# UNIVERSIDAD MAYOR DE SAN ANDRÉS
# FACULTAD DE INGENIERÍA
# CARRERA DE INGENIERÍA ELECTRÓNICA


## PROYECTO DE GRADO

**Para optar el Título de Licenciatura en Ingeniería Electrónica**

## DISEÑO DE CENTRO DE DATOS E INFRAESTRUCTURA TECNOLOGICA DE INFORMACION Y COMUNICACIÓN PARA LA FACULTAD DE INGENIERÍA U.M.S.A.

**POSTULANTES:** CESAR EFRAIN CHINCHE VELASQUEZ
GROVER SILVA LOAYZA
**TUTOR:** ING. EDUARDO LAURA PIZARRO
**DOCENTE:** ING. LUIS ALFONSO JURADO

**LA PAZ - BOLIVIA**

**2023**

**UNIVERSIDAD MAYOR DE SAN ANDRÉS**
**FACULTAD DE INGENIERIA**

**LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.**

## LICENCIA DE USO

El usuario está autorizado a:

a) Visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) Copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) Copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la cita o referencia correspondiente en apego a las normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

## RESUMEN

El proyecto propone realizar el diseño de un Centro de Datos y la infraestructura de red para la Facultad de Ingeniería U.M.S.A., tomando en cuenta Normas y Estándares Internacionales. La situación actual de la infraestructura tecnológica de la Facultad de Ingeniería, no cumple con las normas y estándares del sector. Se pretende realizar un diseño acorde a las necesidades actuales, en aspectos como la ampliación de la infraestructura física para el mejoramiento integral, además de permitir la ampliación de los servicios digitales que brinda el Centro de Datos (*IngeTIC*), utilizando nuevas tecnologías. Se propone diseñar una nueva infraestructura para el centro de datos y se plantea realizar un nuevo diseño del cableado estructurado de red en base a normas, para el edificio ubicado en la plaza del Obelisco, en la ciudad de La Paz.

Se plantea diseñar el cableado estructurado (cableado vertical y cableado horizontal) del edificio ubicado en el Obelisco, tomando en cuenta modularidad y escalabilidad, también se planifica los dispositivos de red *(networking)* basado en el modelo jerárquico de 3 capas (cisco), el cual permitirá migrar hacia una red basada en IPv6. Por otro lado, para el diseño del Centro de Datos *ingeTIC* se realiza la planificación y dimensionamiento de la infraestructura informática *(equipos TIC),* también se dimensiona la infraestructura critica (*facilities*) para el centro de datos *ingeTIC*. Todos los procesos desarrollados están basados en Metodologías, Normas y Estándares internacionales actuales, que satisfacen los requerimientos actuales de servicios digitales en la Facultad de Ingeniería (edificio del Obelisco). Finalmente se presenta un análisis de costos.

# ÍNDICE

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# 1. CAPITULO I. MARCO REFERENCIAL

## 1.1. INTRODUCCIÓN

Un ***Data Center o Centro de Datos*** es una instalación o espacio físico que se usa para brindar un espacio seguro a sistemas computacionales y a sus componentes, que son:

- Servidores/Switchs/Routers.
- Sistemas de Almacenamientos (SAS, NAS, SATA, SSD).
- Sistemas de Comunicaciones o cableado estructurado del Centro de Datos.

También es necesario un ***Cableado Estructurado***, que constituye la columna vertebral de la red informática, dentro un edificio y sus plantas o pisos, constituye la forma de interconectar los equipos informáticos de los usuarios o terminales remotas (ubicados dentro los ambientes físicos: oficinas), constituyéndose en una red que depende de los servicios que brinda el centro de datos.

- Hoy en día tenemos el surgimiento de nuevas tecnologías más flexibles que se adaptan a la creciente demanda y rapidez de los cambios y las demandas de los servicios mediante las tecnologías de virtualización de infraestructuras, equipos y servicios.
- Los componentes más comunes del ***equipamiento IT*** (Information Technology) son: firewalls, gateways, VPN, routers, computadores, servidores de bases de datos, servidores de archivos, servidores de aplicaciones, servidores web y otros. Es decir, el equipamiento IT es todo hardware físico o plataforma virtual (lógico).
- Por otro lado, *la* ***Infraestructura Física del Data Center*** es el que permite mantener el correcto funcionamiento del equipamiento IT dentro el Centro de Datos, consiste sobre todo de: Racks, Piso Técnico, UPS, Aire Acondicionado de Precisión, cableado entre racks, control de accesos, puertas de seguridad, cámaras de video vigilancia y otros. Estos elementos deben ser dimensionados de acuerdo al consumo eléctrico y la carga térmica que genera el equipamiento IT. También La Infraestructura del Data Center se proyecta en base al ***Índice de Disponibilidad*** (TIER), según normas y estándares internacionales (TIA, BICSI, ICREA, ASHRAE, IEC, otros).

- El ***Cableado Estructurado***, también deberá estar acorde a las nuevas tecnologías emergentes para esta área, que permiten velocidad en el orden de Gbps, tales como: CAT 6, CAT6A, CAT7, CAT8 en base al cable de cobre UPT/STP (Unshielded Pair Twisted/Shielded Pair Twisted) o también a través de medios como la fibra óptica Multimodo (OM1, OM2, OM3, OM4, OM5) y Monomodo (OS1, OS2).

## 1.2. ANTECEDENTES

Debido a la situación actual a nivel global, con prolongados confinamientos y restricción de actividades presenciales, se ha impulsado en gran medida el trabajo a distancia, así como las actividades académicas de manera virtual y remota.

Para desarrollar todas estas actividades hoy en día los requerimientos tecnológicos se han incrementado logrando convertirse en indispensables y fundamentales, como pilar de la sociedad comunicada e interconectada.

Las tecnologías de la información y las comunicaciones (TIC), han estado transitando en este siglo XXI por un proceso de transformación muy importante, que impacta hoy con fuerza a todas las actividades que rodean al hombre. Se trata de la unión de tres nuevos paradigmas: computación en la nube, movilidad y comunicación de igual a igual (P2P). Si bien cada una cumple un papel diferente, no son independientes. De hecho, se encuentran correlacionadas y se retroalimentan mutuamente. Por un lado, surge una multiplicidad de terminales de conexión a Internet, cambiando el escenario existente en el cual la PC era antes prácticamente el único sistema final de acceso a la red.

La nube (*cloud*) y los centros de datos (*data center*) han impactado en la arquitectura cliente-servidor, trayendo una nueva visión más centralizada y asociada al procesamiento de datos. La solución a problemas de altas latencias en una arquitectura centralizada ha sido un tema a solucionar para lo cual se propone hoy en día el concepto descentralizado (*edge*).

***"En tal sentido el avance tecnológico debe permitir atender las necesidades de teletrabajo, educación a distancia y clases virtuales por parte de sus instituciones hacia las diferentes actividades académicas y de la sociedad en general".***

Hoy en día el requerimiento de la creciente demanda de manejo de información en formato digital requieren para este propósito la implementación de infraestructura tecnológica adecuada y equipamiento de centros de datos capaces de almacenar y gestionar dicha información de manera digital.

Todo esto conlleva una gran variedad de nuevos servicios y automatización de procesos que contribuyen al manejo de la información, aportándole mayor eficiencia, competitividad, flexibilidad, confiabilidad y buen desempeño. Esta la razón principal para la informatización de las instituciones gracias a la Implementación de Centros de Datos de alto impacto.

Por tanto, se requiere de una instalación de computo adecuada dentro la infraestructura general de las instituciones y empresas, con aspectos tales como centros de datos, cableado estructurado, cámaras de video vigilancia, telefonía IP, sistema eléctrico, servidores, refrigeración, etc. Todo esto debe ser implementado bajo normas y estándares internacionales, para un adecuado funcionamiento.

## 1.3. PLANTEAMIENTO DEL PROBLEMA

La situación actual de la infraestructura tecnológica en la Facultad de Ingeniería U.M.S.A. no garantiza a futuro un óptimo funcionamiento para los servicios informáticos que van en constante crecimiento. Los actuales requerimientos en cuanto a Teletrabajo, Teleducación, clases virtuales y/o remotas, tienen un crecimiento exponencial. En el presente posiblemente la instalación de la infraestructura tecnológica no había sido contemplada bajo normativas y estándares vigentes, en su etapa inicial de implementación ha estado gobernada por una implementación improvisada tanto para la sala de servidores (*IngeTIC*), así como el cableado de red de las plantas del edificio de la Facultad de Ingeniería ubicada en la plaza del Obelisco.

En el trabajo de relevamiento e inspección general que se realizó en el edificio de Ingeniería, se pudo evidenciar que tanto el *Centro de Datos (IngeTIC)* en el piso 6, así como la *Infraestructura de Red en todo el Edificio* "no" se encuentran instaladas de acuerdo a normas y estándares internacionales, por cuanto se pudo evidenciar un crecimiento caótico y sin tomar en cuenta las normativas de instalación vigentes.

La infraestructura tecnológica en Facultad de Ingeniería UMSA, se encuentra en la actualidad descrita de la siguiente manera:

**a) INFRAESTRUCTURA DEL CENTRO DE DATOS.**

En la actualidad se cuenta con un Centro de Datos, también denominado sala de servidores "IngeTIC" (TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN – INGENIERÍA) en ambientes del piso 6 del edificio de la Facultad de Ingeniería de la universidad Mayor de San Andrés, ubicado en la plaza del obelisco, Av. Camacho esq. Ayacucho Nro. 1175, en la ciudad de La Paz, Bolivia. El área que ocupa este Centro de Datos (IngeTIC) es de 30,2m$^2$ con una altura 2,90m, en el cual trabajan dos operadores encargados de dicha sala. Actualmente se cuenta con una división dentro dicho ambiente, con una mampara de vidrio templado, dentro el cual se tienen 2 Racks o gabinetes de piso de una altura de 2.1m, 0,6m de ancho y 0,9m de profundidad, así como un tercer rack de pared de 10RU. El centro de datos actual (IngeTIC) no cuenta con un tablero principal de distribución eléctrica, simplemente se tiene un par de termomagnéticos:1 de 40A y 1 de 20A, en una caja plástica (práctica no recomendada). También en la actualidad el ingeTIC es energizada a través de un sistema Trifásico Delta 220Vac del cual se están utilizando 2 de las líneas para obtener una alimentación de 220Vac monofásica, entre Fase – Fase.

El actual centro de datos IngeTIC no se cuenta con un sistema de refrigeración adecuado para enfriamiento de los servidores, simplemente se pudo evidenciar 2 ventiladores instalados en la ventana lateral del centro de datos, para extraer el calor generado por los equipos (práctica no recomendada). Se tienen escalerillas metálicas (FEMCO) de un ancho de 55cm para albergar el cableado de datos que ingresa al IngeTIC, la cual está anclada y soportada por el techo.

**b) SERVIDORES/ROUTERS.**

Los equipos IT están contenidos dentro 2 racks, incluyen 2 servidores rackeables y dispositivos de interconexión (routers, switch, etc.). Actualmente las plataformas instaladas en estos servidores dan un servicio para alrededor de una población de 10.000 estudiantes, con una capacidad de almacenamiento cercana al límite de funcionamiento. El equipamiento IT actual con el que se cuenta, actualmente tiene un consumo promedio medido de 12 Amperios (2760 Watts). Esta corriente de consumo total medida sirve para poder dimensionar la Infraestructura Física del Centro de Datos "IngeTIC", en aspectos tales como la carga térmica a refrigerar para su adecuado funcionamiento y capacidad del equipo de energía de respaldo UPS (Ininterruptible Power System) y otros, sin embargo, actualmente no sucede tal situación.

**c) INFRAESTRUCTURA DE RED.**

Por otro lado, se tiene el cableado de red horizontal, actualmente con cable UTP categoría 5e, en cada uno de los 7 pisos, así como en mezzanine, planta baja y sótanos. El cableado horizontal en cada planta implementada actualmente consta de un promedio de 50 puntos de red. Se constituye en un cableado obsoleto para las necesidades actuales, pues al ser Categoría 5e está limitado a velocidades de transferencia de 100 Mbps. El cableado vertical (*backbone*) se encuentra realizado con fibra óptica de tipo Multimodo, para la interconexión entre pisos, instalado sin los elementos de sujeción adecuados o entubado, de manera que están expuestos a fallas producidas por manipulación externa, cada vez que alguna persona ingresa a los IDF de los pisos. También se cuenta con ambientes pequeños en cada planta los cuales son destinados como IDF (Intermedia Distribution Frame), que es el nodo central para el cableado horizontal de cada planta. Cada IDF cuenta también con un tablero de distribución eléctrica de piso el cual tiene las dimensiones de 60x40x20, con termomagnéticos para alimentar el equipamiento informático dentro cada IDF de piso:

**d) CENTRAL TELEFONICA Y CONTROL DE ACCESOS.**

La Facultad de Ingeniería U.M.S.A. dispone en la actualidad de 2 centrales telefónicas analógicas (PANASONIC), en el ambiente del sótano 1, cuyas características son: 8 líneas

externas, 56 líneas internas. Cada uno de los controles de acceso biométrico instaladas en las aulas del edificio de ingeniería, en la actualidad es gestionada por cada carrera.

**e) SISTEMA ELECTRICO.**

En ambiente del sótano 1 se dispone de un tablero de distribución principal de energía A.C., el cual incluye energía Trifásica 220 VAC (delta). El tablero principal se encuentra en el sótano, donde llega la acometida eléctrica de la empresa distribuidora de energía eléctrica comercial (*DeLaPaz*).

La situación de la infraestructura tecnológica actual no garantiza un adecuado funcionamiento de los actuales requerimientos en cuanto a Teletrabajo, Teleducación, clases virtuales y/o remotas, es decir no había sido contemplado instalar bajo normativas vigentes en su etapa inicial de implementación, tanto para la sala de servidores (*IngeTIC*) así como el cableado de red del edificio.

En la inspección general que se realizó en el punto anterior, se pudo evidenciar que tanto el ***Centro de Datos*** (IngeTIC) en el piso 6, así como la ***infraestructura de red en todo el edificio*** no están instaladas de acuerdo a normas y estándares internacionales, por cuanto se pudo evidenciar un crecimiento caótico y sin tomar en cuenta las normativas de instalación adecuadas.

## 1.4. OBJETIVOS

### 1.4.1. OBJETIVO GENERAL

Diseño y Planificación de la Infraestructura Tecnológica para el edificio de la Facultad de Ingeniería – Universidad Mayor de San Andrés, el cual incluye diseño del Centro de Datos (IngeTIC) así como la estructura Física y Lógica de Red a planificarse, considerando tecnologías actuales, en base a normas, estándares y recomendaciones internacionales.

### 1.4.2. OBJETIVOS ESPECÍFICOS

- Dimensionamiento del equipamiento informático IT para el Centro de Datos IngeTIC.
- Diseño de la Infraestructura Critica del Centro de Datos IngeTIC.

- Diseño del Cableado Estructurado del edificio:
  - Cableado Horizontal
  - Cableado Vertical (backbone).
- Diseño Lógico de la Red (implementación de VLANs mediante IPv6).
- Planteamiento de las configuraciones de los equipos informáticos.

## 1.5. JUSTIFICACIÓN

### 1.5.1. Justificación Técnica

Se pretende dar solución o minimizar la caída y saturación del servicio informático, lo cual genera contratiempos, altas latencias, quejas y pérdida de tiempo en las actividades académicas y administrativas. La finalidad del proyecto es mejorar los servicios informáticos que se brinda a estudiantes, docentes y administrativos para obtener un rendimiento lo más óptimo posible, pues es importante mejorar la educación universitaria con ayuda de la infraestructura tecnológica adecuada. En nuestro caso pretendemos diseñar una infraestructura tecnológica que permita elevar el nivel académico tanto de estudiantes como docentes y una eficiencia en la parte administrativa que beneficie a los estudiantes en sus diferentes tramites regulares académicos.

Mediante la implementación de equipos informáticos de última generación y la infraestructura de red adecuada, se podrá lograr este objetivo académico y administrativo.

### 1.5.2. Justificación Económica

La pérdida de información repercute en un incremento del presupuesto destinado a estas caídas del servicio que ofrece el centro de datos IngeTIC, se generan daños a los equipos informáticos, que posteriormente deben ser adquiridos para ser reemplazados. Esto genera contratiempos, quejas y pérdida de tiempo en las actividades académicas y administrativas. (postergación de exámenes debido a caída del sistema, inatención de la parte administrativa), lo cual también incide en un malestar general en estudiantes, docentes y administrativos, generando contratiempos que causan gasto adicional a los usuarios del servicio por causa de la deficiencia en la infraestructura tecnológica actual.

### 1.5.3. Justificación Académica

Actualmente no se brinda servicios informáticos eficientes, lo cual incide en la postergación y poco desarrollo académico, así como administrativo, retardando la conclusión adecuada de actividades académicas durante el semestre. Es muy importante que la universidad aporte a la sociedad con profesionales bien capacitados, capaces de dar solución a la industria. La infraestructura propuesta permitirá desarrollar con mayor eficiencia las actividades académicas (inscripciones, matriculación, clases virtuales, evaluaciones virtuales, bases de datos de bibliografía, biblioteca virtual, mejoras en la investigación, publicaciones científicas, etc.).

El presente proyecto pretende solucionar los servicios informáticos para el crecimiento vegetativo anual, así como los actuales y futuros servicios digitales que podrá brindar el *IngeTIC*, constituyéndose en la vanguardia dentro las 13 facultades de la U.M.S.A.

## 1.6. ALCANCES Y LÍMITES

El presente documento concluye con la planificación, diseño y recomendaciones para una futura implementación de la Infraestructura Tecnológica de la Facultad de Ingeniería – Universidad Mayor de San Andrés, acorde a los estándares y normas internacionales vigentes.

### 1.6.1. Alcances

- Realizar el Análisis y Evaluación de la infraestructura tecnológica actual de la Facultad de Ingeniería U.M.S.A.
- Presentar la adecuación de obras civiles en el Centro de Datos (IngeTIC).
- Realizar el Dimensionamiento de la Infraestructura IT (equipamiento Informático) para el Centro de Datos (IngeTIC).
- Realizar el diseño de la Infraestructura Critica (facilities) del Centro de Datos IngeTIC.
- Proyectar el diseño del cableado estructurado de red Horizontal y Vertical (Backbone).
- Planificación del diseño Lógico de la Red mediante IPv6.

### 1.6.2. Límites

- En el presente proyecto a diseño final, no se contempla la etapa de implementación del centro de datos, tampoco la implementación del cableado estructurado. El proyecto se concentra en realizar el dimensionamiento, diseño y planificación, el cual estará pensado en cubrir la necesidad actual y a futuro para brindar servicios tecnológicos eficientes, bajo una infraestructura adecuada.
- El proyecto planteado no incluye la operación del Centro de Datos, tampoco el manejo e instalación de los servidores ni la administración de las bases de datos. Tampoco se contempla la gestión y monitoreo de los dispositivos de red, además no contemplamos la instalación y administración de cámaras de seguridad, telefonía IP, mantenimiento de la red y mantenimiento del centro de datos.
- Con referencia al sistema eléctrico el presente proyecto no contempla su diseño o planificación y/o modificaciones.

# 2. CAPÍTULO II. MARCO TEÓRICO

## 2.1. INFRAESTRUCTURA IT (Equipamiento Informático)

### 2.1.1. Utilidad de la Infraestructura IT

La ***transformación digital*** da la posibilidad de poder adaptarse a los nueva era de cambios tecnológicos. Con esta evolución digital se pueden utilizar plataformas virtuales para brindar servicios informáticos a empresas y así impulsar los resultados positivos en los negocios. Las soluciones de estos servicios van desde las aplicaciones hasta sistemas empresariales, productos inteligentes o registros digitales, todos ellos necesitan esta esencial infraestructura para ponerse a tono en un mundo globalizado y digital.

Una plataforma tecnológica ayuda a acelerar la innovación e incrementa la participación de los clientes. Esta infraestructura es necesaria para ofrecer estos servicios de la transformación digital, pero no tiene que residir en ninguna instalación física del propietario necesariamente. Tampoco es una característica obligatoria la necesidad de ser propietario de un centro de datos. Todo lo que ocurre en este sistema puede pasar dentro de los servidores en la nube (*cloud*), de esta forma conseguimos más agilidad, más facilidad de administración y de reacción ante demandas futuras de los usuarios. Además, la visibilidad que posee en las redes y proveedores aumenta y es capaz de gestionar una gran capacidad de información sobre el uso de la propia infraestructura. (Saavedra, 2018)

### 2.1.2. Función de la Infraestructura IT

La ***infraestructura IT*** se ha convertido en el principal componente de los servicios tecnológicos en la actualidad. Como hemos señalado anteriormente, esta nos aporta varias funcionalidades de redes de almacenamiento de información seguro y de procesamiento de datos a gran escala. Dentro del sistema los usuarios se pueden comunicar con estas infraestructuras a través de teléfonos inteligentes, laptops y/o tabletas para gestionar los datos personales y de negocios, utilizando las aplicaciones y los servidores de la red. (Saavedra, 2018)

### 2.1.3. Beneficios de la infraestructura IT en la transformación digital

En primer lugar, el hecho de contar con una infraestructura tecnológica hace que podamos trabajar con una enorme cantidad de datos, alojados en la nube con una gran seguridad, pero con formas fáciles para accederlas. En segundo lugar, la infraestructura IT debe ofrecer soporte en un contexto de tecnologías disruptivas en una sociedad mundialmente conectada, considerando un ecosistema que agiliza, según Gartner, hay más de 25 billones de los más diversos dispositivos y cosas conectadas para 2020. En todo ese proceso de cambios, contar con la infraestructura tecnológica IT adecuada, será un factor determinante para la competitividad de los negocios y el éxito de la transformación digital.

Por otro lado, adquirir un sistema IT va a brindar una organización limpia y ordenada para incrementar las funcionalidades de los clientes, junto con la rapidez que va a aportar al servicio. Esta característica unida a los avances del *cloud computing* va a facilitar todas las gestiones. Además, la infraestructura IT es creada a partir de unos componentes que pueden ser o no optimizados. Todo esto quiere decir que podemos adaptar esta infraestructura tecnológica IT a las necesidades de los usuarios para alcanzar los objetivos específicos y las metas marcadas para el éxito. (Saavedra, 2018)

### 2.1.4. Elementos de la Infraestructura IT

El servicio que ofrece el conjunto de dispositivos y aplicaciones informáticas necesarios para el funcionamiento digital de una empresa, es conocido como *infraestructura IT*. Este sistema gestiona la información a través de equipos, dispositivos, software y otros.

Los elementos principales que forman la **infraestructura tecnológica IT:**

- **Servidores***:* Equipos informáticos de grandes capacidades que hospedan las aplicaciones principales. Existen distintos tipos de servidores en función de las necesidades de las empresas y el tamaño de estas, servidores de archivos, web, etc.
- **Terminales***:* Medio de acceso a la infraestructura tecnológica de los usuarios o clientes, pueden ser Desktop PC o terminales remotas.
- **Almacenamiento***:* Son diferentes soluciones de almacenamiento de información, entre las que pueden aplicarse, soluciones de tipo convergente, cabinas de almacenaje,

dispositivos NAS (Network Attached Storage), redes de tipo SAN (Storage Area Network), así como otros dispositivos adicionales para copias de seguridad.

- **Networking***:* Dispositivos que, con distintas funcionalidades, permiten correr sin riesgos a la seguridad del sistema. Permiten agilidad, flexibilidad, logran aumentar la visibilidad en las redes, estos dispositivos vienen a ser los switches y enrutadores.
- **Seguridad***:* En este punto podemos incluir la seguridad de la información a través de dispositivos Firewall (cortafuegos) y otros. También elementos de resguardo de la información (*BackUp*) que proporcionan a la empresa copias de acceso a los datos en caso de pérdida o un ataque al sistema informático. (Saavedra, 2018)

## 2.2. TECNOLOGÍA DE SERVIDORES

### 2.2.1. Servidores tipo Torre

Los servidores tipo torre, son unidades verticales e independientes que constan de todos los componentes tradicionales de un servidor. Es decir, disco duro, procesadores, placa base, placa de red, entre otros.

Ya que, son muy parecidos a un ordenador común en tanto al coste y al espacio, se recomiendan como un primer servidor, ideal para pequeñas empresas que cuentan con un espacio limitado, pero aun así se necesitan monitorear los recursos en su red.

Asimismo, son la mejor opción para las empresas que buscan protegerse de intrusiones y ataques al sistema, utilizados en una ubicación central.

**Figura 1.** Servidores tipo Torre. (LAGE, 2019)

**Características técnicas de los servidores tipo torre:**

Entre las características de los servidores tipo torre, principalmente, están pensados para dar servicio a otros usuarios, aplicaciones, etc., por lo cual, no se utilizan como un puesto de trabajo.

Además, cuentan con un sistema operativo de servidor (la familia Windows Server en lugar de Windows 7, Windows 8 Windows 10, etc.). Y puesto que, se considera un equipo de gama de entrada (básico), no cuenta con prestaciones demasiado potentes, al menos de base. Sin embargo, a diferencia de las PC de trabajos convencionales, ofrece grandes capacidades de ampliación. Por ejemplo:

- Pueden incorporar varios procesadores.
- La memoria RAM (con frecuencia el recurso más necesario en este tipo de máquinas) se puede aumentar en gran medida. No es raro encontrar equipos con 16 bancos de memoria y que soportan hasta 512 GB de RAM.
- Ofrecen un almacenamiento mixto: con controladoras RAID, discos sólidos, SAS y SATA, etc.

**Ventajas del servidor tipo torre:**

Los servidores tipo torre cuentan con múltiples beneficios, tales como:

- **Aplicación:**

  Es esencial tener claro para qué utilizarás el servidor y si no necesitas demasiado almacenamiento ni escalabilidad, un servidor tipo torre es la mejor opción para administrar y compartir archivos en la red**.**
- **Tamaño de la empresa:**

  Los servidores tipo torre son ideales para pequeñas empresas que no tienen un área de tecnología encargada de administrarlos, carecen de espacio suficiente y, sobre todo, sólo requieren de algunas funciones básicas.

- **Inversión:**

  Los servidores tipo torre suelen ser más económicos, pues, las aplicaciones son de uso general: impresión, almacenamiento y red.

  Los servidores torre, de marcas como HP y DELL puedes encontrarlos desde precios modestos con componentes básicos como memoria RAM y disco duro. Aunque, se debe considerar que el precio del servidor depende de la configuración que la empresa necesite.

Los servidores tipo torre de HP, son ideales para pequeñas organizaciones y cuentan con aplicaciones de uso general para realizar funciones simples como almacenamiento de documentación e impresión, entre otros. Algunos de sus beneficios son:

- **Ambiente:** No requiere un ambiente adaptado a sus necesidades para poder funcionar correctamente.
- **Inversión:** Los servidores tipo torre de HP suelen ser modelos económicos, una inversión recomendada para las empresas cuyo modelo de negocio no está centrado en la tecnología. (LAGE, 2019)

### 2.2.2. Servidores tipo Rack

El **servidor rack** es compacto y puede apilarse uno encima de otro, lo que facilita la escalabilidad de la infraestructura.

**Los servidores tipo rack** son sistemas que ahorran espacio pues apilan los servidores en gabinetes también denominados racks, por lo que, son ideales para las pequeñas empresas que tienen mucha experiencia en el mundo de los servidores o para empresas medianas que necesitan más capacidad de sus servidores. Los servidores rack son equipos de gama alta, estandarizados, que se incluyen dentro de bastidores o gabinetes, permitiendo una mejor organización y hacer cambios sin reiniciar todo el sistema.

**La función de un servidor rack** se basa en un modelo que cuenta con ranuras de expansión, conocidas como mezzanine, las cuales, se usan para añadir tarjetas de interfaz de red, entre otras cosas. Estos componentes se apilan de la misma manera que un organizador de

CD apila los discos. Se trata de una configuración que optimiza el espacio e incrementa la escalabilidad de la infraestructura, al permitir la adición de nuevos servidores según se necesiten.

**Figura 2.** Servidor tipo RACK. (LAGE, 2019)

**Características técnicas de los servidores rack:**

El **servidor tipo rack** recibe su nombre de los armarios que los albergan y es capaz de desarrollar las mismas funciones que los demás servidores. Algunas de sus características son:

- El ancho de los servidores rack, así como, de los armarios y bastidores rack, está estandarizado en 19 pulgadas. Por ello, los servidores rack de distintos fabricantes pueden integrarse en el mismo armario.
- Los armarios con medidas para rack tienen siempre el mismo ancho, pero, la altura y el fondo puede variar para permitir mayor personalización de la instalación.
- A pesar de permitir almacenar más datos en menos espacio que con otro tipo de sistema, los servidores tipo rack pueden llegar a ocupar dos metros cuadrados.
- En caso de no contar con mucho espacio, se recomienda optar por servidores de gama más baja y más económica, que ocupen menos espacio.

**Ventajas del servidor rack:**

Los servidores tipo rack cuentan con múltiples beneficios, tales como:

- La principal ventaja de los servidores rack para sus usuarios, es la posibilidad de sustituir piezas estropeadas o cambiar la fuente de alimentación sin tener que apagar todo el sistema, sino únicamente las secciones afectadas.
- **Aplicación:**

  Si requieres un sistema capaz de almacenar grandes cantidades de información o bases de datos de un programa, además de escalable si requieres más almacenamiento, los servidores rack son la mejor opción.
- **Tamaño de la empresa:**

  Son ideales para empresas medianas y grandes o empresas en crecimiento, pues, facilitan la expansión de los servidores e infraestructura tecnológica.
- **Escalabilidad:**

  La estructura de los servidores tipo rack es ideal para empresas que necesitan más de 3 servidores, pues, la característica de su forma ayuda a optimizar el uso del espacio, en comparación con los servidores tipo torre. Por ejemplo, si a futuro se está pensando en tener de 4 a 5 servidores en el SITE de la empresa, con los de tipo rack ocuparías alrededor de 5U de rack, mientras que con los de tipo torre, el espacio que necesitarías sería mucho mayor. Además, la administración de los servidores tipo rack es más sencilla, ya que, permite la conexión de todos los servidores a un sistema de almacenamiento externo. (LAGE, 2019)

### 2.2.3. Servidores BLADE (cuchilla)

Los servidores blade son uno de los 3 tipos principales de servidores, siendo los otros dos los de tipo rack y los de tipo torre. Un servidor blade es básicamente un servidor al cual se le han quitado varias partes y se le ha dado un diseño modular, todo esto con el objetivo de reducir todo lo posible el uso de espacio físico por parte del server y también reducir el consumo de energía eléctrica.

A los servidores blade se le quitan varios componentes para ganar espacio y reducir el consumo de energía, manteniendo lo necesario para que el server pueda funcionar de manera correcta, conservando los componentes necesarios para que aún pueda ser considerado un servidor.

Al contrario que los servidores que se montan en racks, los servidores blade se montan en unas cabinas especialmente diseñadas para ellos, las cuales pueden contener múltiples servidores blade, y estas son las encargadas de brindarle a cada servidor el enfriamiento, la energía eléctrica, la conexión a la red y más.

Básicamente, los componentes que se quitaron de los servidores blade están presentes en estas cabinas, y todo el conjunto, es decir las cabinas y los servers blade que estas contienen, es lo que se conoce como sistema blade.

La cabina, o el chasis, donde se encuentran los servidores blade tienen el propósito de brindar a los servers aquello que le brindan los componentes que no fueron incluidos en el servidor, que es energía eléctrica, enfriamiento y conexión a la red, o dicho de otra forma los servidores blade no suelen contar con una fuente propia, ni sistema de enfriamiento ni placa de red.

Todo esto va directamente incorporado en el chasis de forma masiva y de allí distribuido a cada servidor, una configuración que permite ahorrar espacio y energía, algo extremadamente útil en los centros de datos, donde puede haber miles de servidores, ya que tener este tipo de configuración puede ayudar a ahorrar mucho dinero y espacio físico.

Es importante aclarar que no todos los servidores blade son compatibles con todos los chasis, ni viceversa por supuesto. Los servidores blade y los chasis suelen ser diseñados teniendo en mente cómo se usarán el uno con el otro, debido a esto es normal que un servidor blade de una marca no pueda usarse en un chasis de otra marca o, dicho de otra forma, lo mejor es siempre usar servidores blade y chasis blade de una misma marca.

También cabe destacar que no todos los fabricantes optan por montar los servidores blade de la misma manera, mientras que algunos pueden quitar todos los componentes posibles, otros pueden quitar una menor cantidad, por ejemplo, quitar solo la fuente y el sistema de

enfriamiento, pero dejar la placa de red intacta. Esto es algo que varía de un fabricante a otro. (Borges, 2020)

**Figura 3.** Servidor Blade. (Borges, 2020)

**Ventajas y desventajas de los servidores blade:**

Los servidores blade tienen algunas ventajas estupendas, pero de la misma forma también presentan ciertas desventajas o puntos que les juegan en contra. Lamentablemente no existe el servidor perfecto, pero los blade se acercan bastante a ello. Veamos entonces cuáles son las principales ventajas y desventajas de los servidores blade. (Borges, 2020)

**Ventajas de los servidores blade:**

- **Bajo consumo energético**: los blade servers son muy bueno en lo que al consumo de energía eléctrica refiere, ya que en lugar de encontrarse en racks separados y hacer uso de sus propias fuentes, se encuentra en chasis especializados donde esta propia cabina es la que le brinda la electricidad necesaria para que funcione, sin gastar de más, lográndose un ahorro de energía eléctrica importante. A pequeña escala puede no parecer mucho, pero si tenemos en cuenta que un d (Borges, 2020)ata center puede tener miles de estos servidores entonces veremos que marcan una gran diferencia.
- **Gran poder de procesamiento en poco espacio**: la mayoría de los servidores blades nos brindan un gran poder de procesamiento si las contras de necesitar espacio físico adicional para lograrlo. Esto supone un ahorro de espacio muy importante, que nuevamente a pequeña escala se nota poca, pero a una gran escala marca una gran diferencia.

- **Son multipropósitos**: podemos alojar prácticamente cualquier cosa que queramos en ellos, por ejemplo, sistemas operativos, hipervisores, bases de datos, aplicaciones, servicios web y mucho más.
- **Disponibilidad**: gracias a los sistemas blade se simplifican mucho las tareas de monitorización y mantenimiento, el balanceo de carga, etc. La posibilidad de hacer un hot swapping (recambio en caliente) de algunos componentes de los servidores también ayuda a optimizar su uptime (disponibilidad), ya que de esta manera se pueden cambiar componentes sin necesidad de apagar el servidor y cero paradas del sistema. (Borges, 2020)

**Desventaja de los servidores blade:**

- **Costos iniciales**: quizá la única desventaja real de los servidores blade son los costos iniciales. Si bien a largo plazo es una estupenda inversión, lo cierto es que inicialmente se va a requerir de mucho dinero para montar este tipo de sistemas. Los costos de implementación y configuración de estos servidores son muy altos en un comienzo. Los sistemas blade requieren estar en ambientes extremadamente controlados en cuanto a temperatura y ventilación, lo cual contribuye a que la inversión inicial sea realmente grande. (Borges, 2020)

### 2.2.4. Servidores Convergentes

La ***infraestructura convergente*** es una solución definida por hardware diseñada para superar las limitaciones e ineficiencias de la estructura de silos independientes del almacenamiento y la computación de la TI tradicional. Para minimizar los problemas de compatibilidad y simplificar la gestión, las soluciones convergentes unen la computación, la red, el almacenamiento, los sistemas de administración y el software en un paquete preconfigurado que funciona y se gestiona como un único sistema convergente que acelera la obtención de beneficios.

La infraestructura convergente permite que las organizaciones utilicen sus recursos informáticos de formas más eficientes y rentables, reduzcan sus costes de gestión de TI e incrementen la velocidad de implementación del software y los servicios. Muchos ven la

infraestructura convergente como el primer paso en la evolución hacia una infraestructura definida por software/servicios. Ofrece:

- **Gestión de infraestructura más sencilla:** Centraliza la gestión de servidores, la red y el almacenamiento para optimizar el mantenimiento diario.
- **Capacidad de almacenamiento escalable:** Las estructuras comunes y los protocolos integrados en la infraestructura convergente convierten el proceso de añadir gigabytes en una tarea mucho más sencilla y rápida.
- **Aprovisionamiento más rápido:** Reduce el tiempo de aprovisionamiento de tres semanas a menos de una hora.
- **Respuesta de TI más rápida:** proporciona la agilidad para responder a los cambios en el mercado y las prioridades de negocio.
- **Ruta más fácil hacia la nube:** facilita la implementación de nubes privadas o híbridas.
- **Mayor control:** habilita la gestión simultánea de múltiples funciones y dispositivos. (Packard, 2022)

### 2.2.5. Servidor Hiperconvergente

A diferencia de los servidores convergentes, una plataforma ***Hiperconvergente*** consta de cuatro componentes de software perfectamente integrados:

- Virtualización del almacenamiento
- Virtualización de los recursos informáticos
- Virtualización de la red
- Funciones de gestión avanzadas, incluida la automatización

Los sistemas hiperconvergentes funcionan de manera muy similar a como lo hacen los servicios cloud. Los servicios que se ofrecen corren en servidores virtuales comúnmente denominadas *"máquinas virtuales",* mientras que la solución de hardware queda en un segundo plano, ni es visible ni relevante para el usuario, es decir la infraestructura se ejecuta en una máquina virtual en la capa del hipervisor, bajo la cual se ubica el hardware actuando como un pool común de recursos.

El software de virtualización desvincula y agrupa los recursos subyacentes y después, los asigna dinámicamente a aplicaciones que se ejecutan en *máquinas virtuales* o contenedores. La configuración basada en políticas adaptadas a las aplicaciones elimina la necesidad de utilizar estructuras complejas, como LUN y volúmenes. (Salinas, 2021)

Los sistemas ***Hiperconvergentes*** reducen la complejidad de los centros de datos, lo que supone un aumento de la productividad y la eficiencia.

**Vamos a enumerar algunas de sus ventajas:**

**Administración:** Como hemos citado anteriormente la infraestructura hiperconvergente se gestiona desde un único punto, lo que nos simplifica muchísimo la gestión del entorno.
Nos olvidamos de entrar a diferentes consolas de administración para gestionar por ejemplo el almacenamiento o el Networking. Se eliminan procesos manuales y la necesidad de contar con personal de operaciones con conocimientos aislados. Se simplifica la gestión los recursos informáticos y de almacenamiento, lo que facilitara las tareas al personal encargado.

**Costes:** Se ahorra tanto en componentes hardware como en el contrato de soporte que va vinculado a ese hardware, como puede ser, por ejemplo, el de la cabina de almacenamiento. Por otro lado, se reduce también el consumo energético y la formación a los Técnicos de TI.

**Implementación:** Los sistemas de Hiperconvergencia suele venir preinstalados y certificados para su correcto uso, por lo que la implementación suele ser muy rápida en comparación con sistemas convergentes tradicionales.

**Escalabilidad:** Solamente con añadir servidores en paralelo a nuestro *cluster,* estaremos ampliando los niveles de computación exponencialmente sin sufrir ningún tipo de disrupción en el servicio. Esto es debido a que la *hiperconvergencia* se basa en software, es capaz de proporcionar niveles superiores de flexibilidad y agilidad a las empresas en comparación con la infraestructura tradicional. La infraestructura hiperconvergente permite implementar y mover cargas de trabajo con mayor rapidez.

**Disponibilidad:** Los sistemas hiperconvergentes son muy estables por lo que tus cargas de trabajo ya sean máquinas virtuales o contenedores, estarán siempre disponibles. La hiperconvergencia nos permite configurar un activo/activo entre distintos CPDs proporcionando no solo alta disponibilidad a nivel del cluster de HCI, sino que además también lo hará a nivel de CPD. (Salinas, 2021)

## 2.3. CARACTERISTICAS DE LOS SERVIDORES.

Un servidor utilizado en un centro de datos debe cumplir con ciertas características para garantizar la eficiencia, la confiabilidad y el rendimiento en el entorno del centro de datos. Algunas de las características importantes que un servidor para data center debería tener incluyen:

- **Escalabilidad:** El servidor debe tener la capacidad de expandirse o actualizarse para satisfacer las demandas cambiantes del centro de datos. Por ejemplo, debería ser posible agregar más capacidad de almacenamiento, memoria o procesamiento.
- **Eficiencia energética:** Los servidores deben tener una eficiencia energética alta para reducir los costos de energía y minimizar la generación de calor en el centro de datos. Un servidor eficiente energéticamente consumirá menos energía y producirá menos calor en comparación con un servidor menos eficiente.
- **Fiabilidad:** Los servidores en un centro de datos deben ser confiables y capaces de funcionar durante largos períodos de tiempo sin interrupciones. La confiabilidad se puede lograr mediante la selección de hardware de alta calidad y la implementación de redundancia en los componentes críticos, como fuentes de alimentación, ventiladores y discos duros.
- **Gestión remota:** Es importante que los servidores puedan ser gestionados y monitoreados de forma remota. Esto permitirá a los administradores del centro de datos solucionar problemas y realizar actualizaciones de software sin tener que acceder físicamente al servidor.

- **Escalabilidad horizontal:** Es importante que los servidores puedan escalarse horizontalmente. Esto significa que es posible agregar más servidores idénticos para aumentar la capacidad de procesamiento y/o almacenamiento en el centro de datos. Esto también ayuda a lograr la redundancia y alta disponibilidad en el centro de datos.
- **Capacidad de virtualización:** Los servidores en un centro de datos a menudo se utilizan para virtualización. Por lo tanto, los servidores deben tener la capacidad de ejecutar múltiples sistemas operativos virtuales y alojar varias aplicaciones y servicios.
- **Seguridad:** La seguridad es fundamental para cualquier infraestructura de TI, y los servidores no son la excepción. Los servidores deben tener características de seguridad robustas, como autenticación fuerte, cifrado y protección de datos, y capacidades de prevención de intrusiones.

La elección del servidor depende de los requisitos específicos del centro de datos y de la carga de trabajo que se espera ejecutar en el servidor.

### 2.3.1. Elección del Servidor

La elección del tipo de servidor adecuado, considerando que se tendrá una gran cantidad de usuarios dependerá de varios factores, como el tipo de aplicaciones que se ejecutan, el presupuesto disponible, los requisitos de rendimiento y la escala prevista.

Sin embargo, para una institución con una gran cantidad de usuarios, generalmente se recomienda utilizar servidores de gama alta que sean escalables y capaces de manejar una gran cantidad de tráfico y procesamiento de datos. Los servidores de nivel empresarial, como los servidores *Blade* o de tipo *Hiperconvergente,* pueden ser una buena opción ya que ofrecen un alto grado de escalabilidad y eficiencia energética. Estos servidores son capaces de alojar múltiples procesadores y discos duros en una sola unidad, lo que reduce el espacio necesario en el centro de datos y ayuda a reducir los costos.

Además, dado que las empresas tienen una gran cantidad de usuarios, también se deberá implementar una solución de virtualización en el servidor. La virtualización puede ayudar a mejorar la eficiencia del servidor al permitir que múltiples sistemas operativos se ejecuten en

una sola máquina física. También ayuda a mejorar la disponibilidad y la recuperación ante desastres mediante la creación de copias de seguridad y la migración de máquinas virtuales a través de servidores.

Otra consideración importante es la redundancia en el servidor. Dado que la institución tiene una gran cantidad de usuarios y depende de los servicios del servidor, es importante asegurarse de que el servidor tenga una alta disponibilidad y pueda funcionar de manera confiable. Esto se puede lograr mediante la implementación de redundancia en los componentes críticos del servidor, como las fuentes de alimentación, los discos duros y las conexiones de red.

*En general, se deberá utilizar un servidor de gama alta escalable y eficiente en términos de energía con una solución de virtualización y redundancia en el servidor*. Además, es importante que el servidor pueda manejar una gran cantidad de tráfico y procesamiento de datos para satisfacer las necesidades de todos los usuarios.

Hay algunos modelos de servidores de gama alta que cumplen con las características que se mencionaron anteriormente, el presupuesto vs. rendimiento será un factor determinante para la elección del Servidor.

### 2.3.2. Funcionamiento del Servidor

Un servidor en un centro de datos (data center) tiene varias funciones importantes, algunas de las cuales son:

- **Almacenamiento y procesamiento de datos:** El servidor es responsable de almacenar y procesar grandes cantidades de datos para su posterior acceso y uso por parte de los usuarios y aplicaciones.
- **Suministro de recursos computacionales:** El servidor proporciona recursos computacionales como potencia de procesamiento, memoria y almacenamiento a los usuarios y aplicaciones que los necesitan.
- **Alojamiento de sitios web:** Un servidor en un centro de datos puede alojar múltiples sitios web, ofreciendo servicios de alojamiento web a empresas y organizaciones.

- **Hosting de aplicaciones:** El servidor también puede alojar aplicaciones web y proporcionar servicios de alojamiento de aplicaciones a los usuarios.
- **Procesamiento de transacciones:** Los servidores en centros de datos también se utilizan para procesar transacciones comerciales, como el procesamiento de pagos. Sin embargo, esta opción no está considerada en los servicios, pero será posible implementarla si es requerida.
- **Acceso remoto:** Los servidores en un centro de datos pueden proporcionar acceso remoto a aplicaciones y datos almacenados en ellos.
- **Administración de red:** Los servidores también se utilizan para administrar y controlar la red en el centro de datos, incluyendo la gestión del tráfico de red y la asignación de recursos de red.

En resumen, un servidor en un centro de datos es una parte fundamental de la infraestructura tecnológica, ya que proporciona los recursos y servicios necesarios para el almacenamiento, procesamiento y acceso a los datos y aplicaciones críticos.

## 2.4. ALMACENAMIENTO.

El almacenamiento en los centros de datos es una parte crítica de la infraestructura de TI, ya que permite a las instituciones almacenar y acceder a grandes cantidades de datos de manera segura y eficiente.

Hay varias formas de almacenamiento utilizadas en los data centers, incluyendo:

- **Almacenamiento de disco duro (HDD):** los discos duros son los dispositivos de almacenamiento más comunes en los data centers. Ofrecen una gran capacidad de almacenamiento y son adecuados para almacenar grandes cantidades de datos no estructurados.
- **Almacenamiento de estado sólido (SSD):** los SSD son dispositivos de almacenamiento más nuevos que utilizan chips de memoria flash para almacenar datos. Son más rápidos y confiables que los discos duros, pero también son más caros.

- **Almacenamiento en la nube:** la nube es una forma de almacenamiento en línea que permite a las empresas almacenar y acceder a datos a través de Internet. Los servicios de almacenamiento en la nube ofrecen escalabilidad y flexibilidad, pero también pueden presentar desafíos en cuanto a seguridad y privacidad.

En los centros de datos, el almacenamiento se organiza en matrices de almacenamiento (*arrays*), que consisten en una serie de discos duros o SSDs conectados a un controlador de almacenamiento. Los datos se distribuyen a través de los discos en la matriz, lo que permite una mayor velocidad y fiabilidad en la recuperación de datos.

La gestión del almacenamiento en el data center también implica la implementación de estrategias de copia de seguridad y recuperación de desastres para garantizar la disponibilidad y protección de los datos críticos.

### 2.4.1. Matriz de Discos

Una matriz de discos, también conocida como un array de almacenamiento, es un sistema de almacenamiento de datos utilizado en los data centers para proporcionar una mayor capacidad, rendimiento y confiabilidad.

La matriz de discos utiliza múltiples discos duros o unidades de estado sólido (SSD) interconectados para formar una única unidad de almacenamiento. Estos discos se organizan en grupos que se llaman conjuntos de discos (también conocidos como RAID, por sus siglas en inglés *Redundant Array of Independent Disks*). Existen varios niveles RAID, cada uno con su propio nivel de redundancia y rendimiento.

Los niveles RAID más comunes son:

- **RAID 0:** los discos se configuran para trabajar en conjunto como una única unidad de almacenamiento, lo que permite una mayor velocidad y rendimiento. Sin embargo, no hay redundancia de datos, por lo que, si uno de los discos falla, se pierde toda la información.

- **RAID 1:** los discos se duplican para proporcionar una mayor redundancia y protección de datos. Cada disco tiene una copia exacta de la información, por lo que, si uno de los discos falla, la información se puede recuperar del otro disco.
- **RAID 5:** se distribuye la información a través de varios discos, proporcionando una mayor velocidad y redundancia. En este nivel, se utiliza una paridad para detectar y corregir errores de datos.
- **RAID 6:** similar a RAID 5, pero con una mayor redundancia. Se utilizan dos bloques de paridad en lugar de uno para garantizar la integridad de los datos en caso de la falla de dos discos.

Además de la redundancia de datos, las matrices de discos también pueden incluir funciones como la gestión del almacenamiento en caché, el equilibrio de carga y la recuperación de desastres. Todo esto ayuda a garantizar que los datos estén disponibles y protegidos en todo momento en el data center. De acuerdo al siguiente esquema:

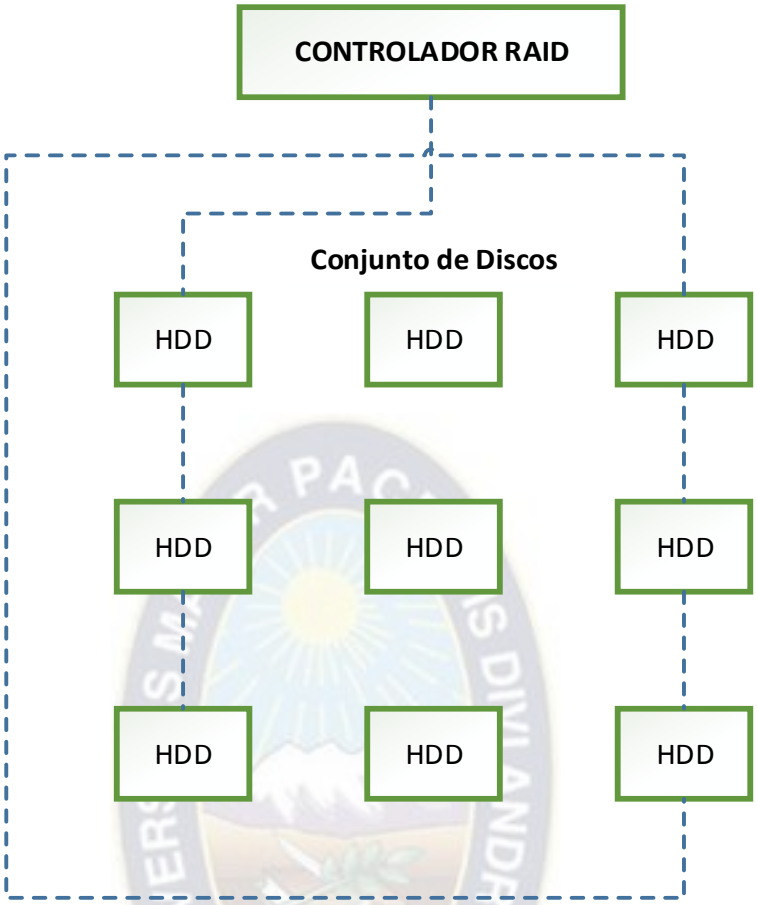



**Figura 4.** Esquema de la Matriz de Discos.

En este esquema, el controlador de la matriz de discos se encarga de la gestión de los discos duros (HDD) y la distribución de los datos en el conjunto de discos RAID. La matriz de discos en sí está compuesta varios discos duros interconectados, que forman el conjunto RAID 5. También en este esquema, el controlador RAID se encarga de la gestión de un conjunto de discos duros interconectados que proporcionan un alto rendimiento y capacidad de almacenamiento.

Los datos se distribuyen en los discos duros de tal manera que se garantiza la redundancia de los mismos. Si uno de los discos duros falla, los datos se pueden recuperar de los otros dos discos.

Los discos duros se agrupan en conjuntos RAID para proporcionar redundancia y protección de datos, lo que permite una mayor disponibilidad y fiabilidad. Además, la matriz de discos está diseñada para soportar múltiples usuarios y un gran flujo de datos.

En un escenario como este, también se podrían incluir otras tecnologías de almacenamiento, como unidades de estado sólido (SSD) o almacenamiento en la nube, para proporcionar una mayor flexibilidad y escalabilidad. La configuración exacta de la matriz de discos dependerá de las necesidades específicas de almacenamiento y de los requisitos de rendimiento y seguridad.

### 2.4.2. Almacenamiento en red

De acuerdo a las configuraciones previas todos los archivos que se generen se almacenaran en los discos del Servidor, también todos los diversos tipos de archivos que se carguen se almacenaran en los discos. Se tomará el modelo de almacenamiento NAS (Network Attached Storage), esto permitirá que los usuarios carguen los archivos desde sus dispositivos y estos sean dirigidos al servidor de acuerdo al siguiente esquema:

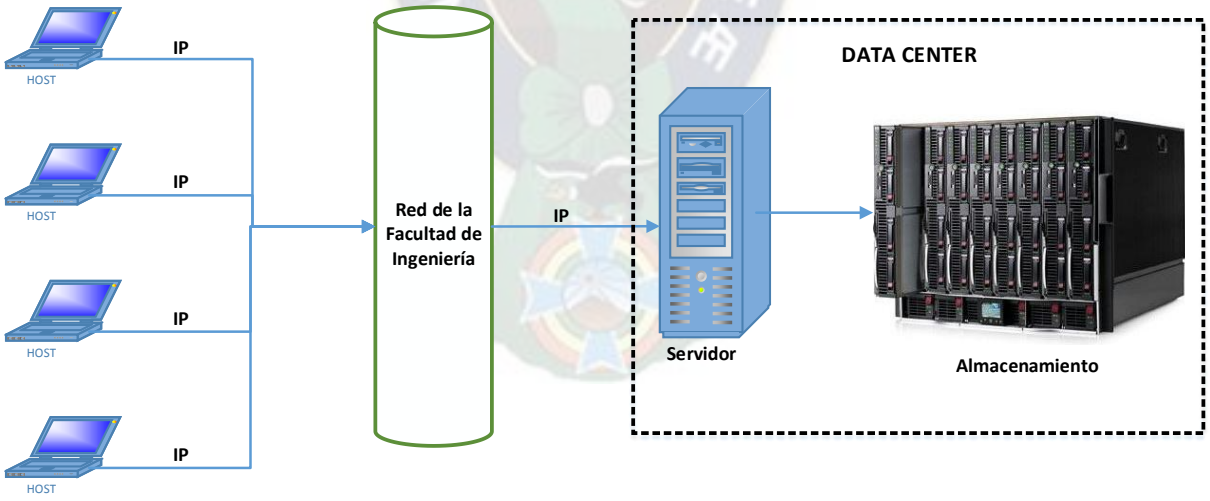



**Figura 5.** Esquema del Almacenamiento en Red.

### 2.4.3. Respaldo

El respaldo se hará mediante backups o copias de seguridad, para esta tarea existen diferentes métodos y herramientas los cuales garantizan que los datos almacenados en el servidor no tengan ningún riesgo de ser perdidos por algún evento desastroso.

Todos los archivos y documentos serán generados por distintos dispositivos, es sumamente importante generar copias de seguridad, además, estas copias deben estar cifradas para proteger la privacidad de los documentos usados por los usuarios. Para esta función utilizaremos una herramienta llamada ***Duplicati*** que es una solución bastante práctica que no sólo ayudará con la generación de copias de seguridad, sino también, asegurar que las mismas estén cifradas.

Mediante *Duplicati* se realizarán los backups o copias de respaldo, para asignar el espacio de memoria donde se guardarán estas copias se tienen dos formas de hacerlo las cuales son:

- **Asignando discos externos en el mismo servidor:** De esta manera se garantiza que si el disco principal sufre de algún daño y deja de funcionar el disco de respaldo podrá sustituir al disco principal casi de inmediato.
- **Establecer una conexión externa al servidor:** Para este caso se asignará un disco externo que estará fuera de la institución (no importa el lugar), y se establece una conexión al servidor utilizando un servicio de hosting, de esta manera se realizaran las copias en discos fuera de la Empresa o institución y así en caso de que hubiese algún caso extremo donde el disco del servidor perdiera la información y en si el servidor dejara de funcionar se garantizaría que la información no se perdiera. Para establecer esta conexión es necesario tener una conexión constante a internet.

Mediante *Duplicati* se pueden configurar diferentes parámetros tanto en el volumen de archivos y el tiempo en el cual se harán dichas copias, el proceso de respaldo se realiza de acuerdo al siguiente diagrama.

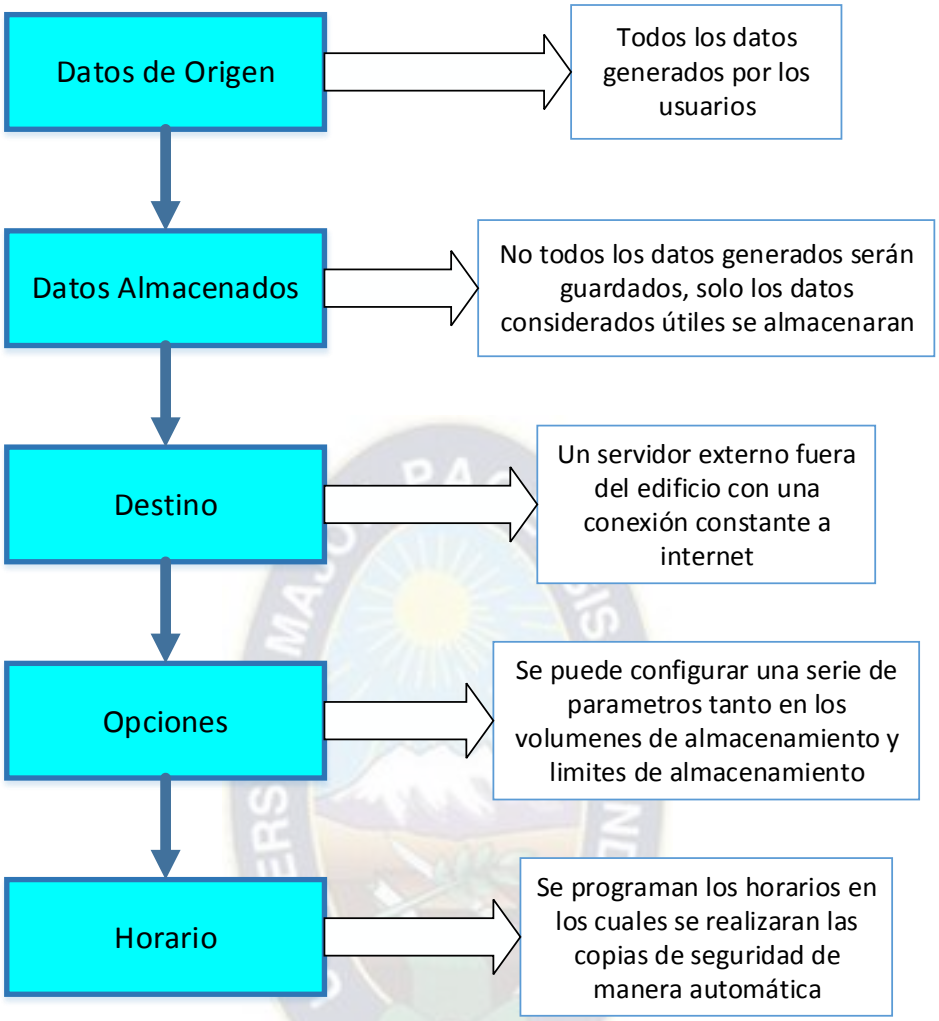



**Figura 6.** Diagrama de Copias de Seguridad.

## 2.5. VIRTUALIZACIÓN

### ¿Qué es virtualización?

La virtualización es una tecnología que permite crear servicios de TI útiles mediante recursos que normalmente se ejecutan en el hardware. Gracias a ello, permite utilizar toda la capacidad de una máquina física, pues distribuye sus capacidades entre varios usuarios o entornos.

Una máquina virtual es un contenedor de software perfectamente aislado que puede ejecutar sus propios sistemas operativos y aplicaciones como si fuera un ordenador físico.

Una máquina virtual se comporta exactamente igual que lo hace un ordenador físico y contiene sus propios CPU, RAM, disco duro y tarjetas de interfaz de red (NIC) virtuales (es decir, basados en software). El sistema operativo no puede establecer una diferencia entre una máquina virtual y una máquina física, ni tampoco lo pueden hacer las aplicaciones u otros ordenadores de una red. Incluso la propia máquina virtual considera que es un ordenador "real". Sin embargo, una máquina virtual se compone exclusivamente de software y no contiene ninguna clase de componente de hardware. El resultado es que las máquinas virtuales ofrecen una serie de ventajas con respecto al hardware físico.

Los tipos de máquinas virtuales se pueden clasificar en dos grandes categorías según su funcionalidad y su grado de equivalencia a una verdadera máquina.

- ***Máquinas virtuales de sistema*** (en inglés System Virtual Machine)
- ***Máquinas virtuales de proceso*** (en inglés Process Virtual Machine)

En informática, la virtualización se refiere a la abstracción de los recursos de una computadora, llamada Hypervisor o VMM (Virtual Machine Monitor) (keloko03, 2009) el cual crea una capa de abstracción entre el hardware de la máquina física y el sistema operativo de la máquina virtual, siendo un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo, donde se divide el recurso en uno o más entornos de ejecución.

La máquina virtual en general es un sistema operativo completo que corre como si estuviera instalado en una plataforma de hardware autónoma. La virtualización se encarga de crear un interfaz externo que esconde una implementación por debajo del sistema, mediante la combinación de recursos en locaciones físicas diferentes. Típicamente muchas máquinas virtuales son simuladas en un computador central. Para que el sistema operativo virtual funcione, la simulación debe ser lo suficientemente grande.

Esta capa de software gestiona los cuatro recursos principales de una computadora, que son la CPU, la Memoria, la Red, y el Almacenamiento, y así podrá repartir dinámicamente

dichos recursos entre todas las máquinas virtuales definidas en el computador central. De modo que permite tener varios ordenadores virtuales ejecutándose sobre el mismo ordenador físico.

**Ventajas de la Virtualización:**

- Rápida incorporación de nuevos recursos para los servidores virtualizados.
- Reducción de los costes de espacio y consumo necesario de forma proporcional al índice de consolidación logrado (Estimación media 10:1).
- Administración global centralizada y simplificada.
- Nos permite gestionar nuestro CPD como un pool de recursos o agrupación de toda la capacidad de procesamiento, memoria, red y almacenamiento disponible en nuestra infraestructura
- Mejora en los procesos de clonación y copia de sistemas: Mayor facilidad para la creación de entornos de test que permiten poner en marcha nuevas aplicaciones sin impactar a la producción, agilizando el proceso de las pruebas.
- Aislamiento: un fallo general de sistema de una máquina virtual no afecta al resto de máquinas virtuales.
- No sólo aporta el beneficio directo en la reducción del hardware necesario, así como de sus costos asociados
- Reduce los tiempos de parada.
- Migración en caliente de máquinas virtuales (sin pérdida de servicio) de un servidor físico a otro, eliminando la necesidad de paradas planificadas por mantenimiento de los servidores físicos.
- Balanceo dinámico de máquinas virtuales entre los servidores físicos que componen el pool de recursos, garantizando que cada máquina virtual ejecute en el servidor físico más adecuado y proporcionando un consumo de recursos homogéneo y óptimo en toda la infraestructura.
- Alto grado de satisfacción general.

### 2.5.1. TIPOS DE VIRTUALIZACIÓN.

**Virtualización de Servidores.**

Es una técnica de virtualización que involucra la partición de un servidor físico en una cantidad de pequeños servidores virtuales con la ayuda del software de virtualización. En la virtualización de servidores, cada servidor virtual ejecuta varias instancias del sistema operativo al mismo tiempo. es el enmascaramiento de los recursos del servidor, incluidos el número y la identidad de servidores físicos individuales, procesadores y sistemas operativos, de los usuarios del servidor (Ortiz, 2018).

**Virtualización de Almacenamiento.**

La virtualización del almacenamiento es el proceso de consolidar varios dispositivos físicos de diversos fabricantes reorganizándolos en agrupamientos virtuales, además de lógicos, o en unidades de almacenamiento (Intel, 2010). La virtualización de almacenamiento, de acuerdo al lugar en que se realice en sí, se puede clasificar en tres grupos, pudiendo ser: Virtualización basada en dispositivo, y en la red (Lugo Cardozo, 2014).

**Virtualización de Redes.**

La virtualización de red es la segmentación o partición lógica de una única red física, para usar los recursos de la red. Esta es lograda instalando software junto con los servicios para gestionar el almacenamiento compartido, los ciclos de computación además de las aplicaciones. La virtualización de red trata a todos los servidores y servicios en la red como un único grupo de recursos al que pueden acceder sin considerar sus componentes físicos. Se pueden tener varios tipos de virtualización de redes, entre los que se puede mencionar principalmente: Virtual LAN, Virtual IP y Virtual Private Network. (Lugo Cardozo, 2014).

**Virtualización de Estaciones de Trabajo.**

Para (Lugo Cardozo, 2014), la virtualización de estaciones de trabajo o de escritorio es aquella que permite la separación del medio de procesamiento y almacenamiento local del escritorio del usuario con la máquina personal que hace uso. Este tipo de virtualización da lugar a que dichos medios se realicen en un servidor central que virtualiza un escritorio.

### 2.5.2. HYPERVISOR.

Es un software que crea y ejecuta máquinas virtuales (VM) y que además aísla el sistema operativo y los recursos del *hypervisor* de las máquinas virtuales, las crea y las gestiona.

