UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE UN SISTEMA DE TERCERIZACIÓN DE SERVICIOS DE ALMACENAMIENTO DE DATOS DE ALTA DISPONIBILIDAD

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ALEX ARAFAT PINEDO VARGAS

PROMOCIÓN
2006-II

LIMA-PERÚ
2010

IMPLEMENTACIÓN DE UN SISTEMA DE TERCERIZACIÓN DE SERVICIOS DE ALMACENAMIENTO DE DATOS DE ALTA DISPONIBILIDAD

Doy infinitas gracias.

A Dios, por el camino recorrido.

A mis padres, por su amor y apoyo.

A mis hermanos, por su fortaleza.

A Stefanee, enamorada fiel y sincera.

A la vida, por lo aprendido y aprehendido

SUMARIO

En el presente trabajo se describe el la implementación de un sistema de almacenamiento de datos de alta disponibilidad con la finalidad de brindar servicios de tercerización a empresas poseedoras de bases de datos.

La solución propuesta reduce los costos de inversión en este tipo de sistemas, permite la continuidad de las labores de la empresa en caso de interrupción del acceso a la información o de degradación de la misma debido a agentes internos o externos, evitando a su vez la pérdida de grandes sumas de dinero

El sistema involucra centrales de datos y sistemas de comunicaciones. Los primeros son llamados también "Data Center" y cubren las necesidades de la empresa de alojar datos de sus clientes (sitios de Internet, cuentas bancarias, etc.), los segundos permite el intercambio o traslado de información entre el cliente y entre las centrales de datos. Ambos subsistemas son esenciales para el tráfico, procesamiento y almacenamiento de Información.

La solución cumple con las recomendaciones de los proveedores de software y hardware tal cómo Oracle, Hewlett-Packard y SAP.

ÍNDICE

INTRODUCCIÓN

Actualmente las empresas buscan disminuir su inversión y gastos en operación e infraestructura tecnológica y adquirir los mismos o mayores beneficios a través de un servicio brindado por terceros. En Perú ese concepto se denomina tercerización, en habla inglesa se demoniza outsourcing.

La tendencia de tercerización se refleja en la necesidad de las empresas de centrarse en las actividades principales de su negocio, delegando el manejo de las actividades de soporte o secundarias a especialistas externos con acuerdos de nivel de servicios o SLA (Service Level Agreement de sus siglas en inglés).

Uno de los servicios de tercerización importantes, para una empresa que maneje datos estratégicos, es la tercerización de bases de datos. Es sumamente necesario que la disponibilidad de estos datos sea alta en cuanto a accesibilidad y al respaldo de los mismos.

Los proveedores de tercerización de base datos deben tener experiencia comprobable en los servicios de administración de bases de datos de alta disponibilidad. La propuesta de los proveedores debe contener información tanto sobre las plataformas de sistemas operativos y bases de datos (uno de sus clientes cómo muestra.) así cómo información resumida sobre el personal y funcionarios que estarán a cargo del sistema de tercerización de bases de datos de alta disponibilidad.

El personal debe contar con conocimientos de las versiones de las bases de datos y de las plataformas de interés (Unix, Linux, Windows, Solaris, Aix, Hp-ux, entre otros). Los funcionarios deben poseer preparación a nivel universitario y experiencia comprobable en el sector de negocio donde se encuentre la empresa contratante.

En el Perú actualmente sólo cuatro empresas pueden ofrecer la tercerización de los servicios de comunicación, además de la infraestructura adecuada con monitoreo, respaldo y soporte de aplicación las veinticuatro horas del día durante todo el año (24X7). Estas empresas son IBM, Telefónica del Perú, Global Crossing y GMD.

El presente trabajo describe y expone la mejor solución para poder brindar óptimos servicios de tercerización de base de datos con alta disponibilidad a empresas que lo requieran. Se expondrá la solución establecida en grandes empresas mediante la aplicación de una infraestructura sólida de telecomunicaciones y de almacenamientos de datos. Estas centrales de datos están enfocadas en la importancia de los datos del cliente

y en los beneficios económicos que se obtienen de la tercerización de estos servicios.

La solución propuesta consta de dos sedes, el principal y el de contingencia. De esta manera se asegura la continuidad del negocio sin interrupción (tiempo de respuesta mínimo) ante cualquier desastre ocurrido. Esta solución se realizaría utilizando las infraestructuras de los centros de procesamiento de datos o CPD (Data Center su equivalente en inglés) a través de replicación de datos en los equipos que sirven para almacenar gigas (10^9) y teras (10^{12}) de datos. Estos equipos usualmente son conocidos cómo "Storages".

Ambos emplazamientos se mantienen comunicados mediante un enlace de fibra óptica cuya capacidad de ancho de banda les permite mantener sincronizados (replicar) los datos almacenados. Si el emplazamiento principal falla por cualquier motivo, el de contingencia lo reemplaza en todas las operaciones de almacenamiento y consulta de datos.

Esta solución ofrece al cliente una garantía de continuidad de casi el 100%. Sólo habría una perdida de servicio durante el tiempo que demore en activarse el emplazamiento de contingencia para la replicación de datos y para la operación de los aplicativos relacionados.

El desarrollo de este trabajo se realizó gracias a la experiencia adquirida durante mi formación laboral cómo implantador de Soluciones de Alta Disponibilidad a clientes empresariales alojados en el centro de procesamiento de datos de Telefónica del Perú

El contenido del primer capítulo se centra en la descripción del problema a resolver, es decir se describirá las características más resaltantes de la solución así como las alternativas que se puede brindar. Para poder dar una adecuada solución, se establecerán objetivos implantados así como sus alcances.

El segundo capítulo presenta una referencia teórica de los aspectos relacionados con la tercerización de servicios, el almacenamiento y de los diferentes componentes que se requiere para asegurar la alta disponibilidad de datos en la implementación de las CPD bajo el concepto de "Edificaciones Seguras" (instalaciones eléctricas redundantes, UPS (sistema de potencia ininterrumpida), climatización redundante, sistemas de protección contra incendios, sistema de detección de aniegos e intrusos), seguidamente conceptos sobre almacenamiento de datos (Storage XP, RAID, SAN, Servidores Integrity) y finalmente conceptos relacionados con las redes de datos (topología, ancho de banda, protocolos, etc.) y el estándar Fibre Channel.

En el tercer capítulo se presenta la propuesta técnica o ingeniería del proyecto. Se explican aspectos tales cómo la conectividad, y los elementos básicos del servicio en el CPD. En el cuarto capítulo se describiré el alcance del proyecto, su estructura detallada,

y los componentes de la solución.

Por último, se exponen las conclusiones que se han obtenido a lo largo de la implementación y desarrollo de la solución. También se hacen algunas recomendaciones que deben tenerse en cuenta para futuras implementaciones.

Agradezco a Telefónica del Perú por haberme brindando las facilidades y la autorización para plasmar mi conocimiento y experiencia en el informe de suficiencia.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA DE INGENIERÍA

En este capítulo se describe el problema, se expone el objetivo principal y los objetivos secundarios, se evalúa el problema y se hace una síntesis del trabajo.

1.1 Descripción del Problema

El problema a resolver es la reducción de la excesiva inversión en recursos económicos, para montar una infraestructura adecuada que almacene los datos estratégicos de la empresa, y en recursos humanos calificados necesarios para administrarla. La inversión incluye el soporte lógico (software), el respaldo y el monitoreo, que garanticen la continuidad de los datos ante cualquier desastre (humano y natural).

En la actualidad los datos de las pequeñas, medias y grandes empresas son de vital importancia para el manejo del negocio y mantenerse competitivas.

1.2 Objetivos del Trabajo

En la presente sección se describe el objetivo principal del trabajo, y los beneficios que logra el cliente al adoptar el servicio de tercerización de almacenamiento de datos.

1.2.1 Objetivo principal

Diseñar un sistema que pueda ofrecer servicios de alta disponibilidad del almacenamiento de datos a empresas que así lo requieran, que necesiten ahorra los costos en infraestructura y en costos operativos.

1.2.2 Objetivos secundarios

Los siguientes son los objetivos que busca la empresa contratante al adoptar el sistema propuesto (ahorro en costos en infraestructura y operativos):

- Enfocar sus recursos internos hacia actividades propias del objetivo de la compañía.
- Mejorar la eficiencia de sus procesos e incrementar sus niveles de servicio.
- Obtener mayor flexibilidad y capacidad de respuesta ante exigencias del mercado.
- Asegurar la operatividad del servicio incrementando los niveles de disponibilidad.
- Disminuir sus necesidades de inversión en Tecnología de Información y Comunicaciones, contando con un esquema de conversión de costos variables en fijos.
- Reducir los Costos unitarios de Operación y Gestión de los servicios de Tecnología de la Información y Comunicaciones.

Reducir los riesgos propios del manejo de las Tecnologías de la Información y Comunicaciones.

Facilitar el acceso a nuevas tecnologías

Entregar una calidad de servicio predecible y medible en un entorno 7x24x365

- Afrontar un índice acelerado de cambio y asimilación de tecnología.
- Soportar las presiones del "Time to Market" o TTM (tiempo que toma desde que un producto o servicio es concebido, hasta que está disponible para la venta).
- Afrontar la necesidad de crear Valor Añadido en los servicios de Tecnologías de Información y Comunicaciones.
- Alta disponibilidad de sus sistemas ante cualquier inconveniente.

1.3 Evaluación del Problema

Actualmente las empresas buscan disminuir su inversión y gastos en operación e infraestructura tecnológica y adquirir los mismos o mayores beneficios a través de un servicio brindado por terceros ya que estas empresas cuentan con el personal altamente calificado para administrar dichas plataformas que se encuentra a la vanguardia de los avances tecnológicos. Esta tendencia se refleja en la necesidad de las empresas de centrarse en las actividades principales de su negocio, delegando el manejo de las actividades de soporte o secundarias a especialistas externos.

Anteriormente las empresas montaban una infraestructura no adecuada para sus centros de cómputo teniendo problemas con la continuidad de estos por presentarse problemas de climatización, continuidad eléctrica, no estar preparados para soportar temblores, no brindar seguridad perimetral, etc.

La utilización de sistemas de almacenamiento de alta disponibilidad y la contratación de sus servicios por empresas que así lo requieran se ve justificada por la enorme inversión y responsabilidad para el manejo de su información estratégica. Cómo ejemplo de ello se tiene el percance ocurrido el 28 de febrero de 2008 en el edificio de seguros La Positiva ubicado en San Isidro. Su estación eléctrica no soporto la Carga eléctrica que soportaba todo el edificio y al no tener un generador eléctrico de respaldo, éste estalló generando grandes pérdidas económicas.

Un ejemplo similar es el que ha ocurrido el 23 de Setiembre del 2008 en Madrid en donde una avería eléctrica afectó un centro de cómputo de Telvent. Este CPD es uno de los más importantes de España y en él se presta servicio a decenas de empresas. Los afectados principales fueron los usuarios de Ya.com, puesto que los servidores DNS se alojan en este sitio.

Nota:
Los servidores DNS o Domain Name System, permiten conectarse con la máquina sin

necesidad de usar una dirección IP, por ejemplo http://190.81.186.12; basta con ingresar el nombre de dominio, (por ejemplo www.orce.uni.edu.pe), para que el servidor DNS resuelva y establezca una conexión.

Los emplazamientos deben poseer una adecuada infraestructura y a la vez se debe disponer de un emplazamiento de respaldo para cubrir cualquier desastre. También es importante disponer de personal calificado para realizar las tareas de monitoreo y administración.

Los emplazamientos deben asegurar servicios las veinticuatro horas durante los trescientos sesenta y cinco días de año (24x7) y ante cualquier degradación del servicio.

Los CPD de las empresas no brindaban una rápida escalabilidad de sus plataformas ni de personal permanente para solucionar las fallas que se presentaran. Es así que surge la tercerización de servicios de almacenamiento de datos de alta disponibilidad cómo solución a estos problemas.

1.4 Síntesis del trabajo

Este sistema se logra mediante un adecuado diseño de los CPD. Los CPD o datacenters están diseñados para cubrir las necesidades de alojamiento, seguridad, conectividad, gestión y operación de los equipos designados a atender los servicios de los sistemas alojados en ellos, permitiéndole así desarrollar y explotar soluciones avanzadas según sus necesidades y requerimientos.

El sistema se apoya en servicios de comunicación que brindan las empresas de telecomunicaciones. Estas deben garantizar un óptimo funcionamiento, máxima disponibilidad y los mejores tiempos de respuesta, en las mejores condiciones ambientales y de seguridad.

El sistema en general debe permitir a los clientes una gran escalabilidad y fácil adaptación al crecimiento de su negocio, eliminando así posibles problemas de espacio que podrían generar ampliaciones, cuando éstas se realizaran en su domicilio o en un centro no dimensionado de forma adecuada para ello.

La solución propuesta está diseñada para mantenerse operativa ante cualquier desastre que ocurriera en uno de los emplazamientos (principal o de contingencia). La solución está limitada al área metropolitana de Lima. Un temblor de más de 8 grados en la escala de Richter afectaría las edificaciones de los emplazamientos en los cuales se ubican las CPD. En este caso la solución no aseguraría alta disponibilidad por la gran probabilidad de que los emplazamientos hayan sufrido daños graves. Una solución más segura sería la habilitación de un emplazamiento de contingencia fuera del área metropolitana, sin embargo esto elevaría el costo de manera considerable. El presente diseño solo se circunscribe al área metropolitana. El tiempo para implantar estas soluciones es de noventa días después de haber firmado el contrato.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

El presente capítulo explica los conceptos esenciales para la comprensión del diseño propuesto. Se explica aspectos tales cómo tercerización, edificaciones seguras, almacenamiento de datos y la plataforma de comunicaciones de fibra óptica

2.1 Tercerización

El Perú, ante las nuevas tendencias mundiales de prestación de servicios, adecuó estas prácticas en el territorio nacional mediante la promulgación de la ley que regula los servicios de tercerización, Ley Nº 29245, publicada el 26 de junio de 2008. Esta señala lo siguiente:

" Se entiende por tercerización, la contratación de empresas para que desarrollen actividades especializadas u obras, siempre que éstas asuman los servicios prestados por su cuenta y riesgo, cuenten con sus propios recursos financieros, técnicos o materiales, sean responsables por los resultados de sus actividades y sus trabajadores estén bajo su exclusiva subordinación.

Constituyen elementos característicos de tales actividades, entre otros, la pluralidad de clientes, que cuente con equipamiento, la inversión de capital y la retribución por obra y servicios. En ningún caso se admite la sola provisión de personal. La aplicación de este sistema de contratación no restringe el ejercicio de los derechos individuales y colectivos de los trabajadores"

El uso común del concepto de tercerización es "outsourcing", subcontratación o extemalización. El término outsourcing se extiende al de Business Process Outsourcing (BPO), Knowledge Process Outsourcing (KPO), Information Technology Outsourcing (ITO), etc., que precisan que tipo de servicio se está tercerizando, es decir, funciones de procesos de negocios en proveedores de servicios, funciones de mayor valor y de procesos intensivos de conocimiento, y servicios de tecnología de información, respectivamente. Este último se aplica al presente trabajo.

2.2 Edificaciones seguras

Está vinculado estrechamente al concepto de alta disponibilidad. Una edificación segura asegura la atención de las necesidades de los clientes en cada país y si el cliente lo requiere.

Para asegurar la alta disponibilidad todos los CPD deben interconectarse entre sí a través de una red de datos. En Lima se debe contar con dos CPD conectados entre sí mediante fibra óptica. Cada CPD puede trabajar indistintamente cómo principal o de contingencia, caso las necesidades del cliente y sus aplicativos así lo requieran. Estos emplazamientos también deben contar con nodos de comunicaciones. Esta ventaja facilita la provisión de los distintos tipos de conectividad tales cómo IP/VPN, Infointernet, Telefonía RTB/RDSI, Red Internacional, etc., los cuales son explicados en el Anexo A "Tipos de Conectividad".

