FACULTAD DE INGENIERÍA

PROYECTO DE GRADO

DISEÑO DE DATA CENTER MULTIPROPÓSITO Y MULTISERVICIO PARA LA PROVINCIA DE SALTA

TIER III

Alumna

Blanco, Ana Paula Agostina

Director

Ing. Vargas, Pablo Sebastián

SALTA – 2023

INGENIERÍA EN TELECOMUNICACIONES

Director: **Ing. Vargas, Pablo Sebastián** Firma: ……

Tribunal Evaluador:

…… Firma: ……

…… Firma: ……

…… Firma: ……

Fecha de Exposición del Trabajo: …….. /…….. /…….

AGRADECIMIENTOS

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO I: INTRODUCCIÓN

Breve descripción y su importancia

La implementación de un data center de nivel Tier 3 implica una serie de ventajas y beneficios altamente significativos para las organizaciones que buscan asegurar una disponibilidad óptima, un rendimiento excepcional y una confiabilidad inquebrantable en todas sus operaciones tecnológicas.

Para lograr este nivel de excelencia, resulta esencial llevar a cabo un diseño meticuloso que analice con precisión todas las variables posibles. Esto incluye una evaluación detallada de los tipos de equipos que se incorporarán, la configuración del piso técnico, la altura del techo y la infraestructura del cableado, entre otros aspectos cruciales.

Un componente fundamental en este proceso es la seguridad, tanto a nivel físico como lógico. Se debe considerar minuciosamente la identificación y mitigación de posibles riesgos que puedan surgir. Esta precaución no solo garantiza la protección de los activos críticos de la organización, sino que también asegura la integridad de los datos y la continuidad de las operaciones en cualquier circunstancia.

Motivación para abordarlo

Este proyecto propone la creación de un data center Tier 3 en la zona de entrada de la ciudad de Salta, a la altura de La Lagunilla.

Salta es reconocida por su exuberante belleza natural y su creciente dinamismo económico, brinda un escenario propicio para cultivar su potencial tecnológico en expansión, lo que la convierte en el lugar ideal para establecer una infraestructura tecnológica de vanguardia.

La implementación de un data center nivel Tier 3 puede estimular aún más la inversión y el desarrollo de la tecnología local, generando empleo y oportunidades en el sector tecnológico.

Podemos mencionar características esenciales que hacen que la ubicación elegida para el data center sea excepcionalmente adecuada.

1. Disponibilidad de Reserva de Agua:

Uno de los principales desafíos en la operación de un data center es el control de la temperatura interna. La Lagunilla proporciona una valiosa fuente de agua, que puede ser empleada para la refrigeración de los equipos. Esta fuente de agua local garantiza una solución eficaz y sostenible para mantener las condiciones ambientales adecuadas, lo que es esencial para un centro de datos de alta disponibilidad.

2. Acceso Confiable a Energía Eléctrica:

La electricidad ininterrumpida es fundamental para la operación de un data center Tier 3. Lagunilla se encuentra estratégicamente ubicada en el camino de acceso de la energía eléctrica proporcionada por TRANSNOA, el proveedor de energía que abastece a la distribuidora local, EDESA. Esta conexión directa a la red eléctrica principal de la ciudad garantiza una fuente de energía confiable y de alta calidad. Además, la cercanía al electroducto de la empresa TermoAndes hacia Chile brinda una segunda fuente de energía disponible, lo que aumenta aún más la redundancia energética.

3. Seguridad Física y Protección:

La ubicación geográfica de Lagunilla, alejada de la ciudad y respaldada por una elevación montañosa, proporciona una protección natural contra posibles amenazas y ataques externos. La seguridad física es esencial para garantizar la integridad de los datos y la infraestructura del data center en un entorno donde prevalece un clima de ciberamenazas.

4. Infraestructura de Comunicaciones Avanzadas:

Además de las características mencionadas, Lagunilla se beneficia de la instalación de canalizaciones de fibra óptica por parte de empresas líderes en telecomunicaciones como Telecom y Claro en la Ruta Nacional N°9. Además, el proceso en curso para la construcción de la vinculación de la ciudad de Salta con la red federal de fibra óptica REFEFO, gestionada por el organismo gubernamental y la empresa estatal ARSAT, promete una conectividad de alta velocidad y confiable para el centro de datos. Esto es esencial para garantizar la conectividad y el acceso rápido a nivel nacional e internacional.

Por otro lado, esta iniciativa no solo tiene un impacto a nivel macroeconómico, sino que también ofrece un recurso invaluable para las empresas locales. Un data center Tier 3 de alta disponibilidad proporciona una plataforma fiable para resguardar sistemas y datos críticos, lo que potencia la confianza y la capacidad de adaptación de las empresas en un entorno empresarial cada vez más digital y competitivo.

Fases para su diseño

Para el diseño de un data center multipropósito y multiservicio para la provincia de Salta Tier 3, con un enfoque en la refrigeración a base de agua se deben contemplar las siguientes etapas:

1. Estudio técnico y normativo: comenzar con un estudio exhaustivo de las regulaciones y normas locales, provinciales y nacionales relacionados con la construcción y operación de data centers, así como las pautas ambientales.

2. Marco teórico: Desarrollar un diseño conceptual que integre los principios de un data center nivel Tier 3. Evaluar los posibles impactos ambientales y desarrollar estrategias para minimizarlos, como la gestión del uso de agua y la implementación de tecnologías eco amigables.

3. Diseño detallado: Detallar las especificaciones técnicas del diseño, incluyendo la ubicación del data center, la disposición de los equipos, el diseño de los pasillos fríos y calientes, y la implementación de la refrigeración a base de agua. Desarrollar un plan integral de seguridad que abarque tanto aspectos físicos como lógicos, incluida la protección de los datos y la infraestructura.

CAPÍTULO II: MARCO TEÓRICO

¿Qué es un data center?

Un data center o centro de datos es una sala, edificio o instalación física que alberga infraestructura de TI para crear, ejecutar y entregar aplicaciones y servicios, además de almacenar y gestionar los datos asociados con dichas aplicaciones y servicios [1].

En lo que respecta al diseño de un Centro de Datos, cuenta con determinadas características físicas especiales de protección, refrigeración y redundancia, cuyo objetivo es atesorar toda la información lógica de las organizaciones brindando disponibilidad y seguridad.

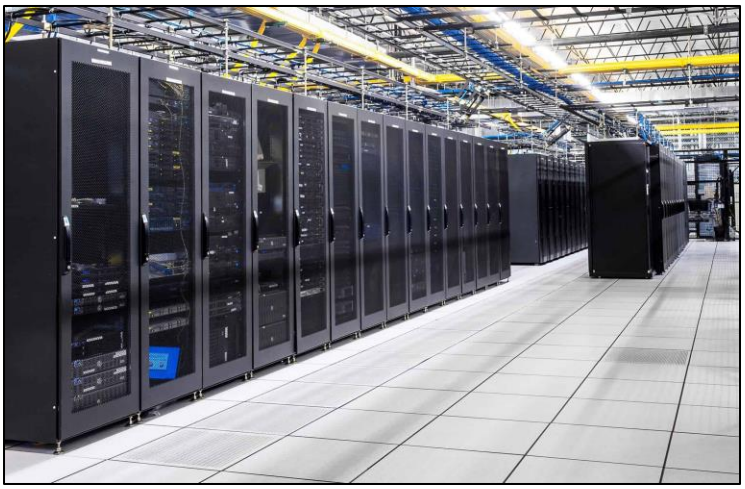

Figura 1. Ejemplo de data center

Existen diferentes áreas dentro del Centro de Datos donde cada una de ellas trabaja de manera interdependiente. Podemos mencionar:

- Infraestructura física: Debe ser un espacio con dimensiones adecuadas como para poder alojar los racks teniendo en cuenta el peso y el tamaño de los mismos.

- Sistema eléctrico: Este sistema debe ser robusto y confiable con el fin de minimizar cualquier falla o interrupción en el suministro de energía, para esto debe cumplir con determinadas condiciones entre las principales podemos mencionar que debe proveer un sistema redundante, UPS, generación de respaldo, entre otras características. Se necesita de un sistema autónomo que provea el sistema de energía eléctrica dentro del Centro de Datos.

- Sistema de climatización: Los equipos de telecomunicaciones deben funcionar dentro del rango de temperatura óptimo según lo indican sus especificaciones técnicas. Por tal motivo es indispensable contar con un sistema de climatización apropiado que controle y provea niveles de humedad y temperatura en el sitio.

- Seguridad: Un centro de datos Tier 3 es un centro de alta disponibilidad y redundancia, por lo tanto la seguridad es un aspecto crítico para garantizar que los datos y la infraestructura estén protegidos de amenazas internas y externas. Los aspectos de seguridad contemplan medidas administrativas, físicas y técnicas. Donde estas abarcan la seguridad tanto a nivel físico como a nivel lógico de la información e infraestructura. La información debe mantenerse segura y confiable. A nivel físico debe tener tanto un sistema de video-seguridad monitoreado constantemente, como un sistema de control de accesos en cada área.

- Telecomunicaciones: El área de telecomunicaciones cumple un rol fundamental en el funcionamiento de un Tier 3, es responsable de garantizar la conectividad y la comunicación confiable tanto dentro del data center como hacia internet, debe proveer que la transmisión de datos sea óptima y los servicios de conectividad permanezcan operativos. Pueden variar dependiendo del tamaño y la complejidad de la red. El tipo y calidad depende de los equipos que se utilicen.

Diseño de un data center según TIA-942

TIA-942 es una serie de normas establecidas por la Telecommunication Industry Association (TIA), una asociación de la industria de las telecomunicaciones en los Estados Unidos.

La norma TIA/EIA -942 proporciona un enfoque detallado para el diseño y la construcción de data centers, abordando aspectos como la topología de la red, la redundancia eléctrica y de enfriamiento, la seguridad física y otros elementos críticos para el funcionamiento de un data center de alta calidad [2].

La serie de normas TIA-942 se ha desarrollado en varias ediciones a lo largo del tiempo para mantenerse actualizada con los avances tecnológicos y las mejores prácticas en la industria.

Tipos de data centers

Los data centers pueden variar en su configuración según las necesidades empresariales y las demandas de carga de trabajo.

Data centers local (On-Premises)

En este tipo de data centers, toda la infraestructura de tecnología de la información y los datos se encuentran en las instalaciones de la empresa. Muchas compañías eligen esta opción debido a la sensación de mayor control sobre la seguridad de la información. En un data center empresarial, la empresa asume la responsabilidad de todas las actividades.

Data centers en la nube (Cloud Computing)

Las empresas utilizan servicios de nube proporcionados por proveedores de servicios cloud, como Amazon Web Services (AWS), Google Cloud Platform (GCP) o Microsoft Azure. Estos proveedores gestionan la infraestructura y los recursos informáticos, lo que permite una escalabilidad y flexibilidad significativas.

Data centers gestionados e instalaciones de coubicación

Las organizaciones que carecen de los recursos, el espacio físico o la experiencia necesaria para implementar y administrar completamente su propia infraestructura de tecnología de la información en sus instalaciones, pero que desean mantener un mayor grado de control y no recurrir a la nube pública para alojar sus recursos informáticos, pueden encontrar opciones adecuadas en los centros de datos gestionados y las instalaciones de colocalización.

En un centro de datos gestionados, la compañía cliente alquila servidores, almacenamiento y hardware de red dedicados del proveedor del data center, y el proveedor del data center se encarga de la administración, la supervisión y la gestión para la compañía cliente.

En una instalación de coubicación, la compañía cliente es la propietaria de toda la infraestructura y alquila un espacio dedicado para alojarla dentro de la instalación. En el modelo de coubicación tradicional, la compañía cliente tiene acceso exclusivo al hardware y total responsabilidad por su gestión; esta opción es ideal para la privacidad y la seguridad, pero no suele ser práctica, sobre todo durante interrupciones o emergencias. Hoy en día, la mayoría de los proveedores de coubicación ofrecen servicios de gestión y supervisión para los clientes que los desean [3].

Clasificación de niveles de data centers

Uptime Institute creó los niveles de clasificación Tier de los Data Centers hace más de 25 años y, en la actualidad, sigue siendo el estándar internacional para el rendimiento de los centros de datos. Las definiciones en niveles de nuestro centro de datos explican la infraestructura necesaria para las operaciones del centro de datos. Existen diferentes Tiers según la disponibilidad del sistema que se necesite. Estas clasificaciones son métodos objetivos y confiables para comparar el rendimiento de la infraestructura de un sitio con otro [4].

La clasificación se divide en cuatro niveles según la medida en que cumplen con los criterios para el mantenimiento, sistema energético, enfriamiento y redundancia. Entonces, los niveles Tier de los Data Centers son:

Tier I: Data center básico

Los requisitos para una instalación de este tipo incluyen:

- Un Sistema de Alimentación Ininterrumpida UPS que nos permite tener energía almacenada de respaldo en caso de que el suministro eléctrico falle.
  Un UPS también sirve para proteger los dispositivos que se encuentran conectados cuando hay una elevación o disminución de tensión, o sostener su funcionamiento cuando existen pequeños cortes de energía.
- Un área para sistemas informáticos.
- Equipo de refrigeración dedicado.
- Un motor generador para cortes de energía.

La tasa de disponibilidad máxima del Data Center es de 99.671 % del tiempo.

Tier II: componentes redundantes

Las instalaciones incluyen componentes de capacidad redundante para energía y refrigeración que ofrecen mayor seguridad frente a interrupciones. Estos componentes son:

- Generadores de motor
- Almacen de energia.
- Enfriadores.
- Unidades de refrigeración.
- Módulos SAI.
- Equipo de disipación de calor.
- Tanques de combustible.
- Celdas de combustible.

La tasa de disponibilidad máxima del Data Center es 99.741 % del tiempo.

Tier III: mantenimiento concurrente

Las instalaciones permiten que se realicen actividades de mantenimiento sobre cualquier componente de la infraestructura sin que existan interrupciones en el servicio. Dichas actividades de mantenimiento pueden ser preventivas y programadas, para agregar, cambiar o eliminar elementos, entre otros.

Por lo general, los Data Centers Tier III son diseñados con proyección de actualizarse a tier IV, siempre que los requerimientos del negocio justifiquen los costos.

La tasa de disponibilidad máxima del Data Center es del 99.982 % del tiempo.

Tier IV: Tolerante a fallas

Provee capacidad para realizar cualquier actividad planeada sin interrupciones y además la funcionalidad tolerante a fallas permite que el servicio continúe operando aun ante eventos no planeados. Requiere dos líneas de distribución simultáneamente activas.

La tasa de disponibilidad máxima del Data Center es 99.995 % del tiempo.

Considerando que un año consta de 8,760 horas, se presenta a continuación en la Tabla 1 el tiempo anual de interrupción expresado en horas para cada nivel de tier, en función del porcentaje de disponibilidad correspondiente.

TIER	**% Disponibilidad**	**% Interrupción**	**Tiempo anual de interrupción en horas**
Tier I	99.671 %	0.329 %	28.82 horas
Tier II	99.741 %	0.259 %	22.68 horas
Tier III	99.982 %	0.018 %	1.57 horas
Tier IV	99.995 %	0.005 %	0.44 horas

Tabla 1. Tiempo anual de interrupción en horas de cada tipo de Tier

La Figura 2 muestra de forma ilustrativa como crece la disponibilidad de un TIER de acuerdo a su clasificación, mencionando también algunas características más relevantes que incorpora cada nivel.

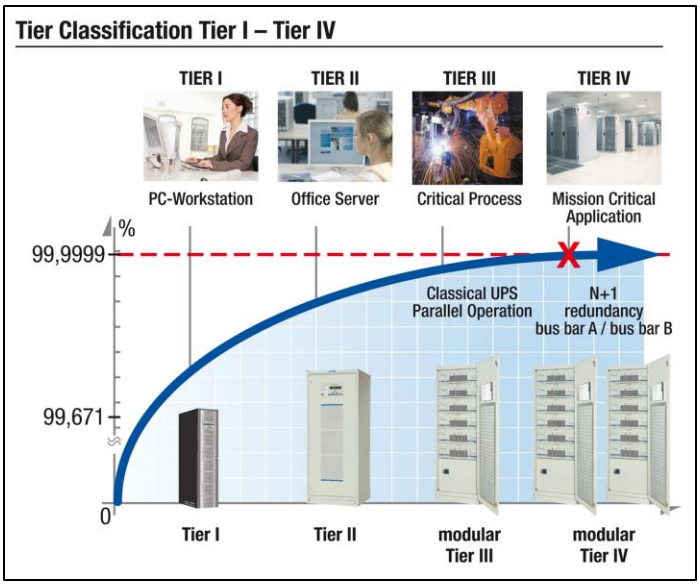

Figura 2. Clasificación de Data Center según su redundancia

Principios del diseño de un data center

Lo primero a tener en cuenta es la ubicación física donde estará el Data Center y los diferentes riesgos que existen tanto físicos como ambientales en relación al sitio elegido. A continuación, se detallarán los diferentes requerimientos a la hora de diseñar [5]:

- La ubicación ideal para un Data Center tiene que tener fácil acceso a todos los servicios, principalmente diferentes proveedores de internet, agua, energía, ser una zona segura en cuanto a robos o vandalismo, entre otros aspectos.

