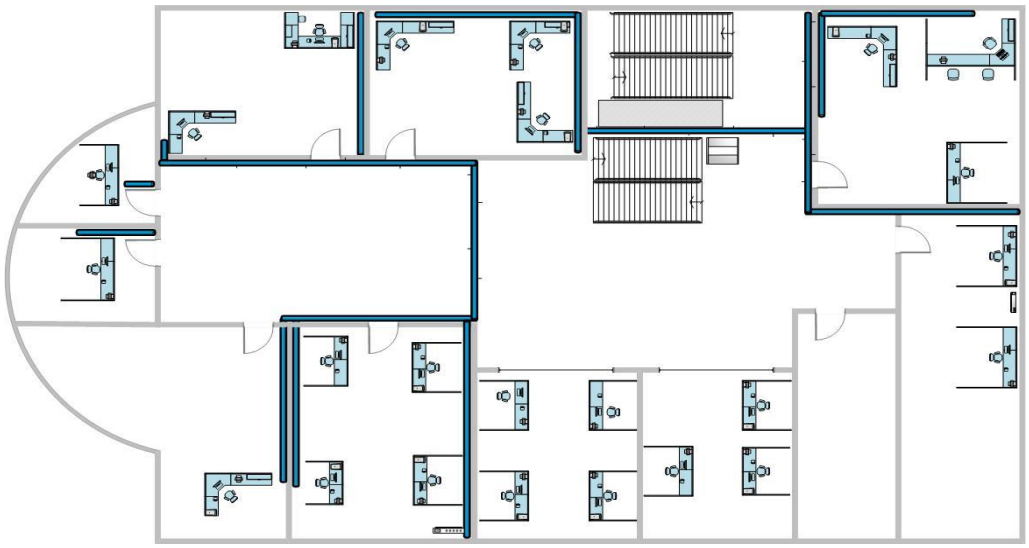


Figura 23. *Plano de Primer Planta*

3.2.2.1.3.- Plano de la Infraestructura General de Segunda Planta

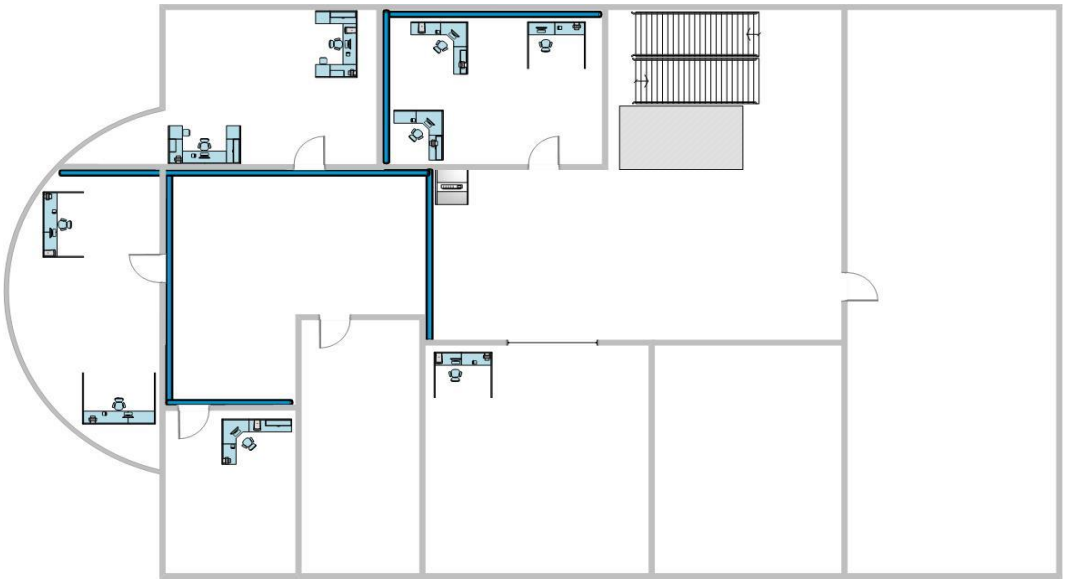


Figura 24. *Plano de Segunda Planta*

3.2.2.1.4.- Plano de la Infraestructura General de Tercer Planta

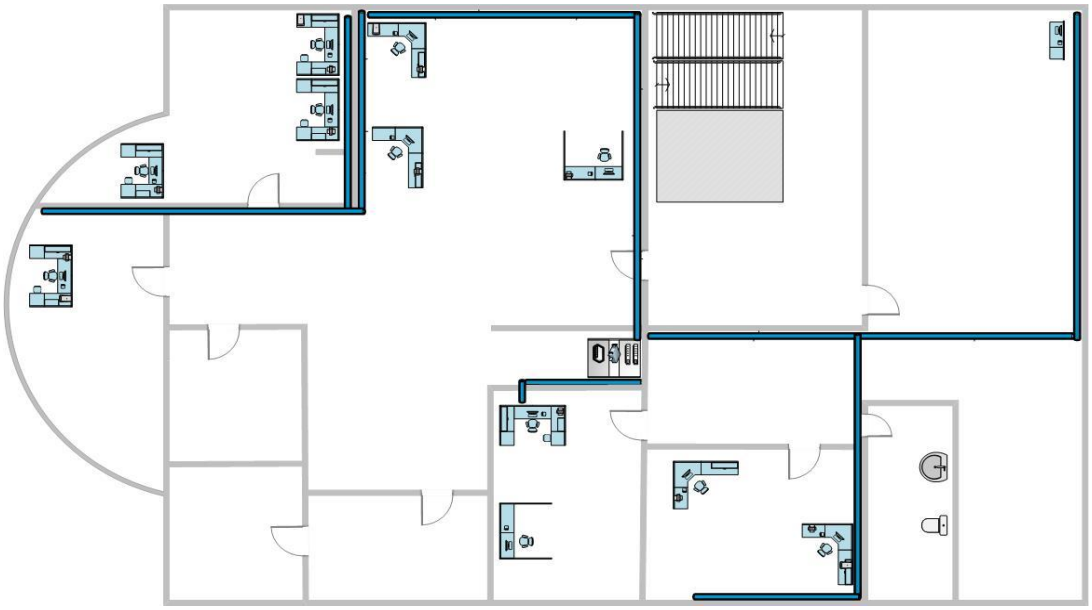


Figura 25. *Plano de Tercer Planta*

3.2.2.1.5.- Plano de la Infraestructura General de Cuarta Planta

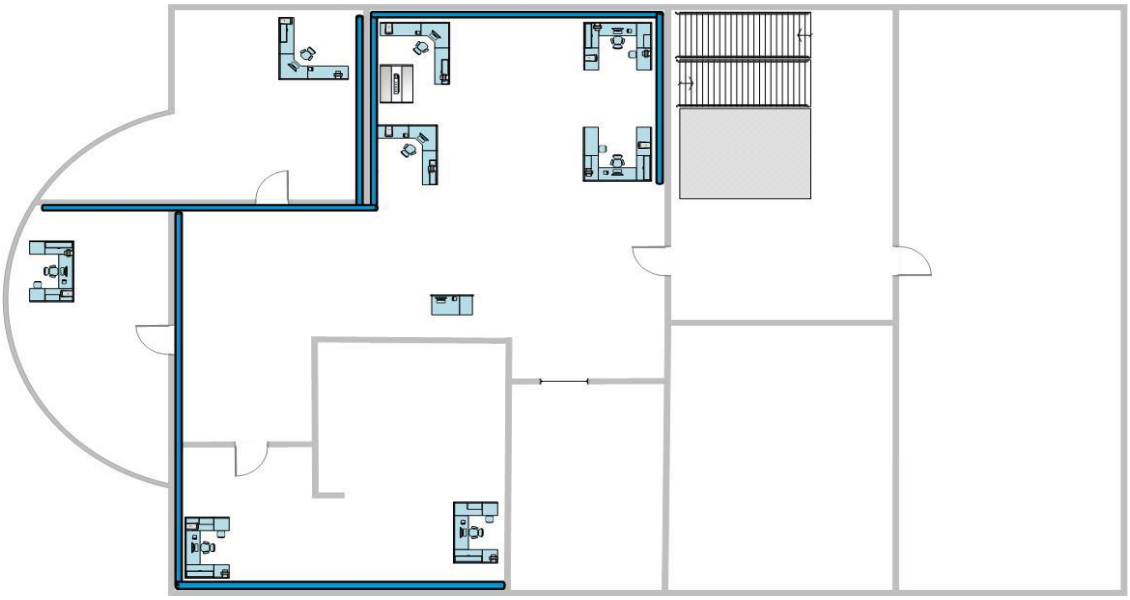


Figura 26. *Plano de Cuarta Planta*

3.2.2.1.6.- Explicación de los planos

- En planta baja se encuentran 13 computadoras de escritorio y 10 scanner donde se subdividen para los trabajadores para Ventanillas, Fiscales, Denuncias Verbales, Asistente de Fiscales y Médicos Forenses.
- En Primer Planta se encuentran 20 computadoras de escritorio y 18 scanner donde se subdividen para los trabajadores de Investigador Sexuales, Litigación, Asist. de Litigación y Genero, Trabajadores Sociales y Psicólogos.
- En Segunda Planta se encuentran 7 computadoras de escritorio y 5 scanner donde se subdividen para los trabajadores en Litigación, Régimen y Psicólogo.
- En Tercer Planta se encuentran 12 computadoras de escritorio y 11 scanner donde se subdividen para los trabajadores en Informática, Notificadores y Administración.
- En Cuarta Planta se encuentran 7 computadoras de escritorio y 7 scanner donde se subdividen para los trabajadores en Distrito, secretaria, Coordinadora y Fiscal Departamental.

3.2.3.- Analizar tráfico de red existente

El tráfico de la red es la para el uso del sistema donde se maneja la documentación de casos de la Fiscalía donde se trabaja con los demás provincias y nivel nacional con los demás departamentos de Bolivia. Se utiliza diferentes tipos de aplicaciones de red y se maneja de manera virtual casos dependientes de donde sucedan estos. Se maneja información en nube y diferentes accesos a páginas del sistema donde se registra todo tipo de actividad referentes a los casos que se presentan de manera continua y donde se hace un largo seguimiento en cada caso por ende la información es muy requerida en disposición de cada trabajador de la fiscalía.

Cuentan con dos tipos de suministro de internet por fibra óptica de las empresas Tigo y Entel para suministrar las áreas de los trabajadores y de las personas generales de la población.

Figura 27. *Análisis de Trafico de Red Existente*

3.3.- Fase 2: Desarrollo de diseño lógico e infraestructura actual

3.3.1.- Diseño de topología de Red

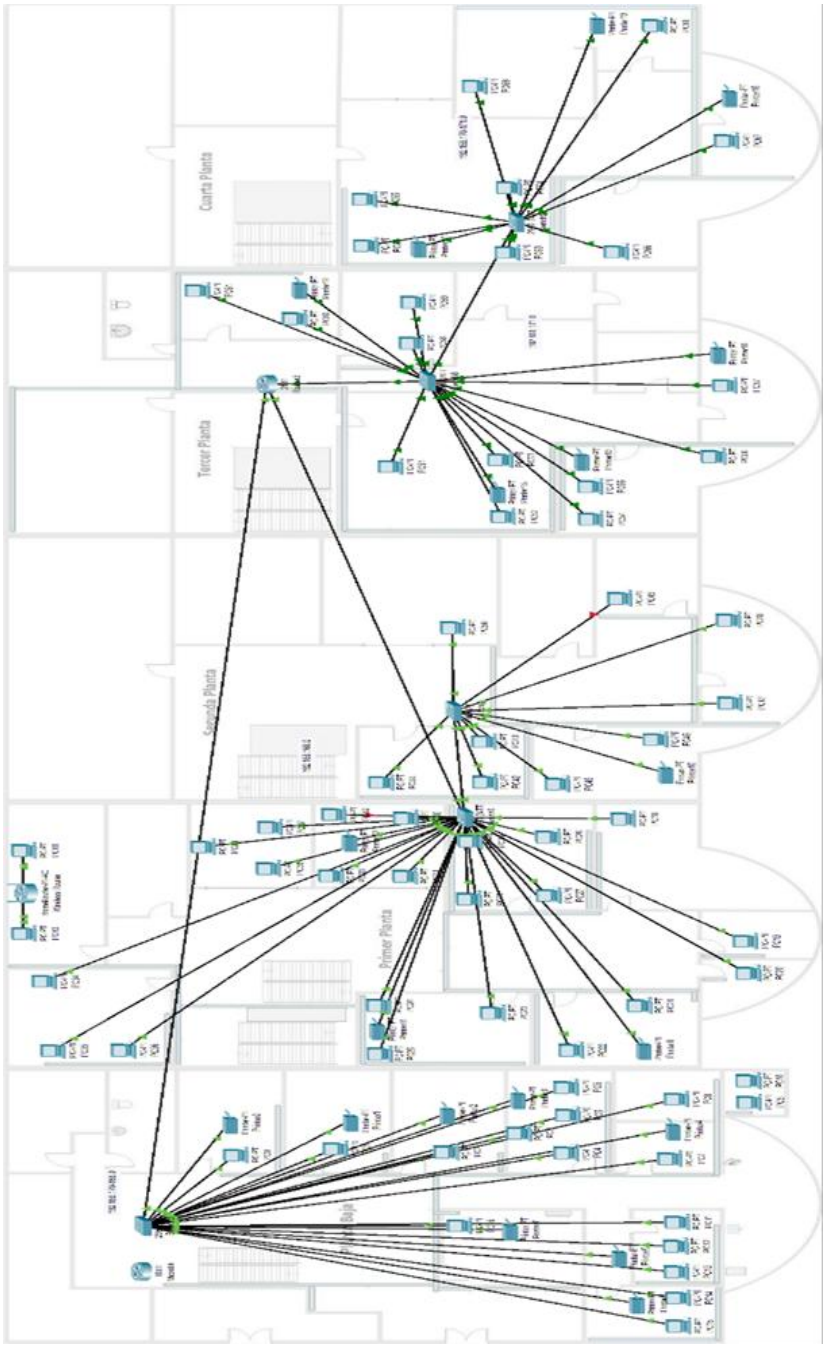


Figura 28. *Topología de red de la Institución*

3.3.2.- Equipos de la infraestructura tecnológica

3.3.2.1.- Planta Baja

Se tiene como equipos de red:

Tipo	Marca	Modelo	Cantidad
Rack	dLux	GAB-24U-SE	1
Patch Panel	CAT. 5E de 24P	PUERTOS 19″ 1U, DLUX	2
Switch	alhua	16-Port POE	1
FortiSwitch	Fortinet	448D-POE	1
Microtik	Router Board	RB201 1UiA5-RM	1
Conexión de Cable	UTP	Cat 5e	-
Disco duro UDP	alhua	Vision HD CCTV Security	1
Distribuidor de Energía	dLux	PDU	1
Monitor	DELL	Monitor Dell 24 Lcd	1
Bandejas de Rack	dLUX	-	2

Tabla 8. *Equipos de Red Planta Baja*

3.3.2.2.- Primera planta

Tipo	Marca	Modelo	Cantidad
Mini Rack de Pared	dLux	9U	1
Switch	TP-link	24-Port TL-SG3428	1
Conexión de Cable	UTP	Cat 5e	-

Tabla 9. *Equipos de Red Primer Planta*

3.3.2.3Segunda Planta

Tipo	Marca	Modelo	Cantidad
Mini Rack de Pared	dLux	9U	1
Switch	TP-link	24-Port TL-SG3428	1
Conexión de Cable	UTP	Cat 5e	-

Tabla 10. *Equipos de Red Segunda Planta*

3.3.2.4.- Tercer Planta

Tipo	Marca	Modelo	Cantidad
Rack de Pared	-	12U	1
Patch Panel	dLux	54 puertos	1
Router	ZTE	ZXHN F660	
Cortafuegos	Fortinet	FortiGate 90G	1
ONT	GPON/EPON 1	PON/EPON 1 RJ45, 1Gb.SC/PC	1
Central IP	Grandstream	UCM6304	1
Conexión de Cable	UTP	Cat 5e	-
Distribuidor de Energia	dLux	PDU	2
Bandejas de Rack	dLUX	-	2
Bandeja de Separacion	dLux	24-Sep.	1
Aire Acondicionado	TAKA	-Sin funcionar	1

Tabla 11. *Equipos de Red Tercer Planta*

3.3.2.5.- Cuarta Planta

Tipo	Marca	Modelo	Cantidad
Mini Rack de Pared	dLux	9U	1
Switch	TP-link	24-Port TL-SG3428	1
Conexión de Cable	UTP	Cat 5e	-
Aire Acondicionado	TCL	TCL 12000 Btu	1

Tabla 12. *Equipos de Red Cuarta Planta*

3.3.3.- Direccionamiento IP Actual

3.3.3.1.- Planta Baja

División	Atención	Cargo	Dirección IP	Mascara	Gateway
PLATAFORMA	VENTANILLA 1	ASISTENTE	192.168.170.11	255.255.255.0	192.168.170.1
PLATAFORMA	SCAN VENT 1	ASISTENTE	192.168.170.12	255.255.225.0	192.168.170.1
PLATAFORMA	VENTANILLA 2	ASISTENTE	192.168.170.13	255.255.255.0	192.168.170.1
PLATAFORMA	SCAN VENT 2	ASISTENTE	192.168.170.14	255.255.255.0	192.168.170.1
PLATAFORMA	VENTANILLA 3	ASISTENTE	192.168.170.15	255.255.255.0	192.168.170.1
PLATAFORMA	SCAN VENT 3	ASISTENTE	192.168.170.16	255.255.255.0	192.168.170.1
PLATAFORMA	DENUNCIA VERB.	ASISTENTE	192.168.170.17	255.255.225.0	192.168.170.1

PLATAFORMA	SCAN DEN VER.	ASISTENTE	192.168.170.18	255.255.255.0	192.168.170.1
ANALISIS	FISCAL ANAL.	FISCAL	192.168.168.11	255.255.255.0	192.168.168.1
ANALISIS	SCAN ANALISTA	FISCAL	192.168.168.12	255.255.255.0	192.168.168.1
ANALISIS	ASIST. ANALISIS	FISCAL	192.168.168.13	255.255.255.0	192.168.168.1
URI-UST	FISCAL URI	FISCAL	192.168.168.14	255.255.225.0	192.168.168.1
URI-UST	SCAN URI	FISCAL	192.168.168.15	255.255.255.0	192.168.168.1
URI-UST	ASIST. URI	FISCAL	192.168.168.16	255.255.255.0	192.168.168.1
IDIF	MED. FORENSE 1	FISCAL	192.168.168.17	255.255.255.0	192.168.168.1
IDIF	SCAN MED. FOR. 1	FISCAL	192.168.168.18	255.255.255.0	192.168.168.1
IDIF	MED. FORENSE 2	FISCAL	192.168.168.19	255.255.225.0	192.168.168.1
IDIF	SCAN MED. FOR. 2	FISCAL	192.168.168.20	255.255.255.0	192.168.168.1
IDIF	MED. FORENSE 3	FISCAL	192.168.168.21	255.255.255.0	192.168.168.1
IDIF	SCAN MED. FOR. 3	FISCAL	192.168.168.22	255.255.255.0	192.168.168.1
UC	CONCILIACION 1	ASISTENTE	192.168.170.19	255.255.255.0	192.168.168.1
UC	SCANCONCI.1	ASISTENTE	192.168.170.20	255.255.225.0	192.168.168.1

Tabla 13. *Direccionamiento IP de Planta Baja*

3.3.3.2.- Primer Planta

División	**Atención**	**Cargo**	**Dirección IP**	**Mascara**	**Gateway**
GENERO	GABRIELA SORUCO	FISCAL	192.168.168.29	255.255.255.0	192.168.168.1
GENERO	SCAN GABRIELA S.	FISCAL	192.168.168.30	255.255.225.0	192.168.168.1
GENERO	LORENA F.	FISCAL	192.168.168.31	255.255.255.0	192.168.168.1
GENERO	SCAN LORENA	FISCAL	192.168.168.32	255.255.255.0	192.168.168.1
GENERO	MARIA PARRA	FISCAL	192.168.168.33	255.255.255.0	192.168.168.1
GENERO	SCAN MARITA	FISCAL	192.168.168.34	255.255.255.0	192.168.168.1
GENERO	NICKOL	FISCAL	192.168.168.35	255.255.225.0	192.168.170.1
GENERO	SCAN NICKOL	FISCAL	192.168.168.36	255.255.255.0	192.168.168.1
UC	CONCILIACION 2	ASISTENTE	192.168.170.33	255.255.255.0	192.168.168.1
UC	SCAN-CONCI. 2	ASISTENTE	192.168.170.34	255.255.255.0	192.168.168.1
UPAVT	TRAB SOCIAL	FISCAL	192.168.168.37	255.255.255.0	192.168.168.1
UPAVT	SCAN TRAB SOCIAL	FISCAL	192.168.168.38	255.255.225.0	192.168.168.1
UPAVT	PSICOLOGO	FISCAL	192.168.168.39	255.255.255.0	192.168.168.1
UPAVT	SCAN PSICOLOGO	FISCAL	192.168.168.40	255.255.255.0	192.168.168.1

LITIGACIÓN	ALVARO ARCE	FISCAL	192.168.168.41	255.255.255.0	192.168.168.1
LITIGACIÓN	SCAN ALVARO A.	FISCAL	192.168.168.42	255.255.255.0	192.168.168.1
LITIGACIÓN	GABRIEL ALARCON	FISCAL	192.168.168.43	255.255.225.0	192.168.168.1
LITIGACIÓN	SCAN GABRIEL A	FISCAL	192.168.168.44	255.255.255.0	192.168.168.1
LITIGACIÓN	JHOVANA SALINAS	FISCAL	192.168.168.45	255.255.255.0	192.168.168.1
LITIGACIÓN	SCAN JHOVANA	FISCAL	192.168.168.46	255.255.255.0	192.168.168.1

Tabla 14. *Direccionamiento IP de Primer Planta*

3.3.3.3.- Segunda Planta

División	**Atención**	**Cargo**	**Dirección IP**	**Mascara**	**Gateway**
LITIGACIÓN	ALI MARTINEZ	FISCAL	192.168.168.47	255.255.255.0	192.168.168.1
LITIGACIÓN	SCAN ALI MARTINEZ	FISCAL	192.168.168.48	255.255.255.0	192.168.168.1
LITIGACIÓN	GRACIELA COPAS	FISCAL	192.168.168.49	255.255.255.0	192.168.168.1
LITIGACIÓN	SCAN GRACIELA	FISCAL	192.168.168.50	255.255.225.0	192.168.168.1
LITIGACIÓN	JEANNETHE R.	FISCAL	192.168.168.51	255.255.255.0	192.168.168.1
LITIGACIÓN	SCAN JEANNETHE	FISCAL	192.168.168.52	255.255.255.0	192.168.168.1
RÉGIMEN	JULIA	FISCAL	192.168.168.53	255.255.255.0	192.168.168.1
RÉGIMEN	ASIST. JULIA	FISCAL	192.168.168.54	255.255.255.0	192.168.168.1
RÉGIMEN	SCAN JULIA	FISCAL	192.168.168.55	255.255.225.0	192.168.168.1
IDIF	PSICOLOGO	FISCAL	192.168.168.56	255.255.255.0	192.168.168.1
IDIF	SCAN PSICOLOGO	FISCAL	192.168.168.57	255.255.255.0	192.168.168.1

Tabla 15. *Direccionamiento IP de Segunda Planta*

3.3.3.4.- Tercer Planta

División	**Atención**	**Cargo**	**Dirección IP**	**Mascara**	**Gateway**
PROYECTISMO	LUIS SILVERIO	FISCAL	192.168.168.58	255.255.255.0	192.168.168.1
PROYECTISMO	SCAN SILVERIO	FISCAL	192.168.168.59	255.255.225.0	192.168.168.1
PROYECTISMO	ASIST. SILVERIO	FISCAL	192.168.168.60	255.255.255.0	192.168.168.1
INFORMÁTICA	ROLANDO G	SISTEMAS	192.168.171.4	255.255.255.0	192.168.171.1
INFORMÁTICA	SCAN ROLO G	SISTEMAS	192.168.171.5	255.255.255.0	192.168.171.1
INFORMÁTICA	LUIS BURGOS	SISTEMAS	192.168.171.6	255.255.255.0	192.168.171.1
INFORMÁTICA	SCAN LUIS B.	SISTEMAS	192.168.171.7	255.255.225.0	192.168.171.1
INFORMÁTICA	MANT.	SISTEMAS	192.168.171.8	255.255.255.0	192.168.171.1