Ambos emplazamientos deben contar con áreas independientes donde se encuentren ubicados los CPD, aislándolos así de áreas administrativas. En estas áreas independientes se ubican cintotecas (almacén de los medios magnéticos), almacén de equipos en tránsito, sala de operadores, sala de equipos críticos. Asimismo, en el local se cuenta con áreas designadas para albergar UPS, generadores, subestación eléctrica, etc. La edificación de ambos locales debe estar diseñada para soportar sismos de grado 8 en la escala de Richter, con lo cual se garantiza su disponibilidad aún ante casos de catástrofes naturales.

Otros aspectos importantes vinculados al concepto de edificaciones seguras lo constituyen los siguientes elementos:

Instalaciones eléctricas redundantes.

- Climatización redundante.
- Sistemas de Seguridad y vigilancia.

Los cuales serán explicados en las siguientes líneas.

2.2.1 Instalaciones eléctricas redundantes

La energía eléctrica comercial es proporcionada por las empresas que proporcionan el alumbrado público ya sea Luz del Sur o Edelnor, hacia una subestación de 10,000 voltios ubicada dentro del edificio.

Las instalaciones eléctricas redundantes requieren de grupos electrógenos y de UPS. Estos se unen al sistema eléctrico mediante un tablero de transferencia automática (TTA). El TTA supervisa el ingreso de energía comercial y, en caso se presente un corte o variación, transfiere toda la carga al banco de UPS y enciende el generador principal, el mismo que en un máximo de dos minutos se encuentra listo para asumir toda la carga eléctrica.

En el hipotético caso que el generador principal no encienda, el sistema está preparado para arrancar el segundo generador en un plazo máximo de 05 minutos de detectado el corte o variación. El sistema eléctrico como elemento vital para garantizar la continuidad de operatividad del data center, tiene semanalmente un exigente simulacro y

protocolo de pruebas, todo esto debidamente supervisado por personal especializado residente de la empresa proveedora de estos equipos durante las 24 horas los 7 días de la semana en los CPD.

La salida del TTA alimenta la entrada del banco de UPS, los mismos que operan en línea y proporcionan energía monofásica y trifásica. La salida de los UPS alimentan los tableros de distribución de energía eléctrica donde se ubican llaves térmicas que alimentan de manera independiente a cada uno de los gabinetes ubicados en la sala de equipos.

Son recomendables las siguientes especificaciones:

- Grupo de energía principal.- Grupo electrógeno diesel marca Caterpillar. Suministra energía en 220 VAC, trifásico, tres hilos, 60 Hz, sistema aislado de tierra, 820 Kw, cuenta con dos cisternas de combustible los cuales garantizan una autonomía de tres días de operatividad sin reabastecimiento de combustible.
- Grupo de energía secundario.- Grupo electrógeno diesel marca Cummins. Suministra energía en 220 VAC, trifásico, tres hilos, 60 Hz, sistema aislado de tierra, 156 KVA, este generador está dimensionado para atender sólo la carga eléctrica de los servidores.
- UPS.- El sistema de UPS está compuesto por un banco de 8 UPS de 80 KVA en configuración paralelo redundante N+1, los cuales proveen energía estabilizada con una autonomía de 30 minutos a los distintos ambientes del CPD.

Nota:
N+1 es una configuración en la que 2 UPSs soportan la carga de los sistemas a la vez; siendo cada una capaz de soportar toda la carga por completo. Esta es una de las configuraciones más habituales; requiere que las UPSs estén sincronizadas y habitualmente que sean del mismo fabricante.

2.2.2 Climatización redundante

Sistema de aire acondicionado necesario para asegurar las condiciones de temperatura y humedad en los ambientes críticos. Los equipos propuestos son marca Liebert del tipo precisión, adecuado para las necesidades de un CPD. Las unidades que atienden las salas de equipos críticos se mantienen trabajando en un esquema N+1 de redundancia.

El aire acondicionado se distribuye a través del falso piso y el retorno es a través de la misma sala. La capacidad de enfriamiento total para las salas de equipos críticos es de 155 toneladas de capacidad distribuidas en los distintos equipos instalados. La unidad de condensación se ubica en el techo del CPD y es enfriada por aire. Una edificación segura debe contar con personal técnico especializado presente permanentemente en los locales para atender incidencias en su funcionamiento. La temperatura debe estar

distribuida en todo el ambiente y debe estar entre 19 y 21, valores óptimos y la humedad bajo del 50% Humedad

Nota
Una tonelada es la medida del tamaño o de la capacidad de enfriamiento del aire acondicionado. Una tonelada es equivalente a quitar 12,000 *BTUs de calor por hora. Por ejemplo, un aire acondicionado de tres toneladas puede quitar 36,000 BTUs por hora. BTU (British Termal Unit) es la cantidad de energía requerida para aumentar la temperatura.

2.2.3 Sistemas de seguridad y vigilancia

Los CPD deben contar con altos niveles de seguridad física, así como con personal adecuado que permita garantizar la privacidad y confidencialidad de la información y procesos gestionados por él.

Forman parte de las características de seguridad y vigilancia del local los siguientes elementos:

- Seguridad perimetral
  - Acceso peatonal único.
  - Reflectores de alta potencia.
  - Cámaras de (CCTV) Circuito cerrado de televisión perimetrales.
  - Vigilancia permanente 24x7x365.
- Sistemas de seguridad interna
  - Detectores de presencia.
  - Puertas metálicas.
  - Cámaras de vigilancia.
  - Vídeo centralizado, grabación las 24 horas.
  - Control de acceso mediante sensores biométricos y tarjetas de proximidad.
  - Vigilancia permanente 24x7x365.
  - Sistema de protección contra incendio.
  - Sistema detección de inundación e intrusión.

Para garantizar que las normas de seguridad y control de acceso sean cumplidas, un área distinta a la de gestión del CPD debe fijar y controlar las políticas a ser seguidas por el personal que ingresa al local, ya sea personal de la empresa, proveedores, clientes o visitas. El CPD debe pasar por auditorias tanto en sus sistemas de control en el ingreso y seguridad de la parte operativa. Estos procesos son llevados a cabo en muchos casos por los auditores de los clientes, tales como Verisign Inc., Defensa Civil, etc.

Especificaciones complementarias sobre los sistemas de seguridad y vigilancia en el presente diseño son mencionadas a continuación:

Sistema de CCTV Circuito cerrado de televisión.- El sistema de CCTV permite vigilar de manera constante y simultánea las distintas salas del CPD. En la sala de control se dispone de dos monitores de 20" conectados a un switch de monitoreo que permite administrar las 8 cámaras del CPD. Se dispone de cámaras fijas, móviles así como domos (360° de rotación) distribuidas en los puntos estratégicos del CPD. Asimismo, dos videograbadoras ubicadas en la misma sala permiten mantener un registro constante de cualquier incidente ocurrido en el CPD.

Sistema de detección de inundación e intrusión.- El sistema de detección de inundación está instalado para detectar aniegos de agua producidos por los equipos de de Aire Acondicionado (AA) y la posibilidad de ingreso de agua del exterior. El sistema de detección de intrusión está diseñado para detectar el ingreso no autorizado al CPD y a los diferentes ambientes del mismo, incluidos la sala de grupo electrógeno, sala de UPSs y subestación.

Se mencionan estos dos sistemas de manera conjunta debido a que éstos reportan sus alarmas en un mismo panel. El sistema de detección de inundación e intrusión se componen de:

- Sensores electromagnéticos en todas las puertas del CPD.
- Sensores de inundación cerca de los AA y uno cerca de la puerta de ingreso del CPD.
- Tablero de recepción de señales y un panel de alarma y visualización ubicado en la sala de control del CPD.

Sistema de control de acceso.- Está diseñado para controlar y monitorizar el tráfico dentro del CPD y permitir llevar una bitácora del personal. El mismo dispone de tarjetas de proximidad personales que permiten traspasar la puerta de ingreso del CPD en el cual se ubica la sala de control en la cual se puede efectuar una identificación visual de la persona por parte del operador de la sala de control. El ingreso al ambiente 2 se hace a través de una esclusa que permite el paso de una sola persona por vez y requiere el uso de la tarjeta de proximidad.

El ambiente 2 es una zona de paso camino al ambiente 3. A medida que se incrementa el nivel del ambiente se incrementa el nivel de seguridad exigido, en este caso el ingreso al ambiente 3 requiere la identificación mediante huella digital y clave además de emplear la tarjeta de proximidad.

El ambiente 4 es la zona de máxima seguridad en la cual se requiere la identificación biométrica mediante la lectura completa de la palma de la mano y clave además de requerir el uso de la tarjeta de proximidad.

- Sistemas de protección contra incendios.- Consta de un sistema de detección y de un

sistema de extinción los cuales trabajan de la siguiente forma:

- Para el sistema de detección se tienen distribuidos detectores de humo tanto iónicos como fotoeléctricos distribuidos bajo el falso piso, en el falso techo y sobre el falso techo.
- La activación de estos detectores (mediante referencia cruzada) da inicio a alarmas sonoras y estroboscópicas, las mismas que indican que se debe evacuar el edificio. Las puertas del CPD, cuentan con cerraduras magnéticas, son desactivadas para facilitar la evacuación del edificio.
- Dicha alarma es reportada en la sala de control del CPD en paneles especiales. En el caso propuesto es el Notifier AFP400 indicando la ubicación física de la zona afectada.
- En el caso que dos alarmas de distinto tipo y que pertenezcan a la misma zona, se activen, se inicia la secuencia de descarga del gas FM-200 o Ecaro 25 (en función de la sala afectada). Estos gases se encuentran almacenados en tanques distribuidos en las áreas del CPD y mediante tuberías son descargados tanto sobre el falso techo, falso piso y la sala propiamente dicha. Para el caso de la sala de equipos críticos y por tratarse de un ambiente de gran tamaño se dispone de tanques independientes para atender el falso piso y el falso techo. Debe indicarse que la descarga no es inmediata sino luego de transcurridos 30 segundos, de tal manera que se pueda evacuar el local, tiempo suficiente para detener la secuencia de disparo (en caso se trate de una falsa alarma) y poner a resguardo al personal que se encuentre en la zona afectada.
- Existen además disparadores manuales distribuidos en las distintas salas del CPD de tal manera que la secuencia de disparo pueda ser activada de manera manual y no automática a través de las alarmas.

2.3 Almacenamiento de datos

La manera tradicional de interconectar los dispositivos de almacenamiento con las computadoras ha sido a través de una arquitectura de bus (ver anexo B "Topología de Redes"). Estas son conexiones dedicadas a un solo servidor, que es quien gestiona todo el movimiento de datos desde y hacia el almacenamiento. Este modelo es el que ahora se denomina DAS (Direct Attached Storage, almacenamiento directamente conectado) DAS evolucionó a lo largo del tiempo proporcionando capacidad en la gestión de los datos a la parte del almacenamiento, por ejemplo, memorias caché (sistema especial de almacenamiento de alta velocidad) propias, y RAID (Redundant Array of Independent Disk), una colección de discos independientes redundantes.

También es importante mencionar al estándar SCSI (Small Computers System

Interface) y su uso a lo largo del tiempo. El SCSI es un estándar tan antiguo como lo es Ethernet (estándar de redes de computadoras de área local) o TCP/IP (Protocolo de control de transmisión/Protocolo de Internet). SCSI es un estándar actual y con mucha proyección al igual que los mencionados. El SCSI es una especificación para la conexión mediante un bus paralelo entre procesadores y dispositivos puramente física, pero también es un potente protocolo de comunicaciones entre los procesadores centrales y los dispositivos que sirven los datos.

En las redes de almacenamiento o SAN (storage area network) los elementos que interactúan son los mismos que en el modelo anterior. La diferencia es la forma de interconexión, es decir, lo que era un bus de hasta 15 dispositivos y distancias no superiores a 25 metros evoluciona en una infraestructura de red que permite aumentar el número de dispositivos y servidores, y las distancias entre los mismos. La tecnología que hace posible una SAN es el estándar "Fibre Channel".

Nota:
El estándar Fibre Channel se define como una interfase de transferencia de datos de alta velocidad que puede ser utilizada para conectar estaciones de trabajo, servidores, supercomputadores, sistemas de almacenamiento masivo (SAN), etc. Este estándar está dirigido a cubrir la necesidad de manejar altas tasas de transferencia de datos y grandes volúmenes de información. La tasa de transferencia típica de los dispositivos de gama alta Fibre Channel se sitúa a velocidades de hasta 4 Gb/s. El medio físico utilizado para estas tasas es la fibra óptica

Otro modelo para compartir almacenamiento de datos a través de una red es el NAS (Network Attached Storage, almacenamiento conectado a red). Un dispositivo NAS se conecta directamente a las redes de datos tradicionales basadas en TCP/IP a través de interfaces Ethernet y pone a disposición de los equipos de esta red el almacenamiento que gestiona mediante un protocolo de sistema de ficheros en red o NFS (Network File System), CIFS (Common Internet File System) o incluso HTTP (Hypertext Transfer Protocol). En conclusión, un dispositivo NAS comparte ficheros mientras que en una SAN se comparten dispositivos de bloques. En el modelo NAS se utiliza una infraestructura de red de datos, mientras que en una SAN se crea una infraestructura de red nueva dedicada y orientada a compartir dispositivos de almacenamiento. Cada uno de los modelos tiene aplicaciones específicas y no son incompatibles entre sí.

En las siguientes líneas se complementarán las definiciones de los dispositivos de almacenamiento.

Los dispositivos de almacenamiento son la base de la SAN. La SAN libera el almacenamiento de tal manera que ya no forma parte del bus particular de un servidor, es decir, el almacenamiento se extemaliza y su funcionalidad se distribuye. Las unidades de cinta magnética o librerías y robots de cintas como cabinas de discos, se conectan

directamente a la red Fibre Channel.

Las cabinas de discos son diseñados tomando en consideración la importancia de la disponibilidad y seguridad de los datos contenidos en sus dispositivos. Son utilizados elementos redundantes e intercambiables en caliente, tales cómo controladoras, módulos de caché, baterías, fuentes de alimentación, discos, etc.. El componente fundamental de una cabina de discos es su controladora, normalmente emparejada con otra igual.

Las controladoras se conectan a la SAN mediante puertos Fibre Channel y a la estructura interna de la cabina mediante buses SCSI o conexiones Fibre Channel internas formándose un doble bucle balanceado. Los discos serán dispositivos propiamente SCSI o discos Fibre Channel. Las controladoras tienen funcionalidades de redundancia y paridad tipo RAID, y de acceso a los volúmenes (LUN) por ellas gestionadas (LUN Masking), además capacidad de tomar el control del sistema transparentemente si su pareja falla.

Nota:
Los LUN son divisiones de las unidades de almacenamiento. LUN significa Logical Unit Number.

Elementos importantes a mencionar en el presente diseño son el Storage XP, el RAID, las redes de almacenamiento, las SAN y los servidores Integrity, que serán descritos en las líneas siguientes.

2.3.1 Storage XP

Hewlett-Packard ofrece una nueva generación de soluciones de almacenamiento especialmente dirigidas a grandes empresas que necesiten acceso constante a los datos críticos y de continuidad en las operaciones. Los últimos modelos de HP Storage XP duplican la capacidad, el rendimiento y la disponibilidad de los datos principalmente debido a su flexibilidad y a las posibilidades de particionamiento y virtualización de que dispone.

Nota:
Particionamiento es la capacidad de los Storages en dividir un grupo de discos en varias unidades lógicas o LUN de distintas capacidades (15Gigas, 100Gigas), para los distintos requerimientos de los sistemas
La virtualización se refiere a la capacidad de los Storages en generar varios LUN pequeños sobre un LUN de gran capacidad ya creado.

Lo nuevo que destaca en HP Storage XP es el "Thin Provisioning". Esta es una herramienta que evita la parada de los sistemas al configurar desde el principio toda la capacidad de almacenamiento que se necesitará en el futuro, asignando espacio de almacenamiento virtual cuando se necesite. Esta herramienta también reduce el consumo de energía de los CPD al no tener equipos sobredimensionados en previsión de mayores

necesidades. En esta situación, el modelo HP StorageWorks XP24000 es la cabina de almacenamiento más idónea para cualquier gran compañía que necesite disponer de una solución tolerante a desastres permitiendo a la vez aumentar su capacidad sin parar los sistemas.