**TIPOS DE HYPERVISOR:**

- **TIPO 1:** Nativos ***(Bare-Metal Hypervisor)***
- **TIPO2:** Alojados ***(Hosted Hypervisor)***

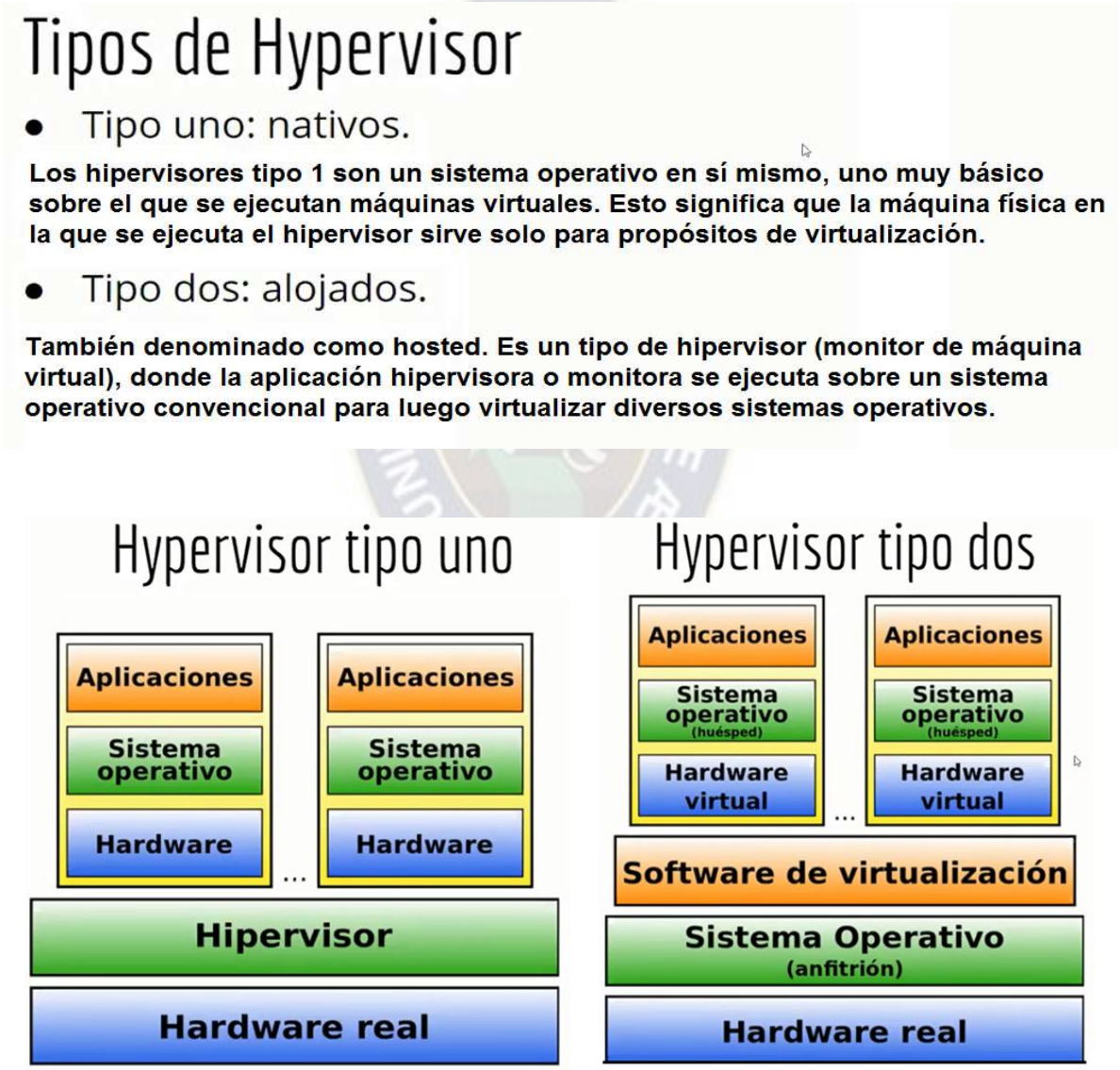
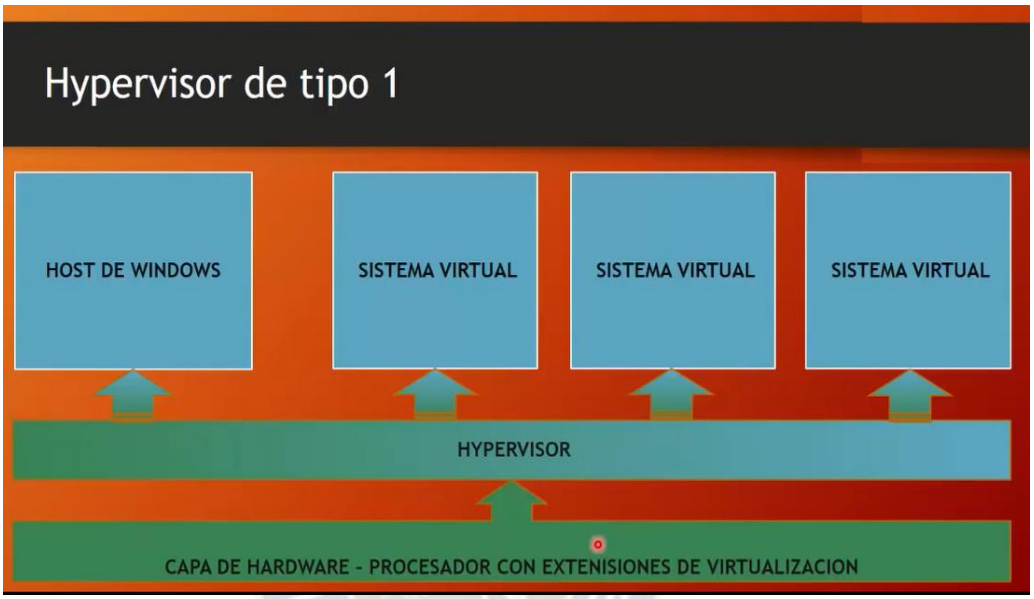



**Figura 7.** Tipos de Hypervisor.

**a). Hypervisor de tipo 1:**

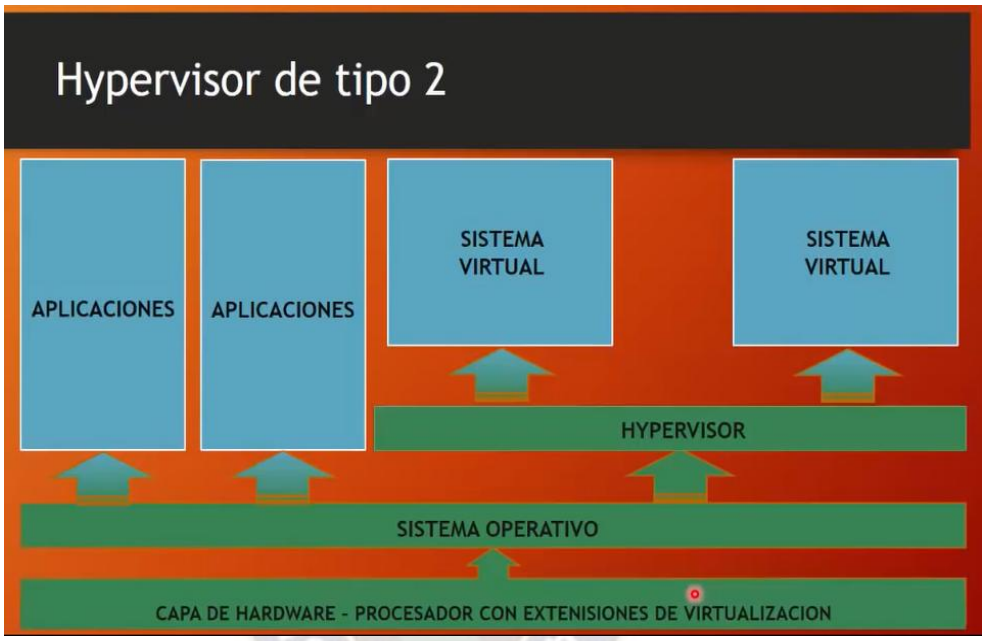
- Son también conocidos como Bare-Metal o nativo, y tienen acceso directo al Hardware. Contar con acceso directo al hardware ofrece un mayor rendimiento y escalabilidad, pero por el contrario tiene mayor problema de controladores.
- Las máquinas virtuales, así como los sistemas operativos instalados sobre esta capa, son independientes unas de otras, es decir tienen independencia de software.




- Entre los más comerciales tenemos a los Hypervisores tipo 1:

**b). Hypervisor de tipo 2:**

- El hypervisor tipo 2 se ejecuta sobre el sistema operativo, el cual se conoce también como "*hosted*".
- Por el contrario, la estabilidad y el rendimiento son menores, ya que toda la carga es soportada por un entorno de software (el sistema operativo) y además su estabilidad también es menor.




- Entre los más conocidos Hypervisores tipo 2 tenemos:


**OTROS: Parallels Desktop, VMware Player, QEMU, Bhyve, Estacion de Trabajo, Microsoft Virtual Server**

### 2.5.3. CLUSTER.

**¿Qué es un cluster?**

Un cúmulo, granja o cluster de computadoras, lo podemos definir como un ***sistema de procesamiento paralelo o distribuido***. Consta de un conjunto de computadoras independientes, interconectadas entre sí, de tal manera que funcionan como un solo recurso computacional.

En informática: Clúster se aplica a los ***conjuntos o conglomerados de ordenadores construidos mediante la utilización de hardware comunes y que se comportan como si fuesen una única computadora***. Clúster Un clúster se puede definir como un sistema de procesamiento paralelo o distribuido.

**¿Cómo funciona un clúster?**

Un clúster ***es una red de gestores de colas que están asociados lógicamente de alguna manera***. Los gestores de colas de un clúster pueden estar remotos físicamente. Por ejemplo, pueden representar las sucursales de una cadena de tiendas internacional y pueden estar situados físicamente en distintos países.

**¿Cómo se hace un clúster?**

Para crear un clúster, ***debe incluir como mínimo un nodo en el clúster y debe tener acceso a como mínimo uno de los nodos que formarán parte del clúster***. Si se especifica sólo un nodo, debe ser el sistema al que está accediendo actualmente.

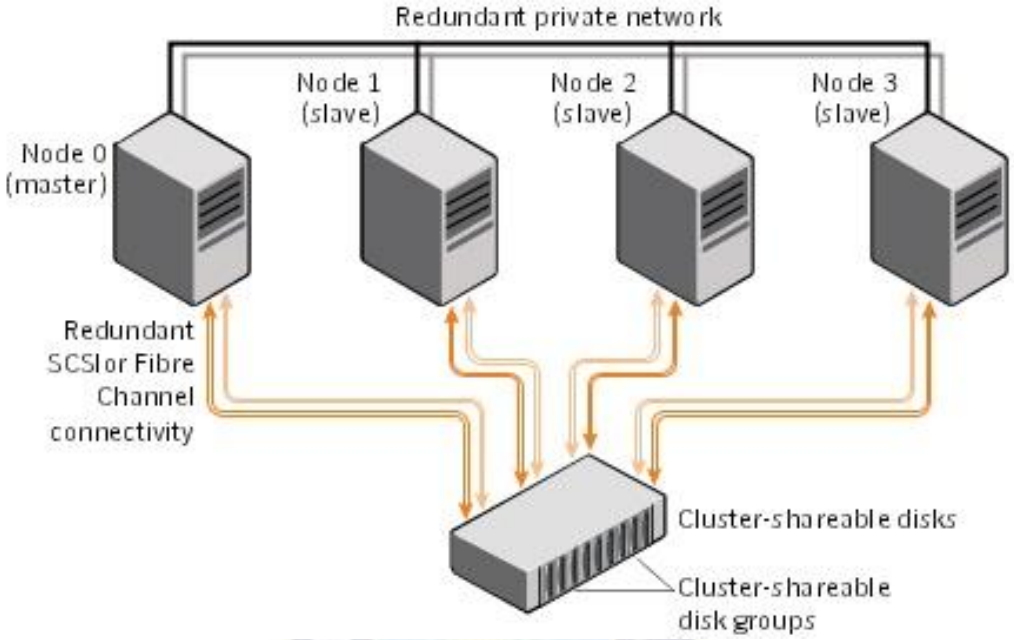



**Figura 8.** CLUSTER.

**Un clúster consta de varios componentes de hardware, entre los que se incluyen:**

- Nodos de ***clúster*** con discos locales (no compartidos)
- Almacenamiento multisistema (discos compartidos entre nodos)
- Medios extraíbles (cintas y CD-ROM)
- Interconexión del ***clúster***.
- Interfaces de red públicas.
- Sistemas cliente.

De manera general, ***un clúster necesita de varios componentes de software y hardware para poder funcionar.***

## 2.6. TERMINALES.

Una terminal es un dispositivo de hardware, ya sea de naturaleza electromecánica o electrónica, que se puede usar tanto para ingresar como para transcribir información. Esas tareas se pueden llevar a cabo bien desde un ordenador o echando mano de un sistema informático. Un ejemplo claro de terminal son los teletipos, esos textos informativos redactados por periodistas

de las agencias de noticias. Los de copia impresa aparecieron en nuestras vidas antes incluso que las pantallas de los ordenadores, aparecieron varias décadas antes. En el presente, es común una configuración que consta de monitor y teclado conectada a un ordenador más grande mediante una interfaz de red.

Los hay también de mano y dispositivos dedicados, como los que se utilizan normalmente para leer tarjetas de crédito y en los puntos de venta de un comercio determinado. La proliferación del hardware informático económico ha hecho posible que se pueda emplear un sistema totalmente funcional como terminal, para lo que se ha echado mano de software de emulación terminal que proporciona acceso a un ordenador central más grande. (GSC, 2022)

**Tipos de terminales informáticas:**

Con la definición del término ya hecha al respecto, es el momento de ir al tema central del post. Fundamentalmente, hay 5 tipos de terminales informáticas:

**Terminales Tontas**. Por su nombre parece una broma, pero no lo es. Su curiosa nomenclatura se debe a que tienen una capacidad muy escasa de procesamiento propio. Esto se traduce en que solamente envía y recibe señales de un ordenador central con el que conectan mediante líneas serie más grande, el cual se encarga de elaborar el procesamiento al completo. En resumen, las terminales tontas solamente pueden desplegar, recibir y enviar texto, pero no puede ejecutar un programa en dichas líneas serie. A ellas se conectan las derivadas de editores de texto, correo electrónico y juegos, entre otros. A su favor, hay que decir que son económicas y seguras dado que no pueden almacenar datos en un disco duro local y han de enrutar la información y las solicitudes mediante el sistema informático principal.

**Terminales Inteligentes.** Las terminales inteligentes son ordenadores o sistemas informáticos portátiles que gozan de los elementos básicos de una computadora personal estándar, como un disco duro, una memoria y varios puertos periféricos. Se encuentran conectados en red a un sistema informático central, de manera que pueden funcionar de dos formas. La primera consiste en ejecutar un software de cliente personalizado con el fin de interactuar con el mainframe, mientras que la segunda implica usar un software de emulación

terminal para imitar a un terminal tonto en una ventana dedicada. Su principal ventaja se halla en la permisividad que otorga al procesador local para hacer algunas tareas de procesamiento en vez de estar sujeto a dicho mainframe para todas las acciones.

**Terminales Portátiles.** Las terminales inteligentes portátiles se pueden observar en las empresas de envíos de paquetes o de comidas a domicilio, puesto que sus empleados van cambiando de ubicación durante el transcurso de su jornada laboral y echan mano de una pantalla y teclados en miniatura. Sin embargo, no es la única actividad profesional en las que son habituales, ya que se pueden ver también en el control de inventario de tiendas y compañías dedicadas al comercio, la topografía y la fabricación.

**Terminales En red.** Se distinguen de las inteligentes por el hecho de que el software completo que se ejecuta en ellas se extrae del mainframe. Eso sí, el ordenador local ejecuta los programas una vez que son recuperados.

**Terminales De transacciones.** Se emplean fundamentalmente para realizar funciones como la lectura de tarjetas de crédito o permitir el acceso a una cuenta bancaria. Un claro ejemplo son los cajeros automáticos que se ven en las calles. (GSC, 2022)

### 2.6.1. Terminales PC Desktop

Una terminal de computadora es el hardware que se utiliza para ingresar, recuperar y mostrar datos electrónicos. Si bien muchas personas piensan en la computadora de escritorio o portátil moderna que se coloca en una estación de trabajo como una terminal, estos dispositivos son solo los últimos tipos de terminales que se han utilizado a lo largo de los años. Con el advenimiento de las computadoras de las décadas de 1940 y 1950, surgió el concepto de estación de trabajo que permitía introducir información en la base de datos, así como recuperar información a partir de consultas, surgió el concepto original de terminal de computadora.

Uno de los primeros ejemplos de este tipo de hardware electromecánico fue la teleimpresora común. Si bien varias marcas y modelos variaban un poco en diseño, la mayoría incluía un teclado que se parecía mucho a una máquina de escribir. Esta estación de

mecanografía se adjuntó al sistema informático que albergaba los datos almacenados. Al usar el teclado para ingresar una consulta y luego presionar una tecla específica para comenzar la búsqueda, el sistema ubicaría la respuesta y luego imprimirá la respuesta en el papel con clavijas utilizado por la teleimpresora. Los terminales de este tipo ganaron popularidad en muchas editoriales y empresas de medios durante la década de 1950, ya que el uso de estos cerebros electrónicos para realizar verificaciones de datos ayudó a estas empresas a actualizar y mantener constantemente grandes cantidades de información sobre todo tipo de datos.

La mayoría de estos primeros dispositivos requerían el uso de tarjetas perforadas para agregar información a una base de datos. Las tarjetas perforadas se crearon utilizando equipo para perforar una pequeña tarjeta rectangular en puntos específicos a lo largo del cuerpo de la tarjeta. Cada tarjeta se introducía en una ranura del terminal, lo que permitía al sistema leer la tarjeta y convertir la información en datos electrónicos que luego se almacenaban en los bancos de memoria del sistema. Eran estos datos almacenados a los que el sistema podía acceder cuando se realizaba una consulta, traducir los datos a un lenguaje común y usar uno o más teletipo para proporcionar una impresión de la respuesta.

Con los avances tecnológicos de las décadas de 1970 y 1980, el concepto de terminal de computadora comenzó a cambiar algo. En lugar de una pequeña cantidad de terminales conectados a un mainframe, surgió la idea de una red de conexiones de escritorio a través de un servidor central. En la década de 1990, las estaciones de trabajo de muchas empresas ya no estaban equipadas con dispositivos como máquinas de escribir, sino que tenían un disco duro, un monitor y un teclado lo suficientemente pequeños como para caber en un escritorio de trabajo típico. En algunos casos, estos terminales más nuevos también incluían una impresora, aunque muchas empresas optaron por usar una sola impresora para dar servicio a varios terminales a la vez. A medida que la tecnología continuó mejorando las funciones electrónicas de estos sistemas más nuevos, las impresoras individuales en estaciones de trabajo individuales se volvieron más comunes.

Hoy en día, una terminal de computadora no solo permite al usuario conectarse con los datos guardados en un disco duro, o los datos almacenados en un servidor común dentro de la

empresa, sino también con la gran cantidad de información que se encuentra en Internet. Esta configuración contemporánea de la terminal continúa sufriendo cambios. Los avances tecnológicos ahora hacen posible el uso de computadoras portátiles e incluso algunos dispositivos de mano para conectarse de forma remota con bases de datos, ingresar y recuperar datos y, en general, realizar todas las tareas que antes solo eran posibles en un entorno de oficina. (Quesignificado, n.d.)

### 2.6.2. Terminal de Impresión

Son dispositivos que permiten imprimir en un medio físico como el papel la información local o remota enviada por los usuarios, el cual se constituye como un nodo más de la red informática. Con la popularización de estos dispositivos su masificación está constituido por Impresores, Plotters, en versiones a color o en blanco/negro. En la actualidad estos dispositivos son multifunción, con capacidades de escaneo y fotocopiadora. Con tecnologías de Impresión Láser o de tipo Tinta.

### 2.6.3. Terminal Dispositivo Móvil

Hoy en día, el dispositivo móvil, junto con su software asociado, cuenta con una gran capacidad de procesamiento y conectividad; esto, aunado a la disponibilidad de una enorme cantidad de información y al uso de técnicas avanzadas de tratamiento de datos y algoritmos de análisis cada vez más rápidos y eficientes, han convertido al dispositivo móvil en el centro de muchas de las actividades que el usuario final lleva a cabo cotidianamente desde hace ya algunos años. De este modo, el dispositivo móvil puede ofrecer una gran gama de prestaciones y servicios que antes no eran posibles

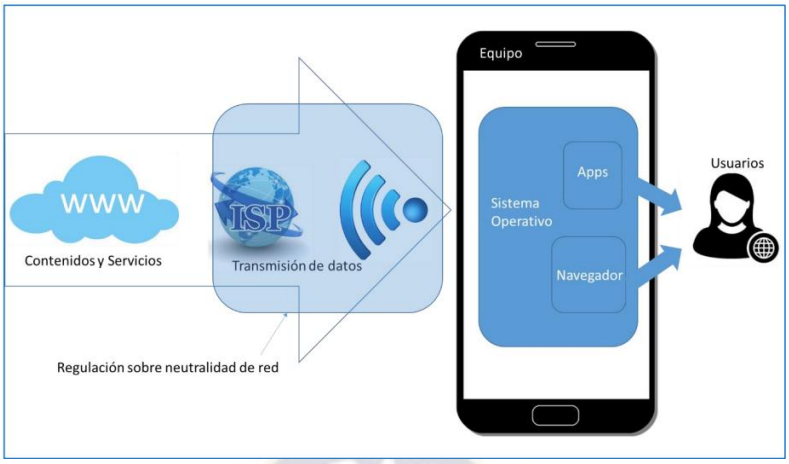



**Figura 9.** Terminal Dispositivo Móvil. (Cuevas, 2020)

Los elementos que integran esta cadena de acceso pueden identificarse de la siguiente manera:

- Dispositivo móvil (hardware), que incluye sensores y accesorios de entrada/salida, como bocinas, pantalla táctil, conexiones bluetooth, etc.
- Sistema operativo que gestiona las funcionalidades y recursos del dispositivo móvil, así como también permite que las aplicaciones instaladas en el dispositivo puedan acceder a las funcionalidades que el hardware brinda. En la actualidad, la tienda de aplicaciones puede estar estrechamente vinculada con el sistema operativo y el dispositivo mismo, lo que facilita que ciertas aplicaciones puedan ser instaladas con mayor facilidad y usadas de manera más eficiente que otras.
- Aplicaciones (Apps), que permiten el acceso a determinadas plataformas por medio de las cuales el usuario accede a servicios y contenidos.
- Un proveedor de acceso a Internet (ISP), que gestiona el medio por el cual el dispositivo puede acceder a Internet. (Cuevas, 2020)

## 2.7. CARACTERISTICAS DEL ALMACENAMIENTO

Conocemos algunas posibilidades de almacenamiento en Data Centers que posibilitan nuevas formas de archivar datos de forma segura y práctica. No obstante, nuevas tecnologías se desarrollan en busca de la reducción de costos. Algunas de esas tendencias incluyen desde la

configuración diferenciada de las redes hasta la utilización de nuevos equipos que puedan soportar y guardar una mayor cantidad de datos.

### 2.7.1. Unidades de discos duros (HDD)

La unidad de disco duro (HDD o Hard Disk Drive) es el disco duro original. Son dispositivos de almacenamiento magnéticos que se han utilizado desde la década de los cincuenta, aunque han evolucionado en el transcurso del tiempo. Un disco duro está compuesto de una pila de discos metálicos giratorios conocidos como platos. Cada disco giratorio tiene millones de diminutos fragmentos que se pueden magnetizar para representar bits (1s y 0s en código binario). Un brazo actuador con un cabezal de lectura y escritura escanea los platos giratorios y magnetiza los fragmentos para escribir información digital en la HDD o detecta las cargas magnéticas para leer la información de esta.

Las unidades de discos duros se utilizan para grabadores de TV, servidores y almacenamiento de computadoras portátiles y PC.

### 2.7.2. Discos de estado sólido (SSD o Solid State Drive)

Los discos de estado sólido surgieron mucho más recientemente, en la década de los noventa. Los SSD no dependen de imanes y discos, en su lugar, utilizan un tipo de memoria flash llamada NAND. En un SSD, los semiconductores almacenan información cambiando la corriente eléctrica de los circuitos que contiene la unidad. Esto significa que, a diferencia de los discos duros, los SSD no requieren partes móviles para funcionar.

Por ello, los SSD no solo funcionan de forma más rápida y fluida que las HDD (las HDD tardan más tiempo en recopilar información debido a la naturaleza mecánica de sus platos y cabezales), sino que también suelen durar más que las HDD (con tantas piezas móviles intrincadas, las HDD son vulnerables a los daños y al desgaste).

Además de las nuevas PC y las computadoras de gama alta, se pueden encontrar SSD en los smartphones, tablets y, a veces, en las cámaras de video.

### 2.7.3. Tendencias de almacenamiento

**Tecnología NAND 3D**

Hace mucho tiempo que los **SSD** son opciones de almacenaje en el mercado. Sin embargo, la presión para que sean más accesibles financieramente, y también en el aumento de su capacidad, han hecho que las empresas de tecnología especialistas en este chip desarrollaran una nueva tecnología: NAND 3D.

Este tipo de memoria usa una tecnología capaz de colocar en el chip, capas de células de almacenaje verticalmente, y no de forma horizontal (2D) como tradicionalmente se hace. En este momento, ya es posible encontrar dispositivos con hasta 48 capas, pero ingenieros ya están desarrollando tecnologías para una con 64 capas.

Según el formato estándar de 2.5 pulgadas, los nuevos SSD están en el mercado con una capacidad de hasta 16 Terabytes. El costo de estos dispositivos aún es elevado. (MundoContact, 2016)

**Compresión de datos**

Reducir el espacio ocupado por datos en determinado dispositivo, eliminar redundancias y aumentar el desempeño en transmisiones, son los principales beneficios traídos por la tecnología de compresión de datos. Con el desarrollo de nuevas matrices **AFA** (All-flash Arrays) es posible disminuir **80%** el espacio utilizado por un objeto. (MundoContact, 2016)

**NVDIMM: Non-Volatile Dual In-line Memory Module**

NVDIMM es una memoria RAM DIMM del computador que guarda datos eléctricos inclusive cuando se remueve la fuente de energía o cuando hay una inesperada pérdida de potencia, falla en el sistema o cuando se apaga el CPU, lo que cambia la forma en la que los computadores funcionan desde hace ya algunos años.

La idea es que la memoria principal ahora sea persistente y muy grande. Este es un cambio radical para las operaciones del banco de datos. Las NVDIMM pueden ser usadas para mejorar

el desempeño del aumento de una aplicación, la seguridad de datos y el tiempo de recuperación de fallas en el sistema. (MundoContact, 2016)

**RoCE**

RDMA over Converged Ethernet (RoCE) es un protocolo de red que permite que se acceda directamente a la memoria remota (RDMA) a través de una red de Ethernet. La ganancia está en poder reducir la sobrecarga y la latencia en el sistema. (MundoContact, 2016)

**Infraestructura Definida por Software**

SDI (Software-Defined Infrastructure) es un abordaje de Nube que llegó al mercado para transformar los Data Centers en instalaciones consolidadas y con un consumo optimizado de energía, con sistemas ágiles, de bajo consumo y basados en estándares abiertos. Algunos de sus beneficios son reducir las inversiones en hardware y software como también automatizar la provisión manual para mejorar la eficiencia de la administración y calidad de los servicios. (MundoContact, 2016)

**Nube Híbrida**

El costo del almacenamiento en la Nube (*cloud*) cayó a lo largo de los años. La Nube Híbrida es un lugar que permite el almacenamiento de hardware y software a un bajo costo y que inclusive es accesible para computadoras domésticas. (MundoContact, 2016)

**Almacenamiento WhiteBox**

La posibilidad de montar el propio sistema de almacenamiento, buscando en el mercado soluciones específicas para las necesidades de cada empresa, sugiere que exista la participación de COTS (Commercial off-the-shelf), ya que los proveedores tradicionales están desarrollando equipos que se conectan entre sí, aunque de marcas diferentes.

Este nuevo enfoque permite el acceso a las mismas tecnologías de grandes proveedores de Nube con precios más bajos. (MundoContact, 2016)

### 2.7.4. Storage Área Network (SAN)

Una SAN (Storage Área Network) aplica un modelo de red a los ambientes de almacenamiento en los Data Center. Las SANs operan detrás de los servidores para proveer una ruta común entre los servidores y los dispositivos de almacenamiento. A diferencia de las soluciones DAS (Directly Attached Storage) basadas en servidores y de los NAS (Network Attached Storage) orientadas a archivos, los SANs proveen un acceso a nivel de bloque o de archivo a los datos que son compartidos entre los recursos computacionales y personales. La tecnología SAN predominante se implementa en una configuración *Fibre Channel* (FC). A partir del crecimiento de los SANs y la denominación global del Internet Protocol (IP), el almacenamiento por medio de redes IP para transportar tráfico de almacenamiento se encuentra al frente del desarrollo técnico. Las redes IP proveen niveles crecientes de manejabilidad, interoperabilidad y costo-beneficio. Se pueden observar beneficios inmediatos en la consolidación de almacenamiento, virtualización, espejos, respaldo, y administración, gracias a la convergencia del almacenamiento con las redes existentes IP (LANs/MANs/WANs). La convergencia también provee incrementos en capacidad, flexibilidad, expansibilidad y escalabilidad.

Las dos principales normas que utilizan el protocolo IP son FCIP (Fibre Channel over IP), también conocido como iFCP en forma híbrida, e iSCSI (IP Small Computer System Interface). Ambas transportan comandos tanto Fibre Channel como SCSI incorporados dentro de un datagrama IP. Ambas fueron desarrolladas por la IETF (Internet Engineering Task Force). La diferencia entre las dos es que SCSI puede trabajar con los dispositivos existentes Ethernet, mientras que FCIP o iFCP, alternativamente definidos como Tunelaje Fibre Channel, pueden solamente trabajar con componentes Fibre Channel.

El Tunelaje es el encapsulamiento de comandos Fibre Channel dentro de un paquete IP para su transmisión en una red IP. Actualmente, 10Gigabit ethernet está ganando rápidamente popularidad para los backbones de los centros de datos corporativos. (Galvan, 2013)

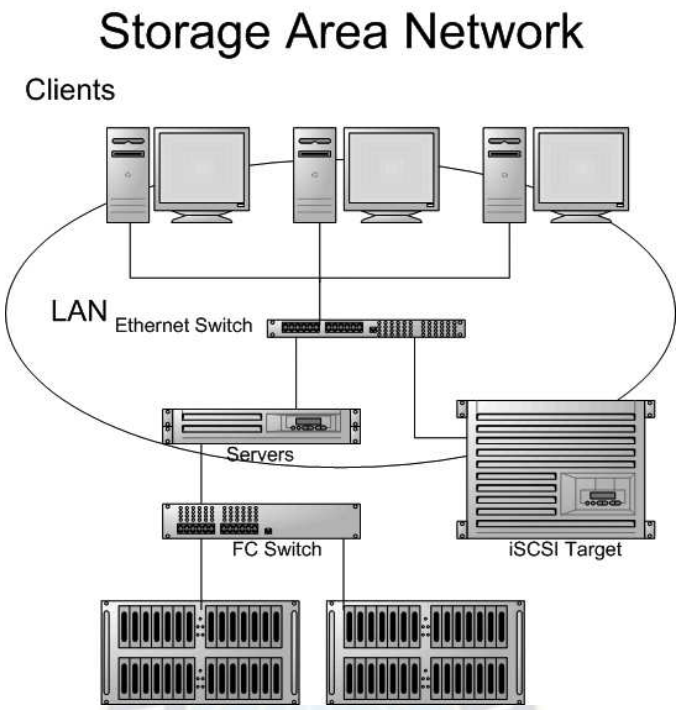



**Figura 10.** Storage Area Network (SAN). (Galvan, 2013)

### 2.7.5. Direct Attached Storage (DAS)

DAS es el método tradicional de anexar localmente dispositivos de almacenamiento a los servidores por medio de una ruta de comunicación directa entre el servidor y los dispositivos de almacenamiento. Tal como se muestra en la siguiente figura, la conectividad entre el servidor y los dispositivos de almacenamiento se encuentran en rutas dedicadas separadas de la conectividad a la red. El acceso se proporciona por medio de un controlador inteligente. El almacenamiento sólo puede ser accedido a través del servidor directamente conectado. Este método se desarrolló primordialmente para satisfacer demandas pequeñas en los puertos de unidades de los sistemas host de computadoras. Por lo que, cuando un servidor necesita más espacio de unidades, una unidad nueva de almacenamiento es anexada, permitiendo a un servidor ser espejo de otro. Esta funcionalidad también puede conseguirse por medio de servidores directamente anexados a las interfaces del servidor. (Galvan, 2013)

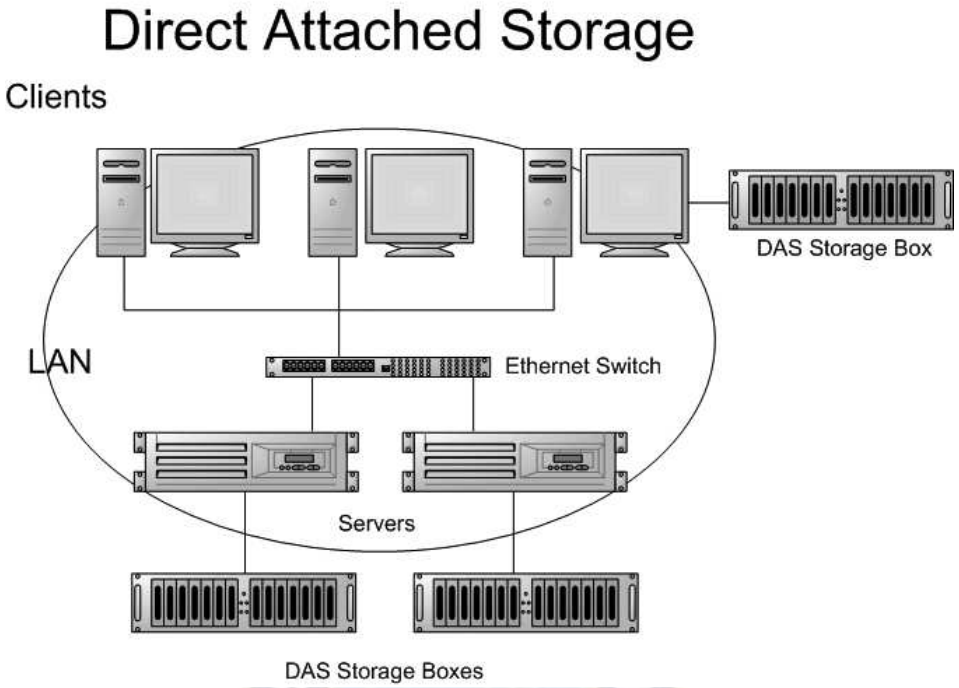



**Figura 11.** Direct Attached Storage (DAS). (Galván, 2013)

**Nota:** Las implementaciones 10G Categoría 6 se basan en una capacidad de canal teórica de cableado no blindado categoría 6/clase E. La transmisión de 10Gb/s sobre UTP se encuentra en evaluación por el grupo de estudio 10GBASE- T y puede estar limitada en longitud y requerir alguna mitigación, dependiendo de las capacidades de los equipos electrónicos.

### 2.7.6. Network Attached Storage (NAS)

NAS es una arquitectura de almacenamiento con acceso a un nivel de archivo con elementos de almacenamiento conectados directamente a una LAN. Este provee acceso a archivos a un sistema de computadoras heterogéneo. A diferencia de otros sistemas de almacenamiento, a este se accede directamente por medio de la red. Una capa adicional es agregada para cubrir los archivos almacenados compartidos. Este sistema generalmente utiliza NFS (Network File System) o CIFS (Common Internet File System) las cuales son aplicaciones IP. Una computadora separada usualmente actúa como "archivador", el cual es básicamente un controlador de acceso de tráfico y seguridad para el almacenamiento. La ventaja de este método es que varios servidores pueden compartir almacenamiento en una unidad separada. A diferencia de DAS, cada servidor no necesita su propio almacenamiento separado lo cual permite una

utilización más eficiente de la capacidad de almacenamiento disponible. El servidor puede soportar diferentes plataformas siempre y cuando usen el protocolo IP. (Galvan, 2013)

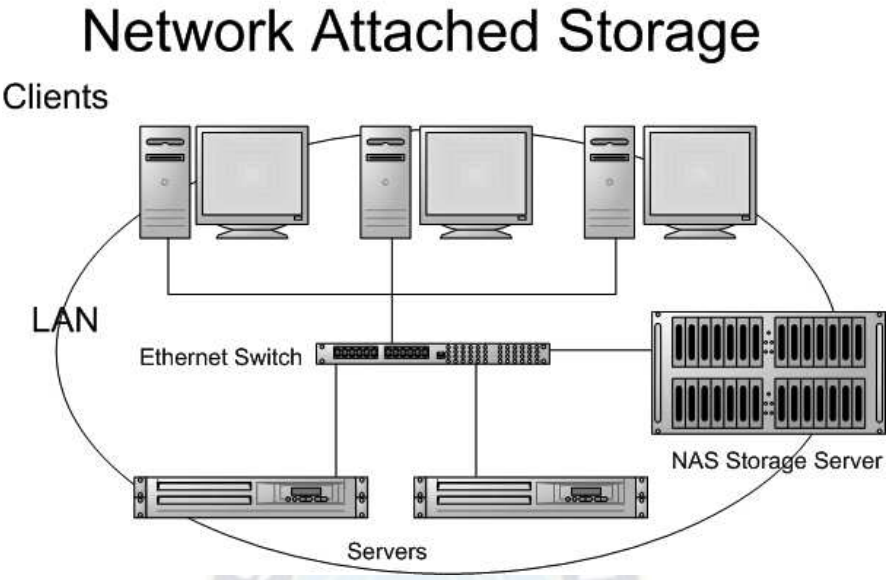



**Figura 12.** Network Attached Storage. (Galvan, 2013)

## 2.8. INFRAESTRUCTURA DE NETWORKING.

El centro de datos intranet se basa en la propuesta SAFE de Cisco para su diseño lógico. De acuerdo a dicha propuesta, estará constituido por las capas de: *Core, Agregación, Servicios, Acceso y acceso virtual.* La implementación del centro de datos intranet bajo este esquema, permite y facilita el crecimiento del centro de datos. Debido a que se diseña un centro de datos en base a TIER II, es necesario contar con un nivel de redundancia N+1 es decir, que todos los elementos tengan un respaldo (esto es aplicable para todo el equipo del centro de datos). A continuación, se presenta el diseño de cada una de las capas mencionadas. (Torrez, 2013)

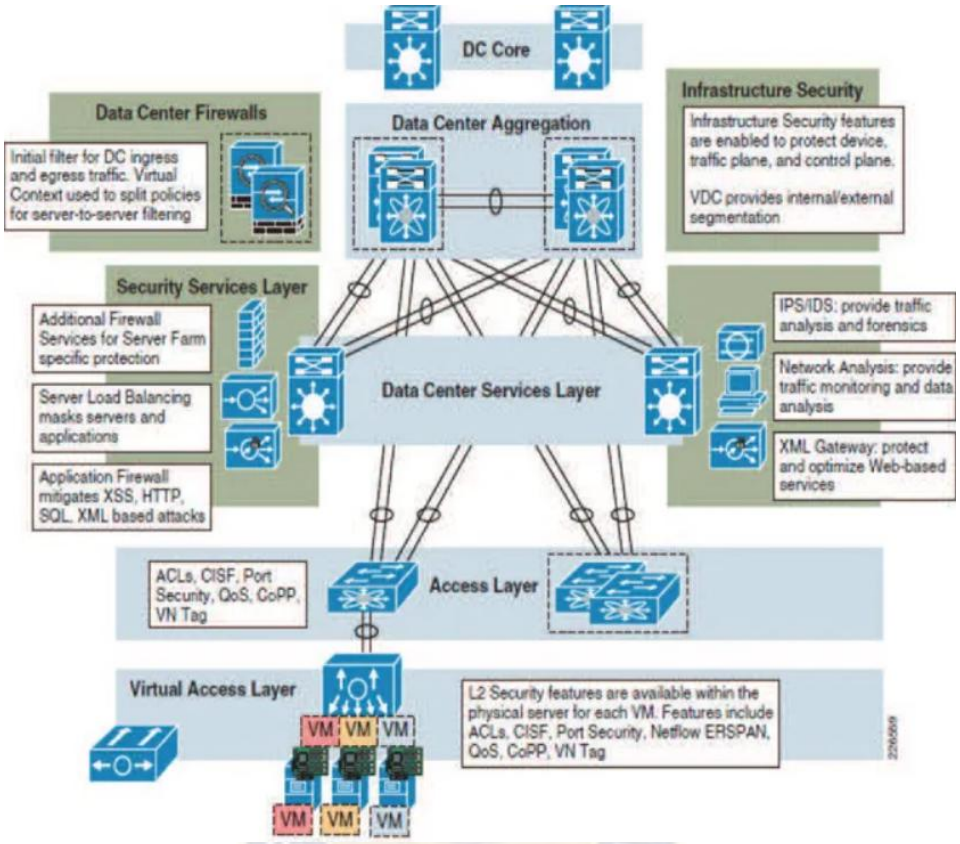



**Figura 13.** Estructura del módulo centro de datos intranet. (Torrez, 2013)

### 2.8.1. Capa de Core del Centro de Datos intranet

La capa de Core es la encargada de proveer conectividad de capa 3 entre el centro de datos intranet y la red del campus. Como la capa de Core es por la que atraviesa todo el tráfico del centro de datos intranet; y al ser un requerimiento el diseño de un centro de datos TIER 2 (N+1); se debe contar con redundancia para que el servicio no se vea interrumpido y tener puertos Gigabit Ethernet. Para tener una visibilidad completa de lo que sucede, debe permitir la implementación de SNMPv3 y Syslog. Para el manejo y autenticación de usuarios los equipos deben seguir las consideraciones hechas para el módulo de Core. Además, deben soportar IPv6 para cumplir con el requerimiento de la demanda.

Los switches de la capa de Core deben trabajar en capa 2 y 3 del modelo OSI. Para la capa 3 deben permitir los protocolos de enrutamiento EIGRP, OSPF y static IP Routing (para IPv4 e IPv6). Se utilizará OSPF (Open Shortest Path First) (OSPFv3 es la versión que soporta IPv6 definida en el RFC 2740) ya que es un protocolo abierto definido en el RFC 1583, a diferencia

de EIGRP que es propietario de Cisco (si bien EIGRP en equipos Cisco presenta una convergencia más rápida que OSPF). OSPF es un protocolo de estado de enlace, lo que le permite crear una topología exacta de la red (lo que le da ventaja sobre protocolos como RIP, que es del tipo vector distancia) y buscar la ruta más corta en función del ancho de banda. OSPF presenta una convergencia más rápida que IS-IS, y que RIP si bien su implementación es más compleja que ambos. En lo relativo a crecimiento y escalabilidad OSPF es más escalable que RIP. OSPF permite configurar autenticación MD5 para aceptar nuevas rutas o avisos de estado de enlace solo de routers cuya autenticidad sea comprobada. OSPF no utiliza TCP o UDP ya que tiene definido su propio paquete IP (protocolo IP 89), por lo que los firewalls y ACL deben estar configurados para permitir el paso de dicho protocolo. Debido a normas se debería tener redundancia implementada en la red Facultativa de Ingeniería U.M.S.A. es necesario configurar el balanceo de carga de OSPF para que ambos router funcionen al mismo tiempo. Para manejar los router redundantes se usará HSRP, de tal forma que si uno de los router falla el otro se haga responsable de todo el tráfico.

Para capa dos se deben tener los protocolos 802.1d (Spannig tree), 802.1s (Multiple Spanning Tree), 802.1w (RapidSpannig Tree), 802.1Q (VLAN), 802.1p para implementar calidad de servicio (QoS) mediante lo que se conoce como CoS. Debe tener 802.1x para control de acceso basado en puerto, ACLs y port security que es una funcionabilidad para implementar medidas de seguridad en los puertos. Como medidas de seguridad se filtrarán las rutas que se pueden propagar. Para el caso de la red Facultativa de Ingeniería U.M.S.A. esta función estará concentrada en el módulo de Core de la red principal, y será desempeñada por los switches de capa 3. (Torrez, 2013)

### 2.8.2. Capa de Agregación

La capa de agregación es la encargada de aislar la red del centro de datos intranet de la red del campus. En esta capa se ubican los firewalls encargados de controlar el tráfico que entra y sale de la red del centro de datos. Los equipos de esta capa deben permitir la implementación de al menos 10 contextos de seguridad para los diferentes perfiles de usuario. Debe trabajar con IPSec, SSL VPN, deben soportar VLANs y permitir la implementación de ACLs. Su función principal es realizar un NAT entre la red del centro de datos intranet y la red externa. Para

monitoreo deben contar con syslog, SNMPv3, NTP (todos los equipos deben contar con estos protocolos para monitoreo). Para algún caso se puede contar con dos firewalls para llevar a cabo esta tarea. Todo el tráfico que entre y salga del centro de datos intranet pasa por estos firewalls. Si bien es posible concentrar todas las funciones de esta capa en los equipos del módulo de Core (para disminuir los costos) no es recomendable sobrecargar de muchas funciones a la capa de Core ya que esto puede conducir a errores y la capa de Core es por donde atraviesa todo el tráfico. (Torrez, 2013)

Los firewalls que se ubican en esta capa deben permitir al momento de su implementación los siguientes protocolos y sus respectivos puertos:

- DHCP: 67, 68 (UDP)
- DNS: 53 (TCP, UDP)
- Proxy: 3128 (TCP)
- SNMP: 161, 162 (TCP, UDP)
- NTP: 123 (TCP) o Syslog: 514 (UDP)
- SQL: 3306 (TCP)
- Kerberos: 88 (TCP)
- LDAP: 389 (TCP, UDP)
- TACACS+: 49 (TCP)
- NFS: 2049 (TCP)
- SAMBA: 137, 138, 139, 445 (TCP, UDP)
- SSH: 22 (TCP)

Una vez la red se encuentre en funcionamiento se debe monitorear para establecer que otros protocolos son necesarios. (Torrez, 2013)

### 2.8.3. Capa de Servicios

La capa de servicios es la capa donde se ubican los IDS, IPS, firewalls de aplicación web (WAF) y demás equipos de monitoreo. Constituye una capa adicional que permite la expansión de los servicios de monitoreo y seguridad sin que se requiera un rediseño de la red. Todas las

funcionalidades de esta capa serán realizadas por los firewalls de la capa de agregación, los cuales estarán configurados para trabajar como firewalls, IPS y WAF.

La configuración como IPS o *inline mode*, si bien consume más recursos que la configuración como IDS o *promiscuous mode*, proporciona una protección en tiempo real deteniendo los ataques conocidos antes de que alcancen su objetivo. Para el tráfico entre servidores virtuales se configurará un *puerto mirror* en el switch virtual de tal forma que todo el tráfico pueda ser monitoreado. (Torrez, 2013)

### 2.8.4. Capa de Acceso

Es la encargada de proporcionar conectividad de capa 2 a los servidores. Su función es incrementar la densidad de puertos con los que se cuenta para la granja de servidores. En esta capa es imprescindible el uso de VLANs, para segmentar el tráfico de los servidores, así como de ACLs para impedir flujos de tráfico no deseados. Se utilizarán switches de capa 2. Los switches deben cumplir los protocolos de capa dos mencionados para la capa de core del centro de datos intranet.

Los switches de la capa de acceso del módulo centro de datos intranet contarán con un puerto mirror conectado al IDS (esto con el fin de monitorear el tráfico de los servidores virtuales). (Torrez, 2013)

### 2.8.5. Capa de Acceso Virtual

La capa de acceso virtual reside en los servidores físicos que implementan el software de virtualización. Debido a que con el uso de tecnologías de virtualización puede existir tráfico entre servidores virtuales, que se encuentren en una misma máquina física. Este tráfico no tendría que abandonar la máquina física en cuestión; es decir no circularía por la red física, lo que a su vez impediría que sea monitoreado y/o controlado por las políticas existentes de la red. Para lidiar con este tipo de problemas se utilizará un software de virtualización de servidores que permiten la implementación de switches virtuales (como VMWare vSphere). Los switches virtuales permiten la implementación de *puertos mirrors* lo que permiten. Además, los switches virtuales permiten implementar las políticas de seguridad de la red física de tal

forma que no se pierda el control de la red. El software que se utilizaría es VMware vSphere versión 546, ya que este es el software más común que cuenta actualmente la mayor parte de redes IP. La configuración de adaptador virtual que se utilizaría para las máquinas virtuales seria e100047, ya que es la recomendada para arquitecturas de 64 bits (vlance es para arquitectura de 32 bits). Se elige la configuración e1000, ya que vmxnet necesita que el sistema "guest" tenga instalado los vmware tools (para evitar posibles incompatibilidades con los sistemas), y; vswif y vmknic son solo para los servicios de consola ESX server.

La interfaz física del equipo estará conectada directamente a un puerto trunk del switch físico y virtualmente asignada a un puerto uplink48 del switch virtual. El switch virtual tendrá configuradas dos VLANs, una para administración y otra para el resto de datos. La configuración de las VLANs será en modo virtual switch ta-gging VST, en este modo se crea un Port group en el switch virtual para cada VLAN que se tenga (el switch virtual es el encargado añadir o quitar las etiquetas de VLANs). Además, cada servidor contará con dos interfaces de red por motivos de disponibilidad. Ambas interfaces estarán conectadas a la red física mediante un puerto trunk del switch. En la red virtual se configurará las interfaces para que trabajen una a la vez, y cuando falle la conexión de la primera, esta sea inmediatamente sustituida por la segunda para lo que se utilizará la configuración Beacon Probing de VMware vSphere 5. (Torrez, 2013)

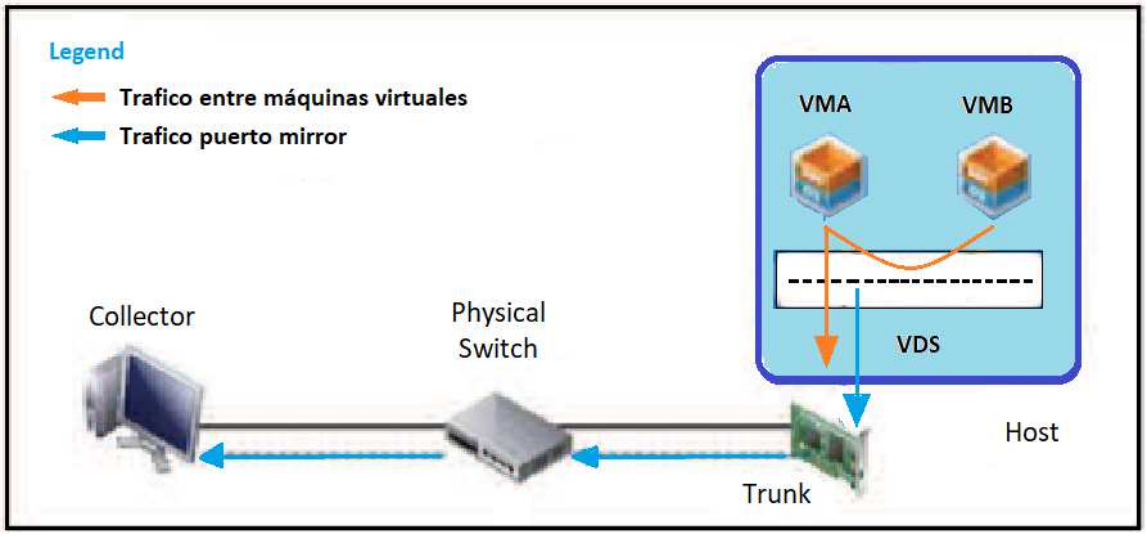



**Figura 14.** Flujo de tráfico de monitoreo. (Torrez, 2013)

## 2.9. RESPALDO (BackUp)

La copia de seguridad, también llamada respaldo o *backup,* se refiere a la copia de archivos físicos o virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo u otra catástrofe. El proceso de copia de seguridad de los datos es fundamental para un plan de recuperación de desastres (DRP) exitoso.

Un proceso de copia de seguridad se aplica a las bases de datos críticas o aplicaciones de línea de negocio relacionadas. El proceso se rige por políticas predefinidas de respaldo que especifican la frecuencia con la que se realiza la copia de seguridad de los datos y la cantidad de copias duplicadas (conocidas como réplicas), con la que se deben restaurar los datos.

Las mejores prácticas sugieren que se debe programar una copia de seguridad completa de los datos al menos una vez a la semana, a menudo durante los fines de semana o fuera del horario laboral. Para complementar las copias de seguridad completas semanales, las empresas generalmente programan una serie de tareas de respaldo de datos incrementales o diferenciales que solo realizan copias de los datos que han cambiado desde la última copia de seguridad completa. (Rouse, 2022)

### 2.9.1. Medios de almacenamiento de copia de seguridad

Las empresas suelen realizar respaldo de datos clave en dispositivos de copia de seguridad dedicados o sistemas de cinta magnéticos. Los sistemas de duplicación de datos contienen unidades de disco duro (HDD) y están equipados con software para establecer políticas de respaldo.

Los sistemas de copia de seguridad de disco a disco aparecieron inicialmente como una alternativa a las bibliotecas de unidades de cinta de copia de seguridad magnética. Tanto el disco como la cinta todavía se usan hoy, y con frecuencia en conjunto.

A medida que aumentan los tamaños de los archivos, algunos proveedores de sistemas de respaldo han lanzado al mercado dispositivos de protección de datos integrados para simplificar

el proceso de copia de seguridad. Un dispositivo de datos integrado es esencialmente un servidor de archivos equipado con HDD y software de respaldo desarrollado por el proveedor. Estos dispositivos de almacenamiento de datos *plug-and-play* a menudo incluyen funciones automatizadas para monitorear la capacidad del disco, el almacenamiento expandible y las bibliotecas de cintas preconfiguradas.

La mayoría de los dispositivos de respaldo basados en disco permiten que las copias se muevan de medios giratorios a cintas magnéticas para una retención a largo plazo. Los sistemas de cinta magnética todavía se utilizan como medios de respaldo debido al aumento de las densidades de cinta y al aumento de los sistemas de archivo de cinta lineal. Una biblioteca de cintas virtuales (VTL) proporciona una opción menos costosa para una matriz de duplicación. Una VTL es un sistema basado en disco cuyo comportamiento imita al de una biblioteca de cintas físicas.

Las unidades de estado sólido (SSD) generalmente no se utilizan para la copia de seguridad de datos debido a problemas de tecnología de la red. Algunos proveedores de almacenamiento incluyen SSD como una herramienta de almacenamiento en caché o de niveles para administrar escrituras con arrays basados en disco. Los datos se almacenan inicialmente en caché en el almacenamiento flash y luego se escriben en el disco. (Rouse, 2022)

### 2.9.2. Copia de seguridad local y respaldo sin conexión para el almacenamiento primario

Los sistemas de almacenamiento primario modernos han evolucionado para ofrecer capacidades nativas más sólidas para el respaldo de datos. Estas características incluyen esquemas avanzados de protección RAID, instantáneas ilimitadas y herramientas para replicar instantáneas en una copia de seguridad secundaria o incluso en una copia de seguridad terciaria externa. A pesar de estos avances, el respaldo basado en el almacenamiento primario tiende a ser más costoso y carece de las capacidades de indexación que se encuentran en los productos de copia de seguridad tradicionales. La duplicación de datos, por ejemplo, apareció por primera vez en los dispositivos de respaldo de EMC Data Domain, pero gradualmente se está convirtiendo en una característica de referencia de los arreglos de almacenamiento primario de marca.

Los respaldos locales colocan copias de datos en discos duros externos o sistemas de cinta magnética, que generalmente se encuentran en o cerca de un centro de datos local. Los datos se transmiten a través de una conexión de red segura de banda ancha o de una intranet corporativa. Una de las ventajas de la copia de seguridad local es la capacidad de realizar una copia de seguridad de los datos detrás de un firewall de red. La copia de seguridad local también es mucho más rápida y proporciona un mayor control sobre quién puede acceder a los datos.

La copia de seguridad sin conexión o en frío es similar al respaldo local, aunque a menudo se asocia con la copia de seguridad de una base de datos. Un respaldo fuera de línea incurre en tiempo de inactividad desde que se realiza el proceso de copia de seguridad mientras la base de datos está desconectada de su red. (Rouse, 2022)

### 2.9.3. Respaldo y almacenamiento en la nube

A la inversa, la copia de seguridad fuera del sitio transmite copias de datos a una ubicación remota, que puede incluir el centro de datos secundario de una empresa o la instalación de colocación arrendada. Cada vez más, la copia de seguridad de datos fuera del sitio equivale al almacenamiento en la nube basado en suscripción como un servicio, que proporciona una capacidad escalable y de bajo costo y elimina la necesidad del cliente de comprar y mantener hardware de respaldo. A pesar de su creciente popularidad, la elección de la copia de seguridad como un servicio requiere que los usuarios cifren los datos y tomen otras medidas para salvaguardar la integridad de los datos.

El respaldo en la nube se divide en lo siguiente:

- **Almacenamiento público en la nube:** los usuarios envían datos a un proveedor de servicios en la nube, que les cobra una tarifa de suscripción mensual basada en el almacenamiento consumido. Hay tarifas adicionales por ingreso y egreso de datos. Amazon Web Services (AWS), Google Compute Engine y Microsoft Azure son actualmente los mayores proveedores de nube pública.

- **Almacenamiento en la nube privada:** se realiza un respaldo de los datos en diferentes servidores dentro del firewall de la compañía, generalmente entre un centro de datos local y un sitio de recuperación de desastres secundario. Por esta razón, el almacenamiento en la nube privada a veces se denomina almacenamiento interno en la nube.
- **Almacenamiento híbrido en la nube:** una empresa usa almacenamiento local y externo. Las empresas suelen utilizar el almacenamiento en la nube pública de forma selectiva para el archivo de datos y la retención a largo plazo. Utilizan el almacenamiento privado para el acceso local y la copia de seguridad para un acceso más rápido a sus datos más críticos.

La mayoría de los proveedores de copias de seguridad permiten respaldar las aplicaciones locales en una nube privada dedicada, tratando de manera efectiva la copia de seguridad de datos basada en la nube como una extensión del centro de datos físico del cliente. También conocido como recuperación de desastres como un servicio (DRaaS), este campo de maduración permite a una organización arrendar espacio en los servidores de almacenamiento de un proveedor de servicios para la copia de seguridad centralizada y la gestión de datos de la línea de vida.

La copia de seguridad de datos de nube a nube es un enfoque alternativo que ha ido ganando impulso. Con este método, los datos de un cliente se copian de una plataforma de copia de seguridad en la nube a otra nube. También se refiere a las copias de seguridad basadas en la nube de datos almacenados en plataformas de software como servicio (SaaS). (Rouse, 2022)

### 2.9.4. Tipos de copia de seguridad definidos

***La copia de seguridad completa*** captura una copia de un conjunto de datos completo. Aunque se considera el método de copia de seguridad más confiable, realizar un respaldo completo requiere mucho tiempo y requiere una gran cantidad de discos y/o cintas. La mayoría de las organizaciones ejecutan copias de seguridad completas solo periódicamente.

***La copia de seguridad incremental*** ofrece una alternativa al respaldo completo al hacer una copia de seguridad de los datos que han cambiado desde la última copia completa. El inconveniente es que una restauración completa toma más tiempo si se utiliza una copia de respaldo de datos basada en incrementos para la recuperación.

***La copia de seguridad diferencial*** copia datos cambiados desde la última copia de seguridad completa. Esto permite que una restauración completa ocurra más rápidamente al requerir solo la última copia de seguridad completa y la última copia de seguridad diferencial. Por ejemplo, si crea un respaldo completo el lunes, el respaldo del martes, en ese momento, sería similar a una copia de seguridad incremental. El respaldo del miércoles luego haría una copia de seguridad del diferencial que ha cambiado desde la copia de seguridad completa del lunes. El inconveniente es que el crecimiento progresivo de las copias de seguridad diferenciales tiende a afectar negativamente su ventana de respaldos. Una copia de seguridad diferencial genera un archivo al combinar una copia completa anterior con una o más copias incrementales creadas posteriormente. El archivo ensamblado no es una copia directa de ningún archivo actual o creado anteriormente, sino que se sintetiza a partir del archivo original y cualquier modificación posterior de ese archivo.

***La copia de seguridad completa sintética*** es una variación de la copia de seguridad diferencial. En una copia de seguridad completa sintética, el servidor de respaldos produce una copia completa adicional, que se basa en el respaldo completo original y en los datos obtenidos de copias incrementales.

***Las copias de seguridad incrementales continuas*** minimizan la ventana de copia de seguridad al tiempo que proporcionan un acceso más rápido a la recuperación de datos. Un respaldo incremental continuo captura el conjunto de datos completo y luego lo complementa con copias de seguridad incrementales a partir de ese momento. El respaldo de bloques modificados también se conoce como diferenciación delta. Las copias completas de los conjuntos de datos normalmente se almacenan en el servidor de copia de seguridad, lo que automatiza la restauración.

***Las copias de seguridad incrementales inversas*** son cambios realizados entre dos instancias de un espejo. Una vez que se realiza un respaldo completo inicial, cada copia de seguridad incremental sucesiva aplica cualquier cambio a la copia completa existente. Básicamente, esto genera una nueva copia de seguridad completa sintética cada vez que se aplica

un cambio incremental, al mismo tiempo que proporciona una reversión a los respaldos completos anteriores.

***La copia de seguridad en caliente***, también conocida como copia de seguridad dinámica, se aplica a los datos que permanecen disponibles para los usuarios a medida que la actualización está en proceso. Este método evita el tiempo de inactividad del usuario y la pérdida de productividad. El riesgo con la copia de seguridad activa es que, si los datos se modifican mientras el respaldo está en curso, la copia resultante puede no coincidir con el estado final de los datos. (Rouse, 2022)

### 2.9.5. Técnicas y tecnologías para complementar el respaldo de datos

La ***protección continua de datos (CDP)*** se refiere a capas de tecnologías asociadas diseñadas para mejorar la protección de datos. Un sistema de almacenamiento basado en CDP realiza un respaldo de todos los datos de la empresa cada vez que se realiza un cambio. Las herramientas CDP permiten crear múltiples copias de datos. Muchos sistemas de protección continua de datos contienen un motor incorporado que replica datos de un servidor de respaldo primario a uno secundario y/o almacenamiento basado en cinta. La copia de seguridad de disco a disco a cinta es una arquitectura popular para los sistemas CDP.

El sistema ***CDP casi continuo*** toma instantánea de respaldo a intervalos establecidos, que son diferentes de las instantáneas de proveedores basados en matrices que se toman cada vez que se escriben nuevos datos en el almacenamiento.

La ***reducción de datos*** disminuye su huella de almacenamiento. Existen dos métodos principales: compresión de datos y duplicación de datos. Estos métodos se pueden utilizar individualmente, pero los proveedores a menudo combinan los enfoques. Reducir el tamaño de los datos tiene implicaciones en las ventanas de copia de seguridad y los tiempos de restauración.

La ***clonación de discos*** implica copiar el contenido del disco duro de una computadora, guardarlo como un archivo de imagen y transferirlo a los medios de almacenamiento. La

clonación de discos se puede usar para el aprovisionamiento, aprovisionamiento del sistema, recuperación del sistema y reinicio o retorno de un sistema a su configuración original.

El ***código de borrado***, también conocido como *corrección de errores directa*, evolucionó como una alternativa escalable a los sistemas RAID tradicionales. La codificación de borrado más a menudo se asocia con el almacenamiento de objetos. RAID distribuye las escrituras de datos en varias unidades, utilizando una unidad de paridad para garantizar la redundancia y la capacidad de recuperación (resiliencia). La tecnología divide los datos en fragmentos y los codifica con otros bits de datos redundantes. Estos fragmentos codificados se almacenan en diferentes medios de almacenamiento, ubicaciones geográficas o nodos. Los fragmentos asociados se utilizan para reconstruir datos corruptos, utilizando una técnica conocida como sobre-muestreo (*oversampling*).

La ***copia de seguridad plana*** es un esquema de protección de datos en el que una copia directa de una instantánea se traslada al almacenamiento de bajo costo sin el uso del software de respaldo tradicional. La instantánea original conserva su formato y ubicación nativos; la réplica de respaldo plana se monta, en caso de que el original no esté disponible o sea inutilizable.

La ***duplicación, espejeo o mirroring***, coloca los archivos de datos en más de un servidor de cómputo para garantizar que permanezca accesible a los usuarios. En la duplicación síncrona, los datos se escriben en el disco local y remoto simultáneamente. Las escrituras desde el almacenamiento local no se reconocen hasta que se envía una confirmación desde el almacenamiento remoto, lo que garantiza que los dos sitios tengan una copia de datos idéntica. A la inversa, se considera que las escrituras locales asíncronas están completas antes de que se envíe la confirmación desde el servidor remoto.

La ***replicación*** permite a los usuarios seleccionar el número requerido de réplicas o copias de los datos necesarios para mantener o reanudar las operaciones comerciales. La replicación de datos copia los datos de una ubicación a otra, proporcionando una copia actualizada para acelerar la recuperación de desastres.

La ***recuperación en el lugar, o la recuperación instantánea***, permite a los usuarios ejecutar temporalmente una aplicación de producción directamente desde una instancia de máquina virtual (VM) de copia de seguridad, manteniendo así la disponibilidad de datos mientras se restaura la VM principal. El montaje de una instancia física o de máquina virtual directamente en un servidor de respaldo o de medios puede acelerar la recuperación a nivel de sistema en minutos. La recuperación de una imagen montada produce un rendimiento degradado, ya que los servidores de respaldo no están dimensionados para las cargas de trabajo de producción.

Las ***instantáneas de almacenamiento*** capturan un conjunto de marcadores de referencia en el disco para una base de datos, archivo o volumen de almacenamiento determinado. Los usuarios se refieren a los marcadores, o punteros, para restaurar datos desde un punto seleccionado en el tiempo. Debido a que se deriva de un volumen de origen subyacente, una instantánea de almacenamiento individual es una instancia, no una copia de seguridad completa. Como tal, las instantáneas no protegen los datos contra fallas de hardware.

Las instantáneas generalmente se agrupan en tres categorías: bloque modificado, clones y CDP. Las instantáneas aparecieron por primera vez como una herramienta de administración dentro de una matriz de almacenamiento. El advenimiento de la virtualización agregó instantáneas basadas en hipervisor. Las instantáneas también pueden implementarse mediante un software de respaldo o incluso a través de una máquina virtual. (Rouse, 2022)

## 2.10. SEGURIDAD (Firewall)

La **seguridad del centro de datos** aborda las prácticas y la preparación que mantienen un centro de datos protegido frente a amenazas, ataques y el acceso no autorizado. Algunos aspectos de la seguridad del centro de datos son la seguridad física, que requiere la planificación de las instalaciones para evitar intrusiones físicas, y la seguridad de la red, donde los ingenieros de seguridad instalan contraseñas y programas de protección ante programas maliciosos para evitar vulneraciones. Más recientemente, la seguridad de ingeniería social se ha convertido en

un aspecto importante de la protección del centro de datos. Implica educar a los usuarios sobre buenas prácticas de seguridad y cómo mantenerlas a través de campañas de concienciación que garanticen que las personas autorizadas no revelen sin querer información que otras personas no autorizadas puedan utilizar para superar las medidas de seguridad existentes.

**¿Quién necesita la seguridad del centro de datos?**

Todas las empresas que confíen en un centro de datos para todas sus operaciones o algunas de ellas deberían aplicar varias medidas de seguridad físicas y de red que protejan la información incluida en el centro de datos contra pérdidas, una manipulación malintencionada y el robo. Hoy en día, todas las empresas se pueden considerar empresas tecnológicas, puesto que muy pocas podrían hacer negocios sin algún tipo de tecnología. La mayoría de las empresas han hecho la transición del soporte en papel al entorno digital, y actualmente la mayor parte de la información se encuentra en un ordenador en vez de un archivador. Todas las empresas necesitan una forma de asegurarse de que la información de sus centros de datos esté segura y protegida.

**¿Por qué elegir la seguridad del centro de datos?**

Dado que los centros de datos alojan información, aplicaciones y servicios que las empresas utilizan cada día, las organizaciones deben asegurarse de que usan las medidas de seguridad adecuadas para proteger esos centros de datos. La falta de una seguridad eficaz del centro de datos puede dar lugar a una vulneración de los datos en la que se revele o se robe información confidencial de la empresa o, lo que sería peor, información de los clientes. Este tipo de vulneración de los datos puede salir muy cara, tanto en el plano económico como para la reputación de la empresa. Algunas empresas no llegan a recuperarse de una vulneración de los datos.