También es imprescindible ubicar el Data Center lejos de fuentes de vibración como son los aeropuertos, instalaciones industriales y constructoras de camino, debido a que los servidores y distintos dispositivos de red son vulnerables a las vibraciones que éstos producen.

- La altura del edificio debe contemplar las dimensiones de un rack de 42 unidades, el uso de piso técnico, y distribución eléctrica con un cielorraso.

- Sistema de refrigeración, ya que, los equipos producen calor en exceso y esto provoca el mal funcionamiento de los mismos, pudiendo desembocar en un incendio.

- Sistema energético primario y de respaldo

- Sistema de video vigilancia que incluye cámaras de seguridad, una sala de monitoreo, instalación de alarmas, detectores de movimiento, validador biométrico de datos, tarjetas de identificación.

- Sistemas de monitoreo ambiental para el control de humedad y control de temperatura. Extintores de fuego.

¿Qué es un NOC?

Un Centro de Operaciones de Red, conocido como NOC (por sus siglas en inglés, Network Operations Center) es un lugar centralizado desde donde se monitorean y administran sistemas informáticos, de telecomunicaciones y redes satelitales durante todo el día, todos los días de la semana. Cumple un rol fundamental como la primera instancia de protección contra cualquier interrupción o problemas en la red. [6]

Industrias como las telecomunicaciones, servicios financieros y energía operan sin parar, y necesitan una conectividad constante. Mantener este nivel de operación global las 24 horas, los 7 días a la semana, requiere una supervisión continua de la red. Esto puede ser un desafío dentro de los departamentos de TI tradicionales. Ahí es donde entra en juego el NOC, encargándose de monitorear y abordar rápidamente problemas que puedan afectar el rendimiento de la red, como la detección de malware y la gestión del tráfico del sitio web. También se enfoca en mejorar la red mediante actualizaciones y mantenimiento.

¿Cómo funcionan?

Los NOC colaboran directamente con las organizaciones para vigilar sus entornos de red complejos, abarcando servidores, bases de datos, firewalls, dispositivos y servicios externos relacionados. La infraestructura de tecnología de la información (TI) puede estar ubicada tanto en las instalaciones de la empresa como en la nube, dependiendo de las necesidades.

La operación de los NOC suele seguir un proceso escalonado, donde los incidentes se categorizan en niveles del uno al tres. El nivel uno se refiere a incidentes menos críticos, como la evaluación de alertas de dispositivos de infraestructura, mientras que el nivel tres aborda situaciones más graves, como ataques de ransomware o cortes de la red. Si un técnico no puede resolver un problema de manera oportuna, se deriva a un experto con mayor experiencia. Los ingenieros del NOC trabajan en la resolución de problemas y buscan estrategias para prevenir futuros tiempos de inactividad de la red y problemas de conectividad.

Beneficios de los NOC

Los NOC ya sea que sean administrados internamente o a través de proveedores externos, ofrecen una serie de beneficios significativos para las empresas.

En primer lugar, permiten que los departamentos de TI sean más eficientes al liberar a los empleados de tareas relacionadas con la supervisión y administración de la red, lo que les permite centrarse en proyectos estratégicos y nuevas iniciativas.

Un beneficio crucial es la eliminación del tiempo de inactividad, ya que los NOC operan las 24 horas del día, los 7 días de la semana, asegurando que siempre haya personal disponible para garantizar el funcionamiento continuo del software, hardware y redes.

Por último, se destacan por su capacidad de respuesta rápida a incidentes. Están diseñados para supervisar constantemente los sistemas de red, identificar problemas de manera temprana y corregir errores antes de que se conviertan en problemas mayores. Esto garantiza que los incidentes se resuelvan de manera eficiente y sin interrupciones significativas.

CAPITULO III: CONSIDERACIONES TÉCNICAS DE DISEÑO

Sala de equipos

La sala de equipos es el corazón de un Data Center, por lo que es fundamental considerar cuidadosamente ciertos aspectos, como el espacio disponible. Es esencial que el área de la sala de equipos sea lo suficientemente amplia para alojar todos los racks, servidores, sistemas de enfriamiento y otros equipos esenciales. Además, debe garantizarse que haya espacio adecuado para que el personal se desplace sin dificultades y realice el mantenimiento de manera eficiente.

Para dimensionar adecuadamente una sala de equipos, se debe tener en cuenta la capacidad actual y futura de los equipos. Esto incluye considerar la expansión de la infraestructura y la adición de nuevos equipos a medida que la demanda aumente.

Capacidad de carga del piso

El piso debe estar diseñado para soportar el peso de los equipos y racks sin riesgo de hundimiento o daños.

Resistencia al fuego

Para garantizar una adecuada resistencia al fuego se implementan varias medidas y características:

1. Materiales de construcción resistentes al fuego: Los materiales utilizados son seleccionados por su capacidad para resistir el fuego y evitar la propagación de llamas y generación de gases tóxicos.
2. Sistemas de detección de incendios: Se instalan sistemas avanzados de detección de incendios que monitorean constantemente la sala de equipos y otras áreas críticas en busca de señales de humo, calor o llamas. Esto permite una detección temprana y una respuesta rápida en caso de incendio.
3. Sistemas de supresión de incendios: Suelen estar equipados con sistemas automáticos de extinción de incendios, como sistemas de rociadores de agua o sistemas de extinción por gas, que se activan automáticamente en caso de incendio para controlar y extinguir el fuego de manera eficiente y segura.

Tecnologías disponibles de acuerdo a los requerimientos de la NFPA 2001:

La NFPA (National Fire Protection Association) es una organización que establece códigos y estándares de seguridad contra incendios y otros riesgos relacionados. (Nota de pie)

El NFPA 2001 es la norma para la instalación de sistemas de extinción de incendios con agentes limpios. Los agentes limpios son sustancias gaseosas o líquidas que se utilizan para extinguir incendios en áreas ocupadas por equipos electrónicos, documentos y otros materiales sensibles al agua o espuma.

Los dos tipos principales de agentes limpios que cubre la NFPA 2001 son [7] :

- Agentes licuados: Estos son agentes químicos que, bajo presión, se almacenan en estado líquido y se liberan como gas cuando se descargan en el área de incendio. Los agentes licuados más comunes son los halones y los hidroclorofluorocarbonos (HCFC). Sin embargo, debido a su potencial para agotar la capa de ozono, la producción y uso de halones y HCFC han sido restringidos o eliminados en muchos países.

- Agentes inertes: Estos gases no son tóxicos y no deja residuos después de la descarga. Los agentes inertes funcionan reduciendo la concentración de oxígeno en el área de incendio, lo que inhibe la combustión. Algunos ejemplos comunes de agentes inertes son el argón, nitrógeno y dióxido de carbono.

Es esencial seguir las normas y códigos establecidos por la NFPA 2001 para garantizar la efectividad y la seguridad de los sistemas de extinción de incendios con agentes limpios en los espacios críticos y valiosos. Estos sistemas son comúnmente utilizados en entornos como data centers, salas de servidores, instalaciones de telecomunicaciones y otros lugares con equipos y datos sensibles a los daños causados por agua u otros agentes de extinción tradicionales.

4. Caminos de escape y sistemas de evacuación: se establecen caminos de escape claros y seguros para el personal en caso de emergencia.

Figura 3. EA-227 fire systems - Maxxon

La Figura 3 muestra un extintor de fuego por acción física/mecánica y química en forma rápida y eficaz. No es conductivo, ni corrosivo, ni deja residuo alguno.

Iluminación

Es un aspecto importante para garantizar un entorno de trabajo seguro y eficiente. Si bien la iluminación puede parecer un factor menor en comparación con otros aspectos técnicos, su diseño adecuado es fundamental para la operación efectiva del data center y para mantener las condiciones óptimas para el personal que trabaja en él.

- Iluminación adecuada y uniforme: Se deben utilizar lámparas y luminarias de alta calidad para garantizar una iluminación uniforme en todas las áreas del data center, incluyendo las salas de equipos, pasillos, áreas de trabajo y salas de reuniones. Esto ayuda a evitar áreas oscuras o zonas con sombras, lo que facilita la navegación y el mantenimiento.

- Iluminación de emergencia: Es esencial contar con sistemas de iluminación de emergencia que se activen en caso de corte de energía para proporcionar una iluminación mínima y permitir una evacuación segura del personal.

- Eficiencia energética: Para reducir el consumo de energía y los costos operativos, es recomendable utilizar luminarias LED de alta eficiencia energética en lugar de las tradicionales bombillas incandescentes o fluorescentes.

- Control de iluminación: La implementación de sistemas de control de iluminación, como sensores de movimiento y ajuste de niveles de iluminación según la luz natural.

- Ausencia de calor: La elección de luminarias LED también es ventajosa porque generan menos calor en comparación con otras tecnologías de iluminación, lo que puede ayudar a mantener una temperatura adecuada en el data center y reducir la carga sobre los sistemas de enfriamiento.

- Respaldo de energía: La iluminación también debe estar conectada a sistemas de respaldo de energía, como UPS y generadores de respaldo, para asegurar que haya iluminación adecuada incluso durante cortes de energía prolongados.

- Iluminación en pasillos elevados y techos: Es fundamental tener en cuenta la iluminación en pasillos elevados y en el techo para facilitar el acceso y el mantenimiento de los equipos ubicados en racks a mayor altura.

Seguridad

Es un aspecto fundamental para garantizar la integridad, disponibilidad y confidencialidad de los datos y servicios alojados en el data center Tier 3.

Acceso físico restringido

Es una medida de seguridad que limita y controla rigurosamente quiénes pueden ingresar y acceder físicamente a las instalaciones del data center. Se establecen puntos de acceso controlados incluyendo sistemas de identificación, tarjetas de acceso, sistemas de

autenticación biométrica o códigos de acceso. Solo el personal autorizado debe poder acceder a las áreas críticas del data center.

También se lleva un registro detallado de todas las entradas y salidas del personal autorizado. Esto facilita la auditoría y el seguimiento de quienes tuvieron acceso a las instalaciones en todo momento.

Vigilancia y monitoreo

Cuentan con sistemas de vigilancia y monitoreo las 24 horas del día, los 7 días de la semana. Esto incluye cámaras de seguridad, sistemas de detección de intrusos y alarmas para responder a cualquier intento de acceso no autorizado o actividad sospechosa.

Se instalan cámaras de seguridad en ubicaciones estratégicas dentro y fuera del data center para monitorear constantemente el entorno. Estas cámaras pueden ser fijas o móviles y pueden incluir funciones como visión nocturna y grabación en alta resolución. Las cámaras deben cubrir todas las áreas críticas, incluidos los pasillos de acceso, las salas de servidores, las salas de almacenamiento y los puntos de entrada y salida.

Es importante también contar con sistemas de grabación de video para registrar y almacenar el historial de grabaciones durante un periodo de tiempo determinado, lo que facilita la revisión y la investigación de incidentes.

Respaldo y recuperación de datos

Implementan planes sólidos de respaldo y recuperación de datos para garantizar que la información crítica esté protegida y pueda recuperarse en caso de fallos o desastres.

Se establecen políticas de respaldos que definen qué datos se respaldan, con qué frecuencia y durante cuánto tiempo se retendrán los respaldos. Los datos críticos se respaldan regularmente, y la frecuencia de los respaldos puede variar según la criticidad de los datos.

También se deben realizar pruebas regulares de restauración para verificar la integridad de los respaldos y la capacidad de recuperación de datos en caso de un evento de pérdida de información.

Seguridad lógica

La seguridad lógica, también conocida como seguridad de la información o ciberseguridad, se refiere a las medidas y prácticas diseñadas para proteger los sistemas informáticos, la información digital y los datos de una organización contra amenazas cibernéticas, intrusiones no autorizadas, accesos no deseados y otros riesgos relacionados con la tecnología.

En este contexto, se establecen políticas y prácticas para configurar firewalls y dispositivos de seguridad de red, controlando el tráfico y previniendo intrusiones no

autorizadas. Además, se implementan programas antivirus y antimalware para detectar y eliminar software malicioso que pueda infectar sistemas y redes.

Piso técnico

El piso técnico en un data center Tier 3 es una parte importante de la infraestructura que se utiliza para alojar equipos y sistemas críticos. Un piso técnico es un sistema modular de paneles elevados que se instala sobre el piso original del edificio para crear un espacio vacío entre ambos. A continuación se detallan algunos aspectos importantes:

1. Gestión de cables y servicios: El piso técnico permite ocultar y gestionar los cables eléctricos, de red, fibra óptica y otros servicios de infraestructura. Esto ayuda a mantener una apariencia ordenada y profesional, evitando posibles enredos y facilitando el acceso para realizar mantenimientos y cambios.

2. Enfriamiento eficiente: El piso técnico permite el paso del aire frío desde el sistema de enfriamiento hacia los racks y equipos que generan calor. Al canalizar el aire de manera adecuada, se optimiza la refrigeración, lo que puede mejorar la eficiencia energética y reducir los costos de enfriamiento.

3. Flexibilidad y escalabilidad: El piso técnico brinda la posibilidad de mover y reorganizar los racks y equipos con mayor facilidad, lo que permite una mayor flexibilidad en la distribución del espacio y la capacidad para expandirse o hacer cambios en la configuración del data center de manera más ágil.

4. Reducción del riesgo de inundaciones: Al elevar el piso del data center, se disminuye el riesgo de daños causados por inundaciones o derrames accidentales de agua, ya que muchos componentes vitales estarán protegidos por encima del nivel del suelo.

5. Seguridad: El espacio vacío bajo el piso técnico puede utilizarse para colocar sensores y sistemas de detección de humo, calor y otros peligros potenciales, lo que mejora la seguridad y la capacidad de respuesta en caso de emergencias.

6. Facilita el acceso a la infraestructura: El piso técnico permite un fácil acceso a la infraestructura del data center, como las bandejas de cables, equipos de red y sistemas eléctricos. Esto simplifica el mantenimiento y la solución de problemas, lo que contribuye a reducir el tiempo de inactividad.

7. Protección del suelo original: Al instalar un piso técnico, se protege el suelo original del data center de daños causados por el tráfico constante, equipo pesado y posibles derrames.

En general, el uso de un piso técnico en un data center Tier 3 ofrece una serie de ventajas que mejoran la eficiencia operativa, la capacidad de expansión y la confiabilidad del centro de datos, lo que resulta en un mejor rendimiento y una mayor disponibilidad para los servicios y aplicaciones alojados en él.

Techo - Altura del techo

El techo de un data center de nivel Tier 3 debe diseñarse cuidadosamente para garantizar la continuidad operativa, la seguridad y el rendimiento óptimo de las instalaciones.

1. Resistencia estructural: El techo debe tener una estructura sólida y resistente para soportar el peso de los equipos y sistemas que se instalan en la parte superior, así como cualquier carga adicional que pueda ser necesaria para la instalación de sistemas de enfriamiento, paneles solares u otros equipos auxiliares.

2. Aislamiento térmico: Es importante contar con un techo bien aislado térmicamente para evitar que el calor externo afecte la temperatura interna del data center. Un buen aislamiento ayuda a mantener condiciones ambientales estables y optimiza el rendimiento del sistema de enfriamiento.

3. Protección contra filtraciones: El techo debe estar diseñado para evitar filtraciones de agua y humedad, ya que cualquier tipo de filtración puede causar daños graves en los equipos y poner en riesgo la disponibilidad de los servicios del data center. Se deben utilizar materiales resistentes al agua y contar con sistemas de drenaje adecuados.

4. Espacio para sistemas de ventilación y escape de calor: El techo debe proporcionar espacio suficiente para la instalación de sistemas de ventilación y escape de calor, como chimeneas de calor o extractores, que ayuden a eliminar el aire caliente generado por los equipos.

5. Espacio para sistemas de protección contra incendios: El techo debe permitir la instalación de sistemas de detección y supresión de incendios, como detectores de humo, rociadores y sistemas de extinción de incendios. Estos sistemas son cruciales para garantizar la seguridad del data center y proteger los equipos y datos almacenados.