Actualmente el almacenamiento se caracteriza por una deficiente utilización de los recursos existentes, con herramientas de gestión y aplicaciones aisladas, falta de estrategias de respaldo o de recuperación, y un aumento progresivo de costos de operación.

Esta tecnología permite compartir ficheros, volúmenes y protección de datos para distintos entornos (Mainframe, Windows, Linux o HP-UX,) y para cualquier aplicación de negocio de la empresa. Esta tecnología cuenta además con ventajas claves, cómo su capacidad y rendimiento, una gestión más eficiente con "Thin Provisioning", las posibilidades de particionamiento y virtualización y una gran flexibilidad. Esto se puede resumir en lo siguiente:

- Capacidad y rendimiento.- Mejora significativa del rendimiento, con más del doble de los sistemas actuales, así como una capacidad hasta cinco veces mayor que la actual. Además, se lleva a cabo una actualización online sin interrupciones del firmware.
- Thin Provisioning.- Hace posible una gestión más eficiente, evitando la parada de los sistemas y configurando toda la capacidad de almacenamiento que se necesitará en el futuro, pero pagando sólo lo que se necesita en ese momento. Esta herramienta también aumenta la eficiencia energética del sistema, reduciendo potencia innecesaria y la generación de calor, todo lo cual se traduce en una importante reducción de los costes operacionales.
- Virtualización.- Mediante la herramienta "XP External Storage", se reduce los costes además de simplificar la gestión del almacenamiento multifabricante. Para ello, los servidores analizan la capacidad total de las distintas unidades de almacenamiento de que disponga la empresa pero no los dispositivos físicos, haciendo posible una movilidad transparente de los datos y una migración de datos heterogénea.

  Particionamiento.- permite llevar a cabo hasta 32 particiones que aseguran que las aplicaciones críticas tienen los recursos suficientes, previniendo posibles errores del administrador que pueden afectar a una cabina entera.

  Flexibilidad.- Posee gran flexibilidad para conseguir los objetivos de disponibilidad y rendimiento.

Nota:
Firmware o programación en firme, es un bloque de instrucciones de programa para

propósitos específicos, grabado en una memoria de tipo no volátil (ROM, EEPROM, flasr. etc.), que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Al estar integrado en la electrónica del dispositivo es en parte hardware, pero también es software, ya que proporciona lógica y se dispone en algún tipo de lenguaje de programación. Funcionalmente, el firmware es el intermediario (interfaz) entre las órdenes externas que recibe el dispositivo y su electrónica, ya que es el encargado de controlar a ésta última para ejecutar correctamente dichas órdenes externas. El firmware se encuentra en memorias ROM de los sistemas de diversos dispositivos periféricos, como en monitores de video, unidades de disco, impresoras, etc., pero también en los propios microprocesadores, chips de memoria principal y en general en cualquier circuito integrado.

2.3.2 RAID

La distribución de datos en varios discos puede ser gestionada por hardware dedicado o por software Además, existen sistemas RAID híbridos basados en software *y* hardware específico.

Con la implementación por software, el sistema operativo gestiona los discos del conjunto a través de una controladora de disco normal, esto es Interfaces IDE (Integrated device Electronics), ATA (Advanced Technology Attachment), SATA (Serial ATA), SCSI, SAS (Serial Attached SCSI) o Fibre Channel. Considerada tradicionalmente una solución más lenta, con el rendimiento de las CPUs modernas puede llegar a ser más rápida que algunas implementaciones hardware, a expensas de dejar menos tiempo de proceso al resto de tareas del sistema.

Una implementación de RAID basada en hardware requiere al menos una controladora RAID específica, ya sea como una tarjeta de expansión independiente o integrada en la placa base, que gestione la administración de los discos y efectúe los cálculos de paridad (necesarios para algunos niveles RAID). Esta opción suele ofrecer un mejor rendimiento y hace que el soporte por parte del sistema operativo sea más sencillo (incluso totalmente transparente). Las implementaciones basadas en hardware suelen soportar sustitución en caliente (hot swapping), permitiendo que los discos que fallen puedan reemplazarse sin necesidad de detener el sistema.

En los RAIDs mayores, la controladora y los discos suelen montarse en una caja externa específica, que a su vez se conecta al sistema principal mediante una o varias conexiones SCSI, Fibre Channel o iSCSI. A veces el sistema RAID es totalmente autónomo, conectándose al resto del sistema como un NAS.

Los RAIDs híbridos se han hecho muy populares con la introducción de controladoras RAID hardware baratas. De hecho, el hardware es una controladora de disco normal sin características RAID, sin embargo el sistema incorpora una aplicación de bajo nivel que permite a los usuarios construir RAIDs controlados por la BIOS. Por ello es necesario el uso de un controlador de dispositivo específico para que el sistema

operativo reconozca la controladora como un único dispositivo RAID. Estos sistemas efectúan todos los cálculos por software, con la consiguiente pérdida de rendimiento, y típicamente están restringidos a una única controladora de disco.

Una importante característica de los sistemas RAID por hardware es que pueden incorporar un caché de escritura no volátil (con alimentación de respaldo por batería) que permite aumentar el rendimiento del conjunto de discos sin comprometer la integridad de los datos en caso de fallo del sistema. Esta característica no está obviamente disponible en los sistemas RAID por software, que suelen presentar por tanto el problema de reconstruir el conjunto de discos cuando el sistema es reiniciado tras un fallo para asegurar la integridad de los datos.

Los sistemas basados en software son mucho más flexibles (permitiendo, por ejemplo, construir RAIDs de particiones en lugar de discos completos y agrupar en un mismo RAID discos conectados en varias controladoras) y los basados en hardware añaden un punto de fallo más al sistema (la controladora RAID).

Todas las implementaciones pueden soportar el uso de uno o más discos de reserva (hot spare), unidades preinstaladas que pueden usarse inmediatamente (y casi siempre automáticamente) tras el fallo de un disco del RAID. Esto reduce el tiempo del período de reparación al acortar el tiempo de reconstrucción del RAID.

a. Formatos de unidades lógicas de almacenamiento (LUN).

Los tipos de formato de unidades lógicas de almacenamiento a mencionar son explicados a continuación. En los gráficos de esta sección se debe tener en cuenta que cada número representa un bloque de datos; y cada columna un disco.

a.1 RAID 0 o Data Striping

Un RAID 0 (también llamado conjunto dividido o volumen dividido):

- Distribuye los datos equitativamente entre dos o más discos sin información de paridad que proporcione redundancia.
- No era uno de los niveles RAID originales y no es redundante.
- Se usa normalmente para incrementar el rendimiento, aunque también puede utilizarse como forma de crear un pequeño número de grandes discos virtuales a partir de un gran número de pequeños discos físicos.

  Puede ser creado con discos de diferentes tamaños, pero el espacio de almacenamiento añadido al conjunto estará limitado al tamaño del disco más pequeño (por ejemplo, si un disco de 300 GB se divide con uno de 100 GB, el tamaño del conjunto resultante será 200 GB).
- Una buena implementación dividirá las operaciones de lectura y escritura en bloques de igual tamaño y los distribuirá equitativamente entre los dos discos.

Es posible crearlo con más de un disco, si bien la fiabilidad del conjunto será igual a la fiabilidad media de cada disco entre el número de discos del conjunto; es decir, la fiabilidad total es (aproximadamente) inversamente proporcional al número de discos del conjunto. Esto se debe a que el sistema de ficheros se distribuye entre todos los discos sin redundancia, por lo que cuando uno de ellos falla se pierde una parte muy importante de los datos.

Con un RAID 0, si todos los sectores accedidos están en el mismo disco, entonces el tiempo de búsqueda será el de dicho disco. Si los sectores a acceder están distribuidos equitativamente entre los discos, entonces el tiempo de búsqueda aparente estará entre el más rápido y el más lento de los discos del conjunto, pues todos los discos necesitan acceder a su parte de los datos antes de que la operación pueda completarse.

Una desventaja clara es que esto podría llevar a tiempos de búsqueda cercanos al peor escenario para un único disco, salvo si los discos giran sincronizadamente, lo que daría tiempos de búsqueda sólo ligeramente superiores al de un único disco. La velocidad de transferencia del conjunto será la suma de la de todos los discos, limitada sólo por la velocidad de la controladora RAID.

El RAID 0 es útil:

Para configuraciones tales como servidores NFS de solo lectura en las que montar muchos discos es un proceso costoso en tiempo y la redundancia es irrelevante.

- Cuando el número de discos está limitado por el sistema operativo: por ejemplo, en Microsoft Windows el número de unidades lógicas (letras) está limitado a 24, por lo que el RAID 0 es una forma de usar más discos (en Windows 2000 Professional y posteriores es posible montar particiones en directorios, de forma parecida a Unix, eliminando así la necesidad de asignar una letra a cada unidad).

El RAID 0 es una opción popular para sistemas destinados a juegos en los que se desea un buen rendimiento y la integridad no es muy importante, si bien el coste es una preocupación para la mayoría de los usuarios. La Figura 2.1 muestra el diagrama de una configuración RAID 0.

a.2 Concatenación

La concatenación de discos es también llamada JBOD (Just a Bunch Of Drives) que significa "sólo un montón de discos'. La concatenación no es uno de los niveles RAID numerados, pero sí es un método popular de combinar múltiples discos duros físicos en un solo disco virtual. Como su nombre indica, los discos son meramente concatenados entre sí, de forma que se comporten como un único disco.

La concatenación puede ser definida cómo al proceso contrario al particionado, es

decir, mientras el particionado toma un disco físico y crea dos o más unidades lógicas, JBOD usa dos o más discos físicos para crear una unidad lógica. Al consistir en un conjunto de discos independientes (sin redundancia), puede ser visto como un primo lejano del RAID 0. JBOD es usado a veces para combinar varias unidades pequeñas (obsoletas) en una unidad mayor con un tamaño útil.

JBOD puede ser comparado al gestor de volúmenes lógicos LVM (logical ⊐olumen manager) y LSM (Living Stream Media) en los sistemas Unix. JBOD es útil para sistemas que no soportan LVM/LSM cómo Microsoft Windows. Sin embargo Windows 2003 Server, Windows XP Pro y Windows 2000 soportan JBOD vía software, a lo que se le llama spanning de discos dinámicos. La diferencia entre JBOD y LVM/LSM es que la traducción de la dirección lógica del dispositivo concatenado a la dirección física del disco es realizada por el hardware RAID en el primer caso y por el núcleo en el segundo.

Una ventaja de JBOD sobre RAID 0 es que, en caso de fallo de un disco, en RAID 0 suele producirse la pérdida de todos los datos del conjunto, mientras en JBOD sólo se pierden los datos del disco afectado, conservándose los de los restantes discos. Sin embargo, JBOD no supone ninguna mejora de rendimiento. En la Figura 2.2 puede verse un diagrama de la configuración JBOD.

a.3 RAID 1 o Data Mirroring

Un RAID 1 crea una copia exacta (o espejo) de un conjunto de datos en dos o más discos. Esto resulta útil cuando el rendimiento en lectura es más importante que la capacidad. Un conjunto RAID 1 sólo puede ser tan grande como el más pequeño de sus discos. Un RAID 1 clásico consiste en dos discos en espejo, lo que incrementa exponencialmente la fiabilidad respecto a un solo disco; es decir, la probabilidad de fallo del conjunto es igual al producto de las probabilidades de fallo de cada uno de los discos (pues para que el conjunto falle es necesario que lo hagan todos sus discos).

Adicionalmente, dado que todos los datos están en dos o más discos, con hardware habitualmente independiente, el rendimiento de lectura se incrementa aproximadamente como múltiplo lineal del número del copias; es decir, un RAID 1 puede estar leyendo simultáneamente dos datos diferentes en dos discos diferentes, por lo que su rendimiento se duplica. Para maximizar los beneficios sobre el rendimiento del RAID 1 se recomienda el uso de controladoras de disco independientes, una para cada disco (denominada también splitting o duplexing).

Igual que en el RAID 0, el tiempo medio de lectura se reduce, ya que los sectores a buscar pueden dividirse entre los discos, bajando el tiempo de búsqueda y subiendo la tasa de transferencia, con el único límite de la velocidad soportada por la controladora RAID. Sin embargo, muchas tarjetas RAID 1 IDE antiguas leen sólo de un disco de la

pareja, por lo que su rendimiento es igual al de un único disco. Algunas implementaciones RAID 1 antiguas también leen de ambos discos simultáneamente y comparan los datos para detectar errores. La detección y corrección de errores en los discos duros modernos hacen esta práctica poco útil.

Al escribir, el conjunto se comporta como un único disco, dado que los datos deben ser escritos en todos los discos del RAID 1. Por tanto, el rendimiento no mejora.

El RAID 1 tiene muchas ventajas de administración. Por ejemplo, en algunos entornos 24x7, es posible "dividir el espejo", es decir, marcar un disco como inactivo, hacer una copia de seguridad de dicho disco y luego "reconstruir" el espejo. Esto requiere que la aplicación de gestión del conjunto soporte la recuperación de los datos del disco en el momento de la división. Este procedimiento es menos crítico que la presencia de una característica de "snapshot" en algunos sistemas de ficheros, en la que se reserva algún espacio para los cambios, presentando una vista estática en un punto temporal dado del sistema de ficheros. Alternativamente, un conjunto de discos puede ser almacenado de forma parecida a como se hace con las tradicionales cintas. En la Figura 2.3 se observa un diagrama de una configuración RAID 1.

Nota:
Es una copia de un conjunto de datos (imagen) tal cómo se encontraban en un instante en particular.

a.4 RAID 5

Un RAID 5 usa división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos miembros del conjunto. El RAID 5 ha logrado popularidad gracias a su bajo coste de redundancia. Generalmente, el RAID 5 se implementa con soporte hardware para el cálculo de la paridad.

Cada vez que un bloque de datos se escribe en un RAID 5, se genera un bloque de paridad dentro de la misma división (llamado stripe). Un bloque se compone a menudo de muchos sectores consecutivos de disco. Una serie de bloques (un bloque de cada uno de los discos del conjunto) recibe el nombre colectivo de división (stripe). Si otro bloque, o alguna porción de un bloque, es escrita en esa misma división, el bloque de paridad (o una parte del mismo) es recalculada y vuelta a escribir. El disco utilizado por el bloque de paridad está escalonado de una división a la siguiente, de ahí el término "bloques de paridad distribuidos". Las escrituras en un RAID 5 son costosas en términos de operaciones de disco y tráfico entre los discos y la controladora.

Los bloques de paridad no se leen en las operaciones de lectura de datos, ya que esto sería una sobrecarga innecesaria y disminuiría el rendimiento. Sin embargo, los bloques de paridad se leen cuando la lectura de un sector de datos provoca un error de

CRC. En este caso, el sector en la misma posición relativa dentro de cada uno de los bloques de datos restantes en la división y dentro del bloque de paridad en la división se utilizan para reconstruir el sector erróneo. El error CRC se oculta así al resto del sistema. De la misma forma, si falla un disco del conjunto, los bloques de paridad de los restantes discos son combinados matemáticamente con los bloques de datos de los restantes discos para reconstruir los datos del disco que ha fallado "al vuelo".

Lo anterior se denomina a veces Modo Interino de Recuperación de Datos (Interim Data Recovery Mode). El sistema sabe que un disco ha fallado, pero sólo con el fin de que el sistema operativo pueda notificar al administrador que una unidad necesita ser reemplazada: las aplicaciones en ejecución siguen funcionando ajenas al fallo. Las lecturas y escrituras continúan normalmente en el conjunto de discos, aunque con alguna degradación de rendimiento.

La diferencia entre el RAID 4 y el RAID 5 es que, en el Modo Interno de Recuperación de Datos, el RAID 5 puede ser ligeramente más rápido, debido a que, cuando el CRC y la paridad están en el disco que falló, los cálculos no tienen que realizarse, mientras que en el RAID 4, si uno de los discos de datos falla, los cálculos tienen que ser realizados en cada acceso. El RAID 5 requiere al menos tres unidades de disco para ser implementado. El fallo de un segundo disco provoca la pérdida completa de los datos.