INFORMÁTICA	SCAN MANTE.	SISTEMAS	192.168.171.9	255.255.255.0	192.168.171.1
INFORMÁTICA	DANIEL G.	SISTEMAS	192.168.171.10	255.255.255.0	192.168.171.1
INFORMÁTICA	SCAN DANIEL	SISTEMAS	192.168.171.11	255.255.255.0	192.168.171.1
NOTIFICADORES	MARCO RICALDI	SISTEMAS	192.168.171.24	255.255.225.0	192.168.171.1
NOTIFICADORES	SCAN MARCO	SISTEMAS	192.168.171.13	255.255.255.0	192.168.171.1
NOTIFICADORES	ARTURO M.	SISTEMAS	192.168.171.14	255.255.255.0	192.168.171.1
NOTIFICADORES	SCAN ARTURO	SISTEMAS	192.168.171.15	255.255.255.0	192.168.171.1
ADMINISTRACIÓN	ALEX G.	SISTEMAS	192.168.171.16	255.255.255.0	192.168.171.1
ADMINISTRACIÓN	SCAN ALEX	SISTEMAS	192.168.171.17	255.255.225.0	192.168.171.1
ADMINISTRACIÓN	VALERIA	SISTEMAS	192.168.171.18	255.255.255.0	192.168.171.1
ADMINISTRACIÓN	SCAN VALERIA	SISTEMAS	192.168.171.19	255.255.255.0	192.168.171.1
ADMINISTRACIÓN	CONTABILIDAD	SISTEMAS	192.168.171.20	255.255.255.0	192.168.171.1
ADMINISTRACIÓN	SCAN CONTA.	SISTEMAS	192.168.171.21	255.255.255.0	192.168.171.1
ADMINISTRACIÓN	JEFA ADM	SISTEMAS	192.168.171.22	255.255.255.0	192.168.171.1
ADMINISTRACIÓN	SCAN JEFA ADM	SISTEMAS	192.168.171.23	255.255.255.0	192.168.171.1

Tabla 16. *Direccionamiento IP de Tercer Planta*

3.3.3.5.- Cuarta Planta

División	**Atención**	**Cargo**	**Dirección IP**	**Mascara**	**Gateway**
DISTRITO	WILLIAMS	ASISTENTE	192.168.170.35	255.255.255.0	192.168.170.1
DISTRITO	SCAN WILLIAMS	ASISTENTE	192.168.170.36	255.255.255.0	192.168.170.1
DISTRITO	MARY	ASISTENTE	192.168.170.37	255.255.255.0	192.168.170.1
DISTRITO	SCAN MARY	ASISTENTE	192.168.170.38	255.255.225.0	192.168.170.1
DISTRITO	ANTONIO	ASISTENTE	192.168.170.39	255.255.255.0	192.168.170.1
DISTRITO	SCAN ANTONIO	ASISTENTE	192.168.170.40	255.255.255.0	192.168.170.1
DISTRITO	PAOLA	ASISTENTE	192.168.170.41	255.255.255.0	192.168.170.1
DISTRITO	SCAN PAOLA	ASISTENTE	192.168.170.42	255.255.255.0	192.168.170.1
SECRETARIA	MAIDA JIJENA	SISTEMAS	192.168.171.24	255.255.225.0	192.168.171.1
SECRETARIA	SCAN MAIDA JIJENA	SISTEMAS	192.168.171.25	255.255.255.0	192.168.171.1
COORDINADORA	CANDACE FLORES	SISTEMAS	192.168.171.26	255.255.255.0	192.168.171.1
COORDINADORA	SCAN CANDACE	SISTEMAS	192.168.171.27	255.255.225.0	192.168.171.1
FISCAL DEPTAL	SANDRA GUTIERREZ	SISTEMAS	192.168.171.28	255.255.255.0	192.168.171.1
FISCAL DEPTAL	SCAN SANDRA	SISTEMAS	192.168.171.29	255.255.255.0	192.168.171.1

Tabla 17. *Direccionamiento IP de Cuarta Planta*

3.3.4.- Identificación de las necesidades y requerimientos

Según los datos recolectados se muestras la tabla de problemas en la infraestructura actual.

Problemas	**Descripción**
Seguridad en equipamiento principal de red	No poseen con un lugar adecuado para los racks, cableado y dispositivos de red permitiendo vulnerabilidades a sus equipos.
Rendimiento de Red y dispositivos de red.	Tiempos de espera por la lentitud de la red, no cuentan con información general de cómo está funcionando el equipamiento de red y como afecta al personal de la institución
Disponibilidad al manejo de la red	No tienen disponibilidad para el mantenimiento de su red debido a la mala organización de los equipos y del cableado.
Fallos en dispositivos sin mantenimiento (PC, scanners e impresoras).	Los dispositivos poseen fallos y tiempos de espera largos para el cambio de piezas.
Rendimiento lento de dispositivos	Dispositivos con espera de mantenimiento y cambios de hardware y actualizaciones de software (Linux) por el personal encargado.
Cableado con el estándar ANSI/TIAEIA 568B	Poseen mala organización en el cableado y no cumplen a cabalidad con el estándar.

3.3.4.1.- Objetivos de la Fiscalía Departamental de Tarija

En la tabla se puede observar los objetivos planteados para mejorar la calidad de servicio, además de optimizar los costos a futuro. En la tabla se explica de donde se obtendrá la información con un pertinente comentario al respecto.

Objetivos Propuestos	**Obtención de información**	**Comentarios**
Mejorar el servicio la infraestructura tecnológica de la institución.	Encargado de Informática	Datos técnicos, información, distribución y equipamiento.

Añadir nuevos servicios para información de equipamiento.	Servicios Actuales	Lista de futuros servicios
Incrementar Seguridad en la infraestructura tecnológica.	Equipamiento de red	Implementación de seguridad física.
Reducir costos	Encargado de Informática	Los gastos se reducirían con la facilidad de mantenimiento preventivo y correctivo.

Tabla 18. *Objetivos de Mejora de Calidad de Servicio*

3.3.4.2.- Limitaciones de la Fiscalía Departamental de Tarija

En la tabla se indica las posibles limitaciones producidas por diferentes tipos de causas.

Limitaciones de la Institución	**Obtención de Información**	**Comentarios**
Políticas	Preferentemente un único fabricante en equipamiento especial.	Marcas conocidas y avaladas.
Personal	Ingenieros certificados para una mejor distribución de energía.	Planes para contratar nuevos ingenieros especializados en el área.
Presupuesto	Departamento Financiero	Presupuesto para aprobación.

Tabla 19. *Limitaciones para los Servicios de Calidad*

3.3.4.3.- Objetivos para el diseño y configuración

En la tabla se indica los objetivos técnicos tomados en cuenta para la Fiscalía Departamental de Tarija, viendo la importancia de cada uno de ellos.

Objetivos Técnicos	Impor-tancia	Comentarios
Rendimiento	20	Importancia de la red y mantenimiento del equipamiento para toda la institución.
Disponibilidad	25	Debería ser el 99.99%
Gestión	5	
Seguridad	20	Seguridad para el equipamiento y la mejora continua.
Adaptabilidad	5	
Escalabilidad	25	La escalabilidad es importante por el servicio que brinda.
Total	**100**	

Tabla 20. *Objetivos para el diseño y configuracion del servidor*

3.3.4.4.- Analizar los requisitos del edificio para el diseño

3.3.4.4.1.- Ubicación del Edificio

La ubicación de la infraestructura se encuentra en la Avenida O'Connor esquina Av. Víctor Paz Estensoro.

3.3.4.4.2.- Descripción del edificio

El edificio presenta 5 plantas, de las cuales solo se utilizan 4 plantas donde se cuenta con ambientes de atención que se dividen en, plataforma, médicos forenses, conciliadores, administrativos, fiscales, informáticos, secretaria, psicólogos, litigadores, conciliadores, pasantes.

3.3.4.4.3.- Descripción física por pisos

La fiscalía Departamental de Tarija posee un diseño simple de estructura física y lógica de su red de datos. Su cableado estructurado fue implementado sin previo estudio de escalabilidad y planificación. Los puntos de red aumentados simplemente fueron creados tras las necesidades urgentes que debían solucionar los encargados del Área Informática.

La estructura física según las medidas realizadas manualmente de los ambientes de la Fiscalía Departamental de Tarija presenta las siguientes características:

- La altura 3.8 m.

- Todos los pisos de hormigón compacto.
- Las paredes de ladrillo cerámico 6 huecos 12*18 cm.

3.4.- Fase 3: Desarrollo de diseño Fisico del Data Center

3.4.1.- Data Center

Un Data Center es de gran importancia ya que en ella se encuentra alojados toda la información y servicios disponibles para el correcto desarrollo de la institución. Por esta razón es primordial tener un adecuado manejo, para que los equipos siempre estén en un correcto estado así también un monitoreo constante para que los servicios se encuentren disponibles 24/7 (24 horas 7 días a la semana).

El principal objetivo de un diseño de Data Center es ejecutar las aplicaciones centrales de la institución y almacenar los datos operativos.

3.4.2.- Aspectos del diseño de data center según la norma

3.4.2.1.- Análisis de riesgo del lugar

Analizando el tipo de riesgo al realizar en el data center:

- El impacto se clasifica como bajo: Perdida de servicios no críticos.
- La probabilidad de que ocurra un evento de impacto sería muy baja.

Entonces la tabla de medición de riesgo seria la siguiente:

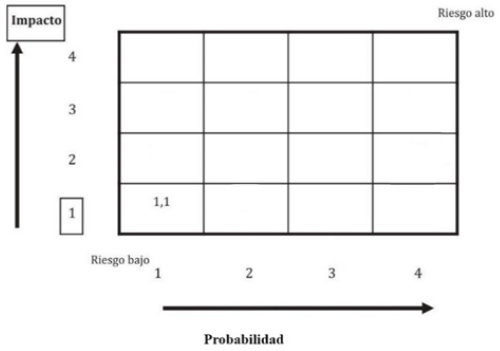


Figura 29. *Impacto y probabilidad de riesgo*

3.4.2.2.- Tratamiento del Riesgo

Luego de realizar y analizar el resultado de la valoración del riesgo se debe dar tratamiento a los riesgos latentes para la institución de la Fiscalía, haciendo uso de la estrategia ya conocida y adaptada que se realizará será la de:

- Evitar

3.4.2.3.- Evaluación De Costos

Los costos únicos que serán significativos de tal manera que el proceso de selección del sitio será:

Costos inmobiliarios: Costos de preparación del sitio.

3.4.2.4.- Evaluación del Sitio.

Según la evaluación de riesgos se vio como siguientes peligros en el proceso de creación física y ocupación para el data center:

- Eventos humanos (por ejemplo, accidentales e intencionales)
- Eventos tecnológicos (por ej., accidentales e intencionales)

3.4.2.5.- Principios de selección de lugar

Según la normativa para garantizar la seguridad y funcionalidad del lugar seleccionado los tres principios a tener en cuenta son:

Resistencia. - El lugar seleccionado soportara el peso de los equipos, rack, cables y otros elementos a usar.

Estabilidad. - El lugar seleccionado es estable y no colapsara ante eventos como el viento.

Resistencia al fuego. - El lugar seleccionado es apto, ya que es construido de hormigón compacto.

3.4.2.6.- Protección antiincendios en el Data Center

Los data center deben contar con sistemas avanzados de detección temprana de incendios que permitan identificar de manera inmediata:

Equipo de Detección de temperatura. -Para cualquier indicio de fuego o humo dentro de las instalaciones.

Extinción Automática. -Se utilizan sistemas de extinción de incendios mediante gases inertes (Extintor).

Ubicación Estratégica. - La norma también recomienda que los edificios estén diseñados y ubicados en zonas de bajo riesgo, evitando áreas propensas a desastres naturales como inundaciones o incendios forestales.

Mantenimiento y Supervisión. - Es fundamental que todos los sistemas de protección antiincendios sean sometidos a pruebas regulares para garantizar su correcto funcionamiento.

3.4.2.7.- Protección contra incendios en el Data Center

La protección contra incendios es un aspecto crítico en la gestión de edificios y la seguridad de las personas. Así se realizará los principios de:

Detectar. - Debe ser Temprana y precisa

Extinguir. - Rápida y efectiva

Proteger. - Se debe priorizar a las personas

Se aplicará planes de evacuación claros y bien comunicados, que incluyan señalización adecuada y rutas de escape accesibles para todos los ocupantes del edificio en caso de algún incidente.

3.4.2.8.- Protección contra Inundaciones en el Data Center

Evitar que ingrese agua al edificio

El Data Center estará ubicado en un área segura ante inundación y estará ubicado en la tercera planta del edificio.

Protección contra electricidad Estática en el Data Center

Por la recomendación de la norma poseen sistemas de conexión a tierra y materiales conductores para disipar la electricidad estática que se pueda generar dentro del data center.

Protección Contra Ruido en el Data Center

Ya que evitar el ruido en los data center es muy importante se utilizará materiales absorbentes de sonido en la adquisición de estos.

3.4.3.- Materiales y Tipo de Construcción a implementar dentro del Data Center

3.4.3.1.- Ubicación física del Data Center

El Data Center se ubicará en la Tercer Planta a la izquierda porque es un lugar más adaptable en espacio y no es apto para cambios de estructura solo para modificación y agregación que se pueda realizar, seguro y no muy lejano para realizar el cambio y no así tener que cambiar demasiado por el tema de que ya está el cableado para llegar a las distintas plantas en la institución. Aquí se muestra el área donde iría ubicado el data center:

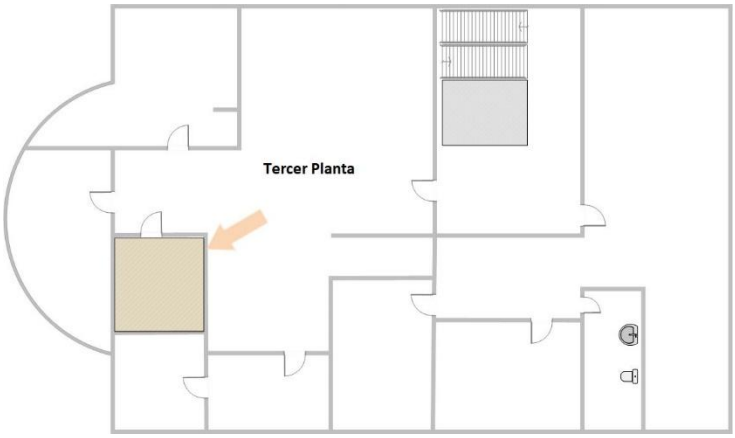


Figura 30. *Ubicación Seleccionada del Data center*

3.4.3.2.- Tamaño y características de acceso

Se realizará el Data Center, con las medidas actuales del lugar seleccionado (Ancho:5m x Largo:5m x Alto:3.8m), se hará pequeñas remodelaciones para así adaptar a las necesidades propuestas.

Medidas

- Piso Técnico (Falso): 30cm
- Perímetro: 20 mts.
- Área del Suelo: 5m x 5m.

3.4.3.3.- Acceso

Puerta ubicada centralmente en el pasillo, con identificador de huella o Lector RFID.

3.4.3.4.- Piso técnico (piso falso)

Debe facilitar el paso ordenado de cables, la ventilación y la distribución del aire frío. Su diseño debe ser resistente para soportar el peso del equipo y cumplir con estándares de carga estática y dinámica. Es esencial que permita un acceso rápido para el mantenimiento de los sistemas ubicados debajo del piso

3.4.3.4.1.- Recomendaciones para el Diseño de Piso Falso

Para el Data Center los paneles serán de 60cm x 60cm x 2,5cm de acero, con un material y bases a una altura de 30 o 40 cm, carga sobre el suelo mínima. El pegamento utilizado debe tener características especiales no combustibles.

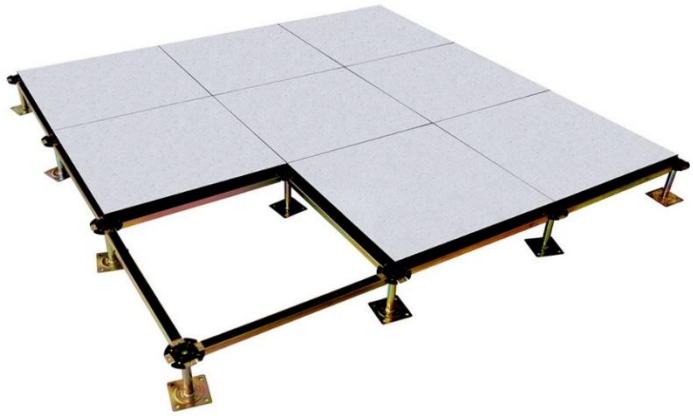


Figura 31. *Tipo de piso falso*

Criterio de medición en proyecto

Superficie medida entre paramentos, según documentación gráfica de proyecto, sin descontar huecos para instalaciones.

Condiciones previas que han de cumplirse antes de la ejecución de los ítems

Del soporte

Se comprobará que los paramentos verticales están terminados, y que todas las instalaciones situadas debajo de la losa están debidamente dispuestas y fijadas a él.

Piso Falso

- Unidad Kg: Imprimación, para reducir la absorción y mejorar la adherencia, a base de resinas sintéticas en dispersión acuosa y pigmentos, sin disolventes.
- Unidad m: Banda perimetral de lana de roca de 12 mm de espesor, 100 mm de anchura y 600 mm de longitud.
- Unidad Ud: Cartucho de 600 cm^3 de pegamento, para fijación de pies regulables a la superficie de apoyo.
- Unidad Ud: Pie regulable de acero galvanizado, para alturas entre 300 mm. Incluso accesorios.
- Unidad m2: Placa de yeso laminado reforzado con fibras, de 600x600 mm y 25 mm de espesor, con los bordes longitudinales machihembrados, para aplicación en falsos pisos continuos; clasificación 3/2/A/1.
- Unidad Ud: Cartucho de 600 ml de pegamento para juntas.
- **Mano de Obra:**
- Unidad H: Especialista en montaje y Ayudante 1ª en montaje.

3.4.3.5.- Iluminación

La norma específica que debe garantizarse una iluminación adecuada para las tareas de mantenimiento y operación, evitando sombras en las áreas críticas. Se deben usar sistemas eficientes, como LED, que minimicen el consumo energético y mantengan un nivel lumínico uniforme en el entorno. Así, se disminuyen las horas de funcionamiento de la iluminación y se programan encendidos y apagados, dependiendo de las labores del personal en el área.

3.4.3.5.1.- Recomendación de Iluminación

La iluminación LED tienen los siguientes beneficios:

- Ahorro energético
- No generan calor
- Arranque instantáneo
- Mayor tolerancia a los encendidos y apagados continuos

Panel Led Cuadrado Sobrepuesto

Panel LED Cuadrado Sobrepuesto, excelente rendimiento con ahorro de energía eléctrica.

Figura 32. *Panel de Luz LED*

Datos Técnicos de equipo de recomendación

- Potencia: 18W
- Modelo: Cuadrado sobrepuesto
- Flujo Luminoso: 1440 lúmenes
- Voltaje: 85-265V
- Regulable: No
- Medidas: 220x220mm
- Vida Útil: 30.000Hrs
- Color: Blanco

3.4.4.- Suministro y distribución de energía dentro del data center

Siguiendo la norma según el tamaño de data center que se realizara tendrá como suministro de energía primario y secundario que se encontrara dentro del edificio. Y se tomara como suministro secundario para el data center.

Data Center de tipo pequeño. – Puede haber solo un gabinete que proporciona energía protegida a los equipos. No se necesita una fuente de energía adicional.

Es fundamental garantizar la continuidad de la energía mediante sistemas UPS que protejan contra interrupciones y fluctuaciones eléctricas. La distribución debe ser redundante y estar diseñada para soportar las cargas críticas sin interrupciones, cumpliendo con los estándares de eficiencia y seguridad

3.4.4.1.- Elementos funcionales del suministro de energía

Suministro primario y secundario. -Puede ser de bajo voltaje o de medio voltaje, la salida de la misma forma va a ser de bajo y medio voltaje dependiendo del tamaño que establece el lugar. Los requerimientos de la entrada de cualquier equipo de suministro que puede ser UPS o también llamado sistema de alimentación interrumpida van a ser instalados entre equipos de distribución primaria y distribución secundaria y estos a su vez pueden ser de medio o bajo voltaje al igual que la entrada del equipo de distribución secundaria.

3.4.4.1.1.- Disponibilidad y Distribución de energía

Redundancia de Trayectorias de Distribución	Diseñar rutas de energía para soportar la carga máxima en caso de falla de la ruta redundante.
Interruptores de Transferencia Estática	Evaluar cuidadosamente debido a su "punto único de falla" y riesgo de corrientes de cortocircuito.
Estado de Tomacorrientes	Mantener y verificar el estado de los tomacorrientes que alimenten equipos para garantizar fiabilidad.
Entrada de Suministro de Energía	Garantizar la protección física y separación de las entradas de energía para mantener la seguridad

Tabla 21. *Disponibilidad y Distribución de Energía*

3.4.4.1.2.- Clasificación de diseño de disponibilidad

Según las clases de disponibilidad de la norma para el tipo de data center a diseñar será más optimo la clase de tipo 3:

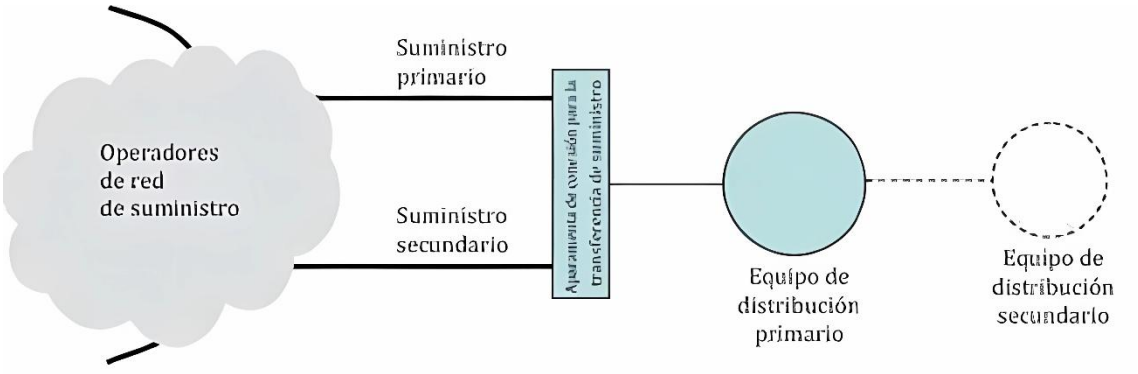


Figura 33. *Tipo de Disponibilidad de Energía Seleccionada*

3.4.4.1.3.- Recomendación de Equipo UPS

Los sistemas de energía interrumpible (UPS) brindan protección de energía garantizada para equipos electrónicos conectados. Cuando se interrumpe el suministro, o cuando este fluctúa por fuera de niveles seguros, instantáneamente la UPS comienza a proveer un suministro de respaldo limpio a través de baterías y protección contra sobretensiones a los equipos sensibles conectados. Las unidades UPS brindan respaldo de baterías y protección para dispositivos electrónicos, que incluyen:

- Equipos inalámbricos para integración en red (routers, modems).

Figura 34. *UPS para Rack*

Datos Técnicos de Equipo UPS Recomendado

- Capacidad: 3000VA/2700W

- Topología: Doble conversión en línea
- Voltaje: 220V
- Tipo de entrada: NEMA 5-15P
- Tipo de salida: 6 x NEMA 5-20R
- Comunicación: USB / SNMP / RS-232
- Indicador visual: Indicador LCD de estado

3.4.5.- Control ambiental

3.4.5.1.- Climatización

Las consideraciones que se tienen para el aire acondicionado y también definitivamente aplican para lo que es energía es que se trata es de hacer mucho énfasis en que todos los diseños deben ser pensando no en el día uno, sino pensando en un tiempo estimado de vida, más o menos unos diez años como mínimo pensando en la realidad como temas financiero, temas contables, temas fiscales es así que independientemente del costo de adquisición, hay que considerar el costo de operación, el costo de mantenimiento, el costo de cambio de piezas , el costo de consumo de energía. Por lo tanto, en la adquisición de elementos se debe considerar cuánto va a costar la solución pensando en un periodo de tiempo. En promedio se estaría hablando de diez años, hay que tener presente que debe tener:

- Un alto valor de la solución
- Valores altísimos de eficiencia
- Un alto nivel de porcentaje de utilización de las máquinas, es así que para cualquier conciliación sean lo más bajos posibles.
- Máquinas de operación sencilla, las interfaces deben ser lo más amigables posibles.
- Alta calidad
- Fácilmente mantenible.