6. Capacidad para pasos de cables: El techo debe permitir la canalización y administración adecuada de los cables de red, energía y otros servicios, para evitar enredos y garantizar una distribución ordenada.

7. Acceso seguro: El techo debe contar con un acceso seguro y restringido para evitar intrusiones no autorizadas y mantener la seguridad de las instalaciones.

8. Resistencia a impactos: En algunos casos, especialmente en ubicaciones propensas a eventos sísmicos o climáticos, puede ser importante considerar la resistencia del techo a posibles impactos.

Para facilitar la disipación del calor, se recomienda una altura de techo adecuada para permitir una buena circulación de aire y la instalación de sistemas de enfriamiento.

Por lo tanto, el techo de un data center Tier 3 debe ser robusto, bien aislado, impermeable, con espacio para sistemas de ventilación y protección contra incendios, y con capacidad para la gestión de cables.

Paredes

Las paredes de un centro de datos Tier 3 deben cumplir con una serie de requisitos esenciales. Esto implica la utilización de materiales de construcción robustos y técnicas de refuerzo adecuadas para asegurar la estabilidad del edificio.

Además, las paredes deben estar diseñadas para ofrecer una protección efectiva contra incendios. Esto incluye el uso de materiales resistentes al fuego, así como la separación cuidadosa de áreas de riesgo de incendio de aquellas donde los sistemas críticos operan.

En términos de aislamiento, las paredes también deben proporcionar una barrera efectiva contra las interferencias electromagnéticas (EMI por sus siglas en inglés ElectroMagnetic Interference) para proteger los equipos sensibles y la integridad de los datos almacenados en el centro de datos. Además, se debe considerar el aislamiento térmico para mantener condiciones ambientales controladas y estables.

La seguridad física es otro factor crucial. Las paredes deben ser sólidas y resistentes para proteger contra intrusiones no autorizadas.

Asimismo, se debe garantizar que las paredes permitan un espacio adecuado para el tendido de cables eléctricos y de datos, así como para la canalización de sistemas de refrigeración y ventilación. Esto facilita la instalación y el mantenimiento de la infraestructura crítica.

Sistema eléctrico

El sistema eléctrico es fundamental para el correcto funcionamiento del data center. Se deben tener en cuenta diferentes aspectos que se mencionan a continuación.

Doble ruta de alimentación

Debe tener una arquitectura con una doble ruta de alimentación eléctrica (Dual Power Path).

Se refiere a que todos los equipos y cargas críticas están conectados a dos fuentes de alimentación independientes para garantizar la redundancia. Si una fuente de energía falla, el equipo conmuta automáticamente a la otra fuente sin interrumpir el suministro de energía.

UPS

La sigla UPS es la abreviación de su nombre en inglés Uninterruptable Power Supply también llamado Sistema de Alimentación Ininterrumpida (SAI). Dicho dispositivo permite tener flujo de energía eléctrica mediante baterías, cuando el suministro eléctrico falla.

Por lo tanto, los UPS son un componente clave en la infraestructura de alimentación eléctrica del data center. Cumplen con las siguientes funciones y ventajas:

- Protección contra apagones: Cuando hay una interrupción en el suministro de energía desde la red eléctrica, el UPS entra en acción y proporciona energía ininterrumpida a los equipos conectados. Esto evita que los routers, switches, firewalls, servidores, sistemas de almacenamiento y otros dispositivos críticos se apaguen repentinamente, lo que podría causar pérdida de datos y tiempos de inactividad.
- Regulación del suministro eléctrico: También actúa como un regulador de voltaje, asegurando que los equipos reciban una alimentación eléctrica estable, lo que es importante para dispositivos sensibles y de alto rendimiento en un data center.
- Reducción del tiempo de transferencia: En una doble ruta de alimentación con dos fuentes eléctricas diferentes, el UPS juega un papel fundamental. Cuando hay un fallo en una de las fuentes, el UPS permite una transición rápida y sin interrupciones hacia la otra fuente, asegurando la continuidad del suministro eléctrico.
- Tiempo de respaldo: Los UPS están diseñados para proporcionar un tiempo de respaldo determinado, lo que permite que el personal del data center tenga tiempo para reaccionar ante un apagón inesperado o realizar una transición controlada a los generadores diésel si es necesario.
- Protección contra sobretensiones y picos: Los UPS también protegen los equipos conectados contra picos de voltaje o sobretensiones, lo que ayuda a evitar daños y problemas eléctricos en el hardware.
- Capacidad de gestión remota: Algunos UPS modernos están equipados con capacidades de gestión remota que permiten monitorear su estado y rendimiento desde una ubicación centralizada. Esto facilita el mantenimiento proactivo y la detección temprana de problemas potenciales.

Figura 4. UPS marca Dell para servidor rackeable

Generadores de respaldo

Los generadores de respaldo son un componente esencial en un data center Tier 3, ya que garantizan un suministro continuo de energía en caso de cortes prolongados. Cuando se detecta una interrupción en la alimentación principal, estos generadores se activan automáticamente en cuestión de segundos, asegurando la continuidad operativa del data center durante períodos prolongados.

Estos generadores funcionan mediante la generación de electricidad a partir de combustible, generalmente diésel. Para mantener la operación durante largos períodos, es

crucial que cuenten con tanques de almacenamiento adecuados para asegurar suficiente suministro de combustible.

Los generadores de respaldo están dimensionados cuidadosamente para manejar la carga completa del data center, incluyendo servidores, sistemas de almacenamiento, refrigeración, equipos de red y todos los dispositivos críticos. Se lleva a cabo un análisis exhaustivo de la carga para asegurar que los generadores puedan mantener todas las operaciones sin sobrecargarse, lo que garantiza un funcionamiento óptimo en situaciones de emergencia.

Sistemas de transferencia estática

Los sistemas de transferencia estática (STS), por sus siglas en inglés Static Transfer Switch están diseñados para conmutar rápidamente entre las fuentes de alimentación principal y de respaldo, en cuestión de milisegundos. Esto asegura que no haya tiempo de inactividad ni interrupción en el suministro eléctrico hacia los equipos críticos cuando se produce un cambio en la fuente de energía.

Monitoreo y gestión centralizada

El sistema eléctrico del data center Tier 3 debe contar con una monitorización y gestión centralizada que permita supervisar el rendimiento y el estado de todas las fuentes de energía, UPS, generadores y otros componentes clave. Esto ayuda a detectar y abordar cualquier problema potencial antes de que cause una interrupción en el servicio.

Protección contra sobrecargas y cortocircuitos

El sistema eléctrico debe contar con dispositivos de protección contra sobrecargas y cortocircuitos para evitar daños en los equipos y garantizar la seguridad del personal.

Puesta a tierra

La principal funcionalidad de la puesta a tierra (p.a.t) en una instalación eléctrica es la de forzar la derivación, al terreno, de las intensidades de corriente, sin importar su origen o naturaleza, ya se trate de corrientes de defecto, bajo frecuencia industrial, o debidas a cargas atmosféricas, de carácter impulsional [8].

Esto conlleva varios beneficios, que incluyen:

- Reducir la posibilidad de que se produzcan diferencias significativas de voltaje en un momento dado entre las estructuras metálicas y la tierra.

- Facilitar la detección de fallas a tierra y garantizar que las protecciones actúen de manera coordinada y efectiva, minimizando o eliminando los riesgos asociados con averías tanto para el equipo como para las personas.
- Controlar y mitigar las sobretensiones internas, tanto transitorias como temporales, que puedan surgir en la red eléctrica en ciertas condiciones de operación.
- Prevenir que las tensiones de frente pronunciado generadas por las descargas de rayos, provoquen "cebados inversos", especialmente en instalaciones exteriores y, en particular, en líneas aéreas.

La circulación de corrientes eléctricas a través de la instalación de puesta a tierra puede generar diferencias de voltaje en varios puntos, como entre la instalación de puesta a tierra y el terreno que lo rodea o entre diferentes puntos dentro de la instalación. Por esta razón, es esencial diseñar la instalación de puesta a tierra de tal manera que, incluso cuando se produzcan estas diferencias de voltaje, se logren los siguientes objetivos:

- Seguridad de las personas: La protección de las personas es la principal preocupación y objetivo fundamental de la instalación de puesta a tierra. Esto implica garantizar que las personas estén a salvo de posibles descargas eléctricas y riesgos relacionados con diferencias de voltaje peligrosas.

- Protección de las instalaciones: Además de la seguridad de las personas, la instalación de puesta a tierra también tiene como objetivo proteger los equipos e instalaciones eléctricas de posibles daños causados por sobretensiones, cortocircuitos u otros eventos eléctricos adversos.

- Mejora de la calidad del servicio: Una puesta a tierra adecuada contribuye a mantener una operación eléctrica confiable y estable, lo que se traduce en una mejor calidad de servicio para los usuarios finales, evitando interrupciones y problemas en la distribución de energía.

- Establecimiento y mantenimiento de un potencial de referencia: La puesta a tierra también se utiliza para establecer un potencial de referencia común en todo el sistema eléctrico, lo que facilita la operación y el funcionamiento seguro de los equipos y sistemas conectados.

Es importante destacar que, si bien todos estos objetivos son relevantes, la seguridad de las personas se considera la máxima prioridad en la instalación de puesta a tierra, lo que no implica que se menosprecie la importancia de los demás objetivos. La instalación de puesta a tierra se diseña para abordar de manera integral estos aspectos y garantizar un entorno eléctrico seguro y confiable.

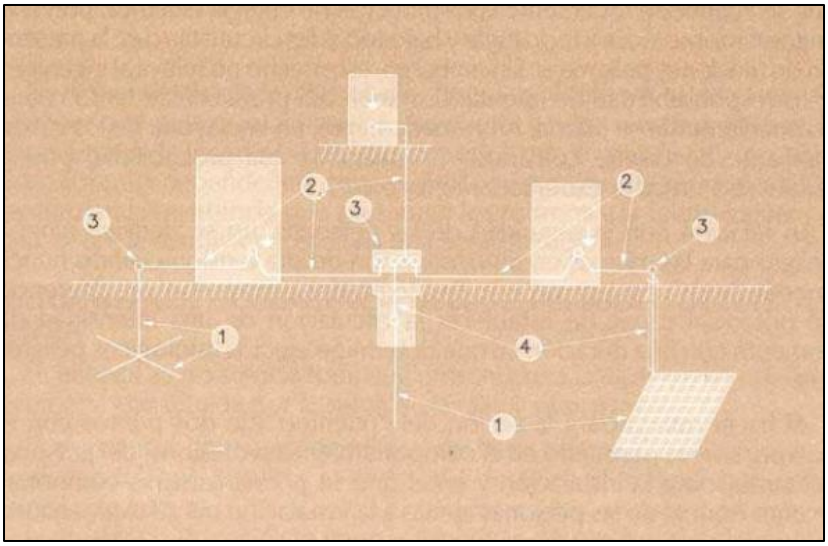

Figura 5. Esquema de una instalación de puesta a tierra y partes que comprende

1. Electrodo de (puesta a) tierra: conductor o grupo de conductores que están enterrados y se utilizan para establecer una conexión con la tierra. Los conductores sin aislamiento que están en contacto con el suelo y se utilizan para conectar al electrodo se considerarán una parte integral de dicho electrodo.
2. Línea de tierra: Se refiere al conductor o conjunto de conductores que conecta el electrodo de tierra con una parte de la instalación que necesita estar conectada a tierra. Esto se aplica cuando estos conductores están ubicados fuera del terreno o incluso si están en contacto con el suelo, pero están aislados de él.
3. Punto de puesta a tierra: Se trata de un punto de conexión que, por lo general, se encuentra fuera del terreno y se utiliza como punto de unión entre las líneas de tierra y el electrodo. Esta conexión puede establecerse directamente o mediante líneas de enlace que conectan con el electrodo.
4. Línea de enlace con el electrodo de (puesta a) tierra: Cuando se encuentra un punto de puesta a tierra, se hace referencia a la "línea de enlace con el electrodo de tierra" como la porción de la línea de tierra que se extiende desde el punto de puesta a tierra hasta el electrodo de tierra. Esto es aplicable siempre y cuando el conductor esté ubicado fuera del terreno o aislado de él.

Tableros eléctricos

Un tablero eléctrico desempeña un papel fundamental en la gestión de sistemas eléctricos al cumplir sus funciones esenciales de medición, control, maniobra y protección. Su relevancia es fundamental en cada instalación eléctrica, lo que justifica su presencia constante sin importar la tensión, la categoría o el tamaño de la instalación.

La trascendencia de los tableros eléctricos es tan significativa que podría afirmarse categóricamente que la ejecución y operación de cualquier tipo de instalación eléctrica resulta inviable sin la incorporación de algún tipo de tablero eléctrico.

Sistema de Climatización

La climatización desempeña un papel crucial al evitar el exceso de calor en los dispositivos y al establecer un entorno controlado para salvaguardar a los servidores y otros elementos esenciales.

Los data center Tier 3 suelen utilizar sistemas de enfriamiento avanzados, como sistemas de aire acondicionado de precisión, enfriamiento por agua, enfriamiento por líquido o incluso técnicas más innovadoras, como el uso de aire exterior en climas adecuados. Estos sistemas están diseñados para mantener una temperatura estable y controlada en el interior.

Refrigeración mediante agua

La utilización de agua de un lago como medio de refrigeración puede ser una opción económica y factible en ciertos escenarios. Sin embargo, existen diferentes aspectos cruciales que se deben considerar antes de poner en marcha este tipo de sistema.

Antes de emplear el agua de un lago, es fundamental asegurar el cumplimiento de todas las regulaciones y permisos necesarios. Podría ser imprescindible obtener la aprobación de entidades gubernamentales para extraer y utilizar el agua de manera responsable, evitando posibles impactos adversos en el entorno. Además, es esencial considerar cómo devolver el agua utilizada de manera adecuada para minimizar cualquier efecto negativo sobre el lago.

La calidad del agua también es un punto crucial a tener en cuenta. Se debe llevar a cabo un análisis exhaustivo para determinar si es adecuada para su utilización en sistemas de refrigeración. La presencia de algas, sedimentos, contaminantes químicos u otros elementos podría afectar negativamente en el desempeño y la durabilidad de los equipos de refrigeración.

El agua del lado se utiliza para absorber el calor generado por los sistemas de refrigeración, lo que hace necesario un sistema eficiente de intercambio de calor, como intercambiadores de calor o torres de enfriamiento. Este sistema debe estar cuidadosamente planificado en términos de ubicación y diseño para maximizar la eficacia del proceso de transferencia de calor.

Por último, los sistemas que aprovechan agua de lago demandan un mantenimiento periódico y una supervisión constante para garantizar un rendimiento óptimo y prevenir la acumulación de sedimentos o el crecimiento de algas. Además, deben considerarse los gastos relacionados con el bombeo y el tratamiento del agua, así como el consumo energético de los dispositivos de intercambio de calor.

Normativa sobre la utilización del agua

En Argentina, la legislación y los permisos relacionados con la extracción y uso de agua de un lago para fines comerciales o industriales están regulados principalmente por la Ley Nacional de Agua N° 25.688 y su Decreto Reglamentario N° 804/2010.

Pasillos fríos - Pasillos Calientes

El significativo consumo energético de los data centers impulsó el desarrollo de estrategias de contención de aire frío y caliente. Tanto la contención de pasillos calientes como de pasillos fríos brindan notables ahorros energéticos en comparación con las configuraciones convencionales que carecen de esta.

Podemos mencionar diferentes ventajas con la implementación de contención del aire caliente o frío.En este contexto, es esencial mencionar que la disposición en fila de pasillos caliente/frío resulta fundamental. Esta alineación precisa implica que los frentes de los racks deben estar orientados hacia los frentes de los racks de la fila adyacente, generando pasillos calientes y fríos de manera alternada. A continuación, se detallarán las ventajas.

- **Optimización de la configuración de refrigeración**: Se posibilita la configuración de sistemas de refrigeración a temperaturas más elevadas, maximizando la eficiencia energética. En comparación, en sistemas de refrigeración que carecen de contención, se requiere una temperatura mucho más baja, en torno a un promedio de 13°C, para garantizar el correcto funcionamiento de los equipos de TI (Tecnologías de la Información, que abarcan servidores, computadoras, routers, switches, puntos de acceso, entre otros).

