UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"MODELO DE CENTRO DE DATOS DE RESPALDO CON REPLICACIÓN EN TIEMPO REAL EN LA MEJORA DEL RENDIMIENTO DE LA GESTIÓN DE LA INFORMACIÓN EN LA EMPRESA ELECTRO PUNO S.A.A."

PRESENTADO POR:

JESUS EMANUEL FARAH MIRAVAL

PARA OPTAR EL TÍTULO PROFESIONAL DE: INGENIERO DE SISTEMAS

PUNO – PERÚ

2017

UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"MODELO DE CENTRO DE DATOS DE RESPALDO CON REPLICACIÓN EN TIEMPO REAL EN LA MEJORA DEL RENDIMIENTO DE LA GESTIÓN DE LA INFORMACIÓN EN LA EMPRESA ELECTRO PUNO S.A.A.".

TESIS PRESENTADA POR:

JESUS EMANUEL FARAH MIRAVAL

PARA OPTAR EL TITULO PROFESIONAL DE: INGENIERO DE SISTEMAS

APROBADA POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE : M.SC. WILLIAM E. ARCAYA COAQUIRA

PRIMER MIEMBRO : M.SC. MILDER ZANABRIA ORTEGA

SEGUNDO MIEMBRO : ING. FIDEL HUANCO RAMOS

DIRECTOR DE TESIS : ING. ALDO H. ZANABRIA GÁLVEZ

Área: Informática
Tema: Comunicación de datos

Puno – Perú

2017

AGRADECIMIENTOS

Agradezco a Dios por todas las oportunidades y desafíos que me pone día a día.

Agradezco a mi familia por el todo el apoyo y guiarme para terminar mi trabajo de investigación.

A mi director de tesis el Ingeniero Aldo H. Zanabria Gálvez por su apoyo para poder terminar un excelente trabajo de investigación, a mis jurados de tesis el M.sc. Ing. William E. Arcaya Coaquira, M.sc. Ing. Milder Zanabria Ortega y al Ing. Fidel Huanco Ramos por su orientación para poder presentar un excelente trabajo de investigación.

Al personal de Electro Puno, en especial a la oficina TIC por brindarme la información que necesite para terminar mi trabajo de investigación.

A Tatiana Reyes Ponce por ser esa persona y soporte en mi vida, que siempre está a mi lado alentándome a ser mejor persona y su apoyo para terminar mi trabajo de investigación.

DEDICATORIA

Dedico el presente trabajo a mis amados padres Alberto y Juana que siempre estuvieron guiándome por el buen camino, a mis hermanos Alberto y Jorge por siempre recordarme quien soy y su apoyo constante y a Tatiana por nunca dejarme caer y estar conmigo en todo momento.

INDICE

INDICE DE FIGURAS

INDICE DE CUADROS

INDICE DE ANEXOS

RESUMEN

El presente trabajo de investigación titulado "**MODELO DE CENTRO DE DATOS DE RESPALDO CON REPLICACIÓN EN TIEMPO REAL EN LA MEJORA DEL RENDIMIENTO DE LA GESTION DE LA INFORMACION EN LA EMPRESA ELECTRO PUNO S.A.A.**" tiene como objetivo principal diseñar un modelo de CPD de Respaldo para mejorar la gestión de la información en la empresa Electro Puno S.A.A. La división de TIC de la empresa Electro Puno S.A.A. tiene como principal tarea, brindar una excelente calidad en los servicios a los trabajadores de la empresa y usuarios de toda la región Puno. Para la solución del problema se diseñó un CPD de respaldo para evaluar y comparar las mejoras en el rendimiento de la gestión de la información de la empresa. Se utilizó la norma ANSI/TIA 942 para validar y certificar la calidad que el CPD debe brindar de acuerdo a las necesidades de la empresa y ser clasificado en un TIER 1 que brindara un 99.671% de disponibilidad y un tiempo de 29.8 horas de inactividad anual programadas o no programadas y también utilizando equipos de red y servidores que realicen el trabajo de copias en tiempo real para que cuando el CPD principal falle o deje de funcionar por algún motivo este entre en reemplazo hasta que el CPD principal entre en funcionamiento nuevamente.

Concluyéndose que el diseño de un CPD de respaldo con replicación en tiempo real mejora favorablemente el rendimiento de la Gestión de la Información en la empresa Electro Puno S.A.A.

Palabras clave: Modelo, CPD de Respaldo, Gestión de la Información, norma TIA 942, TIER.

ABSTRACT

The present research titled "MODEL OF DATA CENTER OF BACKUP DATA WITH REPLICATION IN REAL TIME IN THE IMPROVEMENT OF THE PERFORMANCE OF INFORMATION MANAGEMENT IN THE ELECTRO PUNO S.A.A. COMPANY" has as main objective to design a model of Data Backup Center to improve the management of information in the company Electro Puno S.A.A. The ICT division of Electro Puno S.A.A. Has as main task, to provide an excellent quality in the services to the workers of the company and users of all the Puno region. For the solution of the problem a backup CPD was designed to evaluate and compare the improvements in the performance of the information management of the company. ANSI / TIA 942 was used to validate and certify the quality that the CPD must provide according to the needs of the company and be classified in a TIER 1 that would provide 99.671% of availability and a time of 29.8 hours of annual inactivity Programmed or unscheduled and also using network equipment and servers that perform the copy work in real time so that when the main CPD fails or stops working for some reason it will replace until the main CPD goes back to work.

Concluding that the design of a real-time replication backup CPD improves the performance of the Information Management in the company Electro Puno S.A.A.

Keywords: Model, Data Backup Center, Information Management, TIA 942 standard.

INTRODUCCIÓN

La utilización de Tecnologías de la Información y Comunicaciones o también conocida como las TIC, por parte de la administración pública está aumentando notablemente, ya que es innegable el impulso que da al incremento de la eficiencia y eficacia en la prestación de los servicios públicos en las decisiones de gobierno, fortalece el proceso descentralizado e instaura una administración moderna orientada a la prestación de servicios en línea, para que esto se logre, las TIC deben estar correctamente implementadas y configuradas, de otra manera generarían incidentes como perdida de información y deterioro de los equipos.

La empresa de distribución de energía eléctrica Electro Puno S.A.A. es una institución que atiende a los usuarios y todos los días genera, intercambia y almacena información en sus servidores, su trabajo se basa en la información que posee y puede tener acceso en cualquier momento del día. Esta tesis se encuentra constituida por los siguientes capítulos:

CAPITULO I: Contiene la descripción, justificación del problema y los objetivos de la investigación.

CAPITULO II: Presenta los antecedentes de la investigación, sustento teórico, glosario de términos, hipótesis de la investigación y el cuadro de operacionalización de variables.

CAPITULO III: Detalla el tipo, diseño, población y muestra de la investigación, también la ubicación y descripción de la población, técnicas e instrumentos para recolectar información, y para el procesamiento y análisis de datos, asimismo el plan y tratamiento de datos.

CAPITULO IV: Desarrollo del análisis e interpretación de resultados de la investigación.

CAPITULO V: Finalmente se presentan las conclusiones y sugerencias arribadas de la investigación, además de los anexos.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACION

1.1. Descripción del problema

La evolución tecnológica que ha ocurrido en estos últimos años ha dado cabida al desarrollo de nuevas tecnologías y al mejoramiento de tecnologías ya existentes, observándose un aumento gradual de velocidades de acceso y transporte, esto da lugar a una etapa de actualización de las distintas tecnologías en el mercado actual, haciendo que éste tenga una tendencia a utilizar aquella tecnología que por sus beneficios y aplicaciones supere a otras, satisfaciendo así las necesidades de cada empresa.

En un estudio realizado por Emerson Network Power en el año 2011 basándose en las respuestas proporcionadas por 41 empresas de distintos sectores (financiero, telecomunicaciones, sanidad, gobierno, etc.) se estima que el coste medio por minuto de la caída de un Centro de Procesamiento de Datos (CPD) es $5.600, basados en la pérdida o corrupción de datos, pérdida de productividad, daños en el equipamiento, repercusiones legales, repercusiones en la reputación de la compañía, etc.

La empresa Electro Puno S.A.A. genera grandes cantidades de información que necesita ser almacenada y mantenida en instalaciones seguras, es por eso que el CPD se convierte en un centro de

operaciones crítico de cualquier empresa y que las tecnologías IT son la mejor métrica para evaluar un CPD.

El presento proyecto de investigación está basado en la solución a este tipo de problemas la cual es el modelo de implementación de un Centro de Procesamiento de Datos (en adelante CPD) de Respaldo con replicación en tiempo real, lo que significa que cuando el CPD principal deja de funcionar por algún motivo el CPD de respaldo o secundario toma su lugar y empieza a funcionar sin que los trabajadores noten el cambio de servicios hasta que se solucione el problema y el CPD principal vuela a funcionar nuevamente. Al ser la información uno de los activos más importantes de una empresa, la disponibilidad de la misma se convierte en un factor clave para la adecuada gestión de la información, garantizando la disponibilidad de la información, manteniendo la confidencialidad e integridad.

1.2. Justificación del problema

El presente trabajo de investigación se realizó debido a los diferentes tipos de incidentes que se presentaron en los últimos años en el CPD de la empresa Electro Puno S.A.A. los cuales son resueltos por los trabajadores de la oficina de TIC y si el problema es complejo se requiere el soporte de una persona o empresa externa para poder resolver los incidentes que se presentan dentro de la empresa Electro Puno S.A.A. y el CPD pueda brindar una mejor calidad en los servicios que brinda la división de Tecnologías de la Información y Comunicaciones.

Al plantear un CPD de respaldo que realice copias en tiempo real y pueda brindar una continuidad en los servicios sin que los trabajadores de la empresa y los usuarios se vean perjudicados.

1.3. Objetivos de la investigación

1.3.1. Objetivo General

Diseñar un modelo de CPD de Respaldo con replicación en tiempo real para mejorar el rendimiento de la gestión de la información en la empresa Electro Puno S.A.A.

1.3.2. Objetivos Específicos

- Analizar la situación actual de la gestión de la información en la empresa Electro Puno S.A.A.
- Diseñar un CPD de respaldo utilizando la norma ANSI TIA 942.
- Evaluar los niveles de disponibilidad de la información alcanzados con el modelo de CPD de respaldo con replicación en tiempo real propuesto.

CAPÍTULO II

MARCO TEORICO

2.1. Antecedentes de investigación

Se consideró como antecedentes a los siguientes trabajos de investigación:

Modelo de CPD para mejorar la Gestión de la Información en las PYMES de la ciudad de Puno. (Cabrera & Guerra, 2013)

En la tesis, los investigadores llegan a las siguientes conclusiones:

- Realizando el diagnóstico de la situación actual de la gestión de la información en las PYMEs de la ciudad de Puno, se encontró que los niveles de disponibilidad promedio de la información en las empresas actualmente es de 87% valor que se encuentra debajo de los parámetros mínimos recomendados para asegurar que la información esté disponible cuando se necesite.
- Dado que los niveles de criticidad del uso dela información de las PYMEs de la ciudad de Puno no son altos, se determinó que un modelo de micro CPD es el que más se adapta para satisfacer sus necesidades.
- Al simular el funcionamiento del modelo de CPD propuesto, los niveles obtenidos de disponibilidad de la información en la PYMEs de la ciudad de Puno ascendieron hasta 99.7%, valor que se encuentra dentro de los rangos sugeridos. El tiempo promedio de disponibilidad de la información alcanzó un promedio de 8640 horas al año, y el tiempo en corte un promedio de 22 horas al año.
- Comparando los niveles actuales de disponibilidad de la información en las PYMEs de la ciudad de Puno, y los niveles alcanzados mediante la

simulación del funcionamiento del modelo de CPD propuesto, se obtuvo un 12.7% de mejoras concluyendo en que la utilización de una modelo de CPD permite mejorar la gestión de la información en las PYMEs de la ciudad de Puno.

Diseño de un CPD basado en estándares, caso práctico: Diseño del CPD del Colegio Latinoamericano. (Maldonado, 2010)

En el trabajo de investigación el tesista llego a las siguientes conclusiones:

- La planificación es la clave para un buen diseño de un CPD.
- Mantener el diseño lo más simple posible, con esto se asegura que sea fácil el mantenimiento, soporte, uso y administración. Cuando surja un problema será más fácil de corregirlo.
- Hay que ser flexibles, los cambios tecnológicos evolucionan rápidamente y las actualizaciones en la plataforma se tendrán que dar. Piense de manera modular, esto ayudará a mantener las cosas simples y flexibles.
- Preocuparse por el peso de los equipos, servidores y unidades de almacenamiento que se vuelven cada día más pesados y densos, hay que asegurarse que las estructuras y el piso estén correctamente diseñados para soportar la carga correspondiente.
- Rotule todo, particularmente el cableado.
- Finalmente espere lo mejor del diseño y planifique para lo peor que pudiera ocurrir, así nunca será sorprendido.

Diseño de un Centro de Proceso de Datos. (Acuña, 2013)

La investigadora del proyecto llego a las siguientes conclusiones:

- Los CPD han evolucionado en las últimas décadas desde un concepto más centralizado, pasando por una fase distribuida hasta la actualidad, en la que están enfocados hacia la consolidación y virtualización de los sistemas. Dichos sistemas necesitan un entorno que asegure la disponibilidad, continuidad y estabilidad del entorno, esto lo proporciona un adecuado sistema de refrigeración, de alimentación, de detección y extinción de incendios, de seguridad y monitorización. Un CPD bien diseñado mejora la eficiencia, reduce los costes y optimiza el entorno de la inversión.
- La seguridad estructural del CPD es el primero de los aspectos importantes a la hora de realizar el diseño. El CPD debe estar construido en un espacio resistente al fuego, a la penetración del agua y al acceso por la fuerza. Estas características deben aplicarse a paredes, suelos técnicos y techos suspendidos, de modo que el CPD se convierta en un recinto estanco, dadas las instalaciones disponibles.
- La elaboración de este proyecto me ha permitido adentrarme en el mundo del diseño de CPD que se desarrolla en el departamento de Redes de la empresa en la que estoy realizando las prácticas. Con él he pretendido una guía con buenas prácticas para el diseño de CPD, y demostrar con un caso práctico, su implantación en el mundo real, basándome en casos reales, que he podido conocer de primera mano durante el desarrollo de mis prácticas en la empresa. A pesar

de que las tecnologías se emplean en el diseño de un CPD están en constante evolución en la búsqueda de una mejor eficiencia y rendimiento, he procurado que queden patentes aquellas que en la actualidad son más empleadas, por su funcionamiento y coste en los CPD. Resulta imposible generalizar en el uso de una u otra tecnología cada cliente es un mundo y existen muchas limitaciones o preferencias particulares que hacen que la solución para cada CPD sea única. Es tarea del jefe de proyecto encontrar la solución que mejor se ajuste a cada cliente para lograr la adjudicación del proyecto y que la realización del mismo culmine con el éxito esperado.

Planificación y diseño de un CPD de respaldo basada en la norma ANSI TIA 942. (Pérez, 2014)

El autor de dicho proyecto de investigación refiere las siguientes recomendaciones al finalizar la tesis:

- Utilización del CPD de respaldo en combinación con el centro principal para monitorizar el parque de aplicaciones, identificando aplicaciones y servidores no identificados o no utilizados (por ejemplo, basado en el tráfico de réplica de datos hacia el centro de respaldo), y proporcionando una estrategia de baja de los servicios (por ejemplo, manteniendo la copia del centro de respaldo durante un tiempo tras la baja en el centro principal).
- Ya que el centro de respaldo posee conexiones con diferentes proveedores que no son utilizadas normalmente, surge la posibilidad

de utilizar los puntos de acceso como puntos de interconexión entre proveedores (puntos neutros), encaminando paquetes entre los diferentes proveedores cuando estos recursos no sean utilizados por el centro de respaldo, lo que puede reducir los costes de conexión.

- Dado el uso de virtualización y granjas de servidores, se puede contemplar la disponibilidad de recursos del centro de respaldo para empresas del grupo o socios comerciales, ofreciendo servicios de colocación, permitiendo a terceros el acceso al centro, u ofreciendo servicios de computación en la nube que, en caso de caída del centro principal, puedan desactivarse o encaminarse a otros centros de la nube sin interrumpir los servicios.

2.2. Sustento teórico.

2.2.1. Centro de Procesamiento de Datos – CPD

Un CPD es un lugar que reúne las condiciones técnicas para albergar y proteger recursos informáticos esenciales de una organización y que se mantienen en un entorno muy controlado, estas instalaciones poseen seguridad tanto física como de red (lógico). Todos los sistemas son alimentados por un suministro de energía ininterrumpido, utilizando fuentes de alimentación de respaldo (es decir tanto baterías, generadores o un grupo electrógeno) en el caso de que falle la fuente de energía principal. El software utilizado es controlado cuidadosamente para asegurar que no se infrinjan las patentes o licencias de software, el desarrollo y despliegue de aplicaciones es controlado y evaluado a través de rigurosas fases de prueba. Las copias de seguridad del

sistema se llevan a cabo de manera continua, almacenando las copias de respaldo in-situ, así como fuera de lugar. (Newton, 2004)

Un CPD permite asegurar la disponibilidad de servicios de TI, por lo tanto, la continuidad de las operaciones empresariales de forma ininterrumpida y de acuerdo a los requerimientos o necesidades del negocio, utilizando la infraestructura y los recursos informáticos necesarios. Los recursos informáticos en el CPD incluyen mainframes, racks, servidores web y de aplicaciones, servidores de archivos, servidores de mensajería, software de aplicación y sistemas operativos configurados en los servidores, los sistemas de almacenamiento, la infraestructura de red y SAN.

Las aplicaciones que se ejecuten en el CPD van desde las que controlan las actividades empresariales internas como la gestión de recursos humanos hasta las aplicaciones externas como el comercio electrónico y las aplicaciones B2B. Además de un numero de servidores configurados para dar apoyo a las operaciones de red y aplicaciones basadas en la red. Las operaciones de red pueden incluir NTP (Network Time Protocol), FTP (File Transfer Protocol), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), SNMP (Simple Network Management Protocol), TFTP (Trusted File Tranfer Protocol), NFS (Network File System) y aplicaciones basadas en redes, como telefonía IP, video streaming, video conferencia, entre otros. (Arregoces & Portolani, 2004)

2.2.2. CPD de Respaldo

Un CPD de respaldo es un CPD específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia, grandes organizaciones, tales como bancos o Administraciones Públicas, no pueden permitirse la pérdida de información ni el cese de operaciones ante un desastre en su centro de proceso de datos. Terremotos, incendios o atentados en estas instalaciones son infrecuentes, pero no improbables. Por este motivo, se suele habilitar un centro de respaldo para absorber las operaciones del CPD principal en caso de emergencia.

A pesar de tanta protección, debemos pensar en la posibilidad de que ocurra una catástrofe en nuestro CPD y quede inservible (inundación, terremoto, sabotaje, incendio, etc.). La continuidad de la empresa no puede depender de un punto único de fallo; si disponemos de presupuesto suficiente, debemos instalar un segundo CPD.