La velocidad de los avances tecnológicos conlleva una rápida evolución de las amenazas a la seguridad. Y, dado que las tecnologías de centro de datos están cada vez más virtualizadas, aumenta también la necesidad de seguridad del centro de datos en la capa de infraestructura. La seguridad integrada en el software ofrece un enfoque de seguridad más detallado, junto con una mayor agilidad y adaptación al afrontar amenazas a la seguridad. (VMware, 2022)

### 2.10.1. Cómo proteger un centro de datos

Un centro de datos es un clúster centralizado de recursos informáticos y de red que almacena y procesa información esencial de una empresa en una única ubicación física. Las empresas deben usar medidas de seguridad tanto físicas como virtuales para proteger el centro de datos. La seguridad de la red es una cuestión más que tener en cuenta para proteger el centro de datos, ya que los programas maliciosos y otras amenazas pueden acceder al centro de datos a través de la red. (VMware, 2022)

### 2.10.2. Medidas de Seguridad para el Centro de Datos

Las soluciones de seguridad más eficaces para los centros de datos son aquellas que incluyen herramientas de seguridad tanto físicas como virtuales. Dado que los equipos alojados en un centro de datos son tanto confidenciales como voluminosos, hay que tener en cuenta ciertas consideraciones especiales en cuanto a la seguridad física. El agua y la electrónica no son una buena combinación, de modo que los sistemas antincendios tradicionales no sirven para un centro de datos. Además, como los centros de datos están conectados a redes externas a través del acceso de los usuarios, los administradores de TI deben asegurarse de implantar las políticas se seguridad adecuadas en cuanto a red y usuarios en cada punto que tenga acceso al centro de datos. Las medidas de seguridad virtuales incluyen formas de confirmar la identidad de los usuarios autorizados, como puede ser la autenticación multifactor, y software que mantiene a raya a los usuarios no autorizados, como puede ser un cortafuegos. (VMware, 2022)

### 2.10.3. Seguridad Física

Las medidas de seguridad físicas de un centro de datos dependen de su tamaño. Los centros de datos suelen contener gran cantidad de equipos informáticos: servidores, conmutadores y enrutadores, infraestructuras de alimentación y refrigeración, así como equipos de telecomunicaciones. Estos equipos pueden encontrarse en un armario, que se puede proteger fácilmente con un candado físico, o en un almacén, donde sería más adecuado implantar medidas adicionales de seguridad física como acceso con distintivo, video vigilancia, alarmas o guardias de seguridad.

La protección antincendios es una cuestión de seguridad física aparte. Puesto que un centro de datos contiene equipos electrónicos delicados, los sistemas químicos antincendios son mejor opción que los rociadores para proteger los equipos en caso de incendio. (VMware, 2022)

### 2.10.4. Seguridad Virtual

Hoy en día, muchos centros de datos utilizan tecnología de virtualización, que permite desvincular el almacenamiento, la red y los servidores del centro de datos. Esta desvinculación permite a los administradores de TI gestionar los servicios del centro de datos de forma remota, y usar software para llevar a cabo operaciones del centro de datos y para distribuir cargas de trabajo al instante en varios servidores según las necesidades. Algunos centros de datos utilizan la tecnología de virtualización para acceder a la cloud pública y como componente de su infraestructura del centro de datos. El uso de software o soluciones de cloud para estructurar y gestionar el centro de datos añade flexibilidad, pero también hace que el centro de datos sea más vulnerable a los ciberataques.

Algunos programas de software de red de centro de datos incluyen seguridad dentro de la solución o están diseñados para funcionar con otras herramientas de seguridad virtual como cortafuegos y sistemas de detección y prevención de intrusiones. Los gestores de TI pueden usar este software para establecer políticas que identifiquen a los usuarios y determinen qué usuarios pueden acceder al centro de datos. La identificación de dos factores, donde la identidad de un usuario se confirma preguntando algo que sabe (por ejemplo, una contraseña) y usando algo que tiene (por ejemplo, un teléfono móvil) es un método fiable que los departamentos de TI pueden utilizar para asegurarse de que solo los usuarios autorizados tengan acceso a una red conectada al centro de datos.

El software de seguridad del centro de datos no solo impide que los usuarios no autorizados vean o roben datos confidenciales, sino que también se puede utilizar para hacer una copia de seguridad de la información incluida en el centro de datos para protegerla ante pérdidas. (VMware, 2022)

### 2.10.5. Infraestructura de la Seguridad de Red

Para proteger el centro de datos frente al tráfico malintencionado de entrada, las empresas pueden configurar un perímetro de seguridad eficaz o un cortafuego entre el tráfico externo y la red interna. Los responsables de TI pueden estructurar más la infraestructura de red para reforzar la seguridad del centro de datos con una partición en segmentos aislados entre sí. Si se tiene una infraestructura de red segmentada, una vulneración de seguridad no tiene por qué poner el peligro a toda la red. (VMware, 2022)

### 2.10.6. Vulnerabilidades y ataques habituales

Los ciberdelincuentes utilizan una serie de herramientas para acceder a los centros de datos. Los ataques de ingeniería social se lanzan contra los usuarios para engañarles y que revelen las contraseñas o abran otras vías que permitan el acceso de usuarios no autorizados. Sin sospecharlo, los usuarios pueden descargar programas maliciosos tales como programas de secuestro, que impiden que los usuarios legítimos inicien la sesión y secuestran el ordenador hasta que se pague a los atacantes. Las contraseñas poco seguras son otra forma en que los ciberdelincuentes se aprovechan de los usuarios más descuidados con la seguridad para acceder al centro de datos. Para proteger los centros de datos, los responsables de TI deben educar a sus usuarios sobre los diferentes tipos de ataques y aplicar buenas prácticas de seguridad para usuarios.

Los usuarios no son la única vulnerabilidad de una red. Una red o una herramienta de software mal configurada también puede permitir que los ciberdelincuentes accedan a un centro de datos. Los ciberdelincuentes pueden cerrar un servidor o un programa de software mal configurado, ya sea desbordándolo con solicitudes u ofreciéndole una secuencia de código para la que no está programado. Los centros de datos también son vulnerables a los ataques de suplantación, en los que se enmascara la verdadera fuente o naturaleza de un programa malicioso. En la suplantación de la IP, un mensaje parece venir de un host de confianza para que se considere seguro y así entrar a la red interna. Los cortafuegos son una forma de proteger contra los ataques de suplantación de la IP. (VMware, 2022)

## 2.11. CABLEADO ESTRUCTURADO

Cuando hablamos del cableado estructurado nos referimos a un sistema de conectores, cables, dispositivos y canalizaciones que forman la infraestructura que implanta una red de área local en un edificio o recinto. Su función es transportar señales desde distintos emisores hasta los receptores correspondientes.

Una red LAN (red de área local) se compone de una serie de elementos que hacen posible su funcionamiento. Esto se logra, precisamente, gracias a una serie de cables, conectores, equipos y canalizaciones llamados cableado estructurado.

Su estructura contiene una combinación de cables de par trenzado protegidos o no protegidos (STP y UTP por sus siglas en inglés, respectivamente), y en algunas ocasiones, de fibras ópticas y cables coaxiales. Sus elementos principales son el cableado horizontal, el cableado vertical y el cuarto de telecomunicaciones. (next_u, 2022)

### 2.11.1. Subsistema de Cableado Horizontal

Es el encargado de llevar la información desde el distribuidor de piso hasta los usuarios. La norma EIA/TIA 568A lo define como "la porción del sistema de cableado de telecomunicaciones que se extiende del área de trabajo al cuarto de telecomunicaciones". El cableado horizontal posee un núcleo sólido, normalmente, hecho de cobre. Se deberá evitar que se tuerza y, además, deberá estar ubicado detrás de muros para no tener contacto con él.

**El cableado horizontal incluye:**

- Cables horizontales.
- Tomas/conectores de telecomunicaciones en el área de trabajo.
- Terminación mecánica.
- Interconexiones horizontales localizadas en el cuarto de telecomunicaciones.

**Se reconocen cinco tipos de cable para el sistema de cableado horizontal:**

- Cables de par trenzado sin blindar (UTP) de 100 ohmios y cuatro pares.
- Cables de par trenzado apantallado (FTP) de 120 ohmios y cuatro pares.
- Cables de par trenzado blindado (STP) de 150 ohmios y cuatro pares.

- Cables de fibra óptica *multimodo* de 62.5/125 μm y 50/125 μm.
- Cables de fibra óptica *monomodo* de 9/125 μm.

**Medios de transmisión conocidos:**

Asimismo, la parte del cableado estructurado de forma horizontal UTP/STP está dividido en varias categorías que van desde la 1 a la 6 de acuerdo con su propósito. Por ejemplo:

- **Categoría 1:** cableado para comunicaciones telefónicas hasta 512 kbit por segundo.
- **Categoría 2**: transmisión de datos hasta los 4 Megabits por segundo.
- **Categoría 3:** para redes 10BaseT y velocidades de transferencia de datos hasta los 10 Megabits por segundo.
- **Categoría 4**: utilizado en redes Token Ring y velocidad de transferencia hasta 16 Megabits por segundo.
- **Categoría 5**: cableado estructurado que soporta velocidades hasta los 100 Megabits por segundo.
- **Categoría 6 y 6A**: velocidades que van desde el 1 Gigabit por segundo hasta los 10 Gigabits por segundo, respectivamente.

  Al margen de las diferencias respecto al **ancho de banda** y el **rendimiento** especificado por los estándares, o el hecho de que Cat6 sea mayoritariamente **UTP** mientras que Cat6A tiende a ser apantallado, realmente la gran distancia entre Cat6 y Cat6A la marca el soporte de aplicaciones, ya que la máxima **velocidad de transmisión** que se puede alcanzar sobre un cableado Cat6 es de 1Gbps (1000Base-T), mientras que con un cableado Cat6A podemos instalar electrónica 10GBase-T a 10Gbps.

Ahora bien, existen categorías 7, 7A y 8 que llegan a velocidades de 40 Gigabits por segundo. Sin embargo, son habitualmente utilizadas en organizaciones de investigación científica o en instituciones gubernamentales con una alta demanda. (next_u, 2022).

### 2.11.2. Subsistema de Cableado Vertical

El cableado vertical, también conocido como *backbone* o cableado troncal, es el encargado de crear interconexiones entre los cuartos de equipo, cuartos de entrada de servicios y cuartos de telecomunicaciones.

Está conformado por cables verticales, conexiones cruzadas principales e intermedias, terminaciones mecánicas y cordones de parcheo para conexiones cruzadas.

**Se reconocen cinco tipos de cable de fibra óptica para el sistema de cableado vertical (backbone):**

| | | Minimum modal bandwidth MHz-km | | |
|---|---|---|---|---|
| Wavelength | | Overfilled launch bandwidth | | Effect laser launch bandwidth |
| Fiber Type | Core diameter | 850 nm | 1300 nm | 850 nm |
| OM1 | 62.5 µm | 200 | 500 | Not specified |
| OM2 | 50 µm | 500 | 500 | Not specified |
| OM3 | 50 µm | 1500 | 500 | 2,000 |
| OM4 | 50 µm | 3500 | 500 | 4,700 |
| OM5 | 50 µm | 3500 | 500 | 4,700 |

**Cuarto de Telecomunicaciones.**

Consiste en el área física destinada exclusivamente para el alojamiento de los elementos que conforman el sistema de telecomunicaciones. En este cuarto se encuentran conmutadores y todos los elementos centralizados que corren a través de tramos horizontales hasta el área de trabajo.

Entre las características más representativas del cuarto de telecomunicaciones se destacan:

- La altura mínima recomendada es de 2.6 metros.
- Si posee equipos activos, su temperatura ambiente debe encontrarse entre 18 y 24 °C y la humedad entre 30 % y 50 %. De lo contrario, la temperatura debe estar entre 10 y 35 °C y la humedad inferior a 85 %.
- Debe contener un mínimo de dos tomas corrientes AC de 110 V y 15 A con circuitos independientes.
- Debe encontrarse en un lugar sin riesgo de inundación ni en contacto con agua. En caso de haber riesgo de ingreso de agua, se debe proporcionar drenaje de piso.
- No puede compartir espacio con instalaciones eléctricas que no estén relacionadas con las telecomunicaciones. (next_u, 2022)

### 2.11.3. Normas y Estándares de Cableado Estructurado

- Estándar ANSI/TIA/EIA-568-A: Estándar de Alambrado de Telecomunicaciones para Edificios Comerciales, que soportará un ambiente multiproducto y multifabricante.
- Estándar ANSI/TIA/EIA-569: Estándar para Ductos y Espacios de Telecomunicaciones en Edificios Comerciales
- Estándar de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales. ANSI/TIA/EIA-570: Estándar de Alambrado de Telecomunicaciones Residencial y Comercial Liviano.
- Estándar ANSI/TIA/EIA-606: Estándar de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.
- Estándar ANSI/TIA/EIA-607: Estándar para Requerimientos para Telecomunicaciones de Puesta a Tierra y Puenteado de Edificios Comerciales.
- Norma ISO 11801: Norma de Cableado para facilidades en los clientes finales. Norma que define una instalación completa (Componentes, conexiones).
- Norma IEEE 802.1: Norma para todos los aspectos de Administración de Redes LAN.
- Norma 802.2, 802.3, 802.5: Norma para Protocolos LAN.
- Manual de Método de Distribución de Telecomunicaciones de Building Industry Consulting Service International (BICSI).
- ISO/IEC 11801 Generic Cabling for customer Premises. National Electrical Code 1996(NEC). (qualtytech, 2022)

## 2.12. REDES DE DATOS

Prácticamente todos estamos interconectados gracias a las redes e internet. Lo que antes era una práctica restringida a grandes empresas para comunicarse punto a punto, hoy es necesario para que todos nosotros estemos al alcance de información prácticamente desde cualquier punto del planeta.

### 2.12.1. Redes por su Extensión

Por el alcance y la cobertura del área al cual dan servicio, identificamos los tipos:

**LAN (Local Área Netwok)**

Una red LAN o Local Área Network, es una red de comunicaciones construida mediante la interconexión de nodos mediante cables o medios inalámbricos que operan a través de un software de acceso al medio. El ámbito de conexión está limitado por medios físicos, ya sea un edificio, planta o habitación.

En cada red LAN existen una serie de elementos compartidos y disponibles para los usuarios que estén conectados dentro de esta red interna. Solamente ellos podrán disponer de estos recursos sin intervención o acceso externo.

En teoría las redes LAN deben de proporcionar una velocidad de transmisión alta, de entre 10 Mb/s hasta los 10 Gb/s. Además, la tasa de errores debe ser lo más reducida posible, del orden de 1 bit erróneo por cada 100 millones de bit enviados.

Otra característica que debe tener una red LAN es la de proporcionar la posibilidad de poder ser gestionada por el usuario a la que pertenece. Toda red LAN debe componerse de los siguientes elementos:

- **Modo de transmisión/modulación**: puede ser mediante banda base o banda ancha.
- **Protocolo de Acceso al medio**: CSMA/CD, FDDI, Token Passing, TCP, TDMA.
- **Soporte físico**: cables UTP, Fibra óptica o cable coaxial.
- **Topología**: bus, anillo, estrella y malla (Castillo, 2018)

**Figura 15.** Red LAN. (Castillo, 2018)

**WAN (Wide Area Network)**

Una red WAN se define como una red con una cobertura sin un límite predefinido como es el caso de la red MAN. Es por esto que, tanto las topologías, como infraestructuras, no pueden ser estrictamente definidas, ya que estas redes se apoyan en los medios que proporcionan los operadores de telecomunicaciones en los diferentes países. Cuando es necesario interconectar varios países será necesario establecer una comunicación directa entre distintos medios, lo que hace de esta red una extensión a nivel mundial.

Como es normal, en este tipo de redes las tecnologías que se utilizan pueden ser prácticamente cualquiera de las existentes en el ámbito de cada país. Aunque para conseguir el mejor rendimiento posible, se utiliza el método de conmutación de paquetes, ya que de esta forma el enrutamiento de la información se puede adaptar por cualquier tipo de estándar por el que pase.

Internet es una Red WAN que proporciona cobertura a nivel mundial utilizando el protocolo IP**.** Otro claro ejemplo de red WAN es la RDSI**,** la cual se utiliza para comunicación por voz y datos. (Castillo, 2018)

**Figura 16.** Red WAN (Castillo, 2018)

**MAN (Metropolitan Area Network)**

El término MAN proviene de "Metropolitan Area Network" o en español, red de área metropolitana. Este tipo de red es el paso intermedio entre una red LAN y una red WAN, ya que la extensión de este tipo de redes comprende el territorio de una gran ciudad. Las redes MAN son redes de alta velocidad capaces de dar cobertura a una geografía relativamente extensa, aunque nunca superando las dimensiones de una ciudad.

Las topologías que se emplean en este tipo de redes son generalmente malladas con algunos elementos configurados en forma de redes troncales, que normalmente derivan en subredes más pequeñas. En ella se emplean fundamentalmente conexiones mediante cables de par trenzado y cada vez más mediante fibra óptica.

Una red MAN puede llegar a tener velocidades de hasta 10 Gb/s (Gigabit por segundo) con el uso de fibra óptica. (Castillo, 2018)

**Figura 17.** Red MAN. (Castillo, 2018)

### 2.12.2. Topología de Redes LAN, MAN y WAN

Hablando de redes estamos en la obligación de hablar sobre topologías de red. Las topologías de red es la forma en la que interconectan los nodos para efectuar el intercambio de datos. Cada una de las topologías está orientada a un propósito y ofrecerá determinas ventajas y

desventajas según su utilización. En donde mejor podemos ver este tipo de topologías es en una red LAN, debido a su menor extensión. En las redes MAN y WAN este aspecto es difícil de ver y sobre todo de definir, ya que, debido a la extensión de las mismas, existen una gran cantidad de topologías interconectadas entre sí para forma el concepto de red global.

Normalmente una red MAN o WAN suele funcionar en una topología de red con estructura mallada. De esta forma los nodos estarán interconectados unos a otros proporcionando redundancia en el enrutamiento de paquetes. Así conseguiremos que existan muchos caminos alternativos para que, si una ruta de transmisión falla, sea posible hacerlo por otro lado. Podemos decir que esta es la red de Internet. (Castillo, 2018)

### Topología en BUS

La primera configuración disponible es la topología en bus. Esta se caracteriza por componerse de un cable central o tronco del que cuelgan los diferentes nodos a los que deben llegar los datos. En caso de fallo del tronco, la parte de la red conectada después quedará inutilizable. Para este tronco normalmente se utiliza **cable coaxial o fibra óptica**, y es posible conectar a su vez otras ramificaciones a este para así formar una red en forma de árbol. (Castillo, 2018)

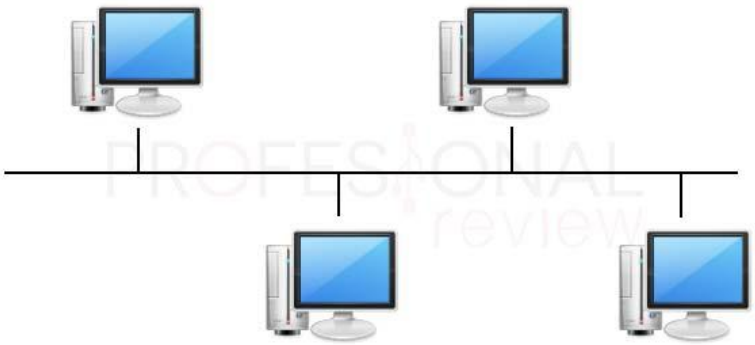


**Figura 18.** Topología en Bus. (Castillo, 2018)

### Topología en Anillo

Básicamente es una red en forma de bus que se cierra en ella misma. En este caso, si una parte del tronco se rompe, podremos acceder al resto de nodos mediante el otro semianillo. Este

tipo de redes pueden utilizar prácticamente cualquier tipo de cable de red y se utilizando para redes Token Ring. (Castillo, 2018)

**Figura 19.** Topología en Anillo. (Castillo, 2018)

**Topología en Estrella**

Actualmente es la más comúnmente utilizada. Esta topología consta de un elemento central que puede ser un hub o switch que sirve de puente para los demás terminales o nodos conectados a él. Con esta estructura se puede aislar cada elemento del fallo de otros, aunque si falla el elemento central la red entera caerá (Castillo, 2018)

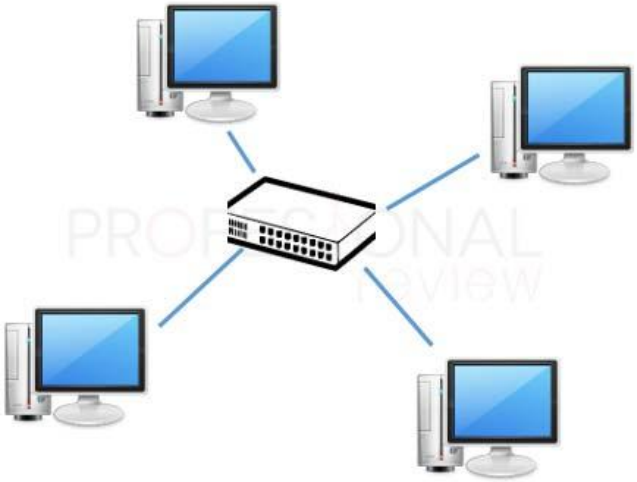


**Figura 20.** Topología en Estrella. (Castillo, 2018)

**Topología en Malla**

Esta es la topología de mayor seguridad, pero considerablemente más completa y costosa que el resto. Se trata de unir todos los elementos de la red entre sí formando una estructura en la en todo momento existen más de dos caminos para acceder a cada nodo. Esta red es utilizada por redes MAN y WAN para que nunca caiga un gran sector de la red en caso de fallo de algún elemento. (Castillo, 2018)

**Figura 21.** Topología en Malla. (Castillo, 2018)

### 2.12.3. Tecnologías utilizadas en una red LAN, MAN y WAN

#### Bonding EFM

Adoptada y certificada en 2004, es una tecnología que permite servicios Ethernet en distancias de aproximadamente 5 km y a latencias muy bajas, de entra 1 y 5 milisegundos. Utiliza conmutación de paquetes mediante pares trenzados. Se puede utilizar para el transporte de vídeo, voz y datos. (Castillo, 2018)

#### SMDS

SMDS o Switched Multi-megabit Data Service, es el servicio implementado en Estados Unidos. Es capaz de proporcionar servicios no orientados a conexión, es decir, sin la necesidad de establecer una sesión y un circuito cerrado para la transmisión.

Los documentos que la definen son TA 772, 773, 774 y 775. Estos proporcionan los requisitos genéricos, a nivel físico, de operación, administración, red y tarificación para los

elementos interconectados. Con SMDS se dispone redes de área local interconectadas entre sí mediante una red general de extensión nacional en forma troncal.

En cuanto al formato de datos, y el acceso desde el punto de vista del abonado, es idéntica al estándar 802 definido por IEEE para redes MAN, y la interfaz de red se denomina SIN o Suscriber Network Interface. (Castillo, 2018)

**FDDI**

Son las siglas de Fiber Distributed Data Interface o interfaz de datos distribuida por fibra. Esta tecnología es la de mayor aplicación en la era de los 100 Mb/s y también utilizada en Europa y son un conjunto de estándares ISO y ANSI para la trasmisión de datos en redes de área extendida como las MAN mediante cables de fibra óptica.

Actualmente opera bajo el estándar IEEE 802.8 del organismo europeo y ANSI X3T9.5 del americano. Esta red está constituida por una topología en Token Ring o de doble anillo de fibra óptica para asegurar la transmisión de datos en las dos direcciones. También cuenta con una implementación mediante hilo de cobre llamado CDDI.

Las tecnologías de Fast Ethernet a 100 Mb/s o también denominadas 100BASE-FX y 100 BASE-TX están basadas en FDDI. Teóricamente tienen capacidad para conectar hasta 500 nodos (1000 accesos MAC en configuración de doble anillo) con una separación de hasta 2 KM entre nodos. Esta hace que la extensión total de un anillo pueda ser de hasta 100 KM o 200 si tenemos en cuenta que es de doble sentido.

El protocolo de acceso al medio se mejoró con respecto al estándar 802.5 para dotar de capacidad de utilizar testigos múltiples. De esta forma se mejora el enrutamiento de información dotando a los nodos con la capacidad de trabajar simultáneamente con varios testigos. (Castillo, 2018)

## 2.13. TECNOLOGÍA ETHERNET

Ethernet es una tecnología para redes de datos por cable que vincula software y/o hardware entre sí. Esto se realiza a través de cables de redes LAN, de ahí que Ethernet sea concebido habitualmente como una tecnología LAN. Así, Ethernet permite el intercambio de datos entre terminales como, por ejemplo, ordenadores, impresoras, servidores, distribuidores, etc. Conectados en una red local, estos dispositivos establecen conexiones mediante el protocolo Ethernet y pueden intercambiar paquetes de datos entre sí. El protocolo actual y más extendido para ello es IEEE 802.3.

Ethernet fue desarrollado a principios de los 1970, época en la que solo se utilizaba como sistema interno de red en la empresa Xerox, y no fue hasta principios de los ochenta que Ethernet se convirtió en un producto estandarizado. Con todo, aún habría que esperar hasta mediados de la década para que empezara a utilizarse más ampliamente. Fue cuando los fabricantes comenzaron a trabajar con Ethernet y con productos relacionados. Así, dicha tecnología contribuyó de manera significativa a que los ordenadores personales revolucionaran el mundo laboral. El estándar IEEE 802.3 tan popular actualmente se utiliza, por ejemplo, en oficinas, viviendas particulares, contenedores y portadores (carrier).

Mientras que la primera versión de esta tecnología solo tenía una velocidad de 3 Mbit/s, los protocolos Ethernet actuales permiten alcanzar velocidades de hasta 1 000 megabits por segundo. Por otro lado, los estándares Ethernet antiguos se restringían a un solo edificio, mientras que hoy en día pueden alcanzar hasta los 10 km gracias a la utilización de la fibra de vidrio. En el transcurso de su desarrollo, Ethernet ha tenido el rol dominante entre las tecnologías LAN y ha destacado entre sus numerosos competidores. La conocida como Ethernet en tiempo real es en la actualidad un estándar industrial para aplicaciones de comunicación. (Ionos, 2022)

### 2.13.1. Funcionamiento Ethernet

En una red Ethernet a cada dispositivo se le asigna una dirección propia denominada dirección MAC (48 bits). Los miembros de esta red conjunta pueden transmitir mensajes con alta frecuencia, para lo que el estándar emplea el método de banda base y el de multiplexación. Por otro lado, para la comunicación mutua se utiliza el algoritmo **CSMA/CD**

(Carrier Sense Multiple Access/Collision Detection; en español, acceso múltiple con escucha de portadora y detección de colisiones). La topología de red de Ethernet es lógica, es decir, puede estructurarse como bus o como estrella.

Ethernet permite conectar diversos dispositivos entre sí. Para ello, a cada uno de los terminales se le asigna una dirección MAC

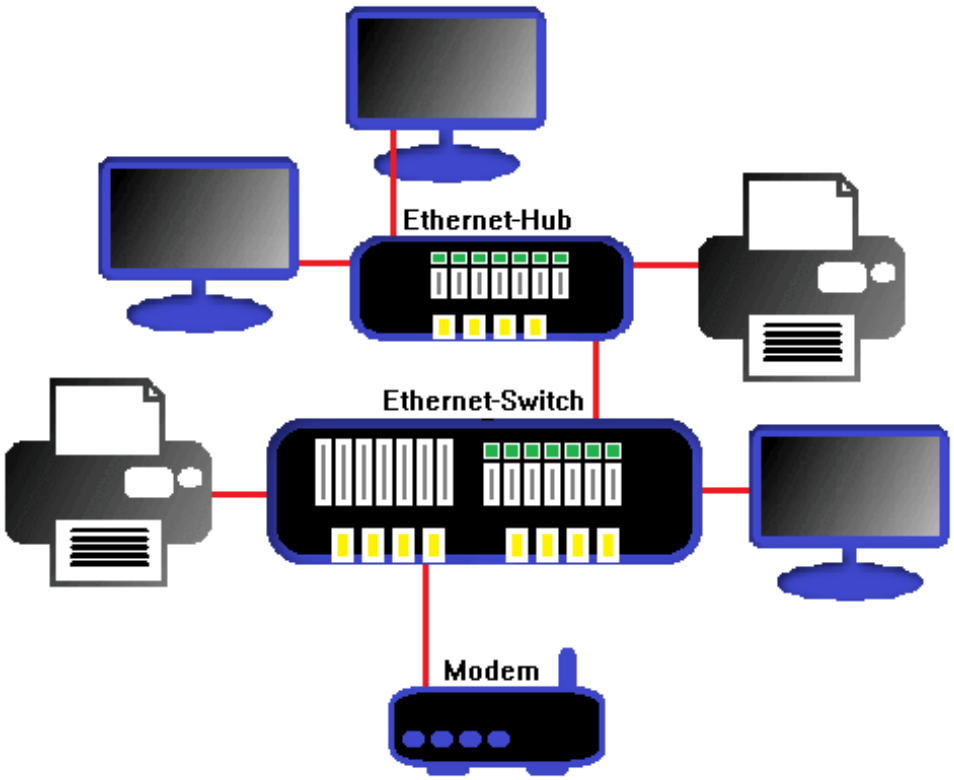



**Figura 22.** Conexión de dispositivos mediante Ethernet. (Ionos, 2022)

La comunicación con este algoritmo es similar a una mesa redonda en la que cada participante deja que el otro se exprese. Si dos mensajes colisionan, los participantes intentarán realizar una nueva transmisión en intervalos aleatorios. Debido a que una comunicación eficaz requiere tanto que se envíe como que se reciba, no debe darse lugar a que haya una obstrucción de datos, por ejemplo, en caso de que un mensaje transmitido resulte muy grande para una potencia de recepción débil, pues de ser así, puede perderse información. La velocidad

de la señal y la tasa de transmisión regulan la comunicación fluida definiendo reglas para los marcos de datos.

Para evitar una colisión de datos, la correspondiente **señal de interferencia** debe llegar al receptor antes que el paquete de datos. Dado que hoy en día la mayoría de redes funcionan en modo dúplex completo, este problema es algo inusual. Sin embargo, sí fue fundamental para el desarrollo temprano de la tecnología Ethernet.

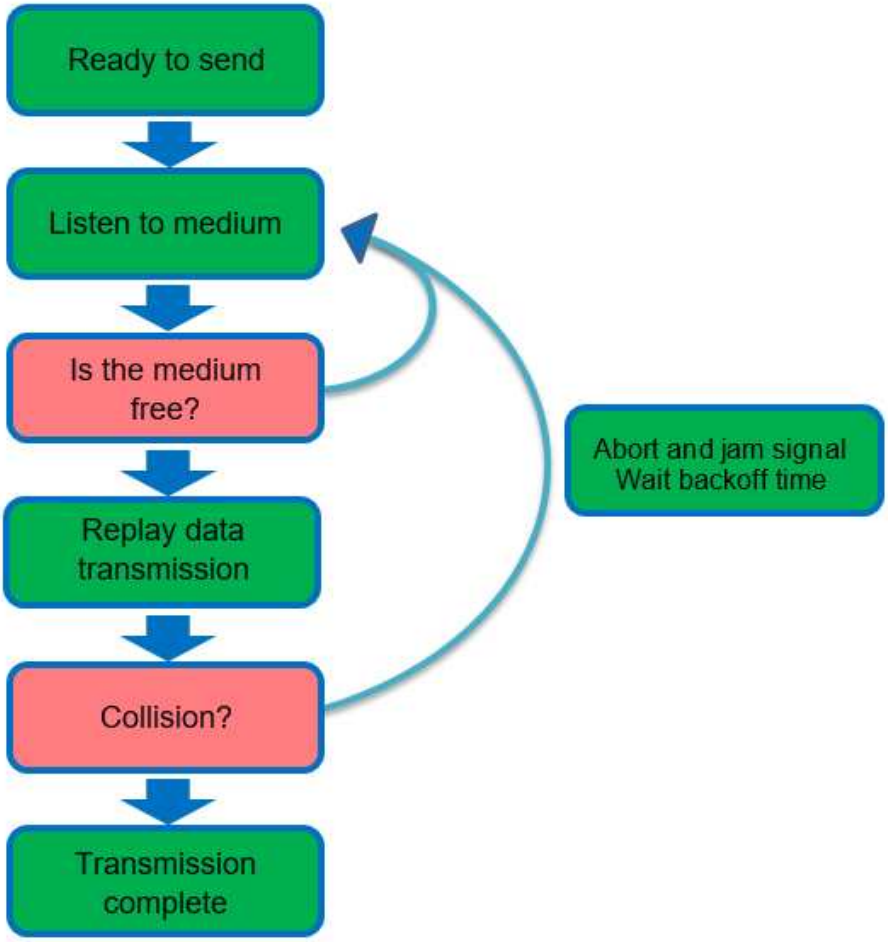



**Figura 23.** Algoritmo de funcionamiento Ethernet. (Ionos, 2022)

Con el algoritmo de Ethernet, la red regula el intercambio sin colisiones de los paquetes de datos Originariamente, cualquier mensaje enviado en una red se distribuía a todos los terminales. Tras ello, estos tenían que filtrar los datos recibidos y decidir si eran relevantes o no. Como consecuencia, este bus común no solo daba cabida a mensajes de difusión, sino que

también protocolizaba todo el tráfico de datos para cada uno de los miembros, lo que constituía una brecha de seguridad del antiguo Ethernet. Así, los datos podían cifrarse, pero el tráfico de datos, sin embargo, no podía controlarse individualmente. Por su parte, los hubs no pueden cerrar estas brechas de seguridad, algo que sí puede remediarse en las redes modernas con puentes de red (bridges) y conmutadores (switches), con cuya ayuda es posible segmentar Ethernet.

No obstante, estas técnicas no solucionan todos los problemas, sino que el uso indebido, por ejemplo, mediante MAC Flooding y MAC Spoofing, es un riesgo para la estabilidad de la red y la seguridad de los paquetes de datos comunicados. El trabajo seguro en una red Ethernet requiere, por lo tanto, el uso serio de todos los sistemas conectados y de los análisis de datos habituales (por ejemplo, análisis LAN) para revelar posibles usos indebidos y averías.

Mientras que el conjunto de datos no sobrecargue la red, Ethernet funcionará bien. En los casos en los que se supere el 50 %, puede que haya un bloqueo de los datos. En el transcurso del desarrollo técnico de los ordenadores personales y con el crecimiento constante del volumen de datos, las redes Ethernet también tuvieron que evolucionar para seguir el ritmo del progreso tecnológico. Los conmutadores se ocupan de una distribución más eficiente de los paquetes de datos y reducen el riesgo de colisiones. Por su parte, las tecnologías por cable modernas como el cable de par trenzado (twisted pair) y la fibra de vidrio tienen tasas de transmisión más elevadas que se corresponden con las necesidades actuales de la red.

Otra de las innovaciones recibe el nombre de “Ethernet Flow Control”, mecanismo con el que se puede detener totalmente y de forma temporal la transmisión de datos para agilizar el flujo de datos en otras partes. Esto resulta especialmente práctico en el modo de dúplex completo cuando una red maneja muchos dispositivos terminales. Tras ello, el mecanismo Flow Control detiene a determinados miembros de la red para optimizar la eficacia de la misma. No obstante, pueden producirse pérdidas de velocidad que pueden atajarse con otros mecanismos como el protocolo de control de transmisión (Transmission Control Protocol, TCP).

En el pasado, Ethernet solía utilizar cables coaxiales tradicionales. En la actualidad, los cables de cobre de par trenzado y los cables de fibra óptica son el estándar industrial y permiten tasas de transmisión mucho más rápidas y un mayor alcance. Otra ventaja es que los cables de cobre pueden abastecer de electricidad a los dispositivos conectados. Este procedimiento, también llamado "Power over Ethernet" (PoE), permite crear redes con una mayor eficiencia energética y viene especificado en IEEE 802.3af. (Ionos, 2022)

### 2.13.2. Tecnologías y Conceptos de Ethernet

| TECNOLOGÍA/TÉRMINO | EXPLICACIÓN |
|---|---|
| **LAN (Local Area Network)** | Red informática que vincula a varios sistemas entre sí a nivel local |
| **Switching (conmutación)** | La conmutación regula la ruta de un paquete de datos en la red; la entrada y salida de paquetes se define según el emisor y el receptor |
| **Ethernet Flow Control** | La transmisión de datos en Ethernet se detiene temporalmente; el objetivo es lograr una menor pérdida de datos y una mayor eficiencia |
| **CSMA/CD (Carrier Sense Multiple Access/Collision Detection)** | Proceso de acceso a los medios que determina qué sistemas en una red pueden acceder a un medio de transmisión; evita colisiones |
| **Marco de Ethernet/marco de datos** | Unidad de protocolo que contiene información importante para la transmisión de datos como, por ejemplo, la dirección MAC |
| **Dirección MAC/dirección del dispositivo** | Dirección única asignada a un dispositivo en la red informática |
| **PoE (Power over Ethernet)** | El cable de Ethernet puede proveer de alimentación eléctrica al dispositivo de destino |
| **Cable coaxial** | Cable bipolar de hasta 10 Mbit/s (tecnología anticuada) |
| **Cable de par trenzado** | Cable con pares de núcleos trenzados, permite PoE hasta 10 Gbit/s |

| | |
|---|---|
| **Cable de fibra óptica** | Fibra óptica, alcance elevado, posibilidad de lograr enormes tasas de transmisión (en teoría hasta aprox. 70 terabit/s) |
| **Modo de semidúplex** | La comunicación solo es posible alternativamente en una única dirección (tecnología anticuada) |
| **Modo de dúplex completo** | La comunicación es posible simultáneamente en ambas direcciones |

**Tabla 1.** Tabla de tecnologías y conceptos Ethernet. (Ionos, 2022)

### 2.13.3. Estándares de Ethernet

| Estándar de Ethernet | Denominación | Velocidad de datos | Tecnología de cables | Año de publicación |
|---|---|---|---|---|
| **802.3** | 10Base5 | 10 MB/s | Cable coaxial | 1983 |
| **802.3a** | 10Base2 | 10 MB/s | Cable coaxial | 1988 |
| **802.3i** | 10Base-T | 10 MB/s | Cable de par trenzado | 1990 |
| **802.3j** | 10Base-FL | 10 MB/s | Cable de fibra óptica | 1992 |
| **802.3u** | 100Base-TX100Base-FX100Base-SX | 100 MB/s | Cable de par trenzado, cable de fibra óptica | 1995 |
| **802.3z** | 1000Base-SX1000Base-LX | 1 GB/s | Cable de fibra óptica | 1998 |
| **802.3ab** | 1000Base-T | 1 GB/s | Cable de par trenzado | 1999 |
| **802.3ae** | 10GBase-SR, 10GBase-SW, 10GBase-LR, 10GBase-LW, 10GBase-ER, 10GBase-EW, 10GBase-LX4 | 10 GB/s | Cable de fibra óptica | 2002 |
| **802.an** | 10GBase-T | 10 GB/s | Cable de par trenzado | 2006 |

**Tabla 2.** Tabla de estándares de Ethernet. (Ionos, 2022)

### 2.13.4. Fast Ethernet

Este estándar es directamente derivado del anterior, de hecho, algunas tecnologías son directamente heredadas de FDDI. Este estándar está controlado por **IEEE 802.3**, y es capaz de trabajar a 100Mb/s.

El estándar surgió ante la necesidad de mejorar la velocidad de las trasmisiones entre equipo, debido a la mejora en la tecnología del hardware y la capacidad para transmitir datos multimedia de mayor calidad y tamaño. Gracias a este estándar, en los siguientes años surgieron otras evoluciones del mismo que multiplicaban por diez al anterior. Hasta situarnos hoy día en los 10Gb/s

Los estándares de soporte para esta tecnología son, para cobre 100BASE-TX, 100BASE-T4 y 100BASE-T2. Y para fibra óptica 100BASE-FX, 100BASE-SX y 100BASE-BX.

**Figura 24.** Fast Ethernet. (Castillo, 2018)

### 2.13.5. Gigabit Ethernet

Es la evolución de estándar Ethernet para dotar de mayor velocidad de transmisión a las redes. En este caso la velocidad aumenta a 1000Mb/s. Opera bajo el estándar de IEEE 802.3ab y 802.3z.

Gracias a la implementación de cables UTP de mayores prestaciones y utilizada también fibra óptica, se consiguió aumentar la velocidad hasta los 1000Mb/s. Los estándares que operan para este modo son 1000BASE-SX, 1000BASE-LX, 1000BASE-EX, 1000BASE-ZX, 1000BASE-CX

**Figura 25.** Gigabit Ethernet. (Castillo, 2018)

### 2.13.6. 10Gigabit Ethernet

Finalmente, este es el estándar utilizado actualmente para las transmisiones de datos en redes LAN, MAN y WAN. Esta bajo el estándar de IEEE 802.3ae y es capaz de alcanzar las velocidades de 10Gb/s.

El medio de transmisión utilizado es, por supuesto, fibra óptica y cables UTP de pares trenzados de categoría 6 en adelante. Los estándares que operan en este modo Ethernet son 10GBASE-CX4, 10GBASE-LX4, 10GBASE-LR, 10GBASE-ER, 10GBASE-LRM, 10GBASE-T, entre otras.


**Figura 26.** 10 Gigabit Ethernet. (Castillo, 2018)

## 2.14. MEDIOS DE TRANSMISIÓN

El medio de transmisión constituye el canal que permite la transmisión de información entre dos terminales en un sistema de transmisión. Las transmisiones se realizan habitualmente empleando ondas electromagnéticas que se propagan a través del canal. A veces el canal es un medio físico y otras veces no, ya que las ondas electromagnéticas son susceptibles de ser transmitidas por el vacío.

### 2.14.1. Medios Guiados

Los medios de transmisión guiados están constituidos por un cable que se encarga de la conducción (o guiado) de las señales desde un extremo al otro. Las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, las distancias máximas que puede ofrecer entre repetidores, la inmunidad frente a interferencias electromagnéticas, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel de enlace. La velocidad de transmisión depende directamente de la distancia entre los terminales, y de si el medio se utiliza para realizar un enlace punto a punto o un enlace multipunto. Debido a esto los diferentes medios de transmisión tendrán diferentes velocidades de conexión que se adaptarán a utilizaciones dispares. (Sanchez, 2011)

#### Par Trenzado

El par trenzado: Consiste en un par de hilos de cobre conductores cruzados entre sí, con el objetivo de reducir el ruido de diafonía. A mayor número de cruces por unidad de longitud, mejor comportamiento ante el problema de diafonía.

Existen tres tipos de par trenzado:

- Protegido: Shielded Twisted Pair (STP)
- No protegido: Unshielded Twisted Pair (UTP)
- Maya externa, como papel de plata: (FTP)

El UTP son las siglas de Unshielded Twisted Pair. Es un cable de pares trenzado y sin recubrimiento metálico externo, de modo que es sensible a las interferencias. Es importante

guardar la numeración de los pares, ya que de lo contrario el Efecto del trenzado no será eficaz disminuyendo sensiblemente o incluso impidiendo la capacidad de transmisión. (Sanchez, 2011)

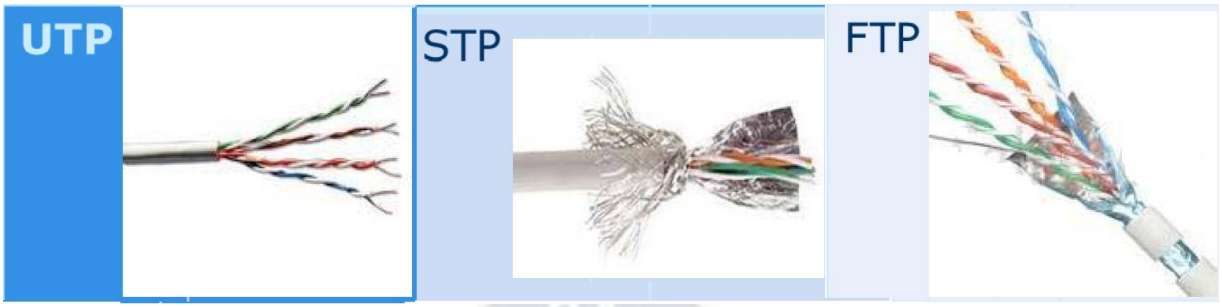



**Figura 27.** Par Trenzado. (Sanchez, 2011)

Es un cable Barato, flexible y sencillo de instalar. Las aplicaciones principales en las que se hace uso de cables de par trenzado son:

- Bucle de abonado: Es el último tramo de cable existente entre el teléfono de un abonado y la central a la que se encuentra conectado. Este cable suele ser UTP Cat.3 y en la actualidad es uno de los medios más utilizados para transporte de banda ancha, debido a que es una infraestructura que está implantada en el 100% de las ciudades.
- Redes LAN: En este caso se emplea UTP Cat.5 o Cat.6 para transmisión de datos. Consiguiendo velocidades de varios centenares de Mbps. Un ejemplo de este uso lo constituyen las redes 10/100/1000BASE- T. (Sanchez, 2011)

**Cable Coaxial**

Consiste en un cable conductor interno (cilíndrico) separado de otro cable conductor externo por anillos aislantes o por un aislante macizo. Todo esto se recubre por otra capa aislante que es la funda del cable.

Este cable, aunque es más caro que el par trenzado, se puede utilizar a más larga distancia, con velocidades de transmisión superiores, menos interferencias y permite conectar más estaciones. Se suele utilizar para televisión, telefonía a larga distancia, redes de área local, conexión de periféricos a corta distancia, etc. Se utiliza para transmitir señales analógicas o

digitales. Sus inconvenientes principales son: atenuación, ruido térmico, ruido de intermodulación.

Para señales analógicas, se necesita un amplificador cada cierto kilómetro y para señales digitales un repetidor cada kilómetro. Este cable lo compone la malla y el vivo. Este tipo de cable ofrece una impedancia de 50 por metro. El tipo de conector es el RG58. (Sanchez, 2011)

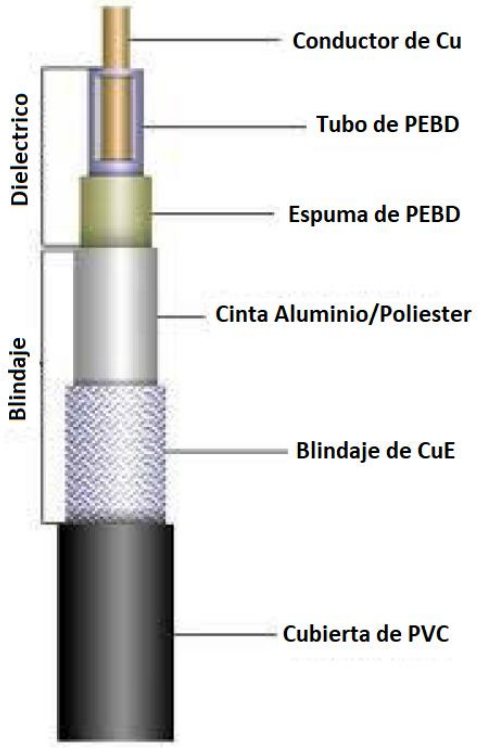



**Figura 28.** Cable Coaxial. (Sanchez, 2011)

Existen básicamente dos tipos de cable coaxial:

**Banda Base:** Es el normalmente empleado en redes de computadoras, con resistencia de 50 (Ohm), por el que fluyen señales digitales.

**Banda Ancha:** Normalmente mueve señales analógicas, posibilitando la transmisión de gran cantidad de información por varias frecuencias, y su uso más común es la televisión por cable. Esto ha permitido que muchos usuarios de Internet tengan un nuevo tipo de acceso a la

red, para lo cual existe en el mercado una gran cantidad de dispositivos, incluyendo módem para CATV. (Sanchez, 2011)

**Fibra Óptica**

Es el medio de transmisión de datos inmune a las interferencias por excelencia, por seguridad debido a que por su interior dejan de moverse impulsos eléctricos, proclives a los ruidos del entorno que alteren la información. Al conducir luz por su interior, la fibra óptica no es propensa a ningún tipo de interferencia electromagnética o electrostática.

Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza óptica. Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta. El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo. Alrededor de este conglomerado está la cubierta (constituida de material plástico o similar) que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad, etc.

Es un medio muy apropiado para largas distancias e incluso últimamente para LAN. Sus beneficios frente a cables coaxiales y pares trenzados son:

- Permite mayor ancho de banda.
- Menor tamaño y peso.
- Menor atenuación.
- Aislamiento electromagnético.
- Mayor separación entre repetidores.

Generalmente esta luz es de tipo infrarrojo y no es visible al ojo humano. La modulación de esta luz permite transmitir información tal como lo hacen los medios eléctricos Su rango de frecuencias es todo el espectro visible y parte del infrarrojo.

El método de transmisión es: los rayos de luz inciden con una gama de ángulos diferentes posibles en el núcleo del cable, entonces sólo una gama de ángulos conseguirá reflejarse en la capa que recubre el núcleo.

Las fibras ópticas se clasifican de acuerdo al modo de propagación que dentro de ellas describen los rayos de luz emitidos. En esta clasificación existen tres tipos. Los tipos de dispersión de cada uno de los modos pueden ser apreciados. (Sanchez, 2011)

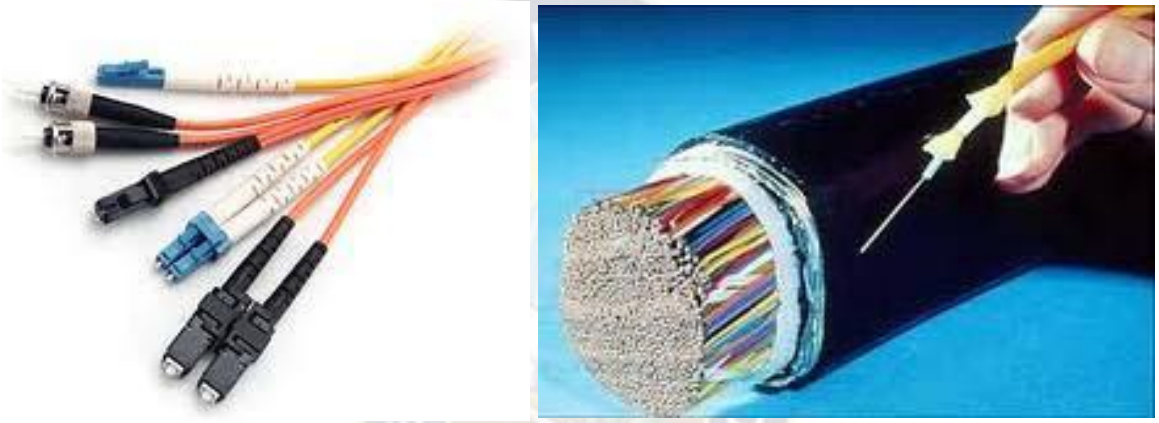


**Figura 29.** Fibra Óptica. (Sanchez, 2011)

**Fibra Óptica Monomodo.** Fibra monomodo significa que la fibra permite propagar un tipo de modo de luz a la vez. El cable fibra monomodo tiene normalmente un diámetro de núcleo estrecho de 8 a 10 µm (micrómetros), que puede propagarse a una longitud de onda de entre 1310 nm y 1550 nm. El tamaño pequeño del núcleo de fibra monomodo y el impulso de luz único eliminan virtualmente cualquier distorsión que pudiese resultar de la superposición de los impulsos de luz. Por lo tanto, el cable de fibra óptica monomodo proporciona una atenuación de la señal menor y velocidades de transmisión más altas que cualquier otro cable de fibra. Por estas razones, la fibra óptica monomodo es la mejor opción para la transmisión de datos a larga distancia. (Worton, 2021)

**Tipos Monomodo: OS1, OS2**

Hay dos tipos de fibra monomodo, denominados OS1 y OS2:

Tipo de cable monomodo OS1 es una fibra con protección interna ajustada, es decir, un cable multifibra de 900 micras, con una fibra ajustada con nylon, Hytrel o PVC. Un cable OS1 también podría ser un cable de interior Micro-core LSZH que consta de fibras de 250 micras, con las fibras firmemente encerradas en un cable con hilo de refuerzo de aramida y una cubierta LSZH. La atenuación de una fibra OS1 es ligeramente superior a la de una fibra OS2 (p. Ej., 0,30 dB / km a 1550 para OS1 frente a 0,119 dB / km a 1550 para OS2).

El tipo de fibra monomodo OS2 es un cable de fibra óptica de tubo suelto y es adecuado para aplicaciones al aire libre donde el proceso de cableado no aplica estrés a las fibras ópticas. Por ejemplo, una fibra múltiple revestida de 250 micras, que está suelta dentro de un recinto o tubo y / o se puede mover libremente, se clasifica como OS2. La distancia máxima de transmisión de la fibra monomodo OS1 es de 2 km, pero la distancia máxima de transmisión de la fibra monomodo OS2 puede alcanzar 5 m / s. km y es de hasta 10 km.

Las características de la fibra monomodo OS1, es que solo se propaga un modo de luz. El diámetro del revestimiento es de 125 µm, y el diámetro del núcleo es de unas 9 µm. longitud de onda 1310nm y una atenuación de 0.5 db/km Este hecho hace que su transmisión sea paralela al eje de la fibra y que permita alcanzar grandes distancias y transmitir elevadas tasas de información.

La fuente de luz utilizada para las_fibras ópticas monomodo es un láser (Light Amplification by Stimulated Emission of Radiation). Este láser es generado por un diodo láser semiconductor. La distancia máxima para un enlace de fibra óptica monomodo es de 20km. Sus principales ventajas (ancho de banda prácticamente ilimitado, bajo nivel de atenuación) utilización normalmente en aplicaciones WAN o Telecom (larga distancia):

- G.652 (C y D): Utilizadas como fibra estándar en Telecom y para transmisión Ethernet a Gigabit y 10 Gigabit. La denominación OS1 es cubierta por las fibras tipo de G652a, b c y d. La fibra tipo OS2 (desde 2006) fija características para las longitudes de onda 1310 nm 1550 nm y 1383 nm (fibras de bajo pico de agua, válidas para CWDM). Asimismo, la fibra OS2 es de aplicación como F.O. SM para aplicaciones de larga distancia. (Rico, 2018)

**Fibra Óptica Multimodo.** La fibra multimodo es un tipo de fibra óptica que se utiliza sobre todo en la comunicación en distancias cortas. El cable de fibra óptica multimodo tiene un núcleo más grande, normalmente de 50 o 62,5 micras, que permite la propagación de múltiples modos de luz. Esto permite que más datos transiten simultáneamente a través del núcleo de la fibra multimodo. La distancia máxima de transmisión del cable MMF es de unos 550 m a una velocidad de 10 Gb/s. De hecho, puede transmitir a distancias más largas, pero con velocidades de datos más bajas como, por ejemplo: 2 km a 100 Mb/s. (Worton, 2021)

**Tipos Multimodo: OM1, OM2, OM3, OM4, OM5**

En ANSI/TIA-568.3-D, TIA adoptó la nomenclatura de la fibra de la norma internacional ISO/IEC 11801. La fibra multimodo tiene el prefijo "OM" y la monomodo "OS".

La nueva designación en ANSI/TIA-568.3-D debería minimizar la confusión asociada con la asistencia que se brinda para los sitios remotos si hay errores con las aplicaciones. Cada "OM" tiene un requisito de ancho de banda modal (MBW) mínimo.

| | | Ancho de banda modal mínimo en MHz-km | | |
|---|---|---|---|---|
| Longitud de onda | | Ancho de banda de transmisión saturada | | Ancho de banda de transmisión de láser efectiva |
| Tipo de fibra | Diámetro de núcleo | 850 nm | 1300 nm | 850 nm |
| OM1 | 62,5 µm | **200** | **500** | No especificado |
| OM2 | 50 µm | **500** | **500** | No especificado |
| OM3 | 50 µm | 1500 | 500 | **2.000** |
| OM4 | 50 µm | 3500 | 500 | **4.700** |
| OM5 | 50 µm | 3500 | 500 | **4.700** |

**Tabla 3.** Designación en ANSI/TIA-568.3-D. (Fluke, 2020)

La saturación es con una fuente LED; el efectivo es con una fuente VCSEL. Nueva fuente frente a la antigua. La comprobación de longitud/pérdidas con respecto a ISO/IEC debe realizarse con un LED y debería realizarse con un LED para la comprobación de TIA, para evitar resultados optimistas.

Para la mayoría de los usuarios, la siguiente tabla podría ofrecer un mayor beneficio:

| | 1000BASE-SX | 10GBASE-SR | 40GBASE-SR4 | 100GBASE-SR10 |
|---|---|---|---|---|
| OM1 | 275 m | 33 m | No especificado | No especificado |
| OM2 | 550 m | 82 m | No especificado | No especificado |
| OM3 | No especificado | 300 m | 100 m | 100 m |
| OM4 | No especificado | 400 m* | 150 m | 150 m |
| OM5 | No especificado | 400 m* | 150 m | 150 m |

**Tabla 4.** Comprobación de longitud/pérdidas con respecto a ISO/IEC. (Fluke, 2020)

Nota de precaución: En ANSI/TIA-568-B.3, el ancho de banda modal de fibra de 62,5 µm fue de 160 MHz.km y no los 200 MHz.km de ANSI/TIA-568.3-D actual. Este cambio se realizó para corresponder con la norma ISO/IEC 11801. Eso reduciría la distancia para 1000BASE-SX a 220 m. y para 10GBASE-S a 26 m.

También hay un límite de pérdida asociado con estas distancias.

| | 1000BASE-SX | 10GBASE-S | 40GBASE-SR4 | 100GBASE-SR10 |
|---|---|---|---|---|
| OM1 | 2,60 dB | 2,4 dB | No especificado | No especificado |
| OM2 | 3,56 dB | 2,3 dB | No especificado | No especificado |
| OM3 | 3,56 dB | 2,6 dB | 1,9 dB | 1,9 dB |
| OM4 | No especificado | 2,9 dB | 1,5 dB | 1,5 dB |
| OM5 | No especificado | 2,9 dB | 1,5 dB | 1,5 dB |

**Tabla 5.** Norma ISO/IEC 11801. (Fluke, 2020)

En cuanto al diseño, tiene que tener en cuenta AMBAS, la distancia y pérdida, para garantizar que sí funcionará su aplicación. La fibra OM4 necesita una reducción en la pérdida de fibra para admitir 100GBASE-SR10 hasta 150 m.

| | 850 nm | 1300 nm | 1310 nm | 1550 nm |
|---|---|---|---|---|
| OM1 | 3,5 dB/km | 1,5 dB/km | | |
| OM2 | 3,5 dB/km | 1,5 dB/km | | |

| | | | | |
|---|---|---|---|---|
| OM3 | 3,0 dB/km | 1,5 dB/km | | |
| OM4* | 3,0 dB/km | 1,5 dB/km | | |
| OM5 | 3,0 dB/km | 1,5 dB/km | | |
| OS1 ISP | | | 1,0 dB/km | 1,0 dB/km |
| OS1 OSP | | | 0,5 dB/km | 0,5 dB/km |
| OS2 ISP | | | 1,0 dB/km | 1,0 dB/km |
| OS2 OSP | | | 0,5 dB/km | 0,5 dB/km |

**Tabla 6.** Distancia y perdida para 100GBASE-SR10 hasta 150 m. (Fluke, 2020)

ISP = planta interior, OSP = planta exterior (aplicable solo a TIA).

Mientras que OM5 tiene valores de rendimiento similares a OM4 para la pérdida de inserción y las distancias compatibles, tiene una característica especial que lo diferencia. La fibra de OM5 está diseñada para usarse en las longitudes de onda más allá de 850 nm, específicamente 880 nm, 910 nm, y 940 nm. This means that it can support four simultaneous transmissions with Wave Division Multiplexing. There is an attenuation value for the 953 nm wavelength, 2,3 dB per KM. Field testing of OM5, however, only needs to be done at 850 and 1300 nm wavelengths. (Fluke, 2020)

### 2.14.2. Medios no Guiados

Los medios de transmisión no guiados son los que no confinan las señales mediante ningún tipo de cable, sino que las señales se propagan libremente a través del medio. Entre los medios más importantes se encuentran el aire y el vacío. Tanto la transmisión como la recepción de información se lleva a cabo mediante antenas. A la hora de transmitir, la antena irradia energía electromagnética en el medio. Por el contrario, en la recepción la antena capta las ondas electromagnéticas del medio que la rodea. La configuración para las transmisiones no guiadas puede ser direccional y omnidireccional. En la direccional, la antena transmisora emite la energía electromagnética concentrándola en un haz, por lo que las antenas emisora y receptora deben estar alineadas.

En la omnidireccional, la radiación se hace de manera dispersa, emitiendo en todas direcciones pudiendo la señal ser recibida por varias antenas. Generalmente, cuanto mayor es la frecuencia de la señal transmitida es más factible confinar la energía en un haz direccional.
La transmisión de datos a través de medios no guiados, añade problemas adicionales provocados por la reflexión que sufre la señal en los distintos obstáculos existentes en el medio. Resultando más importante el espectro de frecuencias de la señal transmitida que el propio medio de transmisión en sí mismo. Según el rango de frecuencias de trabajo, las transmisiones no guiadas se pueden clasificar en tres tipos: radio, microondas y luz (infrarrojos/láser). (Sanchez, 2011)

### 2.14.3. Tecnologías Inalámbricas

Las redes inalámbricas se pueden clasificar en cuatro grupos específicos según el área de aplicación y el alcance de la señal:

- Redes Inalámbricas de Area Personal (*Wireless Personal-Area Networks* - WPAN)
- Redes Inalámbricas de Area Local (*Wireless Local-Area Networks* - WLAN)
- Redes inalámbricas de área metropolitana (*Wireless Metropolitan-Area Networks* - WMAN)
- Redes Inalámbricas de Area Amplia (*Wireless Wide-Area Networks* - WWAN).

La Figura ilustra estas cuatro categorías.

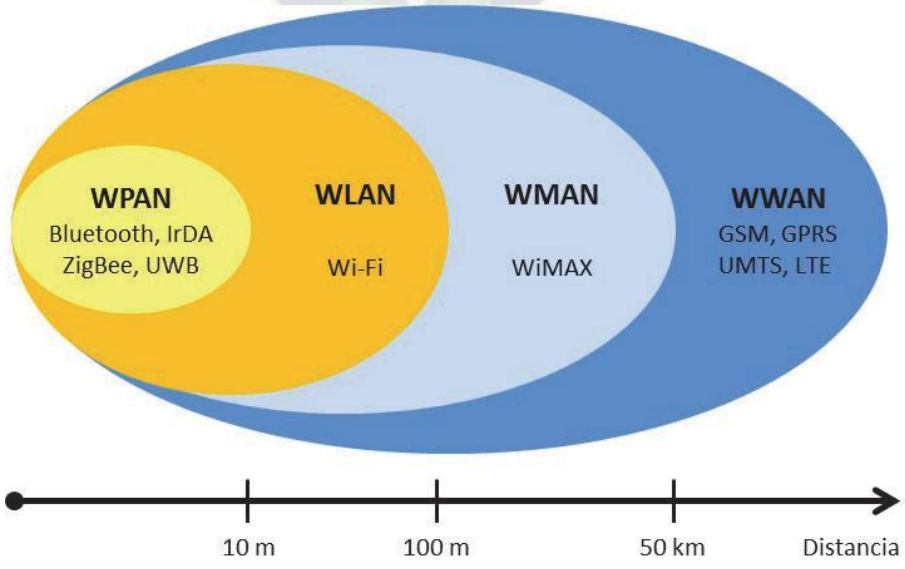



**Figura 30.** Clasificación de las redes inalámbricas. (Salazar, 2022)

Además, las redes inalámbricas pueden dividirse también en dos grandes segmentos: de corto y de largo alcance. Inalámbrica de corto alcance se refiere a las redes confinadas en un área limitada. Esto se aplica a las redes de área local (LAN), como edificios corporativos, los campus escolares y universitarios, fábricas o casas, así como a las redes de área personal (PAN) donde los ordenadores portátiles necesitan estar muy cerca entre sí para comunicarse. Estas redes suelen operar sobre un espectro sin licencia y reservado para uso industrial, científica y médica (banda ISM). Las frecuencias disponibles difieren de país a país. Las bandas de frecuencia más comunes son la de 2,4 GHz y la de 5 GHz, que están disponibles en la mayor parte del mundo. La disponibilidad de estas bandas de frecuencias permite a los usuarios operar con redes inalámbricas sin necesidad de obtener una licencia, y además sin cargo alguno. Al no requerirse una licencia para su uso, ello ha facilitado la expansión de este tipo de redes. En las redes de largo alcance, la conectividad es típicamente proporcionada por las empresas que comercializan la conectividad inalámbrica como un servicio. Estas redes abarcan grandes áreas, tales como un área metropolitana (WMAN), un estado o provincia, o un país entero. El objetivo de las redes de largo alcance es proporcionar cobertura inalámbrica a nivel mundial. La red de largo alcance más 8 común es la red inalámbrica de área amplia (WWAN). Cuando se requiere verdadera cobertura global, también están disponibles las redes de satélites. (Salazar, 2022)

**Bandas de Frecuencia**

Las redes inalámbricas hacen uso de frecuencias en las bandas ISM y UNII.

Banda ISM. Esta banda es para el uso de la WLAN para aplicaciones industriales, científicas y mecánicas.

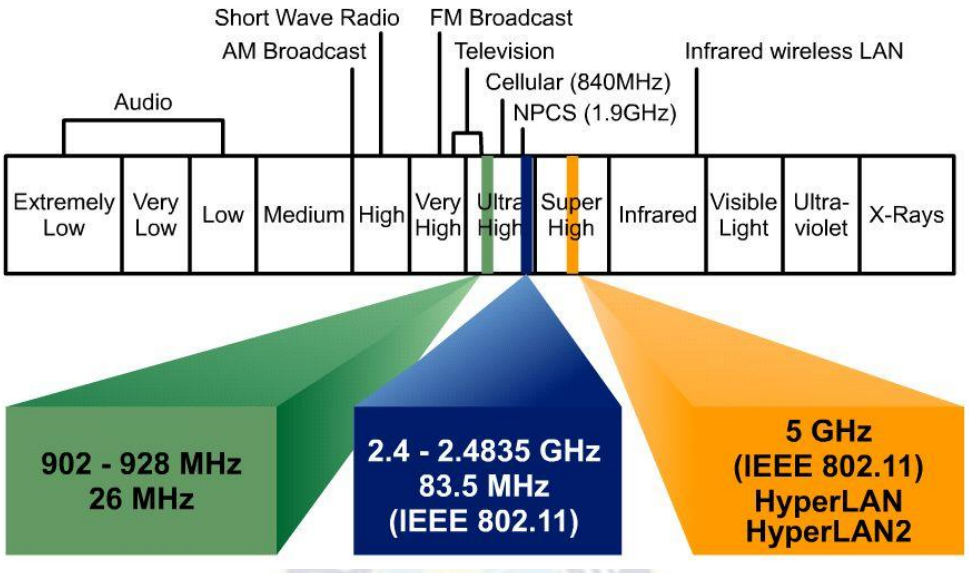



**Figura 31.** Bandas de Frecuencia. (Salazar, 2022)

- **Banda ISM 900 MHz**, esta banda posee un rango de frecuencias desde los 902 MHz a 928 MHz, generalmente usada para la telefonía móvil.
- **Banda ISM 2,4 GHz**, con un rango de 2.4 GHz a 2.4835 GHz, integrada por un conjunto de estándares 802.11 a/b/g y muchos otros más, es utilizada para las comunicaciones en redes inalámbricas.
- **Banda UNI**. Se hallan varias bandas en 5 GHz que son usadas por dispositivos que operan con 802.11ª, se las conoce como muy baja, media y alta.
- **Banda Baja.** Se encuentran en el rango de frecuencias que está entre 5.15GHz a 5.25GHz, para operaciones con 802.11ª la IEEE especifica que la potencia de salida de los dispositivos sea 40mW, para el uso en interiores.
- **Banda Media**. Se encuentra en el rango de frecuencias que se va desde 5.25GHz a 5:35GHz, para aplicaciones con 802.11ª la IEEE recomienda que la potencia de salida sea de 200mW, que normalmente es utilizada frecuentemente para enlazar edificios en espacios cerrados.
- **Banda Alta**. Comprende el rango de frecuencias que esta entre 5.725GHz a 5.825GHz, para 802.11ª la IEEE recomienda una potencia de salida de 800 mW reservada para enlaces exteriores. (Salazar, 2022)

**Canales de Transmisión**

Antes de pasar a un estudio más profundo se hace necesario definir exactamente la banda de frecuencia y la canalización dispuesta. El estándar 802.11 está pensado para operar en la banda de frecuencias entre 2.4 y 2.497 GHz.