El número máximo de discos en un grupo de redundancia RAID 5 es teóricamente ilimitado, pero en la práctica es común limitar el número de unidades. Los inconvenientes de usar grupos de redundancia mayores son una mayor probabilidad de fallo simultáneo de dos discos, un mayor tiempo de reconstrucción y una mayor probabilidad de hallar un sector irrecuperable durante una reconstrucción. A medida que el número de discos en un conjunto RAID 5 crece, el MTBF (tiempo medio entre fallos) puede ser más bajo que el de un único disco. Esto sucede cuando la probabilidad de que falle un segundo disco en los N-1 discos restantes de un conjunto en el que ha fallado un disco en el tiempo necesario para detectar, reemplazar y recrear dicho disco es mayor que la probabilidad de fallo de un único disco. Una alternativa que proporciona una protección de paridad dual, permitiendo así mayor número de discos por grupo, es el RAID 6.

Algunos vendedores RAID evitan montar discos de los mismos lotes en un grupo de redundancia para minimizar la probabilidad de fallos simultáneos al principio y el final de su vida útil.

Las implementaciones RAID 5 presentan un rendimiento malo cuando se someten a cargas de trabajo que incluyen muchas escrituras más pequeñas que el tamaño de una división (stripe). Esto se debe a que la paridad debe ser actualizada para cada escritura,

lo que exige realizar secuencias de lectura, modificación y escritura tanto para el bloque de datos como para el de paridad. Implementaciones más complejas incluyen a menudo cachés de escritura no volátiles para reducir este problema de rendimiento.

En el caso de un fallo del sistema cuando hay escrituras activas, la paridad de una división (stripe) puede quedar en un estado inconsistente con los datos. Si esto no se detecta y repara antes de que un disco o bloque falle, pueden perderse datos debido a que se usará una paridad incorrecta para reconstruir el bloque perdido en dicha división.

Esta potencial vulnerabilidad se conoce a veces como "agujero de escritura". Son comunes el uso de caché no volátiles y otras técnicas para reducir la probabilidad de ocurrencia de esta vulnerabilidad. En la Figura 2.4 se observa un diagrama de una configuración RAID 4 y en la Figura 2.5 la del RAID 5.

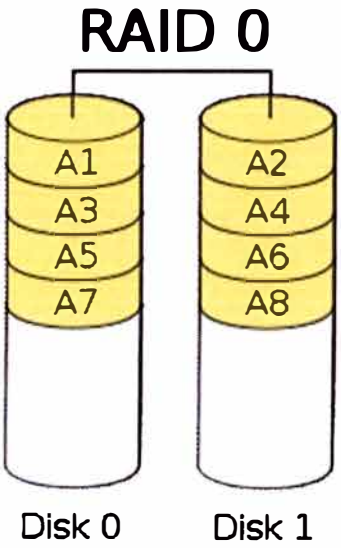


Figura 2.1 Diagrama de configuración RAID 0

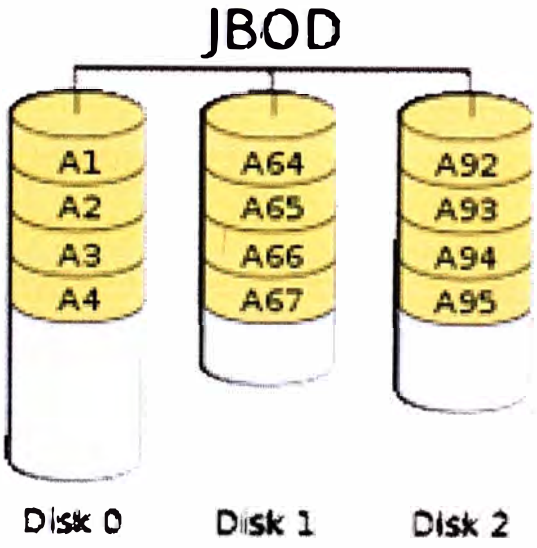


Figura 2.2 Diagrama de una configuración JBOD

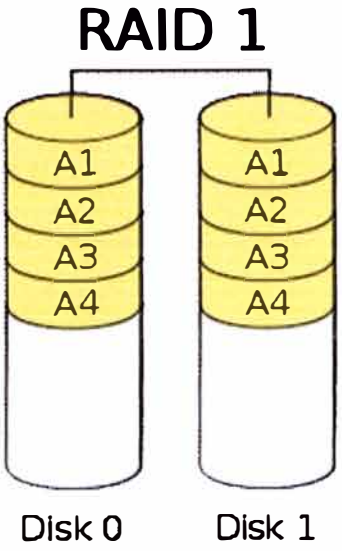


Figura 2.3 Diagrama de una configuración RAID 1

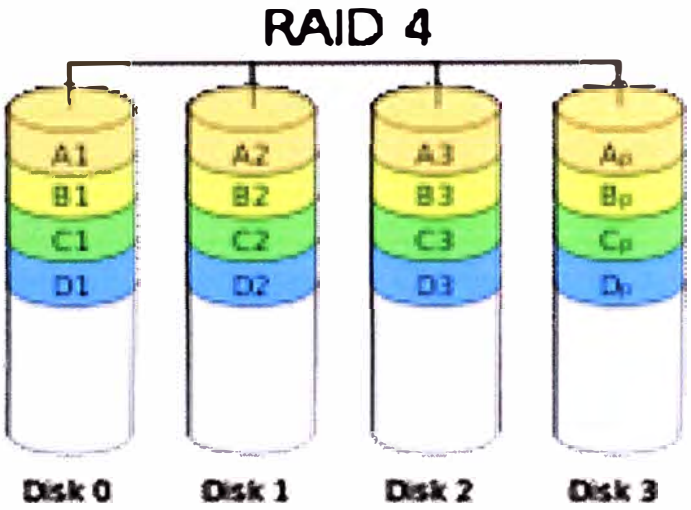


Figura 2.4 Diagrama de una configuración RAID 4

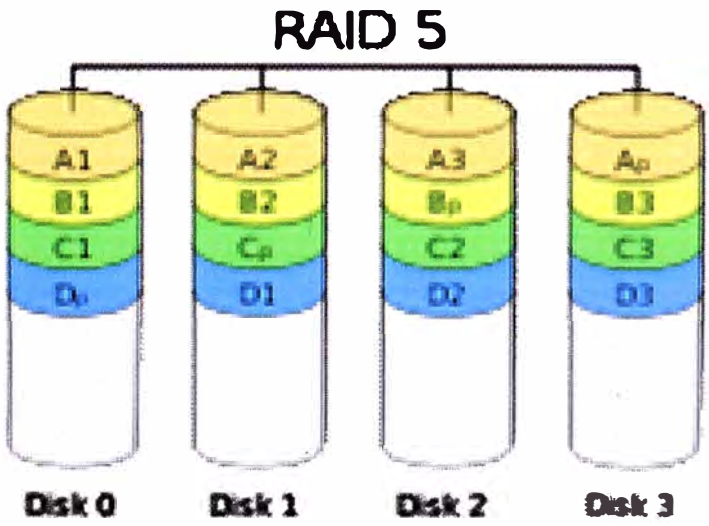


Figura 2.5 Diagrama de una configuración RAID 5

b. Conclusiones del RAID

El RAID puede

- Mejorar el uptime.- Los niveles RAID 1, 0+1 o 10, 5 y 6 (sus variantes, como el 50) permiten que un disco falle mecánicamente y que aun así los datos del conjunto sigan siendo accesibles para los usuarios. En lugar de exigir que se realice una restauración costosa en tiempo desde una cinta, DVD o algún otro medio de respaldo lento, un RAID permite que los datos se recuperen en un disco de reemplazo a partir de los restantes discos del conjunto, mientras al mismo tiempo permanece disponible para los usuarios en un modo degradado. Esto es muy valorado por las empresas, ya que el tiempo de no disponibilidad suele tener graves repercusiones. Para usuarios domésticos, puede permitir el ahorro del tiempo de restauración de volúmenes grandes, que requerirían varios DVD o cintas para las copias de seguridad.

  Mejorar el rendimiento de ciertas aplicaciones.- Los niveles RAID 0, 5 y 6 usan variantes de división (striping) de datos, lo que permite que varios discos atiendan simultáneamente las operaciones de lectura lineales, aumentando la tasa de transferencia sostenida. Las aplicaciones de escritorio que trabajan con ficheros grandes, como la edición de vídeo e imágenes, se benefician de esta mejora. También es útil para las operaciones de copia de respaldo de disco a disco. Además, si se usa un RAID 1 o un RAID basado en división con un tamaño de bloque lo suficientemente grande se logran mejoras de rendimiento para patrones de acceso que implique múltiples lecturas simultáneas (por ejemplo, bases de datos multiusuario).

El RAID no puede

Proteger los datos.- Un conjunto RAID tiene un sistema de ficheros, lo que supone un punto único de fallo al ser vulnerable a una amplia variedad de riesgos aparte del fallo físico de disco, por lo que RAID no evita la pérdida de datos por estas causas. RAID no impedirá que un virus destruya los datos, que éstos se corrompan, que sufran la modificación o borrado accidental por parte del usuario ni que un fallo físico en otro componente del sistema afecten a los datos. RAID tampoco supone protección alguna frente a desastres naturales o provocados por el hombre como incendios o inundaciones. Para proteger los datos, deben realizarse copias de seguridad en medios tales como DVD, cintas o discos duros externos, y almacenarlas en lugares geográficos distantes.

- Simplificar la recuperación de un desastre.- Cuando se trabaja con un solo disco, éste es accesible normalmente mediante un controlador ATA o SCSI incluido en la mayoría de los sistemas operativos. Sin embargo, las controladoras RAID necesitan

controladores software específicos. Las herramientas de recuperación que trabajan con discos simples en controladoras genéricas necesitarán controladores especiales para acceder a los datos de los conjuntos RAID. Si estas herramientas no los soportan, los datos serán inaccesibles para ellas.

- Mejorar el rendimiento de las aplicaciones. Esto resulta especialmente cierto en las configuraciones típicas de escritorio. La mayoría de aplicaciones de escritorio y videojuegos hacen énfasis en la estrategia de buffering y los tiempos de búsqueda de los discos. Una mayor tasa de transferencia sostenida supone poco beneficio para los usuarios de estas aplicaciones, al ser la mayoría de los ficheros a los que se accede muy pequeños. La división de discos de un RAID 0 mejora el rendimiento de transferencia lineal pero no lo demás, lo que hace que la mayoría de las aplicaciones de escritorio y juegos no muestren mejora alguna, salvo excepciones. Para estos usos, lo mejor es comprar un disco más grande, rápido y caro en lugar de dos discos más lentos y pequeños en una configuración RAID 0.
- Facilitar el traslado a un sistema nuevo. Cuando se usa un solo disco, es relativamente fácil trasladar el disco a un sistema nuevo: basta con conectarlo, si cuenta con la misma interfaz. Con un RAID no es tan sencillo: la BIOS RAID debe ser capaz de leer los metadatos de los miembros del conjunto para reconocerlo adecuadamente y hacerlo disponible al sistema operativo. Dado que los distintos fabricantes de controladoras RAID usan diferentes formatos de metadatos (incluso controladoras de un mismo fabricante son incompatibles si corresponden a series diferentes) es virtualmente imposible mover un conjunto RAID a una controladora diferente, por lo que suele ser necesario mover también la controladora. Esto resulta imposible en aquellos sistemas donde está integrada en la placa base. Esta limitación puede obviarse con el uso de RAIDs por software, que a su vez añaden otras diferentes (especialmente relacionadas con el rendimiento).

2.3.3 SAN

Una red SAN se distingue de otros modos de almacenamiento en red por el modo de acceso a bajo nivel. El tipo de tráfico en una SAN es muy similar al de los discos duros como ATA (Advanced Technology Attachment), SATA (Serial Advanced Technology Attachment) y SCSI. En otros métodos de almacenamiento, cómo SMB (Server Message Block) o NFS, el servidor solicita un determinado fichero, por ejemplo: "/home/usuario/rocks".

En una SAN el servidor solicita "el bloque 6000 del disco 4". La mayoría de las SAN actuales usan el protocolo SCSI para acceder a los datos de la SAN, aunque no usen interfaces físicas SCSI. Este tipo de redes de datos se han utilizado y se utilizan

tradicionalmente en grandes main frames como en IBM, SUN o HP. Aunque recientemente con la incorporación de Microsoft se ha empezado a utilizar en máquinas con sistemas operativos Microsoft.

2.3.4 Servidores Integrity

Es una nueva tecnología de servidores corporativos de HP. Posee grandes mejoras en hardware y software cómo el doble núcleo Intel Itanium 2, el chipset zx2, nuevas funcionalidades de Adaptive Enterprise y una nueva versión de OpenVMS (Sistema de Memoria Virtual). Todo ello constituye un cambio radical en los sistemas empresariales, al lograr unos niveles de protección de la inversión, rendimiento, ahorro, solidez, gestión y relación precio/rendimiento sin igual en el mercado.

El proceso de evolución de HP Integrity comenzó en marzo del 2008, con la inclusión del chipset sx2000 en sus servidores de gama media y alta, y que continuó, en junio, con el lanzamiento de las nuevas capacidades en virtualización, con VSE (Virtual Storage Extended), que permiten escalar servidores, así como mover y migrar máquinas virtuales. HP se encuentra en la quinta generación de HP Integrity".

Una de las novedades que presentan los nuevos servidores HP Integrity es la adopción del doble núcleo de Intel Itanium 2 (Montecito), lo que permite duplicar la escalabilidad hasta 128 núcleos. Esto, junto con el resto de novedades introducidas, ha hecho posible obtener unos resultados espectaculares en distintos benchmarks que se han llevado a cabo, confirmando a estas nuevas soluciones como las más preparadas del mercado para aquellas tareas de máxima exigencia a las que puede enfrentarse un servidor empresarial.

Los nuevos servidores HP Integrity, son el HP Integrity rx3600 y el HP Integrity rx6600, que cuentan con una memoria máxima de 96 y 192 GB, 8 y 16 discos internos, y hasta 80 y 160 máquinas virtuales, respectivamente. Todo ello los convierte en unos servidores ideales para consolidar en múltiples máquinas virtuales los entornos Unix, Windows y Linux, a la vez que ejecutar diferentes tipos de aplicaciones como bases de datos, Business Intelligence, ERP y JAVA.

HP Integrity permite a las empresas disponer en sus CPD de unas ventajas hasta ahora inalcanzables, como un máximo rendimiento para diferentes tipos de tareas, una gestión simplificada de distintos entornos operativos, mayor flexibilidad y un ahorro de hasta un 50% en consumo eléctrico y térmico. Todo ello se traduce en más protección de la inversión y el mejor precio/rendimiento del mercado.

2.4 Redes de datos

La presente sección toca los siguientes temas: 1) Conmutación por paquetes, 2) Redes de Área Local, 3) Redes de Área Extendida, 4) Red Privada Virtual, 5) Capas

modelo OSI y TCP/IP, 6) Ancho de Banda, 7) Protocolos.