Este segundo CPD, también llamado centro de respaldo (CR), ofrece los mismos servicios del centro principal (CP). Aunque, si la inversión en hardware resulta demasiado elevada, puede limitarse a los servicios principales, o a los mismos servicios, pero con menos prestaciones. Por supuesto, debe estar físicamente alejado del CPD principal; cuantos más kilómetros entre ambos mejor. (Roa, 2013)

2.2.3. Objetivos de un CPD

El tiempo de inactividad de los servicios de TI conduce a la degradación del servicio, o la imposibilidad de desplegar nuevos servicios, lo que conduce a una pérdida de acceso a los recursos críticos y un impacto cuantificable en las actividades comerciales. El impacto podría ser tan simple como un tiempo de respuesta mayor o tan grave como la pérdida de datos. Se implementa o subcontrata un CPD para apoyar las actividades del negocio mediante el uso de aplicaciones empresariales, como CRM (Customer Relationship Management), ERP (Enterprice Respurce Planning), SCM (Supply Chain Management), SFA (Sales Force Automation), procesamiento de pedidos, Websites, E-commerce, Cloud Computing (Arregoces & Portolani, 2004). Estas aplicaciones deben residir en un entorno bajo condiciones técnicas que garanticen la continuidad de los servicios de TI. Los objetivos de un CPD son proveer:

- Alta disponibilidad de los servicios.
- Almacenamiento, archivo y resguardo de la información.
- Acceso controlado de la información, aplicaciones y equipos, sin importar su ubicación.
- Seguridad física y de red.
- Redundancia.

Estos objetivos se aplican a diferentes áreas funcionales en un CPD:

- Infraestructura: Enrutamiento, switching y arquitectura de servidores.

- Aplicaciones: Balanceo de carga, SSL, control de descarga y almacenamiento de cache.
- Seguridad: Filtrado e inspección de paquetes, detección de intrusión y prevención de intrusos.
- Almacenamiento: Arquitectura SAN, switching del canal de fibra, copias de respaldo y archivado (custodia y conservación de la información).
- Expansión: Extensión de SAN, selección del sitio e interconectividad del CPD.

2.2.4. Ubicación

Un CPD es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones. Por ejemplo, un banco puede tener un CPD con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen algún tipo de CPD, mientras que las más grandes llegan a tener varios.

Las empresas colocan los equipos de usuario cerca del usuario (un ordenador sobre su mesa, un portátil que se lleva a casa); pero los servidores están todos juntos en una misma sala, ambiente (CPD), centralizando todo se consigue:

- **Ahorrar en costes de protección y mantenimiento.** No necesita duplicar la vigilancia, la refrigeración, etc.
- **Optimizar las comunicaciones entre servidores.** Al estar unos cerca de otros no necesitan utilizar cables largos o demasiados elementos intermedios que reducen el rendimiento.
- **Aprovechar mejor los recursos humanos del departamento de informática.** No tienen que desplazarse a distintos edificios para realizar instalaciones, sustituir tarjetas, etc.

Tan importante como tomar medidas para proteger los equipos es tener en cuenta qué hacer cuando esas medidas fallan. Todas las empresas deben tener documentado un plan de recuperación ante desastres, donde se describa con el máximo detalle (en una crisis no hay tiempo para reflexionar) qué hacer ante una caída de cualquiera de los servicios que presenta el CPD. Este plan debe ser actualizado cuando se efectúe un cambio en el CPD (nuevos servicios, nuevos equipos) el plan debe incluir:

- **Hardware:** Que modelos de equipos tenemos instalados (tanto servidores como equipos de red), qué modelos alternativos podemos utilizar y cómo se instalarán (conexiones y configuración).
- **Software:** Qué sistema operativo y aplicaciones están instalados, con el número de versión actualizado y todas las opciones de configuración (permisos, usuarios, etc.).

- **Datos:** Qué sistemas de almacenamiento utilizamos (discos locales, armario de discos), con qué configuración y como se hace el respaldo de datos (copias de seguridad).

2.2.5. Protección

La información es vital para cualquier empresa; si los servidores se paran, la empresa se para. Sucede en todos los sectores: en una empresa de telefonía, en una compañía aérea, en grandes almacenes, en una empresa del sector eléctrico como lo es Electro Puno S.A.A. el CPD debe estar protegido al máximo:

- Elegiremos un edificio en una zona con baja probabilidad de accidentes naturales (terremotos, ciclones, inundaciones).
- También evitaremos la proximidad de ríos, playas, presas, aeropuertos, autopistas, bases militares, centrales nucleares, etc.
- Evitaremos ubicaciones donde los edificios vecinos al nuestro pertenezcan a empresas dedicadas a actividades potencialmente peligrosas: gases inflamables, explosivos, etc.
- Preferentemente seleccionaremos las primeras plantas de edificios:
  - La planta baja está expuesta a sabotajes desde el exterior (impacto de vehículos, asaltos, etc.).
  - Las plantas subterráneas serían las primeras afectadas por una inundación.
  - Las plantas superiores están expuestas a un accidente aéreo, y en caso de incendio iniciado en plantas inferiores, es seguro que nos afectara.

- Se recomienda que los edificios tengan dos accesos y por calles diferentes. Así siempre podremos entrar en caso de que una entrada quede inaccesible (obras, incidente, etc.).
- Es recomendable evitar señalizar la ubicación del CPD para dificultar su ubicación a posibles atacantes. La lista de empleados que entran a esa sala es muy reducida y saben perfectamente dónde está.
- El acceso al CPD debe estar muy controlado. Los servidores solo interesan al personal del CPD.
- En las paredes de la sala deben utilizar pintura plástica porque facilita su limpieza y se evita la generación de polvo.
- En la sala se utilizará piso falso y techo falso, porque facilita la distribución del cableado (para electricidad y comunicaciones) y la ventilación.
- En empresas de alta seguridad, la sala del CPD se recubre con un cobre de hormigón para protegerla de intrusiones desde el exterior.
- Instalaremos equipos de detección de humos y sistemas automáticos de extinción de incendios.
- El mobiliario de la sala debe utilizar materiales ignífugos.

2.2.6. Aislamiento

Los equipos que situamos dentro del CPD utilizan circuitos eléctricos, hay que protegerlas ante:

- **Temperatura.** Los circuitos de los equipos, en especial los procesadores, trabajan a alta velocidad, por lo que generan mucho

calor. Si además le sumamos la temperatura del aire, los equipos pueden tener problemas.

- **Humedad.** No solo el agua, también un alto porcentaje de humedad en el ambiente puede dañarnos. Para evitarlo utilizaremos deshumidificadores.
- **Interferencias Electromagnéticas.** El CPD debe estar alejado de equipos que generen estas interferencias, como material industrial o generadores de electricidad, sean nuestros o de alguna empresa vecina.
- **Ruido.** Los ventiladores de las maquinas del CPD generan mucho ruido (son muchas máquinas trabajando en alto rendimiento), tanto que conviene introducir aislamiento acústico para no afectar a los trabajadores de las oficinas adyacentes.

2.2.7. Tipos de CPD

2.2.7.1. CPD Privado

Denominado también corporativo o empresarial, este tipo de CPD tiene un ámbito privado y ofrece servicios de comunicación y datos a una entidad, que es la propietaria del CPD, esta entidad puede ser empresa privada o institución y organismo gubernamental. Estos centros de datos corporativos son considerados como una inversión, son controlados por un área o departamento de la empresa y son altamente personalizados de acuerdo a sus necesidades (Commscope, Structured connectivity solutions, 2016) tiene las siguientes características:

- La empresa mantiene el control sobre la red y los datos.
- Optimizan la infraestructura de acuerdo a las necesidades del negocio.
- Existe flexibilidad de los servicios de TI para la continuidad del negocio.
- El uso del CPD es exclusivo, no hay con competencia por la prioridad del servicio.

2.2.7.2. CPD Gestionado

Algunas empresas prefieren recurrir a la subcontratación de los servicios de TI a un tercero, un CPD gestionado o un CPD locación comparativa es un negocio dirigido por terceros que genera ingresos mediante la contratación de sus servicios de TI o parte de las capacidades del CPD a clientes empresariales ofreciendo un servicio público seguro. Los clientes pueden ser propietarios de sus propios equipos activos, o estos pueden ser proporcionados por el operado del CPD:

- Los costos de implementación son asumidos por el operador del CPD.
- La empresa que subcontrata, se enfoca en actividades del negocio.
- Servicios de copias de respaldo para recuperación ante desastres.
- Se simplifica el proceso de aumento o disminución de la capacidad de red.

Este tipo de CPD está diseñado para soportar múltiples clientes, por lo tanto, la personalización es limitada a diferencia de un CPD privado. El incremento en la capacidad de TI de los clientes es atendido por el operador con soluciones disponibles de acuerdo a la infraestructura instalada. La actualización y/o renovación de los recursos esenciales son cuidadosamente programadas y ejecutadas de manera que los servicios de TI no se interrumpan.

2.2.7.3. CPD Público

CPD de ámbito público, que es propiedad de un proveedor de servicios tradicionales de datos y servicios a varios clientes a través de Internet como web hosting o VPN (Virtual Private Network). Es un servicio que carece de regulación y está relacionado con operadores comerciales de Internet y web hosting (Commscope, 2011)

2.2.7.4. Otros Tipos de CPD

Se tienen casos particulares de CPD que podrían considerarse híbridos, entre los privados y gestionados. Esto consiste en subcontratar un CPD gestionado para uso exclusivo de un solo cliente. Esta práctica es un intento por mantener los beneficios de un CPD privado, dejando la administración de las instalaciones físicas al operador del CPD gestionado.

Otro tipo de CPD que usualmente basa sus actividades en anuncios o publicidades, se refiere a empresas cuyo negocio es la gestión de redes de datos. Sitios que muestran catálogos en línea, servicios gratuitos, sitios de búsqueda y las redes sociales son un buen ejemplo de este tipo.

Estos centros de datos son grandes en todos los aspectos y suelen ser denominados como mega CPD. Son empresas que operan estrictamente en línea siendo totalmente dependientes de la velocidad y la capacidad instalada de su red para poder ofrecer un acceso instantáneo información y una alta capacidad de respuesta a las transacciones de todos sus clientes. El modelo de negocio para los mega centros de datos obliga a estos a centrarse en costos bajos en general y garantizar una alta disponibilidad del CPD (Arregoces & Portolani, 2004).

2.2.8. Diseño de un CPD de Respaldo

Un centro de respaldo se diseña bajo los mismos principios que cualquier CPD, pero bajo algunas consideraciones más. En primer lugar, debe elegirse una localización totalmente distinta a la del CPD principal con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del CPD principal. La distancia está limitada por las necesidades de telecomunicaciones entre ambos centros.

En segundo lugar, el equipamiento electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el CPD principal. Esto no implica que el equipamiento deba ser exactamente igual. Normalmente, no todos los procesos del CPD principal son críticos. Por este motivo no es necesario duplicar todo el equipamiento. Por otra parte, tampoco se requiere el mismo nivel de servicio en caso de emergencia. En consecuencia, es posible utilizar hardware menos potente. La pecera de un centro de respaldo recibe estas denominaciones en función de su equipamiento:

- Sala blanca: cuando el equipamiento es exactamente igual al existente en el CPD principal.
- Sala de back-up: cuando el equipamiento es similar pero no exactamente igual.

En tercer lugar, el equipamiento software debe ser idéntico al existente en el CPD principal. Esto implica exactamente las mismas versiones y parches del software de base y de las aplicaciones corporativas que estén en explotación en el CPD principal. De otra manera, no se podría garantizar totalmente la continuidad de operación.

Por último, pero no menos importante, es necesario contar con una réplica de los mismos datos con los que se trabaja en el CPD original. Este es el problema principal de los centros de respaldo, que se detalla a continuación.

2.2.9. Infraestructura de un CPD

La palabra infraestructura se utiliza con mayor frecuencia para hacer referencia a la parte eléctrica y el cableado estructurado que tienen lugar en un CPD. Realmente, es un término más amplio que se aplica a los siete sistemas que conforman las instalaciones de un CPD: el espacio físico, el piso elevado, el sistema eléctrico, el sistema de suministro de energía de reserva, el cableado estructurado, el sistema de refrigeración – enfriamiento de precisión y el sistema para la extinción de incendios (Americas, 2010)

2.2.9.1. Espacio Físico

En el espacio físico que ocupa el CPD con todos los subsistemas, componentes y elementos. Esto se aplica generalmente a la superficie total del CPD y sus espacios asociados, tales como salas eléctricas o áreas de almacenamiento. (Commscope, 2011)

2.2.9.2. Piso elevado

El piso elevado es un sistema de rejilla que se instala con frecuencia en los Centros de Datos. El aire enfriado, los cables de suministro eléctrico y algunas veces el cableado de red se instala utilizando el espacio debajo del piso elevando, promoviendo un mejor flujo de aire permitiendo un manejo sencillo y facilitando el tendido de cables. Detectores de humedad detectores de humo pueden ser ubicados aquí.

Los pisos elevados están compuestos por baldosas estándar de 60 centímetros (2 pies) cuadrados. Las baldosas pueden variar en peso, resistencia, fuerza, dependiendo de la carga y disposición. Las baldosas vienen en presentaciones con pequeñas perforaciones o con secciones de corte, que se colocan en lugares estratégicos para que den paso al aire y el cableado entre las áreas por encima y por debajo del piso elevado. (Commscope, 2011)

2.2.9.3. Sistema eléctrico

Son todas las instalaciones relacionadas con el suministro de energía eléctrica en el CPD. Esto normalmente incluye los paneles eléctricos, conductos, contenedores y varios tipos de conectores. El suministro de energía para este sistema por lo general proviene de una fuente de alimentación comercial externa, es decir una compañía local que brinda este servicio. (Commscope, 2011)

2.2.9.4. Sistema de energía de reserva

Incluye todos los sistemas de energía de reserva a cargo de soportar toda la carga eléctrica del CPD, en caso del que el suministro eléctrico comercial falle por cualquier razón. Este sistema incluye los UPS (Uninterrumpible Power Supply) o generadores. (Commscope, 2011)

2.2.9.5. Sistema de cableado

El sistema de cableado estructurado del CPD comprende el cableado de cobre y fibra óptica como medios típicos. Los componentes comunes incluyen los contenedores de cobre y fibra, Patch Panels (conjunto de conectores que se utiliza para recibir y organizar las conexiones de cobre coaxial o fibra óptica), faceplates, racks, patch cords, canalizaciones y demás elementos utilizados para el cableado estructurado. (Commscope, 2011)

2.2.9.6. Sistema de enfriamiento de precisión

El sistema de enfriamiento comprende las cámaras de enfriamiento y el tratamiento de aire para regular la temperatura y controlar la humedad del ambiente en el CPD. Este sistema podría incorporar el sistema de aire acondicionado usado para enfriar las oficinas en el mismo edificio, o puede ser independiente de él. Los racks o gabinetes de servidores individualmente también pueden poseer sus propios métodos de enfriamiento. (Commscope, 2011)

2.2.9.7. Sistema para la extinción de fuego

La extinción de fuego e incendios incluyen todos los elementos o dispositivos asociados con la detección y/o extinción del fuego en el CPD. Los elementos más utilizados son los sistemas gaseosos, extintores portátiles o incluso agua mediante aspersores. También

se instalan dispositivos que detectan humo y miden la calidad del aire. (Commscope, 2011)

2.2.9.8. Otros Componentes de la Infraestructura

Hay también algunos elementos de infraestructura que no se enmarcan dentro de las categorías anteriores, pero comúnmente se encuentran en los CPD. Estos incluyen los dispositivos de detección de fugas, mitigación sísmica, y los controles de seguridad física tales como lectores de tarjetas y cámaras de seguridad. (Commscope, 2011)

2.2.10. Estándar ANSI TIA-942

2.2.10.1. Definición

La TIA (Telecommunication Industry Association) publica el TIA-942 Telecommunications Infraestructure Standard for CPD (Estándar para la infraestructura de Telecomunicaciones de CPD), con la intención de unificar los criterios en el diseño de CPD. El estándar especifica las características para la Infraestructura de telecomunicaciones en el CPD y los servicios relacionados que serán el soporte para la tecnología de la información a instalar, cubriendo aspectos como el TIERing (se utiliza el término para calificar un CPD y puede ser TIER-I, TIER-II, TIER-III, TIER-IV), y la redundancia que harán que un CPD sea menos susceptible a

las interrupciones debido a la falta de suministro de energía a los equipos activos.

Las especificaciones del estándar TIA-942 se aplican el diseño de CPD de ámbito público y de ámbito privado, cubriendo temas como: La arquitectura de red, diseño eléctrico, almacenamiento de archivos, backup y resguardo, redundancia, control de acceso y seguridad, gestión de base de datos, web hosting, app hosting, distribución de contenidos, control ambiental, protección contra riesgos físicos (incendios, inundaciones, tormentas) y administración de energía. (TELECOMMUNICATIONS INDUSTRY ASSOCIATION , 2005)

2.2.10.2. Objetivo del estándar

El estándar establece las directrices y los requerimientos para el diseño e instalación de un CPD de cualquier tamaño. El estándar está dirigido a profesionales que necesiten una comprensión integral del diseño de un CPD, el sistema de cableado, el diseño de la red y la planificación para la instalación.

El diseño proporciona información que permite unificar los esfuerzos del diseño multidisciplinario, promoviendo la cooperación en las fases del diseño y construcción. Una planificación adecuada para la construcción o renovación es

mucho menos costosa y menos perjudicial que ejecutar acciones después de que las instalaciones están en funcionamiento.

La estandarización de la nomenclatura utilizada en el diseño, construcción e implementación de CPD, mejora el intercambio tecnológico entre fabricantes y operadores, permitiendo diseños uniformes en cualquier ámbito y altas capacidades de expansión y escalabilidad. (TELECOMMUNICATIONS INDUSTRY ASSOCIATION , 2005)

2.2.10.3. Alcance del estándar

El estándar especifica los requerimientos técnicos mínimos, para el diseño de la infraestructura de telecomunicaciones de un CPD, ya sean corporativos o empresariales, grandes o pequeños, CPD gestionados, CPD de ámbito público, mega CPD y algunos híbridos. La topología propuesta en el estándar puede ser utilizada durante el diseño de un CPD de cualquier tamaño.