- **Mantenimiento de Temperaturas Uniformes**: La contención asegura que el suministro de aire proveniente de la unidad de refrigeración alcance los frentes de los equipos de TI sin mezclarse con el aire caliente. Este enfoque garantiza que la temperatura del aire de entrada a los equipos sea idéntica a la temperatura del suministro de la unidad de refrigeración, logrando uniformidad en las condiciones de entrada de aire.

- **Reducción de costos de humidificación/deshumidificación**: Al eliminar la mezcla de aire frío y caliente, se permite elevar la temperatura de refrigeración, lo que a su vez facilita el funcionamiento a temperaturas superiores al nivel de humedad. Suministrar aire por encima del nivel de humedad prescinde de la necesidad de deshumidificar. La ausencia de deshumidificación conlleva ahorros de agua y energía, ya que no se requiere la adición ni la eliminación de humedad.

Contención de pasillos calientes

El sistema de contención de pasillos calientes HACS (por sus siglas en inglés Hot Aisle Containment System) se destaca por su capacidad para cerrar el pasillo caliente, limitando así el flujo de aire caliente que emana de los equipos TI. Este enfoque transforma el resto de la sala en un cámara de suministro de aire frío. La contención del pasillo caliente representa una solución que segmenta eficazmente el flujo de aire frío y caliente, logrando un aislamiento térmico óptimo.

La siguiente Figura 6 muestra el principio básico de la técnica HACS.

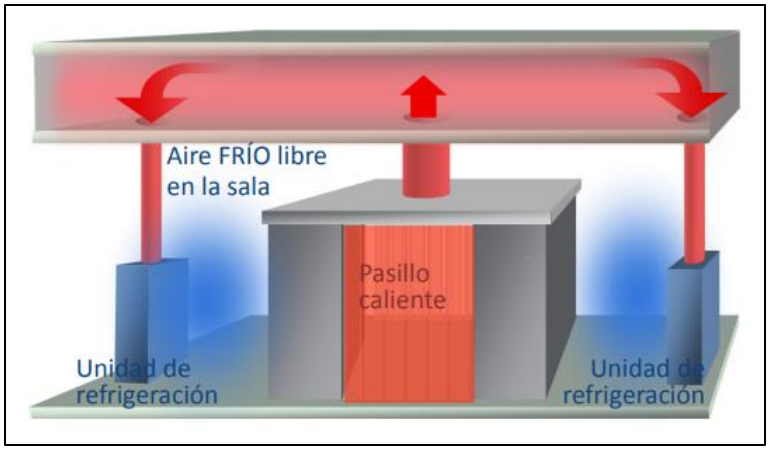

Figura 6. Principio básico de técnica HACS

Finalmente, la Figura 7 ejemplifica un caso del sistema HACS, donde se implementan unidades de refrigeración dispuestas en fila, operando como áreas autónomas e independientes.

Figura 7. Ejemplo de un sistema HACS

Contención de pasillos fríos

El sistema de contención de pasillos fríos CACS (por sus siglas en inglés Cold Aisle Containment System) se destaca por su capacidad para cerrar el pasillo frío, transformando el resto de la sala en una cámara de retorno de aire caliente de gran tamaño. La contención del pasillo frío permite separar el flujo de aire frío del flujo de aire caliente.

La Figura 8, presentada a continuación, ejemplifica el principio básico del sistema CACS en un data center con piso técnico y unidades de refrigeración perimetrales.

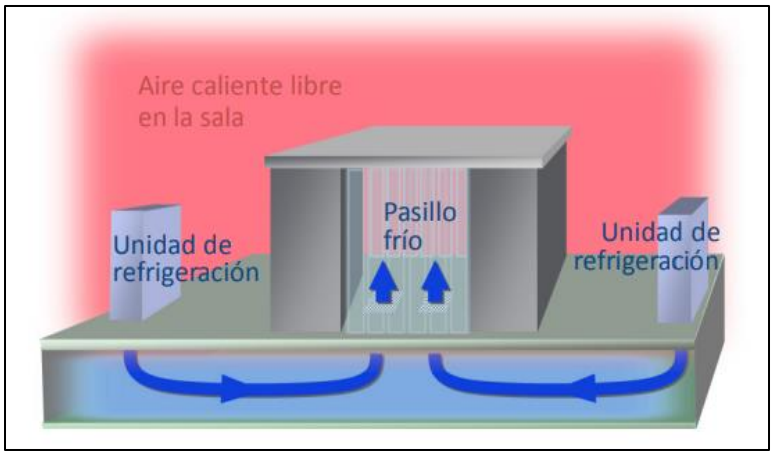

Figura 8. Principio básico de técnica CACS

En la Tabla 2 [9], se presenta una síntesis de los sistemas HACS y CACS en función de las particularidades analizadas anteriormente.

Característica	**HACS**	**CACS**	**Comentario**
Capacidad para mantener una temperatura interior estándar de diseño	Sí	No	A través del sistema HACS, es viable fijar un umbral superior para la refrigeración, preservar una temperatura ambiente de trabajo de 24°C y aprovechar las horas de operación en el modo de economía.
Aprovechamiento de las ventajas de las horas de funcionamiento del modo economizador	Sí	No	La cantidad de horas de funcionamiento del modo economizador en el sistema CACS está restringida tanto por la temperatura máxima de entorno de trabajo como por las restricciones de temperatura de los equipos TI que no se encuentran en los racks.
Temperatura aceptable para equipamiento no dispuesto en racks	Sí	No	En CACS, puesto que la contención se aplica al pasillo frío, el resto del data center adquiere una temperatura elevada. El equipamiento expuesto debe someterse a evaluaciones para determinar si es apto para el funcionamiento a temperaturas elevadas.
Facilidad de implementación con los sistemas de refrigeración de la sala	No	Sí	CACS es la opción preferida para la adaptación de data centers con piso técnico o refrigeración de sala con retorno ambiental.
Nuevos diseños de data centers	Sí	No	El costo de construcción de nuevos data centers con sistema HACS o CACS es idéntico. Sin embargo, implementar un sistema HACS mejorará la eficiencia general del data center.

Tabla 2. Sistemas HACS y CACS

Cableado estructurado

El concepto de cableado estructurado engloba una serie de normas y pautas que rigen la infraestructura de redes y los medios de transmisión, junto con métodos para la correcta instalación y mantenimiento con el objetivo de organizar la infraestructura de red, promoviendo un sistema de cableado flexible y confiable [10]. Este sistema puede ser utilizado por diferentes equipos producidos por diversos fabricantes, ofreciendo facilidades para la reubicación de puntos de trabajo, ya sea como una sustitución de equipos activos, o en la necesidad de una instalación de cables desde cero. El cableado estructurado aporta un fundamento esencial para la gestión eficiente de las redes de comunicación.

Existe una amplia gama de estándares establecidos para el ámbito del cableado estructurado. Las organizaciones estadounidenses TIA (Telecommunications Industry Association) y ANSI (American National Standards Institute) crearon el estándar ANSI/TIA-568, que detalla los procedimientos para proyectar, implementar y administrar un Sistema de Cableado Estructurado (SCE).

Paralelamente, en Europa, Asia y África, se establecieron estándares definidos por la ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission). La norma ISO/IEC 11801 despliega características genéricas de cableado para abordar las necesidades de los usuarios.

ANSI/TIA-568: Define los principales conceptos de cableado estructurado, sus elementos, la topología, los tipos de cables y salidas, distancias y pruebas de certificación.

ANSI/TIA-569: Define el área ocupada por los elementos del cableado estructurado, las dimensiones, porcentaje de saturación de trayectorias y demás información de construcción.

ANSI/TIA-606: Especifica las técnicas y métodos para identificar y administrar la infraestructura de telecomunicaciones.

Basado en estas normas fueron creadas normas específicas para ambientes residenciales (TIA-570). Ambientes industriales (TIA-1005), ambientes de Data Center (TIA-942) y ambientes hospitalarios (TIA-1179) entre otros.

ANSI/TIA-570: Se aplica a los sistemas de cableado y sus respectivos espacio y trayectorias para predios residenciales multiusuarios, así como casas individuales. Específica sistemas de cableado con la intención de soportar una amplia gama de aplicaciones de telecomunicaciones en entornos residenciales.

TIA 1005: Las normas ANSI/TIA 1005 – Telecommunication Infrastruture Standard for Industrial Premises y la norma europea ISO/IEC 24702 Information Technology – Generic Cabling – Industrial Premises, especifican prácticas de diseño y construcción del cableado estructurado para entornos industriales que aborden requisitos, distancias, configuraciones y topologías que complementen el estándar general de Edificios Comerciales (EIA-TIA 568, ISO / IEC 11801 o NBR 14565).

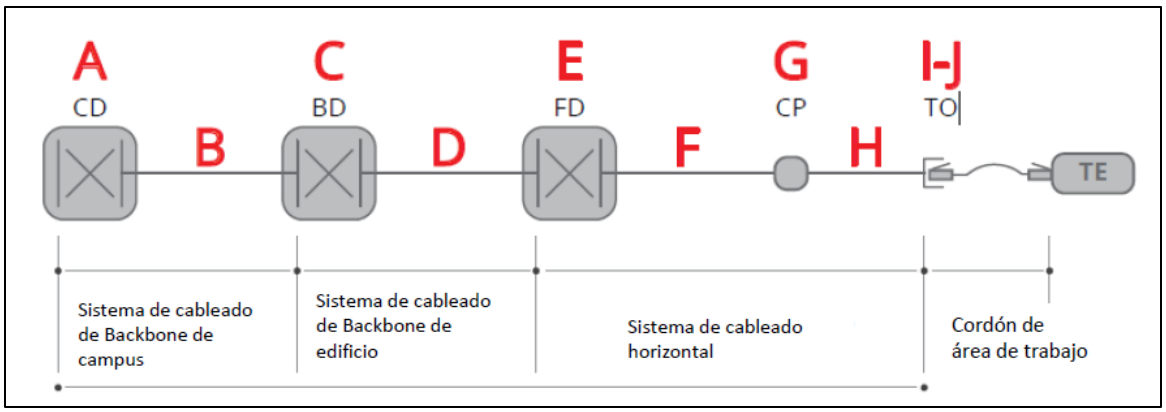

Figura 9. Elementos del cableado estructurado (ISO/IEC 11801)

Estructura del cableado en edificios corporativos

A) Distribuidor de Campus (CD)
B) Backbone de Campus
C) Distribuidor de Edificio (BD)
D) Backbone de Edificio
E) Distribuidor de Piso (FD)
F) Cableado Horizontal
G) Punto de Conexión (CP)
H) Cable de Punto de Conexión (Cable de CP)
I) Toma de Telecomunicaciones Multiusuario (MUTOA)
J) Toma de Telecomunicaciones (TO)

Componentes del cableado estructurado

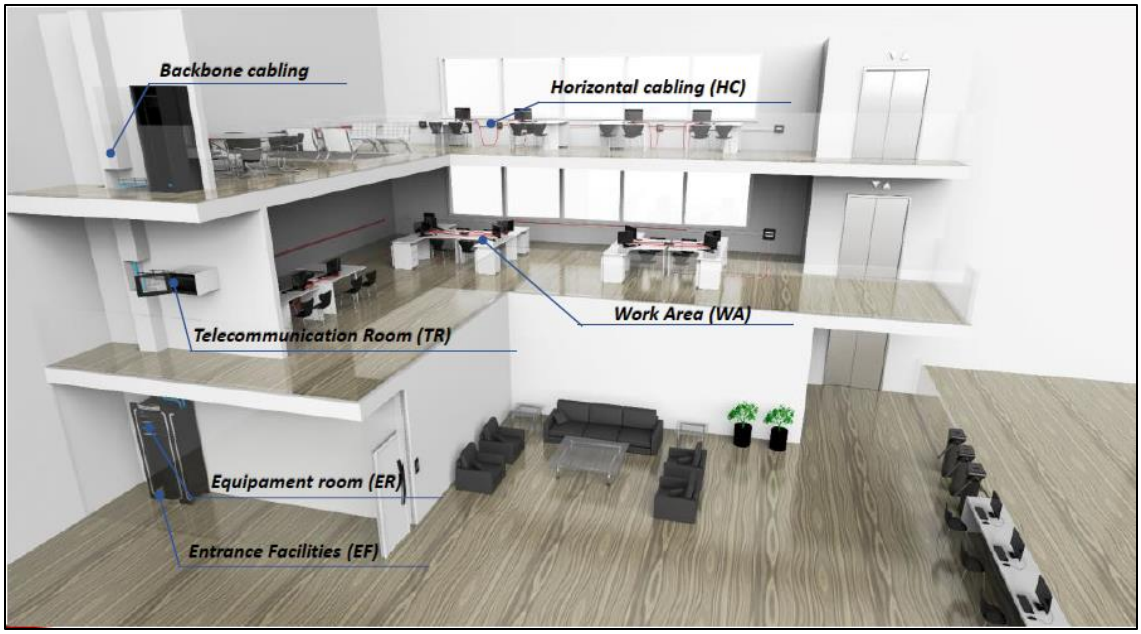

Figura 10. Sistema de Cableado Estructurado - Furukawa

Área de trabajo

Work Area (WA) es el espacio donde los dispositivos de comunicación se conectan con la infraestructura de cableado. Los componentes suelen comprender dispositivos como teléfonos, computadoras, access point, entre otros.

Cableado horizontal

El sistema de cableado horizontal está compuesto por cables y rutas que establecen la conexión entre el cuarto de telecomunicaciones y el área de trabajo.

Este sistema se compone de dos elementos esenciales, por un lado el cable horizontal y el hardware de conexión (también conocido como "cableado horizontal" - "horizontal cabling"). Estos componentes proporcionan la infraestructura básica para transmitir señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones.

Por otro lado, el otro elemento esencial son las rutas y espacios horizontales (también denominados "sistemas de distribución horizontal"). Estas rutas y espacios desempeñan un papel fundamental al distribuir y sostener el cable horizontal, así como al facilitar la conexión del hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. En esencia, estas rutas y espacios son los "contenedores" del cableado horizontal.

El cableado horizontal engloba los componentes esenciales que permiten una comunicación eficaz dentro de un entorno de trabajo. Esto incluye:

1. Salidas de Telecomunicaciones en el Área de Trabajo: estas salidas, también conocidas como Work Area Outlets (WAO) en inglés, son puntos de conexión ubicados en las áreas de trabajo que permiten a los usuarios conectar dispositivos de red y telecomunicaciones, como computadoras y teléfonos.

2. Cables y Conectores de Transición:estos elementos actúan como el enlace vital entre las salidas del área de trabajo y el cuarto de telecomunicaciones. Son responsables de transportar las señales de datos y voz de manera confiable a través de las distancias requeridas.

3. Paneles de Empalme (Patch Panels) y Cables de Empalme: Los patch panels son dispositivos que facilitan la organización y gestión de las conexiones en el cuarto de telecomunicaciones. Los cables de empalme se utilizan para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones, asegurando una distribución efectiva de las señales y facilitando la administración de las conexiones.

Topología

Las normas establecen que el sistema de cableado estructurado siempre adopte la topología en el modelo estrella. Una topología estrella de cables se puede reordenar en los puntos de cross-connects (patch panels) para obtener una configuración de bus o anillo si la situación lo requiere.

El cableado horizontal se define específicamente como una topología estrella, en la que cada punto de trabajo (toma) está conectado al cuarto de telecomunicaciones.

De acuerdo con la norma TIA-568.1-E, el cableado horizontal debe cumplir con las siguientes especificaciones:

- La estructura debe conformar una topología en estrella con una longitud máxima de 90 metros.
- Se deben proporcionar al menos dos enlaces permanentes para cada área de trabajo.
- Los cuatro pares del cable deben ser terminados en el conector.
- El cable de par trenzado debe tener una impedancia de 100 ohms, de acuerdo con la norma ANSI/TIA 568 E.2.

Cuarto de telecomunicaciones

Telecommunication Room (TR) es la sala donde se encuentran todos los elementos de interconexión entre backbone y cableado horizontal.

Cableado Vertical

El propósito fundamental del cableado vertical (backbone cabling) en un entorno como un data center Tier 3 es facilitar conexiones estratégicas y esenciales entre áreas clave del edificio, como los cuartos de entrada de servicios, los cuartos de equipo y los cuartos de telecomunicaciones. Además, este tipo de cableado desempeña un papel fundamental en la interconexión vertical entre los distintos pisos de edificios de múltiples niveles.

El cableado backbone no se limita únicamente a los medios de transmisión, como los cables utilizados, sino que también engloba elementos cruciales como los puntos principales e intermedios de conexión cruzada y las terminaciones mecánicas. Su función principal radica en establecer una red de conectividad confiable entre los diversos gabinetes de telecomunicaciones y, a su vez, entre estos gabinetes y la sala de equipamiento central.