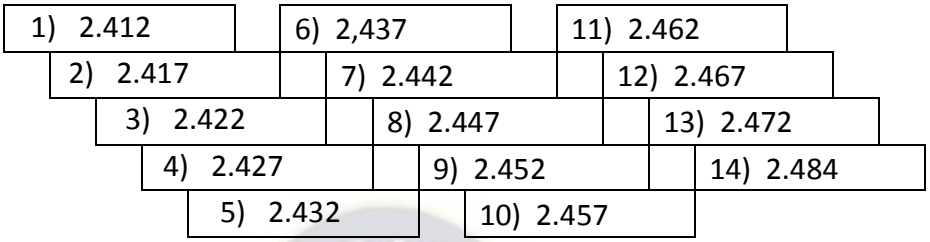



**Figura 32.** Banda de frecuencias estándar 802.11.

**ID de canal, Frecuencia central (MHz), Ancho de banda (Mhz)**

En la figura se muestra los canales específicos disponibles para esta tecnología, pero estas son reguladas en cada país según sus respectivas agencias de regulación del espectro radioeléctrico.

| ID de canal | Frecuencia central (MHz) | Ancho de banda (MHz) |
|---|---|---|
| 1 | 2412 | 20 |
| 2 | 2417 | 20 |
| 3 | 2422 | 20 |
| 4 | 2427 | 20 |
| 5 | 2432 | 20 |
| 6 | 2437 | 20 |
| 7 | 2442 | 20 |
| 8 | 2447 | 20 |
| 9 | 2452 | 20 |
| 10 | 2457 | 20 |
| 11 | 2462 | 20 |
| 12 | 2467 | 20 |
| 13 | 2472 | 20 |
| 14 | 2484 | 20 |

**Tabla 7.** Bandas reguladas.

En nuestro país ocurre un hecho insólito, ya que la frecuencia de operación 2.4GHz fue otorgada a la empresa Multivisión para brindar servicios de TV cable, esto en gestiones anteriores.

Hoy en día, existe en el mercado una gran cantidad de posibilidades para implementar una red inalámbrica. Cada una intenta responder a unas ciertas necesidades y normalmente cada posibilidad pertenece a una cierta compañía que apostó por esta. Las compañías necesitan que sus productos sean compatibles con los de las otras, de aquí que surja la necesidad de tener un estándar que seguir.

| Estándar WLAN | 802.11b | 802.11a | 802.11g | 802.11h | HiperLAN2 | Bluetooth |
|---|---|---|---|---|---|---|
| Organismo | IEEE(USA) | IEEE | IEEE | IEEE | ETSI(euro) | Bluetooth SIG |
| Finalización | 1999 | 2002 | Jun,2003 | 2003 | 2003 | 2002 |
| Denominación | Wi-Fi | Wi-Fi5 | | | | |
| Banda frecuencias | 2.4GHz (ISM) | 5 GHz | 2.4GHz (ISM) | 5 GHz | 5 GHz | 2.4 GHz |
| Velocidad máx. | 11 Mbps | 54 Mbps | 54 Mbps | 54 Mbps | 54 Mbps | 0.721Mbit/s |
| Throughput medio | 5,5 Mbps | 36 Mbps | | | 45 Mbps | |
| Interfaz aire | SSDS/FH | OFDM | OFDM | OFDM | OFDM | DSSS/FHSS |
| Disponibilidad | >1000 | algunos | algunos | algunos | (2004) | Muchos |
| Otros aspectos | | | | TPC, DFA | | |
| Nº de canales | 3c no solapados | 12 no solapados | 3 no solapados | 19 no solapados | | |

**Tabla 8.** Tabla comparativa de los diferentes estándares. (Yunquera, 2017)

En los orígenes de las redes inalámbricas, algunas de las soluciones WLAN se basaban en soluciones propietarias de cada fabricante, este tipo de soluciones no podían funcionar con productos de otros fabricantes. Esto obligaba a cada uno a disponer de toda la infraestructura necesaria para cubrir todas las necesidades del mercado.

El IEEE respondiendo a las necesidades del mercado y los fabricantes, comprendió la necesidad de un estándar que limitase y definiese cada uno, para que su uso fuese lo más eficiente posible. Precisamente ha sido la estandarización de los productos la que ha dado lugar

al tremendo auge que está teniendo este tipo de tecnología. La estandarización ha permitido desvincularse de tecnologías propietarias, consiguiendo una plataforma abierta con productos de mayores prestaciones y a un precio mucho más ajustado. (Yunquera, 2017)

### Seguridad inalámbrica WEP (Wired Equivalent Privacy)

La confidencialidad (impidiendo el acceso no autorizado a los contenidos de un mensaje) se logra mediante la protección del contenido de los datos con el cifrado. El cifrado es opcional en las WLAN, pero sin él, cualquier dispositivo compatible con el estándar dentro del alcance de la red puede leer todo su tráfico.

Principalmente ha habido tres métodos de encriptación para hacer seguras las redes WLAN. Desde finales de 1990, los algoritmos de seguridad Wi-Fi han sufrido múltiples actualizaciones con una pura y simple depreciación de los algoritmos más antiguos y una sustancial revisión de los algoritmos más recientes. En orden cronológico de aparición, estos son:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2 (Wi-Fi Protected Access, version 2)

**WEP.** Fue ratificado como estándar de seguridad Wi-Fi en septiembre de 1999. Las primeras versiones de WEP no eran particularmente fuertes, incluso para el momento en que fueron lanzados, porque las restricciones estadounidenses a la exportación de diversas tecnologías criptográficas llevaron a los fabricantes a restringir sus dispositivos con sólo 64 bits de cifrado. Cuando se levantaron las restricciones, se incrementó a 128 bits. A pesar de la introducción de la encriptación WEP de 256 bits, 128 bits siguen siendo una de las implementaciones más comunes.

A pesar de las revisiones del algoritmo y un aumento del tamaño de la clave, con el tiempo fueron descubiertos numerosos fallos de seguridad en el estándar WEP y, con una potencia de cálculo de los ordenadores cada vez mayor, se hizo más y más fácil explotarlos. Desde 2001 ya circulaban las gestas de la prueba de concepto y antes de 2005 el FBI hizo una demostración

pública (en un esfuerzo por aumentar la conciencia de las debilidades de WEP) en la que rompían las contraseñas WEP en minutos utilizando software de libre distribución.

A pesar de varias mejoras, soluciones temporales y otros intentos para reforzar el sistema WEP, éste sigue siendo altamente vulnerable y los sistemas que se basan en WEP deberían ser actualizados o, si las actualizaciones de seguridad no son una opción, reemplazados. Wi-Fi Alliance retiró oficialmente WEP en 2004. (Salazar, 2022)

**WPA**. Para hacer frente a las vulnerabilidades de WEP, el grupo comercial Wi-Fi Alliance estableció WPA a principios de 2003. La configuración WPA más común es WPAPSK (Pre-Shared Key). Las claves utilizadas por WPA son de 256 bits, un aumento significativo con respecto las claves de 64 bits y 128 bits utilizados en el sistema WEP.

Algunos de los cambios significativos implementados con WPA incluyeron comprobaciones de integridad del mensaje (para determinar si un atacante había capturado o alterado paquetes transmitidos entre el punto de acceso y el cliente) y el protocolo de integridad de clave temporal (Temporal Key Integrity Protocol - TKIP). TKIP utiliza un sistema de claves por paquete que era radicalmente más segura que la clave fija utilizada en el sistema WEP. TKIP fue reemplazado más tarde por el Advanced Encryption Standard (AES).

A pesar de que WPA era una mejora significativa sobre WEP, el fantasma de WEP atormentaba a WPA. TKIP, un componente central de WPA, fue diseñado para ser fácilmente ampliado a través de actualizaciones de firmware en los dispositivos WEP existentes. Como tal, tuvo que reciclar ciertos elementos utilizados en el sistema WEP que, en última instancia, también fueron explotados.

WPA, al igual que su predecesor WEP, se ha demostrado a través de ambas manifestaciones públicas a prueba de concepto y aplicadas a ser vulnerable a la intrusión. Curiosamente el proceso por el cual WPA se suele romper no es por un ataque directo contra el algoritmo WPA (aunque este tipo de ataques se han demostrado con éxito), sino por los ataques contra un sistema complementario que se puso en marcha con la instalación de WPA, la

configuración protegida de Wi-Fi (WPS), diseñada para hacer más fácil la conexión de dispositivos a los puntos de acceso actuales. (Salazar, 2022)

**WPA2.** A partir de 2006, WPA fue sustituido oficialmente por WPA2. Uno de los cambios más significativos entre WPA y WPA2 fue el uso obligatorio de los algoritmos AES y la introducción de CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) como un reemplazo de TKIP (aún se conserva en WPA2 como un sistema de reserva y para interoperabilidad con WPA).

En la actualidad, la principal vulnerabilidad de seguridad para el sistema WPA2 real es una de oscura y requiere que el atacante ya tenga acceso a la red Wi-Fi protegida con el fin de tener acceso a ciertas claves para luego poder perpetuar un ataque en contra de los otros dispositivos en la red. Como tal, las implicaciones en seguridad de estas vulnerabilidades de WPA2 se limitan casi exclusivamente a las redes a nivel de empresa y merecen poca o ninguna consideración práctica en materia de seguridad de red doméstica.

Por desgracia, la misma vulnerabilidad causante del mayor agujero en la armadura WPA, el vector de ataque a través de la configuración protegida de Wi-Fi (WPS), persiste en los puntos de acceso WPA2 actuales. Aunque para irrumpir en una red protegida con WPA/WPA2 utilizando esta vulnerabilidad sean necesarias de 2-14 horas de esfuerzo sostenido con un ordenador actual, todavía es una preocupación legítima de seguridad y WPS debería ser desactivada (y, si fuese posible, el firmware del acceso punto debería ser reprogramado con una distribución que ni siquiera admitiese WPS por lo que el vector de ataque se eliminaría por completo).

La siguiente es una lista básica de clasificación de los métodos actuales de seguridad Wi-Fi, ordenados de mejor a peor:

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES (TKIP aparece como método alternativo)
4. WPA + TKIP

5. WEP

6. Red abierta (ningún tipo de seguridad)

Idealmente, se desactivará la configuración protegida de Wi-Fi (WPS) y se pondrá el nivel de seguridad a WPA2 + AES. Todo lo demás en la lista está por debajo de lo ideal. (Salazar, 2022)

## 2.15. MODELO OSI Y MODELO TCP/IP

El modelo de capas de una red surgió como respuesta al problema de que cada fabricante implementaba su propia solución de red y muchas veces era incompatible con el hardware de otros fabricantes.

El modelo de capas es una abstracción de una red en la que segmentamos o dividimos una conexión en capas independientes una de otra para descomponer el sistema en partes más pequeñas, más fáciles de analizar y de resolver. Cada capa recibe los datos de la capa superior o inferior, los procesa y se los devuelve a la siguiente capa.

### 2.15.1. Modelo OSI

El modelo OSI consta de 7 capas o niveles que van desde el más bajo que es la capa fisca del hardware hasta la capa 7 que serían las aplicaciones.


**Figura 33.** Modelo OSI. (Josan, 2021)

El modelo de capas OSI es el referente, pero a la hora de la verdad utilizamos un modelo con un número menor de capas para hacerlo más sencillo y flexible.

### 2.15.2. Modelo TCP/IP

Como el modelo de capas OSI no se tenían los protocolos bien desarrollados y su implementación era muy cara y complicada surgió el modelo de capas TCP/IP.

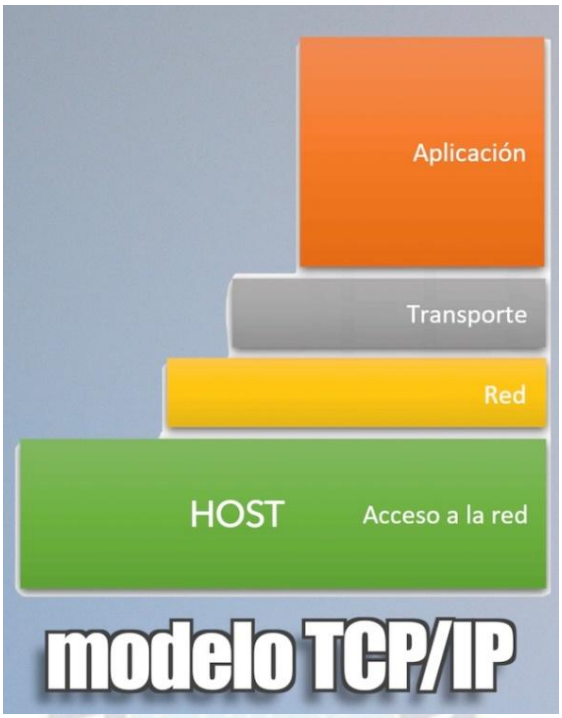



**Figura 34.** Modelo TCP/IP. (Josan, 2021)

El modelo TCP/IP consta de tan solo 4 capas, agrupamos varias capas del modelo OSI en una sola. La capa 1 y 2 la englobamos en una única capa llamada "Host" y la capa 5 y 6 las agrupamos en la capa 7 de aplicación.

Como la capa 2 de enlace se encarga de realizarla el hardware, juntamos la capa 1 y 2 en una sola que llamamos host-red. Esta capa es la encargada de transmitir, recibir y verificar la integridad de los datos.

Las tareas de sesión y presentación las puede realizar las capas inferiores o superiores, por lo que la capa 7 de aplicación es la encargada de realizar las funciones de las 3 capas. Paradójicamente, aunque a la capa de aplicación le correspondería el número 4 se le respeta el número de orden del modelo OSI y se le sigue designando como capa 7. (Josan, 2021)

En esta imagen vemos la comparativa entre el modelo TCP/IP frente al OSI.

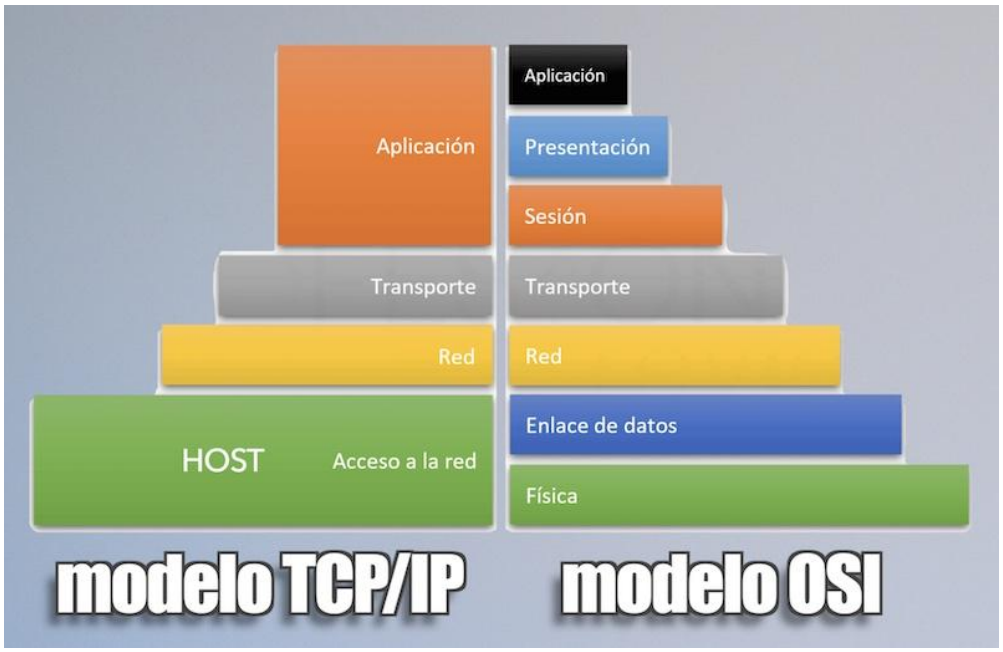



**Figura 35.** Comparativa entre el modelo TCP/IP frente al OSI. (Josan, 2021)

### 2.15.3. Modelo híbrido

A la hora de la verdad utilizamos un **modelo de capas híbrido** en el que la capa 1 del modelo TCP/IP lo dejamos como estaba en el modelo OSI, con 2 niveles: físico y enlace.


**Figura 36**. Modelo Hibrido. (Josan, 2021)

También podríamos verlo como que en el modelo OSI agrupamos las 3 últimas capas en una sola. Es decir, el modelo híbrido podríamos considerarlo como el modelo OSI con 2 capas menos (la 5 y 6) o como el modelo TCP/IP con una capa más (la 1 y 2 separadas). Da igual, es lo mismo, es como ver el vaso medio lleno o medio vacío, el resultado es el mismo. (Josan, 2021).

## 2.16. CENTROS DE DATOS

### 2.16.1. Definición

Un centro de datos (Data Center) son **instalaciones físicas centralizadas donde se alojan ordenadores, redes, almacenamiento y otros equipos de TI que permiten el funcionamiento de una empresa**. Los ordenadores de un centro de datos contienen o facilitan aplicaciones, servicios y datos esenciales para la empresa.

Un Data Center, o **"centro de procesamiento de datos"** es en sí misma una instalación, construcción o inmueble de gran tamaño donde se albergan y mantienen numerosos equipos electrónicos como servidores, ventiladores, conexiones y otros recursos necesarios que se utilizan para mantener una red o un sistema de computadoras, información, conexiones y datos de una o varias empresas.

Muchos de los datos que existen en la actualidad son generados desde teléfonos, tabletas, computadoras, electrodomésticos, relojes inteligentes y otros dispositivos conectados a internet que tienen su almacenamiento en Data Center.

Dichas instalaciones necesitan contar con la suficiente energía para operar todo ese sistema, así como una ventilación adecuada para su funcionamiento óptimo y sistemas de seguridad avanzados para evitar fugas de datos u otros riesgos.

Asimismo, ofrece alojamiento a empresas, les ayuda a compilar, guardar y proteger toda su información digital, así como interconectarse con algunos proveedores para garantizar la continuidad de sus operaciones.

A pesar de que una empresa puede contar con su propio Data Center, lo más recomendable es que la encargada de tener dicho centro de datos y resguardar esa gran cantidad de información, sea una empresa dedicada a este rubro; así podrá mantener la seguridad y continuidad del negocio. Asimismo, es importante contar con un servicio de soporte en informática para ayudar a solventar cualquier incidente que pueda generarse.

Las empresas especializadas que se dedican a brindar estos servicios deben contar con el equipo y espacio suficiente de almacenamiento para poder resguardar de mejor forma las inmensas cantidades de datos que puedan llegar a recibir. (kionetworks, 2022).

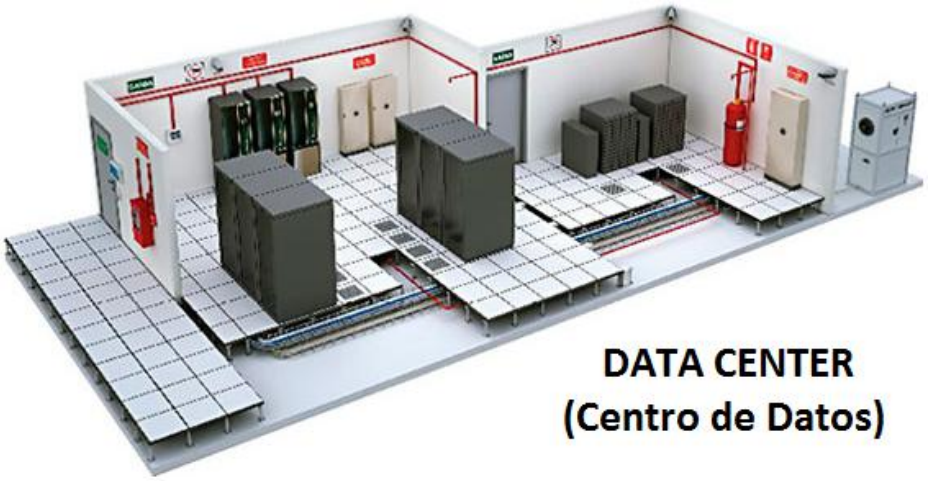



**Figura 37**. Centro de Datos.

Estos son solo algunos de los factores que deben considerarse al diseñar un centro de datos.

- **Ubicación:** La ubicación del centro de datos es crítica y debe estar alejado de cualquier amenaza de desastres naturales, tales como inundaciones, terremotos, huracanes, etc. Además, es importante que la ubicación esté cerca de una fuente de energía eléctrica confiable y que tenga buena conectividad de red.
- **Espacio físico:** El espacio físico debe ser lo suficientemente grande para alojar los equipos de TI y proporcionar espacio para el crecimiento futuro. El espacio también debe estar diseñado para garantizar una buena circulación de aire y evitar la acumulación de calor.
- **Energía:** Un centro de datos necesita una fuente confiable de energía eléctrica. Es necesario considerar la capacidad eléctrica necesaria para el funcionamiento de los equipos, así como la capacidad de respaldo de energía en caso de cortes de energía.

- **Enfriamiento:** Los equipos de TI generan una gran cantidad de calor, por lo que es necesario implementar sistemas de enfriamiento adecuados para evitar el sobrecalentamiento. Esto puede incluir sistemas de refrigeración por aire o por agua, así como la implementación de un diseño que permita una buena circulación de aire.
- **Conectividad:** Es importante garantizar que el centro de datos tenga una conectividad de red adecuada y confiable. Esto puede incluir múltiples proveedores de conectividad y redundancia de red para garantizar la continuidad del servicio.
- **Seguridad:** La seguridad del centro de datos es crítica y debe incluir medidas para prevenir el acceso no autorizado, como sistemas de control de acceso, cámaras de seguridad y sistemas de detección de intrusiones.
- **Gestión:** Un centro de datos bien diseñado debe ser fácil de gestionar y mantener. Esto puede incluir la implementación de herramientas de monitorización y gestión remota, así como la implementación de procedimientos y políticas para la gestión y mantenimiento de los equipos.

### 2.16.2. Características del Centro de Datos.

- **Continuidad de negocio**

  Un Centro de Datos debe ofrecer la garantía de que el negocio siga funcionando de manera correcta sin importar los eventos que se susciten. Los recursos, información y procesos indispensables en una empresa deben estar disponibles siempre y cuando se necesiten para seguir ofreciendo los productos o servicios y no perder dinero por la inestabilidad o indisposición de los sistemas.

- **Velocidad de respuesta**

  No basta que los recursos del Centro de Datos estén disponibles 24*7, también es necesario que estos respondan a las necesidades de la empresa con rapidez. Los centros de datos deben responder rápidamente a las aplicaciones clave del negocio, contar con tecnologías de conectividad óptima desde los servidores, redes de Fibra óptica y gestión de enlaces mediante una solución SD-WAN para garantizar la disponibilidad de sistemas esenciales para el negocio.

- **Seguridad de la información**

  Un centro de procesamiento de datos debe tener altos estándares de seguridad de la información, así como personal calificado para evitar filtraciones o pérdidas. Contar con un centro de datos para recuperación frente a desastres o una solución de *Disaster Recovery* es una de las mejores decisiones que puede tomar una empresa moderna, en especial si es de un sector de alta confidencialidad como la banca, gobierno o seguros.

  Por ejemplo, las entidades bancarias e instituciones de educación superior requieren un centro de datos capaz de servir de respaldo frente a la posibilidad de un ataque de encriptado o pérdida total del centro de datos principal.

- **Alta capacidad de almacenamiento**

  Una infraestructura de data center brinda la posibilidad de almacenar una alta cantidad de información debido a la infraestructura propia o de la empresa proveedora. Así como la virtualización, al ser una de las tecnologías más relevantes para aumentar la capacidad de almacenamiento con menores costos, presenta una gran alternativa para las empresas en crecimiento.

- **Simplicidad**

  La administración de datos puede ser compleja y requerir de profesionales en la administración de redes y comunicaciones, así como especialistas en la correcta implementación de infraestructura. Por el contrario, solicitar a un proveedor de servicios de data center permite a las empresas centrarse en sus actividades y simplificar el proceso de almacenamiento de información.

- **Escalabilidad**

  En los casos de tercerización de servicios de data center, las condiciones tecnológicas modernas permiten que una empresa pueda solicitar un aumento en su capacidad de almacenamiento o infraestructura de forma casi inmediata, incluso mediante el almacenamiento en nube es posible pagar solamente por el espacio empleado sin contar con algún límite predeterminado. En los casos de centros de datos propios, las empresas

deben proyectar su crecimiento e ir escalando sus capacidades a medida que las necesidades crecen.

- **Flexibilidad**

  Debido a su alta disponibilidad y estar cada vez más vinculados a las tecnologías de almacenamiento en nube, los data center pueden permitir que las empresas empleen su información cuando más la requieran, inclusive por transferirla a otros equipos o elaborar un esquema de trabajo remoto.

- **Eficiencia y confiabilidad**

  Los centros de datos de más alto nivel poseen disponibilidades de hasta 99.995% por este motivo se puede confiar en que los datos corporativos estarán disponibles para los miembros de su organización cuando más lo necesite y con una gran velocidad para la descarga de datos o el despliegue de aplicaciones.

- **Ahorro de costos**

  La optimización del presupuesto se da al disponer de la infraestructura tecnológica especializada, donde las empresas ya no deberían de invertir en equipos y disponer constantemente de mantenerlos y actualizarlos. Esto presenta un significativo ahorro de costes en hardware y mantenimiento, así como reducir la contratación de personal propio en el área de TI. (kionetworks, 2022)

### 2.16.3. Clasificación de un Centro de Datos

De acuerdo con la ANSI (American National Standars Institute), los Data Centers poseen una norma de mejores prácticas llamada *ANSI/TIA 942*, su objetivo es certificar la disponibilidad de los componentes que tienen estos inmuebles. El tamaño, el tiempo de respuesta y los niveles de redundancia, son algunos ejemplos de los aspectos que se consideran en dicha certificación.

Aunado a esta clasificación existen varios niveles denominados **"*Tiers*".** El concepto de Tier indica el nivel de fiabilidad de un centro de datos asociados a cuatro niveles de disponibilidad definidos. Mientras más grande sea el número o clase del Tier, mayor

disponibilidad del servicio y, por lo tanto, mayores costos asociados en su construcción y más tiempo para hacerlo. En la actualidad se han definido cuatro tipos de Tier.

### 2.16.4. Alcances del estándar ANSI/TIA-942-B (2017)

Cuando una empresa desea validar sus instalaciones, debe contar con la certificación adecuada, cumpliendo con los estándares o normas que abarcan en ese entorno.

En el caso de los Data Center, deben cumplir los alcances que establece el estándar ANSI/TIA-942-B. Este alcance determina las áreas o funcionalidades que serán revisadas, evaluadas y certificadas según los parámetros de la norma, tales como:

- Infraestructura eléctrica.
- Sistema mecánico de enfriamiento.
- Ubicación del Data Center.
- Arquitectura del Data Center.
- Seguridad de Datos.
- Seguridad de las instalaciones.
- Sistemas de detección y supresión de incendios.

**Por ejemplo, en Rated-2: Redundant Capacity Component Site Infrastructure**

Se le otorga a un Data Center que posee capacidades de redundancia en datos y suministro eléctrico, y una ruta de distribución única no redundante. Adicionalmente, también posee cierta capacidad de protección contra eventos físicos adversos. En general:

- **El Rated 1 es el Centro de Datos básico**: está constituido para las pequeñas y medianas empresas. El servicio puede sufrir interrupciones planificadas o no planificadas. Una desventaja de este nivel es que en caso de que se requiera un mantenimiento, será necesario detener su actividad por completo, por lo que la continuidad del negocio puede interrumpirse en varias ocasiones.

- **El Rated 2 es un Centro de Datos redundante** y es menos susceptible a interrupciones, ya sean planificadas o no. Tiene una conexión a una línea única de distribución eléctrica

y de refrigeración. Al igual que el nivel anterior, en caso de mantenimiento, aquí también se necesita la interrupción del servicio.

- **Rated 3 es un Data Center Concurrentemente Mantenible**. Está enfocado a compañías que prestan un servicio 24/7, es decir, 24 horas, los 7 días de la semana. Un Centro de Datos con estas características está conectado a múltiples líneas de distribución eléctrica y refrigeración, aunque con sólo una activa. Ello ayuda a mantener la continuidad de las operaciones. Lo destacable de este nivel y una ventaja con respecto a los dos anteriores, es que para su mantenimiento no es necesario paralizar el sistema, ya que su capacidad es totalmente ideal para entregar el servicio mediante otras líneas.
- **Rated 4 o Centro de Datos tolerante a fallos**: está enfocado a empresas con una presencia global, como bancos, multinacionales, entre otras. Algo sumamente destacable es su tolerancia a las fallas, debido a que está conectado a varias líneas de distribución eléctrica y refrigeración. Este nivel permite seguir las funciones de un negocio durante un mantenimiento sin afectar al servicio, en especial en compañías que tienen operaciones críticas, y es capaz de enfrentar eventos que no se tenían planeados.

En realidad, la única forma en que pudiera fallar es que suceda al mismo tiempo un corte de energía y el error de dos o más factores eléctricos en cada una de las líneas de suministro. (kionetworks, 2022)

### 2.16.5. Actualización ANSI/TIA-942-B-1 para la infraestructura de los centros de datos tipo Edge

La Asociación de la Industria de las Telecomunicaciones (TIA) acaba de publicar un apéndice (Enero 2022) de la norma ANSI/TIA-942-B de infraestructura de telecomunicaciones para centros de datos, la norma utilizada por los profesionales de las tecnologías de la información y las comunicaciones (TIC) en todo el mundo para diseñar, implementar y verificar la infraestructura de los centros de datos.

El apéndice de la norma define los requisitos iniciales de la infraestructura y las directrices de diseño para los centros de datos tipo Edge, también denominados "microcentros" de datos. Como señala el comité de normas, los centros de datos Edge suelen estar alojados en recintos

prefabricados y pueden ser supervisados y controlados a distancia. Se consideran fundamentales para el éxito de las aplicaciones de próxima generación que exigirán una latencia ultrabaja, como los vehículos autónomos, la realidad aumentada y la telemedicina.

### 2.16.6. Tipos de Centro de Datos

Debido a la gran variedad y flexibilidad que ofrecen los Data Center, es responsabilidad del área de TI de un negocio encontrar el tipo o la combinación ideal que más se ajuste a sus necesidades, tomando en cuenta la disponibilidad, los recursos humanos y técnicos destinados para mantener las correctas operaciones del centro de datos y, por supuesto, la inversión que se tiene pensado destinar para ello.

Si el Data Center se encuentra ubicado en las propias instalaciones de la empresa o negocio, el o los usuarios deben contar con expertos en los distintos tipos de aplicaciones que se ejecutan y contar con contratos de mantenimiento en hardware de servidores y telecomunicaciones, además de la especialización para el mantenimiento en su infraestructura. Las ventajas de tener un Data Center en la oficina propia es que se tiene total libertad para hacer y operar con él en cualquier momento y en lo que se necesite, está disponible.

Al estar el hardware en el sitio, el personal especializado de tu empresa puede acceder cuantas veces desee al espacio para hacer los correctivos de rigor. También la seguridad y el tiempo de actividad son plena responsabilidad del personal de TI.

Sin embargo, tener un Centro de Datos propio también tiene algunas desventajas. Las responsabilidades en todos los aspectos del aprovisionamiento e infraestructura y la administración del Data Center recae enteramente en gente de la propia empresa, esto puede ocasionar un problema cuando, por ejemplo, haya una emergencia en la madrugada o un día festivo y nadie pueda cubrirlo.

Otra desventaja son los costos de construcción, que la empresa asume en su totalidad. Además de que los gastos internos de funcionamiento suelen ser mucho más altos que optar por el “hosting” o un Data Center externo.

Si se decide optar por el hosting, básicamente albergaría los servidores en un Data Center externo. Entre los servicios que proporciona el proveedor son: el espacio para instalar los servidores y equipo del negocio, la energía eléctrica que requiere, la refrigeración para su óptimo desempeño, enlaces de comunicación dentro del Data Center y personal especializado para atender cualquier requerimiento. (kionetworks, 2022).

**Infraestructura Critica y Soporte Operativo.**

Para mantener el equipamiento IT en condiciones óptimas de operación, se debe recurrir a la infraestructura adecuada que permita mantener el centro de datos en condiciones de entorno adecuadas que incluye Refrigeración, Energía, Seguridad Física, etc.


**Figura 38.** Infraestructura Critica y Soporte Operativo.


**Funcionalidad de un Centro de Datos.**

Sin importar el tamaño, todos los Data Centers, cumplen con los mismos propósitos:


**Estándares para Infraestructura Critica de Centros de Datos (Data Center)**

Diferentes instituciones y agrupaciones de fabricantes y entidades gubernamentales relacionadas con el sector de la infraestructura de los Centros de Datos, proliferan a lo largo de los continentes, las cuales pueden ser resumidas en las más principales y sus clasificaciones por **"disponibilidad".**

**INSTITUCIONES Y AGRUPACIONES QUE CLASIFICAN LA INFRAESTRUCTURA DE LOS CENTROS DE DATOS SEGUN LA DISPONIBILIDAD (DOWN TIME)**

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

La estandarización de Centros de Datos es la tendencia con los diferentes sistemas planteados en diferentes países, cada institución presenta sus "**capítulos"** con sus normas y lineamientos en amplios documentos, algunos de libre acceso y otros bajo suscripción.

**ISO/IEC 24764 (2010)**
*Information technology — Generic cabling systems for data centres*
44 pages

**ANSI/TIA-942-A (2012)**
*Telecommunications Infrastructure Standard for Data Centers*
118 pages

**CENELEC EN 50173-5:2007 / A2:2012**
*Information technology — Generic cabling systems - Part 5: Data centres*
48 pages

**ANSI/BICSI 002-2014**
*Data Center Design and Implementation Best Practices*
534 pages

**CENELEC EN 50600 (2012-)**
*Information technology — Data centre facilities and infrastructures*
Multiple Documents

**ASHRAE TC9.9 (2012)**
*Thermal Guidelines for Data Processing Environments, 3rd edition*
150 pages

**NORMA INTERNACIONAL PARA LA CONSTRUCCIÓN E INSTALACIÓN DE EQUIPAMIENTO DE AMBIENTES PARA EL EQUIPO DE MANEJO DE TECNOLOGÍAS DE INFORMACIÓN Y SIMILARES**

**ICREA-Std-131-2017**

**1ª Edición**

### 2.16.7. ESTÁNDAR TIA-942

Concebido como una guía para los diseñadores e instaladores de centros de datos (Data Centers), el estándar TIA-942 (2005) proporciona una serie de recomendaciones y directrices (*guidelines*) para la instalación de sus infraestructuras.


TIA-942 es el Estándar Americano para la Infraestructura De Telecomunicaciones Para Data Center.

### 2.16.8. Estándar ANSI/TIA-942-B

ANSI/TIA-942-B es un estándar de la industria para el diseño de infraestructuras de centros de datos. Fue desarrollado por la Asociación de Industrias de Telecomunicaciones (TIA) y está aprobado por el Instituto Nacional Estadounidense de Estándares (ANSI).

El estándar TIA-942-B proporciona una guía detallada para el diseño, la construcción y el funcionamiento de centros de datos. Incluye requisitos y recomendaciones para la infraestructura física del centro de datos, como la ubicación, el espacio, la energía, el enfriamiento, el cableado, la seguridad y el monitoreo ambiental. También establece los

requisitos para los componentes de la infraestructura de TI, como los servidores, el almacenamiento y los dispositivos de red.

El estándar TIA-942-B es ampliamente utilizado por empresas y organizaciones que buscan mejorar la eficiencia, la fiabilidad y la seguridad de sus centros de datos. Al seguir las recomendaciones y las mejores prácticas establecidas en este estándar, las empresas pueden diseñar y construir centros de datos que sean capaces de satisfacer sus necesidades actuales y futuras de TI, y que también sean capaces de proporcionar una alta disponibilidad y una protección adecuada contra riesgos y amenazas. Con el diseño se pretende cumplir con este estándar.

Las características y requisitos a cumplir del estándar ANSI/TIA-942-B son:

- **Rated de disponibilidad:** El estándar define cuatro niveles de disponibilidad (Rated I a Rated IV) que proporcionan un marco común para evaluar la disponibilidad de los centros de datos. Cada nivel se define en función de los requisitos de redundancia y confiabilidad de los sistemas de energía, enfriamiento y TI.
- **Requisitos de espacio y ubicación:** El estándar establece requisitos para la ubicación del centro de datos, incluyendo criterios de selección del sitio, requisitos de construcción, diseño de interiores y otros factores relacionados con el espacio y la ubicación.
- **Requisitos de energía:** El estándar define requisitos para los sistemas de energía de los centros de datos, incluyendo el suministro eléctrico, la distribución de energía, la protección contra sobretensiones y la redundancia de los sistemas de energía.
- **Requisitos de enfriamiento:** El estándar establece requisitos para el diseño y la operación de los sistemas de enfriamiento de los centros de datos, incluyendo la capacidad de refrigeración necesaria, los requisitos de temperatura y humedad, y los requisitos de redundancia.
- **Requisitos de cableado:** El estándar establece requisitos para el diseño y la implementación de los sistemas de cableado estructurado en los centros de datos, incluyendo los tipos de cable y las normas de instalación.

- **Requisitos de seguridad:** El estándar establece requisitos para la seguridad física y lógica de los centros de datos, incluyendo la protección contra intrusiones, el control de acceso y la supervisión ambiental.
- **Requisitos de monitoreo y gestión:** El estándar establece requisitos para la supervisión y el control de los sistemas de TI y de infraestructura en los centros de datos, incluyendo la monitorización ambiental, la gestión de energía y la gestión de la capacidad.
- **Documentación y verificación:** El estándar establece requisitos para la documentación y la verificación del diseño y la implementación de los centros de datos, incluyendo los procedimientos de prueba y los requisitos de informes.

En resumen, ANSI/TIA-942-B es un estándar detallado que establece los requisitos y las mejores prácticas para el diseño y la implementación de centros de datos confiables y eficientes en términos de energía, espacio, seguridad y conectividad.

Esta estándar entrega las especificaciones de los "**Los 4 pilares de un Data Center según TIA-942"**

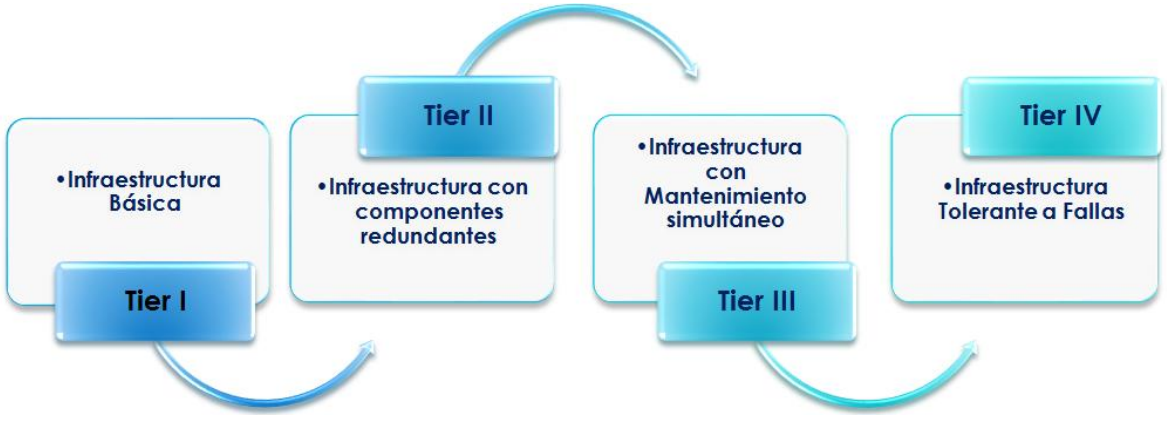
1. **COMUNICACIONES.**
2. **ARQUITECTURA.**
3. **ELECTRICA.**
4. **MECANICA.**

**El Estándar TIA-942-B (2017),** define además **4 niveles (Rated)** basado en las recomendaciones del ***Uptime Institute*** para mantener la **DISPONIBILDAD** 7x24 del **Data Center.**

| RECOMENDACIONES TIA-942 INFRAESTRUCTURA DE SOPORTE PARA UN DATA CENTER | | | |
|---|---|---|---|
| **Telecomunicaciones** | **Arquitectura** | **Eléctrica** | **Mecánica** |
| Cableado de racks | Selección del sitio | Cantidad de accesos | Sistemas de climatización |
| Accesos redundantes | Tipo de construcción | Puntos únicos de falla | Presión positiva |
| Cuarto de entrada | Protección ignífuga | Cargas críticas | Cañerías y drenajes |
| Área de distribución | Requerimientos NFPA 75 | Redundancia de UPS | Chillers |
| Backbone | Barrera de vapor | Topología de UPS | CRAC´s y condensadores |
| Cableado horizontal | Techos y pisos | PDU's | Control de HVAC |
| Elementos activos redundantes | Área de oficinas | Puesta a tierra | Detección de incendio |
| Alimentación redundante | NOC | EPO (Emergency Power Off) | Sprinklers |
| Patch panels | Sala de UPS y baterías | Baterías | Extinción por agente limpio (NFPA 2001) |
| Patch cords | Sala de generador | Monitoreo | Detección por aspiración (ASD) |
| Documentación | Control de acceso | Generadores | Detección de líquidos |
| | CCTV | Transfer switch | |

**Tabla 9.** Recomendaciones TIA-942.

## 2.16.9. CLASIFICACION DE UN DATA CENTER SEGÚN LA DISPONIBILIDAD




Detallando la “disponibilidad” o denominada CLASIFICACION TIER, tenemos:


**Disponibilidad del Data Center.**

- **TIER I** Data Center Básico, susceptible a interrupciones planeadas o involuntarias.
- **TIER II** Componentes Redundantes, Su diseño es lo necesario más uno (N+1).
- **TIER III** Mantenimiento Concurrente, Permite mantenimientos preventivos sin interrupciones.
- **TIER IV** Tolerante a Fallas.

**Cuadro**

| Tier | % disponibilidad | % de parada | Tiempo de parada a año. |
|---|---|---|---|
| Tier I | 99.671 % | 0.329 % | 28.82 horas |
| Tier II | 99.741 % | 0.251 % | 22.68 horas |
| Tier III | 99.982 % | 0.018 % | 1.57 horas |
| Tier IV | 99.995 % | 0.005 % | 52.56 minutos |

**ICREA.**

ICREA (International Computer Room Experts Association), Institución Catalana de Investigación y Estudios Avanzados, es una fundación financiada por el gobierno catalán y dirigida por su patronato. ICREA nació en respuesta a la necesidad de nuevas fórmulas de contratación que permitieran competir en igualdad de condiciones con otros sistemas de investigación, orientándose a la contratación del personal científico y académico más extraordinario y de mayor talento.

ICREA es una institución abierta. Trabaja codo a codo con las universidades catalanas y los centros de investigación para integrar a los investigadores ICREA en el sistema de investigación catalán.

ICREA ofrece a investigadores de todo el mundo plazas permanentes para venir a investigar a Cataluña. Con los años, han llegado a ser sinónimo de excelencia académica a escala mundial.

**Presenta su norma Std-131-2021,** el referente para la continuidad operativa de los centros de datos (disponibilidad).

Ha certificado más de 120 mil metros cuadrados de piso blanco gracias al desarrollo de su norma. • Más de 500 *facilities* han obtenido una certificación o recertificación. • 40 Centros de Datos han sido certificados por ICREA durante 2021.

**El estándar ICREA** define la disponibilidad de servicio en seis niveles, los cuales son:

- **NIVEL I:** Sala de cómputo en ambiente Certificado QADC (Quality Assurance Data Center). Para una disponibilidad del 95%.
- **NIVEL II:** Sala de cómputo en ambiente Certificado de clase mundial WCQA (World Class Quality Assurance). Para una disponibilidad del 99%.
- **NIVEL III:** Sala de cómputo confiable con Ambiente Certificado de clase mundial S-WCQA (Safety World Class Quality Assurance). Para una disponibilidad del 99.9%.

- **NIVEL IV:** Sala de cómputo de alta seguridad con certificación HSWCQA (High Security World Class Quality Assurance). Para una disponibilidad del 99.99%.
- **NIVEL V:** Sala de cómputo de alta seguridad y alta disponibilidad con certificación de clase mundial HSHA-WCQA (High Security High Available World Class Quality Assurance). Para una disponibilidad del 99.999%.
- **NIVEL VI:** Sala de cómputo de alta seguridad y alta disponibilidad con certificación de clase mundial RHA-WCQA (Redundant High Available World Class Quality Assurance Data Center Net). Para una disponibilidad del 99.9999%.

**BICSI**

BICSI (Building Industry Consulting Service International), es una asociación global que impulsa la comunidad de tecnologías de la información y la comunicación. Nuestro objetivo se basa en brindarles a nuestros miembros la oportunidad de tomar la iniciativa y tener éxito en su campo laboral. También ahora, comenzamos a ofrecer nuestros productos y servicios en español.

**ASHRAE**

Sociedad Americana de Aire Acondicionado, Refrigeración y Calefacción, fundada en 1894, ASHRAE es una asociación de tecnología para edificios con más de 57,000 miembros mundialmente. La asociación y sus miembros se enfocan en los sistemas de edificios, la eficiencia energética, la calidad del aire interior y la sostenibilidad dentro de la industria.

A través de la investigación, la redacción de normas, la publicación y la educación continuas, ASHRAE da forma hoy al entorno construido de mañana. ASHRAE fue concebida en 1959 como la Sociedad Americana de Ingenieros de Calefacción, Refrigeración y Aire Acondicionado, debido a la fusión de la Sociedad de Ingenieros de Calefacción y Aire Acondicionado (ASHAE) fundada en 1894, y la Sociedad Americana de Ingenieros de Refrigeración (ASRE) fundada en 1904.

### 2.16.10. Infraestructura Critica del Data Center

Un Centro de Datos deberá contar con todos los elementos requeridos para garantizar la continuidad de la operación de una empresa:

- Sistemas de energía ininterrumpida (UPS).
- Planta de emergencia diésel o a gas (GRUPO GENERADOR).
- Aire acondicionado de precisión (HVAC).
- Sistema de Puesta a Tierra (SPAT).
- Detección y supresión de incendio.
- Sistema de control de acceso y seguridad.
- Control de acceso biométrico.
- Sistemas de Almacenamiento y Respaldo de Información.
- Monitoreo y personal de seguridad 7 x 24.

En la actualidad la Infraestructura Física para Centros de Datos, denominada Infraestructura Física para Redes Críticas (NCPI), constituye el cimiento sobre los cuales las redes Informáticas y de Telecomunicaciones sustentan su funcionamiento.
La NCPI Es la "COLUMNA VERTEBRAL" de los sistemas de comunicación, dado que sus componentes:

- Los equipos de Energía.
- Los equipos de Refrigeración.
- El Área física del CPD y Los Racks.
- La Seguridad Física y Protección contra Incendios.
- El Cableado de Datos y Energía.
- La Administración y Monitoreo.
- Los Servicios de Mantenimiento y Reparación.

Proporcionan un medio eficaz para el funcionamiento ininterrumpido de los sistemas de comunicación actuales.

### 2.16.11. SOLUCIONES DE REFRIGERACION PARA LA INFRAESTRUCTURA DE UN DATA CENTER

Los centros de datos requieren de recursos tecnológicos para garantizar estabilidad en sus procesos. Uno de estos elementos es el aire acondicionado de precisión para data center.

**¿Qué es un sistema de refrigeración de precisión?**

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.

Si se instala un aire acondicionado convencional, se necesita integrar una mayor capacidad para obtener los resultados de un aire acondicionado de precisión. ¿La razón? Estos últimos están diseñados para operar en jornadas laborales largas, sin el riesgo de desgaste prematuro.

Por otro lado, un sistema convencional suele extraer la humedad por debajo de los límites que garantizan la eficiencia de los Centros de Datos. Esto trae dos consecuencias inmediatas: problemas ocasionados por un ambiente muy seco y la necesidad de adquirir sistemas de humidificación.

Gracias a los sistemas de precisión no existen estas consecuencias debido a sus humificadores integrados y la exactitud al gestionar la temperatura correcta.

**Figura 39.** Unidad de Aire de Precisión.

**Arquitecturas de Enfriamiento.**

El objetivo de los sistemas **CRAC** (*Computer Room Air Conditioner*) Sistemas de Aire Acondicionado para centros de Datos, es capturar satisfactoriamente el complejo flujo de calor residual y extraerlo de la sala. ***Proporcionar capacidad de enfriamiento global. Enviar el aire frio a las cargas informáticas.***

**ARQUITECTURAS DE ENFRIAMIENTO:**

- **Por SALA.** Perimetral, poco eficiente para grandes Potencias Térmicas (efectivo hasta 4 KW por rack).
- **Por HILERAS.** Permiten mayor previsibilidad, mayor densidad y eficacia.
- **Por RACKS.** Unidades de enfriamiento instaladas entre Racks (más costosas).
- **Por AUTOCONTENIDA.** Solución integrada dentro los shelter.

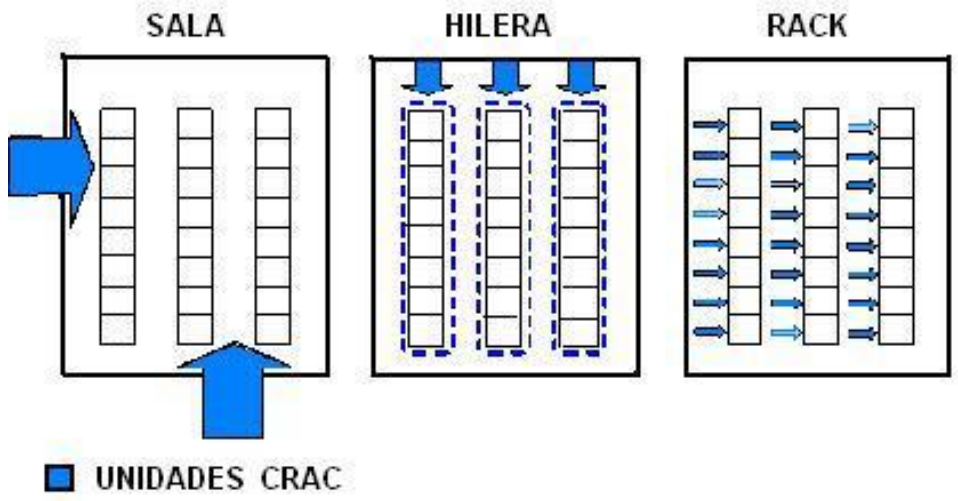



**Figura 40.** Arquitectura de Enfriamiento.

En la actualidad las unidades CRAC disponibles, por el flujo de aire que suministran, están clasificadas en:

***CRAC UPFLOW.*** Flujo de Aire que desprenden hacia arriba, no requieren pisos falsos.

***CRAC DOWNFLOW.*** Flujo de Aire que desprenden hacia abajo, necesitan de piso falso.

***CRAC IN-ROW.*** El flujo de aire se lo realiza de manera horizontal, directamente hacia la parte frontal de los Racks.

***CRAC AUTOCONTENIDA.*** El flujo de aire es a través de la circulación dentro un rack, solución cerrada.

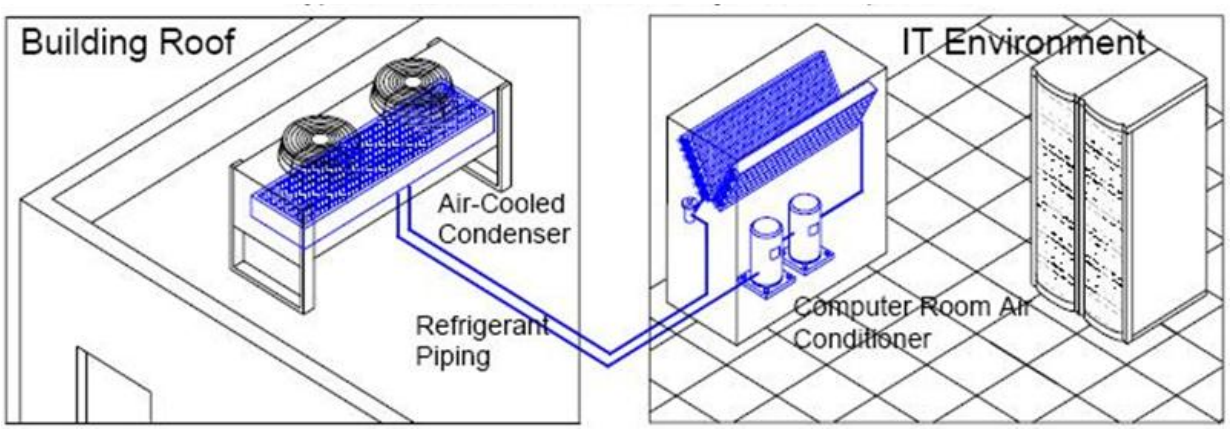



**Figura 41.** Descripción de un típico sistema de Refrigeración de una sala de equipos.

**Las Arquitecturas de Enfriamiento más ampliamente usadas son:**

**PASILLOS FRIOS.** Espacio donde se introduce el aire frio para las unidades informáticas

**PASILLOS CALIENTES.** Espacio donde fluye el aire caliente generado por las cargas informáticas.

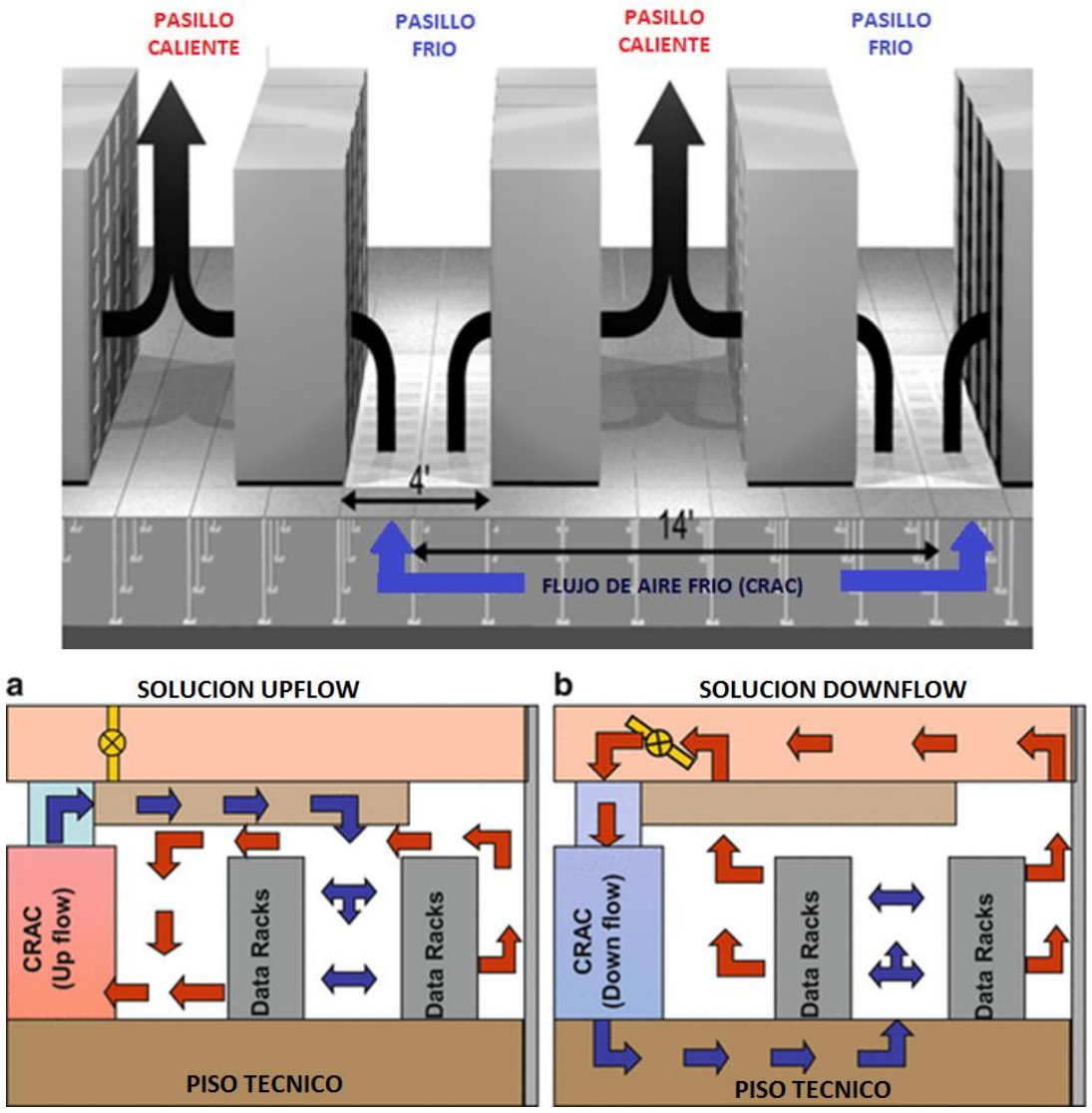



**Figura 42.** Enfriamiento más usado.

### 2.16.12. Carga Térmica en el Data Center.

La carga térmica informática se define como la cantidad de calor que se debe retirar del Centro de Datos, para mantener la temperatura deseada. En este espacio la carga térmica debe ser retirada por enfriamiento.

***La carga térmica representa la suma de las cargas térmicas generadas por aquellos equipos activos dentro el Data Center (equipos informáticos, iluminación, personal eventual y otros).***

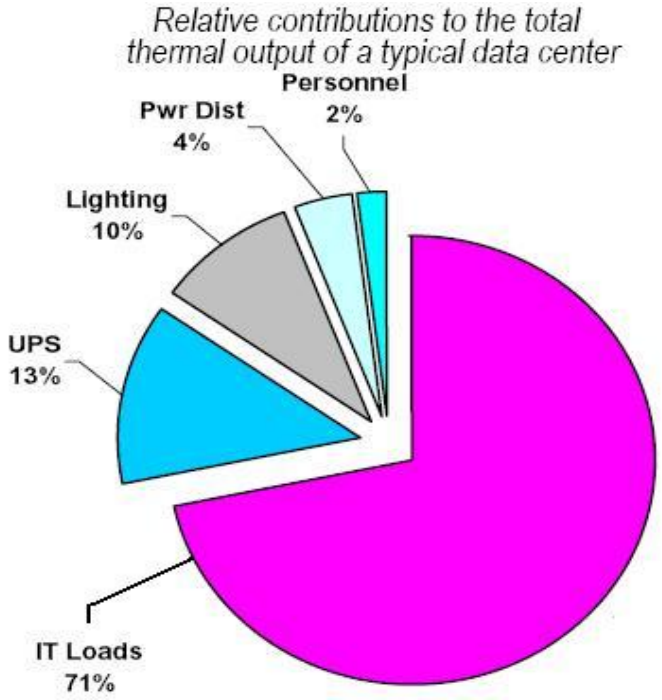



**Figura 43.** Entradas Térmicas.

**BTU/hr vs. Watts.**

Existe una relación entre la carga eléctrica y la carga térmica expresada en BTU/hr (BRITISH TERMAL UNIT /hora).

| Dado un valor en | Multiplicar por | Para obtener |
|---|---|---|
| BTU por hora | 0,293 | vatios |
| vatios | 3,41 | BTU por hora |
| toneladas | 3530 | vatios |
| vatios | 0,000283 | toneladas |

Es decir: **BTU/Hr = 3, 41 x Watts**

En la actualidad las unidades de refrigeración están estandarizadas en términos de potencia o Watts.

Una tendencia definitiva es que la Densidad de Energía en los Racks tiende a aumentar cada año:

- 1.500-watts por Rack para un despliegue de Servidores de la década de los 90.

- 4.000-watts por Rack para los típicos Servidores más actuales desarrollados en la década de los 2000.
- 5.000-8.000-watts por Rack para un despliegue de Servidores 1U.
- Por arriba de los 30.000-watts por Rack para Servidores Blade e Hyperconvergentes.

## 2.16.13. CALIDAD DE LA ENERGIA ELECTRICA Y PERTURBACIONES.

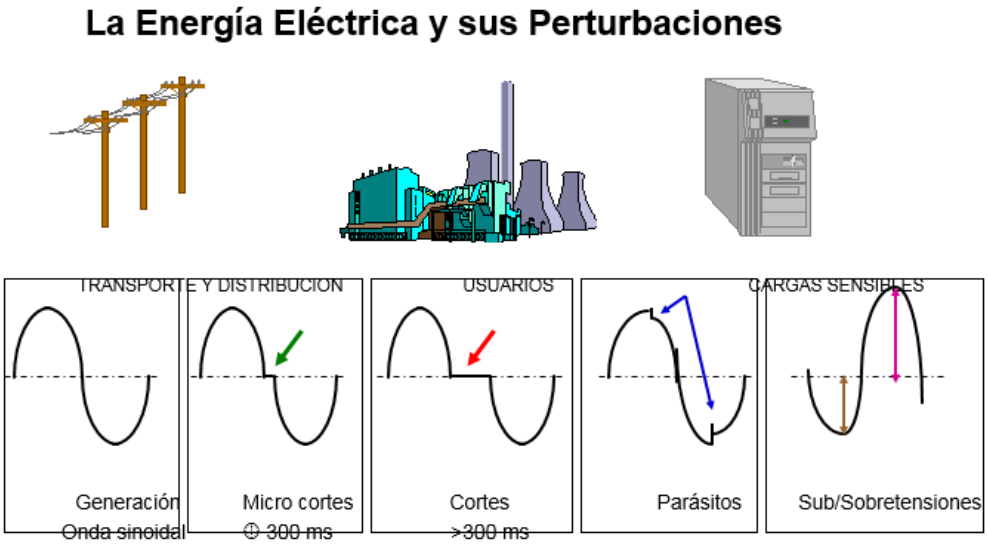



**Figura 44.** Energía eléctrica y sus perturbaciones.

**Sensibilidad de las Cargas Informáticas.**

Todas las cargas Informáticas son sensibles a diferentes fenómenos que se producen en el suministro de Energía Eléctrica.

La energía Eléctrica está expuesta a fenómenos como:

- Caídas y aumentos momentáneos de voltaje o reducciones no planificadas de tensión.
- Sensibles a la interrupción del suministro (cortes de energía).

La Energía Eléctrica en la realidad, son afectados por los varios de estos fenómenos descritos a continuación:

a) **TRANSITORIOS (IMPULSOS / PICOS).** Voltaje alto y angosto o impulso de corriente superpuesto en la onda de CA (Corriente Alterna).

   **CAUSAS:** Conmutación en la compañía eléctrica, Arco causado por una soldadora, Apertura o cierre de un contactor, Arranque de equipo industrial pesado, Rayos

   **EFECTOS:** Falla o daños al equipo, bloqueo del sistema, corrupción/pérdida de datos y fatiga de componentes que pueden causar fallas

   **SOLUCIONES:** Supresor TVSS, Transformadores de aislamiento*, estabilizador UPS.

b) **SOBREVOLTAJE (AUMENTOS MOMENTÁNEOS).** Aumento provisorio del voltaje RMS, puede durar varios ciclos.

   **CAUSAS:** Apagado de cargas grandes (motores, aire acondicionado, etc.), Compañía eléctrica dejando caer la carga.

   **EFECTOS:** Daño permanente a equipos y demás artículos eléctricos.

   **SOLUCIONES:** Regulador de voltaje/acondicionador de energía, Estabilizador UPS con regulación de voltaje.

c) **CAÍDA MOMENTÁNEA DE VOLTAJE.** Caída provisoria del voltaje RMS, puede durar varios ciclos.

   **CAUSAS:** Arranque de cargas grandes (motores, aire acondicionado, etc.), Conmutación en la compañía eléctrica.

   **EFECTOS:** Falla de sistemas, falla ocasional de los equipos, reducción en la eficiencia y vida útil de los equipos eléctricos, especialmente de motores.

   **SOLUCIONES:** Regulador de voltaje/acondicionador de energía, Estabilizadores UPS, Suministros de CC.

d) **BAJO VOLTAJE.** Caída provisoria del voltaje RMS, puede durar varias horas.

   **CAUSAS:** Alta demanda en la red eléctrica, Servicio situado al final de la red de distribución.

   **EFECTOS:** Falla de sistemas y falla ocasional de los equipos, reducción en la eficiencia y vida útil de los equipos eléctricos, especialmente de motores.

**SOLUCIONES:** Regulador de voltaje.

e) **APAGÓN (INTERRUPCIONES DEL SUMINISTRO).** Pérdida repentina de energía de AC.

**CAUSAS:** Apertura de fusibles o cortacircuitos, Tormentas, Accidentes de construcción.

**EFECTOS:** Parada de equipos, pérdida de datos, retrasos de producción, ciclos de arranque largos y problemas de seguridad (pérdida de iluminación, alarmas y sistema megafónico).

**SOLUCIONES:** Estabilizadores UPS.

f) **ARMÓNICOS.** Distorsión de la onda sinusoidal

**CAUSAS:** Suministros eléctricos conmutados, Cargas no lineales.

**EFECTOS:** Alta corriente, conductores neutros y transformadores sobrecalentados, distorsión de voltaje, cortocircuito, pérdida de capacidad del sistema.

**SOLUCIONES:** Estabilizador UPS en línea, Reactor de línea, Filtros activos, Transformadores ferrorresonantes.

g) **RUIDO ELÉCTRICO.** Amplitud baja, corriente baja, disturbios de alta frecuencia

**CAUSAS:** Suministros eléctricos conmutados, otras cargas, puesta a tierra inadecuada.

**EFECTOS:** Errores de software y bloqueo del sistema.

**SOLUCIONES:** Transformador de aislamiento, estabilizador UPS en línea, o supresor TVSS/filtro. Recablear la carga o trasladar la fuente de ruido.

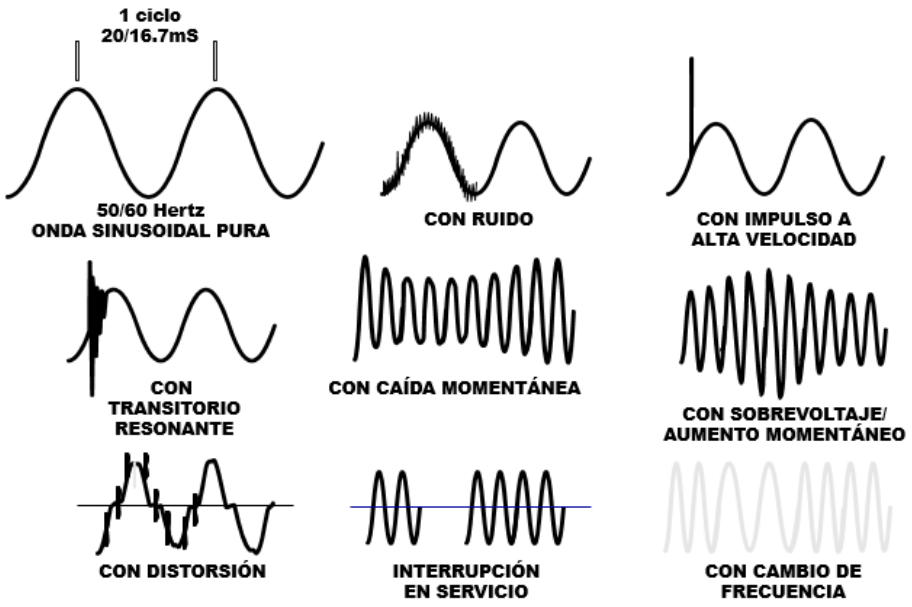



**Figura 45.** Perturbación en la Energía Eléctrica.

**Soluciones de Calidad de Energía:** Mantener la carga informática con una alimentación de energía eléctrica adecuada, libre de fenómenos de perturbación eléctrica requiere el empleo de tecnologías para este efecto, el que se adecua a la solución en un Centro de Datos es el denominado UPS.