2.2.11. Metodología Schneider para CPD

La metodología Schneider para la implementación de proyectos de CPD establece una secuencia de planificación del sistema a utilizar para el diseño de la capa de infraestructura física de un CPD. Esta metodología está basada en las sugerencias del estándar TIA-942. (Rasmussen & Niles, 2006)

La metodología Schneider reconoce como fases del proceso de implementación de proyectos de CPD lo siguiente:

- Diseñar
- Construir
- Explorar
- Evaluar
- Planificar

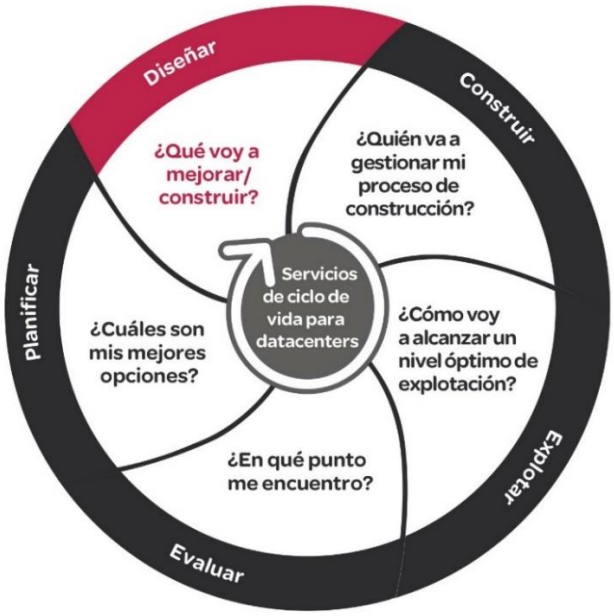


Figura 1: Metodología Schneider para CPD
Fuente: B Schneider

La secuencia de planificación del sistema es el flujo lógico del pensamiento, las actividades y los datos que transforman la idea inicial del proyecto en un plan de instalación detallado. Dicha secuencia de planificación consta de cinco (05) tareas que toman lugar durante las fases de preparación y diseño del proyecto. (Rasmussen & Niles, 2006)

Una vez que se diseñan los parámetros fundamentales de TI, se determina el diseño conceptual del sistema. Esto se puede hacer de manera fácil seleccionando un diseño de referencia que sea compatible con los parámetros calculados y con las características físicas del ambiente en el que se instalara la base de datos. Luego se recolectan detalles específicos de la propuesta realizada por el usuario para determinar cuáles con aquellas que necesiten ser reajustadas. Estos detalles se conocen como requerimientos de usuarios. Estos requerimientos, acompañados de las sugerencias del estándar TIA-942 se convierten en las especificaciones técnicas del sistema. Dichas especificaciones son reglas que se deben seguir al momento de crear el diseño detallado. (Rasmussen & Niles, 2006)

Tarea de Planificación	Descripción de la Tarea	Información de la Entrada	Información de la Salida
Determinar parámetros de TI	Calcular los parámetros fundamentales de TI que guiaran el diseño de la infraestructura física.	Características del negocio.	Criticidad, capacidad, pan de crecimiento.
Desarrollar el concepto del sistema	Desarrollar conceptos para soportar los parámetros TI.	Criticidad, capacidad, pan de crecimiento.	Diseño de la referencia.
Realizar requerimientos del usuario	Evaluar y ajustar los detalles específicos por el usuario para el sistema propuesto.	Diseño de la referencia.	Requerimientos del usuario.
Generar Especificaciones	Combinar los requerimientos del usuario con las especificaciones del estándar TIA-942 para completar las especificaciones técnicas.	Requerimientos del usuario.	Especificaciones técnicas.
Generar el diseño detallado	Crear el diseño detallado utilizando las especificaciones como reglas.	Especificaciones técnicas.	Diseño detallado del CPD.

Cuadro 1: Diseño Conceptual del Sistema
Fuente: Metodología Schneider

Para la determinación de parámetros de TI, la metodología Schneider sugiere recoger información del negocio a fin de

determinar las siguientes características, que llevaran a definir el nivel de criticidad para la implementación de un CPD. (Rasmussen & Niles, 2006)

Criticidad 1:

- El negocio es pequeño.
- Las decisiones empresariales en su mayoría dependen del costo que implican.
- La presencia en línea es limitada.
- Existe muy poca dependencia de servicios de TI.
- El tiempo en corte es un inconveniente tolerable.

Criticidad 2:

- Se tiene ingresos reducidos por la presencia en línea.
- Se necesitan múltiples servidores para atender las necesidades.
- Los sistemas de telefonía IP son vitales para el funcionamiento del negocio.
- Gran parte de las operaciones se realizan con correo electrónico.
- Existe tolerancia al tiempo en corte planificado.

Criticidad 3:

- Presencia a nivel mundial.
- La mayoría de los ingresos provienen de negocios en línea.

- Es necesario implementar sistemas VoIP.
- Existe alta dependencia de servicios de TI.
- Los costos de experimentar tiempo en corte son elevados.
- La marca del negocio es conocida mundialmente.

Criticidad 4:

- El negocio es multimillonario.
- La mayoría de los ingresos provienen de transacciones electrónicas.
- El modelo de negocio depende completamente de los servicios de TI.
- Los costos de experimentar tiempo en corte son extremadamente altos.

2.2.12. Topologías y áreas de un CPD

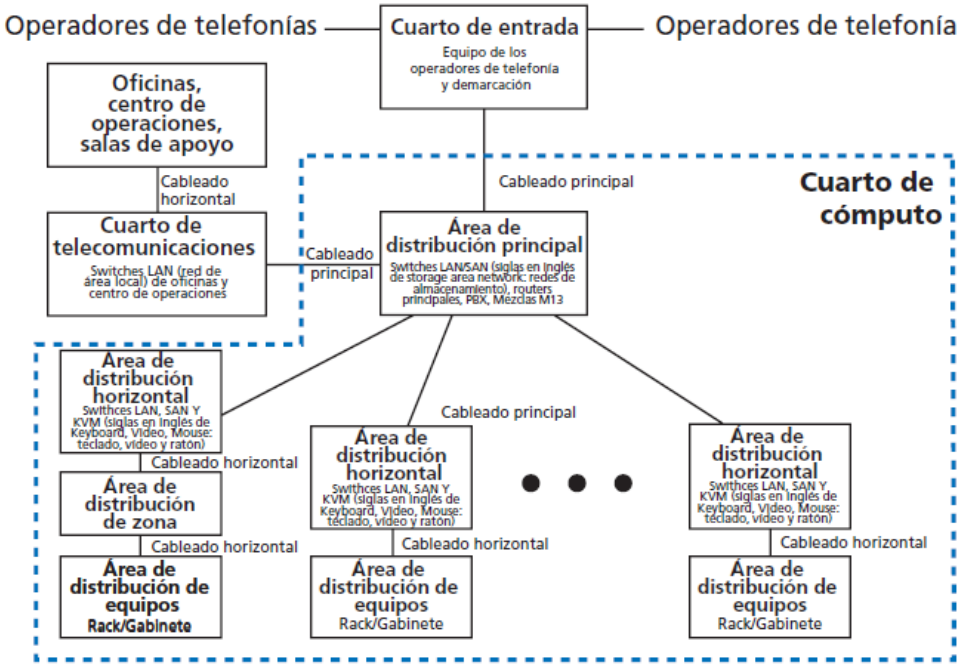


Figura 2: Topología de CPD con la norma TIA-942
Fuente: Estándar TIA 942

El CPD requiere de espacios dedicados para soportar la infraestructura de TI, como el cableado y los equipos. Los espacios que se encuentran dentro de una CPD incluyen la sala de entrada (ER), el área de distribución principal (MDA), el área de distribución horizontal (HDA), el área de distribución zonal (ZDA) y el área de equipos de distribución (EDA), la figura 2 muestra la topología y áreas de un CPD típico. La implementación de algunas áreas depende del tamaño del CPD. (Americas, 2010)

2.2.12.1. Sala de entrada

La sala de entrada (Entrance Room) es la interface entre el proveedor de internet y el CPD, es el espacio utilizado para

albergar equipo y cableado del proveedor de servicios de telecomunicaciones como Internet. Dependiendo del nivel de redundancia o TIERing debe contar con más de una sala de acometida para albergar equipos y cableado de más de un proveedor, y reunir cualidades para la expansión de manera que se pueda restablecer el servicio en caso de emergencia. La entrada principal se encuentra fuera de la sala de equipos por razones de seguridad, pero se conecta con el área de distribución principal (MDA).

La sala de entrada principal sirve como punto de demarcación entre las redes del o de los proveedores de servicios del CPD. Los proveedores de servicios equipan este espacio y controlan los equipos y el cableado correspondiendo, mientras que el operador del CPD controla el rack o gabinete utilizando para albergar las conexiones. (Americas, 2010)

2.2.12.2. Área de distribución Principal (MDA)

El área de distribución principal (Main Distribution Area) es el punto central de distribución para el sistema de cableado estructurado del CPD, y se encuentra dentro la sala de equipos. En CPD grandes, el MDA se ubica, por seguridad, en un ambiente separado. Todo CPD tiene al menos un área de distribución principal. Aquí se instalan los routers centrales (core routers), los

switches centrales (core LAN/SAN switches), la conexión cruzada principal (MC) y puede incluir la conexión cruzada horizontal (HC) cuando las áreas de equipos se sirven directamente desde el área de distribución principal (MDA), todos se encuentran a menudo en el área de distribución principal, ya que este espacio es el núcleo de la infraestructura del cableado para el CPD. Los equipos proporcionados por el proveedor de acceso a menudo se encuentran en el área de distribución principal en lugar de la sala de entrada para evitar la necesidad de una segunda sala de entrada, debido a las restricciones de la longitud del circuito. (TELECOMMUNICATIONS INDUSTRY ASSOCIATION , 2005)

2.2.12.3. Área de Distribución Horizontal (HDA)

El área de distribución horizontal (Horizontal Distribution Area) se utiliza para servir a las áreas de equipos de distribución cuando el HC no se encuentra en el área de distribución principal. Por lo tanto, cuando se utiliza, el área de distribución horizontal puede incluir el HC, que es el punto de distribución para el cableado de las áreas de equipos de distribución. El área de distribución horizontal se ubica dentro de la sala de equipos, pero pueden ser ubicados en un ambiente separados para mayor seguridad. El área de distribución horizontal generalmente incluye los switches LAN, los switches SAN y KVM (interfaces para teclado, video y ratón). Las salidas del cableado horizontal hacia los equipos empiezan aquí. Por lo general un HDA servirá a grupos de

equipos y por lo tanto, requieren menos espacio para la expansión que el MDA. Un CPD pequeño puede no requerir de áreas de distribución horizontal, ya que la sala de equipos puede ser capaz de contar con el apoyo del área de distribución principal. Sin embargo, un CPD típico tendrá varias HDAs. (TELECOMMUNICATIONS INDUSTRY ASSOCIATION , 2005)

2.2.12.4. Área de Equipos de Distribución (EDA)

El área de equipos de distribución (Equipment Distribution Area) es el espacio asignado para los gabinetes, racks, equipos activos de procesamiento (servidores) y equipos para almacenamiento montados en gabinetes o racks (bastidores).

El cableado horizontal termina en el área de equipos de distribución en los conectores dispuestos en el hardware montado en los gabinetes bastidores. Se deben instalar receptáculos de energía suficientes y se debe proporcionar hardware de conexión para cada gabinete o rack de equipos de manera que se puede minimizar la longitud de los patch cords y del cable de alimentación.

El cableado punto a punto está permitido entre equipos ubicados en el área de distribución de equipos. La longitud del cable para el cableado punto a punto entre equipos en el área de equipos de distribución no debe ser mayor de 15m (49 pies) y debe estar en

bastidores entre los equipos y gabinetes adyacentes en la misma fila. (Commscope, 2011)

2.2.12.5. Área de Distribución de Zona (ZDA)

El área de distribución de zona (Zona Distribution Area) es utilizada en CPD de gran envergadura, su disposición es opcional, permite flexibilidad para el cableado adicional y éste se debe limitar a servir a un máximo de 288 conexiones de pares trenzados o coaxiales para evitar la congestión de cables en especial para los recintos en los cuales se instala los cables encima o debajo de baldosas accesibles de 600 mm x 600 mm (o 2 pies x 2 pies). No habrá equipos en el área de distribución de la zona, solamente equipo pasivo y debe estar a 15 m del HDA. (TELECOMMUNICATIONS INDUSTRY ASSOCIATION , 2005)

2.2.12.6. Sala de Equipos (ER)

La sala de equipos (Computer Room) es un espacio muy seguro y con un sistema para el control ambiental, que alberga equipos de datos y telecomunicaciones, así como el cableado correspondiente. Se divide en diferentes áreas de distribución, que son los puntos de conexión para el sistema de cableado estructurado. Los racks (bastidores) / gabinetes que soportan a los equipos se sitúan sobre el piso elevado instalado. El aire refrigerado y el cableado (de datos y eléctricos) son generalmente

instalados por debajo de este piso. (TELECOMMUNICATIONS INDUSTRY ASSOCIATION , 2005)

2.2.12.7. Sala de Telecomunicaciones (TR)

En los CPD, la sala de telecomunicaciones (Telecommunication Room) es un espacio que soporta equipo de telecomunicaciones y el cableado a zonas fuera de la sala de equipos. El TR normalmente se encuentra fuera de la sala de equipos, pero si es necesario, se puede combinar con el área de distribución principal o áreas de distribución horizontal. Dependiendo del tamaño del CPD puede simplificarse a un gabinete de telecomunicaciones. (TELECOMMUNICATIONS INDUSTRY ASSOCIATION , 2005)

2.2.12.8. Sala de Equipos Eléctricos y Mecánicos

El sistema Eléctrico y Mecánico consta de la entrada de servicios públicos, distribución del suministro de energía comercial y el equipo de tratamiento de aire para los servicios de refrigeración, suministro de energía de reserva con UPS o generadores y un sistema de gran fiabilidad, son esenciales para lograr una meta de 100% de disponibilidad. (Americas, 2010)

La sala de equipo eléctrico y mecánico deberá tener al menos un teléfono montado en la pared, así como al menos una conexión de datos para el acceso al sistema de gestión.

2.2.12.9. Áreas de Apoyo del CPD

Las áreas de apoyo del CPD son espacios ubicados preferentemente fuera de la sala de equipos que se dedica a apoyar las actividades del CPD. Estos pueden incluir un centro de operaciones, oficinas de personal de apoyo, salas de seguridad, almacenes, salas de equipos de ensayo o pruebas. Cada uno de estos ambientes debe contar por lo menos con un teléfono de pared.

El centro de operaciones, sala de seguridad, y las oficinas de personal de apoyo será cableado de manera similar a las áreas de oficina como en ANSI/TIA/EIA-568-B.1. Se debe considerar instalar consolas o paneles de control y seguridad en el centro de operaciones que puedan incluir monitores globales en paredes o individuales que faciliten el monitoreo del CPD. (Americas, 2010)

2.2.13. Redundancia en el CPD

La redundancia se implementa para eliminar los posibles puntos de falla. Una instalación sin UPS o sin generador de energía eléctrica tiene un punto de posible falla ante determinadas circunstancias.

Los CPD que están equipados por diversos dispositivos e instalaciones de telecomunicaciones puede ser capaces de

continuar con sus operaciones en condiciones catastróficas que de otra manera interrumpirán los servicios de telecomunicaciones del CPD.

La fiabilidad de la infraestructura de comunicaciones se puede aumentar al proporcionar vías y áreas de conexión cruzada redundantes que estén físicamente separados. Es común que los CPD tengan más de un proveedor de servicios de acceso a Internet, routers redundantes, distribución central redundante y switches de borde. Aunque esta topología de la red proporciona un cierto nivel de redundancia, la duplicación de hardware y servicios por sí sola no garantiza que los puntos de fallo hayan sido eliminados.

2.2.14. Redundancia de Vías de Entrada y Mainholes

Tener múltiples vías de entrada y Mainholes (espacio subterráneo utilizado para albergar y facilitar el mantenimiento de conexiones del proveedor de servicios de acceso) para el proveedor de acceso hacia las salas de entrada, elimina un punto de fallo, en la entrada de los servicios del proveedor de acceso. Preferentemente las vías de entrada y los Mainholes deben estar en lados opuestos del edificio y por lo menos a 20m (66 pies) de distancia.

En CPD con dos salas de entrada y dos Mainholes, no es necesario instalar conductos de cada sala de entrada a cada uno de los Mainholes. En esta configuración, se solicita al proveedor de acceso la instalación de dos cables de la entrada, uno a la sala de entrada principal (primary access room) a través del mainhole principal, y una a la entrada secundaria (secundary access room) a través del mainhole secundario. Conductos desde el mainhole principal hacia la sala de entrada secundaria y del mainhole secundario a la sala de entrada principal proporcionan flexibilidad, pero no son necesarios. (Americas, 2010)

2.2.14.1. Redundancia de Proveedor de Acceso

La continuidad de acceso a los servicios de telecomunicaciones en el CPD se puede asegurar mediante la utilización de múltiples proveedores de acceso y de múltiples vías del proveedor de acceso para el CPD. La utilización de múltiples proveedores de acceso asegura que el servicio continúe en el caso de que un proveedor de acceso suspenda el servicio por algunas circunstancias ajenas al CPD.

La utilización de múltiples proveedores de acceso por sí solo no asegura la continuidad del servicio, ya que los proveedores de acceso podrían ser distribuidores que dependen del mismo proveedor. El cliente debe asegurarse de que sus servicios son

provistos por diferentes proveedores o empresas que tengan sus propios canales de servicios y vías de acceso.

2.2.14.2. Salas de Entrada Redundantes

Varias salas de entrada mejoran la redundancia, pero complican la gestión. Se debe tener cuidado para distribuir las conexiones entre las salas de entrada.

Los proveedores de acceso deben instalar equipos y hacer las conexiones en las dos salas de entrada para que los requerimientos puedan ser suministrados desde cualquiera de las dos salas de entrada. Los equipos instalados por el proveedor de acceso en la sala de entrada no deben estar subordinados a los equipos en la sala entrada de otros. El equipo de proveedor de acceso instalado en cada sala de entrada debe ser capaz de operar en el caso de un fallo en la otra sala de entrada.

2.2.14.3. Área de Distribución Principal Redundante

Un área de distribución principal secundaria proporciona redundancia adicional, pero a costa de complicar la administración. Los routers de core y los switches de core deben ser distribuidos entre el área de distribución principal y el área de distribución secundaria. Los canales y trayectorias también deben ser distribuidos entre los dos espacios.

Un área de distribución secundaria no debe tener sentido si la sala de equipos es un espacio continuo, el área de distribución secundaria y el área principal de distribución deben estar en diferentes zonas de protección contra incendios, y tener diferentes unidades para el suministro de energía, así como diferentes equipos de aire acondicionado.

2.2.14.4. Cableado Backbone Redundante

El cableado backbone redundante protege contra una interrupción. El cableado troncal redundante se puede tender o desplegar de varias maneras, dependiendo del grado de protección deseado.

El cableado backbone entre dos espacios, por ejemplo, el área de distribución horizontal y el área de distribución principal, puede ser establecido mediante el tendido de dos cables entre estos espacios, preferentemente siguiendo rutas diferentes. Si el CPD tiene tanto un área de distribución principal y un área de distribución secundaria, el cableado backbone redundante para el área de distribución horizontal no es necesario, aunque el tendido de cables en el área de distribución principal y el área de distribución secundaria deben seguir diferentes rutas.

Se puede proporcionar cierto grado de redundancia mediante la instalación de cableado backbone entre las áreas de distribución horizontal. Si el cableado backbone del área de distribución principal hacia el área de distribución horizontal se daña, los enlaces pueden ser conectados a través de otra área de distribución horizontal.

2.2.14.5. Cableado Horizontal Redundante

El cableado horizontal en sistemas críticos puede utilizar diversas rutas para una mayor redundancia. Se debe tener cuidado de no exceder las longitudes máximas del cable horizontal durante la selección de rutas.

Los sistemas críticos pueden ser apoyados por dos áreas de distribución horizontal diferentes, siempre y cuando no se excedan las restricciones de longitud máxima del cable y las HDA estén ubicadas en diferentes zonas de protección contra incendios y siniestros. (Americas, 2010)

2.2.15. Disponibilidad del CPD

El grado en que los equipos del CPD funcionen de manera continua se conoce como la disponibilidad del CPD o tiempo de actividad (uptime).