3.4.5.2.- Disponibilidad

El objetivo de la climatización es asegurar que la puerta de los gabinetes o en el lugar de acceso del aire frío hacia la carga crítica, ya sea si el aire lo recibe por abajo, en el lugar exacto donde se reciba el aire frío este debe de cubrir las necesidades de valor en temperatura y valor en humedad. El ASRAE dice que en el ingreso del aire frío en la carga crítica la temperatura debe estar:

AL INGRESO DE LOS RACKS (PASILLO FRIO)	
Temp. De Bulbo Seco	**Humedad Relativa**
18-27◦ C	<60%

Tabla 22. *Temperatura Recomendada para el lugar del Data Center*

3.4.5.2.1.- Distribución de temperatura para aire controlado en el data center

Esta norma habla que se debe de medir la temperatura en humedad ambiente porque la temperatura de humedad ambiente tiene un efecto directo sobre el comportamiento en la eficiencia o disponibilidad de capacidad de los equipos de aire acondicionado las épocas de invierno son las mejores para el sistema de aire acondicionado porque la evacuación de calor es mejor, las épocas de verano son las más complicadas.

Hay que tener muy en claro el tema de medición ya mencionado, hay que considerar las alarmas, basados en los sensores están ubicados en la parte superiores e inferiores de los gabinetes para saber exactamente cómo es el tema de la distribución del aire frío hay que controlar la temperatura y la humedad.

Se debe considerar en este caso específico en el aislamiento y definición de pasillos, un confinamiento para asegurar siempre temperaturas lo mejor distribuidas y retornos lo más caliente posible para poder disiparlas.

3.4.5.3.- Recomendación para climatización en el Data Center

3.4.5.3.1.- Aire Acondicionado de Precisión para Data Center

Son equipos de refrigeración diseñados para entregar un control preciso de la temperatura y humedad en todas las aplicaciones en las que se necesita un grado de precisión elevado.

En otras palabras, tienen una función crítica: conservar la temperatura en niveles óptimos y controlar las densas cargas electrónicas en los data center, así como gestionar la humedad y aire del ambiente o sala. El aire acondicionado de precisión es el más recomendado a utilizar en los Data Centers.

3.4.5.3.2.- Características Generales

Los acondicionadores de aire de precisión serie DW han sido desarrollados para cumplir holgadamente con estas exigencias y asegurar un funcionamiento sumamente confiable. Su función es la de controlar la temperatura y humedad del local durante todo el año, tomando las decisiones necesarias a fin de mantener en todo momento, las condiciones programadas.

Son unidades se fabrican con chapa galvanizada pre pintada, lo que asegura una larga vida útil del gabinete sin requerir repintado periódico ni otro tipo de mantenimiento. A fin de permitir su funcionamiento en refrigeración con bajas temperaturas exteriores los acondicionadores WESTRIC con condensación por aire, cuentan con control electrónico de condensación modulante, lo que permite un perfecto manejo de las condiciones de funcionamiento.
Estas resistencias eléctricas son utilizadas también en el caso de que el ambiente lo requiera, para proveer calefacción.

Los principales elementos constitutivos del equipo lo que le hace apto son:

- Borneras componibles para alimentación eléctrica y salidas de alarma
- Interruptor termomagnético general
- Relee de sobreintensidad en los contactores correspondientes a los motores y motocompresor
- Sensor de anomalías de tensión
- Sensor de humedad relativa
- Sensor de temperatura
- Sistema Automático-Manual

Datos Técnicos de Equipo Recomendado

- Especificaciones DW-003 UI
- Calor Sensible (Kw) 8.9
- Calor Total (Kw) 10.5
- Descarga de Aire Por piso técnico
- Por conductos
- Ancho (mm) 1200-1200-1200
- Alto (mm) 2250-1950-1950
- Profundidad (mm) 750-750-750
- Peso (Kg) 250-240-230

3.4.5.3.3.- Modelo de Aire Acondicionado según las características

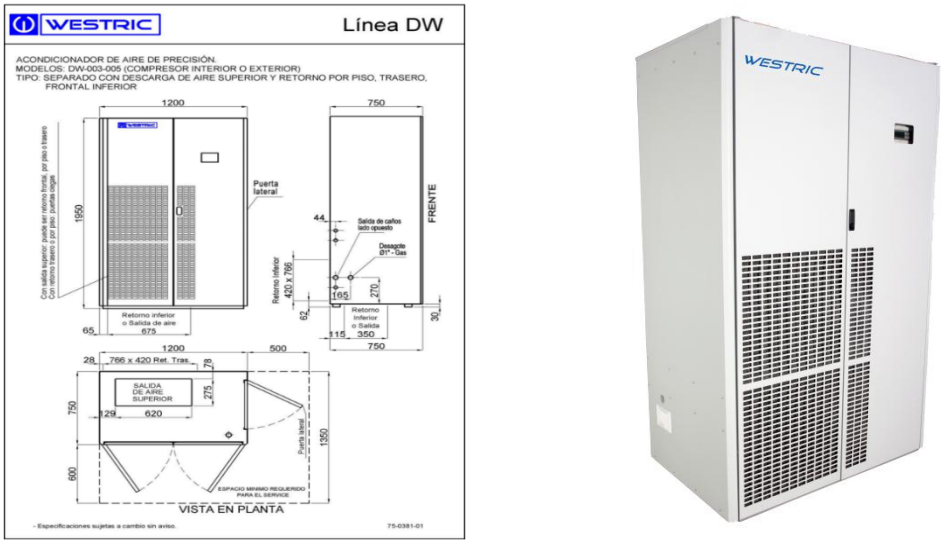


Figura 35. *Equipo de aire de precisión*

3.4.5.3.4.- Distribución del equipo dentro del Data Center

- Altura mínima 1,95 cm para los equipos de rack.
- Los pasillos estarán lateralmente y en el frente de los racks.
- El equipo se situará en la parte de en frente de los racks proporcionando el aire frio en frente, y los sistemas de ventilación pueden absorber el aire caliente y de retorno por la parte trasera para optimizar el aire acondicionado.
- Se realiza mucha más eficiencia por retorno de aire caliente de la parte de trasera o si bien se puede cambiar el retorno al que se requiera con el tiempo de uso y revisión de la temperatura generada.

3.4.6.- Infraestructura de Cableado

La norma prioriza un cableado estructurado y organizado, diseñado para minimizar interferencias electromagnéticas y cumplir con las especificaciones de transmisión. Debe estar identificado claramente para facilitar el mantenimiento y las ampliaciones.

A nivel físico la norma se enfoca en la funcionalidad, en cómo están conectados los equipos, los programas de conexión más la diferencia de lo que se ve a nivel lógico, en este nivel físico o en el nivel de infraestructura de telecomunicaciones prima tres cosas: la distribución, la disposición, las rutas del cableado, y la conectividad, es importante determinar la conexión entre todos los puertos, la topología, y la disponibilidad.

3.4.6.1.- Instalación

3.4.6.1.1.- Punto a punto

La norma nos dice que el cableado punto a punto, significa usar cables discretos o usar cables que normalmente o comúnmente han sido elaborados desde fábrica y cuya función es conectar equipos contra equipos puertos contra puertos, es decir si necesitamos conectar equipos. Para las conexiones punto a punto el cable de conexión, el patch cord, que evidentemente está hecho de fábrica se conecte de puerto a puerto, sin pasar por ningún otro equipo, ningún otro accesorio adicional de cableado y a eso se le llama punto a punto.

Este tipo de cableado de punto a punto no es reutilizable muchas veces, porque se ha hecho, desde la medida, y los accesos para conectar dos puntos en particular y muchas veces este tipo de cableado es un método muy simple o un método muy económico, pero no proporciona la fiabilidad, ni la reutilización a futuro del cableado.

Cableado para disponibilidad de clase 1:

- Conexión punto a punto
- Cables predeterminados
- Conexiones locales limitadas

3.4.6.1.2.- Cableado Fijo

Un cableado fijo es lo que en cableado horizontal se llama como el canal permanente, es el cableado que va a estar fijo en él y que nos va a permitir mayor disponibilidad a futuro y luego vemos siempre que se ha cableado fibra, o cable de cobre cuando hacemos lo que se llama como reflejo. Los reflejos forman parte del cableado fijo de la clase cableada denominada cableado fijo. Otorgan mucha mayor funcionalidad al momento de hacer algún cambio que no es un cableado simple y tampoco es un cableado económico, pero nos permite hacer con el tiempo cambios o modificaciones, sin afectar la instalación del cableado.

Entonces la disposición de los gabinetes, la ubicación del equipamiento y las rutas del cableado son importantes, porque hay soluciones de enfriamiento que necesitan rutas y lutos especiales donde no podría haber cableado estructurado por eso es importante conocer todo el diseño. Es una relación directa, la arquitectura, y la disponibilidad de cableado.

Cableado para disponibilidad de clase 2:

- Cableado fijo con arquitectura de un solo Path y redundancia
- Adecuada gestión de cables y de fácil expansión

- Conexiones cruzadas y centrales y locales

3.4.6.1.3.- Recomendación de Cable Conexión

Lo que sugiere la norma es que se pueda aplicar los 2 tipos de clases el fijo y punto a punto de cableado en este diseño se aplicaran las siguientes clases de disponibilidad. Los cables de conexión Cat.6 son totalmente suficientes para el uso normal en la institución. Además, los cables de red Cat.6 son compatibles con la versión anterior, los cables Cat.5(e), que todavía se utilizan en la infraestructura. Sin embargo, en comparación los usuarios podrán disfrutar del doble de ancho de banda.

3.4.6.1.4.- Cables Reconocidos

- Cable UTP de 100 de par trenzado Cat. 6.

Cat.6	
Velocidad	10/100/1000 Mbit/s
Frecuencia	250 MHz
Longitud máxima	100m (109,36 yds)
Área de aplicación	Redes ATM-Gigabit y Multimedia Ethernet

Tabla 23. *Características de Cable UTP*

Tipos de Cable

Dentro del data center:

- Cobre (UTP Cat. 6).

En las plantas de la institución (planta baja, primer, segunda, tercer y cuarta planta):

- Cobre (UTP Cat. 5e)

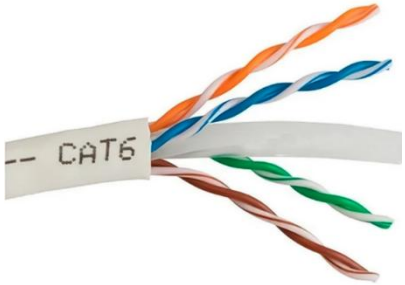


Figura 36. *Cable UTP Cat. 6*

Figura 37. *Conector para cable UTP Cat. 6*

3.4.7.- Sistemas de Seguridad

La norma habla de la seguridad física en la parte de las configuraciones y de los espacios entonces es importante en el caso de la seguridad, tomar estos espacios dependiendo del tamaño del data center estas deben cubrir todas las áreas críticas del data center. La vigilancia debe ser continua para prevenir accesos no autorizados o identificar incidentes rápidamente. Se realizara el tipo de protecion de clase 2:

Clase de protección 2

- Protección física necesaria en cualquier camino abierto que atraviese los límites de esta clase y superiores.
- Importancia de garantizar el funcionamiento normal o de emergencia de las infraestructuras del data center.
- Evitar entrada de objetos que puedan dañar o limitar los servicios.

3.4.7.1.- Proteccion contra acceso no autorizado

La norma de clase de protección 2 opta por la protección física necesaria en cualquier camino abierto de los límites de esta clase y superiores.

3.4.7.1.1.- Recomendación de control de acceso

Lector Biométrico de huella digital es un innovador lector biométrico de huella digital para aplicaciones de control de acceso el cual adopta el avanzada seguridad para ofrecer confiabilidad, precisión y rápida velocidad de verificación. Su cubierta metálica y protección lo hacen resistente al agua, polvo y daños externos.

Ofrece flexibilidad para ser instalado de manera autónoma o con paneles de control de acceso que soporten formato Wiegand. Los usuarios puede ser registrados mediante una tarjeta de administrador cuando el dispositivo funciona en modo autónomo. Cuenta con interfaz TCP/IP y RS485 para una fácil conexión y escalabilidad

Datos tecnicos de Equipo Recomendado

- Capacidad de Huellas Dactilares: 100 Huellas
- Capacidad de Tarjeta Identificación: 1000 Usuarios
- Capacidad de la Transacción: 30,000 Registros
- Plataforma de Hardware: ZEM700 y Sensor: ZK Sensor Óptico
- Interfaz de acceso de control: Bloqueo eléctrico, sensor de puerta, botón de salida, la alarma
- Humedad de Funcionamiento: 10% -90%
- Grado de Protección: IP54 Ø Dimensión (W * H * D) mm: 73 * 148 * 34,5
- Fuente de Alimentación: 12V DC

Figura 38. *Lector Biométrico de huella digital y tarjeta RFID*

3.4.7.2.- Puerta de Seguridad

La puerta de seguridad debe ser protegida contra robo y compuesta por dos planchas de acero gruesas y refuerzos de tubo estructural en el interior. Cuenta con cerradura electromagnética. El marco produce un cierre hermético en contacto con la misma y las bisagras son de alta resistencia al peso y fricción.

Referencia de tipo de puerta a ser seleccionada para el ingreso del data center.

Figura 39. *Modelo de tipo de puerta reforzada*

3.4.7.3.- Protección antiincendios

Se deben instalar detectores de humo de alta sensibilidad para la detección de un incidente y poder alertar al personal.

3.4.7.3.1.- Recomendación de tipo de sensor antincendios

El FireProtect es un detector de última generación diseñado para la seguridad residencial contra incendios. La cámara de humo excepcional no necesita ser limpiada con regularidad, el sensor de doble espectro distingue el humo del vapor, el termistor reacciona rápidamente a la combustión de los materiales sintéticos y el software práctico minimiza las falsas alarmas. El diseño y la fijación bien pensados, así como la configuración en la app proporcionan una instalación sencilla y rápida. El detector inalámbrico de incendio de humo, calor y monóxido de carbono es alimentado por baterías integradas y también por la red eléctrica.

El ManualCallPoint (Red) es una forma sencilla y rápida de activar la alarma de incendio, que está disponible para cualquiera. Al pulsar el botón, se activan las sirenas integradas de todos los detectores de incendio en el sistema y se envía una notificación a los usuarios. Al mismo tiempo, la central receptora de alarmas (CRA) recibe la señal de alarma y llama a los servicios de emergencia.

Características de Tipo de Sensor Antiincendios

- Sensor óptico de doble espectro, detecta humo por el tamaño de partículas en el aire. Protección contra falsas alarmas, no reacciona ante el vapor de agua. Cámara de humo patentada, protege el sensor de humo del polvo, suciedad e insectos.

- Sirena integrada, volumen de 85 dB a una distancia de 3 metros. Notificación sonora de alarmas está habilitada hasta que la causa de activación sea eliminada o hasta que el usuario deshabilite las notificaciones.
- Botón inalámbrico de pared de color rojo para la activación manual de la alarma de incendio. Cuando se pulsa la parte central (elemento frangible), el botón se mueve hacia adentro, activando una alarma o iniciando un escenario. Aparecen dos barras amarillas arriba y abajo, que indican el estado del dispositivo.
- Modos de funcionamiento, alarma de incendio, activador de escenario, alarma de incendio interconectada.
- Alertas críticas, el sistema puede activar sirenas anti intrusión y enviar notificaciones sonoras de alarma a los usuarios, aunque el sonido esté silenciado, el modo No molestar esté activado o los auriculares estén conectados.

Figura 40. *Tipo de Sensor antincendios*

3.4.7.4.- Protección contraincendios

Se debe incorporar sistemas de extinción de incendios con agentes limpios (que no dañen los equipos) para lograr mitigar los daños

Recomendación de Tipo de Extintor

Extintor CO2 (Dióxido de Carbono) de 6 kilos son diseñados específicamente para combatir incendios de Clases B y C. Cuentan con certificación nacional, asegurando máxima eficacia y seguridad. Es un dispositivo vital para garantizar la seguridad en ambientes empresariales. Equipado con Dióxido de Carbono, este extintor ha sido especialmente diseñado para actuar

eficazmente contra incendios en áreas con equipos electrónicos y eléctricos de gran escala, como tableros, servidores y transformadores eléctricos. Incluye un soporte para colgar a muro.

3.4.7.5.- Características Principales de Tipo de Extintor

Certificación: Cumpliendo con el Decreto Supremo DS 44, este extintor posee el sello de aprobación del renombrado Laboratorio INCEN.

Mantenimiento Periódico: Para mantener su funcionalidad y rendimiento, es esencial realizar una revisión anual.

Soporte para colgar a muro: Incluido en el precio

Diseño Sostenible: Cuenta con un cilindro recargable y reutilizable.

Seguridad Ante Todo: No es aconsejable su uso en espacios confinados.

Garantía Integral: Proporcionamos 6 meses de garantía, siempre y cuando el sello esté intacto.

3.4.7.6.- Usos y Aplicaciones de tipo de Extintor

Extintor Especializado BC: Destinado a enfrentar:

Clase B: Incendios originados por líquidos inflamables, gases y grasas.

Clase C: Escenarios con equipos y dispositivos con carga eléctrica.

Figura 41. *Tipo de Extintor de dióxido de carbono*

3.4.8.- Administración y Operación

La norma hace referencia a video vigilancia al interior y exterior de los data centers estas cámaras deben estar ubicados en puntos críticos o neológicos, la idea es cubrir todos los ángulos ningún ángulo puede quedar expuesto para no caer en una vulnerabilidad en el data center. Estas deben cubrir todas las áreas críticas del centro de datos y contar con almacenamiento seguro para registrar y analizar las imágenes y la vigilancia debe ser continua.

3.4.8.1.- Recomendación de Vigilancia Para Seguridad

Las cámaras de tipo IP Domo Metálica ofrecen una resolución de 2MP con opciones de lente de 2.8mm o 3.6mm. La elegante mezcla de estética de la cámara combinada con su forma compacta proporciona una excelente opción para una variedad de aplicaciones pequeñas y medianas, interiores / exteriores.

Figura 42. *Tipo de Cámara de Vigilancia*

Datos Técnicos de Equipo Recomendado:

- Puertos Ethernet 10/100: 1
- Protocolos: IPv4/IPv6, HTTP, HTTPS, TCP/IP, UDP, UPnP, ICMP, IGMP, RTSP, RTP, SMTP, NTP, DHCP, DNS, PPPOE, DDNS, FTP, IP Filter,QoS y Wi-Fi: N/A
- Imagen Sensor: 1/2.7” 2Megapixel progressive scanCMOS
- Max. IR LEDs Length: 30m y Focal Length:3.6mm (6mm opcional)
- Angulo de Vista: H: 93° (63°)
- Comprensión Video: H.264/ H.264H/ H.264B/MJPEG
- Max. Usuarios: 20
- Compatibilidad: ONVIF, CGI

3.4.9.- Material de canalización

La norma establece que la canalización es clave para proteger cables eléctricos y de datos de posibles daños mecánicos. Ayudan a organizar y soportar el cableado de manera eficiente, permitiendo una gestión adecuada del flujo de aire. Estas bandejas deben estar diseñadas para soportar el peso del cableado y facilitar futuras modificaciones. Debe ser resistente al fuego y cumplir con las normas de instalación eléctrica.

3.4.9.1.- Recomendación de tipo de Canalizacion

Mini Cable Canal de PVC 30 x 15 mm:

Sus dimensiones pueden ser de 30 mm de profundidad x 15 mm ancho. Por él irán los cables con una protección frente a incidencias exteriores. La canaleta dispondrá de una tapa desmontable que se podrá poner y quitar para la instalación de los cables. Existen dos modelos con adhesivos y sin

adhesivos que permitirá colocar en la pared o por el piso. Si se utilizara sin adhesivo se puede usar un tornillo para la fijación de la canaleta.

Figura 43. *Mini Cable Canal de PVC*

3.4.9.2.- Recomendación de Bandeja de Rejilla para Cableado de Red:

Sistemas de bandejas portacables que iran bajo piso falso algunas caracteristicas de bandejason:

- Longitud: 4000mm.
- Altura ala: 100mm.
- Anchos: De 100 a 100mm.
- Acabados: Cincado ecológico Z3, Galvanizado en caliente (G), Inox AISI 304/316 pasivado (I), Alta Resistencia (HR).

Figura 44. *Bandeja de Rejilla para Cableado UTP*

3.4.10.- Racks

La norma establece que los racks deben ser robustos, ajustables y diseñados para facilitar la gestión de cables y equipos. Además, es importante que cuenten con sistemas de ventilación para disipar el calor generado por los equipos.

3.4.10.1.- Recomendación de tipo de Rack

Rack de distribución 22U. Es una estructura robusta, polivalente con puerta frontal de cristal, puerta posterior sólida y puerta reversible 180º. Con paneles laterales extraíbles con llave. Se suministra con ruedas, patas y tornillería. Dispone de espacio para instalar ventiladores de techo y ranuras que permiten la circulación de aire. Acceso superior e inferior de tipo cepillo antipolvo para cableado.

Figura 45. *Tipo Rack de Distribución*

Datos Tecnicos de Equipo Recomendado:

- Rack 19" Altura 22U.
- 600 x 600mm (Ancho x Fondo).
- Montaje a suelo y puerta de cristal.
- Maneta giratoria con llave de alta calidad en puerta frontal.
- Guías verticales en frontal y trasera ajustables en profundidad.
- Carga estática 800Kg.
- Color Negro RAL9005.

3.4.10.2.- Recomendación de Patch Panel Cat6

Figura 46. *Tipos de Patch Panel Cat 6*

Datos Tecnicos de equipo recomendado:

- 24 y 48 PUERTOS
- Con soporte trasero, Etiquetado
- Conforme a ANSI/TIA/EIA 568B se instala con cable sólido AWG 22*24 Y 26

3.4.10.3.- Recomendación de Regleta en Bastidor

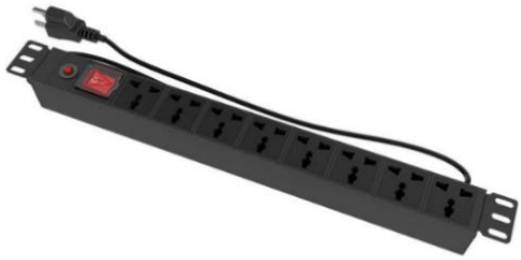


Figura 47. *Regleta de Bastidor para Rack*

Datos Tecnicos de equipo Recomendado:

Regleta para bastidor, de 8 tomacorrientes, corriente de 220VCA, 16A, protección contra sobrecargas, potencia Max. 3500W, margen de temperatura -40° a +75°, normas Internacionales ANSI/TIA/EIA 568.C.2; Italia CEI-23-16 y CEI 23-50; UL 94V-0, con metal y componentes modulares y desmontables.

3.4.10.3.- Recomendación de Organizador Horizontal

Figura 48. *Organizador Horizontal para cableado*

Datos Tecnicos de Equipo Recomendado:

- Organizador de cables de red horizontal para rack

3.4.11.- Recomendaciones de Mantenimiento a Data Center

La operación, la disponibilidad, la capacidad, la estrategia que se debería de contemplar para el centro de datos, las incidencias en tema de seguridad, el tema del ciclo el nivel de servicio, los cambios, el tema de energía, el costo, y el tema a nivel de recursos y activos y asi se estaria tomando la administración de la gestión. La administración de operaciones en la norma lo se debe de priorizar por procesos.

Prioridad uno:

- Administración de operaciones se debe ver el tema de mantenimiento se tendria que hacer todo un programa y un plan de mantenimiento.
- Administración de incidentes, algún incidente que ocurra, y que ese incidente pueda, generar en alguna indisponibilidad en la operación del data center, la administración de la seguridad, donde se debe ver el tema de control, monitoreo, y seguimiento o lo que es el tema de supervisión.