**SUMINISTRO ELÉCTRICO ININTERRUMPIBLE (UPS).** Dispositivo que posee una batería para dar respaldo durante una interrupción del suministro.

**PROBLEMAS RESUELTOS POR EL UPS:** Interrupciones del suministro (limitado a la duración de la batería). Impulsos, ruido, sobrevoltajes, caídas momentáneas, reducciones planificadas y armónicos (dependiendo de la tecnología UPS).

**Sistema de Alimentación Ininterrumpida (SAI)** también denominado **UPS (*Uninterruptable Power System*).**

**Figura 46.** Sistema de Alimentación Ininterrumpida.

**¿Qué es un UPS?**

Un UPS es una fuente de suministro eléctrico que posee un sistema de batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica comercial.

**Componentes típicos de los equipos UPS.**

- **Rectificador:** rectifica la corriente alterna de entrada, proveyendo corriente continua para cargar la batería. Desde la batería se alimenta el inversor que nuevamente convierte la corriente en alterna. Cuando se descarga la batería, ésta se vuelve a cargar en un lapso de 8 a 10 horas, por este motivo la capacidad del cargador debe ser proporcional al tamaño de la batería necesaria.
- **Batería:** se encarga de suministrar la energía en caso de interrupción de la corriente eléctrica. Su capacidad, que se mide en Amperes Hora, depende de su autonomía (cantidad de tiempo que puede proveer energía sin alimentación).
- **Inversor:** transforma la corriente continua en corriente alterna, la cual alimenta los dispositivos conectados a la salida del UPS.
- **By-Pass** de dos posiciones, que permite conectar la salida directamente con la entrada del UPS (By Pass) o con la salida del inversor.

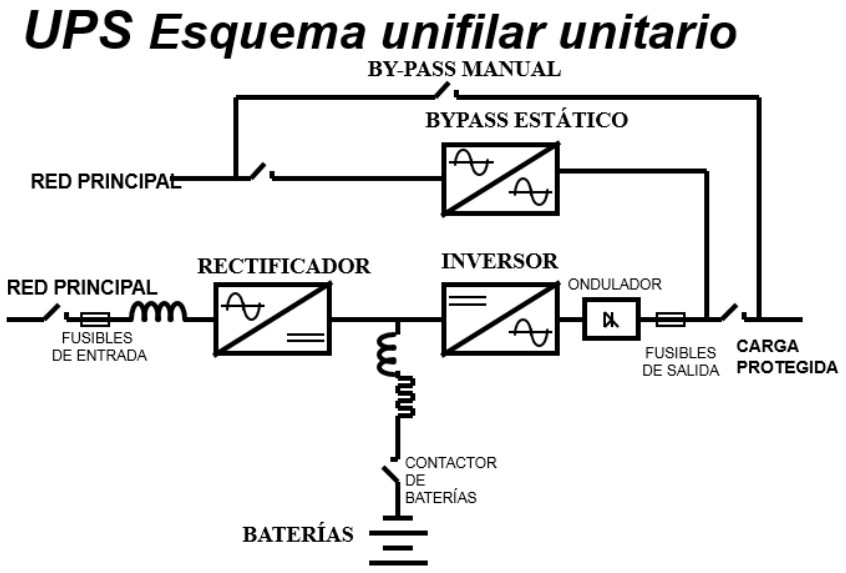



**Figura 47.** Esquema UPS.

**Tecnología de equipos UPS:**

- **STAND-BY PASIVO (OFF - LINE).** El UPS off-line es el más económico, ya que está integrado por pocos componentes, y es el ideal para la protección de computadoras en el hogar.

  Es "off-Line" porque el inversor o conmutador se encuentra fuera del camino principal de la corriente eléctrica (esta en Bypass). Además es "stand-by" porque el inversor se encuentra apagado en estado de espera de que sea requerido para encender. Los UPS off-line no pueden corregir ni estabilizar frecuencia de la corriente (como sí lo hacen los UPS on-line).

- **LINEA INTERACTIVO.** En este diseño, el inversor --que convierte la energía de la batería de corriente directa (CD) a corriente alterna (CA)-- siempre está conectado con la salida del UPS. Cuando la energía de corriente alterna en la entrada es normal el inversor funciona en reversa; es decir carga la batería.

  Una de las características más importantes de la Línea Interactiva (cuando se compara con la topología standby) es que integra un regulador para equilibrar la energía a 230 volts +/- 12% para mantener el voltaje que alimenta al equipo de informático lo más estable posible. Este equipo incluye supresor de picos y filtro.

- **DOBLE CONVERSIÓN (ON - LINE).** Tipo de UPS que evita los milisegundos sin energía al producirse un corte eléctrico, pues provee alimentación constante desde su batería y no de forma directa desde la alimentación de entrada.

  El INVERSOR se encuentra dentro de la línea principal de energía debido a que siempre se encuentra en funcionamiento.

  Generalmente el conmutador está conectado a la salida del inversor. La corriente pasa por el RECTIFICADOR continuamente, cargando la batería y alimentando el inversor el cual, a su vez, da la corriente alterna a la salida del UPS.

Finalmente concluimos que la solución ideal y adecuada para las cargas informáticas dentro un Centro de Datos son la denominadas UPS OnLine Doble Conversión, el cual permite corregir la mayor parte de perturbación en la energía suministrada al Centro de Datos.

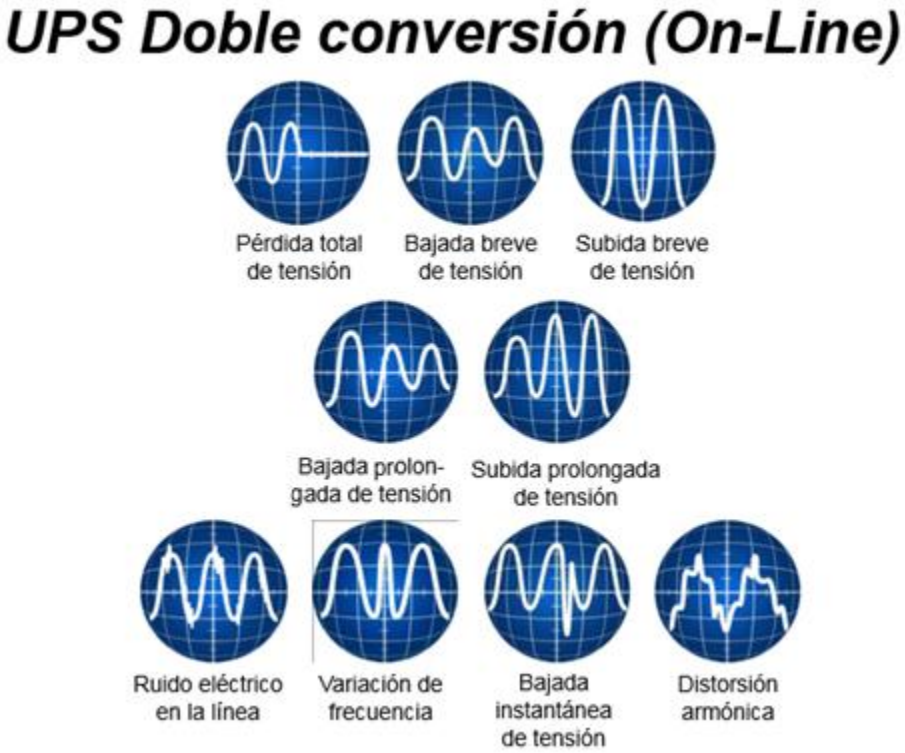



**Figura 48**. Doble conversión UPS.

**GRUPO GENERADOR DEL DATA CENTER.** En muchas situaciones los cortes de energía pueden ser prolongados, una solución complementaria al equipo UPS, es el equipo denominado Grupo Generador.

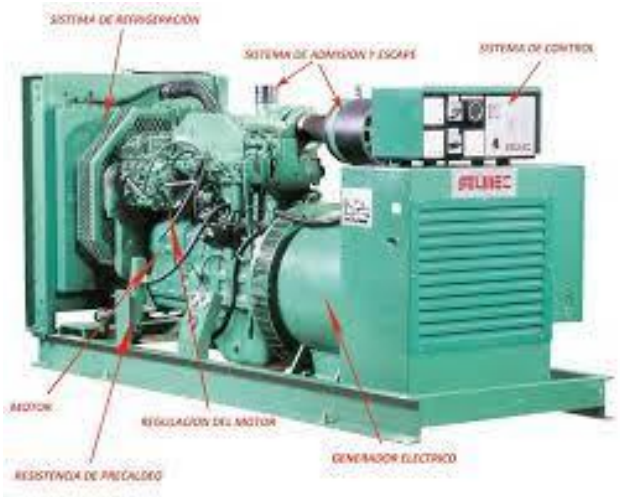



**Figura 49.** Generador del data center.

**El Grupo Electrógeno.**

**Componentes:**

**El motor**

- Es el elemento motriz del sistema
- Está concebido para mantener una velocidad constante, independiente de las exigencias de la carga
- Incorpora un sistema de regulación de velocidad
  - Mecánico ±5%
  - Electrónico ±1%
- **Los motores se clasifican según**
  - El combustible empleado (diésel, gasolina, etc.)
  - El sistema de refrigeración (aire, agua, etc.)
- **Otros elementos auxiliares del motor**
  - Batería de arranque
  - Depósito de combustible propio (habitual)
  - Depósito nodriza y bomba de trasiego (ocasional)
- **El alternador**

- Es un generador síncrono de CA
- Obtiene la energía mecánica del motor a través del volante de inercia para convertirla en energía eléctrica
- Del alternador se obtiene una tensión de forma senoidal, normalmente de 50Hz como el suministro público
- El alternador incorpora un regulador electrónico para mantener la tensión de salida constante para distintos niveles de carga.

**Aplicaciones y clasificación del grupo electrógeno.**

- **Según el servicio a ofrecer**
  - De trabajo continuo (fuente única de suministro)
    - Aplicaciones: Obras, campings, etc.
  - Para situaciones de emergencia (fuente alternativa a la principal)
    - Aplicaciones: Hoteles, hospitales, Centros de Datos, etc.
- **Según el tipo de carga a alimentar**
  - Cargas críticas: Generalmente en conjunción con los SAIs.
    - Aplicaciones: Informática, telecomunicaciones, etc.
  - Cargas esenciales: Plena justificación
    - Aplicaciones: Alumbrado de emergencia, ascensores, etc.
  - Cargas no esenciales: No se precisan

**Grupo Generador como solución complementaria al UPS (opcional).**

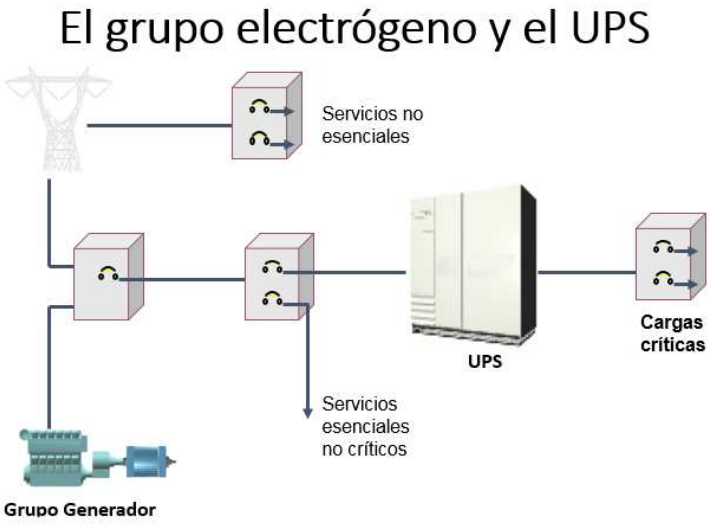



**Figura 50.** Grupo electrógeno.

**LA PROTECCION ANTE EVENTOS CONTRA RAYOS Y SOBRETENSIONES.**

Una buena práctica es contar con un **Tablero de Distribución Secundario** de manera exclusiva para el Centro de Datos. En el cual se debe tener los Termo magnéticos debidamente dimensionados para las corrientes de carga y además contar con sistemas de protección ante eventos tales como Descargas de rayos y sus efectos residuales, los cuales dañan a los equipos informáticos.

En tal sentido, los fabricantes ofertan el tipo de dispositivo capaz de derivar al sistema de puesta a Tierra (SPAT) estas altas corrientes de rayo y sus sobretensiones.

**DESCARGADORES CONTRA RAYO Y SOBRETENSIONES.**

**Figura 51.** Descargadores.

Un protector de sobretensión es un dispositivo diseñado para proteger dispositivos eléctricos de picos de tensión limitando el voltaje que se aplica a un dispositivo eléctrico bloqueando o enviando a tierra voltajes superiores a un umbral seguro.

Estos dispositivos de protección deberán ser instalados en el **Tablero de Distribución Secundario** instalado de manera exclusiva para el Centro de Datos.

**De acuerdo a estándares internacionales, podemos clasificar en los siguientes tipos:**


**Protectores Tipo 2 – 8/20µs – limitador de sobretensiones inducidas para corrientes medias.**

Son los más ampliamente utilizados porque ofrecen un nivel de protección compatible con la mayoría de equipos que se conectan a la red de alimentación.

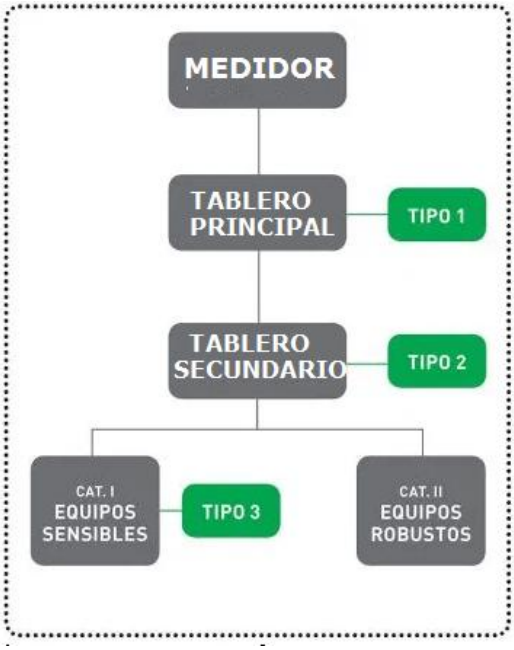
Su uso es adecuado como protección media cuando se tengan instalados protectores de Tipo 1 como primer escalón en viviendas, comercios, Edificios e industria en general.

Los protectores Tipo 2 deben instalarse siempre aguas abajo de los protectores Tipo 1 en todas las instalaciones con protección externa, en el tablero de baja tensión.

Su instalación en cabecera será suficiente cuando no exista protección externa. En los dos casos siguientes, se necesita un limitador de sobretensiones de protección secundaria: Si el nivel de protección (Up) es demasiado alto en relación a la tensión de resistencia a los impulsos (Uchoc) del equipo de la instalación.

Si el equipo sensible se encuentra demasiado alejado del limitador de sobretensiones entrante d = 30 m. Un limitador de sobretensiones de 8 kA debe instalarse en otro tablero subseccional y junto a cargas sensibles.

La Solución para los Centros de datos debe seguir recomendaciones internacionales, para una adecuada protección ante los eventos generados por los Rayos y sus Sobretensiones.




**Sistema de Puesta a Tierra (SPAT).**

En cualquier instalación domestica e industrial, la conexión de una toma a tierra es una de las reglas básicas a respetar para la seguridad de la energía eléctrica, ya sean del tipo residual o de tipo electroestática.

La ausencia de una toma de tierra podría suponer serios riesgos para la vida del personal de los centros de Datos y poner en riesgo las instalaciones eléctricas y sus bienes informáticos.

**Normas Fundamentales para SPAT:**

*NB 148009:2015 Norma Boliviana de Puesta a Tierra.*

*IEEE 81-2012 Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials of a Grounding System.*

*IEEE 142-2017 Recommended Practices for Grounding of Industrial and Commercial Power Systems.*

*ANSI/IEEE 1100-2005 Recommended Practice for Powering and Grounding Electronic Equipment.*

*IEEE 487.2-2013 Standard for Electrical Protection of Communication Trough Optical Fiber Systems.*

**¿Cuál es el valor adecuado de la Resistencia de Puesta a Tierra?**

No existe un valor de umbral único estándar de puesta a tierra que sea reconocido por las diferentes organizaciones.

Sin embargo, la NFPA y la IEEE han recomendado un valor de resistencia de puesta a tierra de 5 Ohmios o menos. Pero en todas ellas especifican que el valor para cargas sensibles debe ser siempre menor a 5 Ohm.

**Tendencia Actual: DATA CENTER CENTRALIZADO vs. DATA CENTER DISTRIBUIDO.**

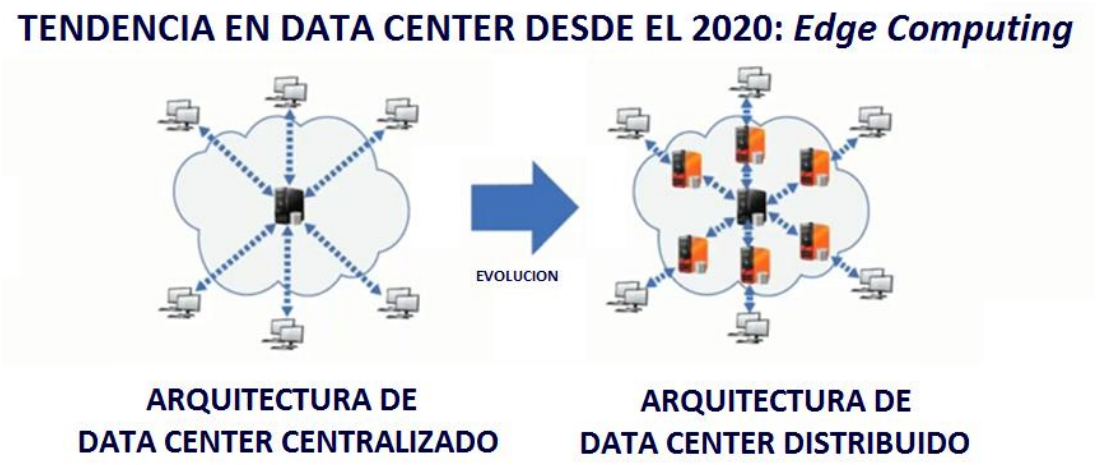



**Figura 52.** Tendencia en Data Center.

### 2.16.14. EDGE COMPUTING

¿Qué es la Edge Computing?

La Edge Computing (informática periférica) es una implementación de TI diseñada para ubicar las aplicaciones y los datos lo más cerca posible de los usuarios o las "cosas" que los necesitan.

**Edge Computing e informática en la nube**

La Edge Computing complementa la informática en la nube en un entorno informático híbrido. Mientras que la informática en la nube utiliza centros de datos centralizados, la Edge Computing emplea microcentros de datos distribuidos en la periferia de la red, donde los datos se utilizan más cerca del lugar donde se generan.

**¿Por qué es necesaria la Edge Computing?**

La Edge Computing es necesaria para compensar las deficiencias de las aplicaciones y los servicios basados en la nube en relación con el rendimiento y los requisitos reglamentarios. En pocas palabras, la informática en la nube no siempre puede satisfacer las demandas necesarias en términos del tiempo de respuesta que requieren las aplicaciones fundamentales. Asimismo, es posible que la informática en la nube tampoco pueda ofrecer el tipo de almacenamiento local

que exigen ciertas normas gubernamentales relacionadas con la ubicación de almacenamiento de los datos, a las que están sujetas algunas empresas.

Esto plantea problema, ya que la tendencia hacia que la digitalización para mejorar la eficiencia y el rendimiento empresarial está impulsando la demanda de aplicaciones que requieren un rendimiento máximo, especialmente las aplicaciones de la Internet de las cosas (IoT, del inglés Internet of Things). A menudo, las aplicaciones de IoT requieren un gran ancho de banda, una baja latencia y un rendimiento confiable mientras cumplen con normas y mandatos reglamentarios, lo que las convierte en las candidatas clásicas para la computación periférica.

### 2.16.15. EDGE DATA CENTER

**Actualización ANSI/TIA-942-B-1 para la infraestructura de los centros de datos tipo Edge.**

La Asociación de la Industria de las Telecomunicaciones (TIA) acaba de publicar un apéndice (enero 2022) de la norma ANSI/TIA-942-B de infraestructura de telecomunicaciones para centros de datos, la norma utilizada por los profesionales de las tecnologías de la información y las comunicaciones (TIC) en todo el mundo para diseñar, implementar y verificar la infraestructura de los centros de datos.

El apéndice de la norma define los requisitos iniciales de la infraestructura y las directrices de diseño para los centros de datos tipo Edge, también denominados "***microcentros***" de datos. Como señala el comité de normas, los centros de datos Edge suelen estar alojados en recintos prefabricados y pueden ser supervisados y controlados a distancia. Se consideran fundamentales para el éxito de las aplicaciones de próxima generación que exigirán una latencia ultrabaja, como los vehículos autónomos, la realidad aumentada y la telemedicina.

El nuevo apéndice, **ANSI/TIA-942-B-1 Telecommunications Infrastructure Standard for Edge Data Centers**, proporciona nuevos requisitos de infraestructura y directrices de diseño para los centros de datos Edge más pequeños que se despliegan en el borde de las redes, que está más cerca de los usuarios finales de las aplicaciones.

Además, el Comité de Estándares TR-42 de la TIA ha abierto oficialmente el estándar completo TIA-942-B para actualizaciones y revisiones de la industria por primera vez desde 2017.

La norma ANSI/TIA-942-B define los requisitos de diseño para la arquitectura de los centros de datos, el cableado, la ventilación, la refrigeración, los sistemas de alimentación, la seguridad, la supervisión/control, la resiliencia, la seguridad y los sistemas de gestión.

La TIA afirmó en un comunicado en 2022, "esta norma se someterá a su primera revisión completa y abierta, que se produce cada cinco años para garantizar la resistencia y la seguridad de estas instalaciones críticas a medida que evolucionan". Además de la actualización, se ha abierto el periodo de revisión de la TIA-942-B, que ofrece a las partes interesadas del sector, incluidos los usuarios de los centros de datos, propietarios, diseñadores, constructores, instaladores, auditores y otros, la oportunidad de ayudar a actualizar la norma para dar soporte a la próxima generación de centros de datos.


**Figura 53.** Micro Data Center.

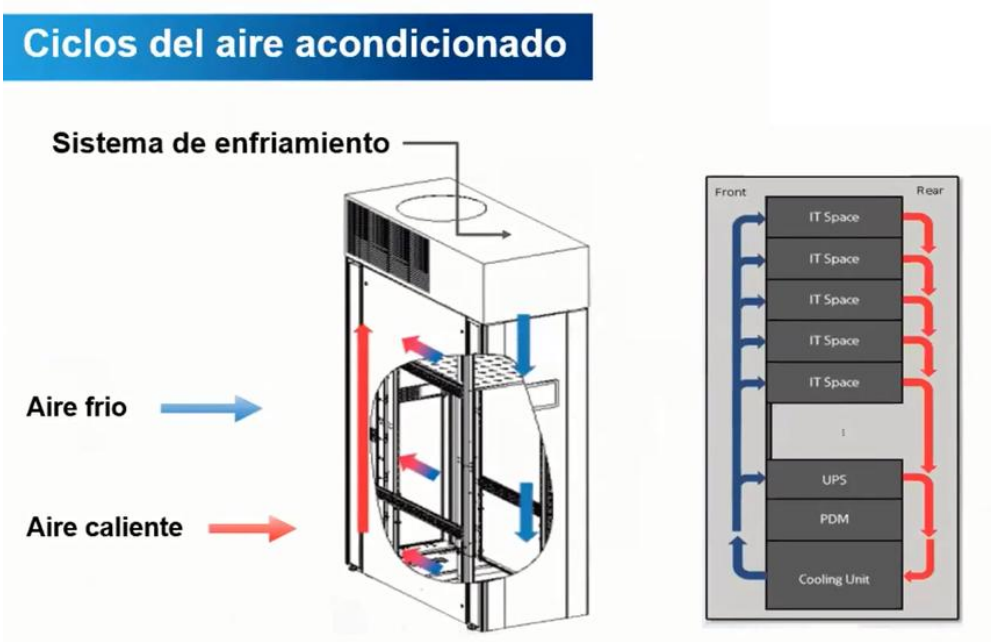
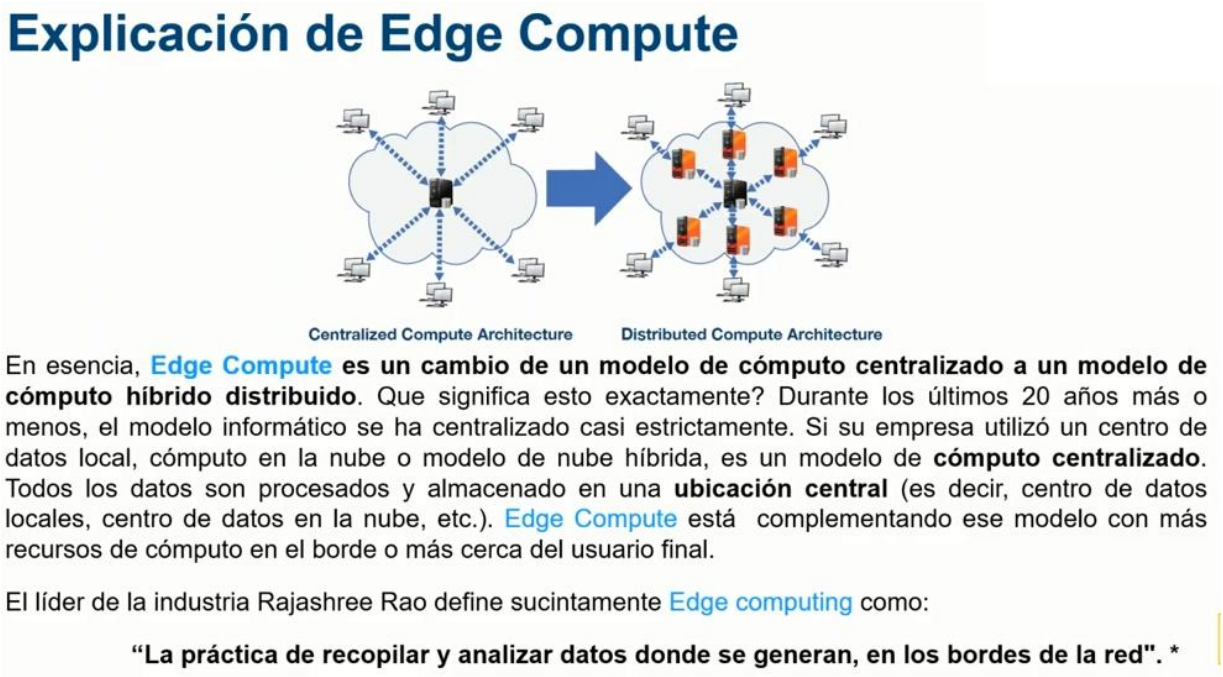



**Figura 54.** Ciclos de aire acondicionado.




## 2.16.16. DISEÑO LÓGICO DEL ENTERPRISE CAMPUS.

Una metodología completa del diseño de infraestructura IT y de red basado en las metodologías:

- BUTTON UP

- TOP DOWN
- Metodología PPDIOO (CISCO)

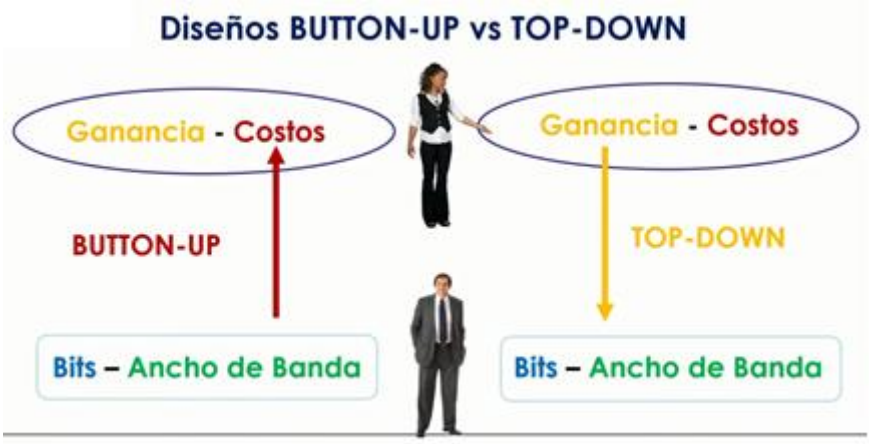
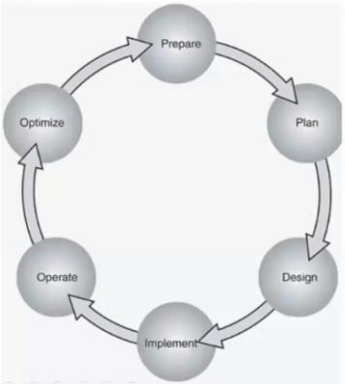



**Figura 55.** Metodologías de Diseño lógico.

## MODELO PPDIOO

Esta metodología fue desarrollada por la Compañía Cisco System en el año 2008, tiene como enfoque principal definir las actividades mínimas requeridas, por la tecnología y complejidad de la red, que permitan asesorar de la mejor forma posible a nuestros clientes, instalando y operando exitosamente las tecnologías. Así mismo logramos optimizar el desempeño a través del ciclo de vida de su red.


## Las fases de PPDIOO




- Preparar
  - Requerimientos de la organización.
  - Funcionalidad.
  - Plan económico de funcionamiento.
- Plan
  - Requerimientos de red
  - Acceso a sistemas existentes
  - Plan de implementación PM
- Diseño
  - Crear el diseño completo
  - Soporte
  - Disponibilidad
  - Seguridad
  - Performance
- Implementación
  - Plantillas
  - Objetivos
  - Cronogramas
- Operación
  - Mantenimientos
  - Detección de fallas
  - Performance Monitor
- Optimización
  - Administración y mantenimiento proactiva.

## 2.16.17. MODELO JERARQUICO DE 3 CAPAS (CISCO).

Modelo Desarrollado por CISCO, para tener un control de la red, tanto en la etapa de diseño, así como en la etapa de administración.

Para dar una solución estructurada y funcional a los sistemas de redes, Cisco cuenta con un diseño jerárquico para ellas. Un modelo que se distribuye en capas que están destinadas a diseñar una red confiable, organizada y estable.

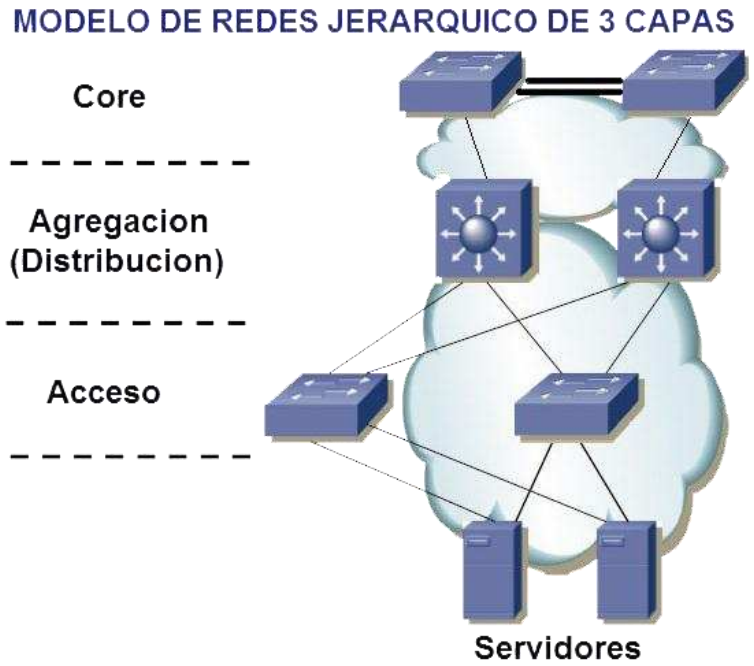



**Figura 56.** Modelo de redes jerárquico.

***Los principales beneficios del diseño jerárquico de redes cisco es que ayuda a diseñar, implementar y mantener una network jerárquica escalable, confiable y, ante todo, muy rentable.***

**Capa de núcleo o capa principal (CORE)**

La capa principal consta de los enrutadores más grandes, rápidos y caros con los números de modelos más altos.

Los routers de esta esta capa se emplean para fusionar redes separadas geográficamente y mueven información en la red lo más rápido posible. Al mismo tiempo, los conmutadores que operan en la capa central conmutan los paquetes lo más rápido posible.

**Capa de distribución**

La capa de distribución se encuentra entre la capa de acceso y la capa del núcleo de la red.

El propósito de esta capa es proporcionar una definición de límites mediante la implementación de listas de acceso y otros filtros. De este modo, la capa de distribución define las políticas de la red.

Al mismo tiempo, la capa de distribución garantiza que los paquetes se enruten correctamente entre las subredes y las VLAN de la empresa que está operando con ellas.

**Capa de acceso**

La capa de acceso es la capa que se sitúa en la parte inferior del diseño jerárquico de redes cisco.

Esta capa incluye interruptores de acceso que están conectados a los dispositivos finales (ordenadores, impresoras, servidores, etc.). De este modo, los conmutadores de la capa de acceso garantizan que los paquetes se entreguen a los dispositivos finales.

# 3. CAPÍTULO III. INGENIERÍA DEL PROYECTO

La Planificación y Diseño del Centro de Datos y la Infraestructura tecnológica para la facultad de Ingeniería U.M.S.A. en el edificio principal ubicado en la Plaza del Obelisco, ciudad de La Paz.

Tenemos 5 etapas principales para el diseño:

- Etapa de Relevamiento de Información del estado actual.
- Planificación y diseño de la Infraestructura Tecnológica del Edificio.
- Dimensionamiento de Infraestructura IT del Centro de Datos.
- Planificación y diseño de la Infraestructura Critica del Centro de Datos.
- Diseño lógico de la red Facultativa.

**Requerimientos Informáticos del Centro de Datos *IngeTIC*:**

En general se define una serie de requisitos que deben cumplir los recursos informáticos:

- Permitir el balanceo y optimización de cargas informáticas.
- Replicar máquinas virtuales en diferentes equipos.
- Contar con una medida de recuperación ante posibles desastres.
- En caso de fallas en uno de los servidores o en la red, el servicio no sea interrumpido.
- Migración de equipos virtuales de forma segura, sin interrumpir el servicio.
- Reducción de cantidad de equipos servidores físicos.
- Las aplicaciones para desplegar deben ser compatibles tanto con sistemas operativos Linux, así como Windows.
- Integración de Dominio basado en Active Directory a partir de Windows 2012.
- Integración con la SAN (Storage Area Network) corporativa.
- Compatibilidad con diferentes sistemas operativos.

## 3.1. RELEVAMIENTO DE INFORMACION.

**Edificio de Ingeniería U.M.S.A.**

Tomando en cuenta que el edificio de la Facultad de Ingeniería U.M.S.A. ubicada en la Plaza del Obelisco de la ciudad de La Paz, actualmente cuenta con una infraestructura de red Categoría 5 y 5e, además de contar con gabinetes de muro en cada IDF de planta.

El relevamiento es el proceso de recopilación sistemática de datos e información sobre los equipos de red existentes en el edificio de la Facultad de Ingeniería, estos datos se utilizarán para plantear mejoras o presentar nuevas propuestas.

Los puntos relevantes que justifican esta recopilación de información son:

- **Mantenimiento y gestión de la red:** El relevamiento de equipos de red en el edificio es necesario para conocer la infraestructura de la red y poder mantenerla adecuadamente. Esto implica conocer la ubicación, cantidad y estado de los equipos para realizar el mantenimiento preventivo y correctivo, y poder gestionar eficientemente los recursos de la red.
- **Seguridad de la red:** El relevamiento de equipos de red permite conocer la topología de la red y los puntos vulnerables que pueden ser atacados por posibles amenazas de seguridad. De esta forma, se pueden tomar medidas para proteger la red y los datos que se transmiten a través de ella.
- **Mejora del rendimiento:** Con el relevamiento de equipos de red se puede identificar cuellos de botella y otros problemas de rendimiento que pueden estar afectando la velocidad y estabilidad de la red. De esta forma, se pueden tomar medidas para mejorar el rendimiento y la calidad de la conexión.
- **Planificación de futuras expansiones:** Conocer la infraestructura de la red en el edificio es esencial para planificar futuras expansiones y mejoras en la red. Se puede identificar la capacidad de la red y de los equipos para soportar nuevos dispositivos y aplicaciones.

### 3.1.1. Existencias de dispositivos de networking en el edificio.

Relevamiento de equipos existentes actualmente por piso en el edificio de la Facultad de Ingeniería, en todos los casos se tiene gabinete de muro de altura de 16U.

También se tiene en cada IDF un Tablero de Distribución Eléctrica cuyas dimensiones son Tablero de: 60 cm Alto x 50 cm Ancho x 25 cm Profundidad.

| SITIO | EQUIPOS | DESCRIPCIÓN |
|---|---|---|
| **PLANTA BAJA** | 2 SWITCH CISCO 2960 | Switch de red de capa 2 de la serie Cisco Catalyst |
| **PISO 1** | CISCO 2960 | Switch de red de capa 2 de la serie Cisco Catalyst |
| **PISO 2** | CISCO 2950 | Switch de red de capa 2 de la serie Cisco Catalyst |
| **PISO 3** | CISCO 2960 | Switch de red de capa 2 de la serie Cisco Catalyst |
| **PISO 4** | CISCO 2950 | Switch de red de capa 2 de la serie Cisco Catalyst |
| **PISO 5** | CISCO 2950 | Switch de red de capa 2 de la serie Cisco Catalyst |
| **PISO 6** | DATACENTER IngeTIC | Centro de Datos de Ingeniería |
| **PISO 7** | CISCO 2960 | Switch de red de capa 2 de la serie Cisco Catalyst |

**Tabla 10.** Relevamiento de equipos de red existentes en el edificio.

### 3.1.2. Existencia de servidores y dispositivos de networking dentro el Centro de Datos IngeTIC.

Relevamiento de equipos instalados y en funcionamiento en el Data Center IngeTIC de la Facultad de Ingeniería en la actualidad**.**

| | EQUIPO (Marca y Modelo) | Cantidad | DESCRIPCIÓN |
|---|---|---|---|
| **RACK 1** | VoIP PBX CXR3000 by XORCOM | 4 | **Sistema telefónico** VoIP de 200 hasta 1500 usuarios |
| | DELL PowerConnect 5524 | 1 | **Switch** de 24 puertos 1000+2 SFP+10g |
| | DELL PowerEdge R720 | 1 | **Servidor** de alto rendimiento para rack de 2U y 2 sockets intel® Xeon® E5-2600 y hasta 24 DIMM. |
| | DELL PowerEdge R310 | 2 | **Servidor** 1000 GB Bastidor (1U) Intel® Xeon® secuencia 3000 2,4 GHz 4 GB DDR3-SDRAM 350 W |

| | | | |
|---|---|---|---|
| **RACK 2** | Edge Router infinity | 1 | **Router** INFINITY de 8 puertos SFP+ 10 G + 1 puerto RJ45 Gigabit, throughput 80 Gbps, 16 núcleos y 16 GB RAM , fuentes de alimentación modulares Hot-Swappable |
| | Mikrotik CSS326-24G-25+RM | 2 | *Cloud Smart **Switch** Administrable multicapa de 24 puertos Gigabit y 2 puertos SFP+ de 10Gbps. Rackeable 1ur 19". Sistema Operativo preinstalado SwOS.* |
| | Router Cloud Core CCR-1016-12G | 2 | Cloud Core **Router**, CPU 16 Núcleos, Throughput 17.8Mpps/12Gbps, 12 Puertos Gigabit Ethernet, 2 GB Memoria |
| | KVM-SWITCH 8-PORT CONSOLE | 1 | **Switch** KVM de montaje en rack de 8 puertos con cables de 6 pies - Conmutador KVM integrado con monitor LCD de 19" - Cajón KVM LCD 1U con todas las funciones - OSD KVM - Durable 50,000 MTBF - Soporte USB + VGA |
| | DELL PowerEdge R520 | 2 | **Servidor** Dell PowerEdge R520 - Xeon E5-2420 - 1.9GHz - 8GB - 2x1TB - Raid 1 - No OS |
| | Servidores tipo CPU | 3 | |
| **RACK 3** | Optical Connectors | 1 | |
| | Fiber Connect Panel | 1 | |
| | Fuente de Refrigeración 1U Fan Unit | 1 | 1U de 19 pulgadas Termostato Digital de la unidad de ventilador con 4 ventiladores para gabinetes y racks de servidores de red |
| | Switch CATALYST 3750 SERIES | 1 | **Switch** Cisco Catalyst 3750 48 10/100/1000T + 4 SFP Standard Multilayer |
| | Switch CATALYST 2960G SERIES | 3 | **Switch** Cisco Catalyst 2960G - 20 puertos 10/100/1000 |
| | Distribuidor PATCH PANEL AMP NETCONNECT | 1 | |
| | Mikrotik Router CCR-1016 | 1 | CORE **ROUTER** \| 12 PUERTOS GIGABIT<br>CPU 1.2 GHz \| 16 NUCLEOS \| RAM 2 GB \| 12 ETHERNET 10/100/1000 \| 1 MICRO USB TIPO AB \| LICENCIA 6 \| PUERTO SEIAL RS232 \| TIENE 2 RANURAS SODIMM VACIAS. |

| | | | |
|---|---|---|---|
| | Servidor HP ML350 | 1 | **SERVIDOR** HP PROLIANT ML350 XEON SILVER 4210R 1P 16 GB-R P408i-a 8 SFF 800W TORRE GEN 10 (204114) |
| | DELL PowerEdge 2850 | 1 | **Servidor** con panel LCD inteligente, ProLiant ML370 G4 de HP, trío de discos duros Seagate Ultra320 de 36 GB |
| | Fuente | 2 | |
| **GABINETE** | PATCH PANEL | 2 | |
| | Switch Cisco CATALYST EXPRESS 520 | 1 | **Switch** Cisco WS-CE520-8PC-K9 Catalyst Express 520-8PC PoE 8 10/100 PoE |
| | Switch CATALYST 2960G SERIES | 1 | |

**Tabla 11.** Relevamiento de equipos de red existentes en el data center.

### 3.1.3. Servidores en funcionamiento y sus aplicaciones.

Actualmente la Facultad de Ingeniería cuenta con varios servidores instalados y en funcionamiento (se detalla en la parte de relevamiento), estos servidores cumplen diversas funciones. Existen una cantidad de servidores físicos y también se cuenta con algunos servidores virtualizados como se detalla a continuación:

| | **Cantidad de Servidores** | **Funciones** | **Sistema Operativo** |
|---|---|---|---|
| **Servidores Físicos** | 8 Servidores | 1 Servidor para Sistemas Académicos | LINUX |
| | | 1 Servidor para Docentes | LINUX |
| | | 1 Servidor para Estudiantes | LINUX |
| | | 1 Servidor para servicios Web | LINUX |
| | | 2 Servidores para Bases de Datos | LINUX |
| | | 1 Servidor DNS | Windows Server |
| | | 1 Servidor de Respaldo | LINUX |

| | | | |
|---|---|---|---|
| **Servidores Virtualizados** | 4 Servidores | Portales web | LINUX |

**Tabla 12.** Servidores en funcionamiento en la Facultad de Ingeniería (2023).

Teniendo en cuenta todos los servidores y sus funciones en la actualidad se propondrá un diseño del Data Center que cubra todas estas funciones, servicios y aplicaciones, tomando en cuenta escalabilidad que puedan incrementar las capacidades actuales de los servicios y aplicaciones. Además, con el diseño se plantea virtualizar la totalidad de los servidores físicos actuales, reduciendo así la cantidad de equipos físicos optimizando el consumo de energía, así como minimizar el espacio físico para la granja de servidores. **ANEXO A** (relevamiento).

### 3.1.4. Consumo actual de energía eléctrica dentro el Data Center IngeTIC

| | | |
|---|---|---|
| **CONSUMO MEDIDO CON PINZA AMPERIMETRICA:** | 12 Amperios | 2760 watts |

### 3.1.5. Energía Eléctrica de tipo doméstico otorgado por DELAPAZ

| | |
|---|---|
| **ENERGIA DEL EDIFICIO** | Trifásica Delta 380 Vac |
| **ENERGIA DEL DATA CENTER** | Monofásica 220/230 Vac Fase-Fase (sin neutro) |

### 3.1.6. VLANs activos en la Facultad de Ingeniería (2023)

Actualmente la Facultad de Ingeniería cuenta con varias VLANs para diferentes áreas, los cuales se muestran en la siguiente tabla 4:

| VLAN ID | Nombre | Estado | Puertos |
|---|---|---|---|
| 1 | Default | Activo | Gi1/0/11 |
| 6 | Voz | Activo | |
| 10 | Servidores | Activo | |
| 15 | Servers2 | Activo | |

| | | | |
|---|---|---|---|
| 20 | ENTEL-PUBLICAS | Activo | |
| 24 | AREA-DESC | Activo | |
| 25 | Labos2 | Activo | |
| 28 | Labo-civil | Activo | |
| 30 | Lan-biblio | Activo | |
| 32 | Labo-ind | Activo | |
| 36 | Priv-UMSA | Activo | |
| 40 | Admin-ing | Activo | |
| 43 | Antenascisco | Activo | |
| 50 | SIU | Activo | |
| 66 | Antenasruckus | Activo | |
| 99 | Clienteswifi | Activo | |
| 110 | Admin | Activo | |
| 112 | Aut-ing | Activo | |
| 114 | Autoridades | Activo | |
| 116 | Labos1 | Activo | |
| 200 | Admin-axs | Activo | |
| 300 | Cámaras | Activo | |
| 1002 | Fddi-default | Act/unsup | |
| 1003 | Token-ring-default | Act/unsup | |
| 1004 | Fddinet-default | Act/unsup | |
| 1005 | Trnet-default | Act/unsup | |

**Tabla 13.** VLANs actualmente activos en la Facultad de Ingeniería.

### 3.1.7. Diagrama de la Infraestructura Tecnológica "actual" del Enterprise Network de la Facultad de Ingeniería – U.M.S.A.

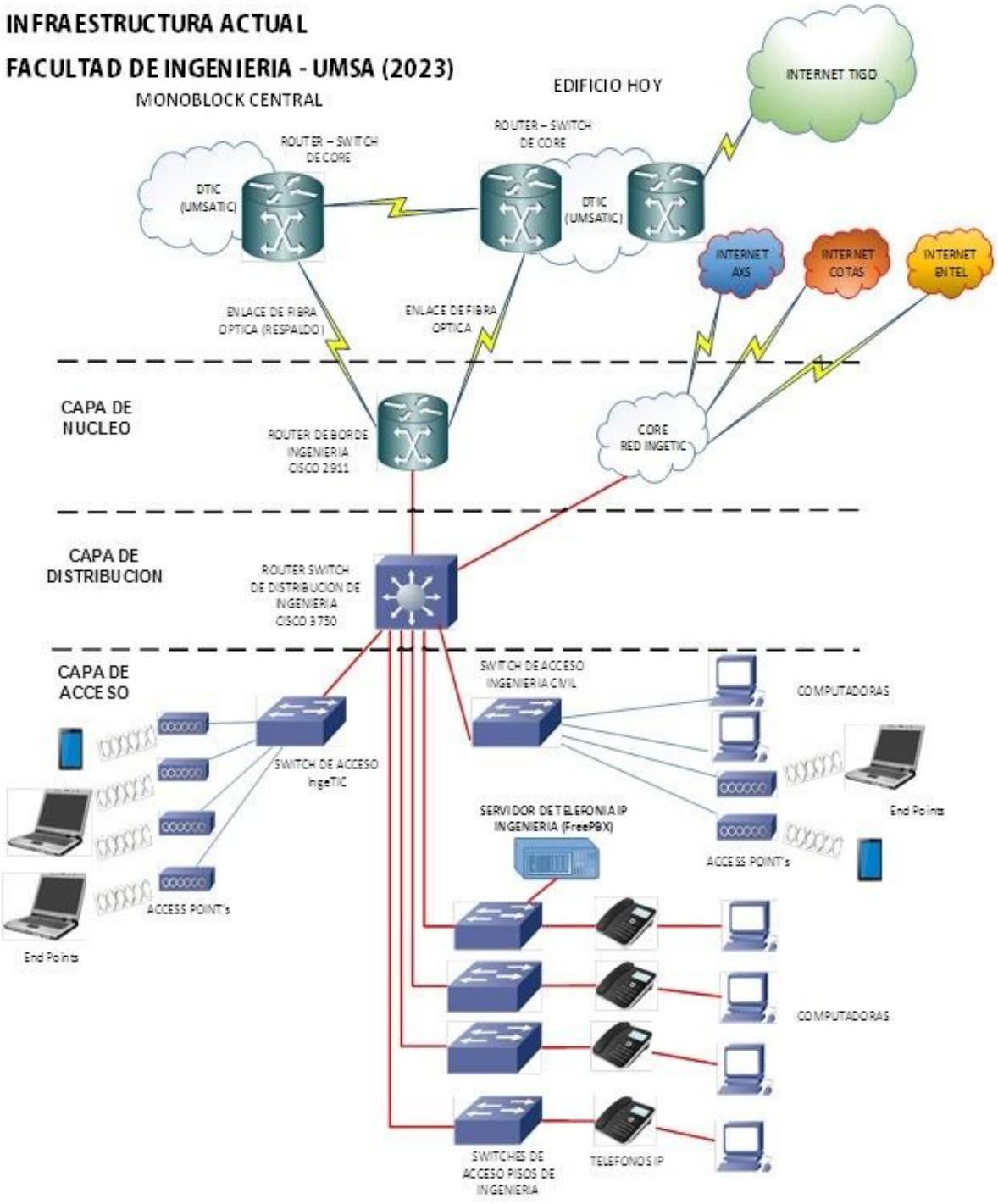



**Figura 57.** Diagrama de infraestructura tecnológica actual (*fuente: ingeTIC*).

## 3.2. PLANIFICACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DEL EDIFICIO DE LA FACULTAD DE INGENIERIA U.M.S.A (Plaza del Obelisco, ciudad de La Paz).

### 3.2.1. Antecedentes.

Se plantea implementar una solución de interconexión del backbone del *Building Distribution* con una solución por fibra óptica (Infraestructura Tecnología de Información y Comunicación), cobertura inalámbrica de acceso y un Centro de Procesamiento de Datos para la Facultad de Ingeniería U.M.S.A., La solución considera aspectos como:

- Relevamiento de información.
- Alta disponibilidad.
- Diseño modular.
- Escalabilidad
- Alto rendimiento
- Fácil de administrar
- Ancho de Banda.

### 3.2.2. Consideraciones y Requerimientos.

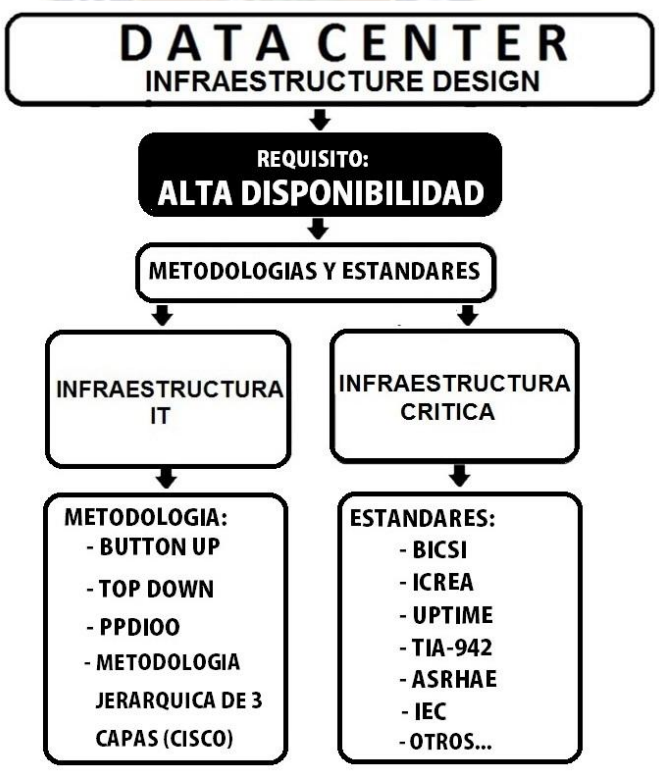
- Se prevé que el diseño sea escalable y esté preparado para brindar servicios simultáneos no solamente Telefonía IP y seguridad.
- Se considera prever una sala de monitoreo y de almacenamiento de información, para este efecto se considera en el proyecto el Centro de Procesamiento de Datos para albergar todos los servicios y aplicaciones Facultativos.
- Se considera el tipo de ambiente donde serán instaladas los IDF y el MDF que tengan ubicación protegida ante Polvo, lluvia, cambios de temperatura, cambios de Luz durante el día, poca iluminación en la noche, etc.) para brindar la mejor solución y tipo de implementación a realizar.
- También se prevé dispositivos tipo PoE para algunos dispositivos como Teléfonos IP y/o cámaras, con esta tecnología solo se realiza el tendido del cable de datos y no así el cable eléctrico.

### 3.2.3. Metodologías y estándares.

El proceso de Planificación y Diseño de una infraestructura de red o ***Enterprise Campus LAN*** y de un ***Centro de Procesamiento de Datos*** de tipo empresarial o ya sea de tipo campus

universitario, es un proceso en el cual intervienen múltiples disciplinas del campo de la ingeniería.

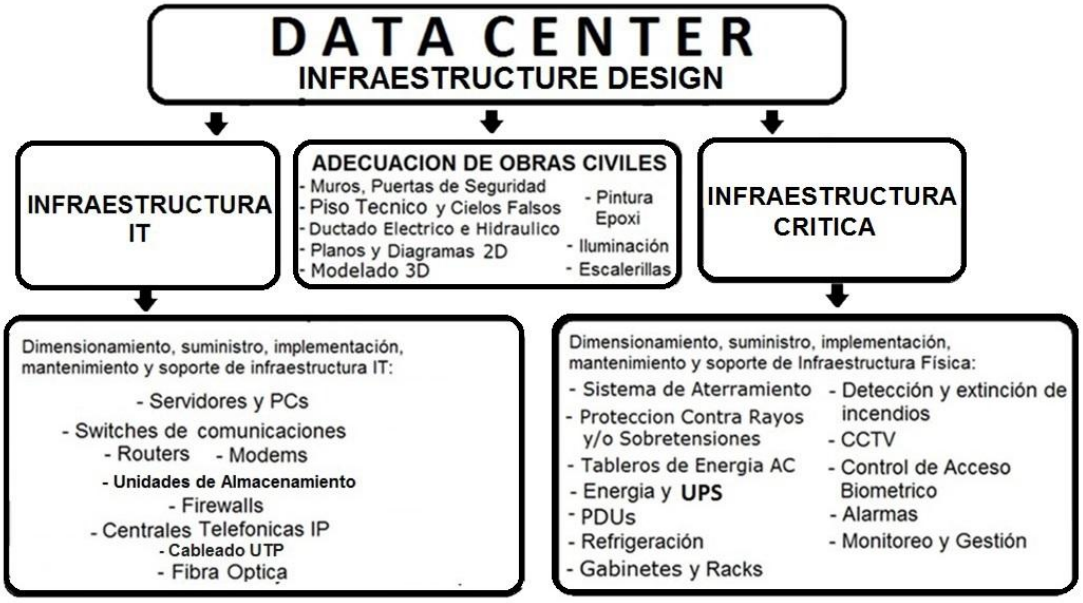
- La solución planteada involucra un diseño en base al modelo TOP/DOWN y posterior interconectividad en un entorno de Campus, además de contar con ayudas como la metodología PPDIOO.
- El modelo Jerárquico de CISCO de 3 capas, es un modelo eficiente para determinar los dispositivos de Networking para la solución de Infraestructura IT del Campus Network.
- Para la solución de Infraestructura Critica (*facilities*), los estándares del UpTime, BICSI, ICREA, TIA-942 y otros, son la base de la planificación y diseño.
- La tarea de planificación y diseño implica múltiples actividades, el uso de metodologías y estándares que permitan implementar la Infraestructura IT, así como la Infraestructura Critica de Data Center (*facilities*), las tareas pueden ser resumidas y mejor comprendidas mediante la siguiente figura *(fuente propia)*:



### 3.2.4. Diseño de la solución de infraestructura Tecnológica

- La Planificación y Diseño de la Infraestructura Tecnológica de tipo campus universitario, involucra 2 tareas (*fuente propia*):


La Planificación y Diseño del Centro de Datos para la facultad de Ingeniería U.M.S.A. consta de Infraestructura IT (equipo informático) así como Infraestructura Crítica (*facilities*):




***(fuente propia)***

**Planificar y Diseñar implica:**

- Dimensionamiento de la Infraestructura IT (equipo informático) del Centro de Datos.
- Diseño de la Infraestructura Critica del centro de Datos (*facilities*).

- En el proceso también será necesario realizar la adecuación mediante obras civiles.

## 3.3. DISEÑO DE LA SOLUCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DEL ENTERPRISE CAMPUS LAN (Edificio de la Facultad de Ingeniería)

### 3.3.1. Sistema de Cableado Estructurado del Campus LAN.

La solución se propone con un Cableado Estructurado acorde a las nuevas tecnologías y bajo los estándares internacionales. El edificio de la Facultad de Ingeniería cuenta con 8 plantas o pisos, adicionalmente también se cuenta con Mezzanine y 2 sótanos.

Por tanto, la solución será en Base a un Cableado Horizontal en plantas combinado con un Cableado Vertical entre IDFs de cada piso, presentando una ***Topología en Árbol o Estrella Extendida.***

Definimos los subsistemas de cableado horizontal y también el cableado vertical.

**Subsistema de cableado estructurado horizontal**

De acuerdo a los planos de construcción los cuales están formato CAD (Autocad), realizamos la planificación de los puntos de red, Proponiendo ***Cableado de Cobre pares trenzados UTP (Unshielded Twisted Pair) Categoría 6A,*** el cual permitirá a futuro implementar velocidades de hasta ***10 Giga bits por segundo.***

El cableado horizontal tiene como finalidad de instalación de los puntos de red en cada planta del edificio.

**Solución:**

**SUBSISTEMA DE CABLEADO HORIZONTAL**

| UBICACION | PUNTOS DE RED | LONGITUD TOTAL DE CABLE (metros) | DOCUMENTACION (PLANOS ADJUNTOS) |
|---|---|---|---|
| **SOTANO 2** | 0 | 0 | **NO APLICA** |
| **SOTANO 1** | 28 | 650 | **ANEXO C** |

| | | | |
|---|---|---|---|
| **PLANTA BAJA** | 24 | 1056 | **ANEXO D** |
| **MEZZANINE** | 52 | 2468 | **ANEXO E** |
| **PISO 1** | 32 | 868 | **ANEXO F** |
| **PISO 2** | 31 | 1095 | **ANEXO G** |
| **PISO 3** | 33 | 927 | **ANEXO H** |
| **PISO 4** | 31 | 940 | **ANEXO I** |
| **PISO 5** | 28 | 1066 | **ANEXO J** |
| **PISO 6** | 25 | 666 | **ANEXO K** |
| **PISO 7** | 33 | 825 | **ANEXO L** |
| **PISO 8** | 14 | 234 | **ANEXO M** |

| | |
|---|---|
| **CANTIDAD TOTAL DE CABLE:** | ***9983 metros*** |
| **TIPO DE CABLE:** | ***UTP Categoria 6A (10 Gbps)*** |
| **TOPOLOGIA (Cableado Horizontal):** | ***Estrella*** |

**Tabla 14.** Subsistema de cableado horizontal.

**Subsistema de cableado estructurado vertical (Backbone)**

El cableado vertical tiene como finalidad la interconexión del ***backbone***, en base a los planos de construcción los cuales están formato CAD (Autocad), planteamos la interconexión de los IDFS de piso a través de ***Cableado de Fibra Óptica del tipo OM3 de 24 hilos, capacidad de distancia de 10Gbps hasta 300 metros,*** utilizado para distancias menores a 200 mt y capacidad de transferencia de datos mayores a 10 Gbps (hasta 40 Gbps con distancia hasta 100 metros), el cual representa una buena solución con tecnologías de cableado.

**Solución:**

Considerando la altura máxima entre plantas de 3,5 metros y teniendo como dato las 8m plantas del edificio más 1 mezzanine y 2 sótanos, la altura máxima vertical del edifico es de 39 metros, considerando los 2 sótanos adicionales tendremos 46 metros en total, y por norma

según recomendación se debe adicionar una reserva de cable del 25% al 50%, lo cual nos da un valor máximo de 70 metros de cable de Fibra Óptica.

**Solución: SUBSISTEMA DE CABLEADO VERTICAL (BACKBONE)**

| LONGITUD TOTAL DE CABLE (mt) | TIPO DE CABLE | TOPOLOGIA | DOCUMENTACION (PLANOS ADJUNTOS) |
|---|---|---|---|
| **70 metros** | **Fibra Óptica Multimodo OM3 Cubierta de PVC de 24 hilos ANSI/TIA-598** | **Árbol-Estrella** | **ANEXO N** |

**Tabla 15.** Subsistema de cableado vertical.

**SOLUCION TOTAL DE CABLEADO ESTRUCTURADO**

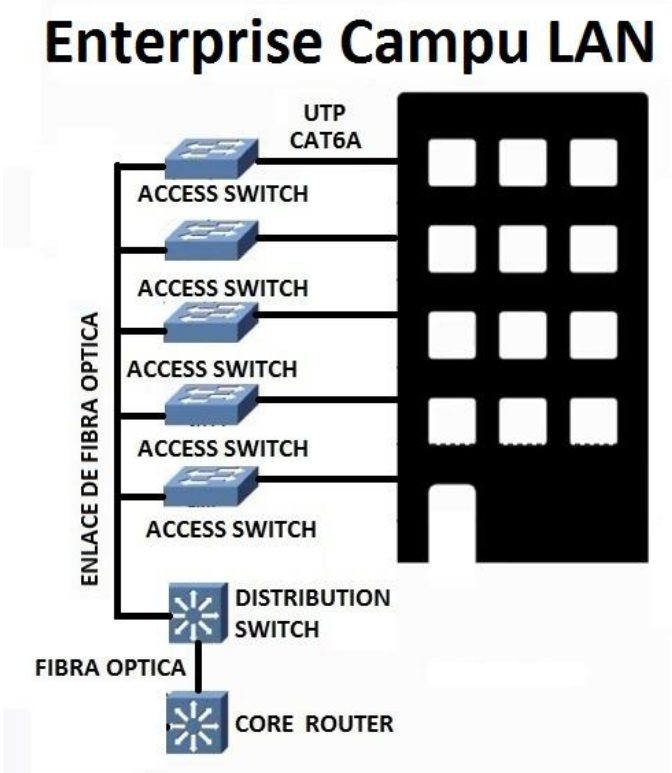
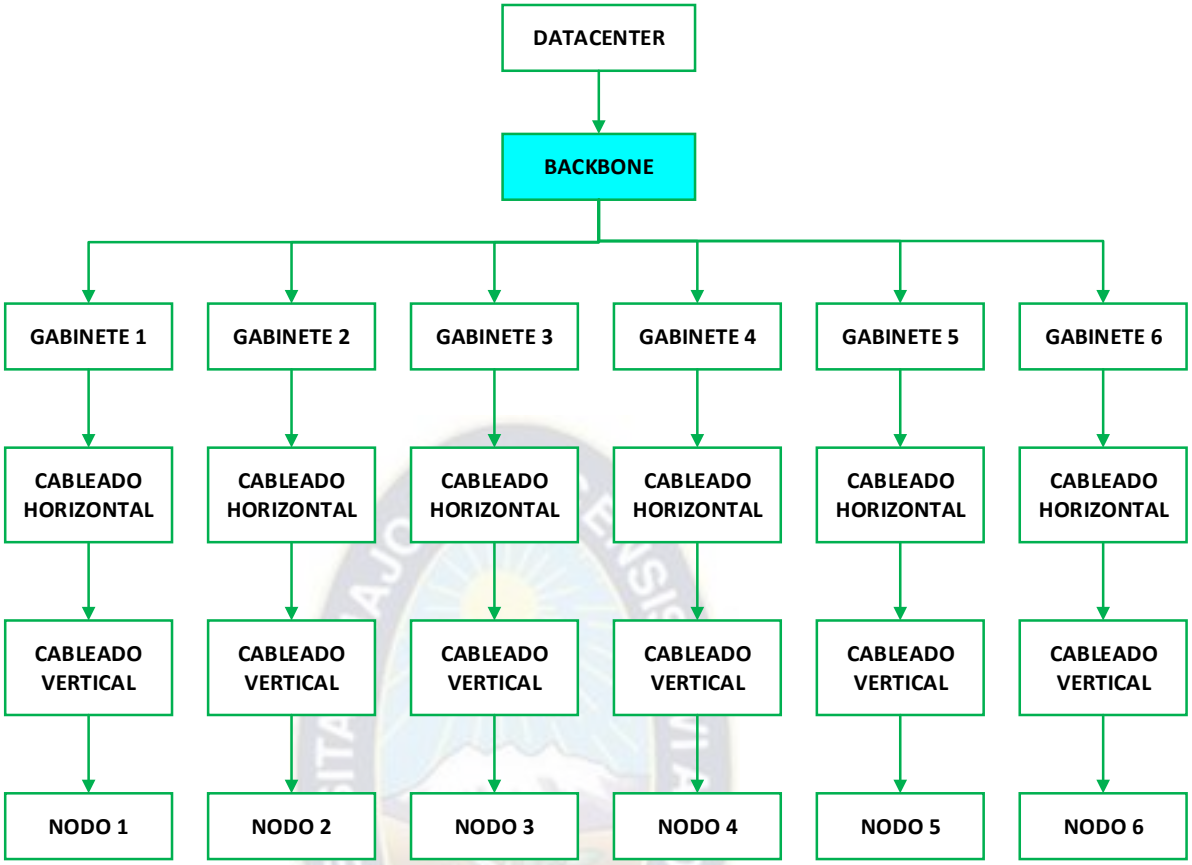



**Figura 58.** Solución de cableado estructurado *(fuente propia)*.

**Esquema general para el diseño del cableado estructurado:**


DATACENTER
BACKBONE
GABINETE 1
GABINETE 2
GABINETE 3
GABINETE 4
GABINETE 5
GABINETE 6
CABLEADO HORIZONTAL
CABLEADO HORIZONTAL
CABLEADO HORIZONTAL
CABLEADO HORIZONTAL
CABLEADO HORIZONTAL
CABLEADO HORIZONTAL
CABLEADO VERTICAL
CABLEADO VERTICAL
CABLEADO VERTICAL
CABLEADO VERTICAL
CABLEADO VERTICAL
CABLEADO VERTICAL
NODO 1
NODO 2
NODO 3
NODO 4
NODO 5
NODO 6

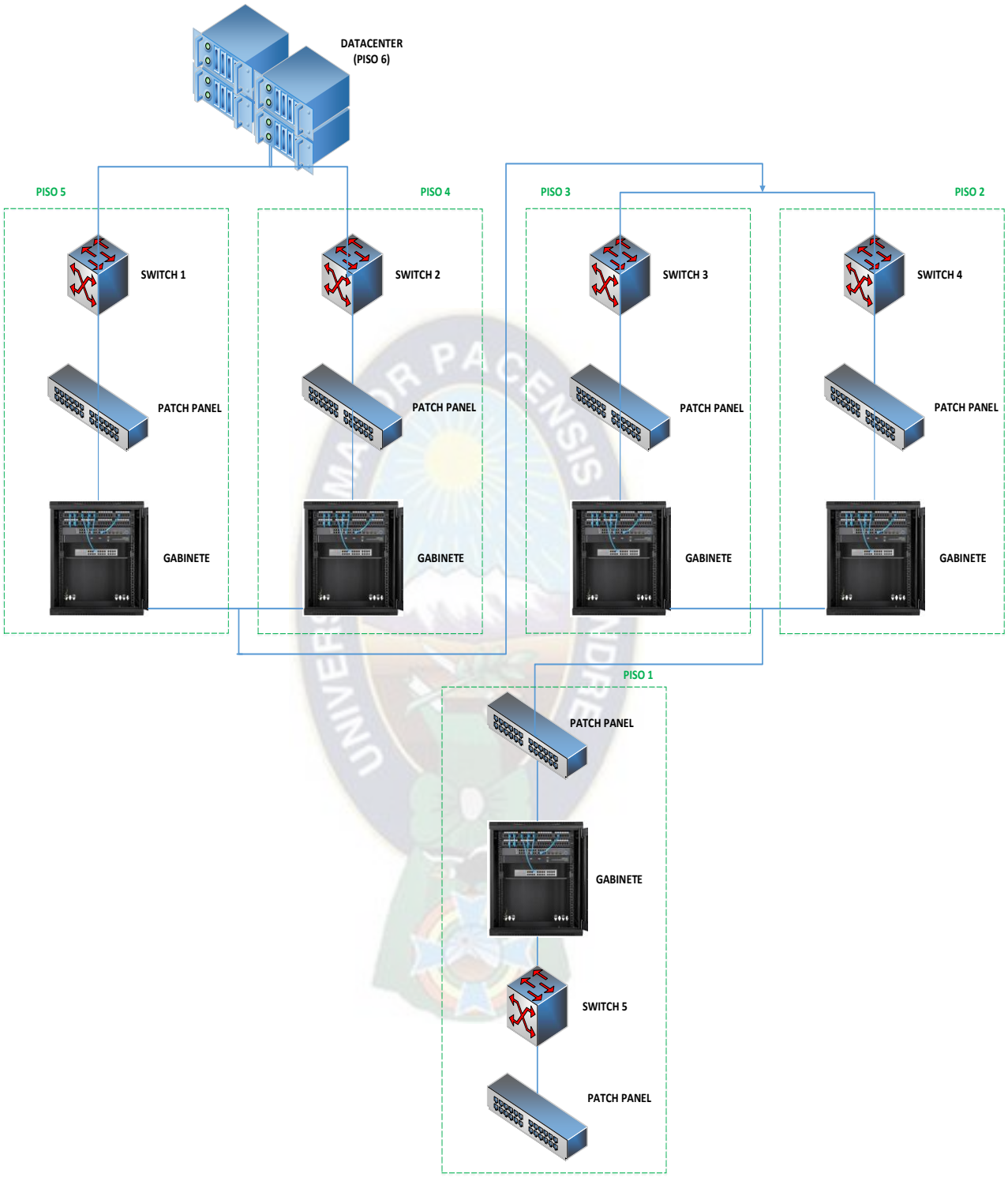



**Figura 59.** Esquema general de diseño de cableado estructurado.

### 3.3.2. Diseño Jerárquico del Enterprise Campus LAN

**Metodología:** Metodología de planificación y diseño utilizada: *TOP DOWN / PPDIOO.*

Solución de Infraestructura IT tomando en cuenta Alta disponibilidad (Minimizar fallos de enlaces y nodos, optimizar tiempos de recuperación y convergencia).