En contraste con el cableado horizontal, que suele mantener una estructura general, el cableado vertical en esta etapa ya no resulta económico ni práctico de mantener en una sola estructura unificada para la telefonía y los datos. Por lo tanto, es conveniente realizar instalaciones independientes para cada uno de estos sistemas. Esto ofrece una mayor flexibilidad para el diseño y permite adaptaciones futuras sin interrupciones significativas.

Topología

El cableado vertical debe ser dispuesto siguiendo una estructura en forma de estrella con una jerarquía establecida. Se prohíbe tener más de dos niveles jerárquicos de puntos de conexión cruzada en el mismo backbone, con el fin de minimizar la pérdida de calidad de las señales y simplificar la administración del sistema de cableado estructurado implantado.

CAPÍTULO IV: DISEÑO DETALLADO

Propuesta

Se presenta la propuesta de establecer y ubicar un data center de nivel Tier 3 en el establecimiento de "La Lagunilla", situado en la provincia de Salta. Esta iniciativa busca brindar un entorno tecnológico de vanguardia, en línea con los estándares de disponibilidad y rendimiento característicos de la categoría Tier 3 en data centers.

Se suministran las coordinadas geográficas precisas del establecimiento propuesto:

- Latitud: -24,76687° o 24° 46' 1" sur
- Longitud: -65,29736° o 65° 17' 51" oeste
- Altitud: 1.301 metros (4.268 pies)

Figura 11. La Lagunilla desde una perspectiva amplia

Figura 12. La Lagunilla

Elementos para la formulación

Para este trabajo se llevó a cabo un exhaustivo análisis en la ciudad de Salta, donde se observó que los establecimientos actuales carecen de data centers que cumplan con los requisitos esenciales para garantizar la disponibilidad y la confiabilidad de los servicios. En vista de esta situación, proponemos la migración de sus operaciones al data center Tier 3 diseñado. Esta migración conlleva una serie de beneficios significativos, entre los cuales se destaca la eliminación de la necesidad de realizar costosos y prolongados mantenimientos de equipos, lo que se traduce en un ahorro de tiempo y recursos.

Además, se identificaron diversas entidades gubernamentales, como el 911, el Ministerio de Economía, la Ciudad Judicial, Edesa y Aguas del Norte, que podrían beneficiarse de nuestros servicios. Asimismo, empresas del sector privado, como Coca Cola, Cosalta y otras, también pueden encontrar en el data center diseñado una solución confiable y eficiente para sus necesidades de almacenamiento y procesamiento de datos. En este proyecto se busca brindar a nuestros potenciales clientes un entorno de alta calidad para respaldar sus operaciones y garantizar la continuidad de sus servicios.

El establecimiento denominado "La Lagunilla" se caracteriza por la disposición de dos accesos distintos y autónomos. Uno de estos accesos se encuentra ubicado en la vía conocida como Acceso Norte Ruta 9, mientras que el segundo acceso está situado en la autopista a través de la Avenida Asunción. La presencia de dos accesos resulta altamente beneficiosa para agilizar el desplazamiento en el sitio.

La distancia media a lo largo de avenidas y autopistas se establece en 30 kilómetros, y el tiempo estimado de desplazamiento desde los puntos más remotos de la ciudad es de aproximadamente 30 minutos en vehículo.

En lo que respecta a los posibles clientes del centro de datos, los tiempos de desplazamiento desde sus respectivas ubicaciones se desglosan de la siguiente manera:

- Ministerio de Seguridad (911): La distancia estimada es de aproximadamente 21 kilómetros, lo que se traduce en un tiempo de viaje aproximado de 33 minutos.
- Ministerio de Economía: La distancia es de 26 kilómetros, lo que implica un tiempo de viaje de alrededor de 40 minutos.
- Edesa: Se encuentra a una distancia de 17 kilómetros, lo que se traduce en un tiempo de viaje aproximado de 30 minutos.
- Aguas del Norte: La distancia es de 20 kilómetros, con un tiempo de viaje estimado de 35 minutos.
- Coca Cola: La distancia es de 20 kilómetros, con un tiempo de viaje estimado de 35 minutos.
- Cosalta: A una distancia de 19 kilómetros, el tiempo de viaje estimado es de aproximadamente 33 minutos.

Estos datos confirman la ubicación estratégica del data center en relación a los principales centros de interés y clientes, optimizando tiempos de viaje y accesibilidad.

Descripción del proyecto

El predio designado para el data center estará equipado con múltiples medidas de seguridad. Para acceder al área, inicialmente se requerirá una tarjeta de identificación. Esta tarjeta se escaneará en un dispositivo y, en caso de que la respuesta sea positiva, se abrirá la puerta de acceso.

A lo largo del trayecto hacia el edificio, se dispondrán cámaras de seguridad en ubicaciones estratégicas. Estas cámaras estarán destinadas a verificar si la persona que ingresa cuenta con la autorización adecuada para el acceso.

El predio contará con una entrada principal donde se encontrará ubicada una recepción. En el ala este, estará ubicada el área técnica la cuál requerirá una tarjeta de identificación que otorgará o negará el acceso. En esta área se encontrará el centro de monitoreo donde emplearán su oficio los administradores de red, técnicos de soporte y técnicos de energía y UPS. Además, se encontrarán dos oficinas (una de las cuales destinada para gerencia y la otra para personal de monitoreo de cámaras de seguridad del lugar) y una cocina - comedor.

Ingresando hacia el ala oeste encontramos la sala de equipos donde un guardia de seguridad supervisará el acceso. Este guardia estará equipado con un detector de metales, que se utilizará como el primer paso para ingresar a la sala de racks. Una vez completada esta etapa, el personal autorizado deberá someterse a un detector de datos biométricos para verificar la autenticidad de su identificación en una última instancia. Dentro de la sala de racks, se implementará un sistema de vigilancia con cámaras que cuentan con detección de movimiento para garantizar la seguridad de la infraestructura y los equipos alojados en esta área.

Dentro de esta ala oeste también se encontrará la sala de energía, la sala de armado de equipos, y la sala de NOC (Network Operations Center - Centro de Operaciones de Red) donde se encontrarán ubicados los jefes del área técnica.

Redundancia de equipos

A continuación, se procederá a describir en detalle cada uno de los sectores que componen el centro de datos tier 3. Es importante destacar que se provee la implementación de redundancia en múltiples aspectos clave, incluyendo:

- **Conectividad**: La redundancia de conectividad al data center se logra al contar con tres rutas de fibra óptica independientes, proporcionadas por ARSAT, Telecom y Claro.
- **Sistema de refrigeración**: Doble sistema de refrigeración de tal modo que, si uno de los sistemas falla o detecta un problema, otro puede asumir el control para evitar cualquier impacto en la temperatura del centro de datos.
- **Sistema de alimentación de energía**: Al poder tomar distribución de energía a partir del electroducto de TermoAndes y el electroducto de TRANSNOA se brindará la correspondiente doble alimentación de energía eléctrica.

- **Sistema de generación mediante grupo electrógeno**: La presencia de dos grupos electrógenos, estos están configurados de manera que uno de ellos pueda entrar en funcionamiento automáticamente el otro en caso de necesidad.
- **Sistemas de alimentación ininterrumpida (UPS)**: La presencia de dos unidades UPS N+1 significa que hay una unidad de UPS adicional en espera para asumir el control en caso de que falle la unidad principal.

La redundancia en un data center Tier 3 es indispensable porque uno de los principales objetivos de un data center Tier 3 es proporcionar alta disponibilidad y confiabilidad de los servicios y datos alojados en él. Un data center Tier 3 está diseñado para minimizar el tiempo de inactividad y garantizar que los sistemas estén disponibles la mayor parte del tiempo posible. La redundancia desempeña un papel crucial en la consecución de este objetivo por varias razones:

- Minimizar el tiempo de inactividad planificado: Para realizar tareas de mantenimiento, actualización de hardware o solución de problemas, es necesario realizar ciertas acciones que pueden afectar la disponibilidad de los servicios. La redundancia permite realizar estas tareas sin interrumpir los servicios principales, ya que los sistemas redundantes pueden asumir la carga de trabajo.

- Tolerancia a fallos: Los data centers Tier 3 están diseñados para ser tolerantes a fallos. Esto significa que pueden resistir fallos de componentes individuales, como discos duros, fuentes de alimentación o incluso servidores completos, sin que los servicios se vean afectados. La redundancia de hardware, como discos en espejo o servidores gemelos, garantiza que haya componentes de respaldo disponibles para reemplazar inmediatamente los componentes defectuosos.

- Disponibilidad continua: La redundancia también se aplica a las rutas de conectividad, la energía y los sistemas de enfriamiento. Esto asegura que, incluso en caso de un fallo en uno de estos sistemas, haya una vía alternativa o un sistema redundante listo para tomar el control y mantener la continuidad operativa.

- Escalabilidad: La redundancia no solo se trata de prevenir fallos, sino también de permitir la expansión y el crecimiento sin interrupciones. Los sistemas redundantes pueden escalarse de manera más efectiva para satisfacer las demandas crecientes de recursos y servicios.