La mayoría de las empresas requieren disponibilidad alta o muy alta del CPD, ya que el tiempo de inactividad (downtime) afecta a su capacidad productiva y restringe las actividades comerciales. ¿Qué tan alta disponibilidad requiere una empresa? Esto puede variar significativamente y está representado por el concepto de los nueves. El mayor número nueves, que es el más cercano al 100%, garantiza la mayor disponibilidad posible de alcanzar. Digamos, por ejemplo, que se realiza mantenimiento al sistema eléctrico del CPD, lo que indica que se debe pasar a un estado de inactividad en línea durante una hora de mantenimiento cada mes. Suponiendo que no haya cortes o fallas adicionales de ningún otro tipo, lo que significa que el CPD está funcionando durante un año menos 12 de las 8.760 horas al año. Eso es 99,863% del tiempo, o lo que es lo mismo a dos nueves de disponibilidad.

Para algunas empresas, esa es una cantidad perfectamente aceptable de tiempo de inactividad. Pero para otras empresas o compañías tales como las entidades financieras, entidades gubernamentales, hospitales, empresas con presencia importante en Internet o que hacen negocios en múltiples zonas horarias, por ejemplo, que basan sus operaciones en la disponibilidad de los CPD, establecer cinco nueves de disponibilidad como su estándar. Eso es 99,999%, o poco más de cinco minutos de tiempo de inactividad en un año. (Americas, 2010)

El estándar utiliza cuatro categorías (TIERs) para clasificar la disponibilidad de un CPD. El estándar va más allá de tiempos de inactividad planificados y no planificados debido a mantenimiento o fallas, pues involucra también los factores de fallas en el funcionamiento parcial o total debido a la interacción humana voluntaria o involuntaria, desastres naturales tales como inundaciones, terremotos, huracanes, actividad criminal, terrorismo y actos de guerra.

El estándar cita un ejemplo para un CPD de categoría (TIER)4:

“Considerando todos los eventos físicos potenciales, ya sean intencionales o accidentales, naturales o artificiales, que podrían causar la caída del CPD de categoría 4 proporciona protección específica y en algunos casos redundante contra estos eventos. Un CPD calificado como categoría o TIER 4, considera los problemas potenciales como los desastres naturales, sismos, inundaciones, incendios, huracanes y tormentas, así como los posibles problemas con el terrorismo y empleados descontentos. Un CPD TIER 4 tiene el control de estos aspectos en sus instalaciones.”

El tiempo de inactividad anual máximo permitido por el estándar es el siguiente:

- TIER 1: 28,8 horas
- TIER 2: 22,0 horas
- TIER 3: 1,6 horas
- TIER 4: 0,4 horas

Si tenemos en cuenta el coso por hora de muchas empresas o industrias que realizan operaciones con apoyo de TI (ver cuadro 2), se puede ver rápidamente la pérdida que representa el tiempo de inactividad. (TELECOMMUNICATIONS INDUSTRY ASSOCIATION , 2005)

Aplicaciones	Sector (Industria)	Costo por hora (USD)
Bolsas de Valores	Finanzas	$6,45 millones
Tarjetas de Crédito	Finanzas	$2,6 millones
Pay-per-view	Media	$150K
Hogar	Comercio minorista	$113K
Catálogos de ventas online	Comercio minorista	$90K
Reservas de pasajes aéreos	Transporte	$89.5K
Tele-Venta de entradas	Media	$69K
Entrega de paquetes	Transporte	$28K
ATM	Finanzas	$14,5K

Cuadro 2: Costos por tiempo de inactividad de un CPD
Fuente: Contingency Research Planning

Cuando se planifica un CPD, es importante considerar el tiempo de inactividad máximo que se puede permitir de acuerdo al sector donde se ejecuta la aplicación. Cuanto mayor es el requerimiento de disponibilidad del CPD, mayor es la infraestructura a implementar. Lógicamente, si una fuente de energía de reserva mantiene el CPD en funcionamiento cuando falla el suministro eléctrico comercial, entonces dos fuentes de energía están allí para hacerse cargo en caso de algún problema con el primero durante un corte de energía.

La capacidad necesaria se conoce como la capacidad N: “N es necesario”. El término puede aplicarse a todo tipo de elementos de la infraestructura del CPD, pero es más comúnmente utilizado cuando se habla de energía de reserva, refrigeración y el cableado de red, la capacidad N está relacionada con los TIERs.

Para un CPD pequeño, la capacidad de N podría consistir de una unidad de refrigeración de aire para mantener el ambiente en condiciones ideales, una pequeña fuente de energía para mantener el suministro eléctrico en el caso de que el suministro de energía comercial falle, y tres dispositivos de red que permitan enrutar todo el tráfico de la red. Para un CPD grande, que proporciona la misma funcionalidad, se podría requerir 15 unidades de tratamiento de aire, dos generadores con una capacidad mucho mayor y 20 dispositivos de red. Considerar que

la capacidad del CPD se refiere al nivel de funcionalidad que ofrece, no al número de componentes de su infraestructura.

Para establecer la infraestructura que asegure la mayor disponibilidad se utiliza el concepto TIER, el cual indica el nivel de fiabilidad de un CPD y está asociado a cuatro niveles de disponibilidad definidos. A mayor número en el TIER, mayor disponibilidad, y por lo tanto mayores costes asociados en su construcción y más tiempo para la implementación. Los TIERs son:

2.2.15.1. TIER 1: CPD Básico

Un CPD de TIER 1 es el escenario de diseño más básico y menos costoso. En este diseño no hay planificación para contingencias, los equipos instalados son todo lo que se necesita para cumplir con las operaciones y es representado por “N” de Need (Necesario), en la mayoría de la documentación. Cualquier plan de mantenimiento a los sistemas críticos o cualquier otro imprevisto o falla, conducirá al tiempo de inactividad parcial o total del CPD. Si bien es evidente que una institución financiera o de otro tipo que tiene centralizada sus operaciones en los centros necesita mucho más que este grado de disponibilidad, existen otras instituciones y aplicaciones que pueden ser capaces de tolerar este nivel de rendimiento.

Puesto que no hay redundancia, es importante seguir las mejores prácticas en el diseño e instalación en este tipo de CPD.

Características:

- El servicio puede interrumpirse por actividades planeadas o no planeadas.
- Ausencia total de componentes redundantes.
- Puede o no puede tener pisos elevados, generadores auxiliares o UPS.
- Tiempo medio de implementación, 3 meses.
- La infraestructura del CPD deberá estar fuera de servicio al menos una vez al año (28,8 horas) por razones de mantenimiento y/o reparaciones.
- Disponibilidad del 99,671%.

2.2.15.2. TIER 2: CPD con Componentes Redundantes

Un CPD de TIER 2 prevee que tendrá algún tipo de mantenimiento en los sistemas, por lo que implementa componentes críticos adicionales (de repuesto). Esto se representa con una “N+1” (Need más 1) en la documentación. El mantenimiento planeado o la falla de algún componente crítico del sistema, no disminuye el funcionamiento del CPD. Sin embargo, más de un evento planificado o no planificado se traducirá en un menor rendimiento o una caída del sistema.

El TIER 2 es la clasificación más comúnmente utilizada para la implementación de la mayoría de los CPD, mientras que los TIER 3 y TIER 4 son costosos. Algunos CPD utilizan las pautas de diseño de TIER 3 en el diseño de componentes de misión crítica, tales como la energía, seguridad y refrigeración. Mientras mantienen la utilización de reglas de TIER 2 para los otros componentes del sistema que generalmente son más caros.

Características:

- El TIER 2 implementa componentes redundantes, pero solamente una ruta o trayectoria.
- Tiene una sola línea o ruta de distribución eléctrica y refrigeración, pero tiene componentes redundantes en esta ruta de distribución.
- El TIER 2 implementa componentes redundantes que son ligeramente menos susceptibles a las interrupciones planificadas y no planificadas que las de TIER 1.
- Tiene pisos elevados, UPS o generadores auxiliares.
- El diseño de la capacidad de suministro de energía para los UPS y/o los generadores de energía es N+1 (Need plus One) y tiene una trayectoria de distribución única.
- El mantenimiento de la ruta del suministro de energía y otras partes de la infraestructura requiere la interrupción del servicio (apagar los equipos).
- De 3 a 6 meses para implementar.
- Disponibilidad del 99.741%.

2.2.15.3. TIER 3: CPD Mantenible Simultáneamente

Un CPD TIER 3 está diseñado completamente con sistemas paralelos, lo que permite realizar una interrupción planificada o no planificada a un sistema completo, sin interrumpir el funcionamiento del CPD. Esto se representa como un “2N” (Need times 2) en el diseño. Aquí se implementa totalmente la redundancia en el suministro de energía, refrigeración (incluyendo todas las tuberías), fuentes de alimentación secundarias, servidores, hardware de red, etc. Básicamente el diseñador tendrá que diseñar dos sistemas idénticos, o lo que es lo mismo una imagen espejo del otro. Un CPD TIER 3 puede manejar múltiples fallas de los componentes críticos del sistema, pero no puede soportar más de un fallo total del sistema crítico. Múltiples UPS o fuentes de alimentación pueden fallar sin afectar el rendimiento del CPD, pero la falta de más de una fuente eléctrica completa, o una fuente de alimentación eléctrica, junto con algunos componentes críticos del sistema de copias de seguridad, afectará el rendimiento.

Es en este TIER donde tienen especial consideración lo requerimiento estructurales y de seguridad para la elección del sitio y la construcción del CPD. Por ejemplo, el diseño ahora puede superar los estándares del código de construcción de algunos muros y techos, las ventanas exteriores deben ser

excluidas de la sala de equipos, requisitos de seguridad más específicos, etc.

Características:

- Un CPD TIER 3 tienen múltiples rutas o líneas de refrigeración y de distribución, pero sólo una ruta está activa.
- Dado que los componentes redundantes no están en una única ruta de distribución, se puede dar mantenimiento al sistema al mismo tiempo.
- Permite cualquier actividad planificada a la infraestructura del CPD sin interrumpir el funcionamiento del hardware de ninguna manera.
- Las actividades previstas incluyen el mantenimiento preventivo, reparación programada, agregar, quitar, reemplazar y probar componentes y mucho más.
- Para los CPD enfriados con agua, se deben instalar dos conjuntos independientes de tuberías.
- Suficiente capacidad y distribución para realizar simultáneamente la carga en una ruta mientras se realiza el mantenimiento o las pruebas en las redundantes.
- Actividades no planificadas, tales como errores de operación o fallas espontáneas de los componentes de la infraestructura, ocasionarán interrupciones del CPD.

- Los CPD TIER 3, a menudo son diseñados para ser actualizados al TIER 4 cuando el modelo de negocio justifica el costo de la protección adicional.
- El sitio debe estar monitorizado, dirigido y gestionado las 24 horas del día.
- Concurrentemente mantenible.
- De 15 a 20 meses para implementar.
- Disponibilidad del 99,982%.

2.2.15.4. TIER 4: CPD Tolerante a Fallos

Un CPD TIER 4 proporciona el mayor nivel de protección, lo que permite menos de 30 minutos de tiempo de inactividad al año. Con el fin de proporcionar este nivel de seguridad, el diseño se basa en 2(N+1) (redundant Need plus 1), diseño donde no sólo hay dos sistemas redundantes como imágenes espejo, sino que cada uno de estos componentes críticos tiene su reposición. Este diseño tiene la capacidad de soportar tiempo de inactividad total previsto o una falla de todo un lado del sistema, sin embargo, sin degradar el rendimiento del CPD en su conjunto.

Características:

- Múltiples rutas activas de suministro de energía y enfriamiento. Por lo menos dos rutas están activas en TIER 4, la infraestructura proporciona un mayor grado de tolerancia a fallos.

- Múltiples vías de alimentación para todos los equipos informáticos y de telecomunicaciones. TIER 4 requiere que todos los equipos informáticos y de telecomunicaciones tengan múltiples entradas de energía.
- Permite planificar actividades de mantenimiento sin afectar al servicio de computación críticos, y es capaz de soportar por lo menos un evento no planificado del tipo 'peor escenario' sin impacto crítico en la carga.
- Rutas activas de distribución simultáneas, esto significa dos sistemas UPS independientes en las que cada sistema tiene redundancia N+1.
- Las Infraestructuras TIER 4 son las compatibles con el concepto de alta disponibilidad de TI que implementan server clustering (agrupación o servidores dentro de una red), RAID (reduntant array of independent disks), DASD (direct-access storage device, "Dazzdee") y comunicaciones redundantes para lograr la confiabilidad, disponibilidad y mantenimiento o servicio técnico.
- Disponibilidad del 99,995%.
- De 15 a 20 meses para implementar.

La clasificación TIER permite identificar la infraestructura necesaria y la calidad del servicio que se desea instalar en el CPD. Por ejemplo, si se diseña un CPD TIER 3, significa que su infraestructura no fallará más de 1,6 horas al año, que no hay

interrupciones por mantenimientos planificados y que puede haber eventos inesperados que causen interrupciones del servicio. Tener en cuenta que se refiere a la infraestructura del CPD y que otros aspectos como la disponibilidad de los equipos y los servicios de TI que soporta el CPD se gestionan de otra manera. (TELECOMMUNICATIONS INDUSTRY ASSOCIATION , 2005)

	TIER 1	TIER 2	TIER 3	TIER 4
Rutas habilitadas	1	1	1 activo 1 pasivo	2 activos
Componentes redundantes	N	N+1	2N	2(N+1)
Relación de apoyo del piso elevado	20%	30%	80-90%	100%
Watts/pies2 iniciales	20-30	40-50	40-60	50-80
Altura del piso elevado	12''	18''	30-36''	30-36''
Carga del piso (pounds/ft2)	85	100	150	150+
Servicio de voltaje	208, 480	208, 480	12-15kV	12-15kV
Meses para implementar	3	3-6	15-20	15-20

Primera instalación	1965	1970	1895	1995
Tiempo de inactividad anual	29.8 hrs	22 hrs	1,6 hrs	0.4 hrs
Disponibilidad	99.671%	99.749%	99.962%	99.995%

Cuadro 3: Comparación de TIER TIA 942
Fuente: TIER reference guidelines from TIA-942
Elaboración: Propia

2.2.16. Gestión de la Información

2.2.16.1. Definición

La gestión de la información es el conjunto de actividades realizadas con el fin de controlar, almacenar y, posteriormente, recuperar adecuadamente la información producida, recibida o retenida por cualquier organización en el desarrollo de sus actividades. La información puede hallarse en casi cualquier formato y provenir de cualquier fuente. La motivación para que una organización gestione la información empresarial surge de varios síntomas comunes: falta de información en el momento adecuado, demasiadas horas extra dedicadas a la generación de reportes e informes, definiciones de flujo del sistema deficientes que causan discrepancias disfuncionales, interfaces manuales entre varios sistemas dispares y múltiples sets de datos sin coordinación alguna. (Bustelo & Amarilla, 2001)

La gestión de la información, consiste no sólo en gestionar los flujos de información y llevar la información correcta a las personas que la necesiten, sino que, es también un marco para establecer líneas de acción y decisiones dentro de la empresa. El crecimiento exponencial del valor de la información y la administración moderna, han definido que el uso de un sistema de gestión de la información en la empresa, pase de ser una opción empresarial costosa a una necesidad estratégica vital para mantener un nivel de competitividad en el mercado.

En la mayoría de las organizaciones, la información es gestionada de manera aislada y con equipos independientes que utilizan diversas herramientas de gestión de la información para la integración de datos, y el aseguramiento de la calidad de los mismos. Sin embargo, existe una tendencia hacia EIM (gestión de la información empresarial), que es una práctica que coordina equipos e integra herramientas en forma holística, procurando mejorar los datos, tanto estructurados para que estos sean claros, coherentes y estén siempre completos.

Desde el punto de vista tecnológico, la integración de herramientas de gestión en una empresa, permite preparar la información para el próximo paso, que consiste en compartir y aprovechar la información entre las múltiples unidades de negocio de la empresa y con socios de negocio o comerciales. Una vez

que la información está lista para ser compartida como un activo de la organización, el objetivo final de la gestión de la información consistirá en alcanzar la excelencia operativa en la empresa y explotar información con herramientas de Inteligencia de Negocios.

Resumiendo todo lo descrito anteriormente, demos afirmar que para una empresa, la gestión de la información es una mejor práctica para crear, administrar, compartir y aprovechar su información de manera holística y alineada con los objetivos estratégicos del negocio. (Russon, 2009)

La estructura organizacional de una empresa debe ser capaz de administrar la información y distribuirla a través de múltiples canales, asegurando que la información indicada llegue a las personas indicadas. Para lograr esto, es fundamental la utilización de soluciones tecnológicas (infraestructura y aplicaciones) para implementar ambientes de gestión de la información que permitan aplicar las mejores prácticas de gestión.

Según AIIM (Association for Information and Image Management), la gestión de la información es una responsabilidad de toda una organización que necesita ser direccionada desde los más altos niveles de gestión hasta la línea base; por ello requiere de la adopción y adherencia de los siguientes principios:

- La información es un activo empresarial. Este principio debería ser reconocido y adoptado por toda la organización; de lo contrario cualquier soporte para la gestión de la información no será lo suficientemente fuerte.
- La información debe estar siempre disponible y debe ser compartida. Por supuesto, no toda la información estará disponible para todos, pero en principio, compartir información ayuda al uso y explotación del conocimiento en la empresa.
- La información que la empresa necesita es manejada y almacenada corporativamente. Es decir, se debe asegurar el correcto almacenamiento de la información. Si se archiva un documento el día de hoy, se espera que esté asegurado y se encuentre disponible el día de mañana.

En la mayoría de casos, las herramientas que utilizan los usuarios finales para ejecutar procesos que les ayuden a gestionar su información, son aplicaciones y/o sistemas de información empresarial. Sin embargo, para que estos últimos puedan cumplir con sus funciones, es necesario contar con una infraestructura adecuada que garantice la seguridad de la información de la empresa.

2.2.16.2. Seguridad de la Información

La información es algo vital para una organización. Si esta se ve comprometida de alguna forma, ello podría traer grandes

consecuencias, que pueden ir desde daños a la reputación de la compañía, hasta penas financieras resultante de procesos regulatorios.

La seguridad de la información es un enfoque estratégico que debe tener como base un marco sólido y holístico que abarque todos los requerimientos de Seguridad de la Información en la organización. Este marco debe construirse sobre una arquitectura que tome en cuenta todos los principios de seguridad, se adecúe a los requerimientos de la organización y se enfoque a la gestión de la información crítica del negocio. (Toal, 2011)

Cuando hablamos de seguridad de la información, no solo nos referimos al control del acceso no autorizado, sino a la protección de la información en todo sentido (Kumar, 2011). Existen tres objetivos fundamentales de la seguridad sobre la información de la empresa y los recursos de procesamiento de información. (Sun Corporation, 2008)

- Confidencialidad; término utilizado para prevenir la divulgación de la información a sistemas o individuos no autorizados.
- Integridad; para evitar que la información sea manipulada indetectablemente.
- Disponibilidad; porque, para que los sistemas de gestión de información puedan cumplir sus propósitos, la información debe estar disponible siempre que se necesite.

2.2.16.3. Confidencialidad de la Información

La confidencialidad es uno de los conceptos principales de la Seguridad de la Información y se refiere a limitar el acceso y divulgación de la información solo a usuarios autorizados.

Para comprender lo que es la confidencialidad, debemos comprender el concepto de privacidad, y reconocer que información debería protegerse, y como definir los accesos autorizados. La confidencialidad comprende la idea de que información específica no debería estar accesible para aquellos que se supone no deben verla. (Clemmer, 2010)

Diariamente, las organizaciones crean, almacenan e intercambian todo tipo de información. Esta última puede incluir detalles de operaciones del negocio, información de ventas, mercadeo, y facturación entre otras cosas. Para la mayoría de estos tipos de información, no existe una gran necesidad de mantener privacidad extrema dentro de la organización; sin embargo, si trabajamos con información personal de clientes, es extremadamente importante que esta esté protegida.