**Propuesta:** Diseño Lógico del *Enterprise Campus LAN*: En base al *Modelo Jerárquico de 3 capas de CISCO.*

El diseño en base al modelo jerárquico de 3 capas (CISCO), en el cual definimos las funcionalidades de cada capa y los dispositivos asociados a ella.

Los principales beneficios del diseño jerárquico de redes cisco es que ayuda a diseñar, implementar y mantener una network jerárquica escalable, confiable y, ante todo muy rentable.

**MODELO JERÁRQUICO DE 3 CAPAS DE CISCO.**

| JERARQUIA | FUNCIONALIDADES | DISPOSITIVO |
|---|---|---|
| **CAPA DE ACCESO** | -Acceso de usuarios finales y hosts<br>-Redundancia de rutas entre componentes de red (varios caminos).<br>-Redundancia de enlaces en capa de acceso<br>-Funcionamiento de VLANs | ***-Switch capa 2***<br>***-Switch PoE*** |
| **CAPA DE DISTRIBUCION** | -Políticas de Trafico y Balanceo IP<br>-QoS<br>-Ofrecer redundancia entre Core y Acceso<br>-Filtrado de Paquetes IP<br>-Routing entre VLANs<br>-Agregación de enlaces | ***-Switch Multicapa (capa 2 y 3)***<br><br>***-Router*** |
| **CAPA DE CORE** | -Alta disponibilidad de Trafico IP<br>-Redundancia del Trafico IP<br>-Transporte de Alta velocidad<br>-Tolerante a fallos<br>-QoS<br>- Tablas de rutas. | ***-Switch Multicapa (capa 2 y 3)***<br><br>***-Core Router*** |

**Tabla 16.** Modelo jerárquico de 3 capas CISCO.

**Diseño de la solución del Enterprise campus LAN, en base al modelo jerárquico de 3 capas:**

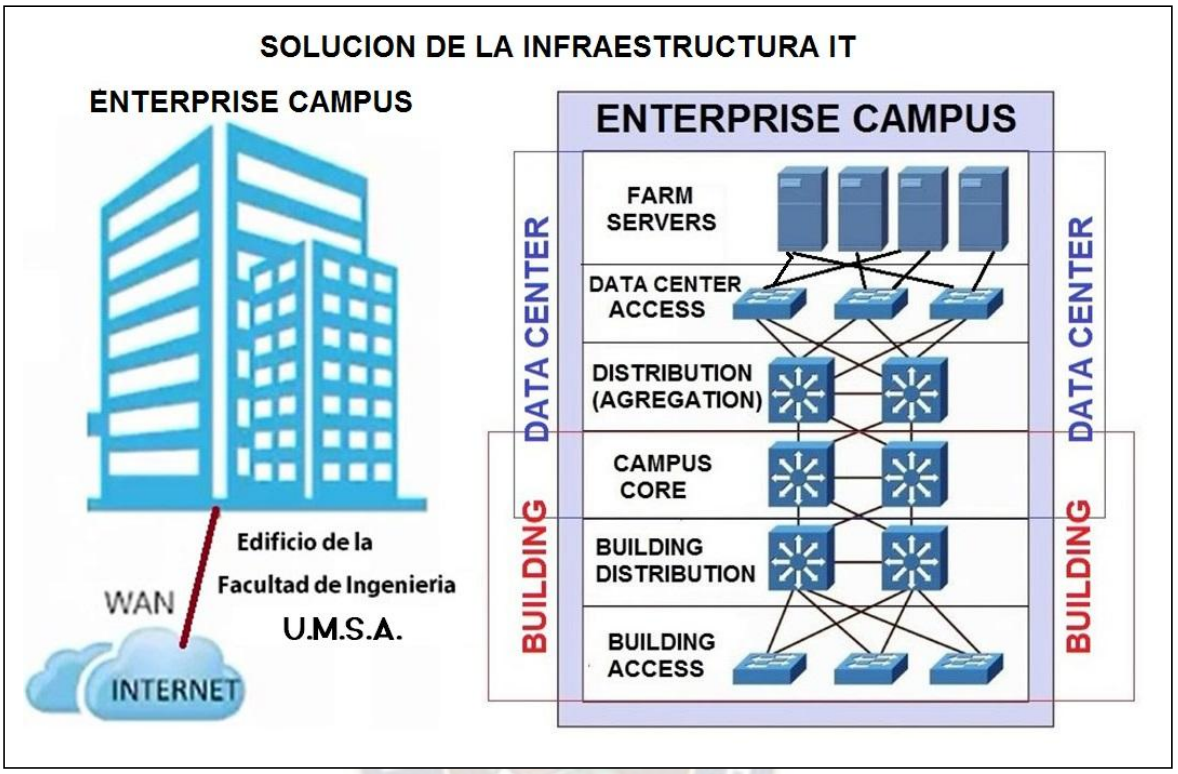



**Figura 60.** Solución de la infraestructura IT *(fuente propia)*.

**CAPA DE CORE***:* En la solución planteada, la Capa de Core (Campus Core) es común, tanto para el Edificio (Building LAN), así como también para el Centro de Datos.

**Solución:**

El equipamiento informático, para el modelo jerárquico de 3 capas, consta de:

Los Switches capa 2, que son suficientes en la *Building Access* y estos deben ser con alta densidad de Puertos, pues conectan a los usuarios finales dentro el edificio.

Se prevé el uso de Switches PoE en la capa de *Acceso Building* para interconectar dispositivos como Telefonos IP o cámaras.

En la Capa *Building Distribution* se prevé el uso de Switch Multicapa (capa 2 y 3) para efectos de redundancia y balanceo de carga.

En la Capa *Building Distribution* se prevé el uso de Switch Multicapa (capa 2 y 3) para intercomunicar las VLANs, dispositivos que soporten el protocolo 802.1Q.

La interconexión física se realiza mediante cableado estructurado horizontal en cada planta, mediante cable UTP Categoría 6A (10 Gbps).

El backbone (cableado Vertical) se la realizara mediante fibra óptica del tipo Multimodo OM3 (10 Gbps).

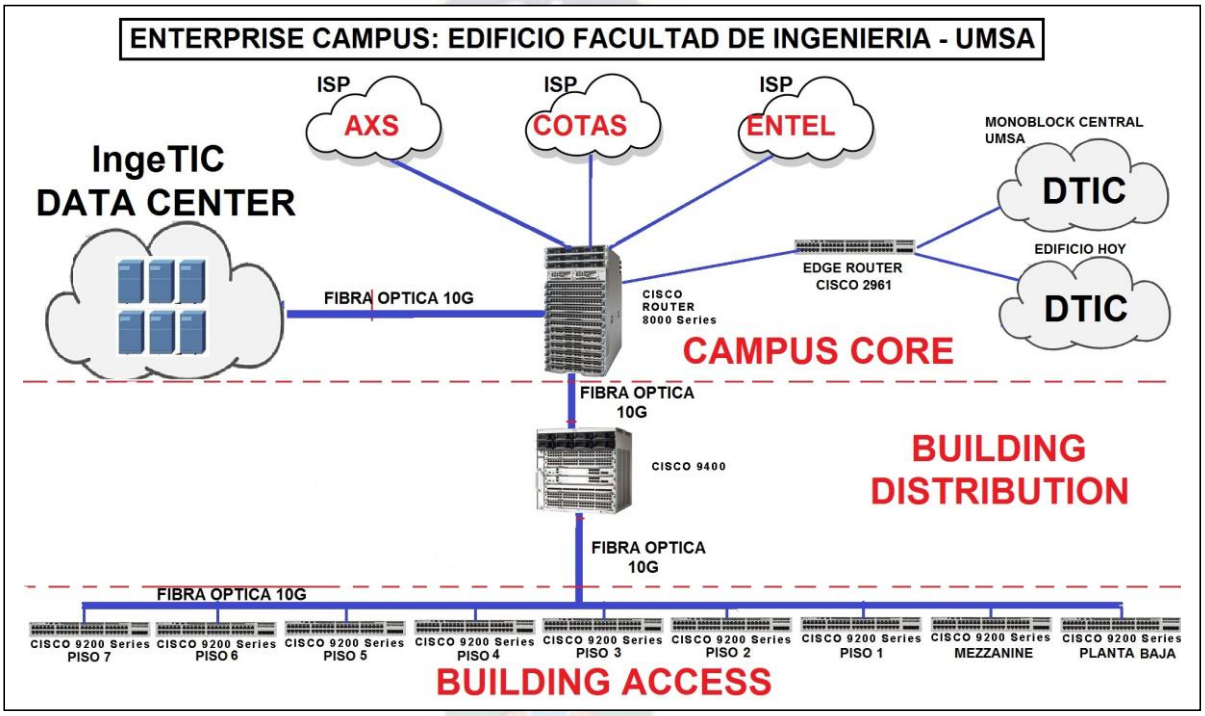



**Figura 61.** Enterprise Campus *(fuente propia)*.

**Soluciones de Infraestructura IT:**

**Dispositivos de Networking CISCO**

| SWITCH MULTICAPA (CAPA 2 Y CAPA 3) | ROUTERS |
|---|---|
| Cisco Catalyst 3650/3750/3850/9200/9300/9400 Series | Cisco Series MX<br>Cisco Series ISR<br>Cisco Series ASR |

**Soluciones de Infraestructura IT:**

| Core Routers (diferentes fabricantes y modelos) |
|---|
| Nokia (7950 Extensible Routing System [XRS] Series, 7750 series)<br>Ciena (Ciena 5430 15T)[4]<br>Cisco Systems (8000 series, CRS (former), Network Convergence System 6000)[5]<br>DriveNets DriveNets Network Operating System (DNOS)[6]<br>Extreme Networks (Black Diamond 20808)<br>Ericsson (SSR series)<br>Huawei Technologies Ltd. (NetEngine 9000 (NE9000), NetEngine 5000E, NetEngine 80E, NetEngine 80)<br>Juniper Networks (Juniper T-Series and PTX Series)<br>ZTE (ZXR10 Series: T8000, M6000) |

## 3.4. DISEÑO DE LA SOLUCIÓN DEL CENTRO DE DATOS (INGE TIC)

### 3.4.1. Diseño de la solución de Infraestructura IT (equipamiento informático).

***Consideraciones para Centro de Datos pequeño-medio***

Switches capa 2 y capa 3 serán conectados a los *Servidores* directamente.

También se prevé en el *Data Center Access* suficientes puertos en los Servidores. La capa de *Data Center Access* interconecta Servidores Clusterizados y será planteada de para cumplir con Alta Disponibilidad en caso necesario.

Para la capa *Data Center Access* los dispositivos deben ser de Alto Rendimiento y Baja Latencia. Los enlaces entre Servidores y los switches de la *Data Center Access* serán de tipo: FastEthernet, GigaEthernet, 10GigaEhternet. Alta Disponibilidad, se prevé un crecimiento con *Redundancia* en la *Data Center Access,* así como en el *Data Center Distribution (Aggregation)*.

La conectividad entre *Data Center Aggregation* y *Data Center* Access está planteada con topología en triangulo y el uso del Protocolo Spanning Tree para solucionar problemas de Bucles.

**Solución:** Diseño Lógico del *Data Center* en base al *Modelo Jerárquico de 3 capas de CISCO.*

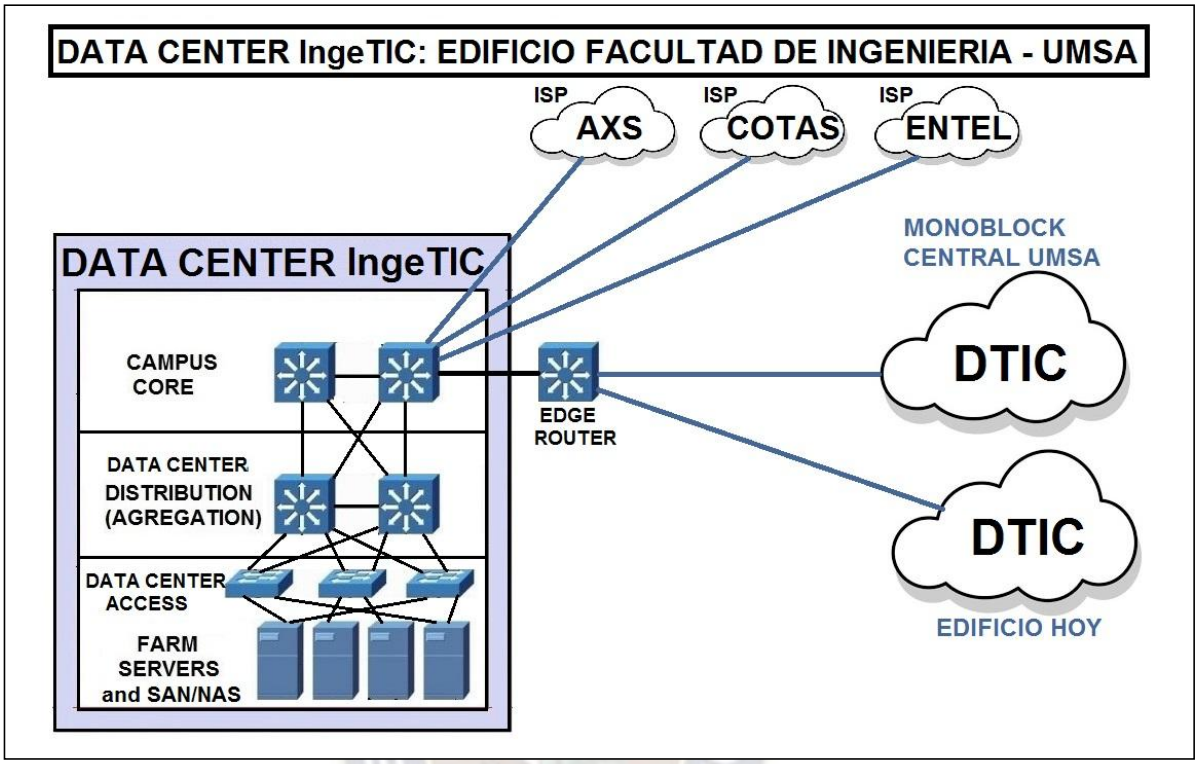



**Figura 62.** Data Center IngeTIC *(fuente propia)*.

**Infraestructura IT: Servidores.**

Un servidor utilizado en un centro de datos debe cumplir con ciertas características para garantizar la eficiencia, la confiabilidad y el rendimiento en el entorno del centro de datos. Algunas de las características importantes que un servidor para data center debería tener incluyen: *Escalabilidad, Eficiencia energética, Fiabilidad, Gestión remota, Escalabilidad horizontal, Capacidad de virtualización, Seguridad.*

La elección del servidor depende de los requisitos específicos del centro de datos y de la carga de trabajo que se espera ejecutar en el servidor.

**Soluciones de Infraestructura IT: Servidores (diferentes modelos y fabricantes).**

| SERVIDOR | CARACTERISTICAS |
|---|---|

| | |
|---|---|
| **HPE ProLiant DL380 Gen10** | Este es un servidor de gama alta de HPE que ofrece un alto rendimiento y una gran capacidad de escalabilidad. Es un servidor en rack de 2U que es capaz de alojar hasta 28 núcleos de procesamiento y 3 terabytes de RAM. |
| **Dell PowerEdge R740xD** | Este servidor de Dell es un servidor de nivel empresarial que ofrece una gran cantidad de potencia de procesamiento y capacidad de almacenamiento. Es un servidor en rack de 2U que puede alojar hasta dos procesadores escalables Intel Xeon de 2da generación y hasta 3 terabytes de RAM. Servidor con 2 procesadores Intel Xeon Escalable, cada procesador con hasta 28 núcleos por procesador. |
| **Lenovo ThinkSystem SR650** | Este es un servidor de gama alta de Lenovo que ofrece una gran cantidad de potencia de procesamiento y escalabilidad. Es un servidor en rack de 2U que puede alojar hasta dos procesadores escalables Intel Xeon de 2da generación y hasta 3 terabytes de RAM. |
| **Intel Xeon Gold 6152 2,1 Ghz** | Servidor con 2 procesadores, con un mínimo de 22 núcleos cada procesador. Almacenamiento de 16 Terabytes, expandible a 28 terabytes. |

**Tabla 17.** Modelos y fabricantes de Servidores.

**Dimensionamiento de los Servidores.**

- Según la etapa de relevamiento, se puede ver que actualmente se tiene 8 servidores Físicos y 4 servidores Virtualizados, que cubren los diferentes servicios (Servidor web, Base de Datos, DNS, Servidor ERP y otros).
- Por lo cual la solución cubrirá el requerimiento actual y prever un crecimiento de nuevos tipos de Servicios y Aplicaciones.

| | **DIMENSIONAMIENTO DEL SERVIDOR** |
|---|---|
| *Primera Regla:* | Un hecho demostrado por los fabricantes como primera regla sencilla y directa, es que 1 *"núcleo"* de procesador puede ser utilizado para implementar 2 a 3 máquinas virtuales como máximo. |
| *Segunda Regla* | Para cada núcleo de 1 procesador es necesario añadir entre 2 a 4 GB de RAM que utiliza el servidor. |

**Tabla 18.** Dimensionamiento del servidor.

**Solución:** Considerando las características mínimas para cubrir los requerimientos actuales, además de escalabilidad para nuevos servicios y aplicaciones. Nos determinan elegir el servidor: ***Servidor PowerEdge R470Xd*** con capacidad de alojar Máquinas Virtuales (Servidores virtuales).

| SERVIDOR: | CARACTERISTICAS: |
|---|---|
| DELL PowerEdge R470xd  | La solución cumple con:<br>-2 ranuras para procesador Intel Xeon Gold 6152 2,1 GHZ.<br>-1 Procesador con un mínimo de 28 núcleos por cada procesador.<br>-Memoria RAM de 48 GB, que cubran las 12 máquinas virtuales a implementarse, asignando 4 GB de RAM por cada máquina virtual.<br>-Memoria RAM expandible hasta 768 GB.<br>- Posee Controladora RAID.<br>-El equipo ***Servidor PowerEdge R470Xd*** es compatible con la solución de hiperconvergencia Vsan y con los equipos que actualmente cuenta el DTIC.<br>-Posee 4 interfaces para la conexión de red con hasta 10 Gpbs de velocidad por cada interfaz.<br>-Montaje en Rack (19 pulgadas).<br>-El servidor es modular y con capacidad de escalabilidad.<br>-Permite la integración de clusters, VCenter, VSphere, vSAN, VMWare y aplicaciones en entornos de virtualización. |

**Esquema de Funcionamiento del Servidor en el Data Center:**

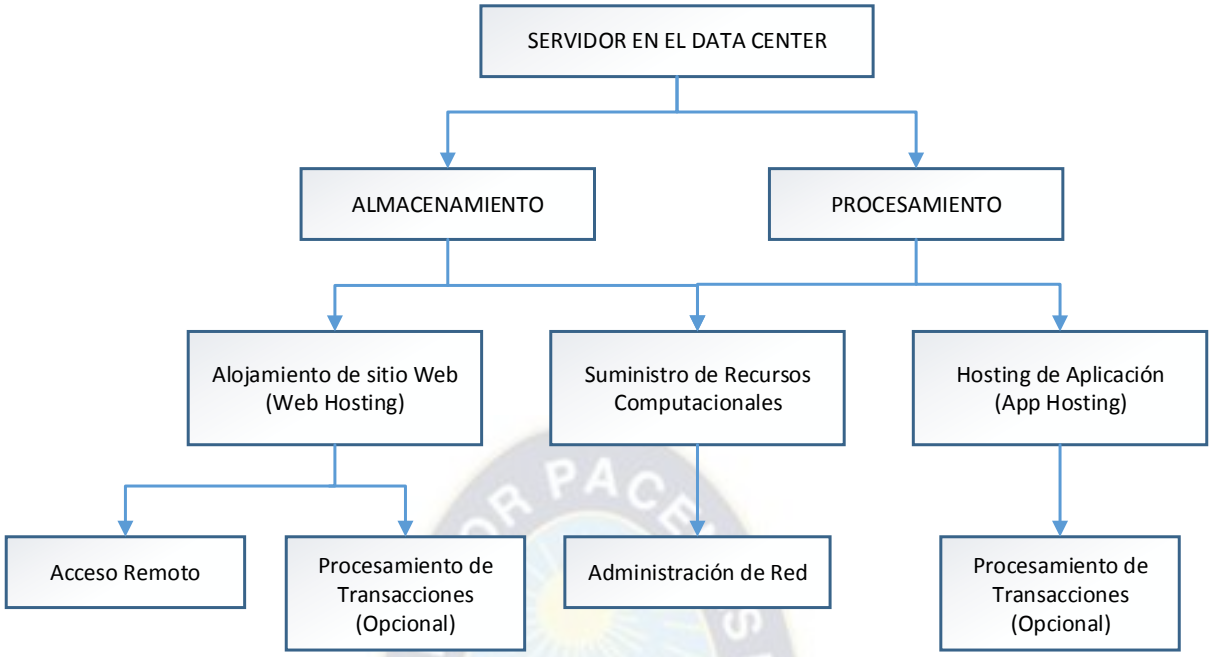



**Figura 63.** Esquema de Funcionamiento del Servidor en el Data Center.

**Infraestructura IT: Almacenamiento.**

Para el almacenamiento se contempla una solución de *Virtualización del Almacenamiento*, es decir consolidar varios dispositivos físicos de diferentes fabricantes reorganizándolos en agrupamientos virtuales, además de lógicos, o en unidades de almacenamiento, las cuales pueden ser:

*Virtualización basada en dispositivo:* En este tipo, la virtualización se realiza en arreglos de dispositivos de almacenamiento. Cada host dispone de un dispositivo virtual que se encuentra relacionado con una ubicación física dentro el arreglo (*array*) de dispositivos, como discos duros.

*Virtualización basada en red:* En este modelo, la virtualización se realiza en la misma red, en la cual se emplean switches inteligente u otros equipos de virtualización, en redes como SAN, NAS y DAS.

**Solución:** Tomando en cuenta las aplicaciones que se ejecutan en los servidores, tomamos como estimado el promedio de almacenamiento requerido para cada tipo de aplicación.

**ALMACENAMIENTO PROMEDIO DE LOS SERVICIOS**

| TIPO DE SERVICIO | ALMACENAMIENTO MAXIMO INTERNO EN PROMEDIO REQUERIDO |
|---|---|
| Servidor WEB | 500 GB/1 TB SAS/SATA ½ discos de 500 GB en RAID 1 |
| Servidor de Base de Datos | 2TB/4TB SAS/SATA 2/4 discos de 1 TB en RAID 1 |
| Servidor DHCP | 500 GB/1 TB SAS/SATA ½ discos de 500 GB en RAID 1 |
| Servidor Controlador de Dominio (Active Directory) bajo plataforma Windows. | 500 GB/1 TB SAS/SATA ½ discos de 500 GB en RAID 1 |
| Servidor de Correo | 500 GB/1 TB SAS/SATA ½ discos de 500 GB en RAID 1 |
| Servidor ERP | 2TB/4TB SAS/SATA 2/4 discos de 1 TB en RAID 1 |
| Servidor de VoIP | 500 GB/1 TB SAS/SATA ½ discos de 500 GB en RAID 1 |
| Servidor Antivirus | 500 GB/1 TB SAS/SATA ½ discos de 500 GB en RAID 1 |
| Servidor Firewall | 500 GB/1 TB SAS/SATA ½ discos de 500 GB en RAID 1 |

**Tabla 19.** Almacenamiento Promedio De Los Servicios.

Si se tiene en cuenta que los diferentes servicios prestados por las organizaciones, como varias aplicaciones, servicios WEB, ERP y Bases de Datos entre los principales. Así como el crecimiento de estos sistemas.

Estudios demuestran el promedio de recursos necesarios de almacenamiento en general. Para el presente proyecto, cuando se requiere para servicios web, bases de datos y otras aplicaciones, consideramos la siguiente solución con valores promedio para ciertos servicios y aplicaciones.

| SERVIDOR TIPO: | ALMACENAMIENTO |
|---|---|
| Bases de Datos | 2 TB |
| Aplicaciones ERP | 1 TB |
| Servidor WEB | 500 GB |
| Servidor de VoIP | 500 GB |
| Servidor Correo | 500 GB |
| Servidor DHCP | 500 GB |
| Antivirus/Firewall | 500 GB |
| **TOTAL:** | **5,5 TB** |

**Configuraciones en RAID del Almacenamiento (Matriz de Discos):**

**Solución:** Para prever alta disponibilidad en almacenamiento se prevé una matriz de discos, la cual utiliza múltiples discos duros o unidades de estado sólido (SSD) interconectados para formar una única unidad de almacenamiento. Estos discos se organizan en grupos que se llaman conjuntos de discos (también conocidos como RAID, por sus siglas en inglés Redundant Array of Independent Disks). Existen varios niveles RAID, cada uno con su propio nivel de redundancia y rendimiento.

**RAID 1:** los discos se duplican para proporcionar una mayor redundancia y protección de datos. Cada disco tiene una copia exacta de la información, por lo que, si uno de los discos falla, la información se puede recuperar del otro disco.

**Solución: Dispositivo SAN.**

Para el almacenamiento principal (máquinas virtuales, sobre todo) se plantea el equipo **SAN de HP modelo *MSA 2040 SFF Storage*** (para discos de 2,5 plg, permite hasta un máximo de 24 unidades, con capacidad máxima de 768 TB). Para utilizar el máximo rendimiento posible se plantea usar *Fiber Channel* de 8/16 Gbps que viene integrada en este modelo.

| ALMACENAMIENTO | CARACTERISITICAS REQUERIDAS |
|---|---|
|  | -Los modelos HP MSA Storage son soluciones de almacenamiento de alto rendimiento que combinan un rendimiento excelente con un alto nivel de fiabilidad, disponibilidad, flexibilidad y facilidad de administración.<br>- Los receptáculos MSA2040 admiten chasis de 2U de factor de forma grande (LFF de 12 discos) o factor de forma pequeña (SFF de 24 discos), con suministros de alimentación CA o bien CC. Los modelos HPMSA Storage incluyen MSA2040 SAN y controladores SAS MSA2040que se presentan a continuación.<br>- Los receptáculos MSA 2040 admiten tanto el almacenamiento lineal tradicional como el virtual, que utiliza tecnología de paginación de almacenamiento. Para el almacenamiento lineal, un grupo de discos con un nivel de RAID asignado se denomina disco virtual, vdisk o grupo de discos lineales. Para el almacenamiento virtual, un grupo de discos con un nivel de RAID asignado se |

| | |
|---|---|
| | denomina grupo de discos virtuales. En esta guía se utiliza el término disco virtual para hacer referencia específicamente al almacenamiento lineal y se utiliza el término grupo de discos en caso contrario.<br>- Los modelos MSA2040 SAN utilizan tecnología de controlador de red convergente, lo que permite seleccionar los protocolos de interfaz de host disponibles: canal de fibra (FC) o Internet iSCSI (iSCSI) admitidos por el sistema. Puede usar la CLI para configurar todos los puertos de host del módulo de controlador y usar uno de estos protocolos de interfaz de host: • FC de 16 GB • FC de 8 GB • FC de 4 GB • iSCSI de 10 GbE • iSCSI de 1 GbE |

**Esquema del Almacenamiento en Red:**

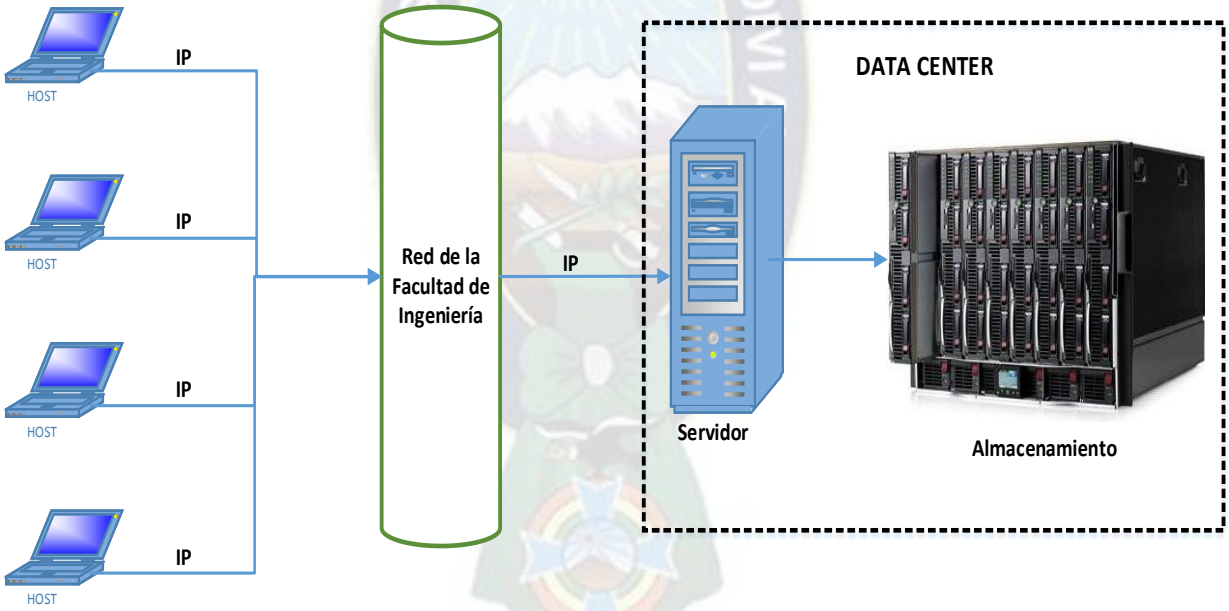



**Figura 64**. Esquema del Almacenamiento en Red.

### 3.4.2. Diseño de la solución de Infraestructura Critica (facilities)

Diseñar una Infraestructura Critica del Centro de Datos *(facilities)* es un proceso complejo que involucra varias especialidades, como ser la parte Arquitectónica, Eléctrica y Mecánica, así

como el conocimiento en Electrónica y Telecomunicaciones. Aquí los estándares y normas deben ser considerados al proponer la solución de la infraestructura critica del *Data Center*.

Los estándares existentes a nivel mundial, como BICSI, ICREA, UpTime, TIA-942, ASRHAE, IEC, solo nos dan los lineamientos para las mejores prácticas en la planificación y diseño de la solución de las *facilities.*

Para la solución adoptaremos el estándar americano **TIA-942 (Infraestructura para Centros de Datos)**. El cual plantea los *niveles de disponibilidad* clasificados en Rated 1, Rated 2, Rated 3, Rated 4.

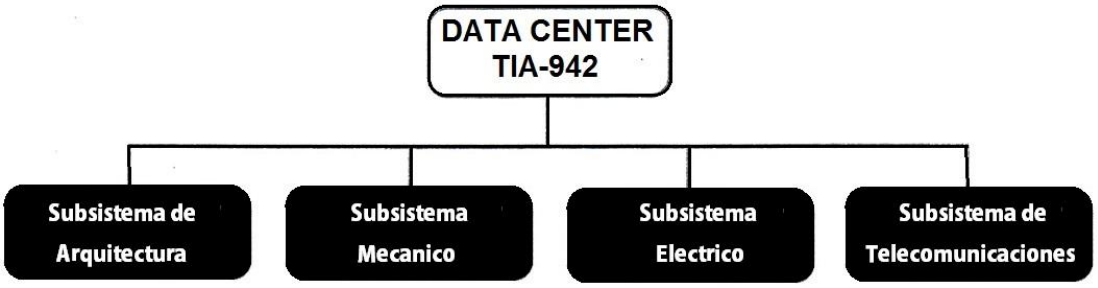
**DISPONIBILIDAD SEGUN TIA-942**

| PARAMETRO | RATED I | RATED II | RATED III | RATED IV |
|---|---|---|---|---|
| Tiempo máximo inactivo al año | 28,82 horas | 22,68 horas | 1,57 horas | 52,56 minutos |

Telecommunications Industry Association

**Diseño de Infraestructura para Centros de Datos TIA-942 según el nivel o Rated seleccionado**

El diseño se realiza bajo los 4 subsistemas según TIA-942, que plantea el dimensionamiento de la infraestructura critica, bajo el siguiente detalle:



La infraestructura critica (facilities) en base al nivel de disponibilidad seleccionado *(Rated)*, plantea el uso de equipos y sistemas en esquemas de redundancia.

| PARAMETRO | RATED I | RATED II | RATED III | RATED IV |
|---|---|---|---|---|
| Instalaciones de Piso Técnico | Opcional | Obligatorio | Obligatorio | Obligatorio |
| Cielo Falso | Básico | Características NFPA | Características NFPA | Características NFPA |
| Estudio geográfico del espacio físico | Irrelevante | Recomendado | Obligatorio | Obligatorio |
| Tiempo máximo inactivo al año | 28,82 horas | 22,68 horas | 1,57 horas | 52,56 minutos |
| UPS | Opcional | Obligatorio | Obligatorio y redundante | Obligatorio y redundante |
| Factor de Redundancia | N | N+1 | N+1 | 2(N+1) |
| Redundancia | Ninguna | Parcial: HVAC y Eléctrico | HVAC, Eléctrico, componentes de hardware | HVAC, Eléctrico, componentes de hardware, componentes tolerantes a fallas |
| Pinturas y acabados antifuegos | Mínimo | Recomendado Norma NPFA 75 | Obligarotio Norma NPFA 75 | Obligarotio Norma NPFA 75 |
| CCTV | No obligatorio | Obligatorio | Obligatorio | Obligatorio |
| Aire Acondicionado | Condiciones mínimas | Exigencias máximas | Exigencias máximas | Exigencias máximas |
| Apagado programado para mantenimiento | 2 eventos anualmente de 12 horas c/u | 2 eventos cada 2 años de 12 horas c/u | No requerido | No requerido |

**Tabla 20**. Tabla Parámetro – Rated.

Es necesario hacer notar que, al plantear una solución en el más alto nivel de disponibilidad (Rated 4), este tendrá impacto directo en el Costo Total de Inversión, pues plantea redundancia en varios de los elementos de la infraestructura Critica del Centro de Datos.

Nuestro planteamiento de solución será en base a RATED I.

| | **INFRAESTRUCTURA CRITICA DEL DATA CENTER (facilities)** |
|---|---|
| **SOLUCION:** | **-Standard TIA-942**<br>**Rated-1:** ***"Basic Site Infrastructure"***<br>***Se requiere un sistema estable, con una disponibilidad mínima adecuada, pero que su falla no presupone un daño importante en la organización.*** **En este nivel se tiene "algunos" elementos con redundancia.** |

Para esta solución según el estándar TIA-942, se debe tomar en cuenta el diseño en base a 4 los subsistemas.

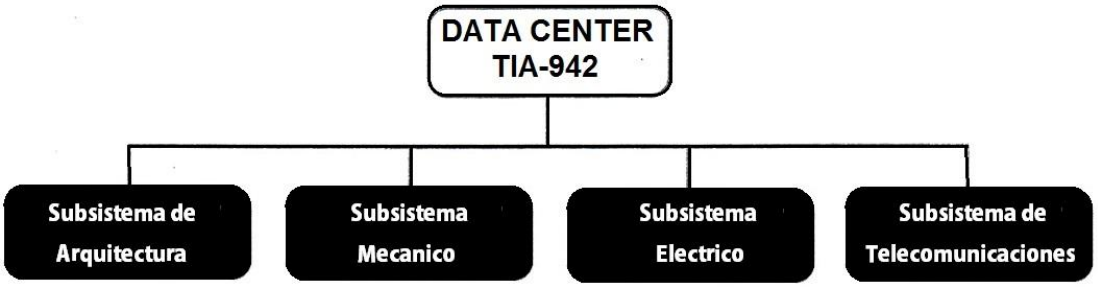
Por tanto, para RATED I, el diseño bajo los 4 subsistemas (Telecomunicaciones, Eléctrica, Mecánica, Arquitectónica), planteamos el dimensionamiento de la infraestructura critica, descrito en el siguiente cuadro:

**Infraestructura para Centros de Datos TIA-942 según Rated I**

| PARAMETRO | RATED I | DATA CENTER IngeTIC |
|---|---|---|
| **Instalación de piso técnico** | Opcional | ***No aplica**, la altura del ambiente destinado en el piso 6, de la facultad de ingeniería no permite implementar piso técnico. |
| **Cielo Falso** | Básico | Implementación de techo falso doméstico |
| **Estudio geográfico del sitio** | Irrelevante | ***No aplica** |
| **Tiempo máximo inactive al año** | 28,82 horas | En base a RATED I, permite mantenimientos programados, de manera que el servicio este inactivo en este lapso de mantenimiento. |
| **UPS** | Opcional | Aplica, se realiza el Cálculo de la Potencia del equipo UPS, con tiempo de autonomía estándar (8 a 10 min). |
| **Factor de Redundancia** | N | 1 solo equipo tanto en UPS, Aire Acondicionado |
| **Redundancia** | Ninguna | No se implementa equipos adicionales UPS ni tampoco Aire Acondicionado. |
| **Pinturas y acabados antifuegos** | Mínimo | Se plantea Pintura Epoxi antihumedad, Tanque de extinción con agente de extinción tipo polvo |
| **CCTV** | No obligatorio | Se plantea 2 cámaras de CCTV dentro el ambiente del Data Center |
| **Aire Acondicionado** | Condiciones Mínimas | Se plantea Aire Acondicionado de Precisión, cálculo de potencia frigorífica en base a consumo total de energía dentro el Data Center |
| **Apagado programado para mantenimiento** | 2 eventos anualmente de 12 horas cada uno | Mantenimiento programado 2 veces al año. |

**Tabla 21**. Centros de Datos TIA-942 según Rated I.

Según el esquema se tiene una serie de elementos en cuanto a infraestructura asociada a cada subsistema, se refiere a los elementos de hardware dentro los denominamos subsistemas.




### a). Subsistema de Telecomunicaciones

**Para crear un subsistema de telecomunicaciones en el Data Center, proponemos:**

| PASOS | TAREA | DESCRIPCIÓN |
|---|---|---|
| **1** | Análisis de necesidades | Identificamos las necesidades de la organización y los requisitos del data center. |
| **2** | Diseño de la arquitectura de red | Se crear un diseño de red que incluya la topología de red, la ubicación de los componentes de red y los requisitos de ancho de banda. |
| **3** | Selección de componentes de red | Seleccionamos los componentes de red adecuados para la arquitectura de red diseñada, teniendo en cuenta los requisitos de rendimiento, escalabilidad y seguridad. |
| **4** | Instalación de los componentes de red | Se instalar y configura los componentes de red en el centro de datos según las especificaciones del fabricante y las mejores prácticas de la industria. |
| **5** | Configuración de la red | Configurar los componentes de red para proporcionar conectividad y seguridad adecuadas, y para optimizar el rendimiento de la red. |
| **6** | Pruebas de red | Realizar pruebas de rendimiento, pruebas de seguridad y pruebas de tolerancia a fallos para asegurarse de que la red funcione correctamente y cumpla con los requisitos de la organización. |
| **7** | Implementación de servicios de red | Implementar servicios de red como VPN, balanceadores de carga, firewall, etc. según las necesidades de la organización. |
| **8** | Documentación de la red | Documentar la red y mantener un registro actualizado de la configuración de la red, las políticas de seguridad, etc. |
| **9** | Mantenimiento y actualización de la red | Realizar mantenimiento periódico y actualizaciones de la red para garantizar su rendimiento y seguridad a largo plazo. |

**Tabla 22.** Guía general para crear un subsistema de telecomunicaciones en el Data Center.

Cabe mencionar que esta tabla puede variar según se avance en la implementación, pero para diseño es una guía general.

### Cableado para la Entrada de Servicios al Centro de Datos

El cableado de la Entrada de Servicios al Centro de Datos (en inglés, Entry Service Point o ESP) se refiere al conjunto de cables y dispositivos que se utilizan para conectar los servicios de red y de comunicaciones externos al centro de datos.

Estos servicios pueden incluir conexiones de internet, líneas de telecomunicaciones, servicios de nube, servicios de seguridad y otros servicios de terceros. El cableado de la ESP es esencial para garantizar que los servicios de red externos lleguen de forma segura y eficiente al centro de datos, lo que permite que los servidores y los dispositivos de red internos se conecten a ellos.

El orden y las conexiones se visualizan en el siguiente diagrama:

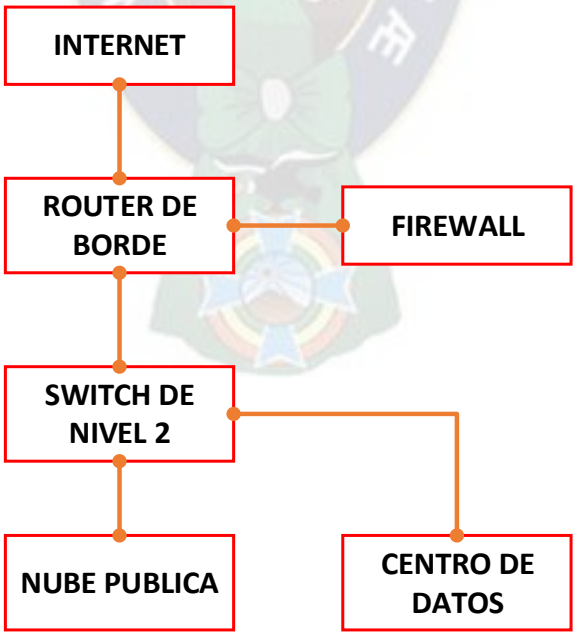



**Figura 65.** Diagrama de cableado de la Entrada de Servicios al Centro de Datos.

El diagrama muestra una conexión de red desde la ESP (Entrada de Servicios al Centro de Datos) a varios dispositivos de red. La ESP está conectada a través de líneas de fibra óptica al router de borde. El router de borde está conectado a un firewall de próxima generación, que está a su vez conectado a un switch de nivel 2. El switch de nivel 2 está conectado a la nube pública a través de una línea de cableado de cobre CAT6A. Finalmente, el centro de datos está conectado al switch de nivel 2.

**b). Subsistema Eléctrico**

**Calculo de la Potencia del equipo UPS.**

**TABLA DE CONSUMO DE LA SOLUCION PROPUESTA**

| ITEM | DESCRIPCION | CONSUMO | CANTIDAD | TOTAL WATTS |
|---|---|---|---|---|
| 1 | Servidor DELL PowerEdge R740xD | 750 watts | 1 | 750 watts |
| 2 | Almacenamiento SAN HP MSA 2040 | 437 watts | 1 | 437 watts |
| 3 | Switch de Distribución CISCO 9400 Series+ASA 5500 NGFW | 2100 watts | 1 | 2100 watts |
| 4 | Router de Core CISCO 8000 Series | 750 watts | 1 | 750 watts |
| 5 | Switch Edge CISCO 2961 | 40 watts | 1 | 40 watts |
| | | | **TOTAL:** | **4077 Watts** |

**Figura 66.** Tabla de consumo de la solución propuesta.

$$\text{CALCULO DE LA POTENCIA DEL UPS} = \frac{4077\ \text{Watts}}{0{,}7} = 5825\ \text{VA}$$

**SOLUCION:**

**UPS:** Implementar el resguardo de energía para los equipos informáticos mediante 1 Equipo **UPS de 6 KVA**, tecnología OnLine Doble Conversión, Factor de Potencia mayor a 0,8, Entrada Monofásica 220/230 VAC.

**Calculo de la sección del cable eléctrico para el UPS.**

$$\text{CALCULO DE LA SECCION DEL CABLE PARA EL UPS} = \frac{4077\ \text{Watts}}{230\ \text{Vac}} = 17,7\ \text{Amperios}$$

**Según la tabla AWG de sección de cables:**

**Tabla AWG Según el Amperaje**

| Sección AWG | Sección $mm^2$ | Corriente (Amperios) |
|---|---|---|
| 20 | 0.5 | 3 |
| 18 | 1 | 7 |
| 16 | 1,5 | 10 |
| 14 | 2,5 | 15 |
| 12 | 4 | 20 |
| 10 | 6 | 30 |
| 8 | 10 | 40 |
| 6 | 16 | 55 |
| 4 | 25 | 70 |

**SOLUCION:** Utilizaremos cable AWG 12, Sección del cable 4 mm4, soporta hasta 20 Amperios de corriente eléctrica. Sistema Monofásico: AWG 12 Cable para Fase (L), Neutro (N) y Tierra (GND).

### 3.4.2.1. Diseño del Tablero Principal (tablero de energía no regulada).

Dimensiones del Tablero: Altura 40 cm. Ancho 30 cm, Profundidad 25 cm.

Ingreso de la energía: Monofásica Fase+Neutro.

Los Termo magnéticos de Entrada: Bipolar de 32 A.

Los Termo magnéticos de Salida deben ser de tipo bipolar de 16 A.

El tablero incluye barra de Aterramiento.

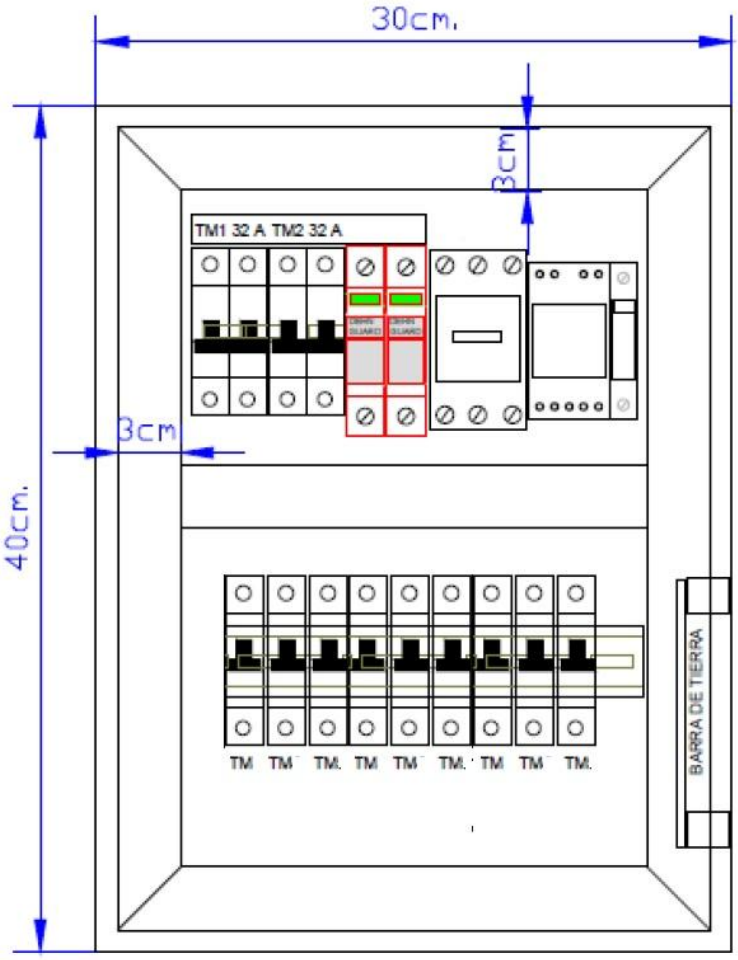



**Figura 67.** Diseño del Tablero Principal *(fuente propia)*

**Descargadores**

**Tipo 2.** Incluiremos en el tablero elementos de Protección Contra Sobretensiones Tipo 2: DEHN GUARD (Según el estándar EN 61643-1), para proteger la línea de Fase (L) y el Neutro (N), derivando estas sobretensiones hacia el Sistema de Puesta a Tierra.

Más información

- Fichas técnicas
- Archivos CAD
- Texto LV
- Manual de instalación

Datos técnicos

| | |
|---|---|
| DPS según EN 61643-11 / ... IEC 61643-11 | Tipo 2 / Clase II |
| Máx. tensión permisible de servicio AC ($U_C$) | 150 V (50 / 60 Hz) V |
| Corriente nominal de descarga (8/20 µs) ($I_n$) | 15 kA |
| Corriente máx. de descarga (8/20 µs) ($I_{max}$) | 40 kA |
| Nivel de protección ($U_p$) | ≤ 0,7 kV |
| Máx. protección contra sobrecorrientes sector primario | 125 A gG |
| Certificaciones | KEMA, UL |

**Iluminación.**

**SOLUCION:** Se debe iluminar los pasillos fríos que estará en la parte frontal del rack de equipos informáticos,

Según TIA-942 la iluminación mínima es de 500 LUX, con paneles tipo Led.

**c). Subsistema Mecánico**

**Calculo de la potencia frigorífica del equipo de Aire Acondicionado de Precisión.**

Realizamos el cálculo de la potencia que permita refrigerar a los equipos informáticos de Data Center.

Podemos convertir la potencia expresada en watts a BTU/hr (British Termal Unit/hora).

| | |
|---|---|
| **CALCULO DE LA POTENCIA FRIGORIFICA DEL EQUIPO DE REFRIGERACION** | **= 3,41 x 4077 Watts = 13902 BTU** |

**SOLUCION:**

El equipo de Aire Acondicionado de Precisión debe ser de capacidad superior a **14000 BTU.**

Expresado en watts, tenemos **4,1 KW.**

**d). Subsistema de Arquitectura**

### 3.4.2.2. Adecuación de obras civiles del ambiente Físico del Data Center

El diseño del Data Center estará contenido en los ambientes ya existentes en el edificio de la Facultad de Ingeniería. El ambiente consta de tres partes los cuales son:

El ambiente principal donde están contenidos los racks, un gabinete con los servidores, switchs, sistema de enfriamiento y demás equipos que se encuentran funcionando actualmente. Junto al cambien principal se encuentra una oficina de administración desde donde se controla y monitorea los equipos del Data Center, el ambiente principal y la oficina de administración están separados por una mampara de vidrio. También está instalada una escalerilla metálica en la parte superior que atraviesa ambos ambientes por donde todos los cables que se conectan a los equipos del Data Center. Y por último existe un pequeño cuarto pegado a la oficina de administración donde está instalado un tablero eléctrico que alimenta a todo el Data Center.
**Acabado de Pintura de las paredes interna** con tipo de pintura *Epoxica*. La pintura *epoxica* está fabricada con componentes elaborados a base *de* una resina *epoxica*, la cual es resistente y *de* alta calidad.

**Diseño 2D de la sala de Servidores y NOC.**

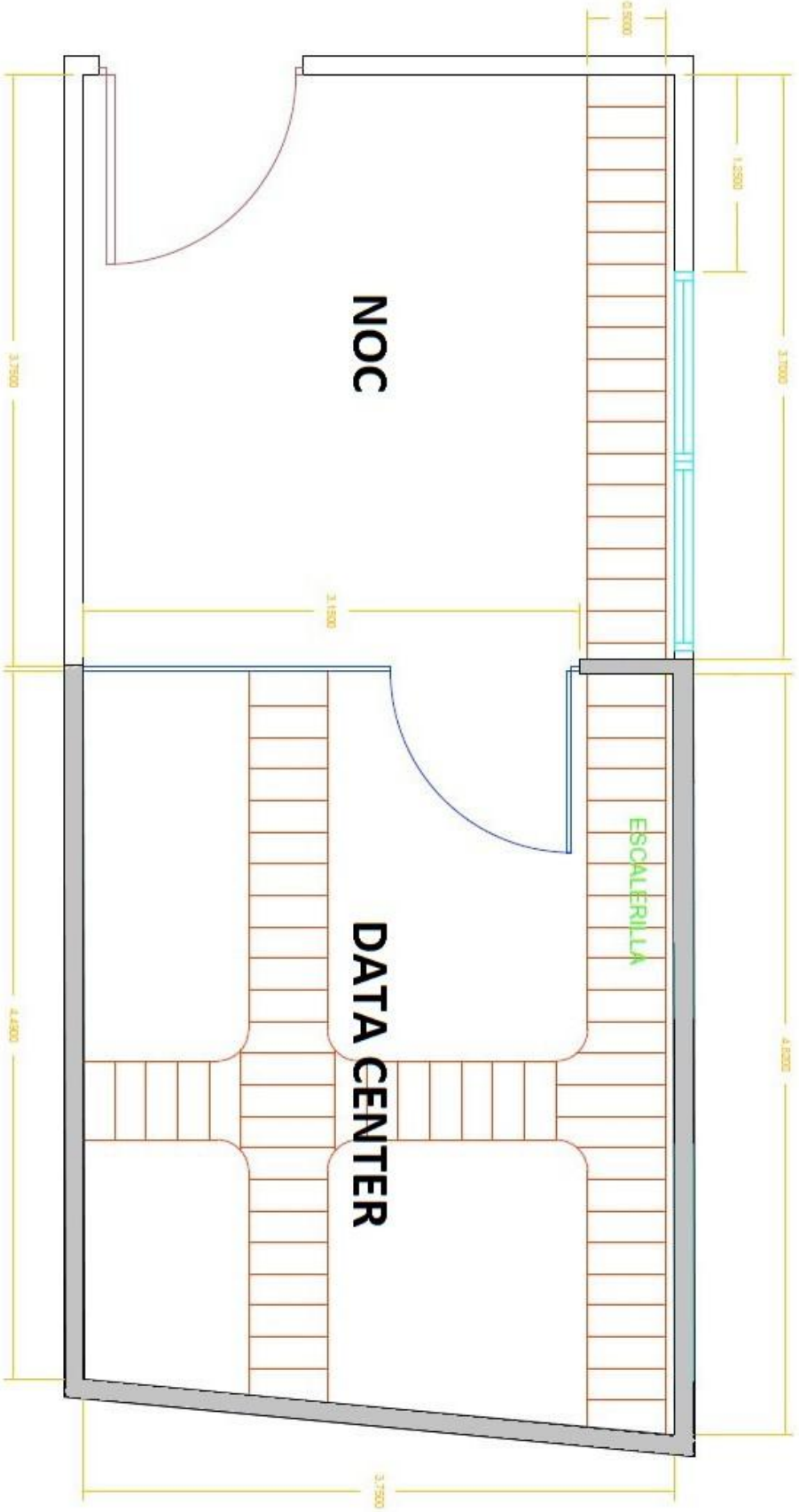

NOC
DATA CENTER
ESCALERILLA

**Figura 68.** Plano actual del Data Center IngeTIC *(fuente propia)*.

**DIAGRAMA DE LA SOLUCION FINAL.**

Esquema de la solución de la Infraestructura Critica del Data Center RATED I (TIA-942-B-1)

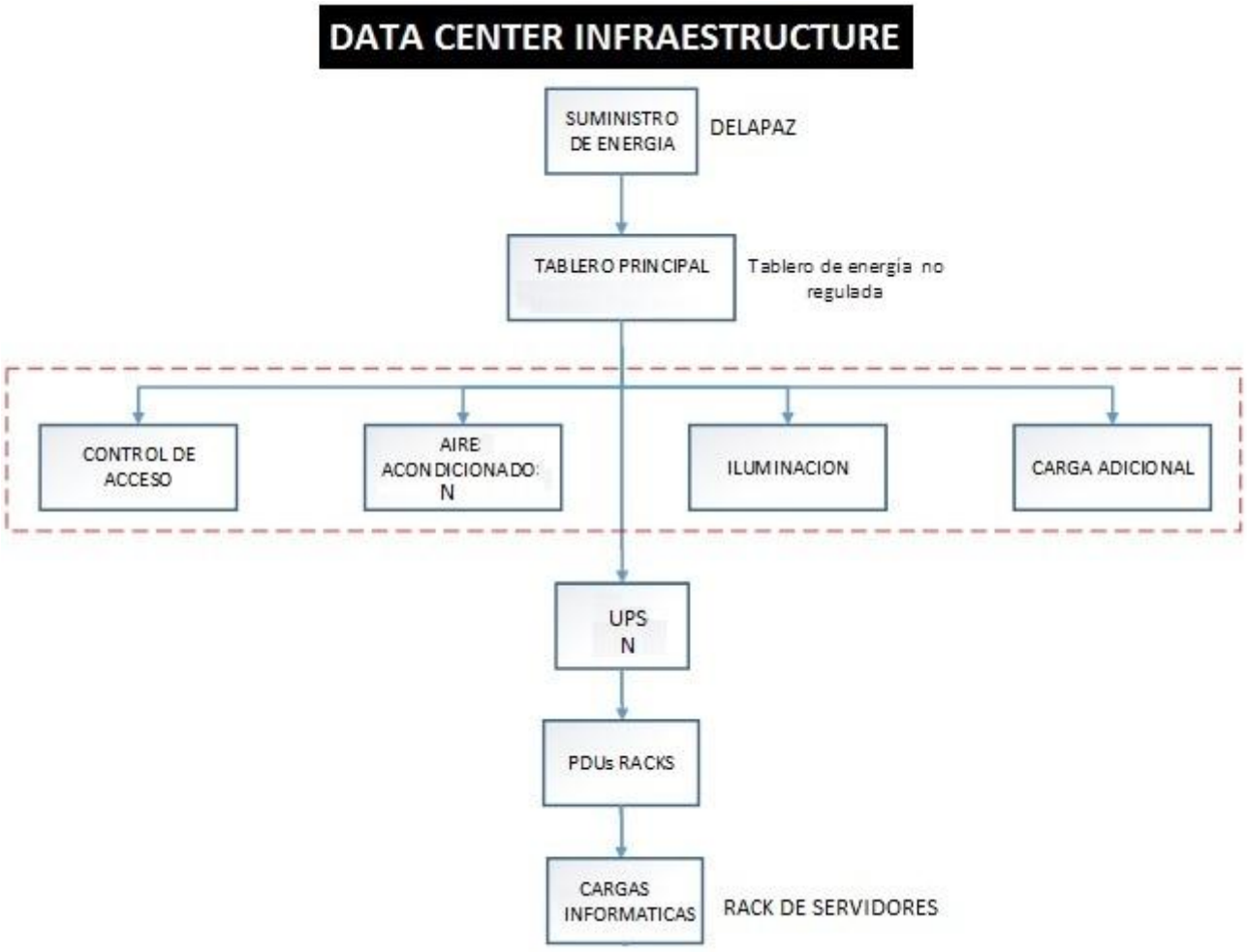



**Figura 69.** Diagrama de la solución final *(fuente propia)*.

**Solución.**

***Actualización ANSI/TIA-942-B-1 para la Infraestructura de los Centros de Datos tipo EDGE***

El apéndice de la norma define los requisitos iniciales de la infraestructura y las directrices de diseño para los centros de datos tipo Edge, también denominados "microcentros" de datos.

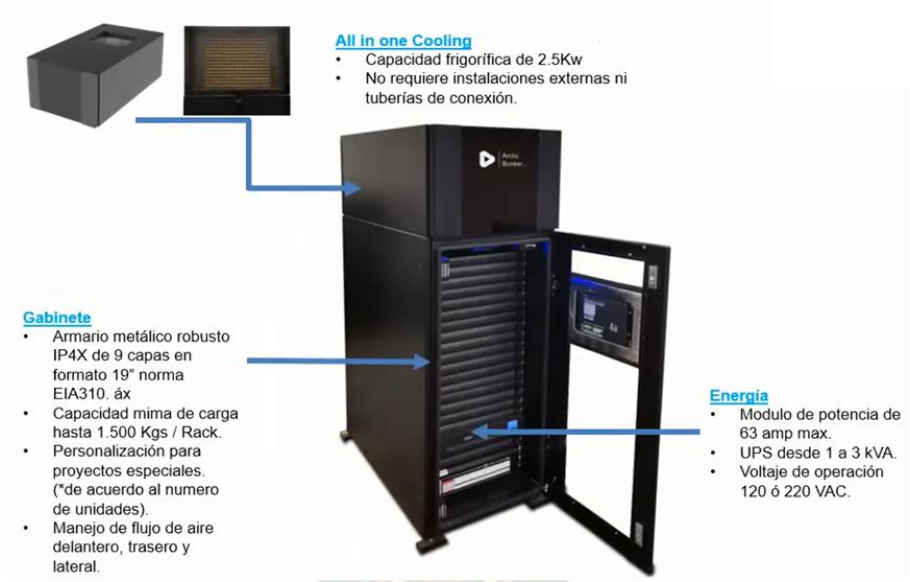
Como señala el comité de normas, los centros de datos Edge suelen estar alojados en recintos prefabricados y pueden ser supervisados y controlados a distancia. Se consideran fundamentales para el éxito de las aplicaciones de próxima generación que exigirán una latencia ultrabaja, como los vehículos autónomos, la realidad aumentada y la telemedicina.

| | **ANSI/TIA-942-B-1** |
|---|---|
| **Telecommunications Infrastructure Standard for Data Centers Addendum 1**: | ***Edge Data Centers*** |
| **Publication date:** | 2022-01-27 |
| **Information:** | This item will be ordered specially for you, therefore delivery may take 1 to 2 weeks. |
| **Original language:** | English |
| **Pages:** | 32 |

El Centro de Datos planificado es de tipo mediano-pequeño, por lo cual la solución se adecua a los nuevos tipos de centros de datos denominados ***Edge Data Center***, también conocidos como ***Mini Data Center*** o ***Micro Data Center***.

**SOLUCION: Planteamos la solución modular con Micro Data Center:**

| **SISTEMA MICRO DATA CENTER** | |
|---|---|
| Diseñado para cumplir con los estándares actuales, una **solución auto contenida**, que permite mantener en funcionamiento adecuado la infraestructura tecnológica de información y telecomunicaciones, que provee servicios de:<br>• *Alimentación eléctrica regulada (UPS).*<br>• *Aire acondicionado de precisión (CRAC).*<br>• *Sensores de Temperatura, Humedad relativa, humo y líquido.*<br>• *Control de Acceso electrónico biométrico y registros.*<br>• *Control de seguridad con cámara frontal.*<br>• *Detección de alarma y extinción de incendio con agente aerosol y ecológico.*<br>• *Doble puerta con acceso controlado.* |  |


**Solución:**

En base a los valores calculados anteriormente:

| | |
|---|---|
| **Equipo UPS** | **Potencia del equipo UPS 6 KVA** |
| **Equipo de Refrigeración** | **Potencia de Refrigeración del equipo de Aire Acondicionado de Precisión expresado en watts 4,1 KW (equivalente a 13903 BTU).** |


*De acuerdo a la hoja de especificaciones técnicas del Fabricante Atlantic Power*

| MODELO | ATP-03N | ATP-03W | ATP-06E | ATP-06T | ATP-06F | ATP-10S | Customized |
|---|---|---|---|---|---|---|---|
| Espacio disponible - U | 18 | 19 | 26 | 29 | 35 | 35 | Per Definition |
| Redundancia | N | N | N | N | N | N | N/N+1/2N |
| Ancho - mm | 600 | 600 | 600 | 600 | 900 | 900 | 600/800 |
| Profundidad - mm | 1100 | 1100 | 1100 | 1400 | 1400 | 1400 | 1000/1100/1200/1400 |
| Altura - mm | 1200 | 1590 | 2000 | 2000 | 2000 | 2000 | 2600 Max. |
| Peso - mm | 162 | 190 | 330 | 374 | 521 | 525 | Per Definition |
| Tipo de potencia de entrada | 208-230V/1P /2P/50-60Hz | 208-230V/1P /2P/50-60Hz | 208-230V/1P /2P/50-60Hz | 208-230V/1P /2P/50-60Hz | 208-230V/1P /2P/50-60Hz | 208-230V/1P /2P/50-60Hz | Customized |
| Sección de poder | | | | | | | |
| UPS - kVA | 3 | 3 | 6 | 6 | 6 | 10 | 3/6/10/20/30/50 |
| Tipo de montaje | Rack | Rack | Rack | Rack | Rack | Rack | Rack |
| Batería estándar | 12V/9AH 6pcs | 12V/9AH 6pcs | 12V/9AH 16pcs | 12V/9AH 16pcs | 12V/9AH 16pcs | 12V/9AH 16pcs | 200Ah Max. |
| PDU | Basic 8Slots | Basic 8Slots | Basic 16Slots | Basic 16Slots | Basic 16Slots | Basic 16Slots | Basic/Smart |
| Sección de enfriamiento | | | | | | | |
| Tipo de enfriamiento | Ventilation | Packaged DX | Packaged DX | Split DX | Split DX | Split DX | Packaged/Split |
| Tipo de montaje | Top | Top | Top | Rack | Row | Row | Top/Rack/Row |
| Capacidad - kW | 2.0 | 2.5 | 3.5 | 3.9 | 5.6 | 7.6 | 40.9 Max. |
| Ventilación de emergencia | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

**SOLUCION: Micro Data Center Atlantic Power, Modelo: ATP-06F.**

*Finalmente adjuntaremos la tabla de* ANALISIS ECONOMICO (**ANEXO B**).

## 3.5. DISEÑO LÓGICO DE LA SOLUCIÓN DE RED DEL EDIFICIO (ENTERPRISE CAMPUS LAN)

El diseño lógico de red se refiere a la planificación de: La estructura, configuración y comunicación de la red a nivel lógico. Es decir, cómo se organiza la información y se transmiten los datos a través de la red.