Plano data center tier 3

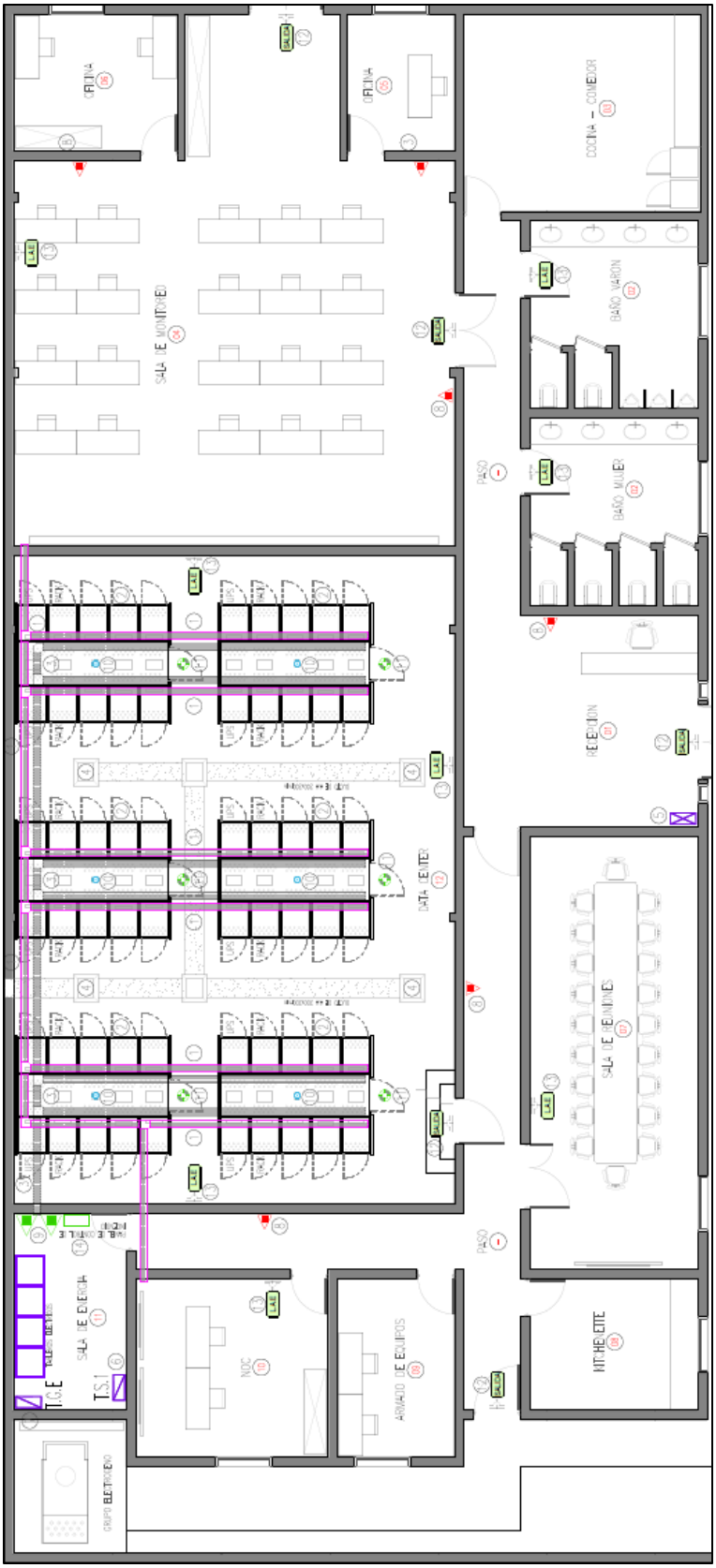

Figura 13. Plano completo data center tier 3

Referencias del plano

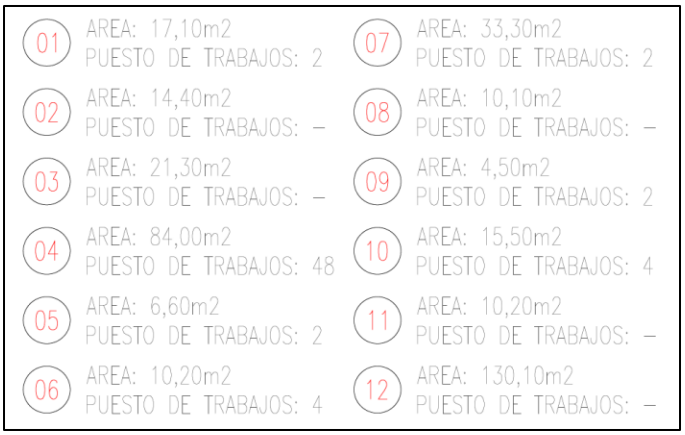

Figura 14. Detalle por local

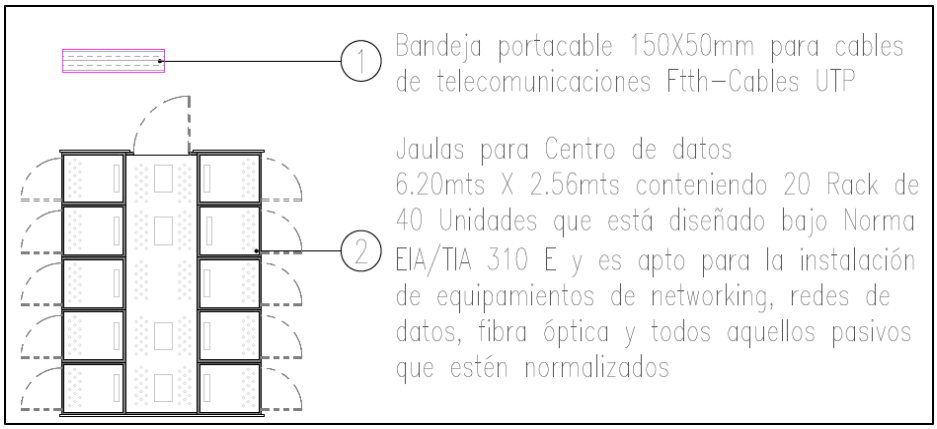

Figura 15. Detalle referencia - Telecomunicaciones

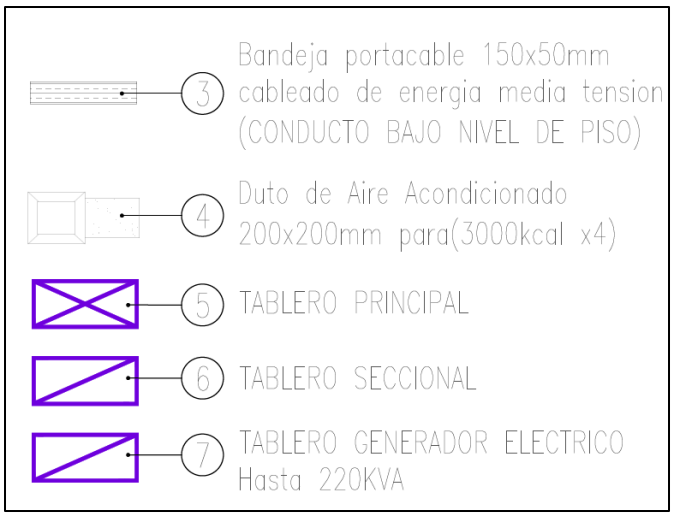

Figura 16. Detalle referencia - Sistema de energía

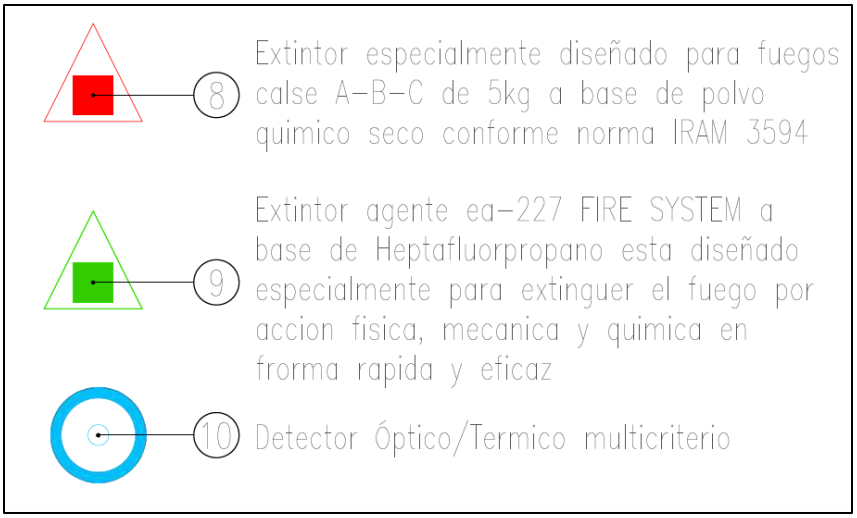

Figura 17. Detalle referencia - Sistema de emergencia

Sala de racks

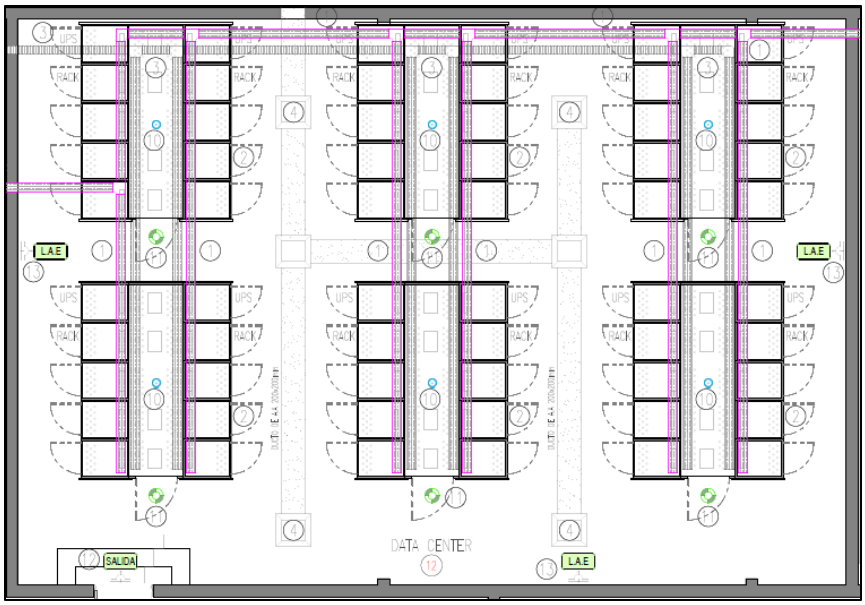

Figura 18. Jaulas de racks

La sala de racks está diseñada con 6 jaulas que incluyen 20 racks cada una. Cada rack tiene capacidad de 40 unidades. En la figura 18 podemos observar las bandejas portacables, piso técnico, extintores, detectores ópticos/ térmicos multicriterio y salidas de emergencia con sus respectivas señalizaciones led.

Sala de Monitoreo - Oficinas

Figura 19. Sala de monitoreo en conjunto con sector oficinas

En la figura 19 se aprecia que la sala de monitoreo está equipada con un total de 20 puestos de trabajo, y presenta una pared completa de pantallas que posibilitan la supervisión continua de todos los parámetros cruciales para el funcionamiento.

Asimismo, se pueden identificar dos oficinas, una de las cuáles es para el encargado de la video vigilancia del lugar mientras que la oficina superior está asignada a la gerencia.

Sala de energía - Armado de equipos - NOC

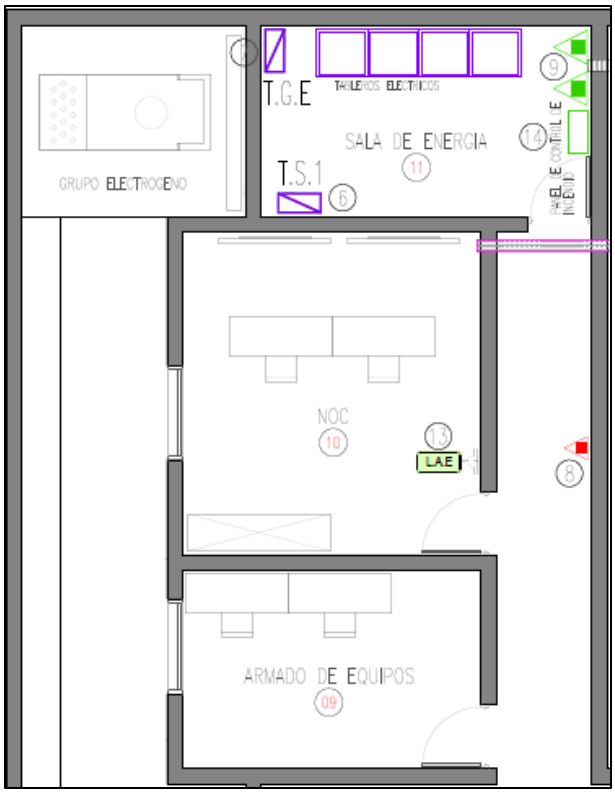

Figura 20. Sector de energía, NOC y armado de equipos

Dentro de la sala de energía, se puede notar la existencia de tableros eléctricos, tanto el tablero principal como el tablero seccional, además de la presencia del generador eléctrico.

En cuanto al Centro de Operaciones de Red (NOC), se disponen de dos puestos de trabajo específicamente destinados para los jefes del área IT.

Sala de reuniones - Kitchenette

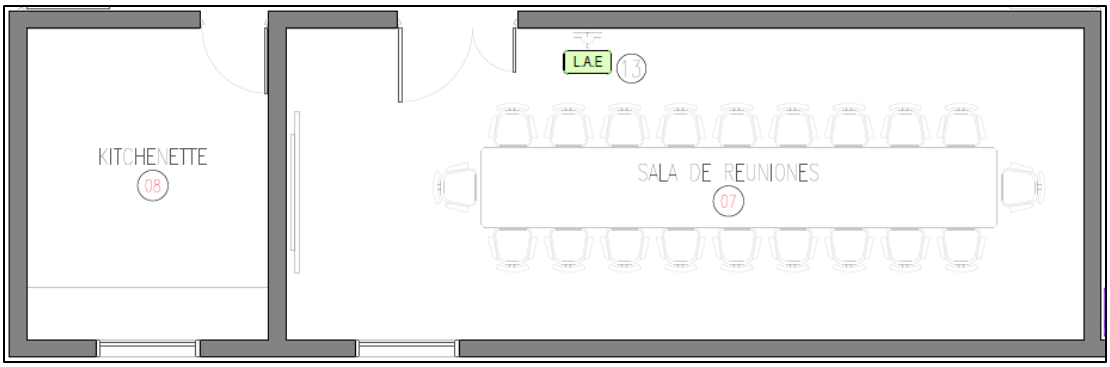

Figura 21. Sala de reuniones para 20 personas y kitchenette

También en el diseño se planificó tener una sala de reuniones amplia con capacidad para 20 personas y una kitchenette.

Recepción - Baños - Cocina - Comedor

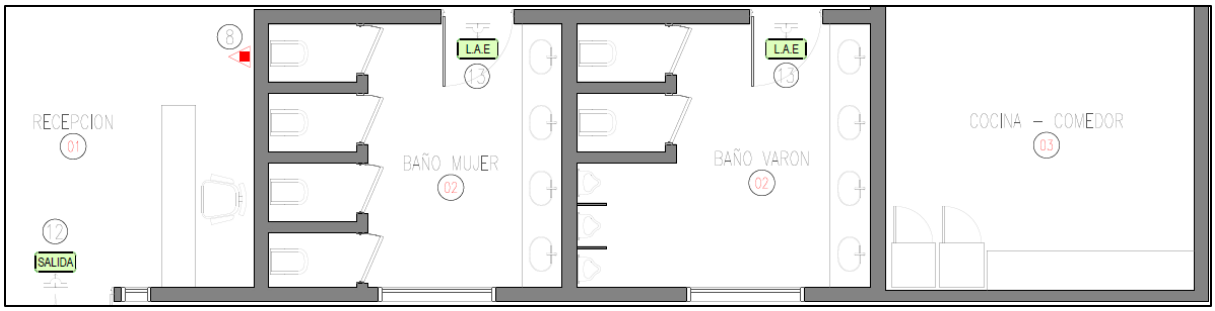

Figura 22. Recepción, sector baños, cocina-comedor

Por último, observamos la recepción que se encuentra apenas se ingresa al edificio, los baños y la cocina - comedor.

CAPÍTULO V: CONECTIVIDAD DEL DATA CENTER

La conectividad del data center se establecerá a través de redes de fibra óptica, con la participación de destacados proveedores de servicios de telecomunicaciones, tales como Telecom, Claro y ARSAT.

¿Qué es la fibra óptica?

La fibra óptica es un sistema de transmisión de datos que utiliza impulsos fotoeléctricos a través de un cable fabricado con vidrio transparente u otros materiales plásticos de características similares. Estos hilos pueden ser extremadamente delgados y son el medio principal para la transmisión de señales. [11]

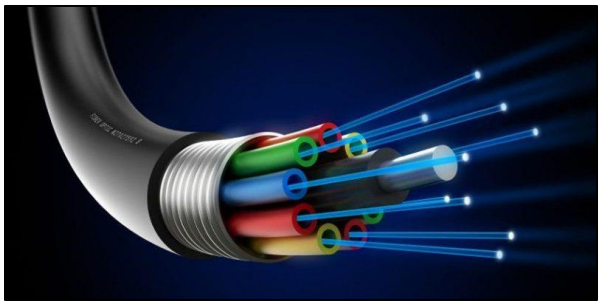

Figura 23. Fibra óptica

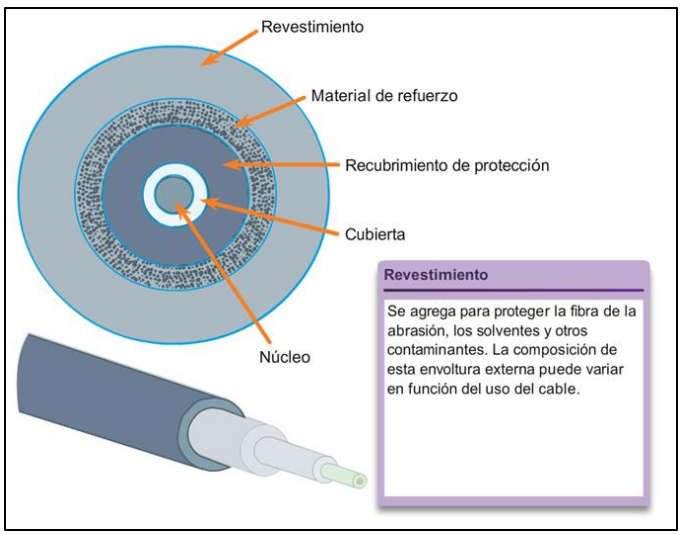

Figura 24. Como está construida la fibra óptica

A través de estos cables, se realiza la transmisión de una señal de luz desde un extremo del cable al otro. Esta luz puede ser generada mediante un láser o un LED, y cuenta con múltiples ventajas mencionadas a continuación:

- Total inmunidad a interferencias electromagnéticas
- Dimensiones reducidas
- Seguridad en el transporte de información
- Mayores distancias de transmisión
- Ancho de banda de comunicación superior

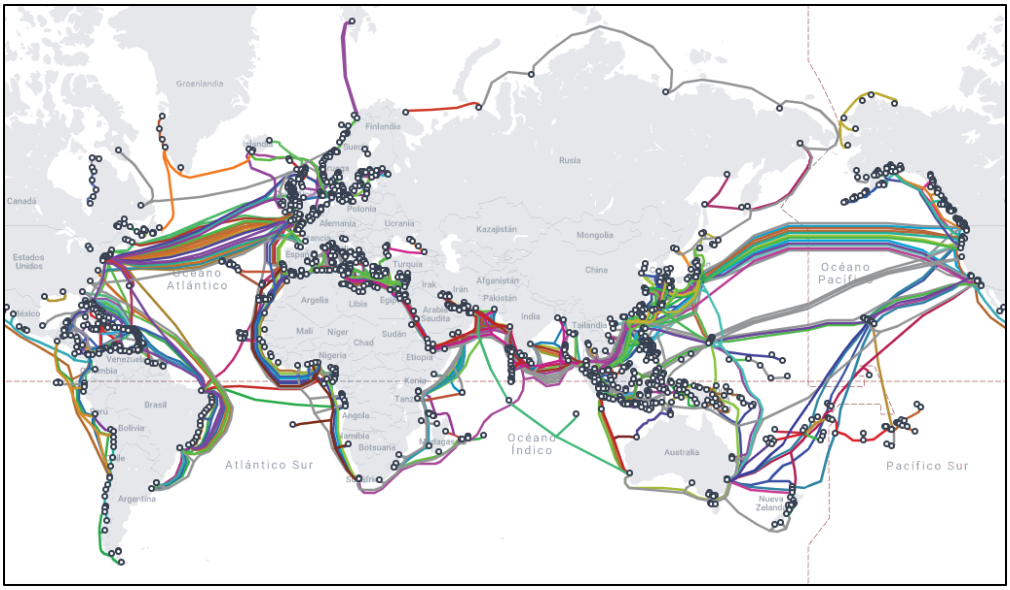

Figura 25. Fibra óptica submarina mundial

Tipos de fibra óptica

Hay diversas categorías de fibras ópticas, que se distinguen por las propiedades de refracción de su núcleo y su revestimiento, así como por cómo varía esta refracción en la transición entre ambas partes.

Fibra Monomodo (Single-Mode)

Esta fibra óptica tiene un núcleo muy delgado y permite la transmisión de un solo modo de luz. Es ideal para largas distancias y alta capacidad de datos, como en redes de larga distancia y telecomunicaciones de alta velocidad.

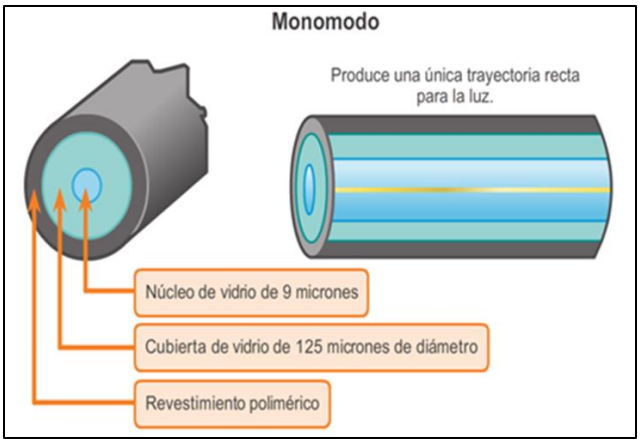

Figura 26. Características fibra óptica monomodo

Fibra Multimodo (Multi-Mode)

Esta fibra tiene un núcleo más grande que permite la transmisión de varios modos de luz al mismo tiempo. Es adecuada para distancias más cortas y aplicaciones como redes locales (LAN) y centros de datos.

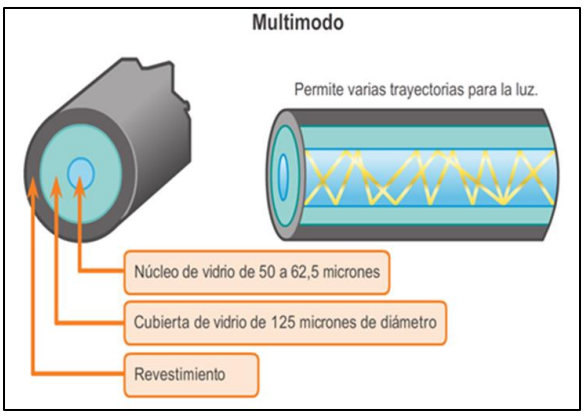

Figura 27. Características fibra óptica multimodo

A continuación, se presenta una Tabla 3 de comparación entre fibra óptica monomodo y multimodo:

Característica	**Monomodo**	**Multimodo**
Núcleo	Vidrio de 9 micrones	Vidrio de 50 a 62.5 micrones
Dispersión	Menor	Permite mayor y , por lo tanto pérdida de señal
Distancias	Adecuado para aplicaciones de larga distancia	Sólo se utilizan en LANs, nunca en largas distancias
Fuente de luz	Utiliza láser	Utiliza LED

Tabla 3. Comparativa entre fibra monomodo y multimodo

Tipos de tendidos

Tendidos aéreos

La implementación aérea de fibra óptica es una práctica extendida en Argentina, especialmente en zonas rurales y suburbanas, donde las distancias a cubrir son considerables y la opción subterránea se torna más costosa o compleja. En esta modalidad, se ubican cables de fibra óptica en postes, torres o estructuras elevadas para garantizar la conectividad en áreas geográficas extensas.