Para decidir qué tipo de información debe ser declarada como confidencial, se deben considerar varios factores. Primero es necesario definir el valor de la información y los riesgos que

existen si esta fuera expuesta; es así que podemos categorizar la información de la siguiente manera:

- Completamente privada; podría incluir cuentas de usuario y contraseñas para administración de los sistemas y también secretos contractuales.
- Privada / de mucho valor; depende del giro del negocio e involucra todo aquello que generaría grandes riesgos si fuera expuesto.
- Interna; incluye todo aquello que una organización no quiere que su competencia conozca.
- Preferencial; información que podría ser compartida con algún socio de negocio solo con fines empresariales.
- Publica; es fácil de comprender y va dirigida a los clientes externos de una organización.

Para proteger la información confidencial de una organización, en Tecnologías de la Información se utiliza los siguientes elementos:

a. Autenticación

Se considera el primer paso para la protección de la información. Es importante verificar que los usuarios que intentan acceder la información efectivamente sean quienes dicen ser. En los sistemas computacionales, como mínimo se debe solicitar un identificador de usuario y una contraseña válida antes de otorgarse el acceso requerido.

b. Autorización

Después de haber validado la identidad del usuario que requiere acceder a determinada información, es necesario verificar los roles que tiene asignados dicho usuario. Los roles agrupan a los usuarios de acuerdo a los privilegios de acceso a la información que se les otorguen. En una organización pueden existir diversos niveles de acceso a la información, cada uno de los cuales debe verse reflejado en un rol de usuario.

c. Control de Acceso

Por último, el control del acceso implica verificar lo que un usuario puede o no hacer dependiendo del rol que tenga asignado. Es importante definir si un usuario debería tener la posibilidad de leer, escribir, modificar, añadir o borrar información.

Como se puede ver, existen implicancias y preocupaciones acerca de la Confidencialidad, las cuales alcanzan cada uno de los aspectos de los negocios modernos. Los conceptos clave involucran conocer la información que se tiene, cuál es su valor, y cuáles son los riesgos a enfrentar en caso no se mantenga su confidencialidad.

2.2.16.4. Integridad de la Información

En términos de Tecnologías de la Información, integridad significa que los datos no sufren modificaciones mientras son almacenados o transmitidos. Los cambios no autorizados a los datos almacenados por un usuario se consideran como una violación a la integridad. Una vez que los datos sean almacenados, los posibles cambios a la información se aplicarán solo si existe la autorización respectiva. (Clemmer, 2010)

La integridad garantiza la exactitud de la información y los métodos asociados a esta durante el procesamiento y almacenaje. Incluso cuando los usuarios tienen necesidad de acceder a la información, no es necesario que todos ellos efectúan cambios. La encriptación de datos, así como los permisos y contraseñas de acceso se pueden utilizar para limitar el acceso solamente a los usuarios que necesiten hacer cambios.

En la actualidad, muchas de las organizaciones crean, transmiten y almacenan diariamente grandes cantidades de información. Generalmente, los usuarios asumen que los documentos que guardan se mantendrán tal como fueron guardados; sin embargo esto no es del todo cierto, pues dichos documentos pueden cambiar por accidente, por error o por un acto malintencionado.

Las fallas de integridad en la información pueden ser causadas por errores en la transmisión, daños en discos duros y/o errores en ingreso o captura de datos. Los medios físicos que contienen o transmiten información también pueden dañarse ocasionando una falla en la integridad de los datos.

La integridad puede definirse también en términos de atributos como la precisión, consistencia y fiabilidad de los contenidos, procesos y sistemas de información (Mandke & Nayar, 2007). En este sentido, la integridad de la información se convierte en una base y un pre-requisito para la utilidad y usabilidad de la información. Es un atributo específico y objetivo que se presta a sí mismo para construir estándares, métricas y oportunidades de mejora. (Madhavan, 2006)

a. Precisión

Se refiere a cuan correctos pueden permanecer los datos durante su transmisión y después de su almacenamiento. Para determinar la precisión, es importante identificar la fuente de la cual proviene la información y utilizar diversas técnicas de comparación con la información actual. La presencia de errores en cualquier segmento de datos, denota automáticamente la ausencia de precisión en la información.

b. Consistencia

La consistencia se mide con respecto de una serie de restricciones. Se dice que los datos o la información son consistentes siempre y cuando satisfagan todas las restricciones del modelo de información implementado en una organización.

Las restricciones pueden aplicar a un mismo atributo en diferentes entidades, o a diferentes atributos en una misma entidad. Si se tiene el número total de restricciones especificas en un modelo y el número de restricciones que no han sido satisfechas en el mismo, se puede cuantificar fácilmente la consistencia de la información.

c. Fiabilidad

La fiabilidad puede ser considerada como la certeza de que la información obtenida mientras se ejecuta el mismo proceso con los mismos datos de entrada. Es decir, no importa cuántas veces ejecute el mismo proceso, siempre se deberán obtener los mismos resultados.

2.2.16.5. Disponibilidad de la Información

La disponibilidad de la información se define como el acceso confiable y a tiempo a los datos y servicios de información por los usuarios autorizados. En un concepto más amplio, podemos decir que la disponibilidad se refiere a que la información sea accesible

en la forma en que se necesita, cuando se necesita y donde se necesita. El objetivo de la disponibilidad es permitir el acceso autorizado a la información o los recursos de una organización. (Andrew & Deepak, 2006)

Tradicionalmente, la disponibilidad en medida por la cantidad de tiempo que un recurso está trabajando o no (uptime y downtime). Una vez que la información ha sido recopilada dentro de una organización, debe ser almacenada de manera segura y estar disponible para los usuarios cuando la necesiten; no importa cuán cuidadosamente archivados o bien organizados estén los datos dentro de una organización, si la gente que lo necesita no pueden acceder a ellos en un momento dado.

2.2.16.6. Componentes de la Disponibilidad de la Información

Está razonablemente bien establecido que la disponibilidad tiene tres componentes: Confiabilidad, Accesibilidad y Tiempo de Acceso.

La confiabilidad es la probabilidad de que un sistema funcione adecuadamente, según su propósito, y por el periodo de tiempo establecido por las condiciones operativas en que se encuentre.

En general, los usuarios no querrán depender de un sistema no confiable para ejecutar consistentemente sus solicitudes.

Con respecto a la accesibilidad, podemos definirla como el grado en el cual un sistema es utilizable por tantos usuarios como sea posible sin sufrir modificaciones. Existen bastante políticas de control del acceso a la información, ya sea por equipos o por roles de usuarios, que se pueden utilizar para asegurarnos que solo las personas autorizadas puedan ver y utilizar la información de la organización.

El tiempo de acceso es la capacidad de respuesta de un sistema o recursos a una solicitud de usuario.

2.2.16.7. Factores que determinan la Disponibilidad de la Información

Existen diversos factores que influencian uno o más de los atributos de la disponibilidad, y por ende contribuyen a la disponibilidad general de un recurso de información. A continuación, se describen cada de estos factores y su impacto en una organización.

a. Políticas de Seguridad

Una política de seguridad es una actividad que establece el marco de procesamiento de la información y el uso de dispositivos de TI dentro de una empresa. Una política es un

plan documentado de alto nivel para la seguridad de la información y los equipos de una organización. Establece una línea base para la toma de decisiones acerca de los mecanismos de defensa a utilizar y la forma en la que se deberán configurar determinados servicios, así como los procedimientos a seguir por parte de los usuarios y administradores de sistema.

La mayoría de las políticas de seguridad no están dirigidas hacia el aseguramiento de la disponibilidad de la información. En realidad, los autores de políticas generalmente se concentran en lo que concierne a confidencialidad. Una política de seguridad debería estar dirigida a las personas que utilizan un sistema y las expectativas de los usuarios de la empresa.

Se pueden definir mecanismos de control de acceso y también establecer los privilegios de cada uno de los usuarios. Una política de seguridad impacta en la confidencialidad de un sistema, ya que establece los umbrales dentro de los que operará dicho sistema.

b. Monitoreo de Sistemas y Controles Operacionales

Mediante la implementación de controles operacionales dentro de un sistema, los profesionales en seguridad pueden definir los límites para proteger la información de una organización. Los

controles operacionales son aquellas reglas y guías necesarias para gestionar las actividades diarias con los recursos de información de la empresa. Estos controles son creados para implementar políticas de seguridad, y así proveer de mecanismos que refuercen dichas políticas.

Los sistemas de monitoreo permiten a los usuarios clave en una organización, medir como están operando los recursos informáticos. El monitoreo en tiempo real puede ser una herramienta útil para identificar actividades no autorizadas y proteger el sistema.

Los controles operacionales y los sistemas de monitoreo pueden trabajar juntos para reforzar las políticas de seguridad y proveer a los profesionales de la capacidad de defender un sistema al nivel deseado.

c. Evaluación de la Efectividad de los Sistemas y Auditoría

La auditoría de recursos de Tecnologías de la Información es un proceso de recolección y evaluación de evidencia para determinar si un sistema salvaguarda los activos, mantiene la integridad de los datos, permite alcanzar efectivamente los objetivos de la organización, y utiliza los recursos de manera eficiente. La auditoría permite verificar que los controles operacionales de los sistemas estén exitosamente

implementados, y analizar el comportamiento de los sistemas a fin de detectar malos usos o abusos dentro de dichos sistemas.

La auditoría se diferencia del monitoreo porque los auditores analizan datos históricos mientras que los monitores activan alarmas basadas en actividades en tiempo real.

La evaluación de la efectividad de un sistema es un tipo específico de auditoria que no solo analiza los reportes y registros, sino que toma una vista general del sistema, la organización y su personal para determinar cuan bien se adapta dicho sistema a las necesidades de la organización. Esta evaluación podría mostrar tendencias de comportamientos inapropiados o no autorizados sobre el sistema que no hayan sido percibidos por el monitoreo en tiempo real.

d. Seguridad Física

La seguridad física es un pre-requisito crítico de la disponibilidad de la información. Si una organización no provee de seguridad física a sus sistemas, entonces personal no autorizado podría tener acceso a los sistemas de la organización. El punto de vista tradicional se enfoca en asegurar los edificios y equipos contra robos, vandalismo, desastres naturales, catástrofes y daños accidentales. Si bien es cierto que la información no está directamente protegida a través de la seguridad física, esta

información reside en equipos que expertos en seguridad se encargan de proteger.

Asegurar los equipos y los medios de comunicación en una empresa es un paso importante para asegurar la disponibilidad de los sistemas. Si un equipo que contiene información que un usuario está solicitando no está disponible por fallas en la provisión de energía o por cables desconectados, el impacto hacia el usuario o hacia el proceso que ejecuta la solicitud será igual a no tener acceso autorizado.

e. Respaldos

Los respaldos generan copias de los datos, aplicaciones y configuraciones del sistema operativo almacenadas en los computadores. Creando copias de respaldo, una empresa puede minimizar el tiempo de inactividad que se experimenta después de un evento que puede dañar o borrar la información almacenada. Adicionalmente, las copias de respaldo se hacen necesarias debido a que la información almacenada dentro de la empresa es un activo muy valioso. Se requiere tener copias de respaldo de los sistemas y de la información de los usuarios para proveer de la máxima capacidad de recuperación en la empresa.

La seguridad física de los medios de respaldo es también un tema crucial, pues se requiere que estas tengan el mismo nivel de seguridad que otras aplicaciones críticas; ya que, para recuperar un sistema sin copias de respaldo, prácticamente se tendría que realizar una instalación desde cero.

f. Continuidad del Negocio

La continuidad del negocio es un componente clave de cualquier plan empresarial para mantener las operaciones ante un evento catastrófico como un desastre natural o un ataque a la red. Es necesario poner bastante énfasis en la creación de un plan de contingencia, ya que, por lo general, la mayoría de los planes no brindan los resultados esperados después de ser probados.

La continuidad del negocio impacta en el tiempo de acceso y accesibilidad de un sistema, ya que establece un proceso conocido y sistemático para restaurar operaciones en el menos tiempo posible. Sin un plan probado de continuidad, no se tiene la certeza de que las operaciones serán restauradas a su estado previo.

2.3. Glosario de términos básicos

- **Modelo**

  Se denomina modelo a una representación abstracta, conceptual, gráfica, visual, física, matemática de fenómenos, sistemas o procesos a fin de analizar, describir, explicar, simular; en general

explorar, controlar y predecir esos fenómenos o procesos. Un modelo permite determinar un output o resultado final a partir de un input o datos de entrada, permite visualizar el flujo de la información de manera conceptual. Esta vista general es el mecanismo utilizado para que un proyecto tenga un enfoque sistémico. (Kalloniatis, 2012)

- **Respaldo**

  Respaldo es la obtención de una copia de los datos en otro medio magnético de tal modo que a partir de dicha copia es posible restaurar el sistema al momento de haber realizado el respaldo. Por lo tanto, los respaldos deben hacerse con regularidad, con la frecuencia preestablecida y de la manera indicada, a efectos de hacerlos correctamente. Es fundamental hacer bien los respaldos, de nada sirven respaldos mal hechos (por ejemplo, incompletos) en realidad, es peor disponer de respaldos no confiables que carecer totalmente de ellos.

- **Estándar**

  En términos tecnológicos, conjunto de especificaciones técnicas que sirven como norma, patrón o referencia en el desarrollo de hardware o de software. Los estándares de tecnologías son elaborados por conceso de las partes interesadas: fabricantes, usuarios, consumidores, centros de investigación, laboratorios, asociaciones, agentes sociales, etc.

- **Gestión**

  Es el conjunto de trámites o diligencias que se llevan a cabo para resolver un asunto, administración por otra parte, consiste en la planificación, organización, dirección y control de los recursos (humanos, financieros, materiales tecnológicos, información, etc.) de la organización con el fin de obtener el máximo beneficio posible; este beneficio puede ser económico o social, dependiendo esto de los fines perseguidos por la organización.

- **Información**

  La información es un conjunto de datos procesados que tiene un significado y que contribuye un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje, de manera que se reduce la incertidumbre y que aumenta el conocimiento de algo. La información es un mensaje con significado dentro de un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones. (Floridi, 2010)

- **Tecnologías de la Información (TI)**

  Uso de la tecnología para el almacenamiento, comunicación o procesado de información. La tecnología incluye típicamente

ordenadores, telecomunicaciones, Aplicaciones y otro software. La información puede incluir datos de Negocio, voz, imágenes, video, etc. La Tecnología de la Información (TI) es a menudo usada para soportar Los Procesos de Negocio a través de Servicios de TI.

- **Disponibilidad**

  El grado en el cual un sistema, subsistema, equipo o información se encuentra en un estado operativo y comprometido desde el inicio de una tarea, y continúa en el mismo estado de forma ininterrumpida.

  La disponibilidad de la información se refiere a la posibilidad de que la infraestructura funcione de acuerdo a las expectativas del negocio durante el tiempo de operación especificado. La disponibilidad de la información asegura que las personas, empleados, clientes, proveedores y socios, puedan acceder a la información cuando la necesiten. (Sumasundaram & Shrivastava, 2009)

- **Redundancia**

  La redundancia en el contexto de los Centros de Datos hace referencia al suministro de recursos por más de una fuente, de manera que, si uno de los suministros falla, la otra fuente de recursos comienza a suministrar para garantizar la disponibilidad de los sistemas.

- **SAN (Storage Area Network)**

  Una red para almacenamiento, es un conjunto de dispositivos de almacenamiento de datos. Un grupo de servidores y dispositivos de almacenamiento que comparten recursos comunes y los usuarios que define el “área de almacenamiento”. En ocasiones, el término puede ser utilizado para una amplia zona o red de área metropolitana que se utiliza para la redundancia de datos central y la protección contra desastres. SAN suelen tener muy baja latencia, alto rendimiento y ofrece entrega asegurada del bloqueo de E / S. La puesta en práctica más común es la SAN de canal de fibra, sin embargo, esta no es la única alternativa. Recientemente se han hecho esfuerzos, tales como iSCI para implementar redes de almacenamiento con Ethernet e IP (Internet Protocol) de la infraestructura.

2.4. Hipótesis de la investigación

El modelo de un CPD de Respaldo con replicación en tiempo real mejora el rendimiento de la gestión de la información en la empresa Electro Puno S.A.A.

2.5. Operacionalización de variables

Variables	Dimensiones	Indicadores	Escala
Variable Independiente: Modelo de CPD de respaldo	Funcionalidad	Adecuación.	Si / No
		Exactitud.	Exacta / No exacta
		Interoperabilidad.	Si / No
	Eficiencia	Utilización la norma TIA 942	Si / No
	Compatibilidad	Coexistencia.	Si / No
		Interoperabilidad.	Si / No
	Usabilidad	Facilidad de aprendizaje.	Si / No
		Operabilidad.	Continuo / no continuo
	Fiabilidad	Tolerante a fallas.	Si / No
		Capacidad de recuperación.	Si / No
	Seguridad	Confidencialidad.	Si / No.
		Integridad.	Si / No
		Autenticidad.	Si / No
		Riesgo de daño económico.	Si / No
	Mantenibilidad	Modularidad.	Si
		Reusabilidad.	No
	Efectividad	Precisión de uso	Preciso / No preciso
		Tiempo de operación.	Porcentaje anual
	Productividad	Cantidad de información usada y	Gigabytes

		almacenada.	
	Satisfacción	Cumplimiento de propósito.	Si / No
		Confianza.	Si / No
	Contexto de uso.	Flexibilidad.	Si / No
Variable Dependiente: Gestión de la Información	Productividad	Nivel de recursos utilizados.	Mucho / Poco
	Eficiencia	Tiempo de disponibilidad	Tiempo
		Tiempo para recuperarse de un incidente.	Tiempo.
	Efectividad	Precisión de la información.	Precisa / No precisa

Cuadro 4: Operacionalización de Variables
Elaboración: Propia.

CAPÍTULO III

DISEÑO METODOLOGICO DE LA INVESTIGACION

3.1. Tipo y Diseño de investigación

3.1.1. Tipo de investigación

El tipo de Investigación es Aplicada, utilizando el método analítico comparativo ya que este método nos permite analizar la situación actual de la Gestión de la Información en la empresa Electro Puno S.A.A., y comparar los resultados proyectados para la implementación del modelo de CPD de Respaldo propuesto y además que el tipo de investigación propone transformar el conocimiento puro en conocimiento útil y que busca obtener un conocimiento con la aplicación a un problema determinado en la realidad.

3.1.2. Diseño de investigación

El diseño del presente proyecto de investigación es No Experimental – longitudinal de tendencia, ya que no se manipulo ninguna variable al momento de recolectar la información, lo que se hizo fue observar los fenómenos tal como se dan en su contexto natural para después analizarlos (Hernandez, 2014).

3.2. Población y muestra de investigación

Población:

La población o en términos más precisos, población objetivo, es un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Esta

queda delimitada por el problema y el objeto de estudio (Arias, 2996m p.81).

La pregunta a formularse a tales efectos, tal como lo indica Hernández Sampieri y otros es: “¿Sobre qué o quienes se recolectarán los datos?, y está relacionada con los sucesos, objetos, sujetos o comunidades de estudio (las unidades de análisis), lo cual depende del planteamiento de la investigación”.