En el diseño lógico de la red establecemos los protocolos de comunicación, los esquemas de direccionamiento IP, las políticas de seguridad, los servicios de red que se ofrecen a los usuarios internos y externos, entre otros aspectos.

Este proceso se enfoca en la forma en que los dispositivos se conectan entre sí, cómo se comunican y cómo se gestiona el tráfico de la red.

Por lo tanto, el objetivo principal del diseño lógico de una red es establecer un modelo de comunicación efectivo, seguro y escalable para los usuarios y dispositivos de la red. Todos estos aspectos se implementan sobre la infraestructura IT (equipamiento informático) del Data Center, por lo cual tendríamos el diseño lógico de red en base a los siguientes aspectos, detallados en la siguiente tabla:

| ELEMENTOS DEL DISEÑO LÓGICO DE RED | DESCRIPCIÓN |
|---|---|
| **Protocolos de red** | Selección de los protocolos de red que se utilizarán para establecer la comunicación entre dispositivos. En nuestro caso el protocolo TCP/IP. |
| **Esquema de direccionamiento IP** | Diseño de las direcciones IP y las subredes que se utilizarán en la red. De acuerdo al diseño se podrán utilizar IPv4 e IPv6. |
| **Políticas de seguridad** | Establecimiento de las políticas de seguridad que se implementarán en la red para controlar el acceso a la misma, autenticación de usuarios, cifrado de datos. Principalmente se utilizara el Firewall del Servidor. |
| **Servicios de red** | Selección de los servicios que se ofrecerán en la red. Los servicios de sistemas para docentes y estudiantes, almacenamiento en red, telefonía IP, servicio de video vigilancia y otros. |
| **Topología de red** | Diseño de la topología de la red, seleccionando la forma en que los dispositivos estarán interconectados en la red. En el diseño se realiza una topología en árbol. |

| | |
|---|---|
| **Capacidad de la red** | Estimación de la capacidad de la red para soportar un número determinado de dispositivos y aplicaciones. De acuerdo al diseño el data center soportara una gran cantidad de equipos conectados y podrá alojar varios aplicaciones web. |
| **Redundancia** | Inclusión de mecanismos de redundancia en la red para evitar puntos únicos de fallo y mejorar la disponibilidad de la red (protocolo STP). |
| **Gestión de tráfico** | Establecimiento de políticas de gestión de tráfico para garantizar la calidad de servicio y evitar la congestión en la red. |

**Tabla 23.** Diseño lógico de Red.

### 3.5.1. Servicio de Hosting

El servidor alojara diversos sistemas, varias aplicaciones web que son utilizados actualmente y deberán ser migrados al nuevo data center y otros nuevos que podrán ser implementados de acuerdo a las necesidades que se requieran, estas aplicaciones tendrán una gran cantidad de flujo de datos debido a que la cantidad de usuarios es bastante grande entre estudiantes, docentes, administrativos y demás usuarios.

Asignar hosts a una gran cantidad de usuarios en un servidor puede ser un desafío, pero hay varias estrategias que pueden ayudar a lograrlo de manera efectiva. A continuación, se mencionan los métodos que utilizaremos:

- **Virtualización:** Una opción es utilizar la virtualización para crear múltiples servidores virtuales en un solo servidor físico. Esto permite la asignación de hosts a más usuarios de manera más eficiente.
- **Balanceo de carga:** El balanceo de carga es una técnica que distribuye la carga de trabajo entre varios servidores para evitar la sobrecarga en un solo servidor. Esta técnica también puede ser útil para asignar hosts a más de 10000 usuarios.
- **Escalado horizontal:** En lugar de aumentar la capacidad de un solo servidor, otra opción es agregar más servidores al conjunto para distribuir la carga de trabajo. Esto se conoce como escalado horizontal y puede ser útil para aumentar la capacidad de asignación de hosts para más usuarios.

- **Optimización del servidor:** Optimizar el servidor para mejorar su rendimiento también puede ser útil para asignar hosts a más usuarios. Esto puede incluir ajustar la configuración del sistema operativo, actualizar el hardware y optimizar las aplicaciones.
- **Implementación de políticas de uso:** Finalmente, una estrategia importante es implementar políticas de uso que limiten el acceso y el uso del servidor a los usuarios y aplicaciones que realmente lo necesitan. Esto puede ayudar a reducir la carga de trabajo en el servidor y permitir una asignación más efectiva de hosts a más usuarios.

Se debe generar una gran cantidad de hosts en el servidor, esto requiriere una combinación de configuraciones y herramientas. Una de las operaciones que se realizara para lograr esto es implementar subredes. Una red de subredes implica dividir una red en varias subredes más pequeñas, cada una de las cuales tiene su propio rango de direcciones IP y su propia máscara de subred. Esto puede permitirte asignar direcciones IP únicas a más de 12000 hosts.

**SOLUCION:**

Teniendo como referencia que la población actual de usuarios (estudiantes) que recurren al servicio entregados por Data Center IngeTIC, está en alrededor de 10000 estudiantes**.**

**Realizamos el siguiente proceso asumiendo 12000 host:**

***Determinamos el número de hosts por subred:*** Con una máscara de red /19, se pueden crear subredes de 8190 hosts cada una. Para crear una red para 12,000 hosts, se necesitarán al menos dos subredes.

***Seleccionamos una dirección IP de red:*** Para esta red, se puede utilizar la dirección IP de red 192.168.0.0.

***Calculamos las direcciones de red y de broadcast de cada subred utilizando una tabla de álgebra booleana:*** Utilizando una máscara de red /19, la tabla de álgebra booleana se vería así:

| Octeto 1 | Octeto 2 | Octeto 3 | Octeto 4 | Máscara | Dirección de red | Dirección de broadcast |
|---|---|---|---|---|---|---|
| 192 | 168 | 0 | 0 | 255.255.224.0 /19 | 192.168.0.0 | 192.168.31.255 |
| 192 | 168 | 32 | 0 | 255.255.224.0 /19 | 192.168.32.0 | 192.168.63.255 |

***Asignar las direcciones IP a cada host en cada subred utilizando una técnica de numeración de subred:*** Para la primera subred, se pueden asignar direcciones IP desde 192.168.0.1 hasta 192.168.31.254, y para la segunda subred, se pueden asignar direcciones IP desde 192.168.32.1 hasta 192.168.63.254.

***Configurando los dispositivos de red:*** Se deben configurar los routers y switches para permitir la comunicación entre las subredes y para enrutar el tráfico de red correctamente.

**Para el caso de IPv4.**

**Partiendo de la dirección IP asignada 192.168.0.0**

**11000000.10101000.00000000.00000000**

***Direcciones de red y de broadcast:*** Utilizando una máscara de red /19 en formato binario.

11111111.11111111.11100000.00000000

***Se pueden calcular las direcciones de red y de broadcast para cada subred:***

***Dirección de red de la primera subred:***

11000000.10101000.00000000.00000000 (192.168.0.0)

***Dirección de broadcast de la primera subred:***

11000000.10101000.00011111.11111111 (192.168.31.255)

***Dirección de red de la segunda subred:***

11000000.10101000.00100000.00000000 (192.168.32.0)

***Dirección de broadcast de la segunda subred:***

11000000.10101000.00111111.11111111 (192.168.63.255)

***Asignando las direcciones IP a cada host*** en cada subred utilizando una técnica de numeración de subred: Para la primera subred, se pueden asignar direcciones IP desde:

11000000.10101000.00000000.00000001 (192.168.0.1)

Hasta: 11000000.10101000.00011111.11111110 (192.168.31.254)

Para la segunda subred, se pueden asignar direcciones IP desde:

11000000.10101000.00100000.00000001 (192.168.32.1)

Hasta: 11000000.10101000.00111111.11111110 (192.168.63.254)

***Configurando los dispositivos de red:***

Para configurar el router para manejar una red con 12000 hosts, necesitamos configurar adecuadamente la interfaz de red conectada a la red de 12000 hosts y asegurarse de que el router tenga suficiente capacidad de procesamiento y memoria para manejar el tráfico de la red. A continuación, se muestra la configuración básica para la interfaz de red de un router:

```
interface GigabitEthernet0/0
description Red de 12000 hosts
ip address 200.1.1.1 255.255.240.0
ipv6 address 2001:0db8::1/52
no shutdown
```

Se está configurando la interfaz GigabitEthernet0/0 con una dirección IP de la red 200.1.1.0/20 (que incluye la red de 12000 hosts), y una dirección IPv6 de la red 2001:0db8::/52 (que también incluye la red de 12000 hosts). La interfaz se habilita utilizando el comando "no shutdown".

Es importante asegurarse de que el router tenga suficiente capacidad de procesamiento y memoria para manejar el tráfico de la red de 12000 hosts. Esto puede incluir la configuración de enrutamiento dinámico, el balanceo de carga y la redundancia de enrutamiento para mejorar la eficiencia y la fiabilidad de la red.

En general, la configuración exacta del router dependerá de los detalles de la red en sí, incluyendo el tipo de tráfico que se espera, la topología de la red y los requisitos de seguridad, entre otros factores.

***Verificando y ajustando la configuración:*** Una vez que se han configurado todos los dispositivos de red, es importante verificar que todo esté funcionando correctamente. Se deben realizar pruebas de conectividad para asegurarse de que los hosts pueden comunicarse entre sí y con los servidores y dispositivos de red en la red. Si hay algún problema, se deben hacer ajustes en la configuración de red para solucionarlo.

***Tareas de Mantenimiento y administración de la red:*** Una vez que la red está en funcionamiento, es importante realizar tareas de mantenimiento y administración para asegurarse de que siga funcionando correctamente. Esto puede incluir la aplicación de parches de seguridad, la actualización del firmware de los dispositivos de red, la supervisión del tráfico de red para detectar posibles problemas y la implementación de políticas de seguridad para proteger la red contra amenazas externas.

**Para el caso de IPv6.**

***Determinamos el número de hosts por subred:*** Con una máscara de red /52, se pueden crear subredes de 2404780 hosts cada una. Para crear una red para 12,000 hosts, se necesitarán al menos cinco subredes.

***Seleccionamos una dirección de red:*** Para esta red, se puede utilizar la dirección de red: 2001:0db8:0000:0000:0000:0000:0000:0000 en formato hexadecimal.

***Calculamos las direcciones de red y de broadcast de cada subred utilizando una tabla de álgebra booleana:*** Utilizando una máscara de red /52 en formato binario:

11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111100

***Se pueden calcular las direcciones de red y de broadcast para cada subred:***

***Dirección de red de la primera subred:***

2001:0db8:0000:0000:0000:0000:0000:0000 (2001:0db8::)

***Dirección de broadcast de la primera subred:***

2001:0db8:0000:0000:0000:0000:0000:ffff (2001:0db8::ffff:ffff:ffff:ffff)

***Dirección de red de la segunda subred:***

2001:0db8:0000:0000:0000:0001:0000:0000 (2001:0db8:1::)

***Dirección de broadcast de la segunda subred:***

2001:0db8:0000:0000:0000:0001:ffff:ffff (2001:0db8:1:ffff:ffff:ffff:ffff:ffff)

***Dirección de red de la tercera subred:***

2001:0db8:0000:0000:0000:0002:0000:0000 (2001:0db8:2::)

***Dirección de broadcast de la tercera subred:***

2001:0db8:0000:0000:0000:0002:ffff:ffff (2001:0db8:2:ffff:ffff:ffff:ffff:ffff)

***Dirección de red de la cuarta subred:***

2001:0db8:0000:0000:0000:0003:0000:0000 (2001:0db8:3::)

***Dirección de broadcast de la cuarta subred:***

2001:0db8:0000:0000:0000:0003:ffff:ffff (2001:0db8:3:ffff:ffff:ffff:ffff:ffff)

***Dirección de red de la quinta subred:***

2001:0db8:0000:0000:0000:0004:0000:0000 (2001:0db8:4::)

***Dirección de broadcast de la quinta subred:***

2001:0db8:0000:0000:0000:0004:ffff:ffff (2001:0db8:4:ffff:ffff:ffff:ffff:ffff)

***Asignar las direcciones IPv6 a cada host en cada subred utilizando una técnica de numeración de subred:*** Para la primera subred, se pueden asignar direcciones IPv6 a cada host utilizando la numeración de subred, que consiste en utilizar los últimos 64 bits de la dirección IPv6 para numerar los hosts en esa subred.

**La primera dirección IPv6 de la primera subred sería 2001:0db8::1:0:0:0:1**

**La segunda sería 2001:0db8::1:0:0:0:2**

Y así sucesivamente hasta la dirección: 2001:0db8::1:0:0:fffe

**La última sería 2001:0db8::1:0:0:ffff.**

***Para la segunda subred***, se pueden asignar direcciones IPv6 utilizando la numeración de subred:

**2001:0db8:1::1:0:0:1**

Para el primer host y así sucesivamente hasta la dirección:

**2001:0db8:1::1:0:0:ffff**

Para el último host.

***Para la tercera subred***, se pueden asignar direcciones IPv6 utilizando la numeración de subred:

**2001:0db8:2::1:0:0:1**

Para el primer host y así sucesivamente hasta la dirección:

**2001:0db8:2::1:0:0:ffff**

Para el último host.

***Para la cuarta subred***, se pueden asignar direcciones IPv6 utilizando la numeración de subred:

**2001:0db8:3::1:0:0:1**

Para el primer host y así sucesivamente hasta la dirección:

**2001:0db8:3::1:0:0:ffff**

Para el último host.

***Para la quinta subred***, se pueden asignar direcciones IPv6 utilizando la numeración de subred:

**2001:0db8:4::1:0:0:1**

Para el primer host y así sucesivamente hasta la dirección:

2001:0db8:4::1:0:0:ffff

Para el último host.

***La configuración del router,*** para manejar una red de 12000 hosts con IPv6 requeriría la configuración de la interfaz de red conectada a la red de 12000 hosts, así como la configuración de enrutamiento adecuada. A continuación, se muestra un ejemplo de configuración básica para la interfaz de red de un router core de Cisco con IPv6:

```
interface GigabitEthernet0/0
description Red de 12000 hosts
ipv6 address 2001:0db8::1/52
no shutdown
```

Se está configurando la interfaz GigabitEthernet0/0 con una dirección IPv6 de la red 2001:0db8::/52 (que incluye la red de 12000 hosts). La interfaz se habilita utilizando el comando "no shutdown".

Además de la configuración de la interfaz de red, se necesitará una configuración adecuada de enrutamiento para asegurarse de que el tráfico IPv6 pueda llegar a su destino correctamente. Esto podría incluir la configuración de enrutamiento estático o dinámico, dependiendo de los detalles de la red. Por ejemplo, si hay varios routers en la red, se podría configurar el enrutamiento dinámico utilizando el protocolo OSPFv3 para que los routers

puedan intercambiar información de enrutamiento y seleccionar automáticamente las rutas óptimas para el tráfico IPv6.

Es importante tener en cuenta que la configuración exacta del router dependerá de los detalles de la red en sí, incluyendo el tipo de tráfico que se espera, la topología de la red y los requisitos de seguridad, entre otros factores.

En resumen, la red IPv6 para 12000 hosts se puede crear utilizando cinco subredes con una máscara de red /52, con una dirección de red de 2001:0db8:: y las direcciones de red y de multicast o broadcast de cada subred se pueden calcular utilizando una tabla de álgebra booleana. Las direcciones IPv6 se pueden asignar utilizando la numeración de subred, utilizando los últimos 64 bits de la dirección IPv6 para numerar los hosts en cada subred.

### 3.5.2. Configuración del Servidor

El sistema operativo elegido en el servidor es Linux, ya que este sistema operativo tiene todas las herramientas necesarias para la implementación de los servicios requeridos. Mediante los siguientes pasos tendremos el servidor listo para ser usado:

- **Primera tarea**, instalación del Software de Virtualización TIPO 1 (Hyper Visor Bare Metal).
- **Descargando e instalando la distribución de Linux:** Primero, se elige una distribución de Linux que se adapte a las necesidades requeridas. Hay muchas opciones, como Ubuntu, Debian, CentOS, entre otros. En nuestro caso elegimos la distribución de Debian.
- **Configurando la red:** Se configura la red en el servidor durante la instalación. Se asegura de configurar la dirección IP y la configuración DNS correctamente.
- **Configurando el usuario y la contraseña:** Se configura el usuario y la contraseña para acceder al servidor. Se asegura de utilizar contraseñas seguras.
- **Actualizando el sistema:** Después de instalar Linux en el servidor, se actualiza el sistema con los últimos parches de seguridad y actualizaciones de software.

- **Configurando el servidor:** Se configura el servidor según las necesidades. Esto incluye la instalación de software adicional, la configuración de servicios como el servidor web, la base de datos, etc.

**Para configurar un servidor con Linux Debian, estos son los comandos a utilizar:**

- **Actualizando el sistema: sudo apt update** && **sudo apt upgrade -y** - Este comando actualiza la lista de paquetes y actualiza todos los paquetes instalados en el sistema.
- **Instalando paquetes: sudo apt install <paquete>** - Este comando instala el paquete especificado. Por ejemplo, para instalar el servidor web Apache, se puede ingresar **sudo apt install apache2**.
- **Reiniciando un servicio: sudo systemctl restart <servicio>** - Este comando reinicia el servicio especificado. Por ejemplo, para reiniciar el servidor web Apache, puedes ingresar **sudo systemctl restart apache2**.
- **Iniciando un servicio: sudo systemctl start <servicio>** - Este comando inicia el servicio especificado. Por ejemplo, para iniciar el servidor web Apache, puedes ingresar **sudo systemctl start apache2**.
- **Deteniendo un servicio: sudo systemctl stop <servicio>** - Este comando detiene el servicio especificado. Por ejemplo, para detener el servidor web Apache, puedes ingresar **sudo systemctl stop apache2**.
- **Habilitando un servicio: sudo systemctl enable <servicio>** - Este comando habilita el servicio especificado para que se inicie automáticamente al arrancar el sistema. Por ejemplo, para habilitar el servidor web Apache, puedes ingresar **sudo systemctl enable apache2**.
- **Deshabilitando un servicio: sudo systemctl disable <servicio>** - Este comando deshabilita el servicio especificado para que no se inicie automáticamente al arrancar el sistema. Por ejemplo, para deshabilitar el servidor web Apache, puedes ingresar **sudo systemctl disable apache2**.

Estos son los comandos básicos para configurar un servidor con Linux Debian. La configuración real dependerá de los servicios y paquetes que desees instalar y configurar en el servidor.

Por último, se instala y configura Apache que es el software elegido para tener el servicio web de acceso para los usuarios al servidor. El procedimiento para la configuración de Apache es el siguiente:

- **Instalar Apache:** Primero, asegurarnos de tener instalado Apache en tu sistema Debian. Podemos instalarlo con el siguiente comando en la terminal:

  sudo apt-get update

  sudo apt-get install apache2

- **Verificando la instalación:** Una vez instalado, podemos verificar que Apache está funcionando correctamente ejecutando el siguiente comando:

  sudo systemctl status apache2

  Si todo está bien, deberías ver un mensaje que indica que Apache se está ejecutando.

- **Configurando el Firewall:** Si se tiene un firewall activado, como UFW, se debe asegurar de permitir el tráfico HTTP y HTTPS para que Apache pueda recibir y enviar solicitudes. Puedes hacerlo con los siguientes comandos:

  sudo ufw allow http

  sudo ufw allow https

- **Configurando el dominio y la carpeta del sitio web:** Por defecto, Apache alojará los sitios web en la carpeta /var/www/html. Para agregar un sitio web, debes crear una carpeta dentro de /var/www y luego configurar Apache para que sirva contenido desde esa carpeta. También se debe asegurar que el dominio esté apuntando a la dirección IP del servidor. Si el dominio es "servfacing.com" y se desea alojar el sitio web en la carpeta /var/www/ servfacing.com, se ejecutan los siguientes comandos:

  sudo mkdir /var/www/servfacing.com

  sudo chown -R www-data:www-data /var/www/servfacing.com

  sudo chmod -R 755 /var/www/ servfacing.com

  sudo nano /etc/apache2/sites-available/servfacing.conf

  Dentro del archivo de configuración "servfacing.com.conf", se agrega la siguiente información:

  <VirtualHost *:80>

```
ServerName servfacing.com
ServerAlias www.servfacing.com
DocumentRoot /var/www/servfacing.com
<Directory /var/www/servfacing.com>
   AllowOverride All
</Directory>
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

- **Activando el sitio:** Una vez que se haya configurado el archivo de configuración para el sitio web, se debe habilitar en Apache. Se aplica el siguiente comando:

  ```
  sudo a2ensite servfacing.com.conf
  ```

- **Reiniciando Apache:** Finalmente, se debe reiniciar Apache para que pueda cargar la nueva configuración. Se ejecuta con el siguiente comando:

  ```
  sudo systemctl restart apache2
  ```

Con estas estas configuraciones el servidor estará listo para alojar todas las aplicaciones web requeridas para que los usuarios tengan acceso a los servicios que brinde el servidor.

### 3.5.3. Aplicaciones Web

Una vez terminadas todas las configuraciones previas, el servidor virtual está listo para ser utilizado y como la principal función es la de alojar aplicaciones web se implementa lenguajes de programación para realizar las tareas requeridas. En nuestro caso instalamos un intérprete de lenguaje PHP y Python con el cual realizaremos las aplicaciones web, realizando el siguiente procedimiento:

- **Instalando el Interprete:**

  Se instala PHP mediante el siguiente comando:

  ```
  sudo apt-get install php libapache2-mod-php
  ```

  Para instalar Python:

  ```
  sudo apt-get install python3
  ```

- **Instalando un gestor de Base de Datos:** Es necesario realizar Bases de Datos por lo cual se instala un gestor como MySQL o PostgreSQL, mediante los siguientes comandos:

  sudo apt-get install mysql-server

  sudo apt-get install postgresql postgresql-contrib
- **Configurando la aplicación web:** Ahora que tenemos el servidor web, intérprete de lenguaje de programación y gestor de base de datos instalados, se pueden configurar las aplicaciones web. La configuración específica dependerá del tipo de aplicación que se esté desarrollando. Sin embargo, generalmente, se debe configurar la ubicación de los archivos de la aplicación, las credenciales de la base de datos y las opciones de seguridad.
- **Lanzando la aplicación web:** Una vez que se haya configurado la aplicación web, ya se puede lanzar en el servidor mediante el siguiente comando:

  sudo service apache2 start

  La aplicación web debe estar ubicada en el directorio correcto del servidor web. Para Apache, el directorio predeterminado es "/var/www/html/".

Ahora se debe poder acceder a la aplicación web mediante un navegador web y la dirección IP del servidor, sin embargo, el acceso a los usuarios estará dado por el servicio de DNS que traduce las direcciones en nombres de dominio, asignando una dirección y dominio específico para cada aplicación.

Para probar que el procedimiento es correcto y que el servidor está en funcionamiento realizamos una emulación del servidor en una máquina virtual y generamos una aplicación web la cual es una interfaz de acceso al servidor mediante un usuario y contraseña, dicha aplicación es realizada mediante código PHP y está alojada en Servidor, de esta manera se prueba que el servidor está en funcionamiento.

**Código:**

```
<!DOCTYPE html>
<html>
<head>
  <title>Bienvenido</title>
```

```
<style>
  body {
    display: flex;
    flex-direction: column;
    align-items: center;
    justify-content: center;
    height: 100vh;
    margin: 0;
    padding: 0;
    font-family: Arial, sans-serif;
    font-size: 16px;
    line-height: 1.5;
    color: #333;
  }
  h2 {
    margin-top: 0;
  }
  form {
    display: flex;
    flex-direction: column;
    align-items: center;
    border: 1px solid black;
    padding: 20px;
    background-color: #fff;
    box-shadow: 0 2px 4px rgba(0,0,0,.1);
    margin-top: 20px;
    max-width: 320px;
    width: 100%;
  }
  form label {
    display: block;
```

```
    margin-bottom: 5px;
   }
   form input[type="text"],
   form input[type="password"] {
    padding: 10px;
    border: 1px solid #ccc;
    border-radius: 4px;
    margin-bottom: 15px;
    width: 100%;
    box-sizing: border-box;
   }
   form input[type="submit"] {
    background-color: #4CAF50;
    color: #fff;
    padding: 10px 20px;
    border: none;
    border-radius: 4px;
    cursor: pointer;
    transition: background-color .3s ease;
   }
   form input[type="submit"]:hover {
    background-color: #3E8E41;
   }
  </style>
</head>
<body>
  <div>
   <h2>Interfaz de acceso</h2>
   <h2>Ingrese sus datos</h2>
  </div>
  <?php
```

```
  if ($_SERVER["REQUEST_METHOD"] == "POST") {
    // Define las credenciales válidas
    $usuarios_validos = array(
      "usuario1" => "contrasena1",
      "usuario2" => "contrasena2",
      "usuario3" => "contrasena3"
    );

    // Comprueba si se han enviado las credenciales correctas
                                    if (isset($usuarios_validos[$_POST["usuario"]]) &&
$usuarios_validos[$_POST["usuario"]] == $_POST["contrasena"]) {
      echo "<h1>Bienvenido, " . $_POST["usuario"] . "!</h1>";
    } else {
      echo "<p>Credenciales incorrectas.</p>";
    }
  }
 ?>
 <form method="post">
  <label for="usuario">Usuario:</label>
  <input type="text" id="usuario" name="usuario" required>

  <label for="contrasena">Contraseña:</label>
  <input type="password" id="contrasena" name="contrasena" required>

  <input type="submit" value="Iniciar sesión">
 </form>
</body>
</html>
```

**Visualización:**

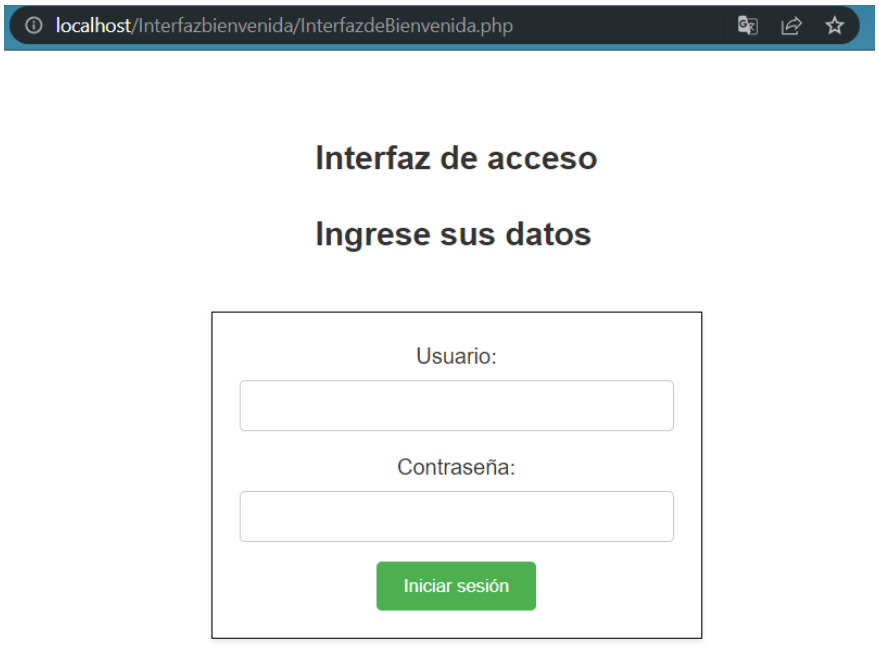



**Figura 70.** Interfaz de Acceso al Servidor.

De esta forma el Servidor ya estaría listo para alojar los servicios web requeridos ya sea migrando los servicios actuales e implementando nuevas aplicaciones web de acuerdo a los requerimientos de servicios que sean necesarios a futuro.

### 3.5.4. ROUTER CORE

**Configuración:**

La configuración del Router Cisco CRS (Carrier Routing System) se realiza a través de la interfaz de línea de comandos (CLI) utilizando el sistema operativo IOS XR de Cisco. La configuración del router incluye la configuración de interfaces, la configuración de enrutamiento, la configuración de seguridad, la configuración de servicios y otras opciones de configuración avanzadas. A continuación, se describe la configuración para un Router Cisco CRS:

- **Configurando de las interfaces:** Primero, debe configurar las interfaces en el Router Cisco CRS. Esto implica la asignación de direcciones IP a las interfaces y la activación de las interfaces para que puedan enviar y recibir tráfico de datos. Por ejemplo, para

configurar la interfaz GigabitEthernet 0/0/0/0 con la dirección IP 192.168.1.1, se puede utilizar el siguiente comando:

```
interface GigabitEthernet 0/0/0/0
ip address 192.168.1.1 255.255.255.0
shutdown
```

- **Configurando de enrutamiento:** A continuación, se debe configurar el enrutamiento en el Router Cisco CRS. Esto incluye la configuración de los protocolos de enrutamiento, la configuración de las tablas de enrutamiento y otras opciones de enrutamiento avanzadas. Para configurar el protocolo de enrutamiento BGP, aplicamos el siguiente comando:

```
router bgp 65000
bgp router-id 192.168.1.1
neighbor 192.168.1.2 remote-as 65001
```

- **Configurando de seguridad:** También se deben configurar las opciones de seguridad en el Router Cisco CRS para proteger la red contra posibles amenazas. Esto incluye la configuración de cortafuegos, la configuración de autenticación y otras opciones de seguridad avanzadas. Para configurar un cortafuego en el Router Cisco CRS aplicamos el siguiente comando:

```
ipv4 access-list ACL-IN
permit tcp any any eq 80
deny ip any any

interface GigabitEthernet 0/0/0/0
ip access-group ACL-IN in
```

Esto permite el tráfico TCP en el puerto 80 y deniega todo otro tráfico entrante en la interfaz GigabitEthernet 0/0/0/0.

- **Configurando de servicios:** Finalmente, se configuran diferentes servicios en el Router Cisco CRS, como VPN, calidad de servicio (QoS) y otros servicios avanzados. Para configurar QoS en el Router Cisco CRS, se aplica el siguiente comando:

```
policy-map QOS
class class-default
shape average 1000000000
```

service-policy POLICE

policy-map POLICE

class class-default

police cir 10000000

Esto configura una política de QoS para limitar la tasa de tráfico a 1 Gbps y para limitar la tasa de tráfico a 10 Mbps.

**Para IPv6:**

Para configurar el Router Cisco CRS para IPv6, seguimos los siguientes pasos:

- **Configurando las interfaces IPv6:** Primero, es necesario configurar las interfaces del Router CRS para que se utilice IPv6. Esto se realiza aplicando el siguiente comando en la interfaz correspondiente:

  ipv6 address <dirección IPv6>/<longitud del prefijo>

  para configurar una dirección IPv6 para la interfaz de salida 1/1/1 con una longitud de prefijo de 64, se aplica el siguiente comando:

  CRS(config)# interface TenGigE 1/1/1

  CRS(config-if)# ipv6 address 2001:db8:abcd::1/64

- **Configurando el enrutamiento IPv6:** A continuación, es necesario configurar el enrutamiento IPv6 en el Router CRS. Esto se realiza aplicando el siguiente comando:

  ipv6 unicast-routing

- **Configurando el protocolo de enrutamiento IPv6:** Después de configurar el enrutamiento IPv6, es necesario elegir un protocolo de enrutamiento IPv6 para el Router CRS. Algunos protocolos de enrutamiento IPv6 comunes son OSPFv3 y BGP. Para configurar OSPFv3, se aplica el siguiente comando:

  ipv6 router ospf <proceso-ID>

- **Configurando la publicación de prefijos IPv6:** A continuación, es necesario configurar la publicación de los prefijos IPv6 en el Router CRS para que los demás routers en la red puedan conocer los prefijos IPv6 que están conectados a este router. Esto se puede hacer aplicando el siguiente comando:

  ipv6 router ospf <proceso-ID>

ipv6 router ospf <proceso-ID> area <número-de-área> range <dirección-IPv6>/<longitud-del-prefijo> advertise

Para publicar el prefijo IPv6 2001:db8:abcd::/64 en el área 0.0.0.0 del proceso OSPFv3 1, se utilizaría el siguiente comando:

CRS(config)# ipv6 router ospf 1

CRS(config-router)# area 0.0.0.0 range 2001:db8:abcd::/64 advertise

- **Verificando la configuración IPv6:** Una vez que se haya configurado IPv6 en el Router CRS, es importante verificar la configuración para asegurarse de que todo esté funcionando correctamente. Se pueden utilizar los comandos "show ipv6 interface", "show ipv6 route" y "show ipv6 ospf" para verificar la configuración IPv6.

Siguiendo estos pasos, se configura el Router Cisco CRS para IPv6. Es importante tener en cuenta que la configuración específica puede variar según el modelo y la versión del software del Router CRS.

### 3.5.5. SWITCH DE ACCESO

**Configuración:**

La configuración de un switch Cisco Catalyst implica varios pasos y puede variar según las necesidades de la red. Realizamos una serie de procedimientos para configurar un switch Cisco Catalyst mediante comandos en la interfaz de línea de comandos (CLI):

- Conectar una computadora al puerto de consola del switch utilizando un cable de consola serie o un adaptador USB a serie.
- Se abre un programa de emulación de terminal, como PuTTY o SecureCRT, y se configura la conexión serial con los siguientes valores: velocidad de baudios: 9600, longitud de datos: 8, paridad: Ninguno, bits de parada: 1 y control de flujo: Ninguno.
- Se inicia sesión en el switch utilizando el nombre de usuario y la contraseña predeterminados. El nombre de usuario predeterminado es "cisco" y la contraseña predeterminada es "cisco" también.
- Se cambia la contraseña del modo privilegiado ingresando el siguiente comando: '**enable secret password**'. Reemplazando "password" con la contraseña deseada.

- Se configura la información básica del switch, como el nombre del switch y la dirección IP, ingresando los siguientes comandos:

```
switch> enable
switch# configure terminal
switch(config)# hostname [nombre del switch]
switch(config)# interface vlan 1
switch(config-if)# ip address [dirección IP] [máscara de subred]
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# ip default-gateway [dirección IP de la puerta de enlace predeterminada]
```

- Se configura las VLAN y los puertos que pertenecen a cada VLAN ingresando los siguientes comandos:

```
switch(config)# vlan [ID de VLAN]
switch(config-vlan)# name [nombre de VLAN]
switch(config-vlan)# exit
switch(config)# interface [nombre del puerto]
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan [ID de VLAN]
switch(config-if)# no shutdown
switch(config-if)# exit
```

- Se configura la seguridad del switch, como la autenticación de usuario y puerto, el control de tormentas de broadcast y las listas de control de acceso, ingresando los siguientes comandos:

```
switch(config)# line console 0
switch(config-line)# password [contraseña]
switch(config-line)# login
switch(config-line)# exit
switch(config)# line vty 0 15
switch(config-line)# password [contraseña]
switch(config-line)# login
```

switch(config-line)# exit
switch(config)# interface [nombre del puerto]
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security maximum 2
switch(config-if)# switchport port-security mac-address sticky
switch(config-if)# switchport port-security violation restrict
switch(config-if)# exit
switch(config)# interface range fastEthernet 0/1 - 24
switch(config-if-range)# storm-control broadcast level 5.00
switch(config-if-range)# exit
switch(config)# access-list 1 permit [dirección IP permitida]
switch(config)# interface [nombre del puerto]
switch(config-if)# ip access-group 1 in
switch(config-if)# exit

- Se configure la calidad de servicio (QoS) para priorizar el tráfico crítico en la red ingresando los siguientes comandos:

switch(config)# mls qos
switch(config)# interface [nombre del puerto]
switch(config-if)# mls qos trust cos
switch(config-if)# exit

- Se guarde la configuración ingresando el siguiente comando: **'write memory'**.

**Para IPv6:**

Para configurar un switch Cisco Catalyst 2960/9400 mediante comandos para IPv6, seguimos el siguiente procedimiento:

- **Habilitando IPv6 en el switch:**

Switch(config)# ipv6 unicast-routing

- **Configurando una dirección IPv6 global en la interfaz de administración:**

Switch(config)# interface vlan 1

Switch(config-if)# ipv6 address

<direccion_ipv6_global>/<mascara_de_red> eui-64

- **Configurando el gateway IPv6:**

  Switch(config)# ipv6 route ::/0 <direccion_ipv6_gateway>

- **Configurando una dirección IPv6 en la interfaz del puerto:**

  Switch(config)# interface <interface>

  Switch(config-if)# ipv6 address <direccion_ipv6>/<mascara_de_red>

- **Habilitando IPv6 en el puerto:**

  Switch(config)# interface <interface>

  Switch(config-if)# ipv6 enable

- **Verificar la configuración de IPv6:**

  Switch# show ipv6 interface

  Switch# show ipv6 route

### 3.5.6. CONFIGURACIÓN DE VLAN

Las VLAN se pueden configurar en un switch y/o en un router, y se pueden configurar utilizando diferentes protocolos, como IEEE 802.1Q o ISL (Inter-Switch Link). Además, se pueden configurar diferentes tipos de VLAN, como VLAN de datos, VLAN de voz, VLAN de gestión, VLAN de invitados, etc.

Para nuestro diseño aplicamos el protocolo IEEE 802.1Q que es un estándar de redes de computadoras utilizado para la implementación de VLAN (Virtual Local Area Networks). Este protocolo permite crear y mantener redes lógicas separadas en una red física compartida. Es decir, permite que varias VLAN compartan el mismo medio físico, como un switch o una conexión de red, y que cada VLAN se trate como una red separada.

El protocolo IEEE 802.1Q es un estándar utilizado para implementar VLAN y permite que varias redes lógicas compartan el mismo medio físico, mejorando la eficiencia, la escalabilidad y la seguridad de las redes.

Para crear VLANs en dispositivos Cisco mediante código, utilizamos el lenguaje de programación Python y la biblioteca Netmiko. Netmiko es una biblioteca Python que simplifica la automatización de tareas de red en dispositivos de red como routers y switches Cisco. A continuación, se realizamos código Python para crear una VLAN en un switch Cisco utilizando Netmiko:

```
from netmiko import ConnectHandler

# Definir los detalles de conexión
device = {
    'device_type': 'cisco_ios',
    'ip': '192.168.1.1',
    'username': 'admin',
    'password': 'password',
    'port': 22,
}

# Conectar al dispositivo
net_connect = ConnectHandler(**device)

# Crear la VLAN 10
vlan_id = '10'
vlan_name = 'VLAN10'
config_commands = ['vlan ' + vlan_id, 'name ' + vlan_name]
output = net_connect.send_config_set(config_commands)

# Verificar la configuración de la VLAN
show_vlan_command = 'show vlan id ' + vlan_id
output = net_connect.send_command(show_vlan_command)
print(output)
```

```
# Cerrar la conexión
net_connect.disconnect()
```

Se definen los detalles de conexión para el dispositivo Cisco, se establece la conexión con el dispositivo y se crea la VLAN 10 con un ID y un nombre específico. Luego, se verifica la configuración de la VLAN utilizando el comando "show vlan" y se cierra la conexión.

Es importante tener en cuenta que la configuración específica puede variar según el modelo y la versión del software del dispositivo Cisco, pero para el caso de los dispositivos presentados anteriormente el código realizado se aplica.

Para aplicar el protocolo IEEE 802.1Q en un switch Cisco, es necesario seguir los siguientes pasos:

- **Creando las VLAN:** Primero, es necesario crear las VLAN que se utilizarán en el switch. Esto se puede hacer utilizando el comando "vlan <vlan-id>" en la consola del switch, donde <vlan-id> es el número de identificación de la VLAN. Es necesario crear una VLAN para cada grupo de dispositivos que se desea aislar en la red.
- **Configurando los puertos de acceso:** Los puertos de acceso son los puertos del switch que se conectan a los dispositivos finales, como computadoras o impresoras. Para configurar los puertos de acceso para una VLAN específica, se utiliza el comando "switchport access vlan <vlan-id>" en la consola del switch.
- **Configurando los puertos troncales:** Los puertos troncales son los puertos del switch que se utilizan para interconectar diferentes switches y routers en la red. Para configurar un puerto como troncal, se utiliza el comando "switchport mode trunk" en la consola del switch.
- **Configurando el enlace de troncalización:** Si hay varios switches en la red y se desea interconectarlos mediante puertos troncales, es necesario configurar el enlace de troncalización (o trunking) entre los switches. Para hacer esto, se utiliza el protocolo IEEE 802.1Q en ambos extremos del enlace de troncalización.

Para habilitar el enlace de troncalización en un switch Cisco, se utiliza el comando "interface <interface-id>" para seleccionar el puerto que se desea configurar como troncal. A continuación, se utiliza el comando "switchport mode trunk" para configurar el puerto como troncal y "switchport trunk allowed vlan <vlan-list>" para permitir que las VLAN especificadas pasen por el puerto troncal.

- **Verificando la configuración:** Finalmente, es importante verificar que la configuración de la VLAN y el enlace de troncalización se haya aplicado correctamente. Para hacer esto, se pueden utilizar comandos como "show vlan" o "show interfaces trunk" en la consola del switch para mostrar la configuración actual de las VLAN y los puertos troncales.

En resumen, para aplicar el protocolo IEEE 802.1Q en un switch Cisco, es necesario crear las VLAN, configurar los puertos de acceso y troncales, configurar el enlace de troncalización y verificar la configuración.

Para aplicar el protocolo IEEE 802.1Q en el switch Cisco mediante código, utilizaremos el lenguaje de programación Python y la biblioteca Netmiko, que permite interactuar con dispositivos de red como switches y routers mediante SSH.

A continuación, se presenta cómo configurar una VLAN y un puerto de acceso para dicha VLAN en un switch Cisco mediante código Python:

```
from netmiko import ConnectHandler

# Definir los parámetros de conexión al switch
switch = {
    "device_type": "cisco_ios",
    "ip": "192.168.1.1",
    "username": "usuario",
    "password": "contraseña"
}
```

```
# Conectarse al switch
conexion = ConnectHandler(**switch)

# Crear la VLAN 10
conexion.send_command("conf t")
conexion.send_command("vlan 10")
conexion.send_command("name VLAN10")

# Configurar el puerto 1 como acceso a la VLAN 10
conexion.send_command("interface gigabitEthernet0/1")
conexion.send_command("switchport mode access")
conexion.send_command("switchport access vlan 10")

# Guardar la configuración
conexion.send_command("end")
conexion.send_command("wr mem")

# Cerrar la conexión
conexion.disconnect()
```

Se definen los parámetros de conexión al switch y se establece una conexión mediante SSH utilizando la biblioteca Netmiko. A continuación, se crea la VLAN 10 utilizando los comandos "vlan 10" y "name VLAN10", y se configura el puerto 1 como puerto de acceso a la VLAN 10 mediante los comandos "switchport mode access" y "switchport access vlan 10". Finalmente, se guarda la configuración y se cierra la conexión.

### 3.5.7. Migración de IPv4 a IPv6

Para migrar las VLANs actuales de IPv4 a IPv6 se requerimos realizar una serie de procedimientos, principalmente que la red ya se encuentra configurada en IPv6. Esto implica

configurar previamente los routers, los switches y otros dispositivos de red para que admitan IPv6. El proceso de migración será de acuerdo al siguiente procedimiento:

- Habilitar IPv6 en la VLAN: Una vez que la red está configurada para IPv6, se debe habilitar IPv6 en la VLAN que va a migrar. Esto se hace a través de la configuración del switch que está conectado a la VLAN.
- Configurar los hosts para IPv6: Todos los hosts que estén conectados a la VLAN deberán ser configurados para admitir IPv6. Esto implica configurar la dirección IPv6 en cada host y asegurarse de que los programas y servicios utilizados por los hosts admitan IPv6.
- Actualizar las políticas de seguridad: Es importante actualizar las políticas de seguridad para que incluyan IPv6. Esto implica configurar firewalls y otros dispositivos de seguridad para que admitan IPv6 y establecer políticas de seguridad adecuadas para IPv6.
- Realiza pruebas: Antes de migrar completamente la VLAN a IPv6, es importante realizar pruebas exhaustivas para asegurarse de que todo funciona correctamente. Esto implica probar la conectividad, el rendimiento y la seguridad de la red.
- Realizar la migración: Finalmente, cuando es seguro que todo funciona correctamente, se realiza la migración de la VLAN a IPv6. Esto implica deshabilitar IPv4 en la VLAN y cambiar todas las configuraciones necesarias para que la VLAN funcione completamente con IPv6.

Actualmente ya se tienen algunas VLANs activas en base a IPv4, los cuales necesariamente tendrá requerimiento de migración, las detallamos en la siguiente tabla:

| **Descripción de VLAN** | **Número ID** |
|---|---|
| Vlan de administración de equipos | 1 |
| Vlan de voz | 6 |
| Servers | 10 |
| Área desconcentrada | 24 |
| Administrativos | 25 |
| Management antenas cisco | 43 |
| Streaming tv | 50 |

| | |
|---|---|
| Management antenas ruckus | 66 |
| Clientes wifi | 99 |
| Autoridades entel | 110 |
| Laboratorios entel | 111 |
| Administrativos entel | 112 |
| Sistema CCTV | 300 |

**Tabla 24.** VLANs para migración de IPv4 a IPv6.

La configuración para habilitar IPv6 en una VLAN en un switch cisco es la siguiente:

- Primero, se asegura que el switch (Cisco) esté configurado para admitir IPv6. Para hacerlo, se debe ejecutar los siguientes comandos:

  switch(config)# ipv6 unicast-routing

  switch(config)# ipv6 cef

  Estos comandos habilitan la función de enrutamiento IPv6 y la tabla CEF de IPv6.
- A continuación, se debe crear la VLAN que se va a migrar a IPv6. Para crear una VLAN, se debe ejecutar el siguiente comando:

  switch(config)# vlan <vlan_id>

  Donde <vlan_id> es el ID de la VLAN que deseas crear.
- Una vez que has creado la VLAN, se debe habilitar IPv6 en ella. Para hacerlo, se debe ejecutar el siguiente comando:

  switch(config)# interface vlan <vlan_id>

  switch(config-if)# ipv6 address <ipv6_address>/<prefix_length>

  Donde <ipv6_address> es la dirección IPv6 que deseas asignar a la VLAN y <prefix_length> es la longitud del prefijo de la dirección IPv6.
- Finalmente, se debe configurar el switch para que enrute el tráfico IPv6 a través de la VLAN. Para hacerlo, se debe ejecutar el siguiente comando:

  switch(config)# ipv6 route <ipv6_network>/<prefix_length> <next_hop>

  Donde <ipv6_network> es la red IPv6 que deseas enrutar a través de la VLAN, <prefix_length> es la longitud del prefijo de la red IPv6 y <next_hop> es la dirección IPv6 del siguiente salto.

Con este procedimiento de configuración, se habrá habilitado IPv6 en la VLAN en el switch (Cisco) y se tendría la migración realizada.

### 3.5.8. TELEFONÍA IP

La activación del servicio de telefonía IP sobre un servidor implica una serie de pasos y configuraciones. A continuación, se presentan los pasos generales para activar el servicio de telefonía IP sobre el servidor:

- Se adquiere el software de telefonía IP adecuado. Hay varios softwares disponibles, como Asterisk, FreeSWITCH, 3CX, entre otros. Nos asegúramos de elegir el software que se ajuste a nuestras necesidades y requerimientos.
- Se configura y prepara el servidor para la instalación del software. El servidor debe tener suficiente capacidad de procesamiento, memoria y almacenamiento para ejecutar el software de telefonía IP. Nos aseguramos que el servidor esté actualizado y configurado correctamente.
- Se instale el software de telefonía IP en el servidor y se realiza las configuraciones necesarias. Esto puede incluir la configuración de troncales, extensiones, colas de llamadas, opciones de seguridad, enrutamiento de llamadas, entre otras.
- Se configura y conecta los dispositivos de telefonía IP al servidor. Estos pueden ser teléfonos IP, softphones o aplicaciones de telefonía IP. Configure cada dispositivo de acuerdo al modelo y protocolo de comunicación.
- Se realiza pruebas y verificaciones de funcionamiento. Se realiza llamadas de prueba y se verifica que el audio se escuche correctamente, que las llamadas se enruten correctamente y que todas las funciones de la telefonía IP estén operativas.
- Se ajusta y optimiza el sistema. Realizando ajustes y optimizaciones de acuerdo a las necesidades y requisitos del servicio de telefonía IP.
- Se pone en marcha el servicio. Una vez que se han realizado todas las configuraciones y ajustes, y se han verificado y optimizado todas las funciones, el servicio de telefonía IP estará listo para ser utilizado.

Para nuestro diseño el software elegido es Asterisk, ya que por sus características y manejo cumple con lo necesario para la activación del servicio de telefonía IP en el servidor.

Asterisk es un software de telefonía IP de código abierto con una amplia variedad de características avanzadas de telefonía, flexibilidad, compatibilidad con una amplia variedad de protocolos, integración con otras aplicaciones, escalabilidad y soporte de la comunidad.

**Instalación y Configuración Servidor VoIP:**

Para instalar y configurar Asterisk en el servidor, se realiza el siguiente procedimiento:

- **Actualizar el sistema operativo:** Antes de instalar Asterisk, es importante actualizar el sistema operativo del servidor. Dependiendo de la distribución de Linux que esté utilizando, se utilizan los siguientes comandos para actualizar el sistema:

  CentOS/RHEL: yum update -y

  Ubuntu/Debian: apt-get update && apt-get upgrade -y
- **Descargar e instalar Asterisk:** Se descarga e instala Asterisk utilizando el siguiente comando en la terminal:

  CentOS/RHEL: yum install asterisk -y

  Ubuntu/Debian: apt-get install asterisk -y
- **Configuración de Asterisk:** Una vez instalado Asterisk, se puede configurar el archivo de configuración principal de Asterisk, llamado "sip.conf", utilizando el siguiente comando:

  nano /etc/asterisk/sip.conf

  Este comando abrirá el archivo de configuración "sip.conf" en el editor de texto "nano". Aquí se puede agregar extensiones, troncales, usuarios y otras configuraciones de SIP para su sistema telefónico.
- **Configuración de las extensiones:** Para agregar extensiones, se agregan las siguientes líneas al archivo "sip.conf":

  [1000] ;Número de extensión

  type=friend ;Tipo de extensión (amigo)

  username=1000 ;Nombre de usuario

secret=mipassword ;Contraseña de la extensión

host=dynamic ;Host dinámico

- Configuración de las troncales: Para agregar troncales, se agrega las siguientes líneas al archivo "sip.conf":

  [mytrunk] ;Nombre de la troncal

  type=peer ;Tipo de troncal (par)

  host=123.123.123.123 ;Dirección IP de la troncal

  username=myusername ;Nombre de usuario de la troncal

  secret=mypassword ;Contraseña de la troncal

- **Pocediendo a reiniciar Asterisk:** Después de configurar "sip.conf", se reinicia Asterisk para aplicar los cambios utilizando el siguiente comando:

  CentOS/RHEL: systemctl restart asterisk

  Ubuntu/Debian: service asterisk restart

- **Para verificar que Asterisk esté en funcionamiento:** Verificando que Asterisk esté en funcionamiento utilizando el siguiente comando:

  asterisk -rvvv

  Este comando permite ingresar al intérprete de comandos de Asterisk y verificar que Asterisk esté ejecutándose correctamente.

Mediante la siguiente grafica se representa el funcionamiento de la telefonía IP en el servidor del data center.

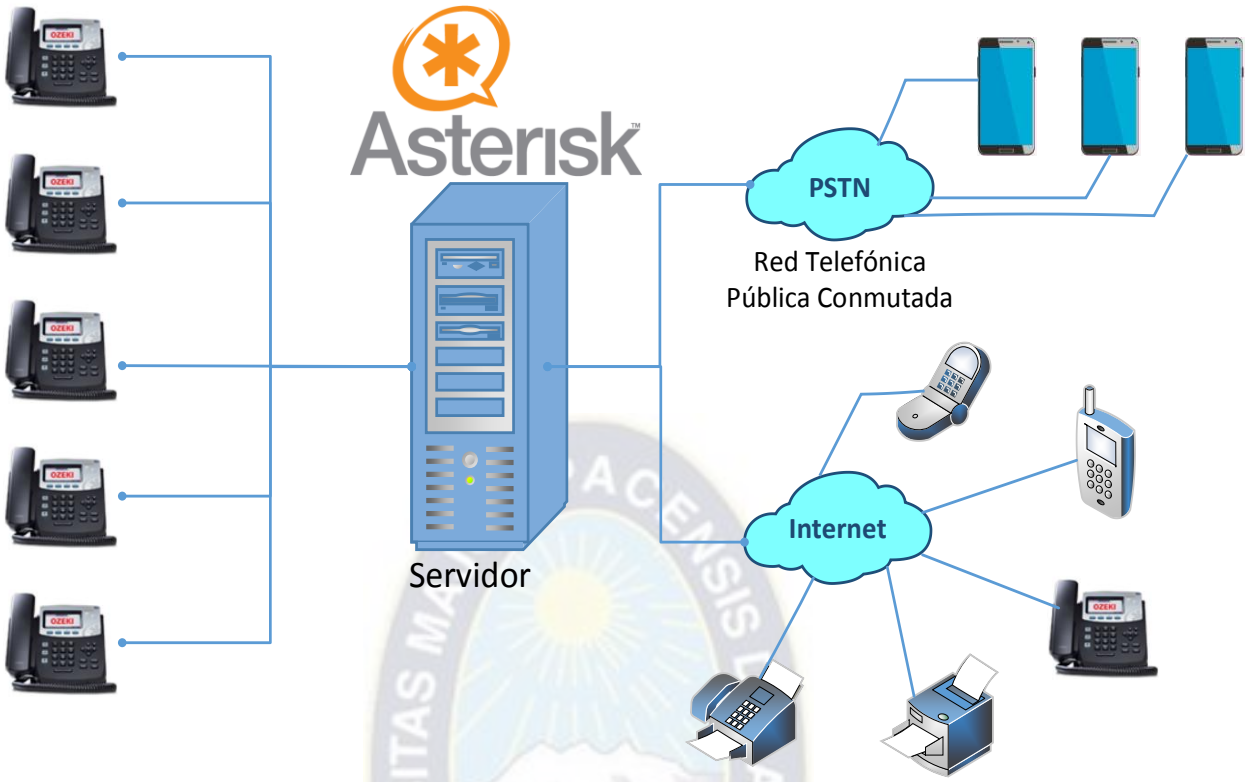



**Figura 71**. Representación gráfica del servicio de Telefonía IP.

### 3.5.9. VIRTUALIZACIÓN

Pasos del proceso de Virtualización:

- **Descargando e instalando el hipervisor de VMware en el servidor Linux:** VMware ofrece varias opciones de hipervisores para Linux, como ESXi o VMware Workstation Player. Elegimos el hipervisor que mejor se adapte a las necesidades.
- **Creando una nueva máquina virtual:** Una vez instalado el hipervisor, se utiliza la interfaz de administración para crear una nueva máquina virtual. Se seleccionan las especificaciones de hardware para la VM, como el número de núcleos de CPU, la cantidad de memoria y el espacio de almacenamiento. También se debe seleccionar la imagen ISO del sistema operativo que deseamos instalar en la máquina virtual.
- **Instalando el sistema operativo en la máquina virtual**: Una vez que la máquina virtual está creada, se inicia la VM y se sigue el proceso de instalación del sistema operativo como se haría en una máquina física.

- **Configurando la red**: Una vez instalado el sistema operativo en la máquina virtual, se configura la conexión de red para la VM. Se puede seleccionar entre varias opciones de red, como una conexión NAT o una conexión de puente.
- **Instalando las aplicaciones necesarias**: Una vez configurada la red, se instalan las aplicaciones y servicios necesarios en la máquina virtual. Se pueden instalar aplicaciones como servidores web, bases de datos, servidores de correo electrónico, etc.
- **Realizando copias de seguridad**: Es importante realizar copias de seguridad regulares de las máquinas virtuales para asegurarte de que los datos estén protegidos en caso de un fallo del sistema.

Con la realización de estos procedimientos se tienen virtualizados los servidores físicos. La configuración del servidor físico con sistema operativo Linux y VMware depende del hardware del servidor y de los requisitos de los sistemas a virtualizar. A continuación, generamos el proceso de configuración el servidor para la virtualización de los servidores físicos que existen actualmente en la Facultad de Ingeniería los cuales fueron mencionados:

- **Creando una red virtual en VMware.** Esto permitirá que las máquinas virtuales se comuniquen entre sí y con el exterior. Para ello, utiliza los siguientes comandos:

```
# Crear una red virtual
sudo vmware-networks --start
sudo vmware-networks --stop
sudo vmware-networks --start
```

- **Creando las máquinas virtuales.** Para crear cada máquina virtual, se puede utilizar la interfaz gráfica de VMware o la línea de comandos. A continuación, se muestra cómo crear una máquina virtual con VMware en la línea de comandos:

```
# Crear una máquina virtual llamada "Servicios web"
vmware-cmd --config /ruta/a/vm/Servicios_web.vmx --create

# Asignar 2 núcleos de CPU a la máquina virtual
vmware-cmd /ruta/a/vm/Servicios_web.vmx -v 2
```

```
# Asignar 4 GB de memoria RAM a la máquina virtual
vmware-cmd /ruta/a/vm/Servicios_web.vmx -m 4096

# Asignar un disco duro virtual de 100 GB a la máquina virtual
vmware-cmd /ruta/a/vm/Servicios_web.vmx -hdd /ruta/a/disco/virtual.vmdk -d ide

# Configurar la máquina virtual para que arranque desde una ISO
vmware-cmd /ruta/a/vm/Servicios_web.vmx --setoption guestos --set-value "linux"

# Iniciar la máquina virtual
vmware-cmd /ruta/a/vm/Servicios_web.vmx start
```

Se repite estos comandos para crear todas las máquinas virtuales necesarias.

- **Configurando la red de cada máquina virtual.** Para ello, utiliza los siguientes comandos:

```
# Configurar la red de una máquina virtual llamada "Servicios web"
vmware-cmd /ruta/a/vm/Servicios_web.vmx --set-network-adapter eth0 --network-name VMnet1