Prioridad dos:

- Administración de cambios es un proceso, por ejemplo, cambio de un gabinete, un equipo. Entonces ese simple cambio de este equipo va a generar todo un proceso de administración y ahí se ve la administración de cambio.
- Administración de nivel de servicio, se debe ver el tema de los proveedores internos, proveedores externos, los proveedores dentro de la administración, se va a administrar el contrato por mantenimiento o el servicio de mantenimiento o através de un contratista o

puede ser el tema de insumos de adquisición de equipos o accesorios y se debe realizar una gestión de acuerdo a lo que la institucion necesite conforme al tiempo.

Prioridad tres:

- La administración de energía es calidad de energía, plan de mantenimiento, tema de control y supervisión. El tema de configuración es el tema de los costos, la administración del ciclo de vida del producto, todo lo que cuenta el centro de datos. Entonces se debe hacer todo una administración, una gestión con respecto a lo que la institucion vaya requiriendo con el tiempo.

3.4.12.- Usos de Seguridad de Fortinet FortiGate 90G

El Fortinet FortiGate 90G es un firewall de última generación (NGFW, por sus siglas en inglés) diseñado para ofrecer seguridad integral, alto rendimiento y facilidad de implementación en redes medianas y pequeñas, como oficinas, sucursales o data center compactos. Este dispositivo combina funciones avanzadas de seguridad y redes, tales como filtrado de contenido, protección contra intrusos, y segmentación interna, todo potenciado por inteligencia artificial (IA) para adaptarse a amenazas emergentes y complejas.

3.4.12.1.- Características clave:

Rendimiento superior: Incluye procesadores de seguridad (SPUs) dedicados para manejar tráfico cifrado y no cifrado sin sacrificar el rendimiento.

Secure SD-WAN: Optimiza la conectividad entre sitios distribuidos y aplicaciones en la nube, reduciendo costos y mejorando el rendimiento.

Servicios FortiGuard impulsados por IA: Permite protección avanzada frente a amenazas, antimalware, filtrado web y control de aplicaciones.

Acceso ZTNA (Zero Trust): Implementa políticas estrictas de acceso basado en confianza cero.

Diseño compacto y eficiencia energética: Es ideal para instalaciones con espacio y recursos limitados.

Fácil integración: Compatible con sistemas de monitoreo y gestión centralizada, como FortiManager y FortiAnalyzer.

En el caso de un centro de datos y la red institucional, el FortiGate 90G permite:

- Proteger los datos críticos mediante segmentación del tráfico interno y prevención de amenazas avanzadas.

- Mejorar la disponibilidad de la red, minimizando interrupciones causadas por ataques cibernéticos.
- Monitorear y gestionar de manera eficiente múltiples nodos y segmentos de la red.

3.4.12.2.- Medidas seleccionadas para seguridad en la red del DC

A continuación, se describen las opciones más relevantes que pueden aplicarse específicamente a un data center y toda la red de la institución:

- **Segmentación del tráfico (Interno y Externo):** Implementa firewalls internos para controlar el tráfico Este-Oeste entre servidores, aplicaciones y usuarios dentro del centro de datos. Utiliza firewalls perimetrales para proteger el tráfico Norte-Sur (ingreso y salida del centro de datos hacia internet).
- **Prevención de Intrusiones (IPS):** Configura el sistema de prevención de intrusos para detectar y bloquear amenazas conocidas y de día cero. Esto protegerá tanto la infraestructura del centro de datos como la red en general.
- **Filtrado de Aplicaciones y Sitios Web:** Restringe el acceso a aplicaciones y sitios web no autorizados mediante políticas de filtrado específicas. Esto previene el uso de recursos maliciosos o no esenciales.
- **Protección Basada en DNS:** FortiGuard DNS evita el uso de dominios maliciosos, incluyendo los utilizados en campañas de phishing y malware, asegurando que las comunicaciones del centro de datos sean seguras.
- **Control y Monitoreo en Tiempo Real:** Conecta el FortiGate 90G a herramientas de monitoreo como FortiAnalyzer para recopilar y analizar datos de tráfico y seguridad en tiempo real. Esto ayuda a identificar y mitigar amenazas proactivamente.
- **Integración con ZTNA (Zero Trust Network Access):** Implementa políticas de acceso basadas en confianza cero para garantizar que solo usuarios y dispositivos autorizados accedan a las redes internas.
- **Protección contra IoT y Dispositivos Conectados:** Dado el posible uso de dispositivos IoT en la infraestructura, FortiGate ofrece herramientas para detectar y gestionar estos dispositivos, aplicando políticas de seguridad adecuadas.

3.4.12.3.- Recomendación de Implementación práctica del Fortinet

Para ser posible esta recomendación de implementación debe adquirir la licencia necesaria que ofrece la empresa de Fortinet para realizar estos tipos de seguridad.

Data Center: Utiliza segmentación interna para proteger servidores y bases de datos sensibles. Configurar reglas de IPS y filtrado web para proteger las aplicaciones alojadas.

Red institucional: Implementar el acceso ZTNA para todos los usuarios y dispositivos. FortiGate controlará las conexiones de dispositivos IoT, bloqueando aquellos no autorizados.

Monitoreo: FortiManager centraliza la gestión de políticas y actualizaciones del firewall, mientras que FortiAnalyzer proporciona reportes detallados y análisis del tráfico.

Estas medidas asegurarán una infraestructura robusta frente a amenazas, con visibilidad y control centralizados sobre todo el tráfico de la red institucional y del centro de datos

3.4.13.- Descripción y Aplicaciones en el Diseño de Centros de Datos

3.4.13.1.- Descripción de Blender

Blender es una herramienta de software libre y de código abierto para la creación de contenido 3D. Fue desarrollado inicialmente en 1994 por Ton Roosendaal y ha evolucionado significativamente, convirtiéndose en una opción popular entre artistas digitales, diseñadores y arquitectos. Blender es compatible con múltiples plataformas, incluyendo Windows, macOS y Linux, y ofrece una amplia gama de funciones que abarcan desde el modelado 3D hasta la animación y la simulación.

Las principales características de Blender incluyen:

- **Modelado 3D y animacion:** Blender proporciona un conjunto completo de herramientas para modelado poligonal, escultura digital y diseño de superficies NURBS, permitiendo a los usuarios crear modelos detallados y precisos.
- **Animación:** Las capacidades de animación de Blender incluyen sistemas de rigging, cinemática inversa y un editor de gráficos para controlar y ajustar las curvas de animación.
- **Renderizado:** Con motores de renderizado como Cycles y Eevee, Blender permite generar imágenes realistas y visualizaciones detalladas de los modelos creados.
- **Interfaz de Usuario Personalizable:** La interfaz de Blender es altamente personalizable, permitiendo a los usuarios adaptar el entorno de trabajo a sus necesidades específicas.

3.4.13.2.- Aplicaciones de Blender en el Diseño de Centros de Datos

El uso de Blender en el diseño de centros de datos ofrece múltiples beneficios, que incluyen:

- **Visualización Realista:** Blender permite crear modelos 3D detallados de la infraestructura del centro de datos, facilitando la visualización y comprensión del diseño propuesto. Esto ayuda a identificar posibles problemas y optimizar el espacio y los recursos.

- **Simulación de Condiciones Ambientales:** Las capacidades de simulación de Blender permiten modelar y analizar el flujo de aire, la distribución de la carga térmica y otros factores ambientales críticos para el funcionamiento eficiente de un centro de datos.
- **Iteración Rápida de Diseño:** Gracias a la flexibilidad de Blender, se pueden realizar ajustes y modificaciones en el diseño de manera rápida y eficiente, evaluando diferentes configuraciones y soluciones.
- **Colaboración y Presentación:** Blender facilita la creación de presentaciones visuales atractivas y detalladas, lo cual es crucial para la comunicación efectiva entre los diseñadores, ingenieros y otras partes interesadas en el proyecto.

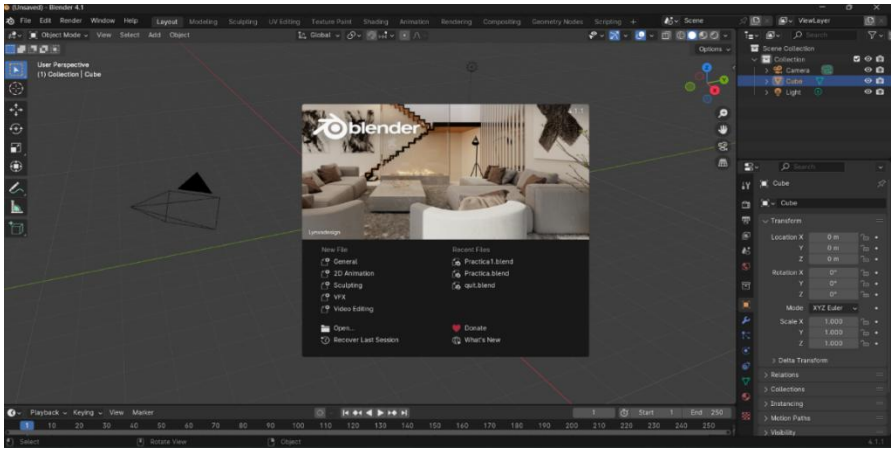


Figura 49. *Herramienta Blender para diseño en 3D*

3.4.14.- Boceto de Diseño de Data Center

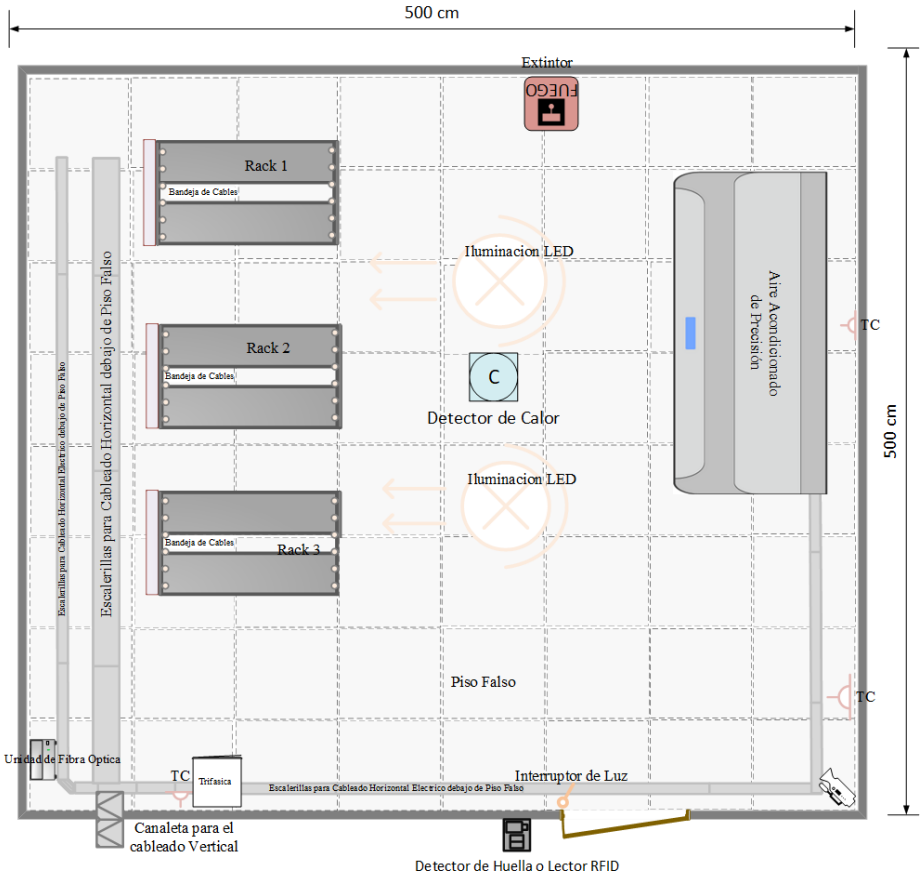


Figura 50. *Boceto del Diseño de Data Center*

3.4.15.- Servicios que maneja la Institucion F. Departamental de Tarija

3.4.15.1.- Internet

Para brindar este servicio la institucion, dispone de fibra Optica para proveer de internet para la parte Administrativa y WIFI. Mediante autorización a través de la dirección IP del equipo que usa el servicio.

3.4.15.2.- Biométricos

Lector de huella de la Fiscalia Departamental de Tarija, cuenta con 2 lectores de huella digital para el control de asistencia del personal administrativo, que labora en la Institución, estos se encuentran conectados directamente desde un punto de red.

3.4.15.3.- Cámaras de vigilancia

La Fiscalia Departamental de Tarija, cuenta con un sistema de video vigilancia que consta con cámaras en cada piso ubicados en sitios estratégicos de la infraestructura física, que está adherida en la red de internet en firewall en la institucion.

3.4.15.4.- Servidores

La Fiscalia Departamental de Tarija, requiere que el departamento de Sistemas cuente con un Data Center, en el cual se pueda administrar de mejor manera los diferentes servidores que prestan los diferentes servicios como son: Internet, Firewall, Antivirus, DNS, DHCP, FTP, AD, Administración de la Base de Datos, Aplicaciones Propias de la institucion.

3.4.15.5.- Aplicaciones

En los servidores actualmente las aplicaciones administrativas y de desarrollo solo requieren instaladores de programas con sus respectivas licencias, como el office y un antivirus de calidad todos ellos licenciados que son utilizados por el personal administrativo.

3.14.16.- Diseño Fisico del Data Center

Se observa como todos los componentes propuestos para el diseño se cumplen correctamente y esta seria una previa visualizacion de como quedaria el Data Center.

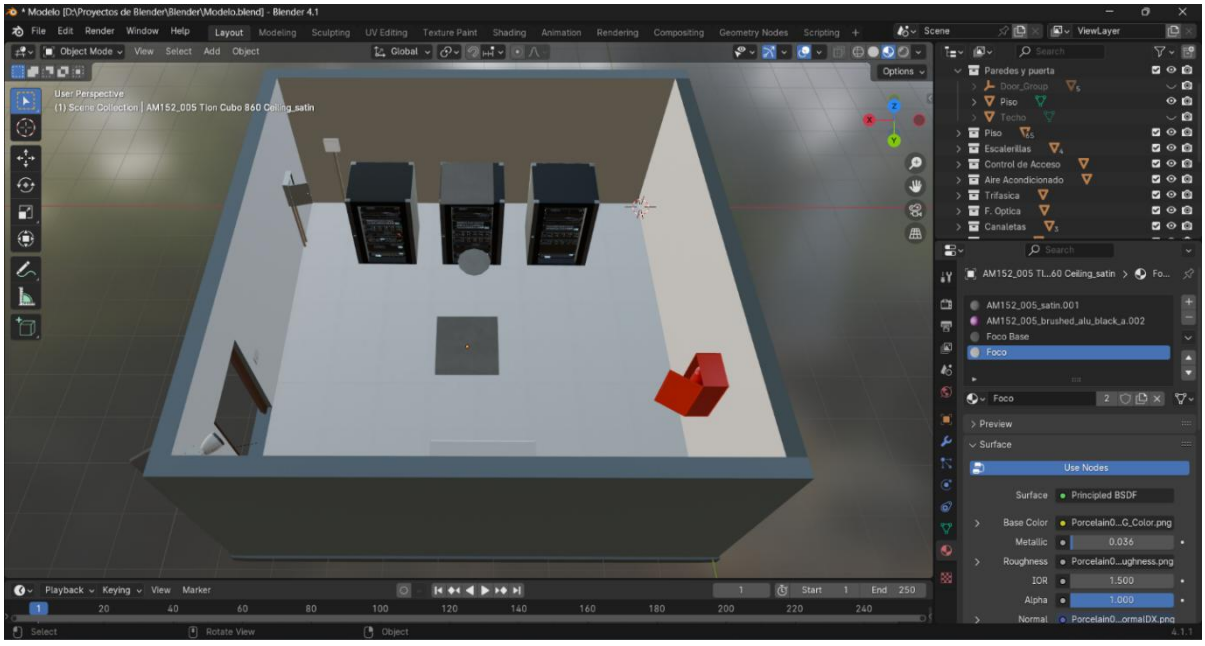


Figura 51. *Diseño en 3D del Data Center en Blender*

3.4.17.- Diseño Logico del data center

Diseño logico de conexión de los equipos en los racks del data center.

Figura 52. *Diseño lógico de los equipos en el data center*

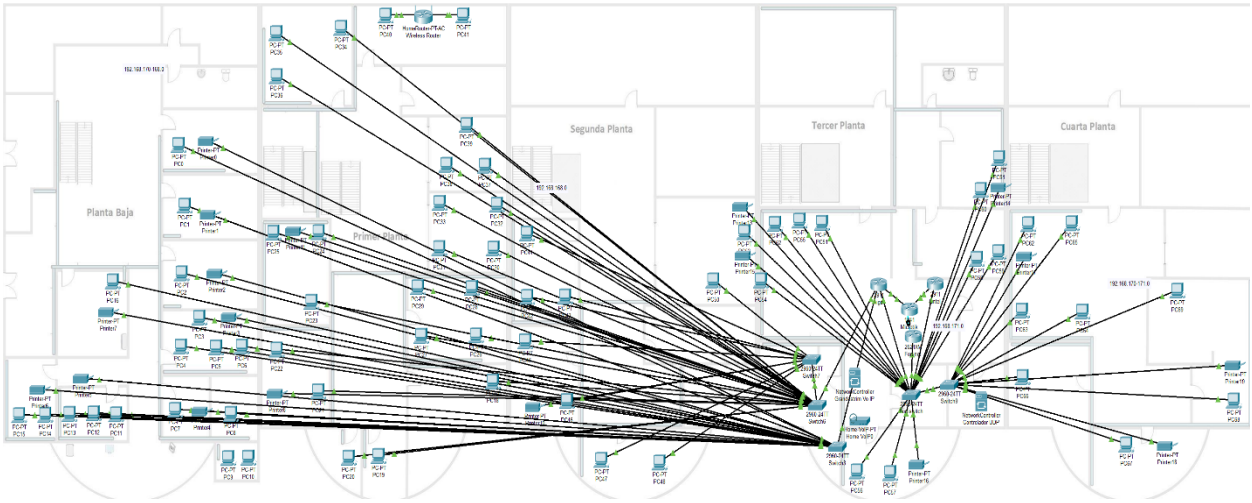


Figura 53. *Diseño lógico de red*

3.4.18.- Diseño Fisico de Cableado

Diseño de cada planta con el cableaod horizontal y vertical junto con el data center propuesto.

Figura 54. *Cableado físico de planta baja, primer y segunda planta*

Figura 55. *Cableado físico de tercer y cuarta planta.*

3.5.- Desarrollo de Presupuesto

3.5.1.- Costos Referenciales de Dispositivos

Para obtener el costo total del diseño se tomará en cuenta: canaletas, cables, conectores, patch cords, rack y demás accesorios. En lo referente a los materiales y accesorios, se detalla una estimación aproximada de las cantidades que se necesitará para el Data Center, ya que si se realiza la implementación según el tiempo y costos actuales en ese tiempo es posible que su número cambie.

3.5.2.- Data Center

Componentes necesarios para la propuesta del Data Center de la Fiscalia Departamental de Tarija.

Descripción	**Cantidad**	**Precio Unitario**	**Total**
Armario Rack 22U 600x600 a suelo 19	2	Bs. 3500	Bs. 7,000
UPS EN LÍNEA 3KVA/2700W, 6 SLDS, SI-NUS, TORRE/BASTIDOR- 220V	2	Bs. 10,000	Bs. 20,000
Cable UTP Cat. 6	150 mtrs	Bs. 5	Bs. 750
Conector RJ45 para Cable UTP Cat 6	15	Bs. 3	Bs. 45
Patch Panel CAT6 48P	1	Bs. 500	Bs. 550
Patch Panel CAT6 24P	1	Bs. 250	Bs. 250
Organizador horizontal 2RU	2	Bs. 147	Bs. 296
Regleta para montaje en Bastidor 220V AC	2	200	400
Canaletas para Cables: - Canaletas 30x20x2000mm Autoadhesivas -Bandeja Rejilla VIAFIL CINCADO Z3 100x100mmx4m(Para el cableado horizontal)	 3 4	 Bs. 20 Bs. 82	 Bs. 60 Bs. 328
Piso Falso: Unidad Kg	Aprox: 56	Bs. 3.50	Bs. 196
Unidad m	Aprox: 56	Bs. 10	Bs. 560
Unidad Ud	Aprox: 25	Bs. 30	Bs. 750
Unidad Ud	Aprox: 81	Bs. 20	Bs. 1620

Unidad m2	Aprox: 56	Bs. 35	Bs. 1960
Unidad Ud	Aprox: 25	Bs. 30	Bs. 750
Mano de Obra Especialista en Montaje	H: 8-12;2-6	Bs. 50 x día	Bs. 300(6 días)
Ayudante en Montaje	H: 8-12;2-6	Bs. 35 x día	Bs. 210(6 días)
Aire de precisión WESTRIC L. DW-003 UI	1	Bs. 40,000	Bs. 40,000
Panel Led Sobreponer 18W-6500K L. Bl.	2	Bs. 50	Bs. 100
Cámara IP Domo metálica	1	Bs. 550	Bs. 550
AJAX - FireProtect 2 Detección de Incendios	1	Bs. 2,000	Bs. 2,000
Lector Biometrico de huella digital MA300	1	Bs. 1,500	Bs. 1,500
Extintor CO2 de 6 Kilos (Dióxido de Carbono)	1	Bs. 400	Bs. 400
Interruptor Conmutador 10A -250V Blanco	1	Bs. 15	Bs. 15
2 Tomacorrientes U.10a-15A -250V B.	2	Bs. 20	Bs. 40
Esmalte Epoxico en Blanco	2	Bs. 130	Bs. 260
Puerta de Seguridad para Acceso	1	Bs. 2,700	Bs. 2,700
Dell i7 6 Gen	1	-	-

Tabla 24. *Costos Referencias de equipos para el data center y el servidor*

3.5.3.- Costos Finales

Presupuesto necesario para los componentes del Data Center de la Fiscalia. Sujeto a cambios.

Descripción	**Total**
Data Center	83,590
Total	**83,590**

Tabla 25. *Costos Finales de Equipos*

COMPONENTE II

Configuración del servidor de Monitoreo en Tiempo Real

4.- Componente II: Configuración del Servidor de Monitoreo en Tiempo Real

4.1.- Fase 4: Configuración de Servidor Observium de Monitoreo en Tiempo Real

4.1.1.- Historia y Evolución de Observium

Observium es una herramienta de monitoreo de redes diseñada para facilitar la supervisión de la infraestructura de red mediante el descubrimiento automático de dispositivos y la visualización de datos detallados. Creado inicialmente en 2006 por Adam Armstrong, Observium se ha desarrollado a lo largo de los años para convertirse en una solución robusta que integra diversas funcionalidades avanzadas, abordando las necesidades de monitoreo en entornos de red modernos.

La evolución de Observium ha estado marcada por su capacidad para adaptarse a las demandas cambiantes de la industria de redes, incorporando características que mejoran la eficiencia y la precisión del monitoreo. Desde su concepción, la herramienta ha pasado de ser un proyecto personal a una plataforma ampliamente utilizada por organizaciones de diferentes tamaños, con un enfoque en la simplicidad de uso y la amplia compatibilidad con diversos dispositivos y sistemas operativos.

4.1.2.- Funcionalidades Principales

4.1.2.1.- Descubrimiento Automático de Dispositivos

Una de las características más destacadas de Observium es su capacidad para el descubrimiento automático de dispositivos en la red. Utilizando protocolos como SNMP (Simple Network Management Protocol), ICMP (Internet Control Message Protocol), y LLDP (Link Layer Discovery Protocol), Observium escanea la red para identificar y mapear dispositivos, reduciendo significativamente el tiempo y esfuerzo requeridos para la configuración inicial.

El descubrimiento automático facilita la identificación de dispositivos como routers, switches, servidores, y equipos de almacenamiento, proporcionando una visión integral de la infraestructura de red y permitiendo una supervisión continua sin intervención manual constante.

4.1.3.- Visualización de Datos

Observium ofrece una interfaz gráfica intuitiva para la visualización de datos de monitoreo. Los datos recopilados se presentan en forma de gráficos y tablas que muestran métricas clave como el uso de la CPU, la memoria, el ancho de banda, y la latencia. Esta visualización detallada permite a los administradores de red identificar rápidamente anomalías y tendencias, mejorando la capacidad de respuesta ante problemas potenciales.