2.4.1 Conmutación de paquetes

Existen 2 tipos y son:

- Red conmutadas por paquetes.- En ellas el mensaje a transmitir se divide en pequeños "paquetes" o porciones de mensaje, que pasan a circular por la red de nodo a nodo, pudiendo seguir rutas diferentes. La información se reensambla al llegar al nodo al que el usuario está conectado. Éste es el modo de funcionamiento de las redes de comunicación entre computadoras. Ver Figura 2.6

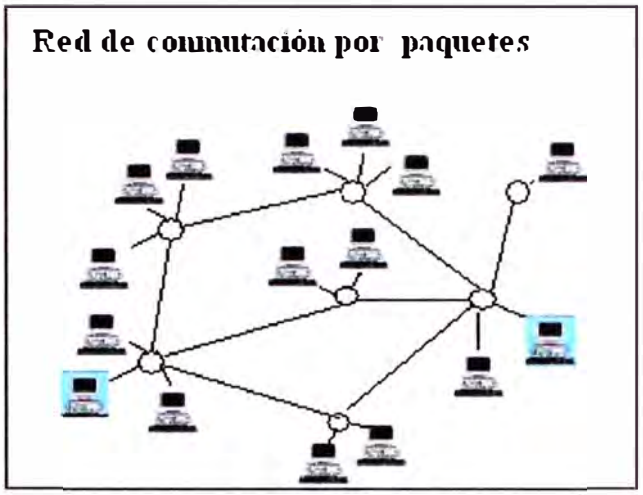


Figura 2.6 Red de conmutación por paquetes

- Red de conmutación de circuitos.- En ellas se establece una trayectoria entre los usuarios, que se mantiene durante el transcurso de la comunicación. En su establecimiento es necesaria una señal que permita que queden reservados los segmentos de la ruta del canal para el par de usuarios. Ejemplo de éste tipo de redes es el de las comunicaciones telefónicas. Ver Figura 2.7.

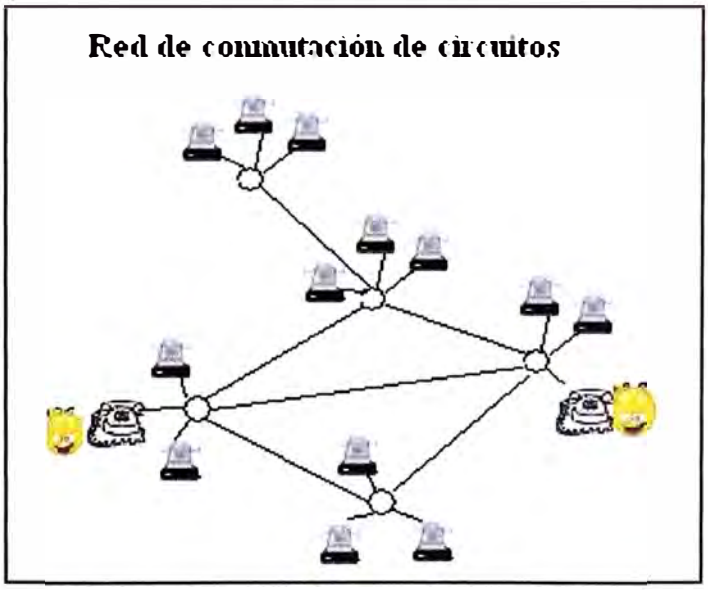


Figura 2.7 Red de conmutación por circuitos

2.4.2 Redes de área local (LAN)

El término Red de área local (LAN) hace referencia a una red local, o a un grupo de redes locales interconectadas, que están bajo el mismo control administrativo. En las primeras épocas del networking, las LAN se definían como pequeñas redes que existían en única ubicación física. A pesar de que las LAN pueden ser una única red local instalada en una vivienda u oficina pequeña, la definición de LAN ha evolucionado y ahora incluye redes locales interconectadas compuestas por muchos cientos de terminales o hosts, instalados en múltiples edificios y ubicaciones. Ver Figura 2.8.

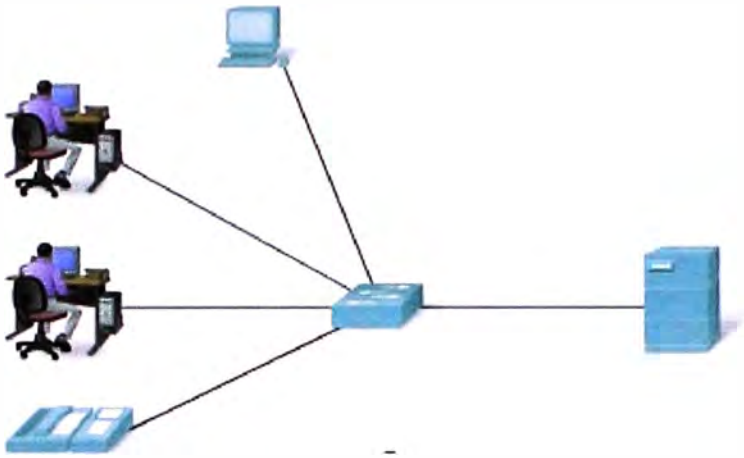


Figura 2.8 Red de área local

2.4.3 Red de área extensa (WAN)

Red que abarca un área geográfica más amplia que una red área local (LAN) sobre redes de comunicaciones públicas. Ver Figura 2.9.

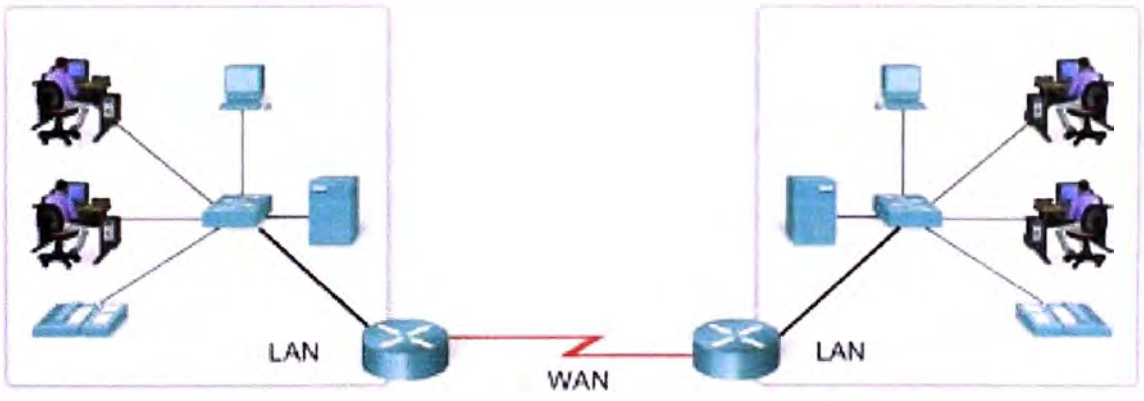


Figura 2.9 Red de área extensa

2.4.4 Red privada virtual (VPN)

Una red privada virtual (VPN) se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo

sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. Ver Figura 2.10.

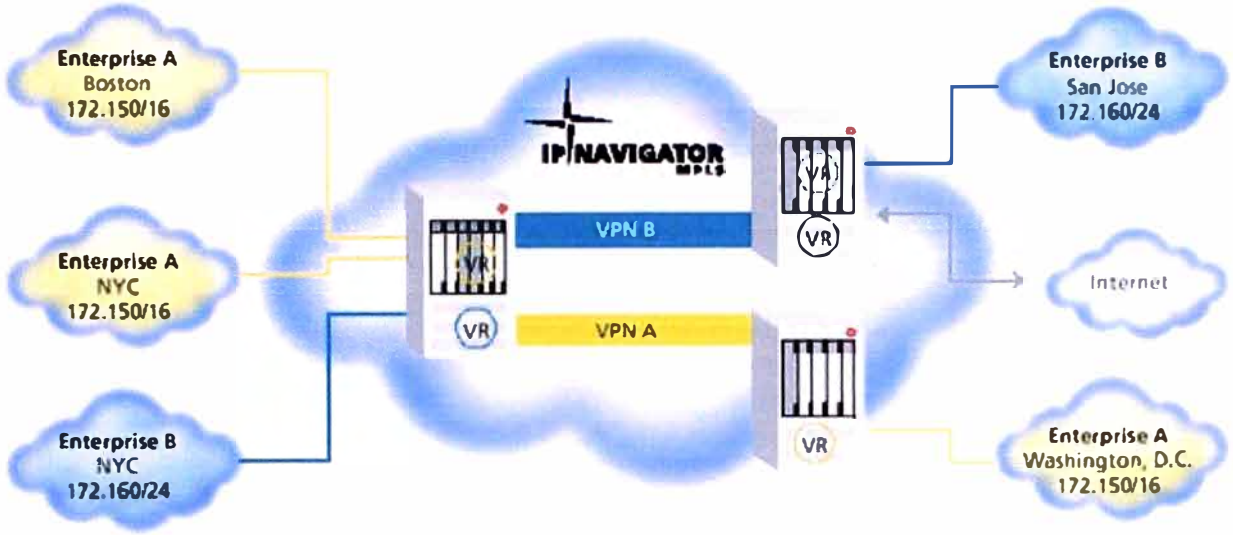


Figura 2.10 Red privada virtual

2.4.5 Capas, Modelo OSI y TCP/IP

El problema de trasladar información entre computadores se divide en problemas más pequeños de tratamiento más simple

a. Modelo de referencia OSI

El modelo de interconexión de sistemas abiertos de sus siglas en inglés (Open System Interconnection), es la propuesta que hizo la Organización Internacional para la Estandarización (ISO) para estandarizar la interconexión de sistemas abiertos.

El modelo de referencia OSI divide el problema en siete problemas más pequeños. Las siete capas del modelo de referencia OSI son:

- Capa 7: La capa de aplicación.- se define como procesos de red a aplicaciones proporciona servicios de red a procesos de aplicación (como correo electrónico, transferencia de archivos y emulación de terminales)
- Capa 6: La capa de presentación .- representación de datos , garantizando que los datos sean legibles para el sistema receptor, formato de datos, estructura de datos, negocia la sintaxis de transferencia de datos para la capa de aplicación.
- Capa 5: La capa de sesión .- comunicación entre terminales, establece, administra y termina sesiones entre aplicaciones.
- Capa 4: La capa de transporte.- conexión de extremo a extremo, se ocupa de aspectos de transporte entre terminales, confiabilidad de transporte de datos, establece mantiene y termina circuitos virtuales, detección y recuperación de falla, control de flujo de información.

- Capa 3: La capa de red .- direccionamiento y mejor ruta, proporciona conectividad y selección de la ruta entre dos sistemas finales, dominio de enrutamiento.
- Capa 2: La capa de enlace de datos .- acceso a los medios, permite la transferencia confiable de los datos a través de los medios, direccionamiento físico, topología de red, notificación de errores, control de flujo.
- Capa 1: La capa física .- transmisión binaria, cables, conectores, voltajes, velocidades de datos

Nota:
Host se refiere a cualquier dispositivo terminal, tal cómo un ordenador, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora.

b. Modelo de referencia TCP/IP

En el modelo del Protocolo de Control de Transmisión/ Protocolo de Internet de sus siglas en inglés (Transmisión Control Protocol/Internet Protocol) el problema se divide en cuatro problemas más pequeños. Las cuatro capas del modelo de referencia TCP/IP son:

- Capa de aplicación:- Los diseñadores de TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación. Simplemente crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y garantiza que estos datos estén correctamente empaquetados para la siguiente capa.
- Capa de transporte.-La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. TCP es un protocolo orientado a la conexión. Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos. Orientado a la conexión no significa que el circuito exista entre los computadores que se están comunicando (esto sería una conmutación de circuito). Significa que los segmentos de Capa 4 viajan de un lado a otro entre dos terminales para comprobar que la conexión exista lógicamente para un determinado período. Esto se conoce como conmutación de paquetes.
- Capa de Internet.-El propósito de la capa de Internet es enviar paquetes origen desde cualquier red en la internetwork y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que recorrieron para llegar hasta allí. El

protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Esto se puede comparar con el sistema postal. Cuando envía una carta por correo, usted no sabe cómo llega a destino (existen varias rutas posibles); lo que le interesa es que la carta llegue.

- Capa de acceso de red.- El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de host a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología LAN y WAN y todos los detalles de las capas física y de enlace de datos del modelo OSI

c. Comparación de los modelos de referencia OSI y TCP/IP

Las diferencias y similitudes se resumen en las siguientes líneas:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación . TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa
- TCP/IP parece ser más simple porque tiene menos capas.
- Los protocolos TCP/IP son los estándares en tomo a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos.

En conclusión las redes típicas no se desarrollan normalmente a partir del protocolo OSI, aunque el modelo OSI se usa como guía. Ver Figura 2.11

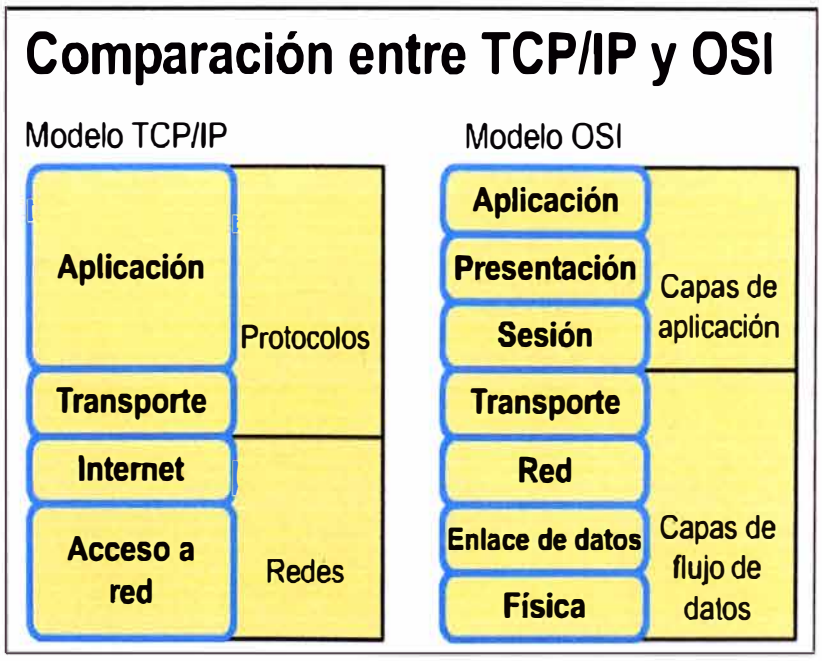


Figura 2.11 Comparacióne entre TCP/IP y OSI

2.4.6 Ancho de Banda

El ancho de banda es un concepto muy importante en los sistemas de comunicaciones. Los más relevantes en el estudio de las LAN son el analógico y el digital.

Generalmente, el ancho de banda analógico se refiere al rango de frecuencias de un sistema electrónico analógico. Este ancho de banda se puede utilizar para describir el rango de frecuencias transmitidas por una emisora de radio o un amplificador electrónico. Las unidades de un ancho de banda analógico son unidades de frecuencia: ciclos por segundo o hertz. Ejemplos de valores de ancho de banda analógico son 3 kiloherz (KHz) en el caso de la telefonía, 20 KHz para las señales de audio, 5 KHz para las emisoras de radio AM y 200 KHz para la FM.

El ancho de banda digital mide la cantidad de información que fluye de un lugar a otro en un tiempo determinado. La unidad básica de medida de los anchos de banda digitales son los bits por segundo (bps). Sin embargo, dado que las LAN son capaces de alcanzar una velocidad de millones de bits por segundo, la unidad representada con mayor frecuencia es de kilobits por segundo (Kbps) o megabits por segundo (Mbps).

Durante un análisis de un cableado, el ancho de banda analógico se utiliza para determinar el ancho de banda digital de un cable de cobre. Las frecuencias analógicas se transmiten desde un extremo y se reciben en el extremo contrario. Entonces se comparan ambas señales y se calcula la cantidad de atenuación de la señal. En general, los anchos de banda digitales soportarán la misma media de los anchos de banda analógicos más altos sin alta graduación de atenuación.

2.4.7 Protocolos

Es un conjunto de reglas usadas por computadoras, para comunicarse unas con otras a través de las redes de comunicación. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

a. Protocolos enrutados

Los protocolos que suministran soporte para la capa de red se denominan protocolos enrutados o enrutables. El protocolo de Internet (IP) es un protocolo de capa de red, y como tal se puede enrutar a través de una rede de trabajo internetwork, que es una red de redes. Otros protocolos enrutados son IPX/SPX y AppleTalk.

Los protocolos pueden se enrutables y no enrutables. Los protocolos cómo, por ejemplo, IP, IPX/SPX y AppleTalk suministran soporte de Capa 3 y, en consecuencia, son enrutables. Sin embargo, hay protocolos que no soportan Capa 3, que se clasifican como protocolos no enrutables. El más común de estos protocolos no enrutables es NetBEUI,

un protocolo pequeño, veloz y eficiente que está limitado a ejecutarse en un segmento.