En el presente caso, relacionado con diseñar un modelo de CPD de respaldo para mejorar la gestión de la información en la empresa Electro Puno S.A.A. se considera que la población está constituida por todos los trabajadores que conforman la empresa Electro Puno S.A.A.

Muestra:

La selección de muestra es de tipo no probabilístico donde se utilizó el método de **muestreo por conveniencia**, para el presente proyecto de investigación está considerada por todos los trabajadores que laboran en las oficinas de Puno (oficina principal Jr. Mariano H. Cornejo N° 160, Oficina de Bellavista Av. Floral S/N y la oficina de Av. El Sol 826). Ya que en esas oficinas es donde se encuentra el CPD principal y donde se genera mayor carga de datos y ancho de banda.

3.3. Ubicación y descripción de la población

El ámbito de estudio está fijado en la totalidad de las Gerencias, Áreas y/u Oficinas pertenecientes a la empresa Electro Puno S.A.A., por ser el caso de estudio, localizados en:

- Oficina principal, ubicado en el Jr. Mariano H. Cornejo N° 160, Oficinas de Av. El sol N° 826.
- Oficinas de Juliaca ubicado en el Jr. Manuel Prado N° 416.
- Oficinas de Bellavista –Tablero Av. Floral S/N.
- Servicios Eléctricos en Provincias.

  Servicios Eléctricos frontera SUR

  - ✓ SE Desaguadero
  - ✓ SE Yunguyo
  - ✓ SE Juli
  - ✓ SE Ilave

  Servicios Eléctricos frontera NORTE

  - ✓ SE Ayaviri
  - ✓ SE Azangaro
  - ✓ SE Huancane
  - ✓ SE Moho
  - ✓ SE Putina

3.4. Técnicas e instrumentos para recolectar información

TÉCNICAS	INSTRUMENTOS
Norma ANSI TIA 942	Protocolos a seguir para instalar un adecuado CPD.
TIER	Clasificación de acuerdo a las necesidades de la empresa.
Edraw Max v7.4	Programa para graficar el modelo de CPD.
Observación	Diario o Libreta de Campo, donde se evidenciarán los sucesos ocurridos durante la investigación.
Análisis	Hojas de cálculo Excel y el programa SPSS.

Cuadro 5: Técnicas e Instrumentos
Fuente: Elaboración Propia

3.5. Técnicas para el procesamiento y análisis de datos

Los datos obtenidos fueron procesados y analizados según la norma ANSI/TIA 942 y la clasificación TIER, también se utilizaron instrumentos electrónicos y el análisis estadístico descriptivo.

3.6. Plan de tratamiento de los datos

Los datos se procesaron en forma cualitativa mediante gráficos, cuadros, tablas, hojas de cálculo y en forma estadística, se utilizó la “prueba t”.

En la comparación entre los indicadores de la gestión actual de la información y los proyectados mediante el modelo propuesto, se utilizará la siguiente tabla:

Indicadores	Gestión de la información actual	Modelo propuesto	Diferencia
Adecuación.			
Exactitud.			
Interoperabilidad.			
Utilización de la norma TIA 942			
Coexistencia.			
Interoperabilidad.			
Facilidad de aprendizaje.			
Operabilidad.			
Tolerante a fallas.			
Capacidad de recuperación.			
Confidencialidad.			
Integridad.			
Autenticidad.			
Riesgo de daño económico.			
Modularidad.			
Reusabilidad.			
Precisión de uso			
Tiempo de operación.			
Cantidad de información usada y almacenada.			
Cumplimiento de propósito.			
Confianza.			

Flexibilidad.			
Nivel de recursos utilizados.			
Tiempo para recuperarse de un incidente.			
Precisión de la información.			

Cuadro 6: Comparación de indicadores
Elaboración: Propia

CAPÍTULO IV

ANALISIS E INTERPRETACION DE RESULTADOS DE LA INVESTIGACION

4.1. Análisis de la situación actual de la gestión de la información

La competitividad es, hoy en día, el factor más importante para el desarrollo de una empresa. En ese sentido contar con información oportuna y con valor de uso es de vital importancia para cualquier empresa en general, toda vez que genera diferencia entre ellas y por ende la competitividad.

Las grandes empresas en este caso de nuestra región como son las entidades financieras (Banco de la Nación, BBVA Continental, Interbank, BCP), Supermercados (Plaza Vea) y Electro Puno S.A.A. disponen de sistemas de información a través de los llamados Sistemas de Información Gerencial, Centros de Datos corporativos, redes Intranet, Internet y otros sistemas de uso privado y público.

El análisis de la situación actual de la gestión de la información se realizó recolectando datos, observando el comportamiento del día a día de la empresa, los trabajadores y también de los equipos que conforman la red de datos y los servidores, revisando y analizando información generada por el personal de la oficina de División de Tecnologías de la Información y Comunicaciones. A fin de conocer la situación actual de la gestión de la información en la empresa Electro Puno S.A.A. se hizo un análisis de la información en los periodos de mitad del año 2014 hasta

principios del año 2017, este análisis, cuya información se obtuvo a través de recolección de datos y observación dentro de la empresa y la cual permitió conocer el estado actual de la red y la información, así como las bondades y carencias en lo que a tecnologías de la información se refiere.

Informes

- **Informe N° 112-2014-ELPU/GSI**

  Asunto : Informe Solicitado

  Fecha : 11 de setiembre de 2014

  Ausencia del servicio de red de datos hacia la cuidad de Puno de 19 horas entre las ciudades de Puno y Juliaca por una ruptura de la fibra óptica 29-08-2014 a las 11:00 horas y la solución definitiva fue realizada el día 30-08-2014 a las 07:00 horas.

- **Informe N° 097-2014-ELPU/GSI**

  Asunto : Mantenimiento correctivo media converter fibra óptica Puno-Juliaca

  Fecha : 30 de julio de 2014

  Por fallas anteriores que impedían el buen funcionamiento de la red entre las diferentes oficinas la cual presentaba cortes de los servicios y malestar en los trabajadores. Se realizó el cambio de los media converter para prevenir futuras fallas.

- **Informe N° 028-2014-ELPU/GSI**

  Asunto : Incidente del día domingo 09-03-2014

  Fecha : 11 de marzo de 2014

  El día domingo 09-03-2014 a las 18:00 horas se recibió el requerimiento de la GA porque la red no estaba presente y no tenían acceso al sistema. Este incidente de corte de energía eléctrica ha causado el deterioro de 6 discos duros de 450 gb y 2 de 650 gb. El problema se solucionó el día 10-03-2014 a las 14:00 horas.

- **Informe 208-2015-ELPU/GSI**

  Asunto : Estado situacional CPD Puno

  Fecha : 28 de diciembre de 2015

  El día 21-12-2015 se presentaron precipitaciones en forma de granizo en la ciudad de Puno a las 18:00 horas se filtró agua y malogro un servidor blade. El día 22-12-2015 sucedió lo mismo.

- **Informe N° 086-2015-ELPU/GSI**

  Asunto : Informe incidente del día 23-05-2015 ausencia de energía en el CPD de Juliaca

  Fecha : 28 de mayo de 2015

  El día 23-05-2015 a las 19:30 horas la red de datos estaba fuera de servicio, no se podía conectar a la red y tampoco se tenía correos. El servicio se restableció el día 25-05-2015 a las 10:20 horas.

Eventos suscitados:

El día 09 de febrero de 2015, se suscitó un inconveniente con la red de la empresa la cual impedía que los equipos finales, computadoras, laptops, impresoras y Access point pudieran conectar con el servidor de dominio de la empresa. Ese día una red externa de la empresa (Red Clínica Americana) ubicada a un costado de las oficinas de la empresa Electro Puno S.A.A. Juliaca se infiltro en la red impidiendo que los equipos pudieran conectarse al dominio electropuno.local, y haciendo que los equipos finales de la empresa Electro Puno se conecten a la red de la clínica y no a la de la empresa generando malestar en los trabajadores y usuarios/clientes, el problema se logró solucionar luego de casi 3 días de arduo trabajo por parte de la división TIC. El principal problema fue que la señal inalámbrica de la clínica llegaba hasta las instalaciones de Electro Puno y haciendo que cualquier equipo con conexión inalámbrica se conecte a la red y así fue como la red de la clínica se filtró dentro de los servidores de dominio e impidiendo el normal funcionamiento de estos.

Igualmente, el día 17 de enero de 2017 por la mala configuración de un servidor se asignó la dirección IP del Router que brinda el servicio de Internet a la empresa des configurándolo y haciendo que se pierda el acceso al internet de la empresa, el problema se pudo solucionar después de casi 1 día de arduo trabajo.

También se presentaron incidentes menores pero que de igual forma perjudicaron el normal funcionamiento de la red y el acceso a la información de los trabajadores, uno de ellos se presentó con frecuencia en las oficinas de Av. Sol 826 donde se encuentran las Gerencias de Operaciones, Planeamiento y Técnica, el Switch del 5to piso que está conectado con uno del tercer piso todos los días a partir de las 8:00 horas aproximadamente por un periodo de 30 – 45 min, el puerto de conexión se apagaba y la solución en ese momento era reiniciar el Switch del 5to piso, la solución final fue cambiar de Switch por uno de mayor capacidad.

Estos informes y eventos demuestran que la red de la empresa Electro Puno no está completamente segura y si el CPD principal de la empresa llegara a fallar nuevamente toda la empresa se vería perjudicada esto a causa de que toda la red está centralizada en las oficinas de Puno Jr. Mariano H. Cornejo N° 160. Sí sumamos el total de horas que estuvo fuera de servicio la red de la empresa se tiene un total de casi 200 horas u 8 días aproximadamente en los que la empresa estuvo sin conexión y fuera de servicio.

Metas del diseño de CPD de respaldo:

- Minimizar el tiempo de fallas en la conexión de la red con los servicios.
- Maximizar la disponibilidad de la información.

- Mejorar la calidad de la gestión de la información.
- Gestionar el uso eficiente de las TIC.

Metas técnicas:

- Diseñar el CPD de respaldo utilizando la norma ANSI TIA 942.
- Clasificar el CPD de respaldo diseñado como un TIER 3, un CPD tolerante a fallos.
- Proveer mayor seguridad de la información y sus sistemas para satisfacer las necesidades de acceso de los trabajadores y usuarios finales a la red e información de la empresa.
- Proveer seguridad de la información de cada trabajador de la empresa almacenada en los servidores de archivos.
- Lograr una conexión redundante entre los 2 CPD, principal y secundario o CPD de respaldo.
- Crear copias de seguridad en tiempo real para que no se pierda ningún dato y tampoco información.

Ámbito

El presente proyecto de investigación comprende el análisis y entendimiento de la gestión de la información en la empresa, la cual comprende las siguientes oficinas.

- Gerencia General
- Oficina de Imagen Institucional
- Oficina de Asesoría Legal

- Oficina de Seguridad y medio ambiente
- Gerencia de Planeamiento
- Oficina de Norma Técnica
- Oficina de División TIC
- Gerencia de Administración
- Oficina de Logística
- Oficina de Contabilidad
- Oficina de Patrimonio
- Oficina de Obligaciones y Tesorería
- Oficina de Recursos Humanos
- Gerencia de Operaciones
- Gerencia Técnica
- Gerencia Comercial
- Oficina de facturación
- Oficina de Plataforma y atención al cliente
- Oficina de Reclamos
- Oficina de Perdidas
- Oficina de Tarifas y Contratos
- Oficina de FISE.

4.1.1. Sistemas y aplicaciones que utilizan los trabajadores de la empresa

Nombre de sistema	Tipo de aplicación	Critica
Sistema comercial SIELSE	File Server	Si
Sistema SAP	ERP	Si
Sistema de distribución	File Server	Si
Tramite documentario	Web	Si
Sistema de Asistencia	File Server	Si
Sistema de tickets	File Server	No
Intranet	Web	No
Service Desk	Web	Si
Sistema de cámaras de vigilancia	File Server	Si
Sistema de Proyectos	Web	Si
Sistema Geográfico ARGIS	File Server	Si
Sistema CITRIX	Web	Si
Correo Corporativo	File Server / Web	Si

Cuadro 7: Sistemas y aplicaciones
Fuente: Div. TIC Electro Puno
Elaboración: Propia.

4.2. Diseño del CPD de respaldo con replicación en tiempo real

4.2.1. Estándar para el Modelo

El modelo usa como referencia la topología de un CPD especificado en el estándar ANSI TIA 942, que ha sido adecuado para ocupar el espacio total de un CPD completo al que en este caso viene a ser el CPD de respaldo o secundario.

4.2.2. Espacio Físico

El CPD de respaldo o CPD secundario estaría ubicado en las oficinas de Juliaca Jr. Manuel Prado N° 416 ya que este cuenta con el espacio suficiente e ideal para instalar un CPD. A continuación, se muestra el plano donde estaría ubicado el CPD de respaldo:

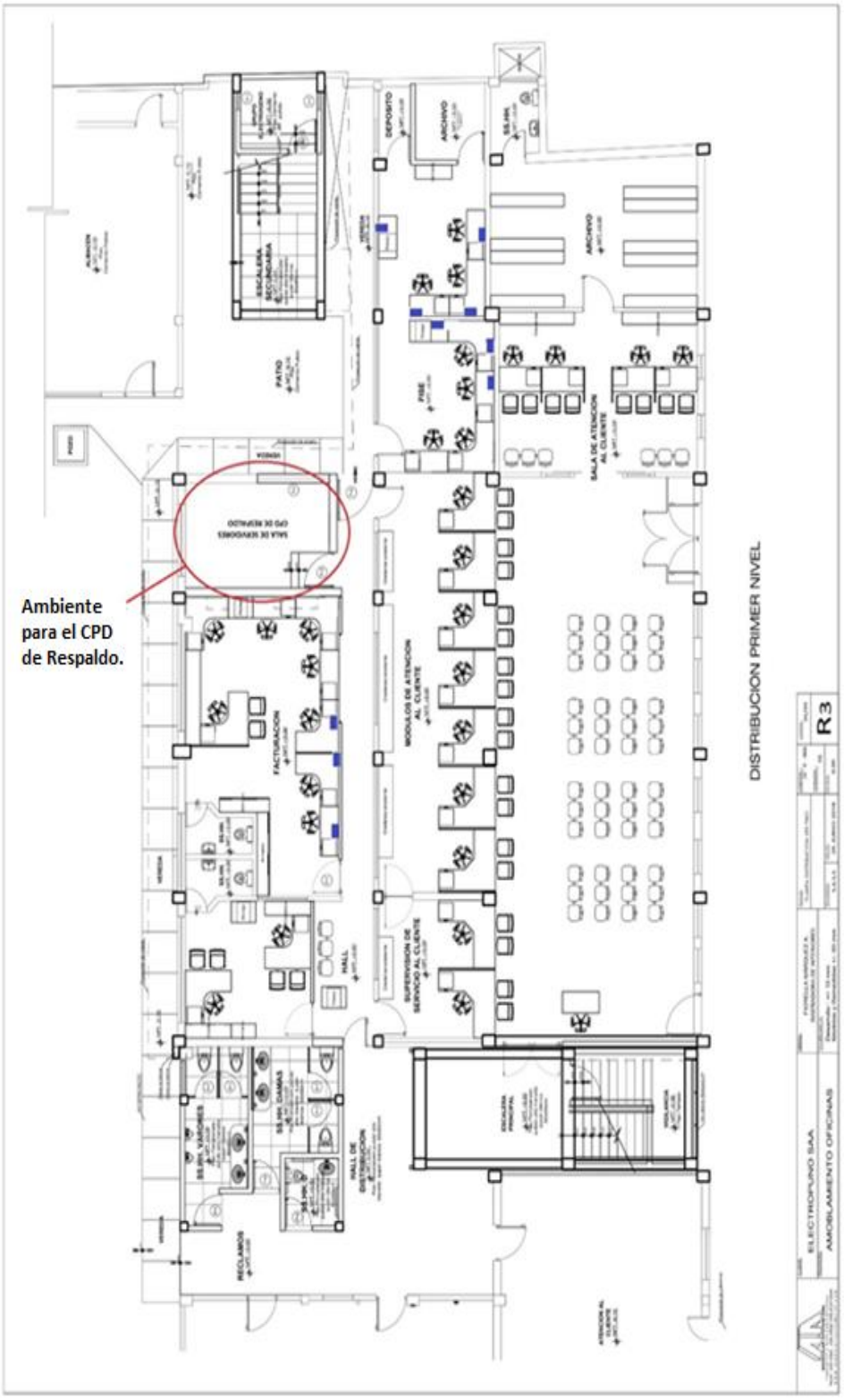


Figura 3: Ambiente para el CPD de respaldo – Ofic. de Electro Puno Juliaca.
Fuente: Div. TIC Electro Puno.

4.2.3. Piso Elevado

El piso elevado ya es una norma que todas las empresas entidades deben cumplir al momento de instalar su CPD y al instalar el piso elevado del CPD se gana mucho espacio para poder realizar la instalación del cableado eléctrico, el cableado estructura, el aire acondicionado y más a continuación mostramos las características que tendrá el piso elevado para el presente modelo de diseño:

- Es reutilizable.
- No se requiere nivelar ni pulir el firme.
- Se pueden realizar cambios aun durante la ejecución de la obra.
- Se evitan obras de albañilería como ranurados de muro para instalaciones eléctricas.
- Las remodelaciones son de bajo costo.
- El tiempo de instalación es muy corto.
- No se requiere esperas en secado aun con personal trabajando.
- Los contactos eléctricos se colocan bajo el Piso Elevado con mangueras flexibles y removibles evitando colocarlas en la pared de forma permanente.

Y también debe cumplir con las siguientes características:

- Resistencia Eléctrica. - No menos de 5 x 105 ohms y no más de 2 x 1010 ohms (norma NFPA99).
- Propiedades Térmicas. - Excelente comportamiento cuando se usa como "cámara plena" para aire acondicionado.

- Propiedades Acústicas. - Amortigua los ruidos del lugar de trabajo, pisadas, ruido exterior, etc.
- Empaques: Conductivos, plastificados y grafitados
- Travesaños: Lámina galvanizada calibre 20 de 56.5 cm de largo.
- Pedestal de aluminio: Diámetro de la base de 11.5 cm. soportando una carga uniformemente distribuida de 1780 Kg. Rangos de altura de 20 cm. a 90 cm. con ajustes de +/-3 cm.

Figura 4: Piso Elevado CPD de respaldo Juliaca.
Fuente: CPD Juliaca

4.2.4. Sistema Eléctrico

En el caso de la energía eléctrica, la empresa siendo una entidad que distribuye energía eléctrica no tendrá ningún inconveniente en instalar el sistema de energía.

Para la instalación se suministrará el servicio de energía con un sistema trifásico a 13.800 voltios, porque a la demanda trifásica de nuestro proyecto es más de 30 KVA y menor a 1.000 KVA.

Se deberá instalar un transformador trifásico de 75 KVA, esta conexión nos brindará 123-240 VAC. Ubicación de tablero de bypass, UPS's y paneles de distribución deberán ir en un área diferente al CPD y estará completamente en otro proyecto y toda la instalación deberá ir en el plenum del piso elevado con tuberías y canalizaciones EMT.

A continuación, detallamos los parámetros eléctricos para la construcción de las acometidas de alimentación de tablero de Bypass, la entrada y la salida de los UPS's y tablero de Bypass, la alimentación del panel de distribución desde el tablero de Bypass.