La capacidad de generar reportes y visualizar el rendimiento de la red en tiempo real y de manera histórica es crucial para la planificación de capacidad y la optimización de recursos, proporcionando información valiosa para la toma de decisiones.

4.1.4.- Beneficios y Limitaciones

4.1.4.1.- Beneficios

Observium proporciona numerosos beneficios que mejoran la gestión y el monitoreo de redes. Entre ellos se incluyen:

- **Automatización:** La capacidad de descubrimiento automático reduce la carga de trabajo manual y acelera el proceso de configuración.
- **Visibilidad:** La visualización de datos en tiempo real y la generación de reportes detallados proporcionan una visión clara y completa del rendimiento de la red.
- **Alertas Proactivas:** Las alertas automáticas basadas en umbrales permiten una respuesta rápida a problemas, minimizando el impacto en el servicio.
- **Compatibilidad:** Observium es compatible con una amplia gama de dispositivos y sistemas, facilitando su integración en entornos de red heterogéneos.

4.1.4.2.- Limitaciones

Sin embargo, Observium también presenta algunas limitaciones, como:

- **Dependencia de SNMP**: Observium depende en gran medida de SNMP para la recopilación de datos, lo que puede ser una limitación en redes que no soportan este protocolo.
- **Requiere Mantenimiento:** Como cualquier herramienta de software, Observium requiere actualizaciones y mantenimiento regular para asegurar su funcionamiento óptimo y la seguridad de la red.

4.1.5.- Comparativa con otras herramientas de Monitoreo

Comparado con otras herramientas de monitoreo de redes como Nagios, Zabbix, o PRTG, Observium destaca por su enfoque en la simplicidad y la automatización. Mientras que Nagios es conocido por su flexibilidad y capacidad de integración con una amplia gama de plugins, puede ser más complejo de configurar y mantener. Zabbix ofrece características avanzadas de monitoreo, pero puede requerir una mayor inversión en tiempo para su configuración y operación. PRTG proporciona una solución integral con una interfaz amigable, pero su modelo de licenciamiento puede resultar costoso para organizaciones más grandes.

Observium, por su parte, se posiciona como una solución intermedia, ofreciendo una buena combinación de funcionalidad, facilidad de uso y automatización, lo que lo hace ideal para organizaciones que buscan una herramienta de monitoreo eficiente sin la complejidad de las soluciones más avanzadas.

4.1.6.- Rendimiento del servidor

El rendimiento del servidor en tiempo real Observium mide a través de diversas métricas y herramientas integradas en esta plataforma de monitoreo. Observium recopila datos de los dispositivos de red, los organiza y los presenta en gráficos y tablas detallados.

- **Uso de recursos del sistema**

CPU: Observium monitorea el porcentaje de uso del procesador del servidor, lo cual es clave para identificar si está siendo sobrecargado.

Memoria RAM: Registra el consumo de memoria para garantizar que no haya cuellos de botella que afecten el rendimiento.

Espacio en disco: Permite visualizar la capacidad utilizada y disponible en los discos, anticipando problemas por falta de almacenamiento.

- **Monitoreo del tráfico de red**

Ancho de banda: Mide la cantidad de datos enviados y recibidos a través de las interfaces de red del servidor.

Latencia y pérdida de paquetes: Analiza la calidad de la conexión para determinar posibles interrupciones o degradaciones en la red.

- **Temperatura y energía**

Observium puede monitorear sensores físicos (si están disponibles) para verificar la temperatura del hardware, evitando sobrecalentamientos que afecten el rendimiento.

- **Gráficos históricos y tendencias**

Observium ofrece gráficos de rendimiento que muestran datos históricos, lo que permite identificar patrones, prever problemas futuros y evaluar el impacto de las optimizaciones realizadas.

4.1.7.- Configuracion del Servidor Observium en Debian

Creación de Usuario Root

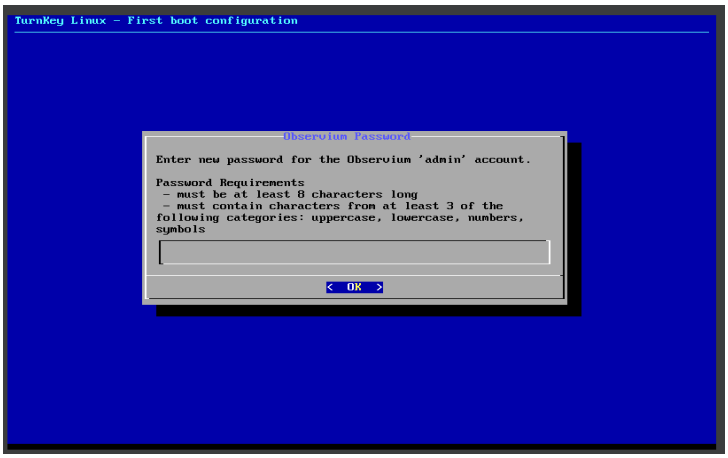


Figura 56. *Configuración de Creación de usuario Root en Servidor Observium*

Creación de Cuenta de Correo Electrónico

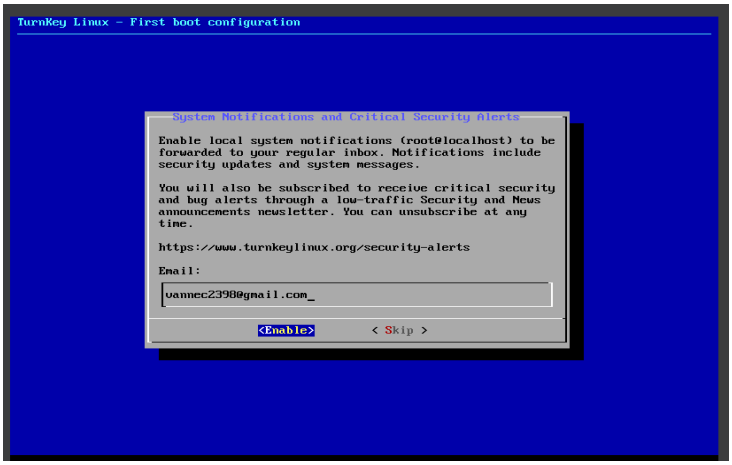


Figura 57. *Creación de Correo Electrónico para el Servidor*

Actualización de Servidor

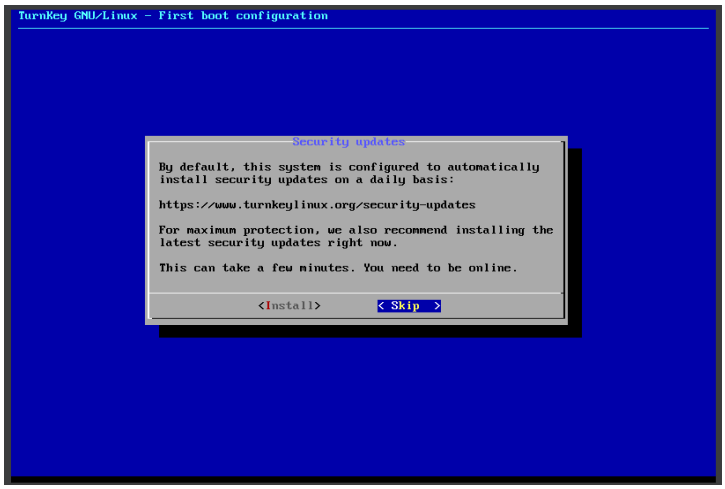


Figura 58. *Actualización de Servidor*

Instalación Finalizada Muestra la Dirección IP que Alojara al Servidor

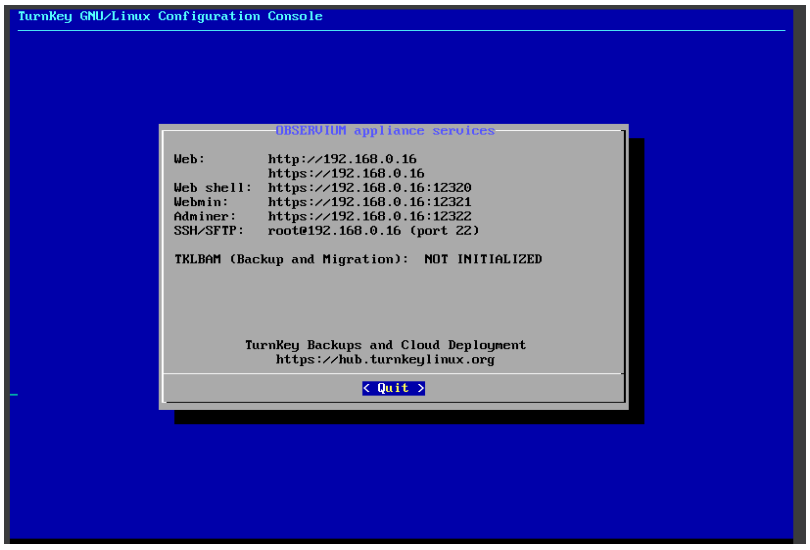


Figura 59. *Instalación Finalizada del Servidor con la IP de la Pagina Web*

Sitio Web de Servidor

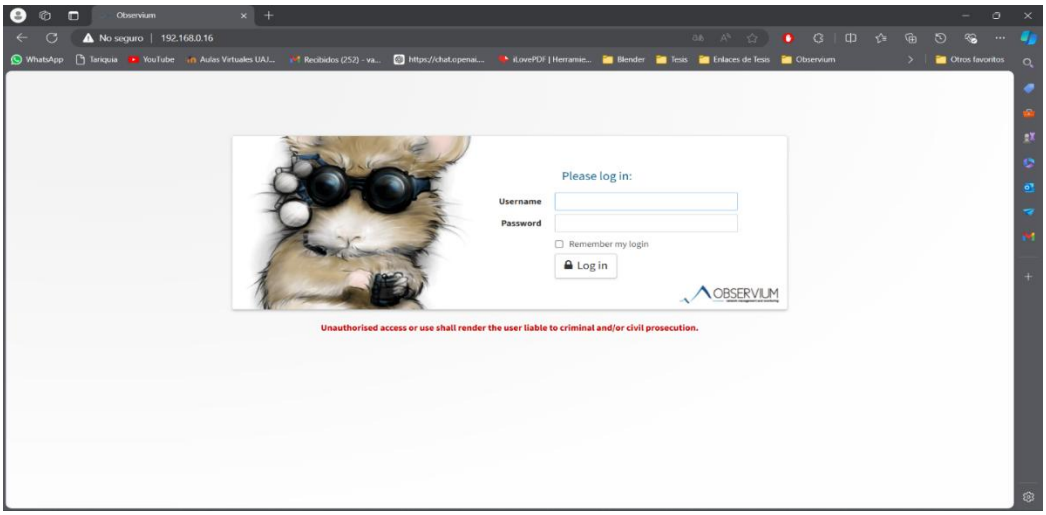


Figura 60. *Sitio Web del Servidor Observium*

4.1.8.- Instalación de Servicio de Protocolo SNMP en PC Windows

Comando: Get-WindowsCapability -Online -Name SNMP*

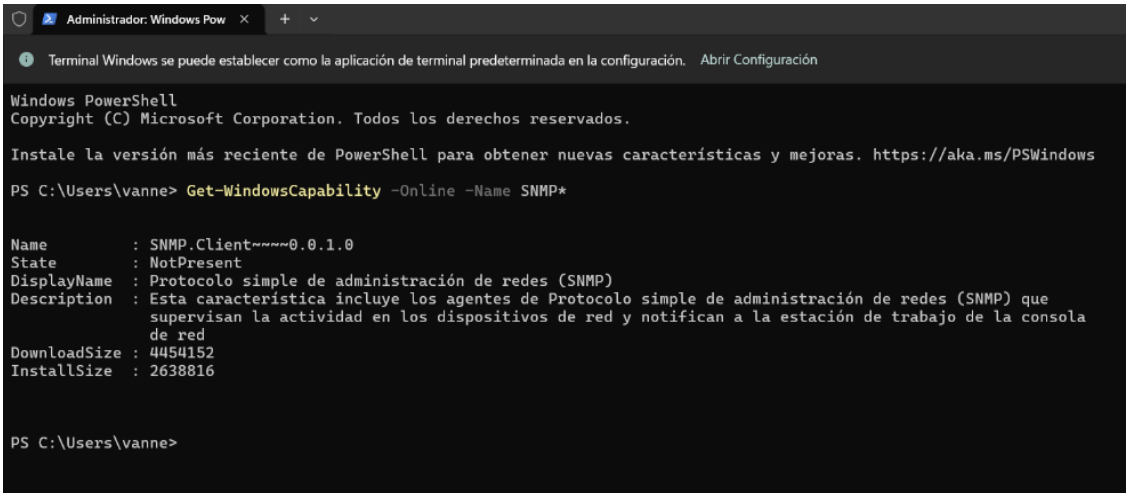


Figura 61. *Configuración de Instalación de Protocolo SNMP en Equipo de Windows*

Instalación con el comando Windows

Comando: Get-WindowsCapability -name SNMP*

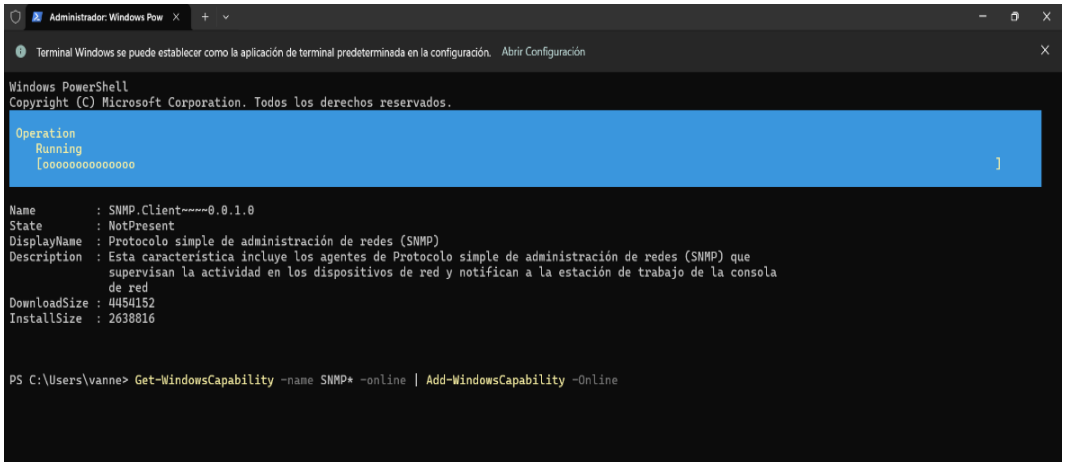


Figura 62. *Instalación y habilitación del Protocolo SNMP en Equipo Windows*

Verificación Servicio Activo

Comando: Get-WindowsCapability -name SNMP* -online | Add-WindowsCapability -Online

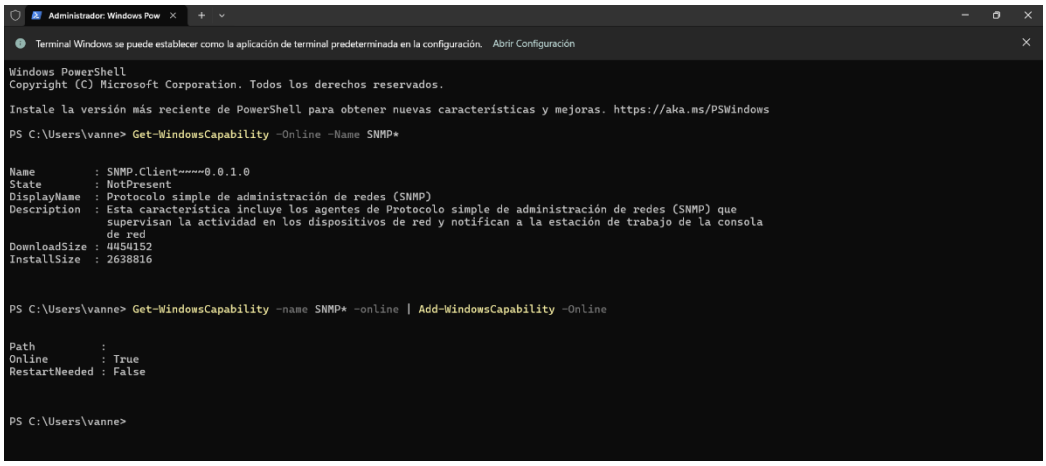


Figura 63. *Verificación de Protocolo SNMP Activo*

Modificación en protocolo para lectura

Comando: Añadir public en seguridad con lectura y escritura

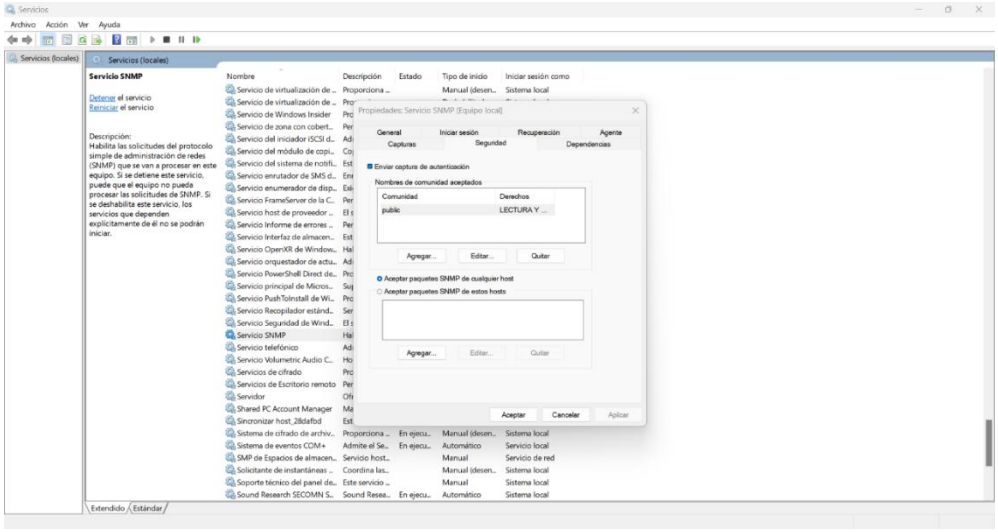


Figura 64. *Configuración y Modificación de Protocolo para Lectura y Escritura*

Verificación de IP de Pc para Adición en Servidor

Comando: ipconfig ; IP: **192.168.0.22**

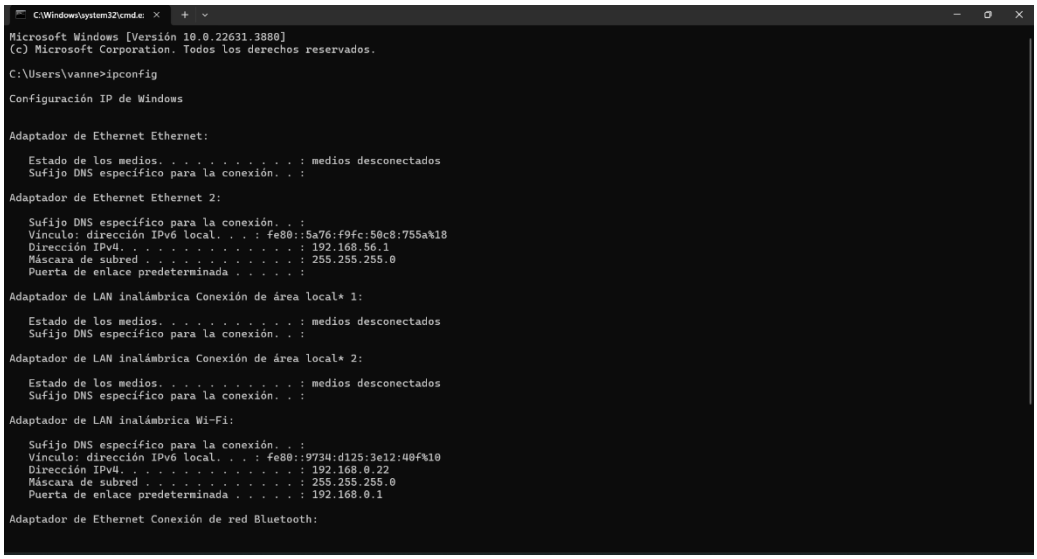


Figura 65. *IP de Equipo Windows*

4.1.9.- Instalación de Servicio de Protocolo SNMP en PC Linux

Comando Actualización de sistema: sudo apt-get update

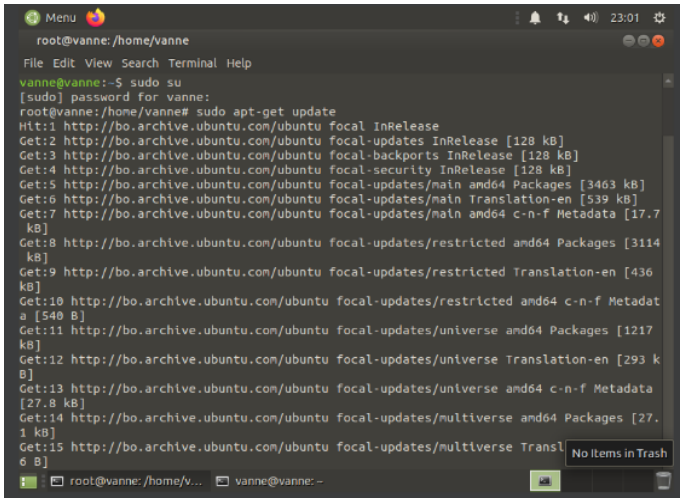


Figura 66. *Actualización de Servicios de Maquina Linux META*

Instalación con el comando Linux

Comando: sudo apt install snmp snmpd

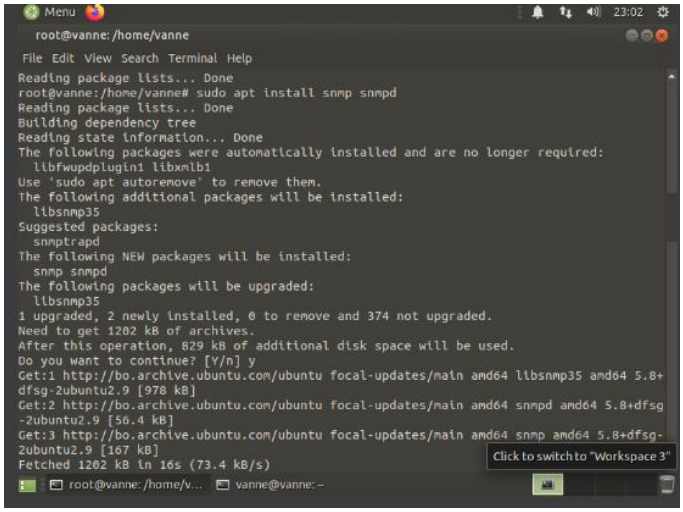


Figura 67. *Instalación de Servicio de Protocolo SNMP en Equipo Linux META*

Verificación Servicio Activo

Comando: sudo service snmpd status

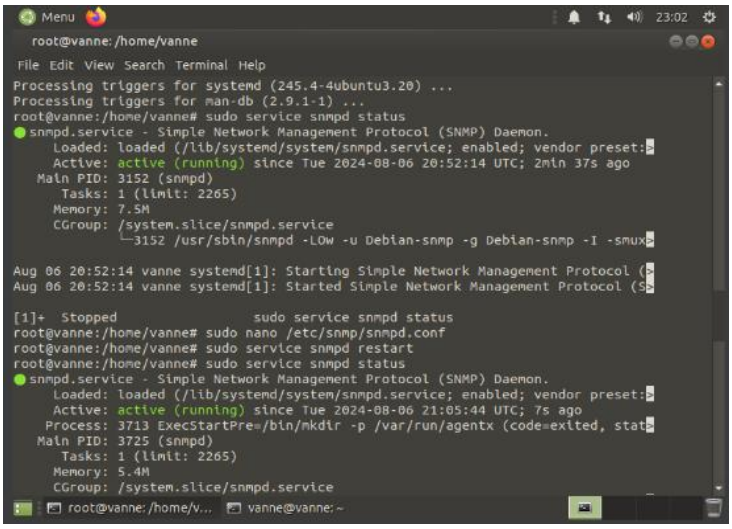


Figura 68. *Servicio de Protocolo SNMP Activo*

Configuración del archivo Snmpd.conf

Comando: sudo nano /etc/snmp/snmpd.conf

Configurar el **SysLocation:** Ubicación o Nombre de Usuario y **SysContact:** Contacto del usuario

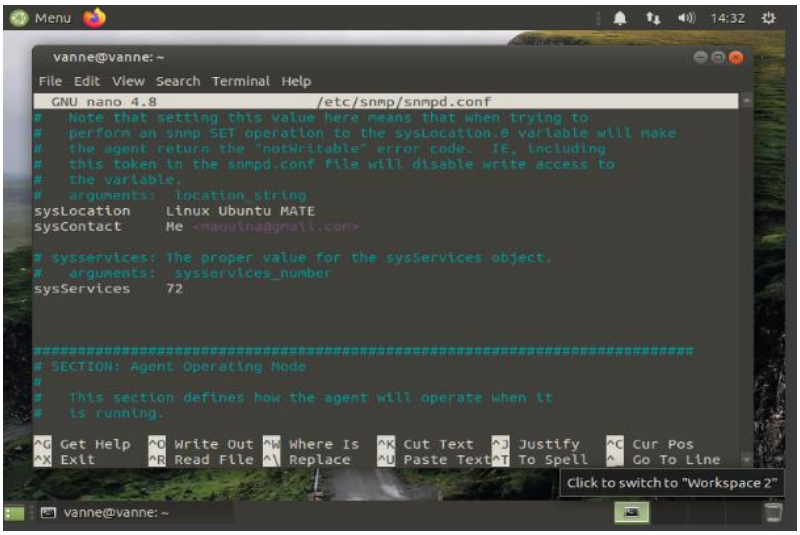


Figura 69. *Configuración de Archivo de Protocolo SNMP*

Comentar el primer agentaddress y escribir agentaddress udp:161 o en caso directo la direccion IP del equipo.