Para que un protocolo sea enrutable, debe brindar la capacidad para asignar un número de red, así como un número de host, a cada dispositivo individual. Algunos protocolos, tal como el protocolo IPX, sólo necesitan que se le asigne un número de red; estos protocolos utilizan una dirección MAC de host como el número de host. Otros protocolos como, por ejemplo, IP, requieren que se suministre una dirección completa, así como también una máscara de subred. La dirección de red se obtiene mediante una operación AND de la dirección con la máscara de subred.

b. Protocolos de enrutamiento

Los protocolos de enrutamiento determinan las rutas que siguen los protocolos enrutados hacia los destinos. Entre los ejemplos de protocolos de enrutamiento se pueden incluir el Protocolo de Información de Enrutamiento (RIP), el Protocolo de enrutamiento de gateway interior (IGRP), el Protocolo de enrutamiento de gateway interior mejorado (EIGRP) y el Primero la ruta libre más corta (OSPF).

Los protocolos de enrutamiento permiten que los routers conectados creen un mapa interno de los demás routers de la red o de Internet. Esto permite que se produzca el enrutamiento (es decir, la selección de la mejor ruta y conmutación). Estos mapas forman parte de la tabla de enrutamiento de cada router.

Los routers usan protocolos de enrutamiento para intercambiar tablas de enrutamiento y compartir información de enrutamiento. Dentro de una red, el protocolo más común que se usa para transferir la información de enrutamiento entre routers ubicados en la misma red, es el Protocolo de información de enrutamiento (RIP). Este Protocolo de gateway interior (IGP) calcula las distancias hacia un host destino en términos de cuántos saltos (es decir, cuántos routers) debe atravesar un paquete. El RIP permite que los routers actualicen sus tablas de enrutamiento a intervalos programables, generalmente cada 30 segundos. Una de las desventajas de los routers que usan RIP es que constantemente se conectan con los routers vecinos para actualizar sus tablas de enrutamiento, generando así una gran cantidad de tráfico de red.

El Protocolo de Información de Enrutamiento (RIP) permite que los routers determinen cuál es la ruta que se debe usar para enviar los datos. Esto lo hace mediante un concepto denominado vector-distancia. Se contabiliza un salto cada vez que los datos atraviesan un router es decir, pasan por un nuevo número de red, esto se considera equivalente a un salto. Una ruta que tiene un número de saltos igual a 4 indica que los datos que se transportan por la ruta deben atravesar cuatro routers antes de llegar a su destino final en la red. Si hay múltiples rutas hacia un destino, la ruta con el menor número de saltos es la ruta seleccionada por el router.

Cómo el número de saltos es la única métrica de enrutamiento utilizada por el RIP, no necesariamente selecciona la ruta más rápida hacia su destino. La métrica es un sistema de medidas que se utiliza para la toma de decisiones. Muy pronto aprenderá que otros protocolos de enrutamiento utilizan otras métricas, además del número de saltos, para encontrar la mejor ruta a través de la cual se pueden transportar datos. Sin embargo, RIP continúa siendo muy popular y se sigue implementando ampliamente. La principal razón de esto es que fue uno de los primeros protocolos de enrutamiento que se desarrollaron.

Otro de los problemas que presenta el uso del RIP es que a veces un destino puede estar ubicado demasiado lejos como para ser alcanzable. RIP permite un límite máximo de quince para el número de saltos a través de los cuales se pueden enviar datos. La red destino se considera inalcanzable si se encuentra a más de quince saltos de router.

En la capa de enlace de datos, el datagrama IP se encapsula en una trama. El datagrama, incluyendo el encabezado IP, se maneja como si fuera datos. El router recibe la trama, elimina el encabezado de la trama, luego verifica la dirección IP destino del encabezado IP. El router luego busca esa dirección destino en la tabla de enrutamiento, encapsula los datos en una trama de capa de enlace de datos y la envía hacia la interfaz correspondiente. Si no encuentra la dirección IP destino, el router descarta el paquete. Un ejemplo de encapsulación de datos se puede ver en la Figura 2.12.

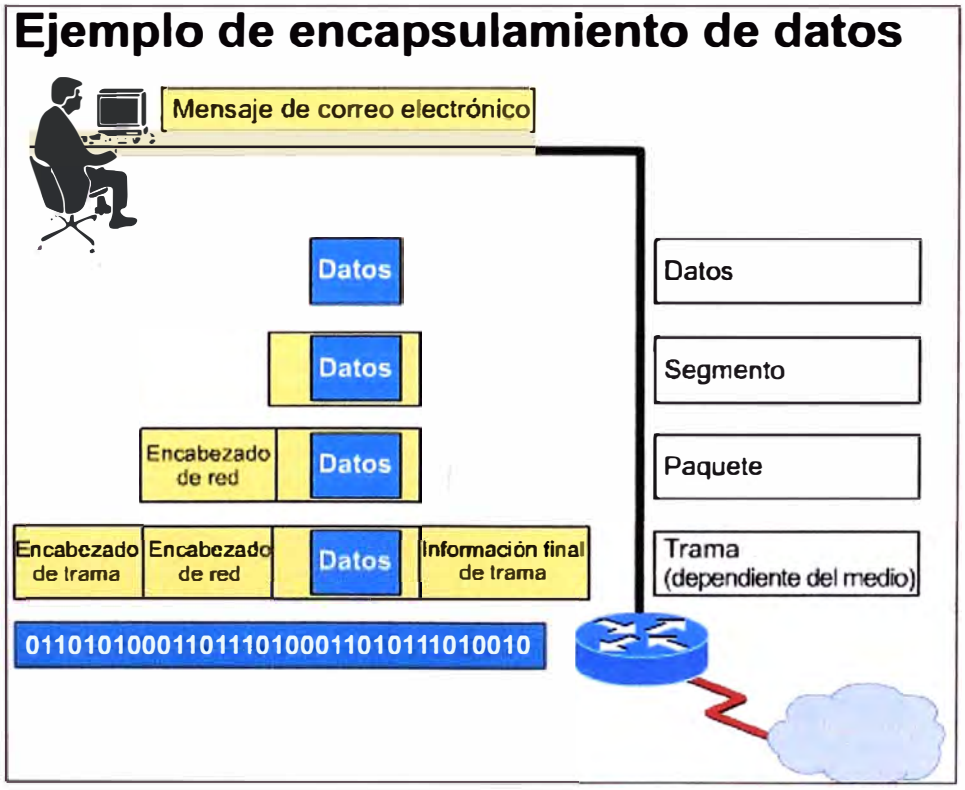


Figura 2.12 Encapsulamiento de datos

Los routers pueden soportar múltiples protocolos de enrutamiento independientes y mantener tablas de enrutamiento para varios protocolos enrutados concurrentemente. Esta capacidad le permite al router entregar paquetes desde varios protocolos enrutados a través de los mismos enlaces de datos. Ver Figura 2.13.

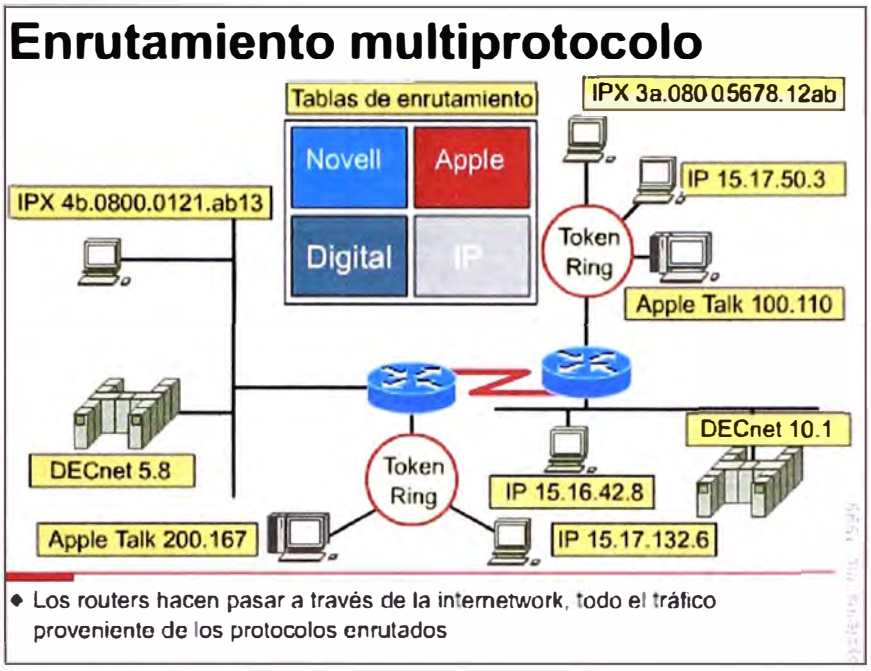


Figura 2.13 Enrutamiento multiprotocolo

2.4.8 Unidades de datos de protocolo

Para que los datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa par en el lugar destino. Esta forma de comunicación se conoce como de par-a-par. Durante este proceso, los protocolos de cada capa intercambian información, denominada unidades de datos de protocolo (PDU). Cada capa de comunicación en el computador origen se comunica con un PDU específico de capa, y con su capa par en el computador destino.

Los paquetes de datos de una red parten de un origen y se envían a un destino. Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego le puede agregar cualquier encabezado e información final que la capa necesite para ejecutar su función. Posteriormente, a medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, se agregan encabezados e información final adicionales. Después de que las Capas 7, 6 y 5 han agregado su información, la Capa 4 agrega más información.

La PDU de la capa 4 se denomina segmento, la de la capa 3 se denomina paquete, la de la capa 2 se denomina trama y la de la capa 1 sólo bits. Ver Figura 2.14.

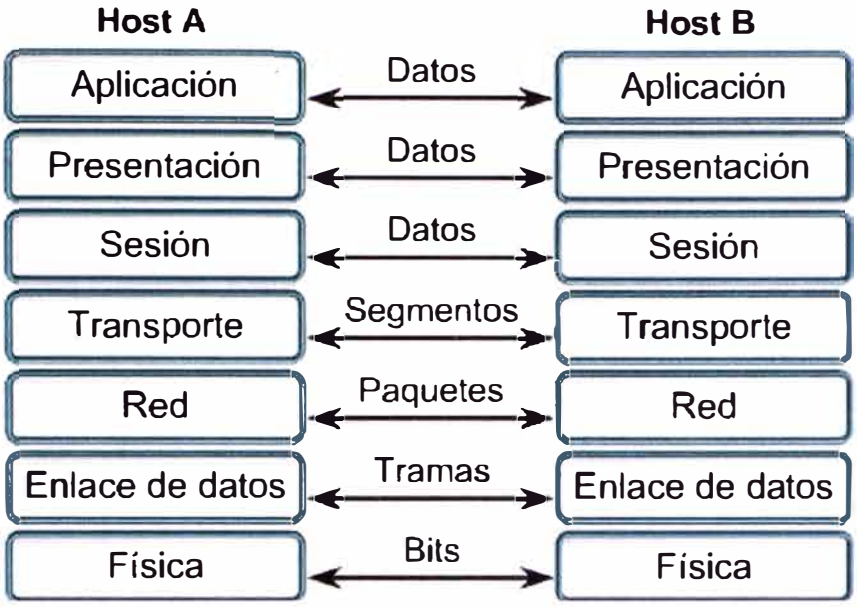


Figura 2.14 PDU de cada capa del modelo OSI

2.5 Estándar de Fibre Channel

Es un estándar que pretende ser abierto y que permite la interacción de los dispositivos y componentes de distintos fabricantes. Está específicamente diseñado para la interconexión de dispositivos de almacenamiento, por lo que trata de aunar las ventajas de una red con las de un canal de datos tradicional. El encargado de redactar este estándar es el comité t11 de la ANSI American National Standards Institute, que por otra parte también se encarga del estándar SCSI en su comité t10.

A continuación se explicaran una serie de conceptos relacionados con el estándar: Los niveles del estándar Fibre Channel, las topologías de redes y las clases de servicio.

2.5.1 Niveles del estándar Fibre Channel

Se dividen en niveles físicos y niveles superiores.

a. Niveles físicos (FC-PH)

Existen tres niveles físicos:

- FC-0 - Interconexiones físicas y velocidades de transmisión. Este nivel define los conectores, transmisores, receptores y cableado. Define conexiones vía cobre y fibra óptica multimodo o monomodo, con distancias de hasta 30m para el cobre y 10 km para la fibra. Se define una velocidad de transmisión de 100MBps full-duplex, aunque se trabaja en ampliaciones del estándar para velocidades más altas.
- FC-1 - Esquemas de codificación para la transmisión. Este nivel y el anterior es en muchos aspectos equivalente al nivel físico de la especificación Gigabit Ethernet.
- FC-2 - Define el control del flujo y el formato de la trama FC, cuyo tamaño es 2K. en esta capa se definen las distintas topologías que pueden presentarse en un puerto Fibre Channel.

b. Niveles superiores

Se consideran el FC-3 y el FC-4:

- FC-3 - Servicios comunes para los nodos. Se implementa en los conmutadores de la red.
- FC-4 - Define el interfase con los protocolos superiores que van a ser transportados por la red Fibre Channel. Estos protocolos pueden ser de red, por ejemplo IP, o de canal de datos, por ejemplo SCSI.

2.5.2 Topologías de red

La interconexión de los nodos de una red Fibre Channel se realiza mediante tres topologías físicas:

- Punto a punto.- Conexión única entre dos nodos. Todo el ancho de banda es usado por estos dos nodos.
- Bucle arbitrado.- En esta topología el ancho de banda es compartida entre todos los nodos conectados al bucle. Para la conexión de todos los dispositivos de un bucle se utilizan hasta un total de 127 concentradores (hubs).
- Conmutado.- Permite múltiples conexiones concurrentes entre todos los nodos conectados a un conmutador o redde conmutadores (Fabric)

2.5.3 Clases de servicio

El estándar Fibre Channel define diferentes clases de servicio para las comunicaciones entre nodos, que se establecen para cada conexión según las necesidades de la misma a través de unos protocolos de negociación definidos entre los nodos y los elementos de la red.

- Clase 1.- Conexión dedicada a través de la red equivalente a un enlace físico.
- Clase 2.- Sin conexión pero con garantía de entrega de las tramas.
- Clase 3.- Sin conexión y sin garantía de entrega. El flujo se controla en las capas superiores.
- Clase 4.- Servicio orientado a la conexión pero con sólo un mínimo de ancho de banda garantizado.
- Clase 5.- Servicio isócrono. No utilizado.
- Class 6.- Servicio multicast con conexión. El hardware existente en el mercado implementa principalmente las clases 2 y 3.

CAPÍTULO III
INGENIERÍA DEL PROYECTO

La ingeniería del proyecto se describe en dos partes: La conectividad, y los elementos básicos del servicio en las CPD.

3.1 Conectividad

Las CPD no sólo se encuentran ubicados en nodos red sino que también se encuentran integrados a la red IP/MPLS. Esto se traduce en:

- Los nodos de core (núcleo) de la plataforma de comunicaciones del CPD del emplazamiento principal es parte de la Red IP/MPLS y se encuentra con un esquema de redundancia intemodal.
- Facilidad de acceso a diferentes redes de comunicaciones.
- Alta disponibilidad en la conexión a la red mediante la provisión de doble enlace hacia equipos redundantes.
- Menor tiempo de atención de requerimientos de provisión.
- Menores costos de habilitación de servicio.

En la Figura 3.1 se muestra el esquema de conectividad del CPD.