Un aspecto destacable es que, en numerosos casos, las empresas de telecomunicaciones hacen uso de la infraestructura preexistente, como postes de electricidad o líneas telefónicas, para llevar a cabo la instalación de cables de fibra óptica. Esto contribuye a la reducción de costos y a una mayor rapidez en la implementación.

La elección del tendido aéreo de fibra óptica en zonas rurales reviste una importancia significativa, ya que resulta fundamental para ofrecer acceso a Internet de alta velocidad a comunidades que, de otro modo, podrían enfrentar deficiencias en su conectividad o incluso carecer de acceso a la red. Además de propiciar la conectividad a Internet, esta modalidad se emplea para establecer vínculos con estaciones base de telefonía móvil y estaciones de radio, facilitando así servicios de telefonía e Internet móvil.

Es necesario mencionar que el despliegue de cables de fibra óptica aéreos está sujeto a regulaciones y requerimientos gubernamentales, lo que garantiza la seguridad y una coordinación efectiva con otros servicios públicos que hacen uso de los mismos postes y torres. Esta inversión en infraestructura contribuye al fortalecimiento de la red de telecomunicaciones en Argentina, beneficiando a la economía y mejorando la conectividad en general.

Figura 28. Tendido aéreo de fibra óptica

Figura 29. Tendido aéreo de fibra óptica

Postes

Los postes utilizados en un tendido de fibra óptica deben estar construidos con materiales duraderos y resistentes a la intemperie, como madera tratada, concreto o acero. El diseño debe ser capaz de soportar el peso de los cables y otros elementos de la red, además de resistir condiciones climáticas adversas.

Tendidos soterrados

El tendido soterrado de fibra óptica implica la colocación de cables de fibra óptica debajo de la superficie del suelo, típicamente dentro de conductos subterráneos o zanjas excavadas. Este enfoque de implementación es ampliamente empleado en proyectos de

infraestructura de telecomunicaciones y redes de datos con el propósito de establecer conexiones entre edificaciones, comunidades, ciudades y regiones.

En la mayoría de los casos, los cables de fibra óptica se acomodan meticulosamente dentro de conductos subterráneos que han sido específicamente diseñados para albergarlos. Estos conductos operan como tuberías protectoras, desempeñando un papel crucial en la preservación de la integridad de los cables y resguardandolos de posibles daños ocasionados por condiciones climáticas adversas, actos de vandalismo y otros riesgos ambientales. Este nivel adicional de salvaguarda se traduce en una prolongada vida útil de la infraestructura.

Un beneficio significativo del tendido soterrado radica en su capacidad para preservar la estética de entornos urbanos, ya que elimina la necesidad de estructuras aéreas como postes o cables suspendidos en el aire. Además, este método posibilita la instalación de cables de fibra óptica de mayor capacidad, lo que facilita la transmisión de volúmenes sustanciales de datos a velocidades extremadamente elevadas.

Cabe destacar que el proceso de despliegue de cables de fibra óptica soterrados está sujeto a regulaciones y permisos gubernamentales. Estas medidas son fundamentales para garantizar tanto la seguridad de la infraestructura como una efectiva coordinación con otros servicios subterráneos, tales como tuberías de agua y gas, lo que contribuye a la integridad de la infraestructura subterránea en su conjunto.

Figura 30. Tendido soterrado de fibra óptica

Metodología empleada

El método de despliegue seleccionado será aéreo, y la fibra óptica utilizada será monomodo con un total de 8 hilos.

Proveedor ARSAT

La ubicación del data center de ARSAT se encuentra en la zona del Cerro 20 de Febrero, y para lograr la conectividad con el data center en La Lagunilla, se ha planificado la implementación de una infraestructura de fibra óptica que se extiende a lo largo de la parte posterior del cerro.

La distancia entre ambos data centers es de 15 kilómetros.

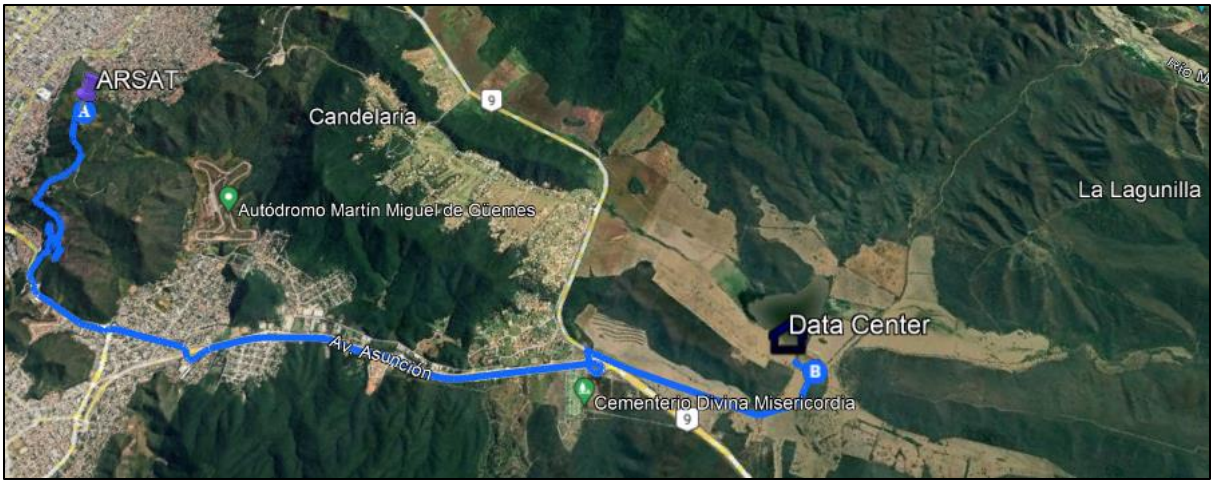

Figura 31. Tendido de fibra óptica desde el dc de ARSAT hasta el dc de La Lagunilla

El despliegue de fibra óptica se inicia en el data center de ARSAT, situado en el Cerro 20 de Febrero. A partir de allí, el trayecto se desarrolla en dirección al Cerro San Bernardo, posteriormente, sigue hacia la Avenida Asunción, abarcando una distancia aproximada de 7.5 kilómetros. Luego, se requiere efectuar un giro a la derecha, cruzando hacia una calle de tierra, con una longitud aproximada de 3.5 kilómetros. Finalmente, se completa el recorrido doblando a la izquierda, donde estará el data center La Lagunilla.

A continuación, se presentará el recorrido planificado desde diversas perspectivas.

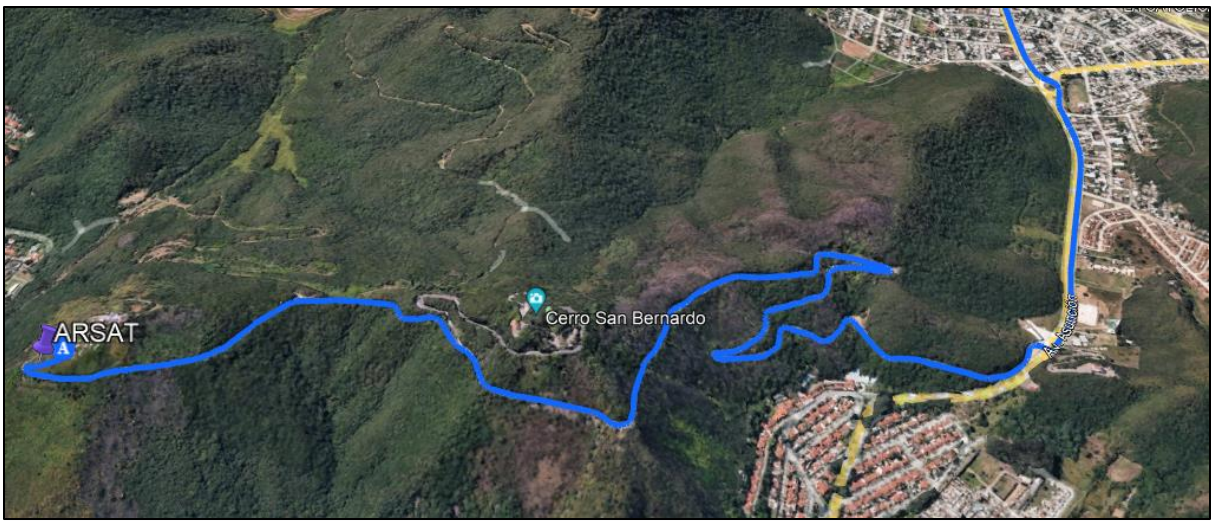

Figura 32. Tendido de fibra óptica desde el dc de ARSAT

Figura 33. Recorrido de fibra óptica

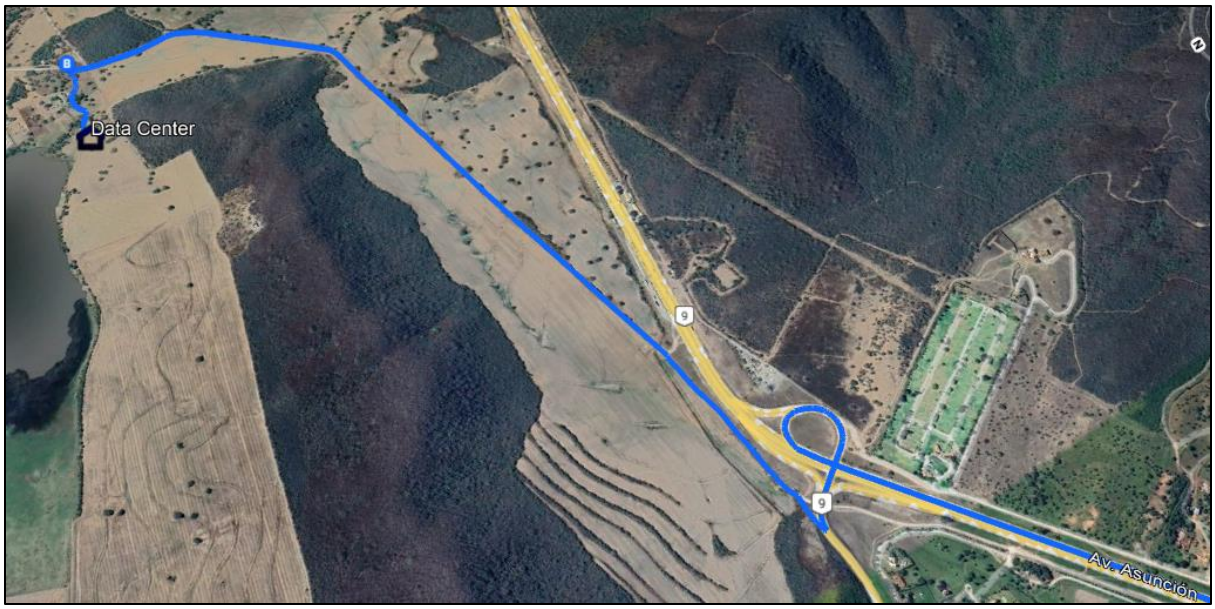

Figura 34. Recorrido de fibra óptica hasta data center en La Lagunilla

Proveedores TELECOM y CLARO

Por otro lado, tanto Telecom (TECO) como Claro tienen su despliegue a lo largo de la RN 9, cada una conectando con su propio centro de distribución (shelter). Ambas redes convergen en la Universidad Católica de Salta.

Figura 35. Tendido de fibra óptica desde el dc de TECO y Claro hasta el dc de La Lagunilla

Figura 36. Tendido de fibra óptica desde el dc de TECO y Claro hasta el dc de La Lagunilla

La distancia entre ambos data centers es de 16 kilómetros.

Equipamiento necesario

Para habilitar la conectividad de fibra óptica en el data center, será necesario disponer de una infraestructura que conste de un ODF, un switch con puertos SFP y los módulos SFP correspondientes.

¿Qué es un ODF?

ODF son las siglas de "Optical Distribution Frame" en inglés, que se traduce al español como "Bastidor de Distribución Óptica" o "Panel de Distribución Óptica".

Es un componente esencial en las redes de fibra óptica que se utiliza para organizar, distribuir y gestionar las conexiones de fibras ópticas dentro de un centro de datos, una red de telecomunicaciones o cualquier otro entorno donde se requiera conectividad de fibra óptica.

Figura 37. ODF marca GLC

¿Qué es un switch?

Un switch es un dispositivo de hardware que opera en la capa de enlace de datos del modelo OSI (Open Systems Interconnection). Su función principal es conectar y gestionar el tráfico de datos entre dispositivos en una red local (LAN), como computadoras, impresoras, servidores y otros dispositivos de red. En la Figura 38 se muestra un switch de la marca Mikrotik modelo CRS317-1G-16S+ que cuenta con 16 puertos SFP+.

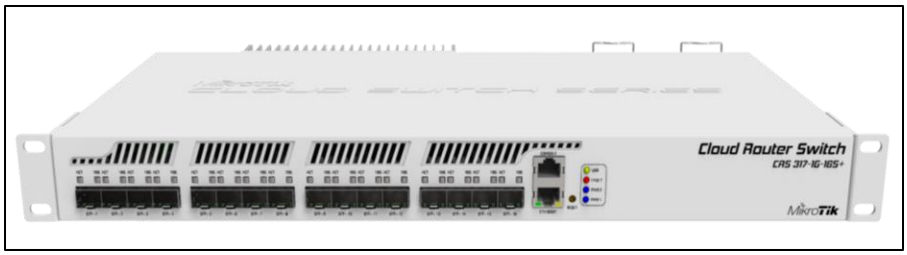

Figura 38. Switch marca Mikrotik

¿Qué es un SFP?

Un conector de factor de forma pequeño, conocido como SFP por sus siglas en inglés "Small Form-Factor Pluggable," es un componente de tamaño compacto ampliamente empleado en aplicaciones de comunicaciones de datos y telecomunicaciones.

Los SFPs ópticos, en particular, se destacan por su capacidad de emplear tecnología de fibra óptica para la transmisión de datos a través de cables de fibra, y su versatilidad para abordar una variedad de tipos de fibras (monomodo o multimodo) y distancias, adaptándose a las especificaciones particulares de cada modelo.

En un nivel superior de rendimiento, los SFP+ representan una evolución optimizada de los SFP estándar, destacándose por su capacidad para alcanzar velocidades de transmisión de datos sustancialmente superiores, como 10 Gbps (Gigabits por segundo) y más.

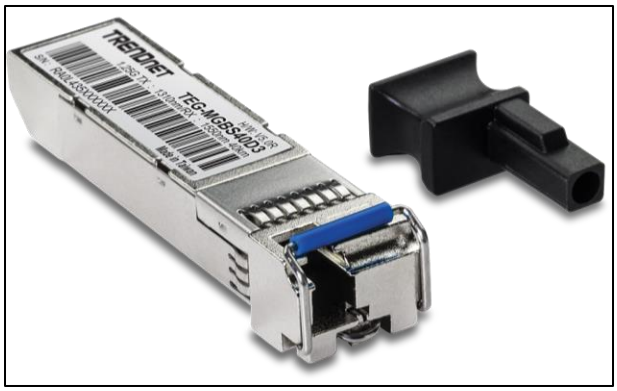

Figura 39. Módulo SFP marca Trendnet

CAPÍTULO VI: PLAN DE SEGURIDAD INFORMÁTICA

Tanto el diseño arquitectónico, civil y técnico del data center como la planificación de su seguridad son de suma importancia. La consideración de aspectos de seguridad desde las etapas iniciales del diseño y la construcción física del sitio conlleva ventajas significativas tanto en términos económicos como de productividad para la implementación de medidas de seguridad física. Del mismo modo, la integración de consideraciones de seguridad de la información desde la fase de diseño de la red que se implementará en el data center también ofrece múltiples ventajas para la posterior aplicación de medidas de seguridad lógica.