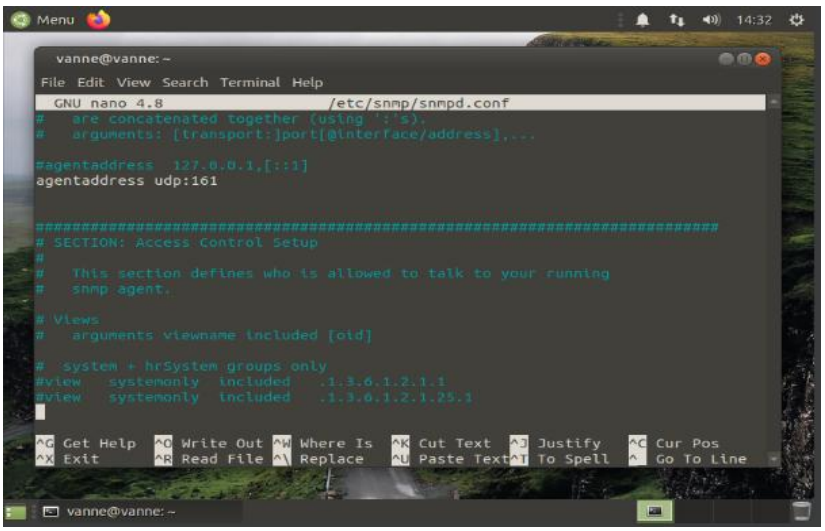


Figura 70. *Configuración de Datos en Archivo SNMP*

Comentar las 2 lineas de view systemonly included .1.3.6.1.2.1.1 y view systemonly included .1.3.6.1.2.1.25.1 y agregar rocommunity public 192.168.0.0/24(Direccion de maquina) o en caso contrario si se agregó la dirección en agentaddress solo escribir rocommunity public.

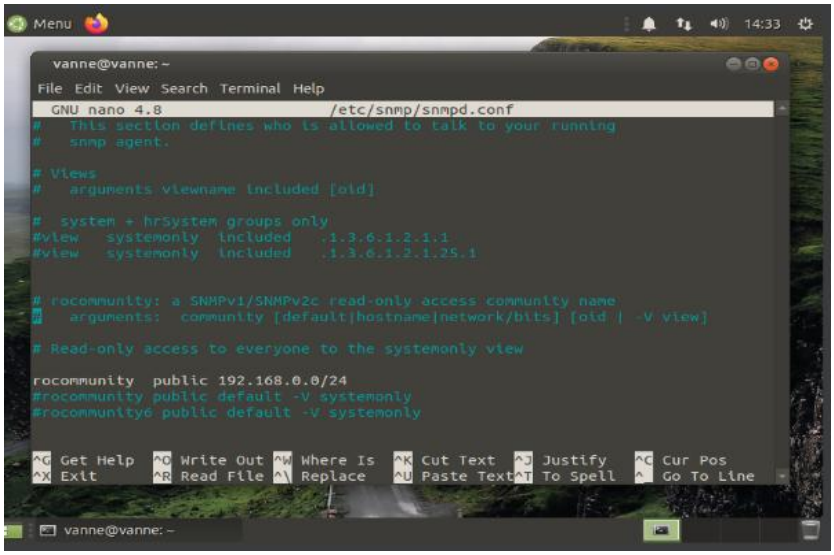


Figura 71. *Configuración de Comunidad de IP en Archivo SNMP*

Reiniciar el servicio SNMPD

Comando: sudo service snmpd restart, luego sudo service snmpd status.

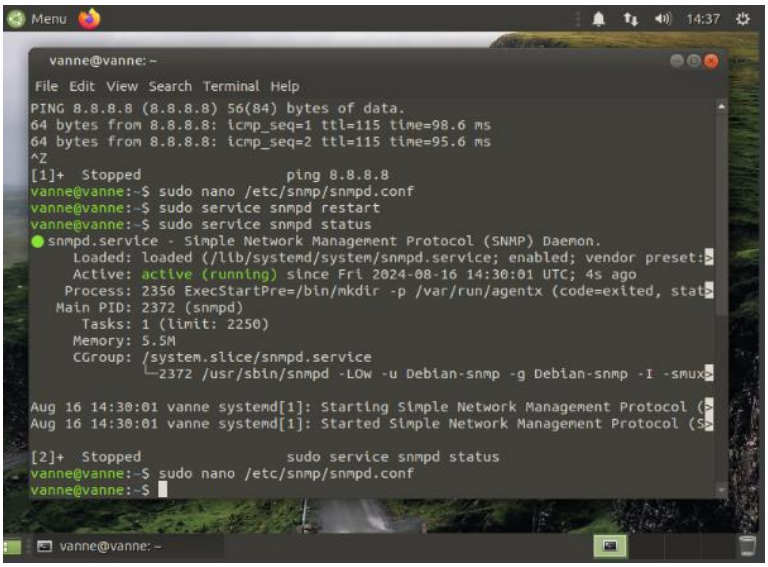


Figura 72. *Reinicio de Archivo SNMP*

Verificación de IP Linux MATE de Pc para Adición en Servidor

Comando: ifconfig; IP: **192.168.0.17**

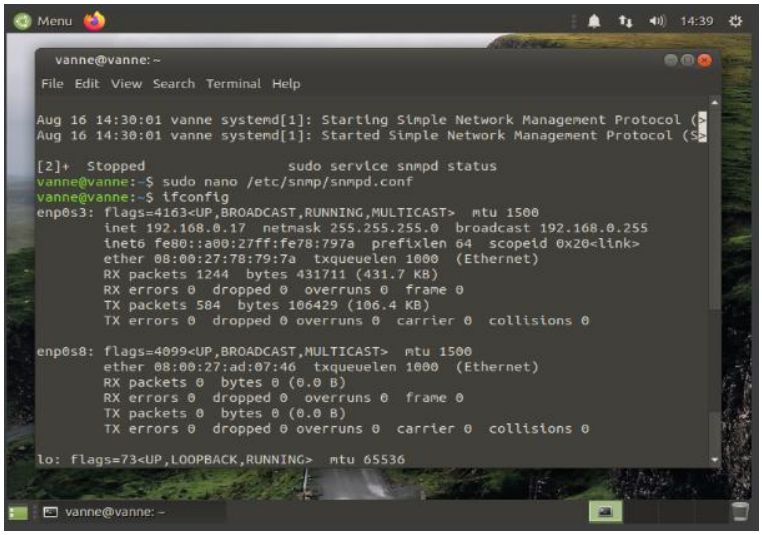


Figura 73. *IP de Equipo Linux MATE*

4.1.10.- Habilitación del Protocolo SNMP en Router Microtik

Habilitar: Enabled; **Location:** Nombre del lugar ubicado del equipo

Trap Community: public

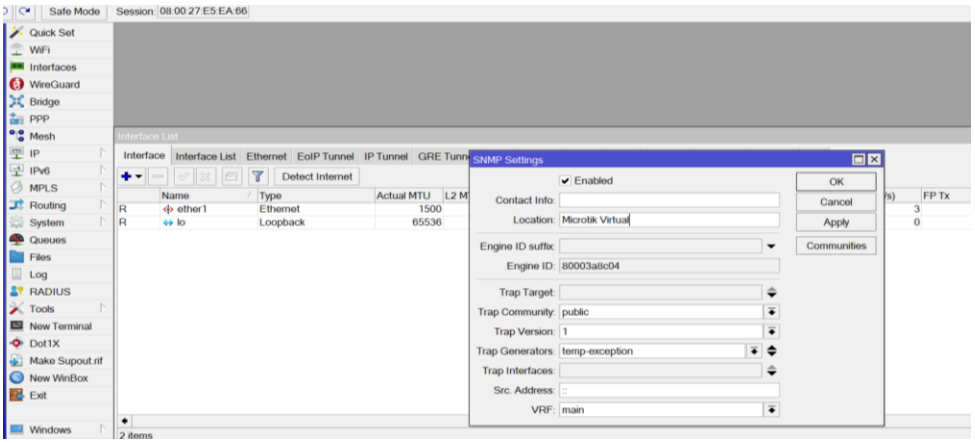


Figura 74. *Habilitación de Protocolo SNMP en Microtick*

IP del Equipo Router Microtick

La IP del equipo es **192.168.0.28/24**

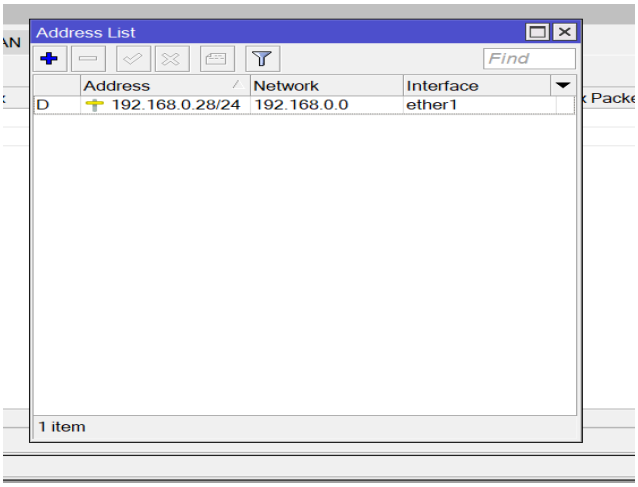


Figura 75. *IP de Equipo Router Microtick*

4.1.11.- Habilitación de IP de Equipos al Servidor Observium

Se observa la Interfaz Gráfica de la Web del Servidor

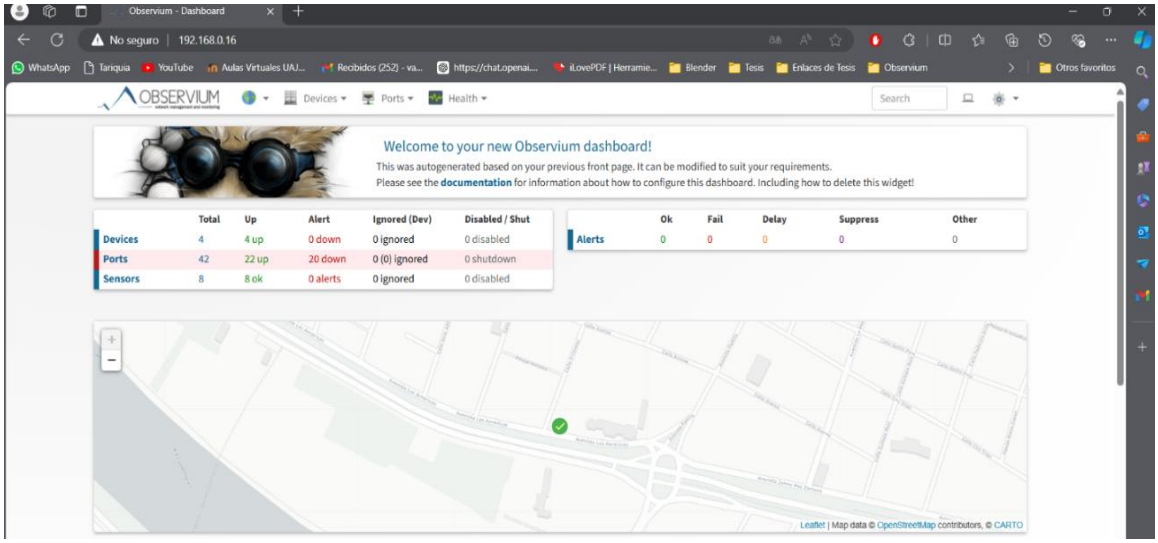


Figura 76. *Sitio Web del Servidor Observium*

Agregación de IP de los Equipos a Adicionar para el Monitoreo

Windows: 192.168.0.22 **Linux MINT:** 192.168.0.42

Linux MATE: 192.168.0.17 **Router Microtick:** 192.168.0.28

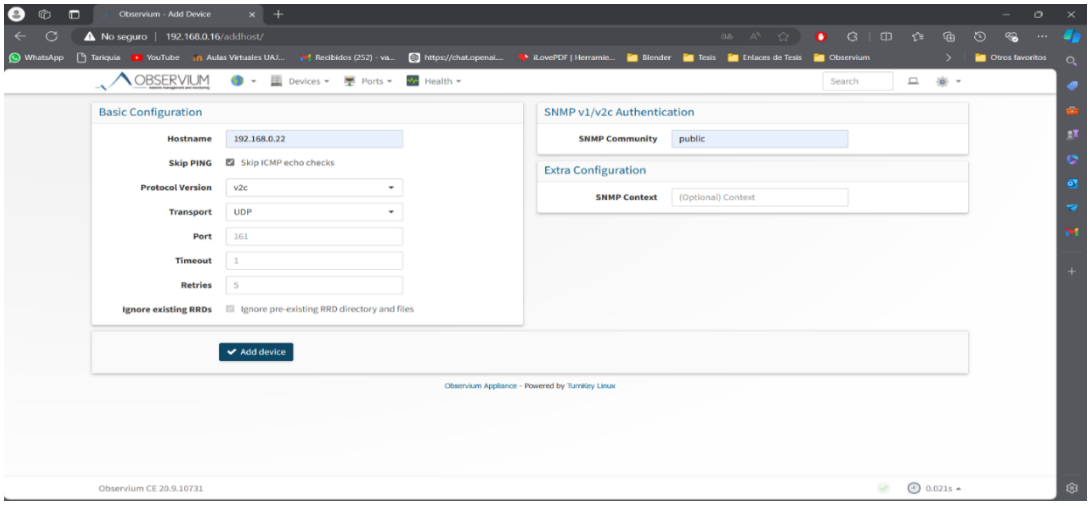


Figura 77. *Agregación de IP's de Equipos a Monitorear*

Esto se realiza con cada direccion IP de cada equipo, si la ip es incorrecta o la configuración del protococolo SNMP no está bien configurado mostrara un mensaje de que el protocolo

UDP(Protocolo de Transporte de Información) no ha establecido conexión al equipo, ya sea que en la parte para equipos de Windows o en la parte de la comunidad de public en lectura y escritura y en equipos de Linux el archivo sudo nano /etc/snmp/snmpd.conf o en otros equipos de red no se habilito el protocolo y no se configuraron correctamente.

Observación de Agregación de IP's en el Servidor Observium

Se observa que los 4 equipos se agregaron correctamente. Y el servidor tiene más opciones de visualización para poder ver cada equipo.

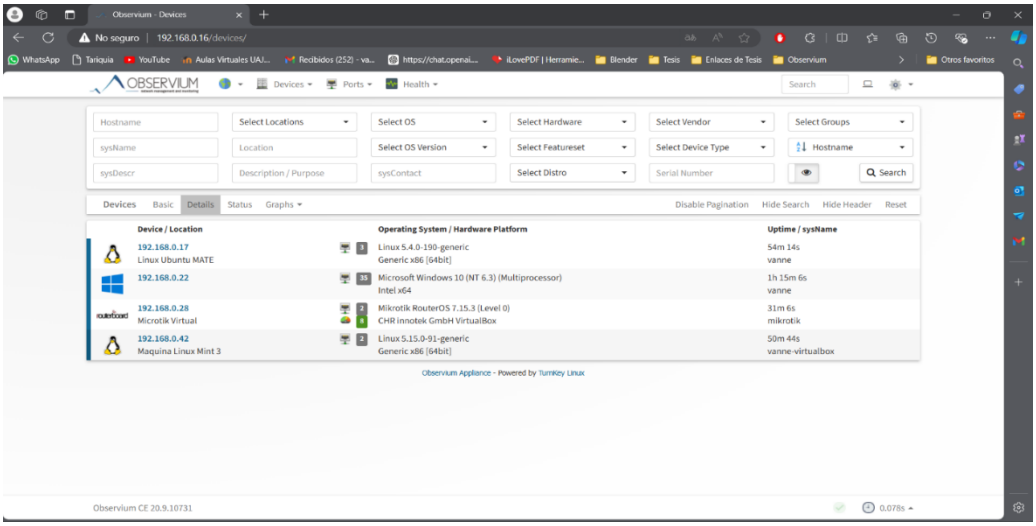


Figura 78. *Agregación de IP's de Equipos a Monitorear en el Servidor*

4.1.12.- Recopilación de Información del Servidor Observium de cada Equipo

Aquí se observa como monitorea y recopila toda la información técnica del equipo y como está trabajando cada segundo y va guardando toda la información importante para las gráficas cada segundo y que posteriormente el administrador pueda observar cómo trabajo el equipo en cada área importante del equipo como en el sistema, memoria, procesador, almacenamiento, red, puertos, temperatura, frecuencia, voltaje y demás, y así poder resolver los problemas de manera oportuna en el equipo.

Sistema: Muestra información general del sistema, incluyendo el nombre del host, sistema operativo, tiempo de actividad (uptime), y otros detalles relevantes como la versión del kernel en sistemas basados en Linux o la versión del sistema operativo en sistemas Windows.

Memoria: Observium monitorea la utilización de la memoria física (RAM) y la memoria de intercambio (swap). Proporciona gráficos detallados que muestran el uso de memoria en tiempo real y tendencias a lo largo del tiempo, permitiendo identificar picos de uso o situaciones de escasez de memoria.

Procesador (CPU): Recoge datos sobre la utilización de la CPU, incluyendo el porcentaje de uso global y por núcleo. Observium también puede mostrar el promedio de carga de la CPU a lo largo del tiempo, lo que es útil para detectar cuellos de botella o procesos que consumen muchos recursos.

Almacenamiento: Monitorea el uso de almacenamiento en discos duros, unidades SSD y otros dispositivos de almacenamiento. Muestra el espacio total, utilizado y libre, así como el porcentaje de uso de cada partición o volumen.

Red: Proporciona información detallada sobre las interfaces de red, incluyendo estadísticas de tráfico (entrada/salida), errores, colisiones, y el estado de cada interfaz (up/down). Además, permite monitorear el rendimiento de las interfaces y el uso de ancho de banda.

Puertos: Observium puede monitorear los puertos en dispositivos de red como switches y routers, proporcionando detalles sobre el estado del puerto, tráfico, y cualquier anomalía detectada como errores o paquetes descartados.

Temperatura: Monitorea los sensores de temperatura en el equipo, mostrando lecturas actuales y tendencias a lo largo del tiempo. Esto es crucial para prevenir el sobrecalentamiento que podría dañar componentes del hardware.

Frecuencia: Observium puede registrar la frecuencia de operación de ciertos componentes, como la frecuencia del CPU o de las interfaces de red, permitiendo verificar que los dispositivos funcionan dentro de los parámetros esperados.

Voltaje: Proporciona lecturas de los sensores de voltaje en el equipo. Monitorear el voltaje es vital para asegurar que los componentes electrónicos reciben la energía adecuada sin sobrecargas ni caídas de tensión, que podrían causar inestabilidad o daño.

Registro de Eventos (Event Logging): El sistema registra eventos importantes, como cambios en el estado de los dispositivos, caídas de red, y otros eventos críticos. Estos logs son útiles para auditorías y análisis forense en caso de incidentes.

Gestión de Dispositivos (Device Management): Observium soporta una amplia gama de dispositivos y sistemas operativos, incluyendo routers, switches, servidores, estaciones de trabajo,

y más. Es compatible con dispositivos de múltiples fabricantes como Cisco, Juniper, HP, Dell, entre otros. Observium detecta automáticamente la mayoría de los dispositivos y ajusta su monitoreo según las capacidades del hardware.

Gráficos Históricos y Tendencias: Observium proporciona gráficos detallados que muestran tendencias históricas de las métricas monitoreadas. Esto es especialmente útil para realizar análisis de capacidad, planificación de recursos, y detectar patrones que podrían indicar problemas futuros.

Soporte para Protocolos de Monitoreo: Observium es compatible con una variedad de protocolos de monitoreo como SNMP (Simple Network Management Protocol), IPMI (Intelligent Platform Management Interface), y otros. Esto le permite recopilar información detallada desde diferentes tipos de dispositivos y sistemas operativos.

Gestión de MIBs (Management Information Base): Observium incluye una amplia colección de MIBs que facilitan la interpretación de datos específicos del fabricante obtenidos a través de SNMP. Esto permite un monitoreo más preciso y detallado de dispositivos que utilizan MIBs propietarias.

Gestión de Usuarios y Roles: Observium permite la gestión de usuarios con distintos roles y permisos, lo que facilita la administración de acceso en equipos de trabajo. Los roles pueden ser configurados para restringir o permitir acceso a diferentes partes del sistema según sea necesario.

Monitoreo de Servicios y Aplicaciones: Además de monitorear hardware, Observium también puede rastrear servicios y aplicaciones específicos, como servidores web (HTTP), servidores de correo (SMTP), bases de datos (MySQL), entre otros. Esto proporciona una visión completa de la disponibilidad y rendimiento de los servicios críticos.

Documentación y Etiquetado de Dispositivos: Permite agregar documentación adicional a cada dispositivo, como etiquetas personalizadas, notas, y otra información relevante. Esto ayuda a mantener un inventario bien documentado y a facilitar la gestión de activos.

Cada uno de estos parámetros es crucial para el monitoreo y mantenimiento efectivo de los sistemas y redes. Observium facilita la visualización y análisis de estos datos a través de gráficos y alertas, ayudando a mantener la salud y rendimiento de la infraestructura.