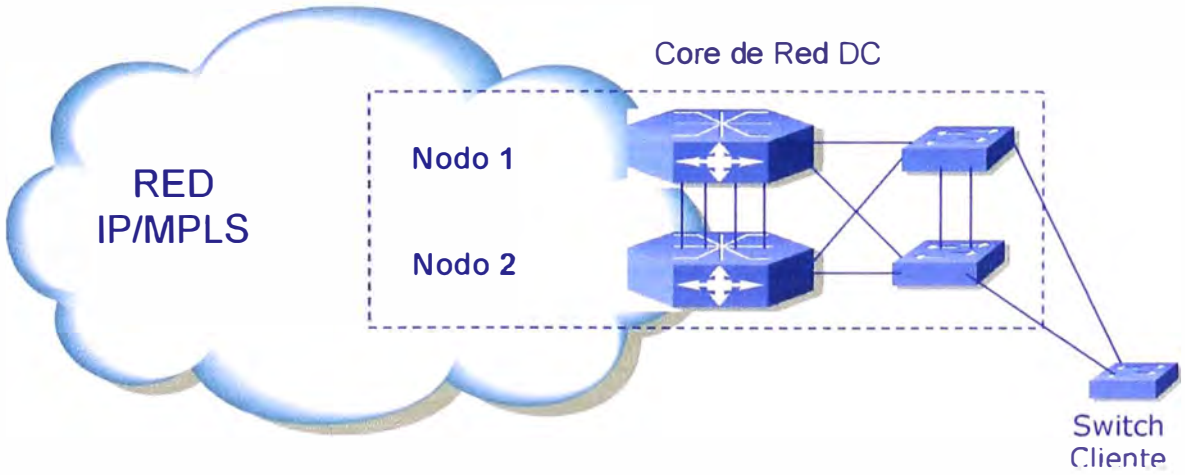


Figura 3.1 Esquema de conectividad de la CPD (Emplazamiento Principal).

MPLS es una nueva tecnología de conmutación creada para proporcionar circuitos virtuales en las redes IP. La migración a IP está provocando profundos cambios en el sector de las telecomunicaciones, inmersos actualmente en un proceso de transformación de sus infraestructuras de cara a incorporar los beneficios de esta tecnología.

MPLS nació con el fin de incorporar la velocidad de conmutación del nivel 2 al nivel 3; a través de la conmutación por etiqueta; pero actualmente esta ventaja no es percibida como el principal beneficio, ya que los gigarouters son capaces de realizar búsquedas de rutas en las tablas IP a suficiente velocidad como para soportar todo tipo de interfaces.

Los beneficios que MPLS proporciona a las redes IP son: realizar ingeniería del tráfico o TE (Traffic Engineering), cursar tráfico con diferentes calidades de clases de servicio o CoS (Class of Service) o grados de calidad de servicio o QoS (Quality of Service), y crear redes privadas virtuales o VPN (Virtual Private Networks) basadas en IP.

La TE permite a los ISP mover parte del tráfico de datos, desde el camino más corto calculado por los protocolos de encaminamiento, a otros caminos físicos menos congestionados o menos susceptibles a sufrir fallos. Es decir, se refiere al proceso de seleccionar los caminos que seguirá el flujo de datos con el fin de balancear la carga de tráfico entre todos los enlaces, routers y switches en la red; de modo que ninguno de estos recursos se encuentre infrautilizado o sobrecargado. La TE, descrita en la RFC 2702, se ha convertido en la principal aplicación de MPLS debido al crecimiento impredecible en la demanda de recursos de red.

Mediante MPLS, los ISP pueden soportar servicios diferenciados o DiffServ, como viene recogido en la RFC 3270. El modelo DiffServ define varios mecanismos para clasificar el tráfico en un pequeño número de CoS. Los usuarios de Internet demandan continuamente nuevas aplicaciones, teniendo los servicios actualmente soportados unos requerimientos de ancho de banda y de tolerancia a retrasos en la transmisión muy distintos y para satisfacer estas necesidades óptimamente, los ISP necesitan adoptar no sólo técnicas de ingeniería de tráfico, sino también de clasificación de dicho tráfico. De nuevo, MPLS ofrece a los ISP una gran flexibilidad en cuanto a los diferentes tipos de servicios que puede proporcionar a sus clientes.

Finalmente, MPLS ofrece también un mecanismo sencillo y flexible para crear VPN. Una VPN simula la operación de una WAN (*Wide Area Network*) privada sobre la Internet pública. Para ofrecer un servicio de VPN viable a sus clientes, un ISP debe solventar los problemas de seguridad de los datos y soportar el uso de direcciones IP privadas no únicas dentro de la VPN. Puesto que MPLS permite la creación de circuitos virtuales o túneles a lo largo de una red IP, es lógico que los ISP utilicen MPLS como una forma de aislar el tráfico. No obstante, MPLS no tiene en estos momentos ningún

mecanismo para proteger la seguridad en las comunicaciones, por lo que el ISP deberá conseguirla mediante cortafuegos y algún protocolo de encriptación tipo IPsec. Existen varias alternativas para implementar VPNs mediante MPLS, pero la mayoría se basan en la RFC 2547.

En la Figura 3.2 se muestra como interactúan los distintos servicios en un CPD. En la Figura 3.3 se muestra la interacción de los firewall virtuales. Un Firewall o Cortafuegos es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

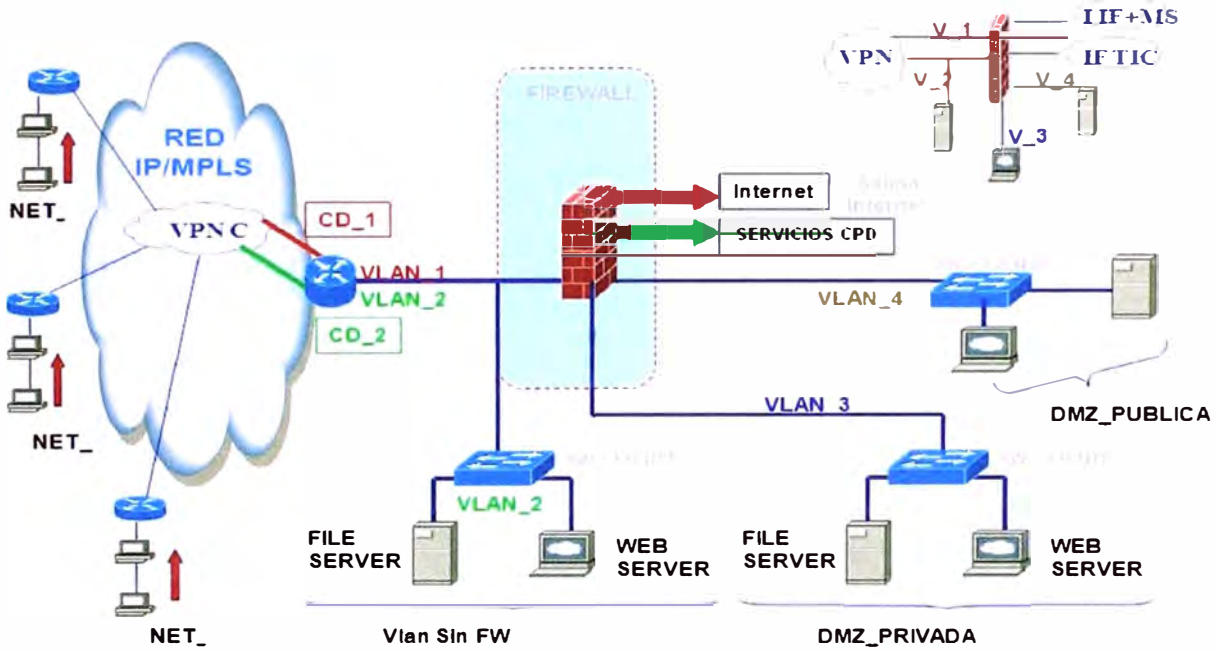


Figura 3.2 Conectividad VPN clientes y sus servicios

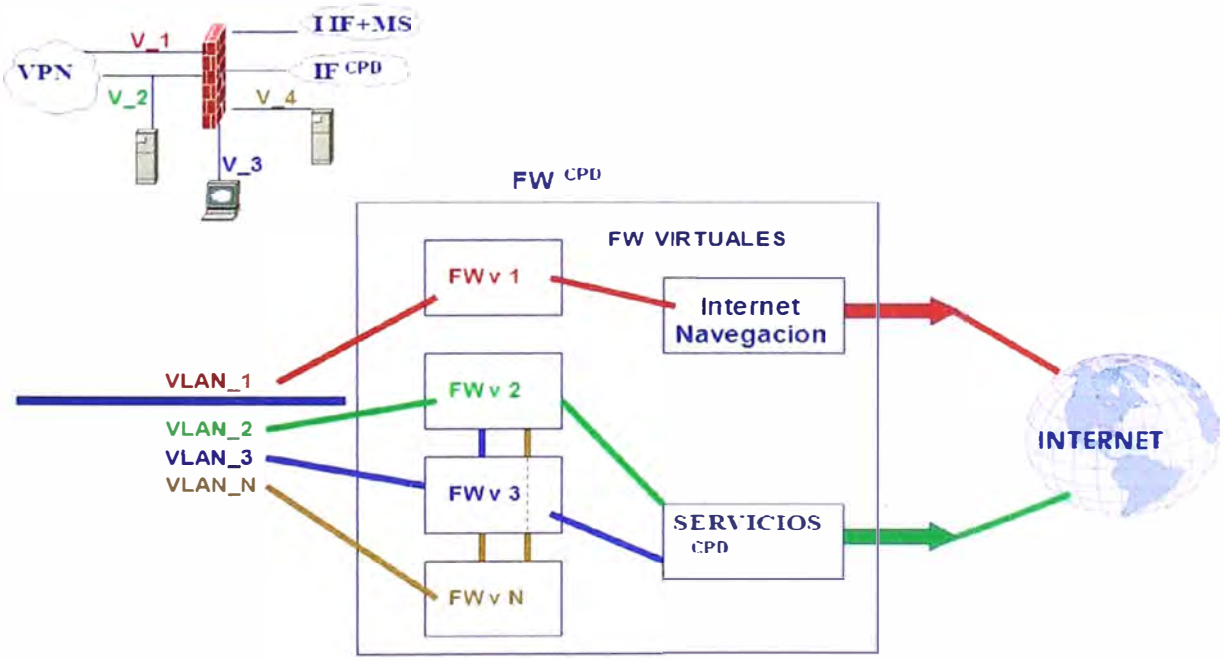


Figura 3.3 Firewall virtual. Interacción con las VLAN

3.2 Elementos básicos del servicio en el CPD

Estos elementos son agrupados en: espacio físico o alojamiento, especificaciones de gabinetes, consumo eléctrico, asignación de puertos, conectividad a Internet, redes de datos IP/MPLS,

3.2.1 Espacio físico o alojamiento

El alojamiento es el espacio físico donde se albergará el equipamiento informático de la solución. La infraestructura que provea la solución, deberá facilitar opciones estándar de mercado y escalables. Esta infraestructura se divide en gabinetes, gabinetes privados, jaulas a medida. Adicionalmente se contempla la reservación de gabinetes y espacio físico para soluciones que requieran ampliar el espacio físico inicial.

a. Especificaciones de gabinetes

Espacio modular para soluciones con pequeñas necesidades de espacio, los equipos estarán montados en gabinetes, con armaduras de aluminio. Cada Gabinete incluye puertas (con llave) y ventilación. El servicio se brinda en función de las "U" requeridas por el solución, estableciéndose así opciones de ¼ de gabinete, ½ gabinete, 1 o más gabinetes. Un gabinete se compone de 40 "U".

Esta opción permite la colocación de mini torres, torres etc. (mediante bandejas) Los servidores en configuración de mini torres y torres serán evaluados para el servicio en función del número de unidades de gabinete que ocupen ellos y la bandeja que sea requerida para soportarlos en el gabinete.

Las siguientes son las características de un gabinete estándar:

- U de Gabinete 40 U
- Ancho 670mm
- Largo 650mm
- Alto 2140mm
- Voltaje 220V
- Amperaje 10A
- Puertos Red 2

Nota:
U es la unidad de medida establecida para describir la altura del equipamiento preparado para se montado en el Gabinete, una unidad equivale a 44.45 cm.

3.2.2 Consumo eléctrico

Los gastos de suministro eléctrico están incluidos dentro del servicio de tercerización y estarán definidos en función del consumo de los equipos instalados en el espacio asignado al cliente. Al momento de elaboración de la solución estos valores serán estimados en función de los datos provistos por el fabricante, los cuales serán

revisados en el momento de la implantación a fin de realizar los ajustes necesarios.

Las CPD se reservan el derecho de realizar mediciones periódicas de este consumo a fin de realizar los ajustes correspondientes.

3.2.3 Conectividad

Se explica mediante tres aspectos fundamentales: la asignación de puertos, la conectividad a Internet y las redes de datos IP/MPLS.

a. Asignación de puertos

Cada solución proveerá 02 puertos de red en equipos redundantes de acceso para asegurar la redundancia de conectividad a la red. Se proveerá troncal (trunk) para el acceso a las diferentes VLANs (redes virtuales) del servicio necesarias para atender la solución/servicio/plataforma del cliente. Si la solución diseñada requiere conectividad a más de dos servidores (cada servidor con 1 puerta de red) se deberá incluir un switch LAN, el que podrá ser provisto como parte del servicio.

Nota:
VLAN significa Red de Área Local Virtual. Es un método de crear redes lógicas independientes dentro de una misma red física
Trunk se refiere a troncal. Designa una conexión de red que transporta múltiples VLANs identificadas por etiquetas (o *tags*) insertadas en sus paquetes.

b. Conectividad a Internet

Esta opción en la soluciones no proporciona navegación hacia Internet sino visibilidad en Internet a los servidores alojados en los CPD. En las soluciones se define un ancho de banda bidireccional en función de sus necesidades vistas, éste estará garantizado por los CPD.

c. Redes de datos: IP / MPLS

La conectividad a través de la red IP/MPLS hace que los equipos alojados en los CPD sean parte integrante de la VPN de la solución. En el Anexo C se muestra el diagrama funcional de los distintos servicios del CPD.

3.2.4 Seguridad lógica

La seguridad lógica es provisionada en firewalls virtuales sobre cada una de las vlans solicitadas en la solución para la segmentación de servicios, conectividad VPN y conectividad para publicación a Internet de servidores.

Los firewalls se encuentran integrados al core de la red del CPD y por lo tanto están una configuración de alta disponibilidad que permite asegurar la continuidad del servicio. No es posible la comunicación de una VLAN con otra si no es a través de sus respectivos firewalls virtuales, los cuales a su vez permite configurar las políticas de seguridad que requiera la solución sin interferir con las otras VLAN.

3.2.5 Facilidades de acceso a los CPD

Los soluciones que se encuentren en los CPD, tendrán todas las facilidades de ingreso en horario 24x7x365 ya sea para personal propio o terceros (proveedores), siempre y cuando se cumpla lo estipulado en el procedimiento de ingreso.

Las facilidades de ingreso al CPD pueden darse por dos motivos:

- Trabajos programados: empresas contratantes tendrán que canalizar su requerimiento a través de su gestor comercial y/o de servicio en horario 8x5.
- Atención de incidencias: Para este caso el procedimiento de ingreso contempla la posibilidad que los contratantes canalicen su requerimiento en horario 24x7. Para esto el contratante designará a dos personas responsables de gestionar y autorizar el ingreso a través del pool de operadores, quienes atenderán las solicitudes y gestionarán la autorización de ingreso en forma inmediata.

El procedimiento de ingreso forma parte de los anexos del Libro de Operaciones que es parte de la documentación entregada al final de la implantación del proyecto y que se detalla más adelante.

Los CPD también cuentan con posiciones de trabajo temporal, ubicadas en la zona externa para los casos en los cuales los clientes requieran contar con esta facilidad, de tal forma que puedan operar sus equipos a través de la red LAN. El cliente, en función de sus necesidades puede contratar de manera adicional las posiciones que requiera.

3.2.6 Alcance del servicio de respaldo en los CPD

El Servicio de Backup & Restore permite programar de manera automatizada y centralizada todas las tareas de respaldo para ambientes UNIX, Windows y Linux. Los principales beneficios de este servicio son los siguientes:

- Administración Centralizada de backup multiplataforma.
- Ejecución de Backups automatizados.