- Se deberá construir una acometida para alimentar el tablero de Bypass de 300 KVA.
- La acometida se realizará para capacidad de 300 KVA con un conductor #8 AWG.
- La acometida conectara la UPS entrada y salida con el tablero Bypass.
- Se deberá construir la acometida de entrada y salida entre el UPS de 300 KVA y el tablero Bypass.
- La acometida deberá ser con un conductor #8 AWG súper flexible para las fases, neutro y línea de TIERra.
- La acometida será recubierta por canaletas decorativas con sus respectivos accesorios.

Se deberá instalar un tablero Bypass de 300 KVA, confirmado por un sistema de barras correctamente dimensionadas y tres breakers bifásicos de las siguientes características:

- El primer breaker de 200A, alimentara el tablero de distribución general.
- El segundo breaker de 200A, será utilizado como Bypass externo y por seguridad debe contener una cerradura o candado, para que solo pueda ser accionado por personal calificado y autorizado.

4.2.5. Sistema de enfriamiento de precisión

Así como el CPD requiere equipos que respalden, protejan y administren energía también requiere soluciones de enfriamiento los cuales mantendrán los servidores, Switches, equipos de telecomunicaciones a una temperatura estable. El CPD de respaldo para la empresa al tener varios equipos como servidores, storage, switches estos generan bastante calor la cual tiene que ser disipada para mantener el ambiente con una temperatura estable y que los equipos funcionen de manera correcta, en la figura 5 se observa como dentro del piso elevado se encuentra instalado el equipo de enfriamiento la cual sale del piso, enfriando todo el CPD.

Figura 5: Sistema de enfriamiento de precisión HiRef
Fuente: Estándar TIA 942
Elaboración: Propia

4.2.6. Especificaciones Técnicas.

El cuadro 8 muestra una referencia de las especificaciones técnicas de los equipos a instalar en el CPD implementado en el modelo.

Equipos	Imagen referencial	Especificación
Switch L3		Montaje en rack 1 RU. Fast ethernet, Gigabit .ethernet, Ten gigabit. IPSerc, L3TPv3.
Switch de distribución		Montaje en rack 1 RU. Administrable terminal/web. 48 puertos RJ45, 2 puertos fibra óptica. Velocidad 100/1000/10000.

Firewall		Montaje en rack 1RU. Filtrado de paquete a nivel de navegación. Https, http, DNS, Socks, POP3, Ident, SMTP. NAT (Network Address Traslation). Protección DoS. Seguridad 2P2 y web filtering. Antivirus, Antimalware. Internal Storage 16Gb. SSL VPN – throughput. IPSec VPN – throughput.
Storage		Montaje en rack 4 RU. 8 bahías para disco duro de 3.5" de 650 Gb. Fuente redundante. Storage based replication Full RAID lvl support Soporte para windows y linux
Servidor		Montaje en rack 4 RU HP Proliant ml350 G6 64Gb de Ram
UPS		Montaje en rack 5RU Potencia de salida 5000 VA, 10000W Autonomía Max (173 min - 1000 W) Autonomía Min (30 min - 1000 W) Tensión de salida nominal 220 V Tiempo de recarga 16 horas Entrada de voltaje 220 V Visualizador de estatus LED

Racks		Altura 180 cm Frente 72 cm Profundidad 100 cm

Cuadro 8: Especificaciones técnicas
Elaboración: Propia.

4.2.7. Sistema para la extinción de fuego

Indiscutiblemente estamos en la edad de las telecomunicaciones. En un mundo cada vez más digital, la industria de CPD está en plena ebullición. Hosting, big data, la nube, son palabras que se van instalando en nuestro día a día. El avance exponencial de la tecnología IT y las redes de datos está haciendo que cada vez más compañías externalicen la localización de sus datas centers, e incluso contraten el CPD como un servicio más -en el reciente evento CPD Dynamics en Madrid se hablaba de todo como un servicio. Esto lleva a la construcción de grandes CPD en los que la disponibilidad es un factor crítico. El desempeño de un CPD se puede clasificar de diversas maneras, siendo la más reconocida la del Uptime Institute utilizando la escala TIER 1, 2, 3 y 4 donde a mayor TIER mayor disponibilidad. El desarrollo de la tecnología también está permitiendo tener cada vez más densidad de potencia por metro cuadrado con lo que el riesgo también se está incrementando, jugando un papel fundamental los sistemas de protección contra incendios.

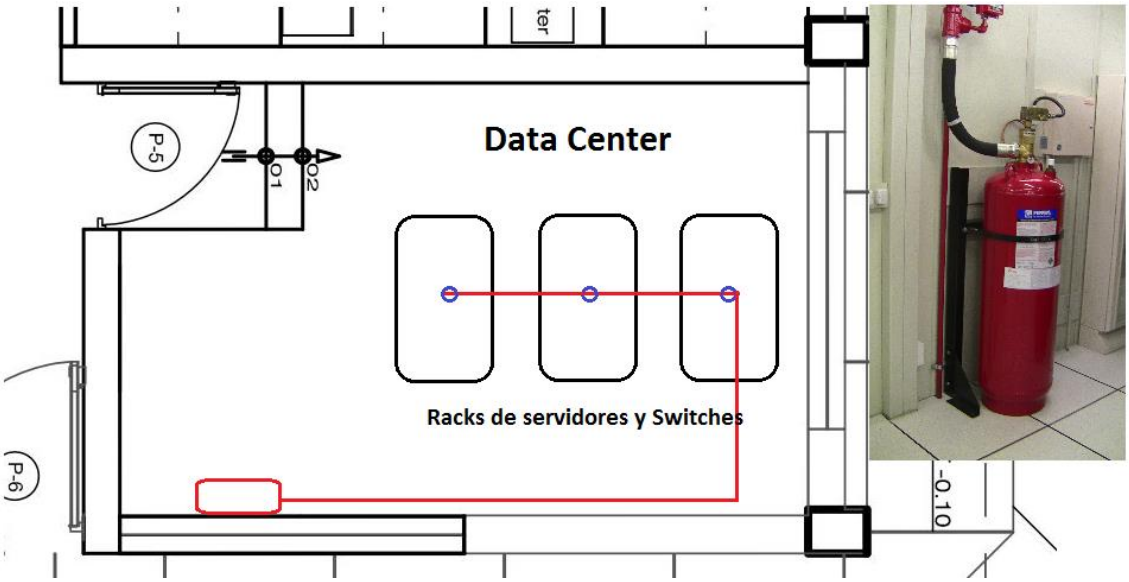


Figura 6: Sistema contra incendios para un CPD
Fuente: Estándar TIA 942
Elaboración: Propia.

4.2.8. Replicación de la información en tiempo real.

Para realizar la replicación de seguridad en tiempo real se utilizará el CPD de respaldo como un CPD espejo, primeramente, tenemos que analizar cuanta data se genera diariamente clasificados entre los diferentes sistemas que utiliza la empresa.

- Sistema Comercial SIELSE V2
- Sistema ERP SAP
- Sistema de Distribución
- Correo corporativo
- Service Desk
- File Server
- Microsoft Office

Para calcular cada uno de ellos se hizo un análisis en un periodo que abarco todo el mes de diciembre y se obtuvieron los siguientes datos.

Nombre sistema	Cantidad generada x día	Cantidad total de información generada y almacenada
Sistema Comercial	800 Mb	24 Gb
Sistema ERP SAP	210 Mb	6.3 Gb
Sistema de Distribución	120 Mb	3.6 Gb
Correo Corporativo	250 Mb	7.5 Gb
Service Desk	10 Mb	0.3 Gb
File Server	300 Mb	9 Gb
Microsoft Office	150 Mb	4.5 Gb
	Total	55.5 Gb aprox.

Cuadro 9: Cantidad de información almacenada en servidores
Fuente: Reportes Div. TIC Electro Puno.
Elaboración: Propia

4.2.9. Análisis de las dimensiones

4.2.9.1. Funcionalidad del CPD de respaldo.

El CPD de respaldo al ser instalado bajo la Norma ANSI TIA 942 y clasificado de acuerdo a las necesidades de la empresa Electro Puno, tiene la capacidad de proveer los servicios necesarios para

cumplir con los requisitos funcionales que demanda cada trabajador al hacer uso de los sistemas de la empresa y a su vez que la gestión de la información esté disponible la mayor cantidad de tiempo. La adecuación, exactitud e interoperabilidad son considerados parte esencial del CPD de respaldo.

4.2.9.2. Eficiencia.

El CPD que cumple con la norma ANSI TIA 942 cumple con todas las características para que la gestión de la información cumpla adecuadamente su función de estar disponible el tiempo que un trabajador la requiera, esto gracias a que la información está disponible el 99.982% de tiempo anualmente esto significa que de las 8760 horas al año, con la clasificación de TIER III la información está disponible 8758.4 horas al año.

4.2.9.3. Compatibilidad.

La compatibilidad tanto de software como de hardware del CPD de respaldo es aceptable porque ambos CPD trabajan bajo las mismas plataformas y el mismo esquema para que la gestión de la información esté disponible en cualquier momento.

4.2.9.4. Usabilidad.

El personal de la empresa, y específicamente la división de TIC este capacitada para poder manejar ambos CPD

satisfactoriamente y que con este los eventos que se suscitan a menudo vayan reduciéndose poco a poco y la cantidad de información perdida también.

4.2.9.5. Fiabilidad.

La empresa Electro Puno, al tener dos CPD, uno principal y otro de respaldo asegura la continuidad de sus servicios, y que los trabajadores no se vean afectados a si mismo que los equipos funcionen de manera correcta en periodos determinados hasta que se pueda hacer algún tipo de mantenimiento correctivo y que no se pierda la información en ese transcurso.

4.2.9.6. Seguridad.

Este es un tema muy importante ya que los CPD al tener conexiones redundantes, la probabilidad de que ambos fallen a causa de algún fenómeno o catástrofe es muy poca o casi nula, asegurando que la empresa reduzca sus costos de recuperación en información y equipos informáticos.

4.2.9.7. Mantenibilidad.

El CPD de respaldo tiene que adaptarse y adecuarse a las exigencias y configuraciones del CPD principal para que ambos trabajen simultáneamente y la información (activo más valioso de la empresa) no se vea perjudica y tampoco los trabajadores.

4.2.9.8. Efectividad.

La división de TIC al tener un respaldo en el manejo de la gestión de la información asegura una continuidad en sus servicios tanto dentro como fuera de la empresa, con el modelo de CPD de respaldo con replicación en tiempo real, se asegura toda la información de la empresa tanto en servicios como calidad.

4.2.9.9. Productividad.

La capacidad del CPD de respaldo que permite al CPD principal utilizar la cantidad apropiada de recursos en relación a la efectividad obtenida.

4.2.9.10. Satisfacción.

La capacidad del CPD de respaldo en cumplir las expectativas al entrar en funcionamiento cuando CPD principal falla y esta toma su lugar hasta que este reestablezca sus servicios nuevamente.

4.2.9.11. Contexto de uso.

El CPD es tolerante a fallas ya que para eso cumple el estándar TIA 942 y es clasificado como un CPD de TIER III.

4.2.10. Cuadro de Costos de implementación del CPD de respaldo

Activo	Cantidad	Costo Total
Switch cisco Core L3	3	S/. 120750.00
Switch cisco 2960 PoE	9	S/. 185850.00
Firewall	1	S/. 59000.00
Storage HP Proliant ml350 g6	4	S/. 19600.00
Servidor EMC2	1	S/. 63000.00
UPS	4	S/. 28000.00
Racks	3	S/. 4500.00
Aire acondicionado	1	S/. 70000.00
Piso Elevado	1	S/. 8750.00
Conexión redundante	1	S/. 5600.00
Total		S/. 565050.00

Cuadro 10: Costo de implementación del CPD de respaldo
Fuente: Cotización con Chanintec S.A.C.
Elaboración: Propia

4.3. Evaluar los niveles de disponibilidad alcanzados con el modelo de CPD con replicación en tiempo real

En los siguientes cuadros se evaluarán y compararan los niveles de disponibilidad alcanzados con el modelo de CPD con replicación en tiempo real propuesto para mejorar la gestión de la información en la empresa Electro Puno S.A.A.

4.3.1. Diferencia de gestión de la información antes y después.

Indicadores	Gestión de la información actual	Modelo propuesto	Diferencia
Adecuación.	No	Si	Si
Exactitud.	No exacta	Exacta	Exacta
Interoperabilidad.	Si	Si	No
Utilización de la norma TIA 942	No	Si	Si
Coexistencia.	No	Si	Si
Interoperabilidad.	Si	Si	No
Facilidad de aprendizaje.	Compleja	Fácil	Fácil
Operabilidad.	No continua	Continua	Continua
Tolerante a fallas.	No	Si	Si
Capacidad de recuperación.	No	Si	Si
Confidencialidad.	No	Si	Si
Integridad.	Si	Si	No
Autenticidad.	Si	Si	No
Riesgo de daño económico.	Si	No	Si
Modularidad.	Si	Si	No
Reusabilidad.	Si	Si	No
Precisión de uso	No	Si	Si
Tiempo de operación.	98.07%	99.982%	1.912%
Cantidad de información usada y almacenada.	55.2 Gb	55.2 Gb	0 Mb
Cumplimiento de propósito.	No	Si	Si

Confianza.	No	Si	Si
Flexibilidad.	No	Si	Si
Nivel de recursos utilizados.	Mucho	Poco	Mucho
Tiempo de disponibilidad de la información (anual)	8702.4 horas	8758.4 horas	56 horas
Tiempo para recuperarse de un incidente.	1 hora	7 minutos	53 minutos
Precisión de la información.	No	Si	Si

Cuadro 11: Cuadro comparativo CPD actual y CPD de respaldo
Elaboración: Propia

Año	Causas	Número de Horas
1	Apagón no comunicado Mala configuración de equipos Intrusión de terceras personas Falla de equipos.	28 horas
2	Apagón no comunicado Mala configuración de equipos Intrusión de terceras personas Falla de equipos.	115 horas
3	Apagón no comunicado Mala configuración de equipos Intrusión de terceras personas Falla de equipos.	25 horas
	Total	168 horas aproximadamente

Cuadro 12: Frecuencia del promedio de fallas en horas del CPD principal
Elaboración: Propia

En el grafico anterior se puede apreciar la cantidad de horas que el CPD principal estuvo fuera de servicio, o se desconectó de la red con las

otras oficinas (Av. El sol y Juliaca), 168 horas en un periodo de 2 años y medio o un promedio de 67.2 horas anuales, es un tiempo no permitido según los niveles TIER y la norma ANSI TIA 942 de un CPD que a continuación mostraremos que especifica la cantidad de horas y minutos mínimos deben de estar inhabilitados los servicios de una empresa y la perdida de dinero que eso genera.

Los niveles describen la disponibilidad de los datos contenidos en el hardware en el CPD.

Al finalizar con el diseño del modelo de CPD de respaldo y la evaluación que se hizo antes y después del tratamiento de los datos obtenidos en el transcurso de la investigación, a continuación, se muestra un cuadro con las diferencias que existe ahora que no se tiene un CPD de respaldo y si se implementa en un futuro.

Indicador	Sin CPD de respaldo	Con CPD de respaldo
Norma TIA 942 implementada	No	Si
Clasificación TIER	No tiene	TIER 3
Cantidad de horas sin servicio	en 2 años y medio más de 168 horas	1 hora, 57 minutos
% de disponibilidad garantizada	98.07%	99.982%

Cuadro 13: Comparación de resultados
Elaboración: Propia.

Para evaluar estadísticamente al indicador más importante se utilizó la "prueba t".

Hipótesis Nula: El modelo de un CPD de Respaldo con replicación en tiempo real no mejora el rendimiento de la gestión de la información en la empresa Electro Puno S.A.A.

Hipótesis Alterna: El modelo de un CPD de Respaldo con replicación en tiempo real mejora el rendimiento de la gestión de la información en la empresa Electro Puno S.A.A.

Por lo tanto, se prueba de validez de la hipótesis general, siendo el diseño de un modelo de CPD de respaldo con replicación en tiempo real en la mejora de la gestión de la información en la empresa Electro Puno S.A.A. una alternativa de solución para el problema de la gestión de la información.

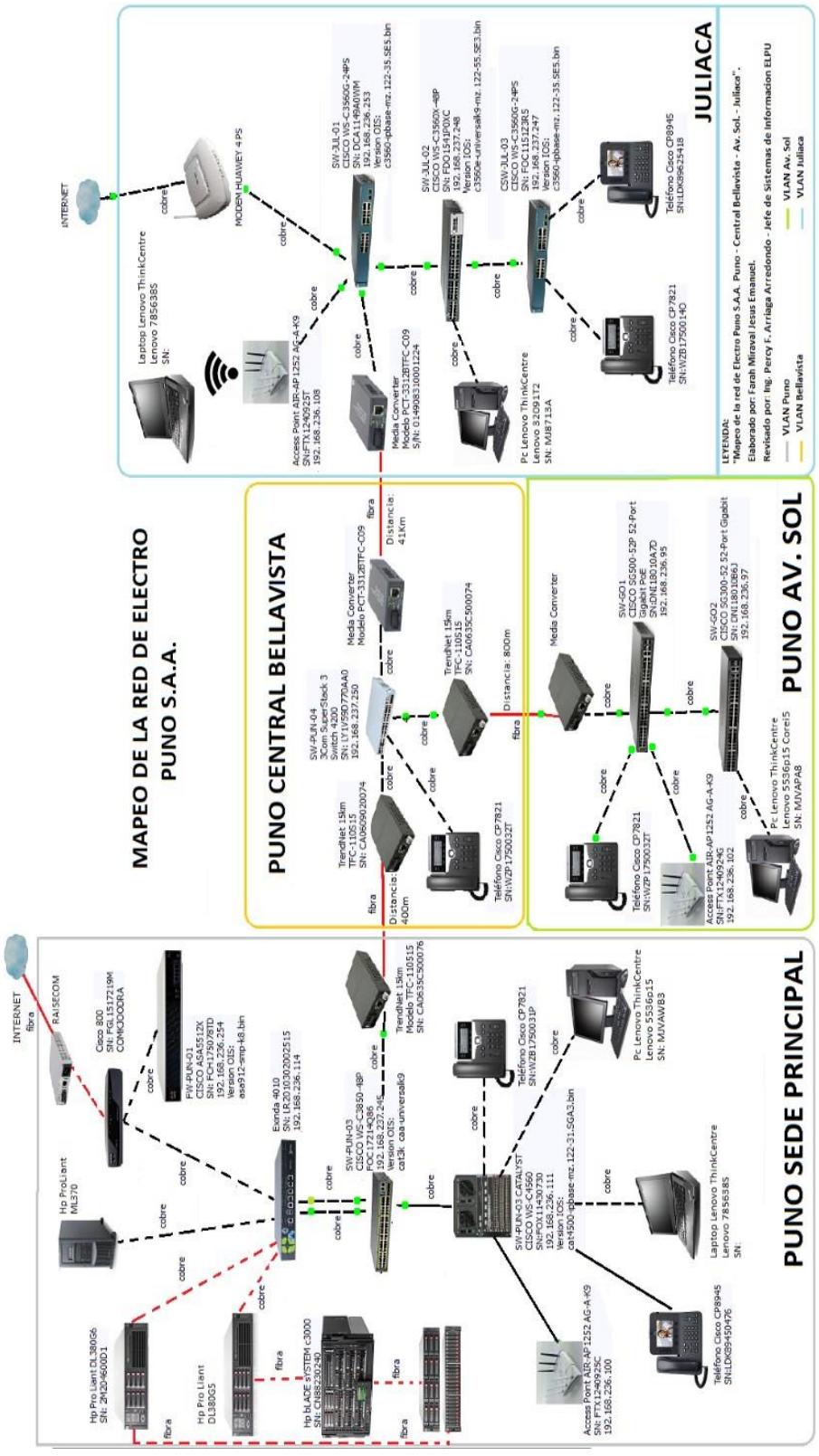


Figura 7: Mapeo de la red actual Electro Puno

Fuente: Div. TIC – Electro Puno.