4.1.12.1.- Datos Recopilados de cada Equipo Monitoreado

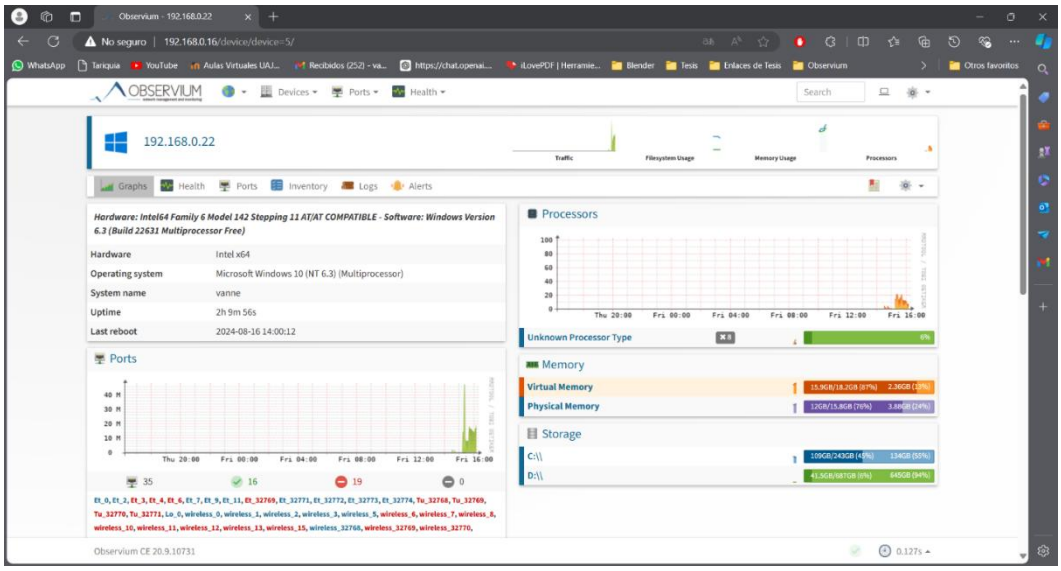


Figura 79. *Datos Recopilados por el Servidor del Equipo Windows*

Equipo Linux MATE IP

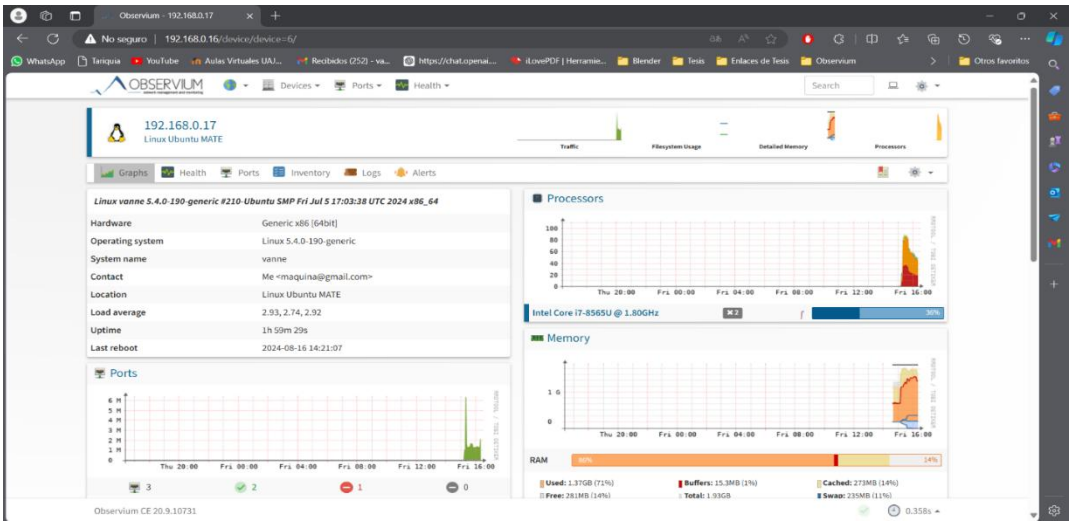


Figura 80. *Datos Recopilados por el Servidor del equipo Linux MATE*

Equipo Linux MINT IP

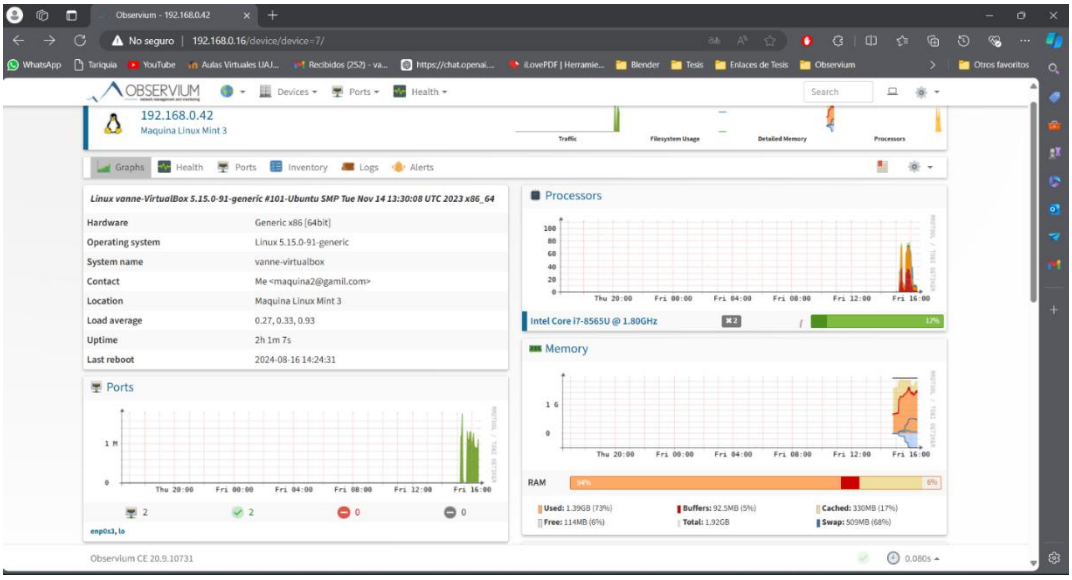


Figura 81. *Datos Recopilados por el Servidor del equipo Linux MINT*

Equipo MICROTIK IP

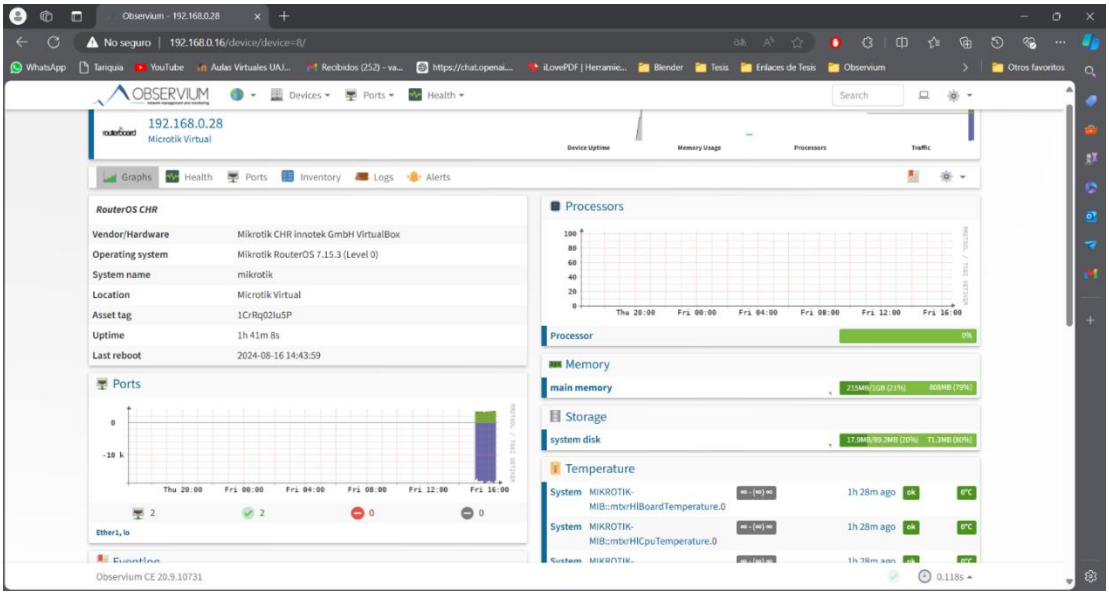


Figura 82. *Datos Recopilados por el Servidor del equipo Router Microtik*

4.1.13.- Datos Recopilados por Tipo de Información de los Equipos

Puertos

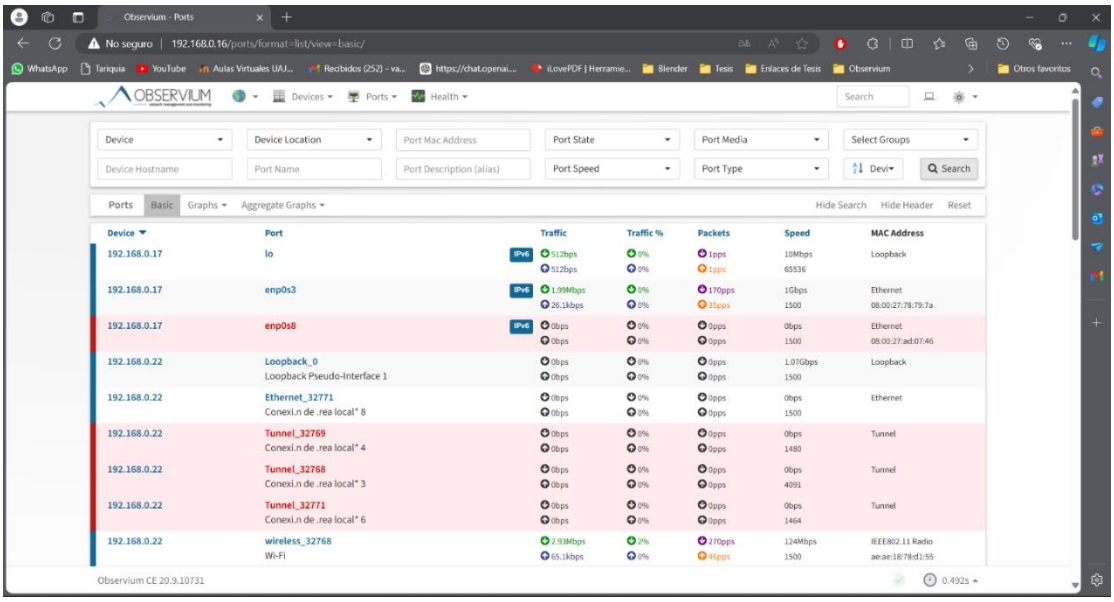


Figura 83. *Datos Recopilados por el Servidor de los puertos de cada Equipo*

Procesadores

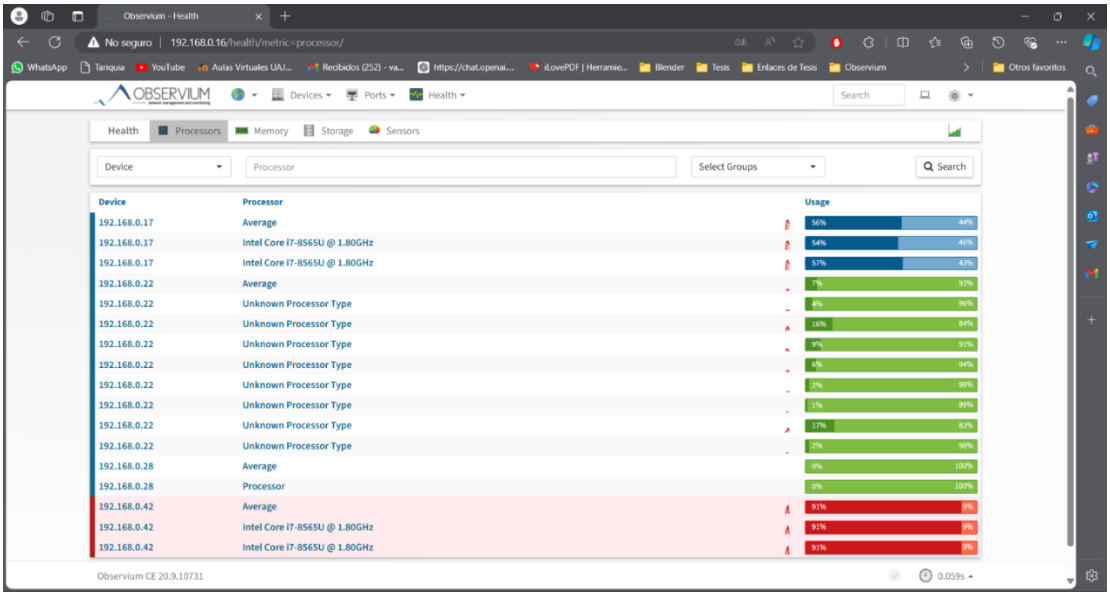


Figura 84. *Datos Recopilados por el Servidor de los Procesadores de cada Equipo*

Memoria

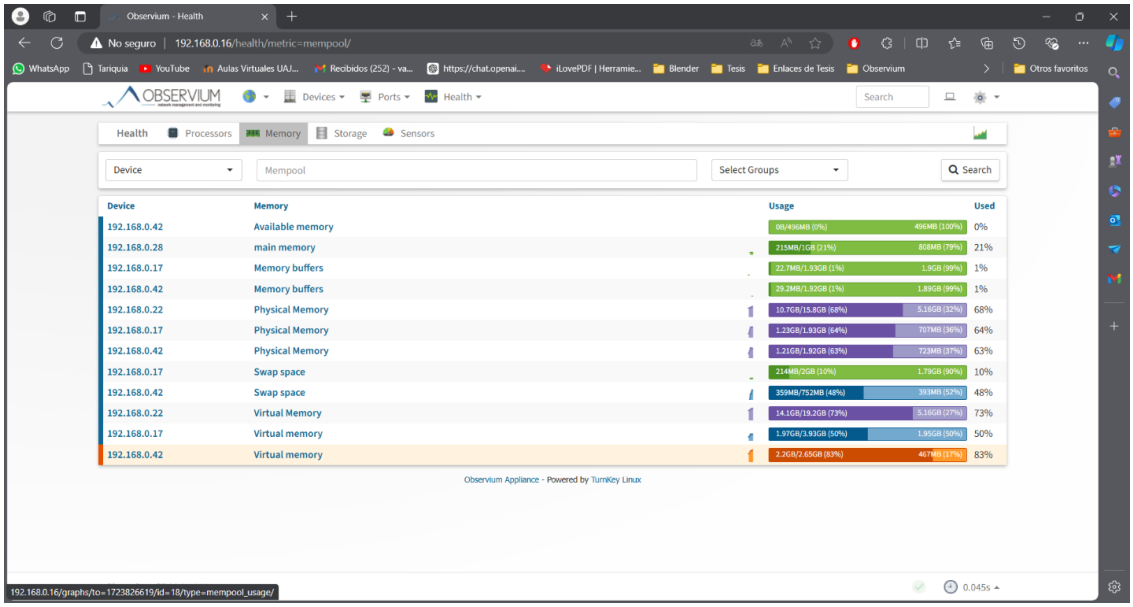


Figura 85. *Datos Recopilados por el Servidor de la Memoria de cada Equipo*

Almacenamiento

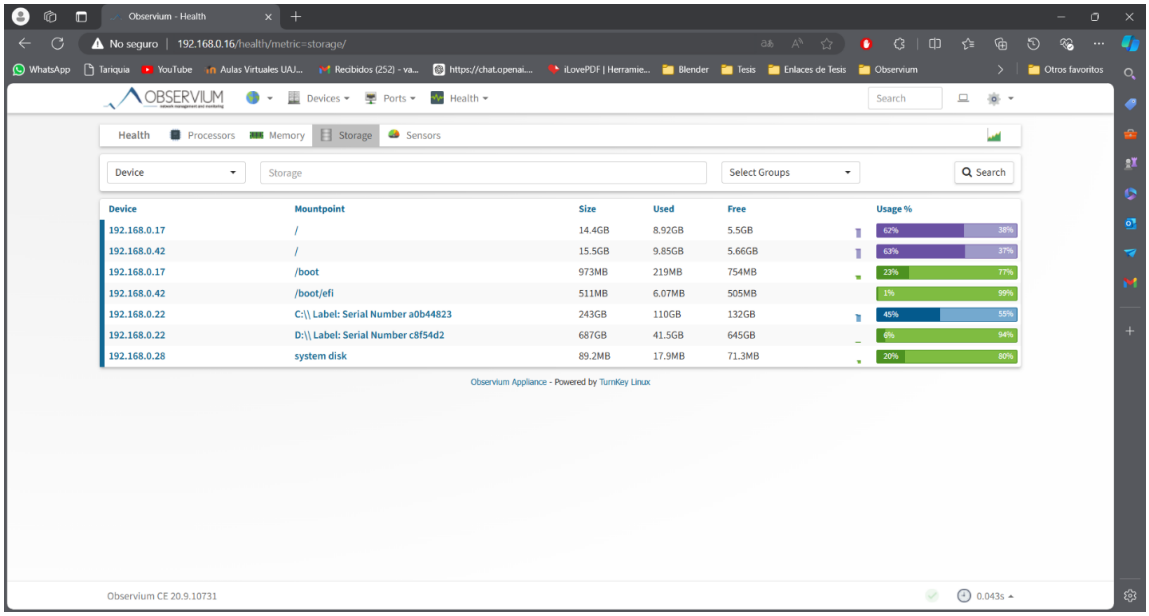


Figura 86. *Datos Recopilados por el Servidor del Almacenamiento de cada Equipo*

Sensores

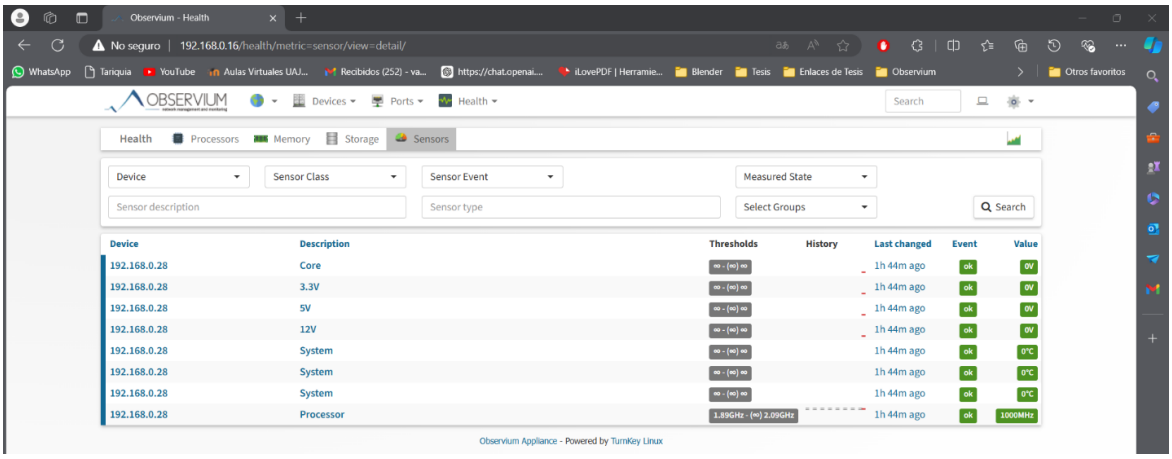
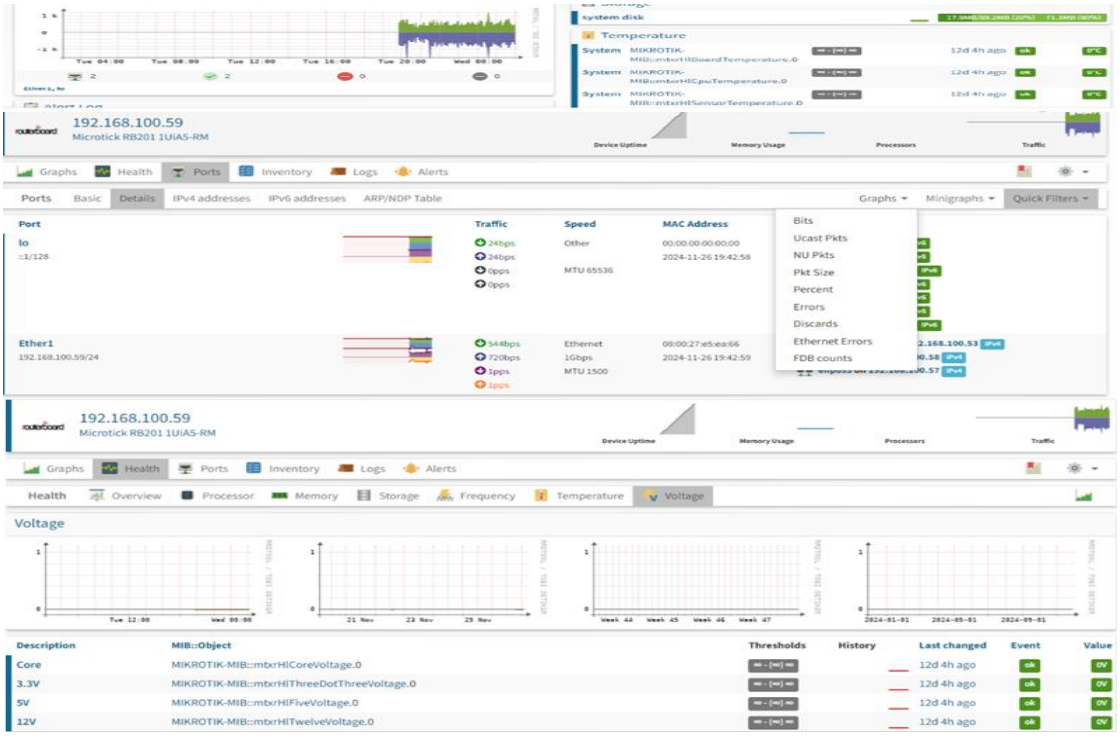