En este trabajo, se aborda la integración de medidas de seguridad tanto físicas como lógicas con el objetivo primordial de establecer un plan de seguridad que permita una respuesta rápida y eficiente ante incidentes. Esta sección comenzará con una breve introducción a los conceptos fundamentales de seguridad de la información, seguida de una exposición y explicación detallada de la metodología empleada.

¿Qué es la seguridad informática?

Seguridad informática y ciberseguridad se consideran sinónimos, se entiende por seguridad de la información a la protección de la confidencialidad, integridad y disponibilidad de la información en todas sus formas. Es un proceso continuo de selección, aplicación y mantenimiento de medidas de seguridad informática (administrativas, físicas y técnicas) [12].

¿Qué es una amenaza?

Se define como "una persona o grupo de personas con motivación, intención y capacidad para cometer un acto doloso". También se puede hacer referencia a una amenaza como adversario [12].

¿Qué es una ciberamenaza?

Las ciberamenazas en relación con la seguridad informática son aquellas que eligen como blanco sistemas informáticos que son capaces de almacenar, procesar o transmitir información, con el fin de comprometerlos y/o sabotearlos [13].

Acto doloso o ciberataque:

Cuando una ciberamenaza está implicada en un acto doloso, estamos ante un ciberataque. Los ciberataques eligen como blanco información electrónica o sistemas informáticos con la intención de robar, modificar o destruir un blanco determinado mediante accesos o acciones no autorizadas.

¿Cómo ocurren los ciberataques?

Los ciberataques buscan explotar las vulnerabilidades de un sistema informático para comprometerse. Las **vulnerabilidades** de un sistema informático son los puntos débiles de un activo o sistema de control que una amenaza puede explotar.

Vulnerabilidades del sistema

Ningún sistema está exento por completo de vulnerabilidades, estas pueden presentarse de diversas formas:

1. Tecnología (hardware o software)
2. Protección física (control de acceso físico)
3. Procesos administrativos

Incluso los empleados inocentes pueden constituir una vulnerabilidad. Es frecuente que los atacantes intenten explotar a personas como punto de partida para comprometer un sistema informático.

A partir de los conceptos y definiciones previamente expuestos, a continuación, se detalla la implementación de medidas de seguridad, incluyendo la metodología empleada y un enfoque innovador que resulta fundamental en el contexto de este trabajo.

Medidas de seguridad informática

Un plan de seguridad debe contemplar todos los aspectos que puedan constituir un vector de ataque, es por ello que en este trabajo se propone hacer hincapié en medidas de seguridad en múltiples entornos como los que se listan y describen a continuación.

Medidas de control administrativo:

Estas medidas refieren al conjunto de políticas y procedimientos creados para proteger los sistemas informáticos mediante procesos de actuación del personal interno y externo. En ellas se definen las acciones permitidas, las obligaciones a cumplir y las acciones prohibidas tanto para el personal interno como para el externo.

Medidas de control físico:

Estas son las barreras o impedimentos físicos empleados que protegen tanto a los sistemas informáticos, instalaciones, infraestructura y personas contra daños físicos y accesos no autorizados. Son medidas típicas de control físico como por ejemplo cercados periféricos, puertas de acceso, cerraduras, personal de seguridad, dispositivos detectores, cámaras de seguridad, entre otros.

Medidas de control técnico:

Estas consisten en las medidas de hardware y/o software que permiten prevenir y detectar una intrusión o ataque como también así las medidas que permiten recuperar dichos sistemas que sean afectados y mitigar consecuencias.

Metodología empleada

El método empleado resulta de la combinación de dos enfoques utilizados actualmente para la protección de infraestructuras críticas por parte de gobiernos y agencias internacionales. En capítulos anteriores se mencionaron los potenciales clientes y vinculado a ello podemos inferir el tipo de información que el centro de datos almacenará, procesará o transmitirá. Esto llevó a desarrollar un plan de seguridad que esté a la altura y cumpla con un alto nivel de requerimientos.

Las medidas de seguridad se implementarán en los entornos mencionados anteriormente (administrativo, físico y técnico) bajo un enfoque graduado, es decir, se realizará un inventario de activos en cada entorno y se los clasifica según su importancia. La siguiente figura muestra de manera ilustrativa una clasificación bajo un enfoque graduado.

Figura 40. Clasificación bajo enfoque graduado.

Esto luego permitirá aplicar medidas de seguridad a cada activo en un nivel o grado acorde a su clasificación, en otras palabras, los activos clasificados con mayor orden de prioridad serán aquellos que en caso de ser atacados las consecuencias que deriven de dicho ataque presenten mayores daños o pérdidas, y por tal motivo estos activos tendrán mayores controles y medidas de seguridad aplicadas que un activo de menor prioridad. Este método facilita en gran medida la tarea del personal de seguridad informática en el momento de realizar

la clasificación de activos, lo que consecuentemente permite optimizar recursos humanos, técnicos y económicos.

A su vez este enfoque se combinará con una metodología de defensa en profundidad, esta consiste en la implementación de capas sucesivas donde cada capa puede estar conformada por medidas de seguridad de naturaleza administrativa, técnica o física, estas capas de medidas de seguridad se aplican para proteger posibles blancos de ataques o los activos de mayor relevancia. La siguiente figura muestra un diagrama esquemático de una forma de defensa en profundidad:

Figura 41. Defensa en profundidad.

La seguridad informática es un proceso continuo que requiere de múltiples capas de protección y una estrategia de defensa en profundidad como medio de prevención y mitigación. Las medidas de seguridad informática deben implementarse por capas, estas medidas son una combinación de medidas de control técnicas como lo son el diseño de la arquitectura informática, medidas administrativas y medidas de control de acceso físico. Por ello nuevamente es importante destacar que en este trabajo se contempló la seguridad física desde el diseño y planificación del centro de datos ubicado en Lagunilla.

Respuesta a incidentes

La respuesta a incidentes de seguridad física o lógica que pongan en riesgo la integridad, confidencialidad y disponibilidad de la información que el centro de datos esté almacenando, procesando o transmitiendo en un determinado momento serán mitigados y atendidos de acuerdo a un plan de respuestas a incidentes que será documentado como procedimiento interno para el personal que cumpla funciones en el sitio. Dicha respuesta consistirá en resolver el incidente en cuestión reaccionando de manera apropiada y conteniendo eficazmente el problema.

La respuesta a incidentes deberá cumplir los siguientes objetivos:

1. Atender a la seguridad de las personas.
2. Impedir el acceso no autorizado de intrusos a nivel físico y/o lógico.
3. Minimizar la degradación del servicio del centro de datos.

4. Determinar el origen y causa del ataque.
5. Protegerse contra posibles ataques futuros.

Fases del plan de respuesta a incidentes

La responsabilidad de las acciones que conforman un plan de respuesta a incidentes corresponden al equipo de respuestas a incidentes de seguridad informática (CSIRT):

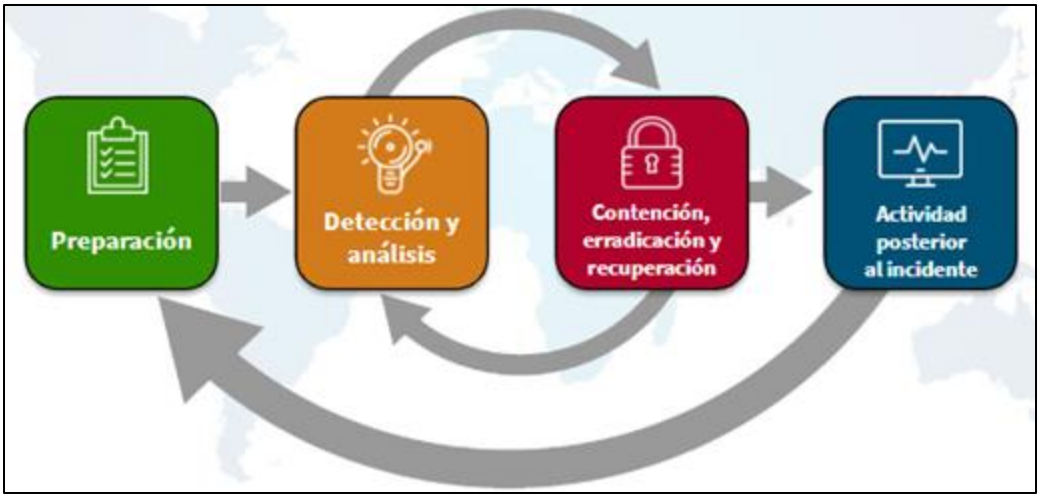

Figura 42. Diagrama de fases de un plan de respuesta a incidentes.

Fases del plan de respuesta a incidentes

Preparación:

La preparación de un plan de respuesta a incidentes consiste en la realización de las siguientes actividades:

1. Establecimiento de una política que defina roles y responsabilidades de todas las partes implicadas en el proceso de respuesta a incidentes.
2. Redacción e implementación de los procedimientos de ejecución de las acciones establecidas en dicha política.
3. Identificación de los activos.
4. Realización de actividades y simulacros de seguridad con el CSIRT.

Detección y análisis:

Las actividades de detección consisten en garantizar la presencia de una infraestructura adecuada de supervisión de los datos que permita detectar, recopilar y proteger la información relativa a un incidente o posible incidente.

Contención, erradicación y recuperación:

El proceso de respuesta a incidentes de seguridad informática es cíclico y continuo. Las actividades de mitigación deben ser continuadas y adaptarse a medida que se vaya recopilando y analizando nuevas informaciones durante la fase de detección y análisis. Los objetivos de esta fase son:

1. Contención del incidente de seguridad informática
2. Erradicación de todo malware presente en los sistemas afectados.
3. Restablecimiento del funcionamiento del sistema

Actividad posterior al incidente:

La última fase de la respuesta es la ejecución de las actividades posterior a un incidente. El objetivo es implementar medidas que en un futuro impida que se repita tal incidente de seguridad informática, permita su detección temprana o minimicen su impacto.

CAPÍTULO VII: PUESTA EN MARCHA

El mantenimiento y funcionamiento de un centro de datos Tier 3 con las dimensiones planteadas requiere una variedad de roles y personal especializado. A continuación, se detalla el personal humano que se llegara a necesitar para operar y mantener un centro de datos de esta magnitud:

1. Gerente de Centro de Datos (Data Center Manager): Es responsable de la gestión general del centro de datos, incluyendo la planificación estratégica, el presupuesto, la supervisión del personal y la coordinación de actividades.

2. Administradores de Red: Se encargan de la configuración, supervisión y mantenimiento de la infraestructura de red del centro de datos.

3. Ingenieros de Sistemas: Responsables de mantener y actualizar los servidores, sistemas de almacenamiento y virtualización, asegurando que estén funcionando de manera óptima.

4. Técnicos de Soporte: Proporcionan asistencia técnica a los clientes que utilizan el centro de datos y resuelven problemas operativos.

5. Equipo de Seguridad: Incluye guardias de seguridad para la seguridad física del centro de datos y profesionales de seguridad de la información para garantizar la seguridad de los datos y sistemas.

6. Personal de Mantenimiento de Instalaciones: Se encargan de mantener y reparar los sistemas eléctricos, sistemas de climatización, fontanería y otras instalaciones del centro de datos.

7. Técnicos de Energía y UPS: Aseguran un suministro eléctrico ininterrumpido mediante la gestión de sistemas de alimentación ininterrumpida (UPS) y generadores de respaldo.

8. Personal de Control de Acceso: Gestiona el acceso al centro de datos, incluyendo la recepción y registro de visitantes.

9. Personal de Sala de Monitoreo: Monitorea de forma constante el rendimiento y la disponibilidad de los sistemas y servicios del centro de datos, y responde a problemas y alertas.

10. Equipo de Servicio al Cliente: Brinda asistencia a los clientes que utilizan el centro de datos y se encarga de la facturación y la coordinación de servicios.

11. Personal de Limpieza y Mantenimiento General: Asegura la limpieza y el mantenimiento general de las instalaciones, incluyendo la sala de equipos, las áreas comunes y las oficinas.

12. Personal de Recepción y Administrativo: Gestionan las tareas administrativas, la recepción de visitantes y la coordinación de reuniones.

13. Personal de Cocina y Comedor: se necesitará personal para la preparación de alimentos y el servicio de comidas.

14. Personal de Almacén y Logística: Se encarga de gestionar el inventario de equipos y suministros, así como de coordinar la logística de entrada y salida de equipos.

Es importante recordar que la cantidad de personal y los roles específicos pueden variar. A continuación, en la Tabla 4, se presenta una estimación que ilustra la posible necesidad de personal en este contexto por turno de trabajo.

Rol	Cantidad de Personal	Horas Anuales (por persona)
Gerente	1	8.760
Administradores de red	4	35.040
Ingenieros de sistemas	2	17.520
Técnicos de soporte	3	26.280
Equipo de seguridad	4	35.040
Personal de mantenimiento	1	8.760
Técnicos de energía y UPS	2	17.520
Personal de control de acceso	2	17.520
Personal de sala de monitoreo	3	26.280
Equipo de servicio al cliente	1	8.760
Personal de limpieza y mantenimiento general	2	17.520
Personal de recepción y administrativo	2	17.520
Personal de cocina y comedor	1	8.760
Personal de almacén y logística	2	17.520

Tabla 4. Cantidad de personal necesario por turno

CONCLUSIÓN

Este proyecto de diseñar un centro de datos Tier 3 en la zona de entrada de la ciudad de Salta, específicamente en La Lagunilla, representa un paso significativo hacia el fortalecimiento de la infraestructura tecnológica y económica de la región. La elección de esta ubicación se fundamenta en una serie de características clave, tales como la disponibilidad de suministro de agua de respaldo, un acceso confiable a la energía eléctrica, un alto nivel de seguridad física, y la presencia de una infraestructura de comunicaciones avanzadas, que la hacen excepcionalmente adecuada para albergar un centro de datos altamente disponible.

Durante la fase de desarrollo del proyecto, se consideraron todos los aspectos necesarios para cumplir con los requisitos estipulados por la normativa TIA-942 en vigor.

Además, se identificaron los tres proveedores responsables de suministrar conectividad al centro de datos y se planificaron las rutas de fibra óptica requeridas para garantizar dicha conectividad. Asimismo, se diseñó un plan de seguridad informática que detalla los procedimientos a seguir en caso de incidentes.

Por último, se estableció el equipo de profesionales y técnicos necesario para operar y mantener el centro de datos una vez que esté en funcionamiento.

La implementación de un centro de datos Tier 3 implica una serie de ventajas y beneficios altamente significativos para las organizaciones que buscan asegurar una disponibilidad óptima, un rendimiento excepcional y una confiabilidad inquebrantable en todas sus operaciones tecnológicas. Este tipo de centro de datos garantiza una disponibilidad del 99.982% anual, esto equivale a 8.758,43 horas sobre un total anual de 8760 horas.

REFERENCIAS

[1] ¿Qué es un data center?. https://www.ibm.com/es-es/topics/data-centers#:~:text=Un%20centro%20de%20datos%20es,con%20dichas%20aplicaciones%20y%20servicios. Accedido el 11/09/2023.

[2] Telecommunications Industry Association (TIA®). Telecommunications Infrastructure Standard for Data Centers, TIA-942. July 2017, Version B.

[3] "Tipos de centros de datos". IBM.

[4] Sistema de clasificación de niveles. https://uptimeinstitute.com/tiers. Accedido el 13/08/2023

[5]"Diseño de Infraestructura de un Data Center TIER IV de acuerdo a las especificaciones técnicas de la norma TIA-942". José Javier Escobar Rodriguez. Pontificia Universidad Católica del Ecuador. 2015.

[6] "Centro de operaciones de red". IBM.

[7] " Criterios de diseño de sistemas contra incendio en Data center ". Mag. Ing. Mario M. Figueroa de la Cruz.

[8] "La puesta a tierra de instalaciones eléctricas". Rogelio García Márquez.

[9]"Impacto de pasillos calientes y fríos en la eficiencia y temperatura del centro de datos".White Paper 135. John Niemann. Kevin Brown. Victor Avelar. Schneider Electric.

[10] "Introducción al cableado estructurado". Furukawa Electric.

[11]"Diseño de red de fibra óptica en la Quebrada del Toro para abastecimiento de internet a las distintas comunidades e instalación de postes WIFI con servicio abierto de internet a la vera de la RN 51". Matias Sant. 2021.

[12] Computer security at nuclear facilities : reference manual : technical guidance. Vienna : International Atomic Energy Agency, IAEA, 2011. ISBN 978–92–0–120110–2.

[13] Seguridad Informática en las Instalaciones Nucleares OIEA. Viena. 2013 STI/PUB/1527. ISBN 978-92-0-337310-4. ISSN 1816-9317.