Elaboración: Propia

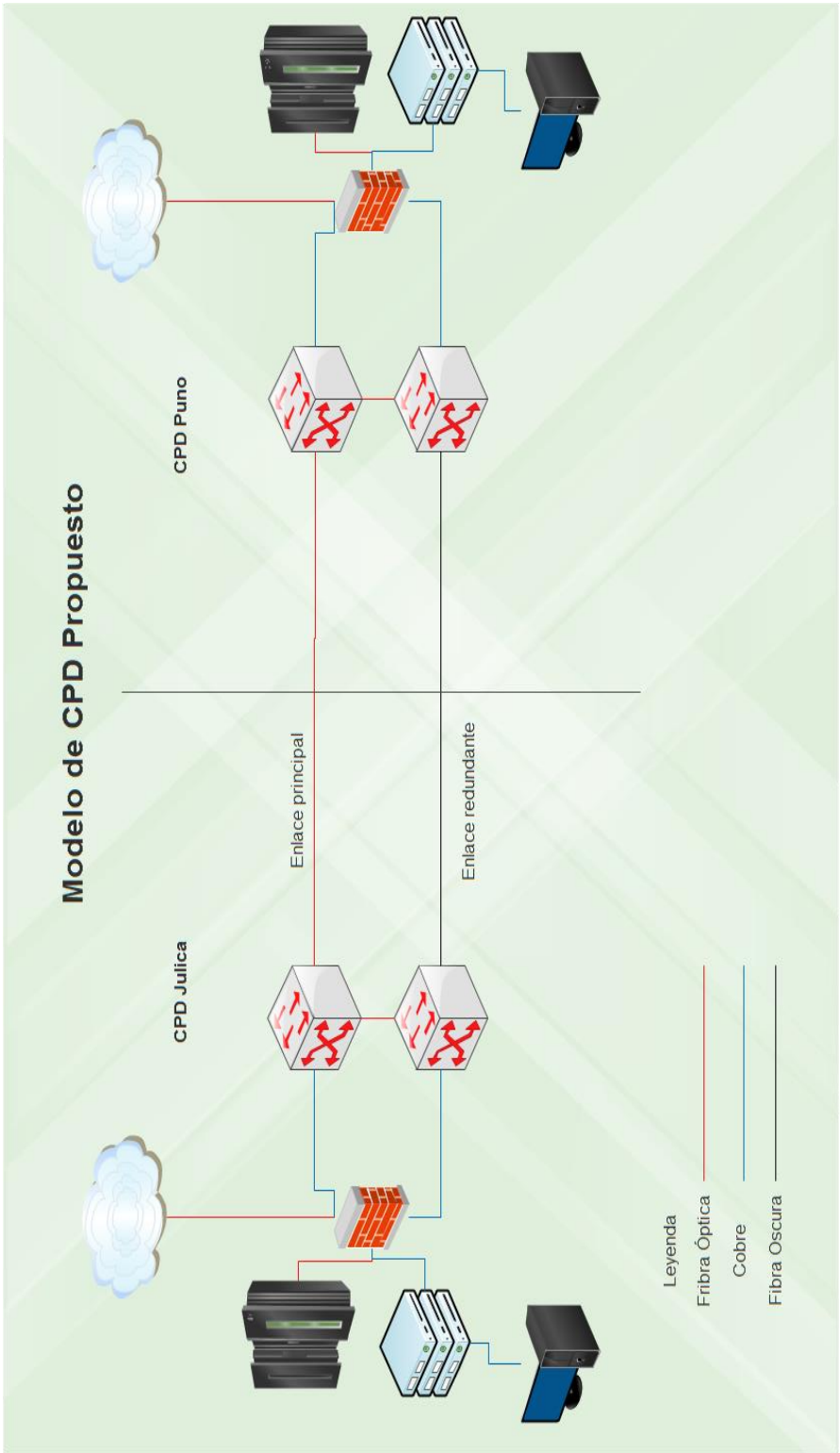


Figura 8: Modelo de conexión de CPD propuesto
Fuente: Edraw Max v7.4
Elaboración: Propia

CONCLUSIONES

PRIMERO: Se diseñó de un modelo de CPD de Respaldo con replicación en tiempo real utilizando la norma ANSI/TIA 942 y clasificando el CPD en TIER III mejorando el rendimiento de la gestión de la información en 1.912% más de disponibilidad de las Tecnologías de la Información dentro de la empresa.

SEGUNDO: Se analizó la situación actual de la gestión de la información con ayuda de programas estadísticos y observación del comportamiento de la información en la empresa Electro Puno, los equipos, llegando a la conclusión de que toda la red, sistemas, información, etc. se encuentra en un grado critico ya que en cada incidente que se presenta se pierde bastante información, la cantidad de horas que estuvo fuera de servicio los sistemas y la red superan el tiempo límite en la clasificación de los TIER con 67.2 horas esto equivale a un 98.07% de disponibilidad anual sobrepasando el porcentaje establecido por la norma TIA 942. Con el diseño del CPD de respaldo con replicación en tiempo real la información estará disponible en un 99.982% que equivale a menos de 2 horas fuera de servicio anual con o sin cortes programados.

TERCERO: Se diseñó el CPD de respaldo utilizando la norma TIA 942 cumpliendo cada uno de los requisitos que esta pide, la cual está incluida el piso elevado, sistema de energía y grupo electrógeno, sistema contra incendios, cableado estructurado, conexiones redundantes y las copias de seguridad en tiempo real utilizando el CPD de respaldo como un CPD espejo, de acuerdo a la información que se genera día a día y toda la información que

se perdió en el transcurso del estudio el CPD de respaldo tendrá una clasificación de TIER III con conexión redundante, el presupuesto para el CPD de respaldo es de S/. 565050.00.

CUARTO: Se evaluó la disponibilidad de la información aplicando la Norma ANSI/TIA 942 y clasificando el CPD de respaldo como un CPD TIER III y se observó que el tiempo total que los servicios están inhabilitados es alrededor de 1.57 horas anuales minimizando los riegos de perdida de información.

SUGERENCIAS

PRIMERO: Se recomienda implementar el diseño del modelo de CPD de respaldo para así poder mejorar la gestión de la información en la empresa Electro Puno S.A.A. y en cualquier empresa que genere grandes cantidades de información.

SEGUNDO: Continuar con las investigaciones ya que las tecnologías e información cambian y mejoran día a día, que este trabajo de investigación sea de aporte a personas interesadas en el tema.

TERCERO: Se recomienda que por el momento no se tiene implementado el CPD de respaldo, se monitoree cuidadosamente el funcionamiento de los equipos y la gestión de la información.

CUARTO: Se recomienda tener un sistema de protección para prever problemas de ruptura de fibra óptica y tener una segunda ruta sin que se pierda la conectividad e información.

BIBLIOGRAFIA

Acuña, T. (2013). Diseño de un Centro de Proceso de Datos. Leganés, España.

Americas, H. (2010). CISCO SYSTEM, INC. *Cisco Data Center Infrastructure 2.5*. USA: Cisco Press.

Andrew, M., & Deepak, K. (2006). Information Availability and Policy. *College of Information Science & Technology*. Nebraska, Omaha: University of Nebraska at Omaha.

Arregoces, M., & Portolani, M. (2004). Data Center Fundamentals. Indianapolis, USA: Cisco Press.

Bustelo, C., & Amarilla, R. (2001). Gestión del conocimiento y gestión de la información. Madrid, España: IAPH.

Cabrera, R., & Guerra, V. (2013). Modelo de Centro de Datos para mejorar la Gestión de la Información en las PYMES de la ciudad de Puno. *Tesis de Grado en Ingeniería de SIstemas*. PUNO, PUNO, PERU: UNA-PUNO.

Clemmer, L. (2010). Information Security Concepts. USA.

Commscope. (2011). Enterprise Data Center Design Guide. USA: Systimax solutions.

Commscope. (2016). Structured connectivity solutions. USA: Systimax solutions.

Floridi, L. (2010). Information: A very Short Introduction . Oxford: Oxford University Press.

Hernandez, R. (2014). *Metodología de la Investigación 6ta Edición.* CUIDAD DE MEXICO: Mc Graw Hill.

Kalloniatis, C. (2012). Innovative Information Systems Modelling Techniques. Rijeka, Croacia: InTech.

Kumar, A. (2011). How to Use Security Metrics. USA.

Madhavan, N. (2006). The Information Integrity Imperative. USA: Infogix, Inc.

Maldonado, J. (2010). Diseño de un centro de Datos basado en estándares, caso práctico: Diseño del Centro de Datos del Colegio Latinoamericano. Cuenca, Ecuador: Universidad de Cuenca.

Mandke, V., & Nayar, M. (2007). Implementing Information Integrity Technology. *A Feedback Control System Approach Unitech Systema, Inc*. India: EMPC Premises.

Newton, H. (2004). Newton's Telecom Dictionary. New York, USA: CMP Books.

Pérez, H. (2014). *PLANIFICACION Y DISEÑO DE UN CPD DE RESPALDO BASADO EN LA NORMA ANSI TIA 942.* MADRID.

Rasmussen, N., & Niles, S. (2006). Data Center Projects: Standardized Process. USA: Schneider Electric.

Reter, B. (2014). *DISEÑO E IMPLEMENTACIÓN CON TECNOLOGÍA CWDM PARA INTERCONECTAR SERVICIOS DE DOS CENTROS DE DATOS DEL REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL.* LIMA.

Roa, J. (2013). Seguridad Informática. Madrid, España.

Russon, P. (2009). Gestión de la Información Empresarial. *The Data Warehousing Institude*. USA.

Simanca, M. (Marzo de 2007). Implementación de un CPD para la operadora CGV Telecomunicaciones C.A. Mérida, Venezuela.

Sumasundaram, G., & Shrivastava, A. (2009). Information Storage and Management: Storing, Managing, and Protecting Digital Information. USA: John Wiley and Sons.

Sun Corporation. (2008). *The Sun Certified Securty Administrator for Salaris Training Course. Fundamental Security Concepts*.

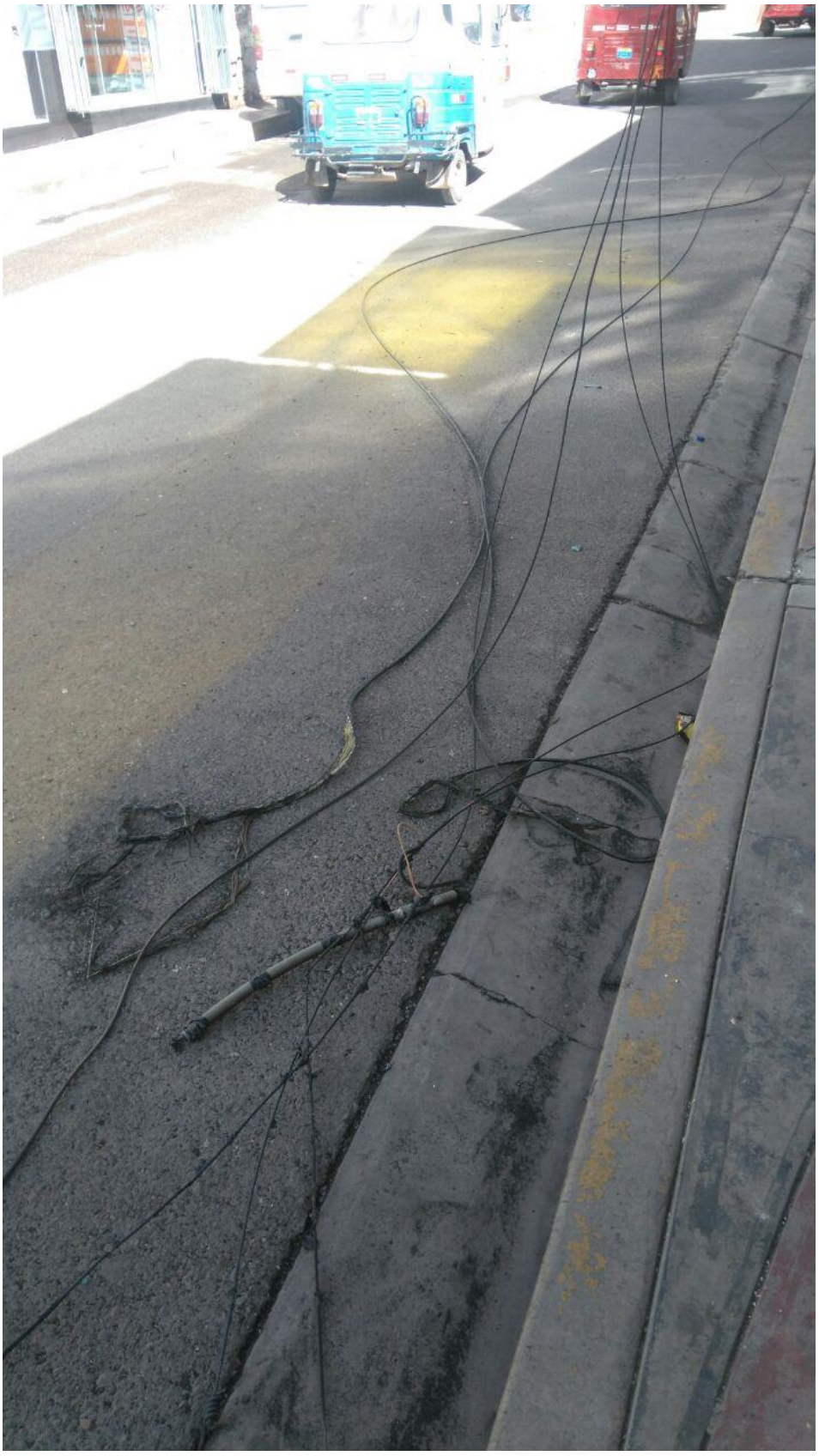
TELECOMMUNICATIONS INDUSTRY ASSOCIATION . (2005). *TIA STANDARD: Telecommunications Infraestructure Standard for Data Center*. TELECOMMUNICATIONS INDUSTRY ASSOCIATION.

Toal, P. (2011). Information Security: A Conceptual Architecture Approach. USA: Oracle Corporation.

ANEXOS

Anexo 1: Conexión de fibra óptica entre Puno - Juliaca quemada

Fuente: Huelga de transportistas Juliaca

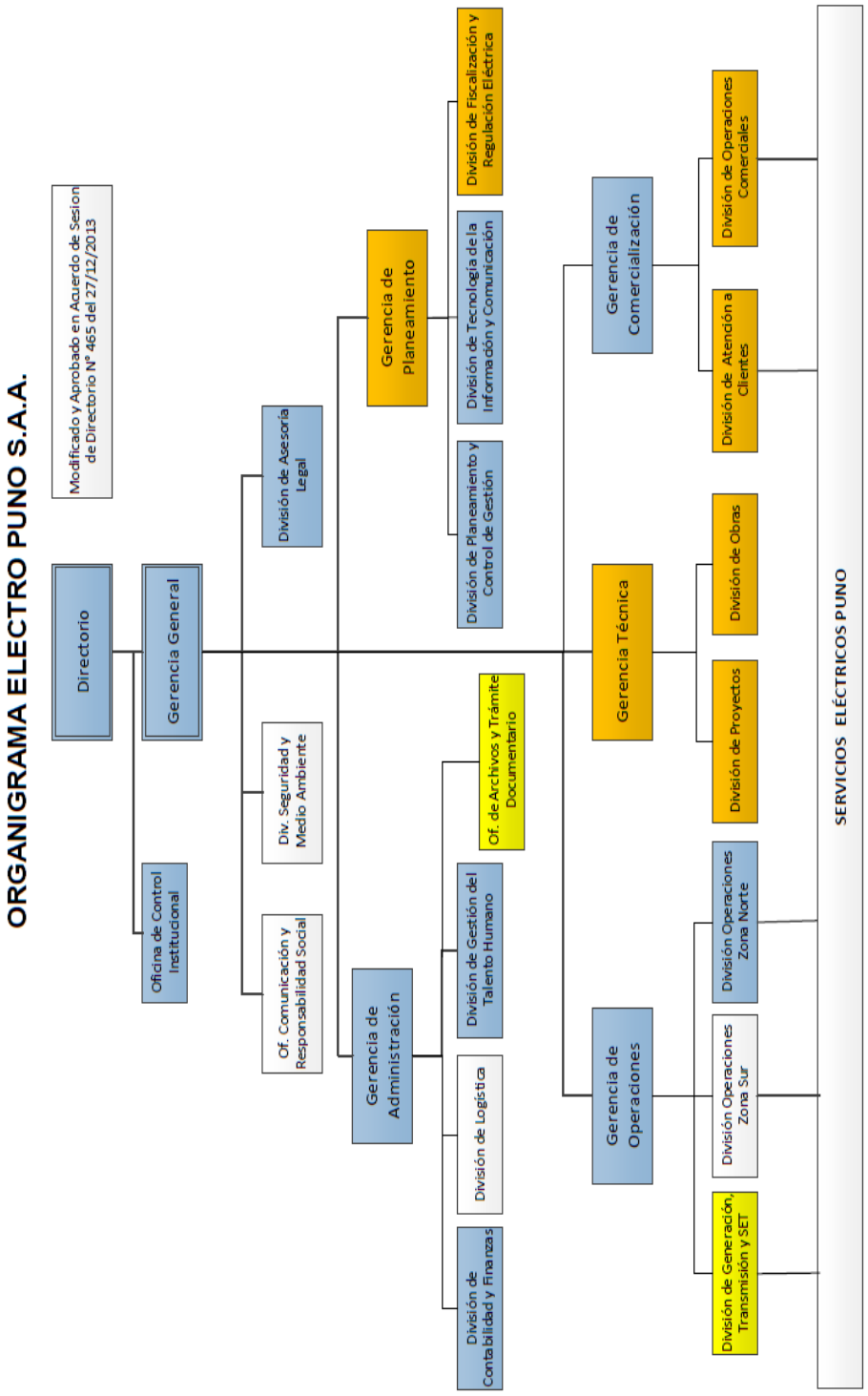


Anexo 2: Fibra Óptica quemada tirada en el suelo.

Fuente: Huelga de transportistas Juliaca

Anexo 3: Mufa de Fiber Lux quemada

Fuente: Huelga de transportistas Juliaca



Anexo 4: Organigrama de Electro Puno

Fuente: Div. Talento Humano ELPU

ANSI/TIA-942-200
Approved: April 12, 200

TIA STANDARD

Telecommunications Infrastructure Standard for Data Centers

TIA-942

April 2005

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Representing the telecommunications industry in association with the Electronic Industries Alliance

Electronic Industries Alliance

Telecommunications Infrastructure Standard for Data Centers

Table of Contents

Anexo 5: Estándar TIA 942 – contenido
Fuente: Revista Estándar TIA 942 año 2005.