Figura 87. *Datos Recopilados por el Servidor de los Sensores*

4.1.14.- Pruebas de Monitoreo de equipos para el data center

Router Microtick

Figura 88*. Datos Recopilados de Router Microtick*



Switch TP-LINK

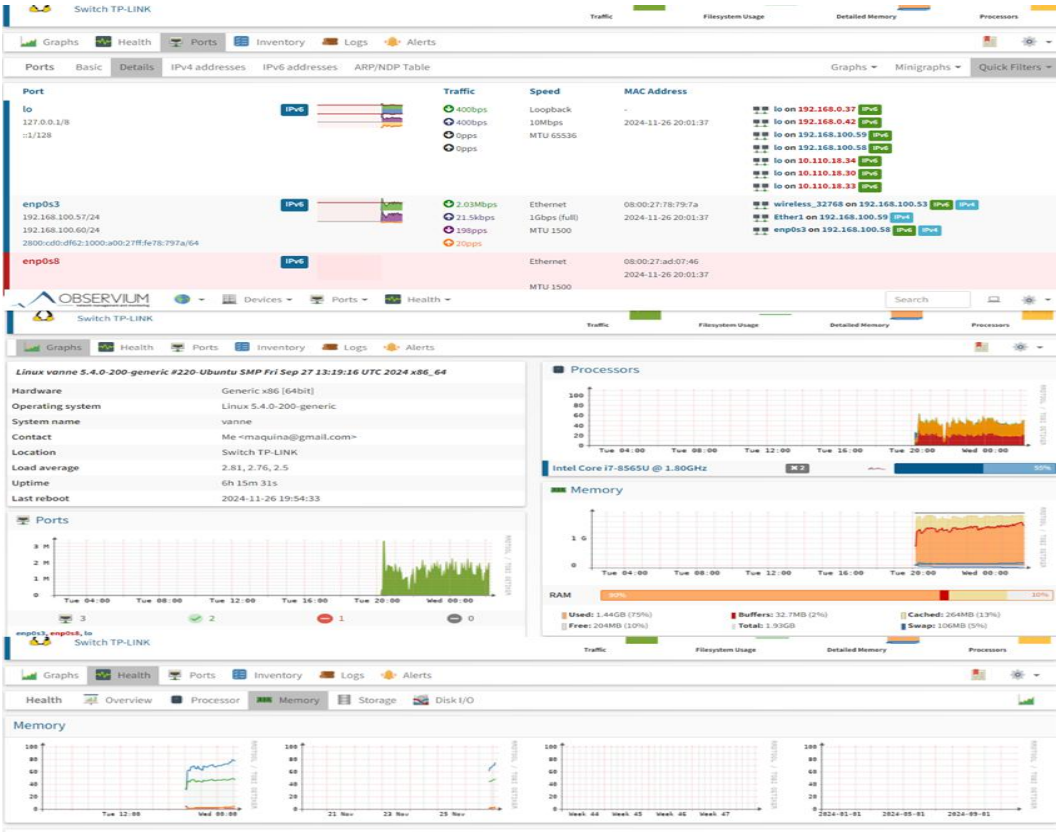


Figura 89. *Datos Recopilados de 4.1.14.2 Switch TP-LINK*

Switch Alhua

Figura 90. *Datos Recopilados de Switch Alhua*

Fortigate 90G

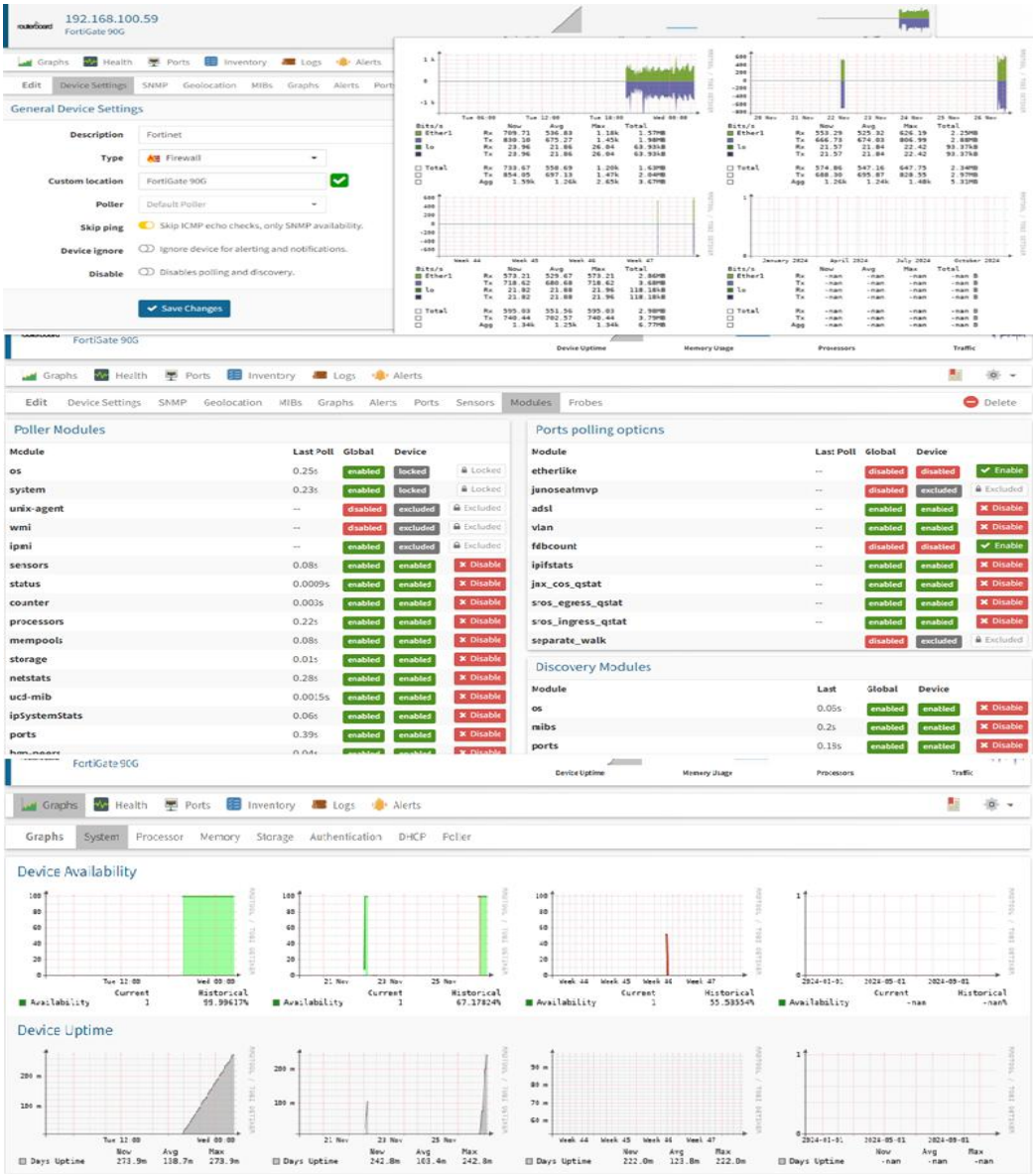


Figura 91. *Datos Recopilados de Fortigate 90G*

PDU Visión H CCV Security

***Figura 92**.Datos Recopilados de PDU Visión H CCV Security*

Capitulo IV

CONCLUSIONES Y RECOMENDACIONES

5.- Conclusiones y Recomendaciones

5.1.- Conclusiones

Mediante el diseño del Data Center bajo la norma ISO/IEC 22237 y la Configuración del servidor de monitoreo en tiempo real se pudo concluir:

- Las prácticas en la institución, junto al ingeniero de sistemas, permitieron identificar claramente los problemas que afectan la infraestructura tecnológica de la Fiscalía Departamental de Tarija. Se constató la falta de seguridad en los equipos de red, fallos recurrentes en dispositivos, la ausencia de un mantenimiento adecuado, y la carencia de etiquetado en routers, switches y otros dispositivos críticos. Estos problemas influyen directamente en la eficiencia operativa y seguridad de la red.
- El diseño del Data Center se fundamentó en la metodología TOP-DOWN, permitiendo abordar cada fase del proceso de manera secuencial y meticulosa. Se identificaron claramente aspectos clave como el cronograma, presupuesto y medidas de seguridad, asegurando que el proyecto se adapte a las necesidades específicas de la institución y garantice la continuidad operativa.
- A través del análisis y los datos recopilados, se diseñó un modelo de Data Center y la configuración del servidor (Observium) de monitoreo en tiempo real aptos para las exigencias tecnológicas de la institución. La implementación de este proyecto solucionaría las deficiencias en la infraestructura tecnológica, optimizando el rendimiento y facilitando el mantenimiento continuo.
- La aplicación de normas internacionales, como la ISO/IEC 22237, permitió alinear el diseño del Data Center con los estándares de eficiencia y seguridad reconocidos a nivel mundial. Esto garantiza que la infraestructura esté preparada para enfrentar futuros desafíos tecnológicos y que el proyecto sea sostenible en el tiempo.
- El proyecto no solo permitió adquirir conocimientos teóricos y prácticos en el diseño e implementación de Data Centers, sino que también habilitó la transferencia de estos conocimientos al contexto educativo, específicamente en la red de la Fiscalía Departamental de Tarija, lo que refleja la aplicabilidad de las soluciones propuestas en otras instituciones.
- La implementación del servidor de monitoreo Observium resultó ideal por su capacidad de ofrecer una visión completa de la red y un monitoreo eficiente en tiempo real. Observium

facilita la identificación temprana de problemas, mejorando la gestión de la infraestructura tecnológica y garantizando su seguridad y estabilidad.

5.2.- Recomendaciones

- Crear un plan de mantenimiento preventivo y correctivo para identificar y resolver fallos de manera oportuna.
- Implementar un sistema de etiquetado adecuado para facilitar la identificación de los equipos y el cableado en general.
- Mantener el diseño del Data Center alineado con normas ISO/IEC 22237 y actualizar conforme evolucionen los estándares.
- Ampliar el monitoreo en tiempo real para cubrir toda la red administrativa y mejorar la supervisión.
- Realizar evaluaciones regulares para ajustar las soluciones a las necesidades cambiantes de la infraestructura tecnológica.

5.3.- Medios de Verificación

5.3.1.- Tabla de Cumplimiento del Data Center según la Norma ISO/IEC 22237

Categoría	Criterio	Descripción/ Especificación	Cumpl. (Sí/No)	Comentarios
Infraestructura Física				
Espacio Adecuado	Dimensiones mínimas del espacio según la norma.	Cumple con las dimensiones adecuadas para servidores y racks	Si	Lugar apropiado según los requisitos que pide la norma.
Acceso Controlado	Control de acceso mediante sistemas de seguridad física.	Verificación de cerraduras, biométricos, CCTV, etc.	Si	Nivel de Seguridad 2 con ingreso con control de acceso.
Sistemas de Energía				
Fuente de Energía	Energía redundante (N+1, N+2) según los estándares	Sistemas de UPS y generadores disponibles.	Si	UPS empotrados para cada rack.
Consumo Energético	Verificación de sistemas de	Equipos con medición de energía en tiempo real.	Si	Consumo de energía desde los UPS a instalar

	monitoreo de energía			
Climatización				
Ventilación	Sistema de climatización 24/7	Implementación de refrigeración según los parámetros ISO/IEC.	Si	Aire Acondicionado para refrigeración con entrada de aire frio adelante y caliente atrás.
Control de Temperatura	Control de temperatura y humedad adecuada.	Parámetros controlados según norma ISO/IEC	Si	Detector inalámbrico de humo y calor que se activa al superar la temperatura adecuada.
Cableado y Red				
Estructura del Cableado	Diseño estructurado de cableado de datos y energía.	Instalación de cableado certificado según la norma EIA/TIA 568B	Si	Se realizará cableado fijo y punto a punto como recomienda la norma.
Etiquetado de Equipos	Etiquetado del cableado y equipos de red.	Identificación adecuada de cables, routers, switches, etc.	Si	Etiquetado de los cables en ambos extremos del cable.
Seguridad				
Protección de Acceso y Incidentes	Clase a usar según la norma de Protección 2.	Control de Acceso, puerta de acero Antiincendios y Contraincendios.	Si	Se estableció la seguridad al tipo de tamaño de Data Center para infraestructura.
Normativas y Procedimientos				
Cumplimiento de Normas	Alineación con la norma ISO/IEC 22237	Toda la estructura diseñada y alineada con la norma	Si	Toda la documentación refleja la alineación con la norma.
Procedimientos de Mantenimiento	Recomendaciones para el mantenimiento de equipos	Recomendaciones de planes de mantenimiento preventivo y correctivo.	Si	Recomendaciones de planes de mantenimiento para el uso general.

Tabla 26. *Verificación de Cumplimiento del Data Center según la Norma*

5.3.2.- Medio de Verificación de Pruebas de red y consumos de energía

Router Entel

Figura 93. *Trafico de Mbps de Internet Entel*

Router Tigo

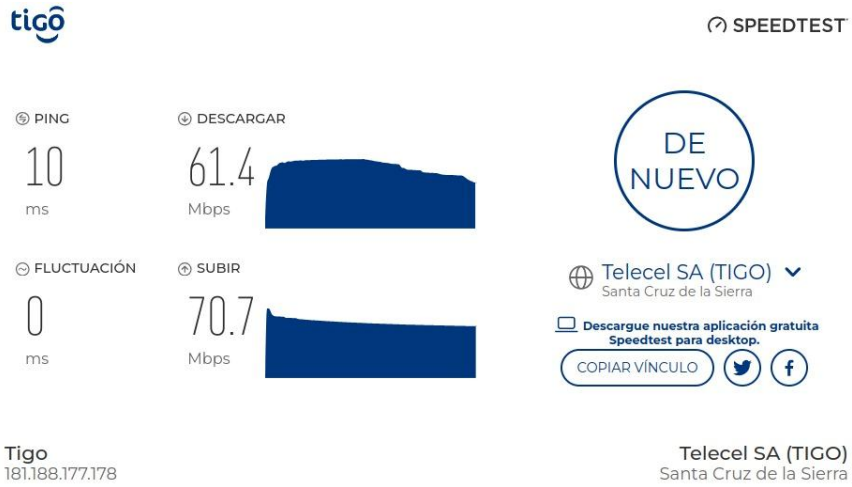
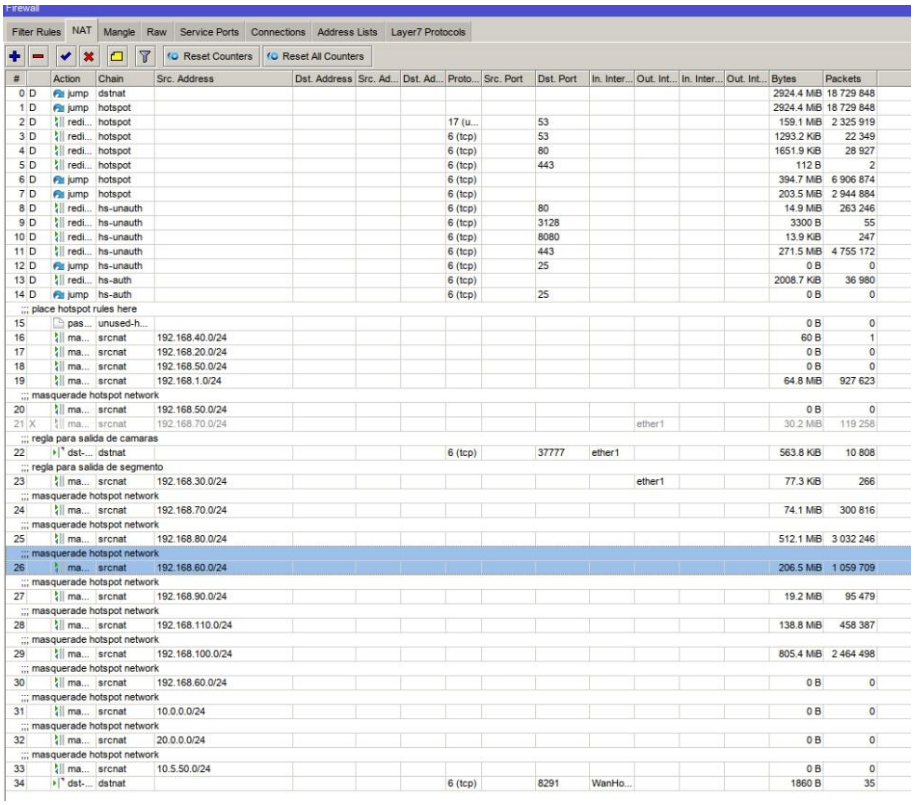


Figura 94. *Trafico de Mbps de Internet Tigo*

5.3.3.- Consumos de Red en Mbps y Kbps de cada Piso



#		Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Bytes	Packets
0	D	jump	dstnat												2924.4 MiB	18 729 848
1	D	jump	hotspot												2924.4 MiB	18 729 848
2	D	redi...	hotspot					17 (u...		53					159.1 MiB	2 325 919
3	D	redi...	hotspot					6 (tcp)		53					1293.2 KiB	22 349
4	D	redi...	hotspot					6 (tcp)		80					1651.9 KiB	28 927
5	D	redi...	hotspot					6 (tcp)		443					112 B	2
6	D	jump	hotspot					6 (tcp)							394.7 MiB	6 906 874
7	D	jump	hotspot					6 (tcp)							203.5 MiB	2 944 884
8	D	redi...	hs-unauth					6 (tcp)		80					14.9 MiB	263 246
9	D	redi...	hs-unauth					6 (tcp)		3128					3300 B	55
10	D	redi...	hs-unauth					6 (tcp)		8080					13.9 KiB	247
11	D	redi...	hs-unauth					6 (tcp)		443					271.5 MiB	4 755 172
12	D	jump	hs-unauth					6 (tcp)		25					0 B	0
13	D	redi...	hs-auth					6 (tcp)							2008.7 KiB	36 980
14	D	jump	hs-auth					6 (tcp)		25					0 B	0
		;;; place hotspot rules here														
15		pas...	unused-h...												0 B	0
16		ma...	srcnat	192.168.40.0/24											60 B	1
17		ma...	srcnat	192.168.20.0/24											0 B	0
18		ma...	srcnat	192.168.50.0/24											0 B	0
19		ma...	srcnat	192.168.1.0/24											64.8 MiB	927 623
		;;; masquerade hotspot network														
20		ma...	srcnat	192.168.50.0/24											0 B	0
21	X	ma...	srcnat	192.168.70.0/24								ether1			30.2 MiB	119 258
		;;; regla para salida de camaras														
22		dst-...	dstnat					6 (tcp)		37777	ether1				563.8 KiB	10 808
		;;; regla para salida de segmento														
23		ma...	srcnat	192.168.30.0/24								ether1			77.3 KiB	266
		;;; masquerade hotspot network														
24		ma...	srcnat	192.168.70.0/24											74.1 MiB	300 816
		;;; masquerade hotspot network														
25		ma...	srcnat	192.168.80.0/24											512.1 MiB	3 032 246
		;;; masquerade hotspot network														
26		ma...	srcnat	192.168.60.0/24											206.5 MiB	1 059 709
		;;; masquerade hotspot network														
27		ma...	srcnat	192.168.90.0/24											19.2 MiB	95 479
		;;; masquerade hotspot network														
28		ma...	srcnat	192.168.110.0/24											138.8 MiB	458 387
		;;; masquerade hotspot network														
29		ma...	srcnat	192.168.100.0/24											805.4 MiB	2 464 498
		;;; masquerade hotspot network														
30		ma...	srcnat	192.168.60.0/24											0 B	0
		;;; masquerade hotspot network														
31		ma...	srcnat	10.0.0.0/24											0 B	0
		;;; masquerade hotspot network														
32		ma...	srcnat	20.0.0.0/24											0 B	0
		;;; masquerade hotspot network														
33		ma...	srcnat	10.5.50.0/24											0 B	0
34		dst-...	dstnat					6 (tcp)		8291	WanHo...				1860 B	35

Figura 95. *Direccionamiento IP Y Trafico de Red Entel y Tigo*

5.3.4.- Consumos de Energía por equipo

Tabla de consumo de energía de cada equipo de la red de la institución:

Energía de consumo: Potencia (W)=Voltaje (V)×Corriente (A)

Kilowatt×horas=kwh Potencia ×Tiempo = Consumo de energia

Conversión: 180W ×(1KW/1000W) =180KW/1000W=0.18KWH

Energía por hora: KiloWatt-hora (KWH)

Conversión de Uso: 24 Horas×30 días = 720 horas

Calculo Final: 0.018KW×720 horas = 12.96 KWH

Equipo	**Voltaje**	**Watts**	**KW**	**KWH**
PC TinkCentre Lenovo I5 8Gen	-	180	0.18	12.96
Monitor Lenovo	-	15	0.015	10.8
Router ZTE	12 V - 1.5A	18	0.0.18	12.96
Router Cisco(Tigo)	-	150	0.15	108

Fortinet	12Vdc 3A	36	0.036	25.92
Switch TP-Link	240V(+) - 0.4A	47.57	0.04757	34.2504
Grandstream	12 V - 2A	24	0.024	17.28
PDU	-	3300	3.3	2,376
UPS Forza	220VAC- 63A	13860	13.86	9,979.2
PDU	220VAC -7.5A	16500	16.5	11,880
Switch Tp-Link 24P	220V/50Hz	22.3	0.0223	16.56
Switch Tp-Link 24P	110V/60Hz	47.57	0.04757	34.2504
Switch Fortinet 28P	-	185	0.185	133.2
Microtick RouterBoard	30V	30	0.030	21.6
DVR Alhua Tecnology	12 VDC, 2 A	10	0.010	7.2
Switch Alhua Tecnology	100V–240V	240	0.24	172.8
PDU	-	3300	3.3	2,376
Total				**27913.7808**

Tabla 96. *Consumo de Energía en KWH de Equipos*

5.3.5.- Funcionamiento del Servidor de Monitoreo de Tiempo Real

Imagenes de Funcionamiento del servidor de monitoreo durante 8 horas continuas de los equipos, Mbps por segundo en uso, procesadores y memoria:

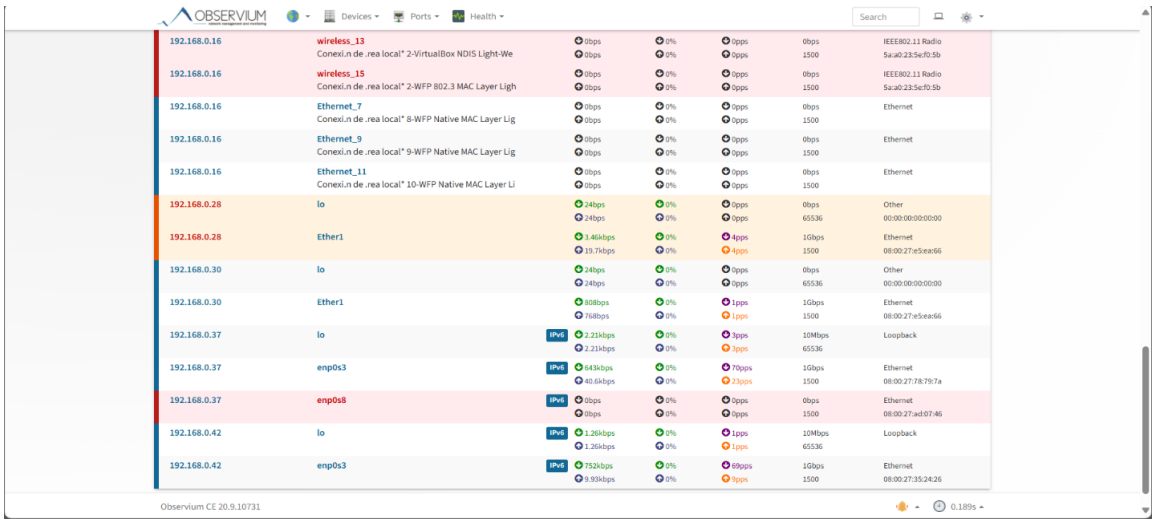


Figura 95. Consumo de MBPS de cada equipo Monitoreado

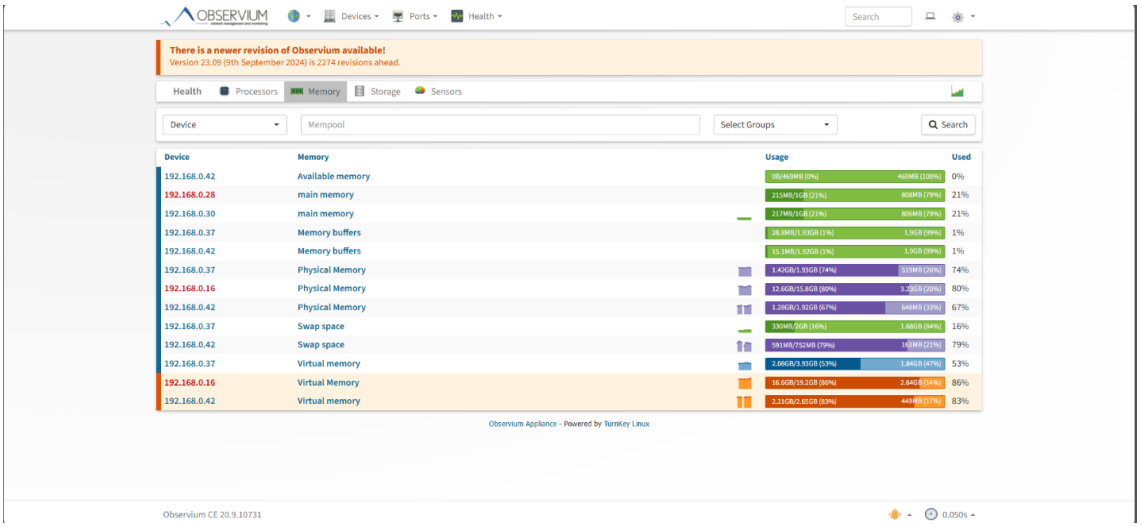


Figura 96. *Consumo de Procesadores de cada Equipo Monitoreado*

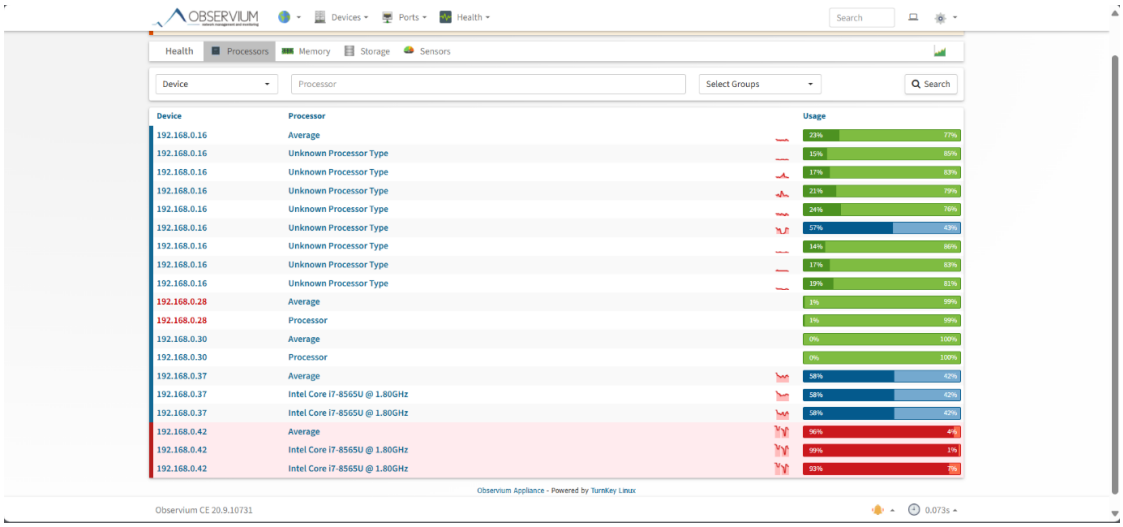


Figura 97. *Consumo de Memoria de cada Equipo Monitoreado*