# Configurar la dirección IP de la máquina virtual
ifconfig eth0 192.168.1.100 netmask 255.255.255.0
```

Se repite estos comandos para configurar la red de todas las máquinas virtuales.

Realizando estos procedimientos el servidor ya está listo para entrar en funcionamiento, mediante las configuraciones realizadas se podrá migrar las funciones de los servidores físicos y aumentar más máquinas virtuales si es que existe el requerimiento. Todos estos procesos podrán ser llevados a cabo considerando que se cuenta con un servidor físico de alta gama para garantizar que todas las funcionalidades no presenten problemas, de esta manera el usuario no vea ninguna diferencia con respecto a los servidores físicos.

A continuación, representamos la Red de edificio con los servicios disponibles a usuario final con acceso al Data Center con topología en árbol:

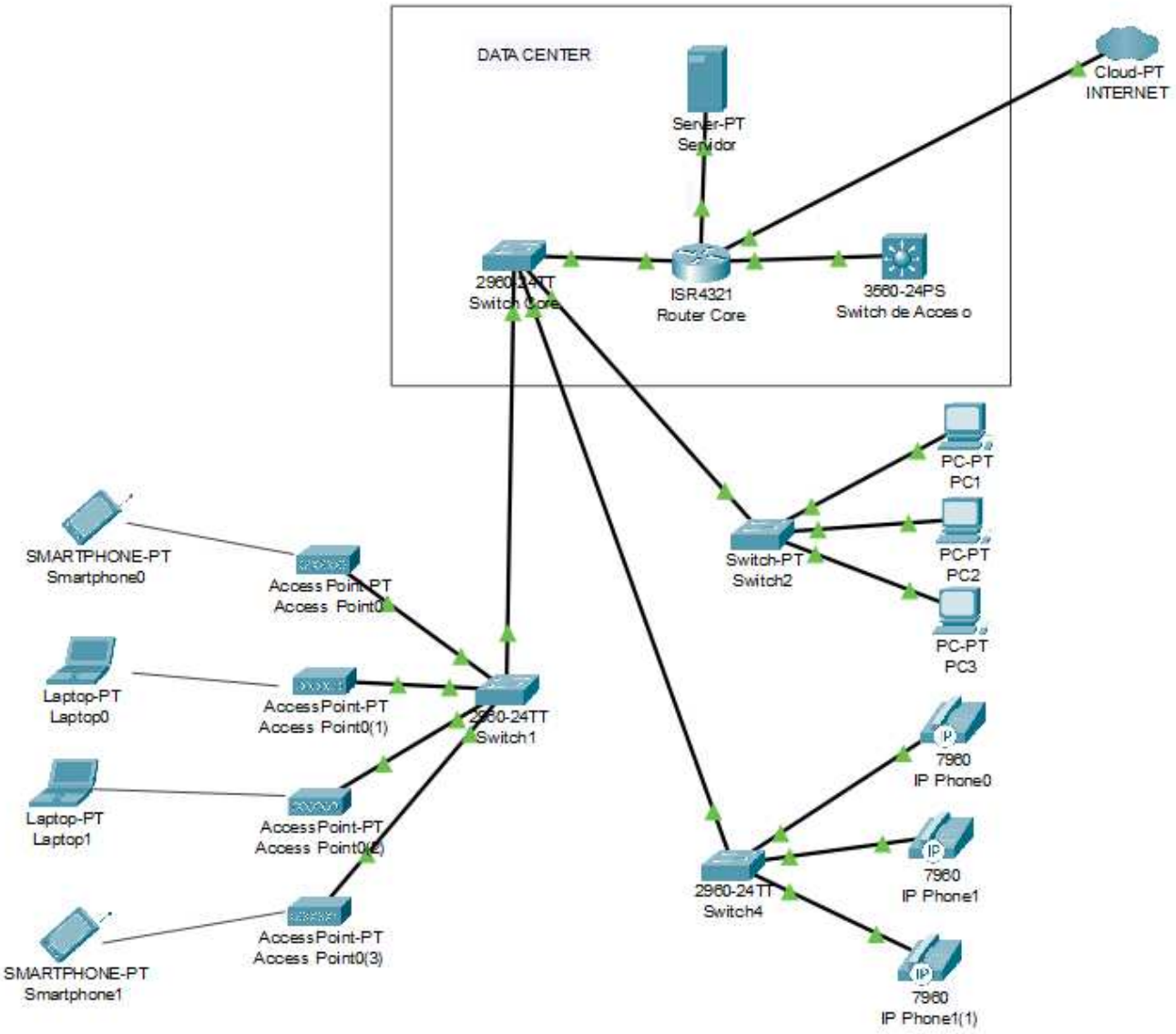



**Figura 72.** Representación de la Red a usuario final.

# 3. CAPÍTULO IV

## 3.1. CONCLUSIONES

En el presente proyecto se lograron realizar los objetivos planteados en cuanto a la planificación, dimensionamiento y diseño, a través de metodologías y estándares que nos guían en este proceso, realizando una serie de procedimientos detallados con el fin de tener el diseño de una Data Center completo, tanto en Infraestructura IT (*equipamiento informático*) así como en Infraestructura Critica (*facilities*) que tiene capacidad de brindar una serie de servicios y al cual los usuarios puedan conectarse de forma fácil y segura.

El diseño del Data Center es un proceso complejo y crítico para garantizar la fiabilidad, disponibilidad y seguridad de los servicios y datos que se alojan en él. Tomando en cuenta las necesidades actuales en cuanto a servicios digitales para la Facultad de Ingeniería se desarrolló este proyecto, tratando de abarcar varios aspectos que consideramos importantes tanto en infraestructura física y lógica como se mostró en toda la parte de ingeniería del proyecto.

Una de las tareas principales del diseño del Data Center es garantizar la disponibilidad continua de los servicios. La redundancia se refiere a la incorporación de sistemas de respaldo y duplicación que se emplea en el Data Center para minimizar la posibilidad de interrupciones del servicio. Al diseñar el Data Center, nos aseguramos de que los sistemas críticos tengan redundancia en base al nivel de disponibilidad seleccionado, incluyendo la alimentación eléctrica en base a equipos de respaldo, la refrigeración de los equipos informáticos y la conectividad de red.

Para el diseño eficiente del Data Center, la solución planteada hace posible reducir el consumo de energía. El uso de sistemas de enfriamiento de alta eficiencia, la consolidación de servidores y la virtualización ayudan a reducir el consumo de energía y el costo asociado.

La seguridad es un aspecto importante en el diseño del Data Center. Las medidas de seguridad físicas y lógicas adecuadas, como el control de acceso, la monitorización de seguridad y la detección de intrusiones, son fundamentales para garantizar la protección de los datos y los servicios alojados en el centro de datos, consideramos todos estos aspectos en el micro data center y consideramos configuraciones en los equipos con estas medidas de seguridad.

Es importante destacar que el diseño del Data Center es escalable y puede adaptarse a las necesidades cambiantes en los servicios que se presentan en la Facultad de Ingeniería. Al diseñar el Data Center, se tomó en cuenta la posibilidad de expansiones y la capacidad de actualizar los sistemas y la infraestructura para satisfacer las necesidades crecientes de los servicios alojados.

## 3.2. RECOMENDACIONES

Se recomienda principalmente un monitoreo constante del funcionamiento de los equipos y los servicios del Data Center para de esta manera evitar fallas o posibles problemas a futuro, realizar un análisis de trafico IP para optimizar el uso de recursos. Plantear también se realice un análisis de la calidad de energía para verificar las condiciones externas que puedan afectar sobre todo a toda la parte informática y electrónica en el Data Center.

El Data Center actualmente se encuentra ubicado en el sexto piso del edificio de la Facultad de Ingeniería, se debe considerar la cercanía a fuente de energía de tipo trifásica del tipo estrella donde se incluya el neutro.

También otorgar las facilidades a los proveedores de conectividad de red ISP (Internet Service Provider) Un ODF de distribución dentro el edificio, de manera que nuevos cableados sean realizados sin dificultad.

Es importante que el diseño del Data Center cuente con la capacidad de crecer y adaptarse a las necesidades de la institución ante nuevos servicios y aplicaciones.

Se recomienda que todos los sistemas críticos, como los equipos de alimentación eléctrica, equipos de refrigeración y la conectividad de red, deben tener una duplicación o respaldo en caso de fallos, nuestra solución está planteada para migrar a un sistema con redundancia (escalable), lo cual tratamos de garantizar en la parte del desarrollo recomendando que las copias de seguridad sean realizadas en otro servidor fuera del edificio de la Facultad de ingeniería, que por lo usual se lo denomina Centro Alterno de Respaldo.

Los Centros de Datos son conocidos por ser grandes consumidores de energía. Por lo tanto, se recomienda que nuevas ampliaciones del Data Center debe enfocarse en minimizar el

consumo de energía y maximizar la eficiencia energética, utilizando tecnologías como la virtualización y la consolidación de servidores. También en la parte de la infraestructura critica (*facilities*), sistemas de enfriamiento del tipo Free Cooling permiten un ahorro de energía.

Es importante que el Centro de Datos tenga un sistema de monitoreo de recursos informáticos y gestión efectiva para garantizar el rendimiento óptimo y la disponibilidad continua de los servicios. Se recomienda implementar herramientas de monitoreo y gestión de sistemas, ya sea bajo Plataforma Windows y/o Linux, además asegurarse de que el personal de sistemas, encargado de operar el Data Center tenga la capacitación necesaria ante desastres y fallas del sistema.

## 3.3. BIBLIOGRAFIA


Santiago Borges (20 de Octubre de 2020). *Servidor blade: Características y Modelos Populares*. Infranetworking: https://blog.infranetworking.com/servidor-blade/

Jose Miguel Salinas Gomez (5 de Junio de 2021). *Hiperconvergencia. ¿Qué es y cómo funciona?* blogvisionarios: https://blogvisionarios.com/articulos-sistemas/hiperconvergencia-que-es-y-como-funciona/

LAGE. (6 de Junio de 2019). *Servidores*. Lage - Blog: https://www.lage.com.mx/blog/servidor-torre-caracteristicas-ventajas

Hewlett Packard (2022). *Infraestructura convergente*. hpe: https://www.hpe.com/es/es/what-is/converged-infrastructure.html

Alberto Saavedra (13 de Febrero de 2018). *Clave i Infraestructura IT, Transformación Digital*. Clave i:

https://www.clavei.es/blog/infraestructura-tecnologica/#:~:text=%C2%BFQui%C3%A9n%20utiliza%20la%20infraestructura%20de,resultados%20positivos%20en%20los%20negocios.

GSC. (2022). *5 tipos de terminales informáticas*. gscmadrid: https://gscmadrid.com/tipos-de-terminales-informaticas/

Joseé Luis Cuevas Ruíz (Enero de 2020). *IMPACTO DE LOS DISPOSITIVOS TERMINALES MOVILES*. Centro de Estudios. IFT: https://centrodeestudios.ift.org.mx/admin/files/estudios/1626657199.pdf

Víctor Gabriel Galván (Ediciones Índigo, Tucumán, 2013). DATACENTER UNA MIRADA POR DENTRO. 1ra Edición.

MundoContact (22 de Agosto de 2016). *Tendencias de almacenamiento en Data Centers*. Mundo Contact: https://mundocontact.com/7-tendencias-de-almacenamiento-en-data-centers/

Quesignificado (s.f.). *Significados, conceptos y definiciones*. QueSignifcado: https://quesignificado.org/que-es-una-terminal-de-computadora/

Diego Fernando Torrez Zambrano (Quito, 2013). *DISEÑO DEL DATA CENTER PARA CERT-ECUADOR*: Escuela Politécnica Nacional - Facultad de Ingenieria Eléctrica y Electrónica.

Margaret Rouse (2022). *Copia de seguridad o respaldo*. ComputerWeekly: https://www.computerweekly.com/es/definicion/Copia-de-seguridad-o-respaldo

VMware. (2022). *Seguridad del centro de datos*. vmware: https://www.vmware.com/latam/topics/glossary/content/data-center-security.html

kionetworks. (2022). *Data Centers*. KIO Networks: https://www.kionetworks.com/blog/data-center/qu%C3%A9-es-un-data-center#:~:text=Un%20Data%20Center%2C%20o%20%E2%80%9Ccentro,o%20un%20sistema%20de%20computadoras%2C

next_u. (2022). *Cableado Estructurado*. next_u Blog: https://www.nextu.com/blog/cableado-estructurado-que-es-rc22/#:~:text=Cuando%20hablamos%20del%20cableado%20estructurado,emisores%20hasta%20los%20receptores%20correspondientes.

qualtytech. (2022). *Cableado Estructurado*. Quality Technology: https://qualtytech.com/productos/cableado-estructurado/

Castillo, J. A. (9 de Diciembre de 2018). *Que son las Redes*. Profecionales Review: https://www.profesionalreview.com/2018/12/09/redes-lan-man-wan/#:~:text=Una%20red%20LAN%20o%20Local,un%20edificio%2C%20planta%20o%20habitaci%C3%B3n.

Ionos. (8 de Diciembre de 2022). *¿Qué es Ethernet (IEEE 802.3)?* Digital Guide IONOS: https://www.ionos.es/digitalguide/servidores/know-how/ethernet-ieee-8023/#:~:text=%C2%BFQu%C3%A9%20es%20Ethernet%20(IEEE%20802.3,habitualmente%20como%20una%20tecnolog%C3%ADa%20LAN.

Marta Rico. (11 de Abril de 2018). *Actualidad en cables y conexión electrónica*. telecocable: https://www.telecocable.com/blog/tipos-de-fibra-optica-monomodo/1577

Fluke. (2020). *Fibra OM1, OM2, OM3, OM4, OM5y OS1, OS2*. FLUKEnetworks: https://es.flukenetworks.com/knowledge-base/copper-testing/om1-om2-om3-om4-om5-and-os1-os2-fiber

Rene Sanchez Vera. (2011). *Redes y Telecomunicaciones*. dyndns: http://ual.dyndns.org/biblioteca/Redes/Docs/Inicio.html

Worton. (6 de Julio de 2021). *Fibra monomodo y multimodo*. Obtenido de FS community: https://community.fs.com/es/blog/single-mode-vs-multimode-fiber-whats-the-difference.html

Jordi Salazar. (Versión de prueba, Praha 6, Czech Republic 2022). *REDES INALÁMBRICAS.*

Juan José Yunquera Torres. (2017). *EL ESTÁNDAR IEEE 802.11*. DOCPLAYER: https://docplayer.es/22789056-Capitulo-3-el-estandar-ieee-802-11.html

Anthony Bruno, Steve Jordan. (2011). *CCDA 640-804 Official Cert Guide, 4th Edition*

Jhon Tiso. (2011). *Designing Cisco Network Service Architectures (ARCH) Foundation Learning Guide (CCDP ARCH 642-874).*

Daniel Fabian Niño Vasquez, (2020). DISEÑO DE UN MODELO DE VIRTUALIZACION PARA LA IMPLMENTACION DE UN SISTEMA DE SERVIDORES EN ALTA DISPONIBILIDAD.

pagina
en blanco

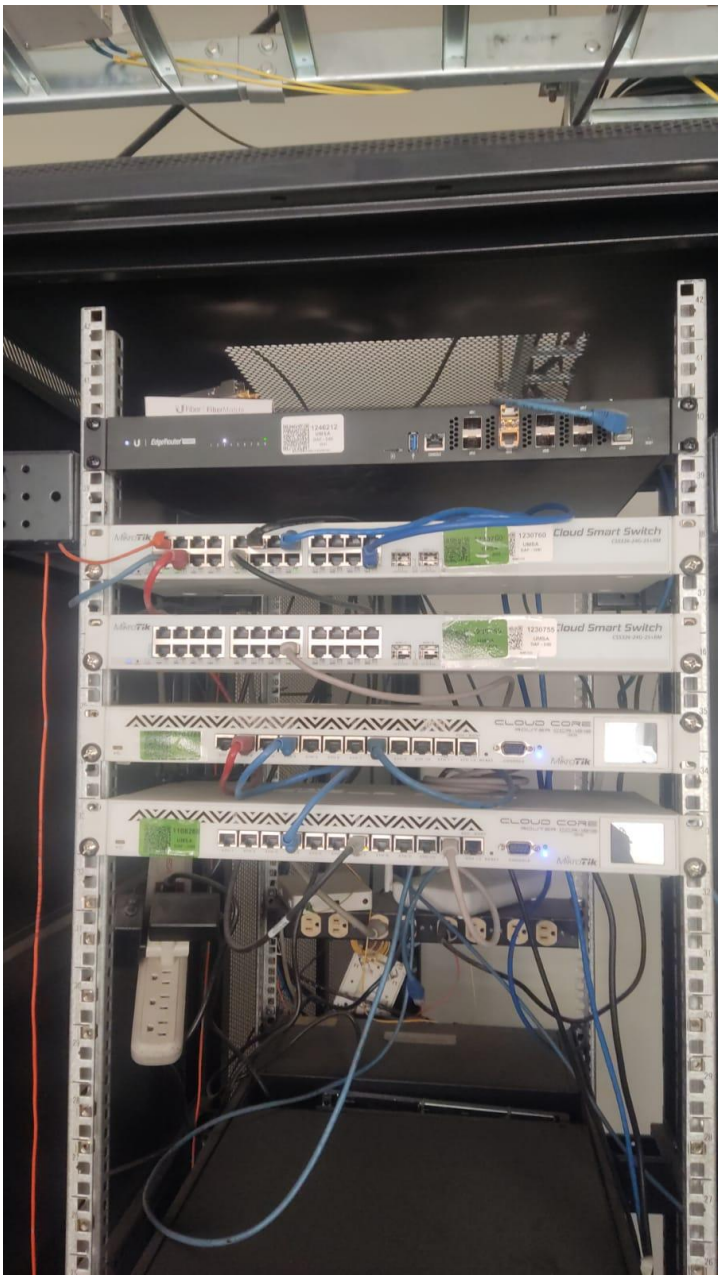
## 3.4. ANEXOS

### ANEXO A: Equipos y Ambiente del Data Center en la actualidad

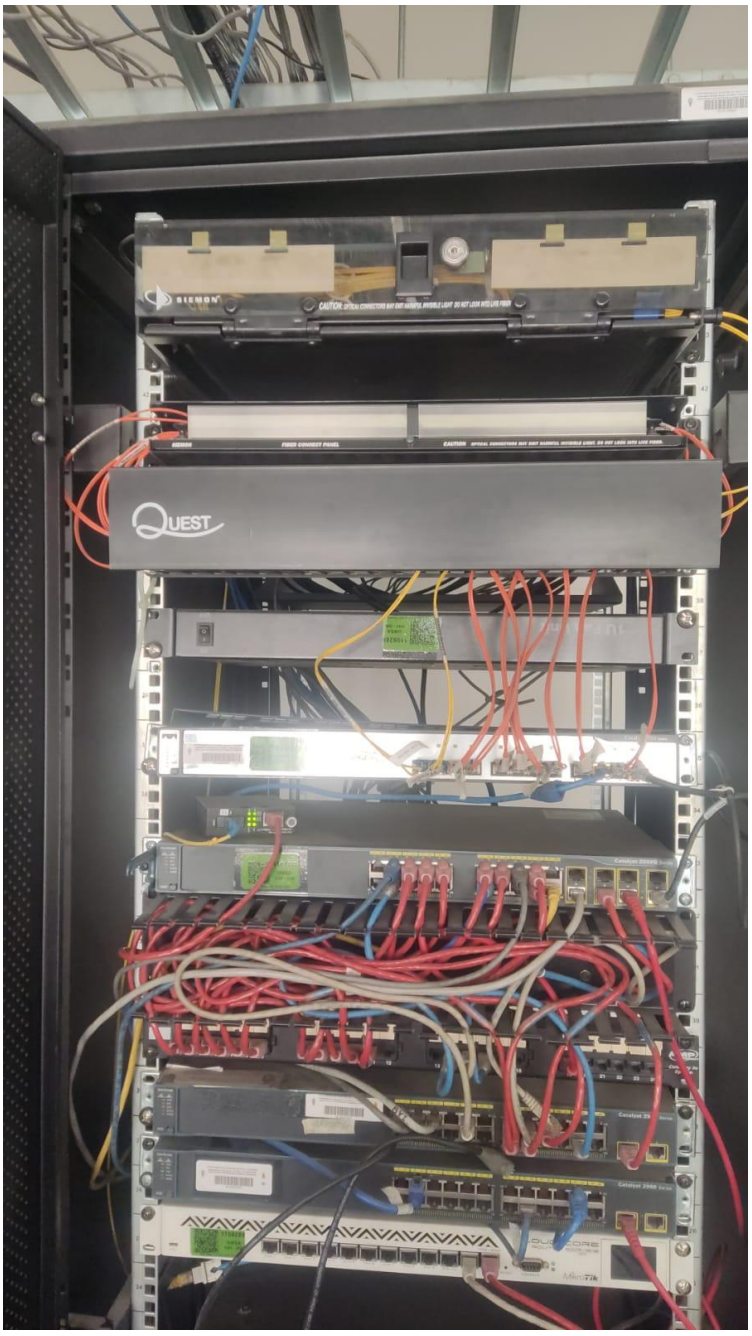
**Racks en la actualidad:**

**Equipos de Telefonía IP, Servidores y Switch en el Rack 1:**


**Switchs, Routers y Servidores en el Rack 2:**

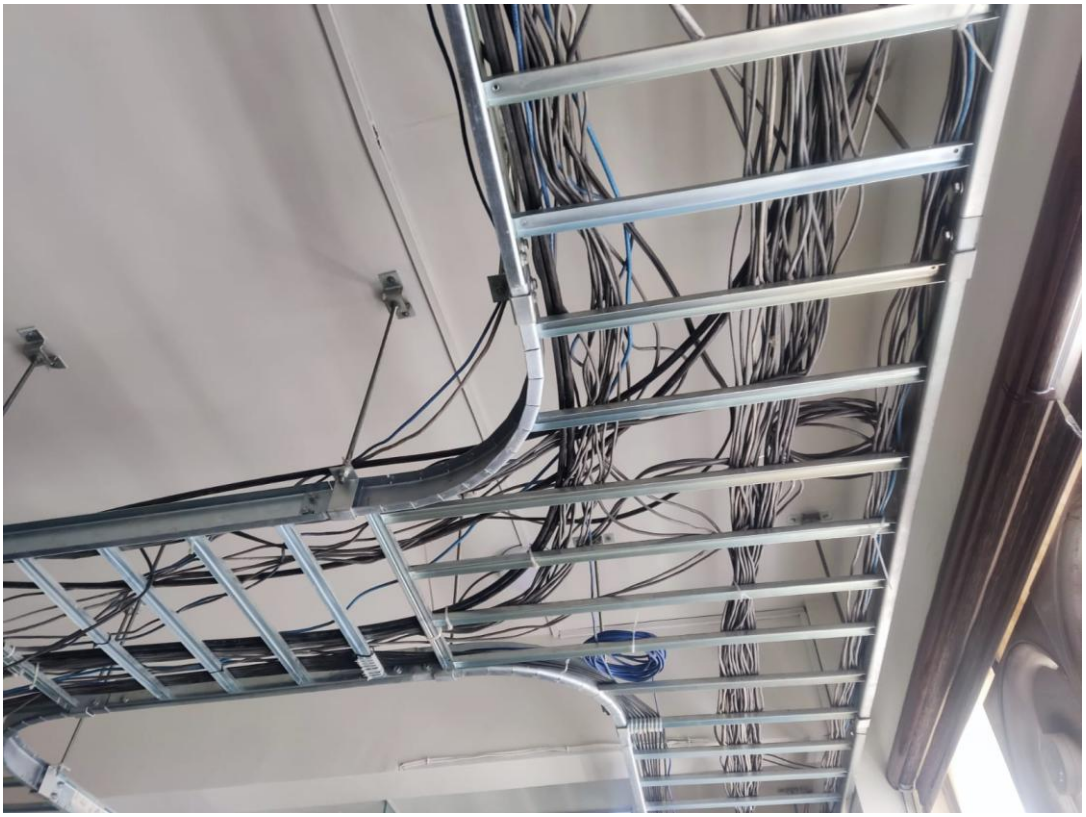



**Switchs, Routers y Servidores en el Rack 3:**



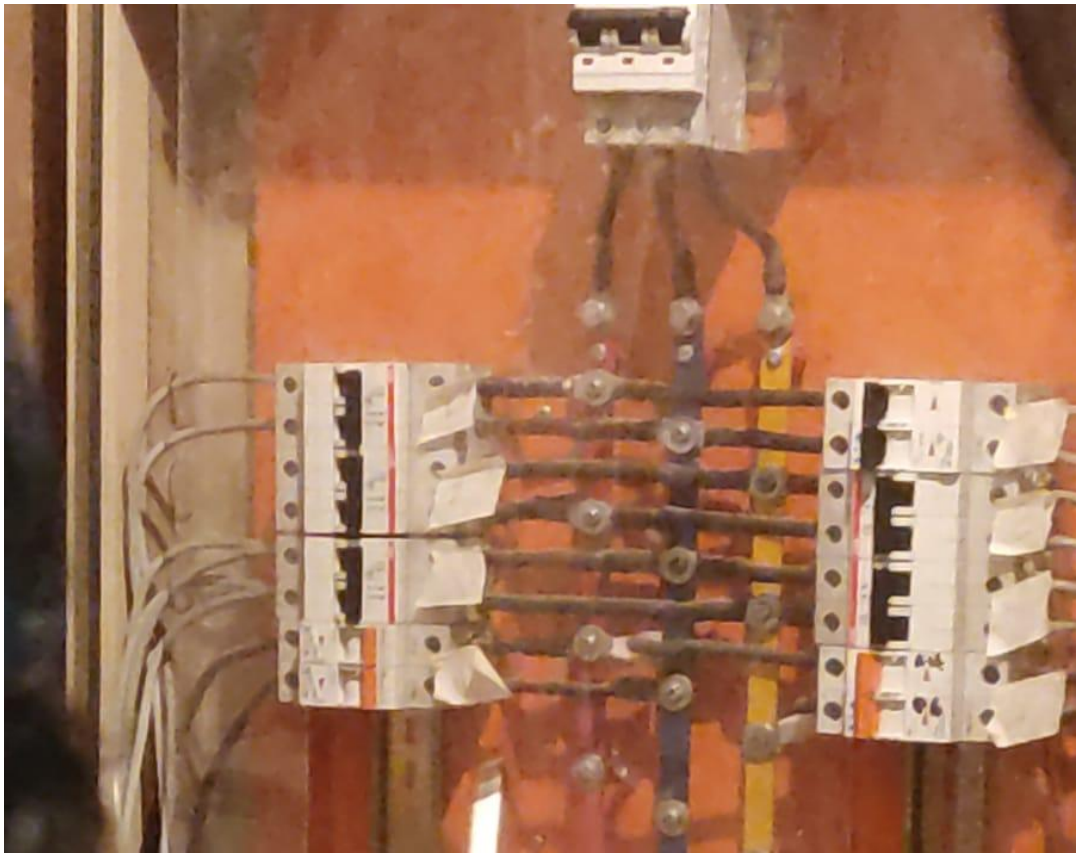
**Gabinetes actualmente:**

**Escalerilla actualmente:**



**Data Center actual:**

**Tablero Eléctrico actual:**



# APENDICE B.

## ANÁLISIS ECONÓMICO

Diseño de Centro de Datos e Infraestructura Tecnológica de Información y Comunicación para la Facultad de Ingeniería U.M.S.A.

| A. INFRAESTRUCTURA TECNOLOGICA DEL EDIFICIO DE LA FACULTAD DE INGENIERIA | | | | | |
|---|---|---|---|---|---|
| **ITEM** | **DESCRIPCION** | **CANTIDAD** | **UNIDAD** | **COSTO U. Bs.** | **COSTO T. Bs.** |
| 1 | Cable UTP Categoría 6A (10 Gbps) | 9983 | mt | 12,00 | 119.790 |
| 2 | Caja de sobreponer de Pared | 331 | pza | 15,00 | 4965,00 |
| 3 | Rosetas RJ-45 Cat 6A | 662 | pza | 55,00 | 36410,00 |
| 4 | Cable Canal PVC 50x100 mm 2 metros/pza, blanco (25 pza/planta, para 12 plantas) | 300 | pza | 40,00 | 12000,00 |
| 5 | Mano de Obra , cableado e instalación de puntos de red Cat 6A | 662 | pza | 70,00 | 46340,00 |
| 6 | Fibra Óptica Multimodo OM3 Cubierta de PVC, de 24 hilos ANSI/TIA-598 | 70 | mt | 80,00 | 5600,00 |
| 7 | Kit de adaptadores ópticos 6F MM LC-PC | 20 | pza | 210,00 | 4200,00 |
| | Kit 3X placa para adaptadores ópticos 8 posiciones LC/SC | 20 | pza | 305,00 | 6100,00 |
| 8 | Cordon dúplex MM (50.0) OM3 10 GigaBit LC-SPC/LC-SPS 1.5 mts | 20 | pza | 245,00 | 4900,l00 |
| 9 | Pig Tail MM (50.0) OM3 10 GigaBit LC-SPC/LC-SPS 1.5 mts | 20 | pza | 235,00 | 4700,00 |
| 10 | Certificación puntos de red Cat6A | 331 | pza | 200,00 | 66200,00 |
| 11 | Fusión de Puntos | 40 | pza | 150,00 | 6000,00 |
| 12 | Entrada de Acometida | 1 | global | 3000,00 | 3000,00 |
| 13 | Switch de Acceso CISCO Series 9200 | 10 | pza | 26960 | 269000,00 |
| 14 | Mano de Obra , cableado e instalación de backbone de Fibra Optica OM3 | 1 | global | 3000,00 | 3000,00 |
| 15 | Cable Canal 25x25 mm 2 metros/pza, blanco (25 pza/planta, para 12 plantas) | 300 | pza | 7,00 | 2100,00 |
| 16 | Patch Panel descargado 24 puertos | 12 | pza | 550,00 | 6600,00 |
| | | | | **COSTO TOTAL:** | **554565,00 Bs.** |
| **A._COSTO TOTAL:** | | | | | **554565,00 Bs.** |

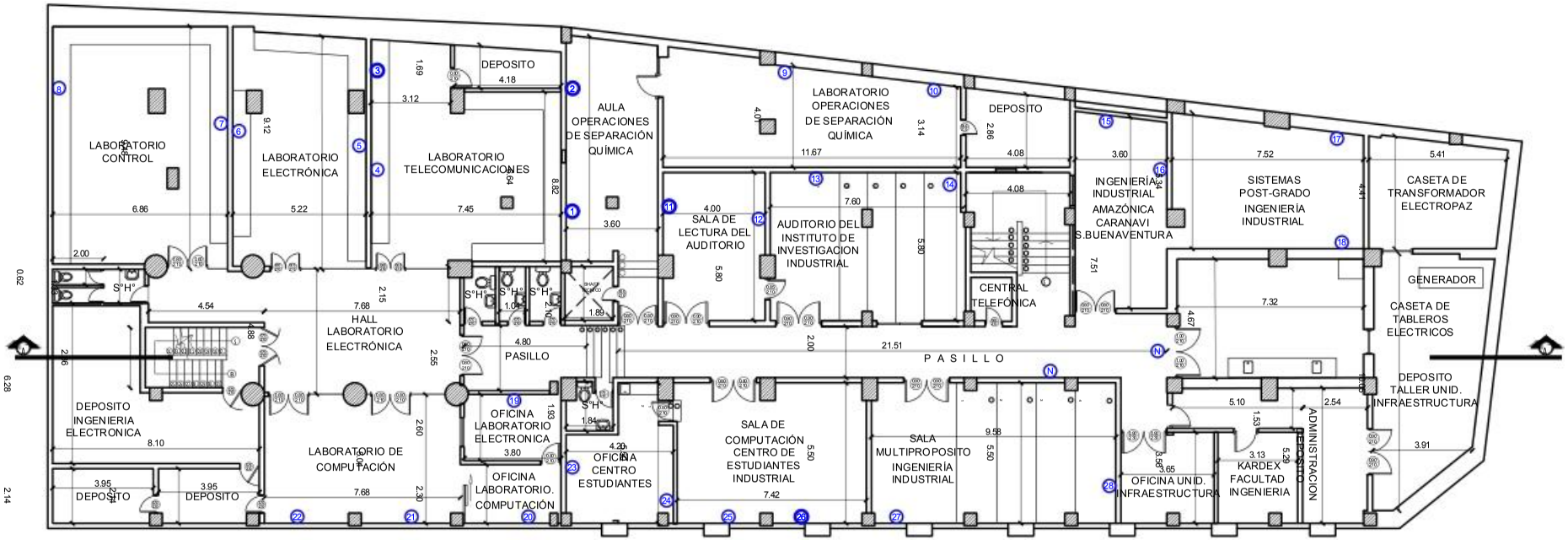
| B1. INFRAESTRUCTURA DEL CENTRO DE DATOS (IngeTIC) | | | | | |
|---|---|---|---|---|---|
| **INFRAESTRUCTURA TECNOLOGICA DEL DATA CENTER (*equipamiento informático*)** | | | | | |
| **ITEM** | **DESCRIPCION** | **CANTIDAD** | **UNIDAD** | **COSTO U. Bs.** | **COSTO T. Bs.** |
| 1 | Switch de Distribución CISCO 9400 | 1 | pza | 60000,00 | 60000,00 |
| 2 | Router de Core, CISCO Router 8000 Series | 1 | Pza | 530000,00 | 530000,00 |
| 3 | Servidor DELL PowerEdge R470xd<br>- 2 procesadores, mínimo 22 núcleos cada procesador (Intel Xeon Gold 6152 2,1 Ghz o superior).<br>- Memoria RAM 256 GB RDIMM<br>- Licencia VMWare VSphere versión 6.7 o superior<br>- *Debe incluir instalación, configuración y soporte.* | 1 | Pza | 235000,00 | 235000,00 |
| 4 | Dispositivo de almacenamiento SAN de HP modelo *MSA 2040 SFF Storage* | 1 | pza | 50000,00 | 50000,00 |
| 5 | Rack de Piso 42U | 1 | pza | 28000,00 | 56000,00 |
| 6 | Patch panel descargado Cat6A 24 puertos | 4 | pza | 700,00 | 2800,00 |
| 7 | Mini GBIC SFP, LC conector 550 metros | 20 | pza | 5000,00 | 5000,00 |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Patch Panel descargado 24 puertos | 2 | pza | 550,00 | 1100,00 |
| 9 | Ordenador de cables 1 RU | 2 | pza | 150,00 | 300,00 |
| | | | | **COSTO SUBTOTAL:** | **940230,00** |

| **B2. INFRAESTRUCTURA CRITICA DEL DATA CENTER (*facilities*)** | | | | | |
|---|---|---|---|---|---|
| **ITEM** | **DESCRIPCION** | **CANTIDAD** | **UNIDAD** | **COSTO U. Bs.** | **COSTO T. Bs.** |
| 1 | SISTEMA MICRO DATA CENTER, ATP 06F, incluye<br>-Alimentación eléctrica regulada (UPS), 6KVA.<br>- Aire acondicionado de precisión (CRAC), 5,6 KW.<br>- *Sensores de Temperatura, Humedad relativa, humo y líquido.*<br>- Control de Acceso electrónico biométrico y registros.<br>- Control de seguridad con cámara frontal.<br>- *Detección de alarma y extinción de incendio con agente aerosol y ecológico.*<br>- Doble puerta con acceso controlado. | 1 | pza | 220000,00 | 220000,00 |
| 2 | Mano de Obra Instalación sistema ATP 06F | 1 | global | 14000,00 | 14000,00 |
| 3 | Tablero de Distribución Electrice 40x30x25 cm | 1 | Pza | 950,00 | 950,00 |
| 4 | Termomagnetico Bipolar 32A | 2 | Pza | 120,00 | 120,00 |
| 5 | Protector Contra descarga atmosféricas, Bipolar, tipo 2/Clase II | 1 | Pza | 2100,00 | 2100,00 |
| 6 | Termomagnetico Bipolar 16A | 4 | global | 90,00 | 360,00 |
| | Instalación y construcción del tablero de distribución | 1 | pza | 1000,00 | 1000,00 |
| 8 | Cable canal ranurado 70x70 para instalación eléctrica dentro el centro de datos | 20 | pza | 100,00 | 2000,00 |
| 9 | Cable AWG 12, para instalación eléctrica dentro el centro de datos | 12 | pza | 5,00 | 60,00 |
| 10 | Iluminación mínima del centro de datos (500 LUX) con paneles tipo Led 60x60 cm 40 Watts | 6 | pza | 220,00 | 1320,00 |
| 11 | Cámara Video Vigilancia centro el centro de datos | 4 | pza | 700,00 | 2800,00 |
| 12 | Grabador video vigilancia DVR | 1 | pza | 2500,00 | 2500,00 |
| 14 | Cable AWG 12, para instalación eléctrica dentro el centro de datos | 72 | Mt | 5,00 | 360,00 |
| 15 | Toma corriente NEMA 16A | 8 | pza | 35,00 | 280,00 |
| 16 | Caja de sobreponer color blanco | 8 | pza | 15,00 | 120,00 |
| 17 | Montaje del tablero de distribución eléctrica y cableado de tomas NEMA | 1 | global | 2000,00 | 2000,00 |
| 18 | Adecuación de obras civiles | 1 | global | 2000,00 | 2000,00 |
| | | | | **COSTO SUBTOTAL:** | **251970,00** |

| **TABLA FINAL DE COSTOS** | | |
|---|---|---|
| **ITEM** | **DESCRIPCION** | **COSTO (Bs.)** |
| **A** | **INFRAESTRUCTURA TECNOLOGICA DEL EDIFICIO DE LA FACULTAD DE INGENIERIA** | **554565,00 Bs.** |
| **B** | **INFRAESTRUCTURA DEL CENTRO DE DATOS (IngeTIC)** | **1192200,00 Bs.** |
| **COSTO TOTAL:** | | **1746765,00 Bs.** |
| **COSTO TOTAL: Un Millon Setecientos Cuarenta y Seis Mil Setecientos Sesenta y Cinco 00/100 Bs.** | | |

# EDIFICIO FACULTAD DE INGENIERÍA

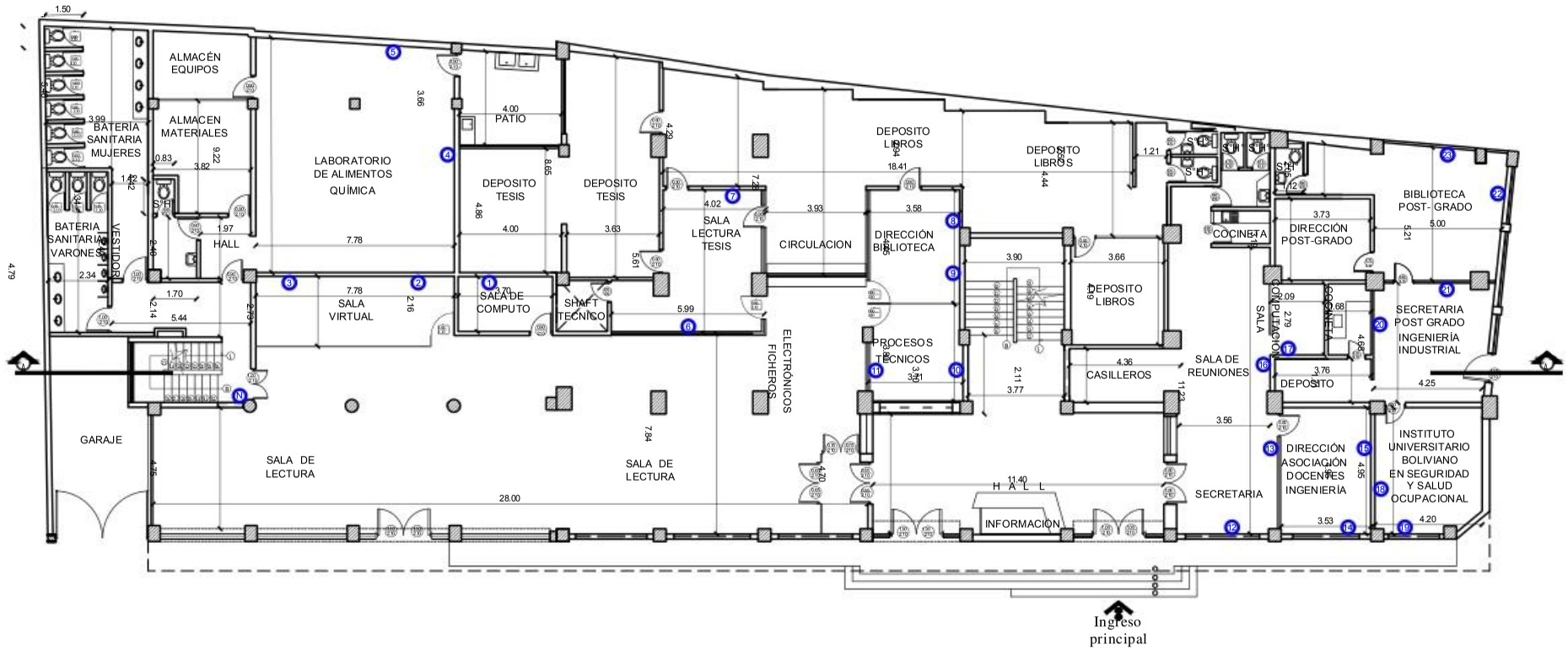



## PLANTA SOTANO UNO

ESC. 1:250, NIVEL - 3.30

## ANEXO C

# EDIFICIO FACULTAD DE INGENIERÍA

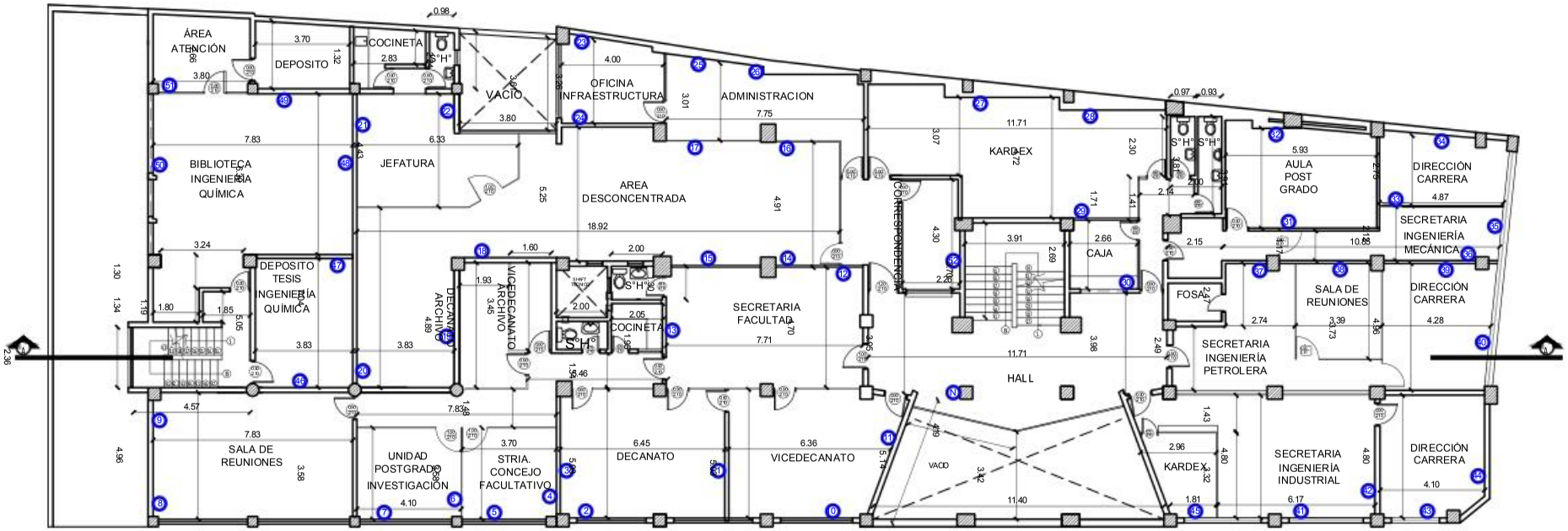



## PLANTA BAJA

ESC. 1:250, NIVEL +/- 0.00

## ANEXO D

# EDIFICIO FACULTAD DE INGENIERÍA

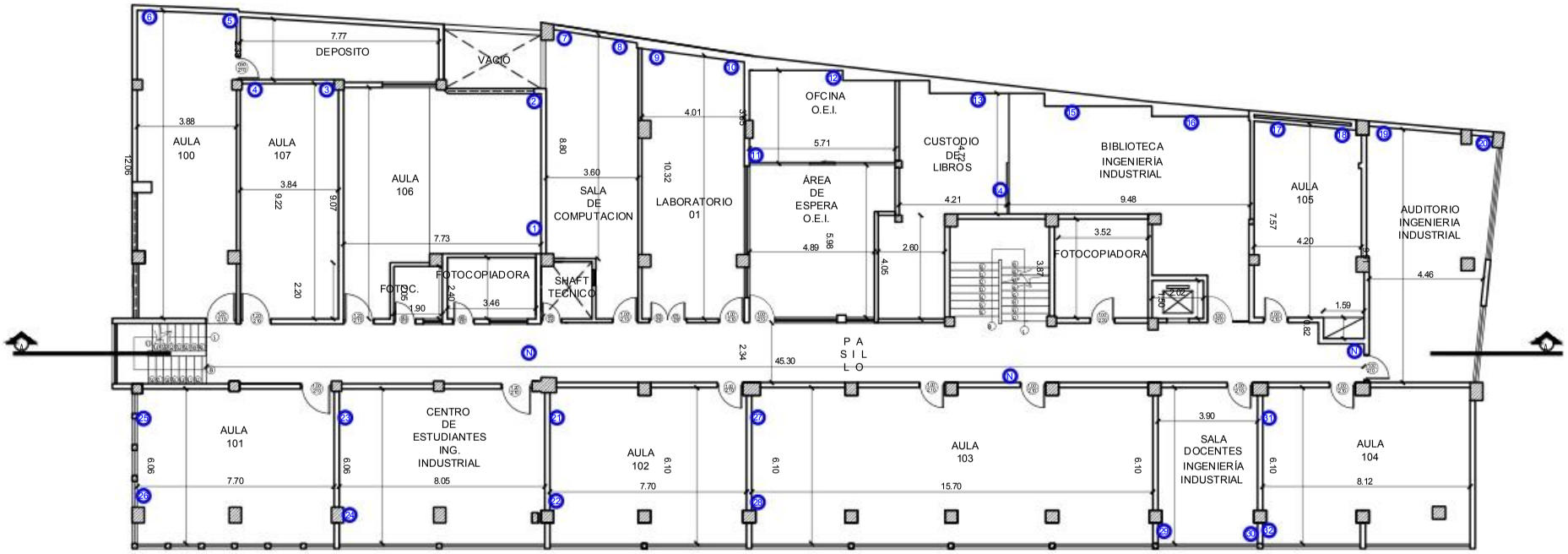



## PLANTA MEZANINE

ESC. 1:250, NIVEL + 3.00

## ANEXO E

# EDIFICIO FACULTAD DE INGENIERÍA

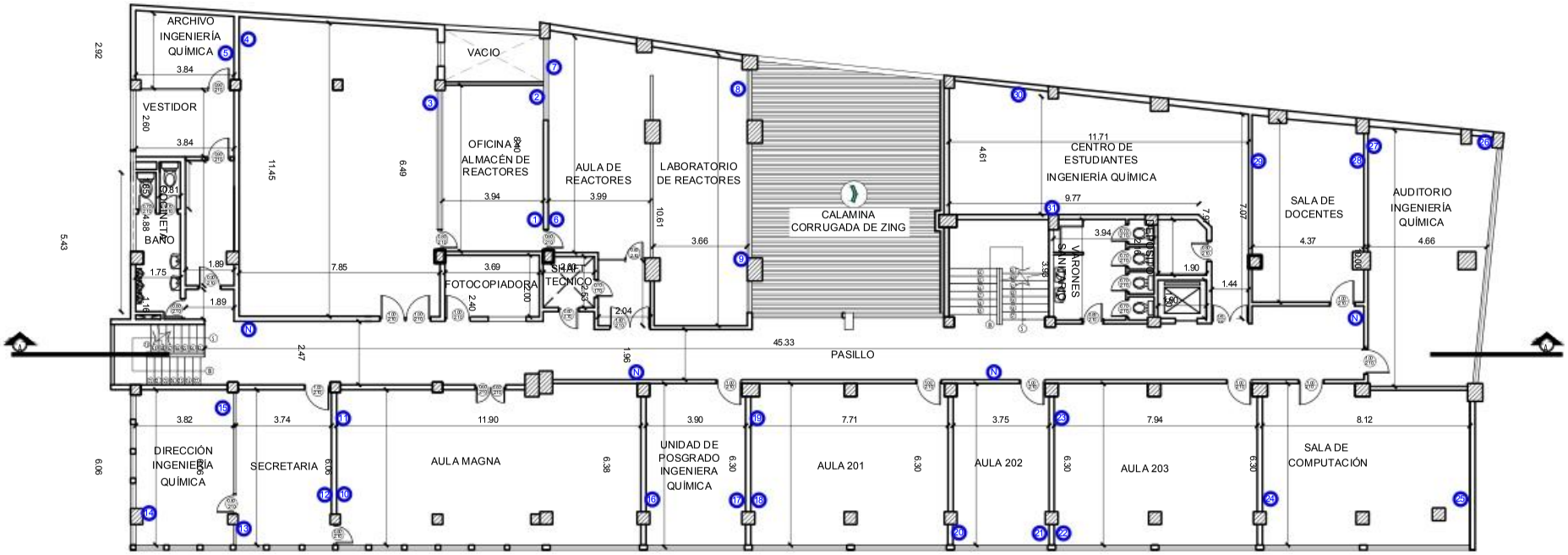



## PLANTA PRIMER PISO

ESC. 1:250, NIVEL + 6.00

## ANEXO F

# EDIFICIO FACULTAD DE INGENIERÍA

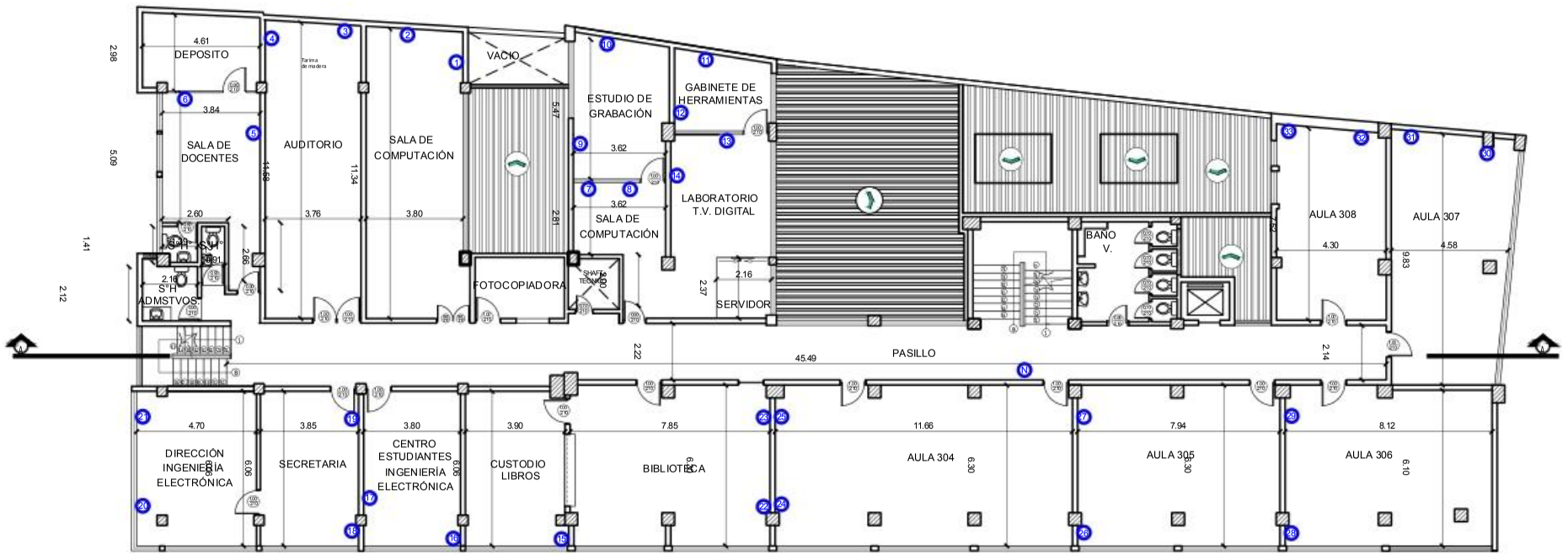



## PLANTA SEGUNDO PISO

ESC. 1:250, NIVEL + 9.00

## ANEXO G

# EDIFICIO FACULTAD DE INGENIERÍA

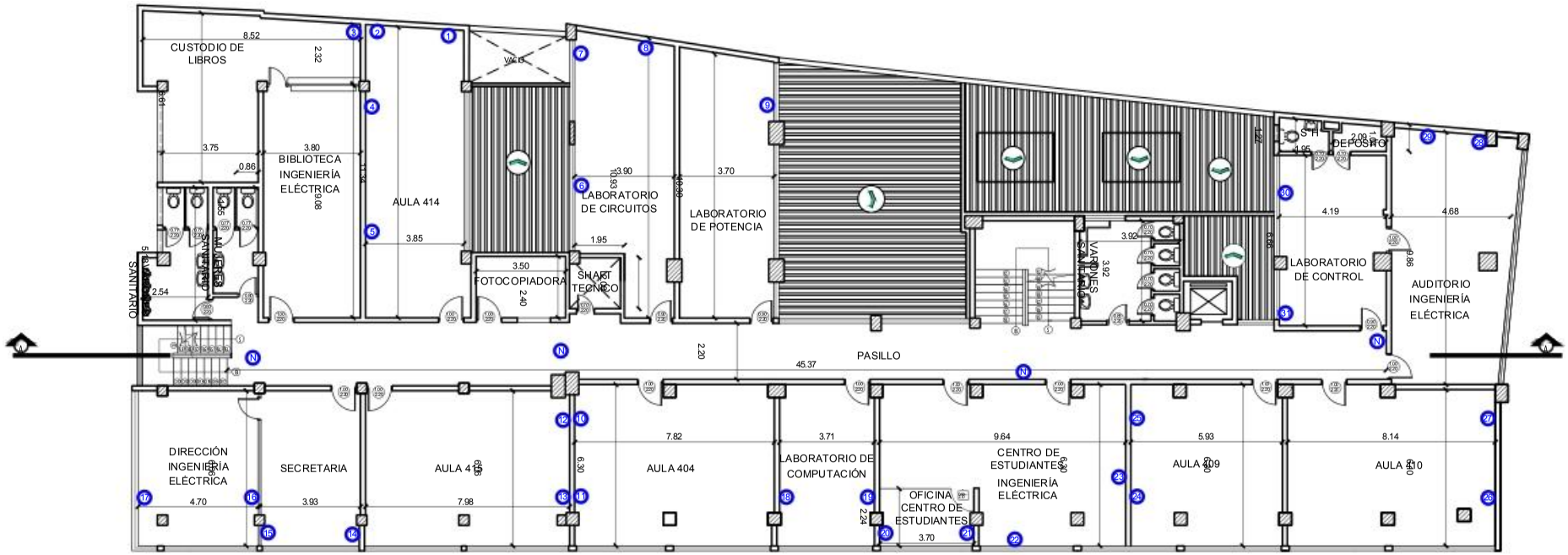



## PLANTA TERCER PISO

ESC. 1:250, NIVEL + 12.00

ANEXO H

# EDIFICIO FACULTAD DE INGENIERÍA

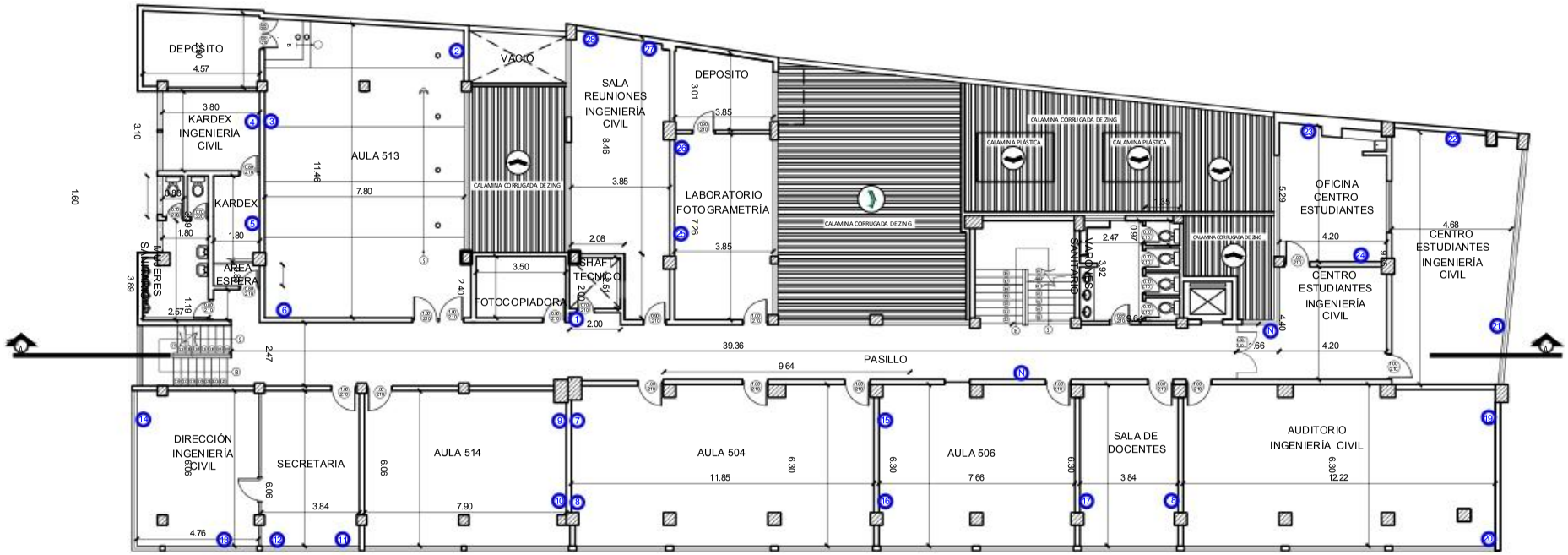



## PLANTA CUARTO PISO

ESC. 1:250, NIVEL + 15.00

## ANEXO I

# EDIFICIO FACULTAD DE INGENIERÍA

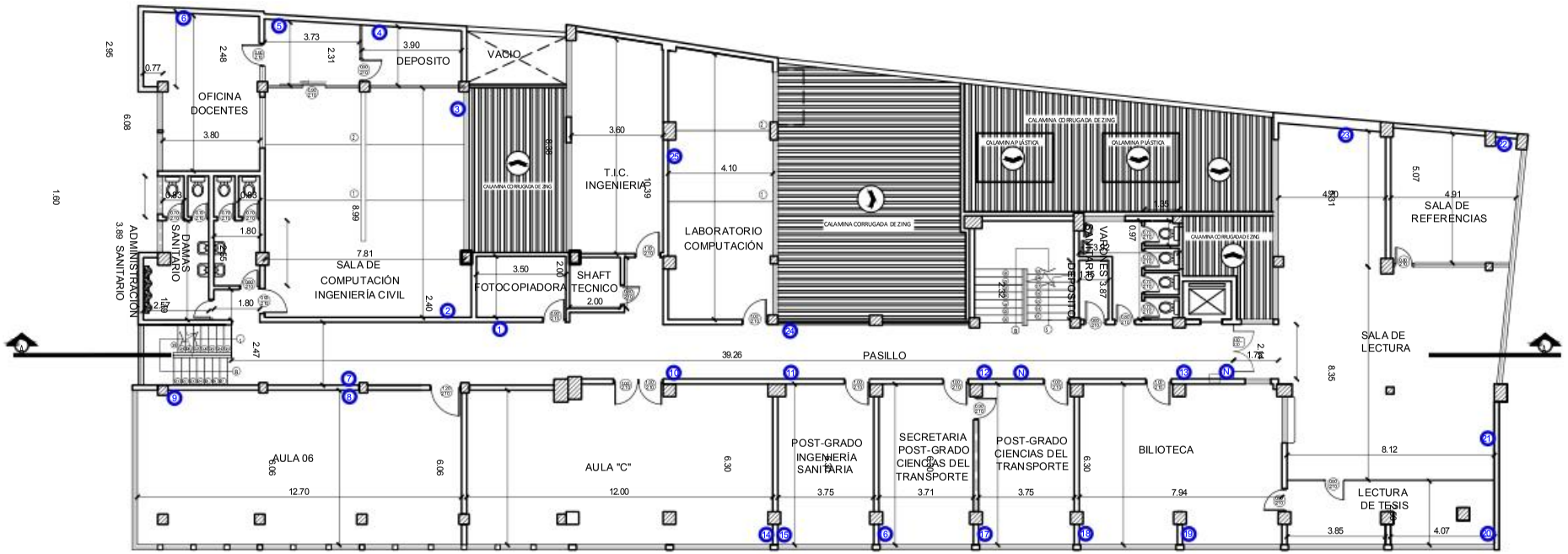



## PLANTA QUINTO PISO

ESC. 1:250, NIVEL + 18.00

ANEXO J

# EDIFICIO FACULTAD DE INGENIERÍA

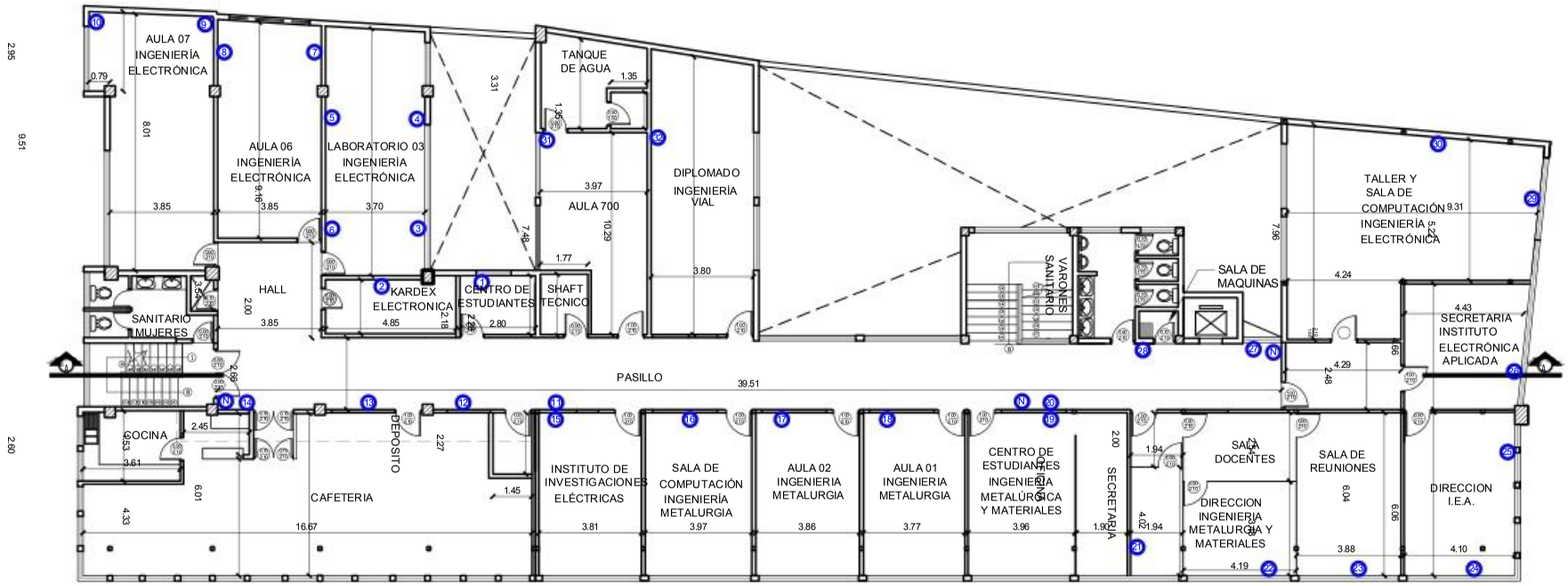



## PLANTA SEXTO PISO

ESC. 1:250, NIVEL + 21.00

## ANEXO K

# EDIFICIO FACULTAD DE INGENIERÍA

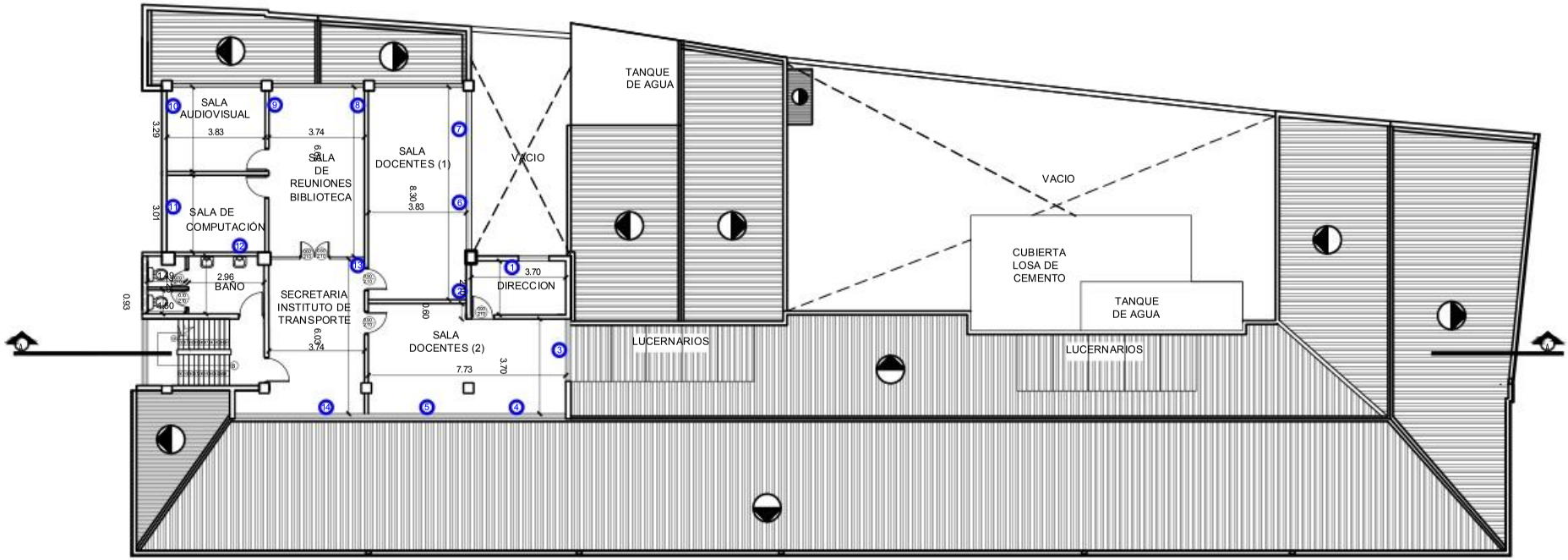



## PLANTA SEPTIMO PISO

ESC. 1:250, NIVEL + 24.00

## ANEXO L

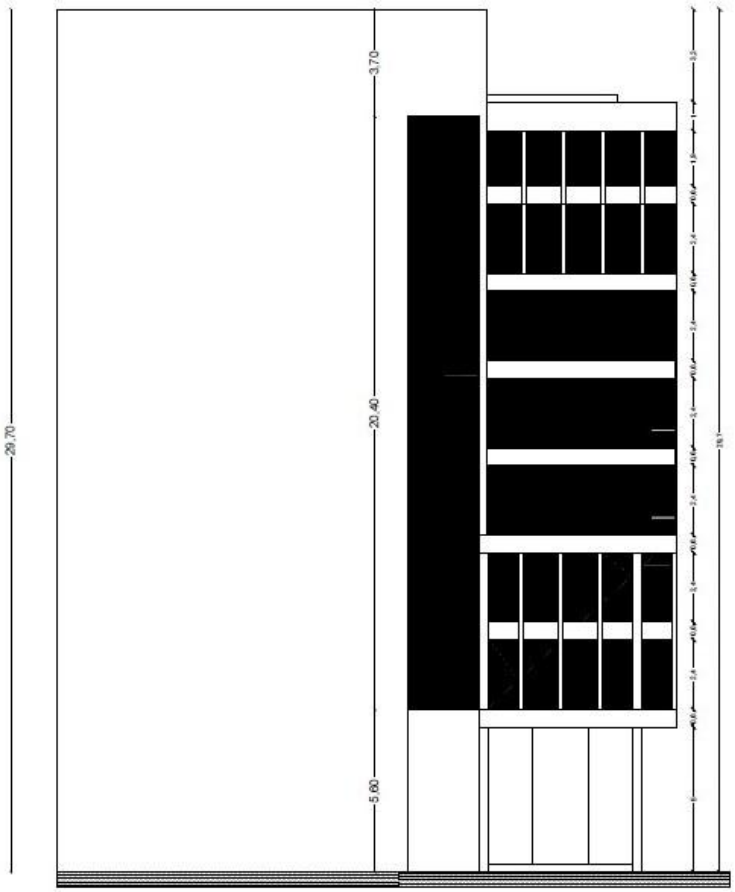
EDIFICIO FACULTAD DE INGENIERÍA



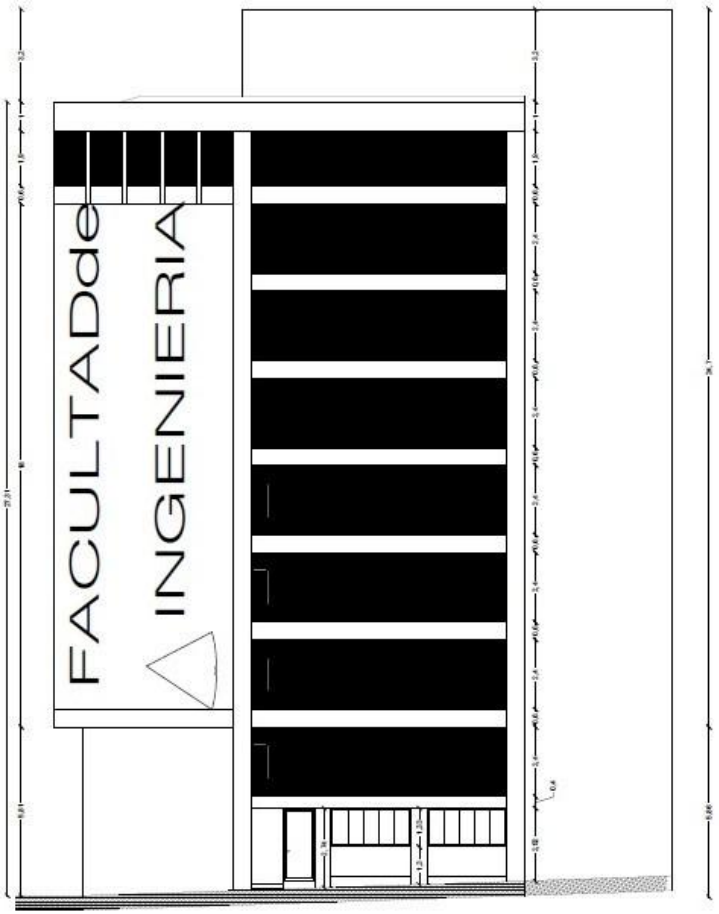

PLANTA OCTAVO PISO Y CUBIERTAS

ESC. 1:250, NIVEL + 27.00

ANEXO M




ELEVACION LATERAL NORTE




ELEVACION LATERAL SUD

ESCALA ——————— 1 : 100

ANEXO N

**Autores:**

**César Efraín Chinche Velásquez**

E-mail: cesar.chinche.velasquez@gmail.com

Cel. 71971042

**Grover Silva Loayza**

**E-mail:** gsilva.1510@gmail.com

Cel. 62429563

La Paz - Bolivia

2024-TTES-924-D-1

**DIRECCIÓN DE DERECHO DE AUTOR**
**Y DERECHOS CONEXOS**
**RESOLUCIÓN ADMINISTRATIVA NRO. 1-2068/2024**
**La Paz, 03 de julio de 2024**

**VISTOS:**

La solicitud de Inscripción de Derecho de Autor presentada en fecha **26 de junio de 2024**, por **GROVER SILVA LOAYZA** con **C.I. Nº 6941770 LP** y **CESAR EFRAIN CHINCHE VELASQUEZ** con **C.I. Nº 2601942 LP**, con número de trámite **DA 1197/2024**, señala la pretensión de inscripción del Proyecto de Grado titulado: **"DISEÑO DE CENTRO DE DATOS E INFRAESTRUCTURA TECNOLÓGICA DE INFORMACIÓN Y COMUNICACIÓN PARA LA FACULTAD DE INGENIERÍA U.M.S.A."**, cuyos datos y antecedentes se encuentran adjuntos y expresados en el Formulario de Declaración Jurada.

**CONSIDERANDO:**

Que, en observación al Artículo 4º del Decreto Supremo Nº 27938 modificado parcialmente por el Decreto Supremo Nº 28152 el *"Servicio Nacional de Propiedad Intelectual SENAPI, administra en forma desconcentrada e integral el régimen de la Propiedad Intelectual en todos sus componentes, mediante una estricta observancia de los regímenes legales de la Propiedad Intelectual, de la vigilancia de su cumplimiento y de una efectiva protección de los derechos de exclusiva referidos a la propiedad industrial, al derecho de autor y derechos conexos; constituyéndose en la oficina nacional competente respecto de los tratados internacionales y acuerdos regionales suscritos y adheridos por el país, así como de las normas y regímenes comunes que en materia de Propiedad Intelectual se han adoptado en el marco del proceso andino de integración"*.

Que, el Artículo 16º del Decreto Supremo Nº 27938 establece *"Como núcleo técnico y operativo del SENAPI funcionan las Direcciones Técnicas que son las encargadas de la evaluación y procesamiento de las solicitudes de derechos de propiedad intelectual, de conformidad a los distintos regímenes legales aplicables a cada área de gestión"*. En ese marco, la Dirección de Derecho de Autor y Derechos Conexos otorga registros con carácter declarativo sobre las obras del ingenio cualquiera que sea el género o forma de expresión, sin importar el mérito literario o artístico a través de la inscripción y la difusión, en cumplimiento a la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina, Ley de Derecho de Autor Nº 1322, Decreto Reglamentario Nº 23907 y demás normativa vigente sobre la materia.

Que, la solicitud presentada cumple con: el Artículo 6º de la Ley Nº 1322 de Derecho de Autor, el Artículo 26º inciso a) del Decreto Supremo Nº 23907 Reglamento de la Ley de Derecho de Autor, y con el Artículo 4º de la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina.

Que, de conformidad al Artículo 18º de la Ley Nº 1322 de Derecho de Autor en concordancia con el Artículo 18º de la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina, referentes a la duración de los Derechos Patrimoniales, los mismos establecen que: *"la duración de la protección concedida por la presente ley será para toda la vida del autor y por 50 años después de su muerte, a favor de sus herederos, legatarios y cesionarios"*

Que, se deja establecido en conformidad al Artículo 4º de la Ley Nº 1322 de Derecho de Autor, y Artículo 7º de la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina que: *"...No son objeto de protección las ideas contenidas en las obras literarias, artísticas, o el contenido ideológico o técnico de las obras científicas ni su aprovechamiento industrial o comercial"*

Que, el artículo 4, inciso e) de la ley N° 2341 de Procedimiento Administrativo, instituye que: *"... en la relación de los particulares con la Administración Pública, se presume el principio de buena*

*fe. La confianza, la cooperación y la lealtad en la actuación de los servidores públicos y de los ciudadanos ..."*, por lo que se presume la buena fe de los administrados respecto a las solicitudes de registro y la declaración jurada respecto a la originalidad de la obra.

**POR TANTO:**

El Director de Derecho de Autor y Derechos Conexos sin ingresar en mayores consideraciones de orden legal, en ejercicio de las atribuciones conferidas.

**RESUELVE:**

**INSCRIBIR** en el Registro de Tesis, Proyectos de Grado, Monografías y Otras Similares de la Dirección de Derecho de Autor y Derechos Conexos, el Proyecto de Grado titulado: **"DISEÑO DE CENTRO DE DATOS E INFRAESTRUCTURA TECNOLÓGICA DE INFORMACIÓN Y COMUNICACIÓN PARA LA FACULTAD DE INGENIERÍA U.M.S.A."** a favor de los autores y titulares: **CESAR EFRAIN CHINCHE VELASQUEZ** con **C.I. Nº 2601942 LP** y **GROVER SILVA LOAYZA** con **C.I. Nº 6941770 LP**, quedando amparado su derecho conforme a Ley, salvando el mejor derecho que terceras personas pudieren demostrar.

Regístrese, Comuníquese y Archívese.

CASA/lm

Firmado Digitalmente por:
Servicio Nacional de Propiedad Intelectual - SENAPI
**CARLOS ALBERTO SORUCO ARROYO**
**DIRECTOR DE DERECHO DE AUTOR Y DERECHOS CONEXOS**
LA PAZ - BOLIVIA

**Firma:** **xWhxl3Pr5Jl74H**

PARA LA VALIDACIÓN DEL PRESENTE DOCUMENTO INGRESAR A LA PÁGINA WEB **www.senapi.gob.bo/verificacion** Y COLOCAR CÓDIGO DE VERIFICACIÓN O ESCANEAR CÓDIGO QR.