El servicio se despliega bajo 3 tipos de respaldo y que son descritos en la Tabla 3.1

Tabla 3.1 Tipos de respaldo:

Tipo de Backup	Archivos Respaldados	Características
Full o completo	Todos	Se respalda la totalidad de la información
Incremental	Aquellos que hayan cambiado o sido creados luego del último respaldo Full o incremental	Los archivos a respaldar son menos y por lo tanto su ejecución es más rápida
Diferencial	Aquellos que hayan cambiado o sido creados luego del último respaldo Full	El proceso de backup es mayor que en el incremental pero el restore es más rápido por requerirse solo el último full y el último diferencial

Estos tipos de backup se configuran de acuerdo a la política de backup definidas con el contratante. En el Anexo D se muestra la arquitectura de la solución

3.2.7 Alcance del servicio de gestión

Para la gestión de los servicios se emplean herramientas especializadas para este fin. El alcance de estas herramientas se enumera a continuación y se agrupan en:

a. Gestión de sistema operativo Windows

Para analizar las incidencias, minimizar el impacto adverso de incidentes, prevenir la recurrencia de incidentes, revisar la capacidad de discos de los servidores, revisar el consumo de recursos de los servidores, para la revisión de registros de eventos del sistema y aplicaciones, la revisión de registros de eventos de seguridad, la actualización de parches de seguridad, la gestión de configuraciones de red del servidor, la instalación de software, la gestión de los servicios nativos del sistema operativo, la gestión de la seguridad servicios nativos del sistema operativo, la gestión de usuarios, grupos, roles y políticas de seguridad; para los procesos de backup, para la gestión del active directory, instalación/reinstalación del sistema operativo, etc.

b. Gestión de sistema operativo Linux

Se encarga del análisis de incidencias, minimizar el impacto adverso de incidentes, prevenir la recurrencia de incidentes, revisar la capacidad de discos de los servidores, revisar el consumo de recursos de los servidores, la revisión del registro de eventos del sistema y aplicaciones, actualización de aplicaciones nativas, gestión de configuraciones de red del servidor, instalación de software, gestión de los servicios nativos del sistema operativo, gestión de la seguridad servicios nativos del sistema operativo, control de políticas de acceso al servidor, la gestión de usuarios, grupos, roles y políticas de seguridad, los procesos de backup, la gestión de servicios de red, la instalación/reinstalación del sistema operativo, etc.

c. Gestión de sistema operativo UNIX

Se ocupa del análisis de incidencias, de minimizar el impacto adverso de incidentes, prevenir la recurrencia de incidentes, revisar la capacidad de discos de los servidores, revisar el consumo de recursos de los servidores, de la revisión del registro de eventos del sistema y aplicaciones, actualizar las aplicaciones nativas, actualizar el sistema operativo, de la gestión de configuraciones de red del servidor, la instalación de software, la gestión de la seguridad servicios nativos del sistema operativo, la gestión del registro de eventos del sistema operativo, los procesos de backup, la gestión de servicios de red, la instalación/reinstalación del sistema operativo, la asignación de recursos, la priorización de servicios, etc.

d. Gestión de base de datos

Efectúa la instalación/reinstalación de la base de datos, la actualización de parches de seguridad, la integridad o mejora de funcionalidades que publica el fabricante, la revisión de la utilización de recursos de la base de datos y el servidor, tuning de la base de datos, la política de copias de seguridad, backups, gestión de la capacidad de discos, los archivos de daots y del registro e eventos de la base de datos, la revisión del registro de eventos de seguridad y del sistema de base de datos, la actualización de la base de datos, la reorganización de la base de datos, la gestión de incidencias.

e. Gestión servicio SAP Basis

La gestión del SAP Basis (Sistemas, Aplicaciones y Productos) se dividen en: Service Desk, operaciones y soporte. El Service Desk es un proceso que se basa en el modelo ITIL ver Anexo E "Modelo de Gestión ITIL" para mayor detalle. La gestión Service Desk realiza la atención y registro de Incidencias 24 x 7. (nuestra mesa de ayuda recibirá las llamadas registrando la incidencia y proporcionando un numero de ticket para que se puese realizar el seguimiento a la evolución del problema) ; el seguimiento de las Incidencias (Ticket registrados por Service Desk) hasta su cierre y aprobación, la resolución de Incidencias estándar (procedimientos que puede ejecutar los agentes de Mesa de Ayuda) ; el escalamiento de Incidencias al Operador, Administradores, Especialistas si así requería la incidencia; el manejo de Incidencias informadas por operador. El service desk podrá brindar reportes mensuales de atención de incidencias para verificar el tiempo que demora en resolver los requerimientos.

3.2.8 Documentación

Es parte del proceso de implantación de proyectos, se ejecuta antes del ingreso en producción del servicio. Los siguientes ítems se documentan en el "Libro de Operaciones":

- El alcance técnico del servicio
- Topología
- Hardware
- Software
- Responsabilidades de cada una de las partes
- Proveedores involucrados
- Personas de contacto
- Procedimiento de escalamiento
- Procedimientos operativos
- Políticas de seguridad
- Compromisos (SLAs)

Este documento tiene como finalidad reflejar el estado final de la solución implantada, así como servir de referencia tanto al contratante como al CPD del alcance del servicio a nivel de detalle técnico.

La aceptación del "Libro de Operaciones" de operaciones por parte del contratante y del personal técnico de CPD es un requisito para la puesta en producción del servicio. Esto permite garantizar que existe un claro entendimiento de ambas partes del alcance, así como la conformidad con este alcance.

3.3 Criterios de selección de elementos de la solución

Este sistema se logra mediante un adecuado diseño de los CPD. Los CPD o datacenters están diseñados para cubrir las necesidades de alojamiento, seguridad, conectividad, gestión y operación de los equipos designados a atender los servicios de los sistemas alojados en ellos, permitiéndole así desarrollar y explotar soluciones avanzadas según sus necesidades y requerimientos.

El sistema en general permite a los clientes una gran escalabilidad y fácil adaptación al crecimiento de su negocio, eliminando así posibles problemas de espacio que podrían generar ampliaciones, cuando éstas se realizaran en su domicilio o en un centro no dimensionado de forma adecuada para ello.

El análisis para la selección de los diversos elementos de software y hardware serán organizados de la siguiente manera para una explicación más didáctica y comprensible: 1) CPD, 2) Plataforma común de comunicaciones del CPD, 3)Plataforma específica para el servicio, 4) Actividades de operación..

3.3.1 CPD

Este concepto involucra la alimentación eléctrica y climatización en los ambientes asignados a sistemas críticos dentro del CPD. Esta plataforma cuenta con una disponibilidad estimada de 99.95%.

3.3.2 Plataforma común de comunicaciones del CPD

La conectividad IP es uno de los elementos del servicio, mediante el cual el cliente puede proporcionar visibilidad a los equipos que aloje en el CPD. Esta conectividad debe ser proporcionada a través de una Plataforma Común de Comunicaciones, la cual asegure la máxima escalabilidad en las conexiones de cliente y una total privacidad entre las conexiones de diferentes clientes. Esta plataforma común involucra al sistema de firewalls del CDP así como a la infraestructura de comunicaciones que brinda la integración con la conectividad WAN.

Esta plataforma debe contar con una disponibilidad estimada de 99.95% y no incluye los equipos de comunicación instalados para la solución particular del cliente.

3.3.3 Plataforma específica para el servicio

Los siguientes sn los criterios considerados para la solución de tal manera que el cliente pueda contar con la máxima disponibilidad y calidad de los datos que son almacenados en el sistema de tercerización:

- Disponibilidad de plataforma: 99.7%
- Tiempo de respuesta:
  - 750 ms promedio mensual "dialog step"
  - 900 ms promedio hora pico
- Ejecución de backup y restore: 100%
- Tiempo de ejecución de backups: 200GB/60 minutos
- Tiempo de ejecución de restore: 200GB/90 minutos
- Tiempo de respuesta/solución Soporte Basis de acuerdo a prioridad definida en servicio Basis vigente
  - Atención de Perfiles: 100% dentro de los plazos acordados
  - Atención de Transportes: 100% dentro de los plazos acordados
  - Emisión de Reportes: 100% dentro del plazo acordado
- Plazo de estabilización para acuerdos de nivel de servicio (SLA): Seis meses contados desde la puesta en productivo del R/3.

3.3.4 Actividades de operación

Se consideran actividades de operación a aquellas acciones rutinarias, procedimentadas y de duración acotada (en unidades mínimas 15 minutos) que realizará personal de operación sobre los servidores que se encuentren alojados en el CPD, bajo petición expresa del cliente o bajo programación preestablecida.

A continuación se tipifican las principales operaciones aceptadas en los servicios de tercerización:

- Reinicio de Servidores
- Comprobación de Servicios
- Verificación visual
- Soporte a procesos de Backup, tales como reemplazo de cintas, etc.
- Ejecución de procedimientos

Se define el Tiempo de Ejecución al tiempo transcurrido desde el momento que el cliente solicita la ejecución de una actividad de operación y el momento que se notifica al cliente que esta ha sido realizada.

El Tiempo de Ejecución de las actividades de operación contempladas en el servicio estará comprendido entre 15 y 45 minutos, tiempos mínimo y máximo correspondientemente bajo un esquema 24 x 7. El nivel de cumplimiento se calculará

comparando el tiempo medio de respuesta mensual de todas las operaciones realizadas, con objetivo planteado.

CAPÍTULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

La propuesta técnica que se plasma ahora se explicará a continuación, corresponde a los diferentes componentes considerados para brindar la mejor solución integrada para el Hosting de Aplicaciones

Para tal fin, se hizo uso de la metodología del Project Management Institute (PMI), para identificar y elaborar la propuesta en base a los Entregables del proyecto.

4.1 Estructura detallada del proyecto

Siguiendo la metodología de Gerencia de Proyectos del Project Management Institute (PMI), metodología estándar a nivel mundial, el planteamiento del proyecto va esquematizado por entregables, el mismo al que podrán ser asignados tiempos de ejecución, identificación de riesgos, roles y responsabilidades de los involucrados en el proyecto (Stakeholders).

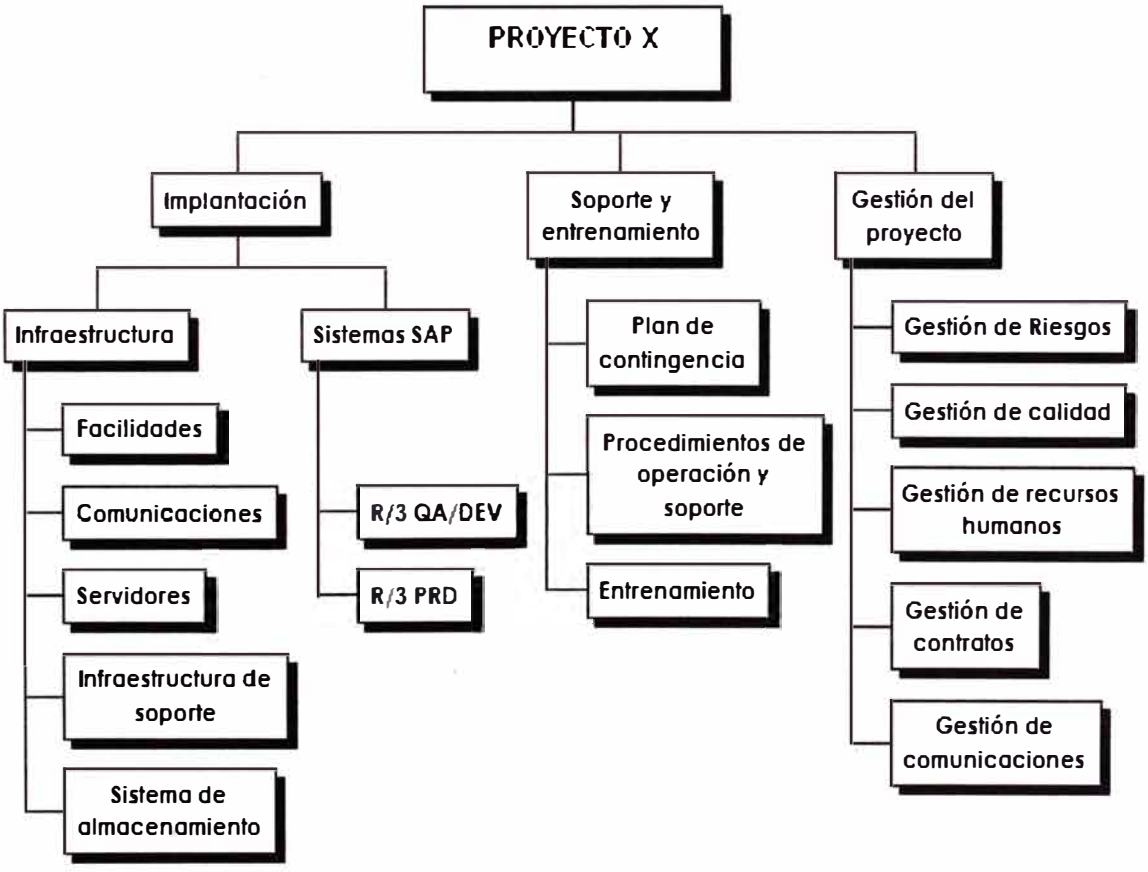


Figura 4.1 Fases para la implementación del proyecto

El proceso de identificar los entregables del proyecto y documentarlos, abordando según la Estructura Detallada del Trabajo (EDT) (en inglés - Work breakdown Structure - WBS), para el proceso de la implementación del servicio, contempla diversas fases a nivel general del proyecto. Ver Figura 4.1.

Cabe indicar que el desarrollo en esta primera parte es a nivel general, para luego describir a un mayor detalle cada uno de los entregables identificados del proyecto.

4.2 Componentes de la Solución

En esta sección se describen los componentes de la solución. Estos son la CPD, el diseño de solución, la conectividad, la seguridad, el hardware, el almacenamiento, y el HP StorageWorks XP Continuous Access.

4.2.1 CPD

La solución contempla la provisión de los bastidores requeridos para instalar la plataforma indicada en el punto 6.3.5. Asimismo, contempla la provisión de todo lo requerido para la instalación eléctrica y de cableado estructurado de datos.

4.2.2 Implementación de la solución

Cómo se ha mencionado hasta el momento, para esta solución se montará sobre los CPD aprovechando la robustez de sus infraestructuras y la confiabilidad de la continuidad de los servicios. A continuación se detallarán, haciendo el uso de ilustraciones, como funciona normalmente la solución y su interacción cuando ocurre un desastre y continúa su funcionamiento.

a. Arquitectura de equipos en CPD principal y secundario

La Figura 4.2 muestra todos los elementos que participan en la solución. En él se pueden destacar los siguientes: Servidores de Aplicaciones uno y Base de Datos (Emplazamiento Principal), Servidor de Aplicaciones 2 y Desarrollo Calidad (Emplazamiento Secundarios) los Storages en cada emplazamiento La IP-VPN . La figura F.1 del Anexo F "Diagramas de funcionamiento de la solución", presenta el diagrama en mayor detalle.

b. Direccionamiento de balanceo normal de la IP-VPN al Emplazamiento Principal

La Figura 4.3 muestra como todos los usuarios de la VPN se conectan de manera normal al servidor de aplicaciones 1 (Ver la línea de color rojo). En la figura F.2 del Anexo F se presenta el diagrama en mayor detalle.

c. Interacción del servidor de Aplicaciones 1 al Servidor de Base de Datos

La Figura 4.4 muestra como el servidor de aplicaciones consulta los datos al servidor de Base de Datos y éste se conecta al storages. Todo esto se realiza en el emplazamiento principal. La figura F.3 del Anexo F presenta el gráfico en mayor detalle.

d. Interacción del Servidor de Aplicaciones 2 al servidor de Base de Datos

La Figura 4.5 muestra como los usuarios se conectan a través de la VPN al servidor de aplicaciones 2 que se encuentra en el emplazamiento secundario y ésta consulta por la red al servidor de Base de Datos que se encuentra en el emplazamiento principal. En la figura F.4 del anexo F se presenta el gráfico en mayor detalle.

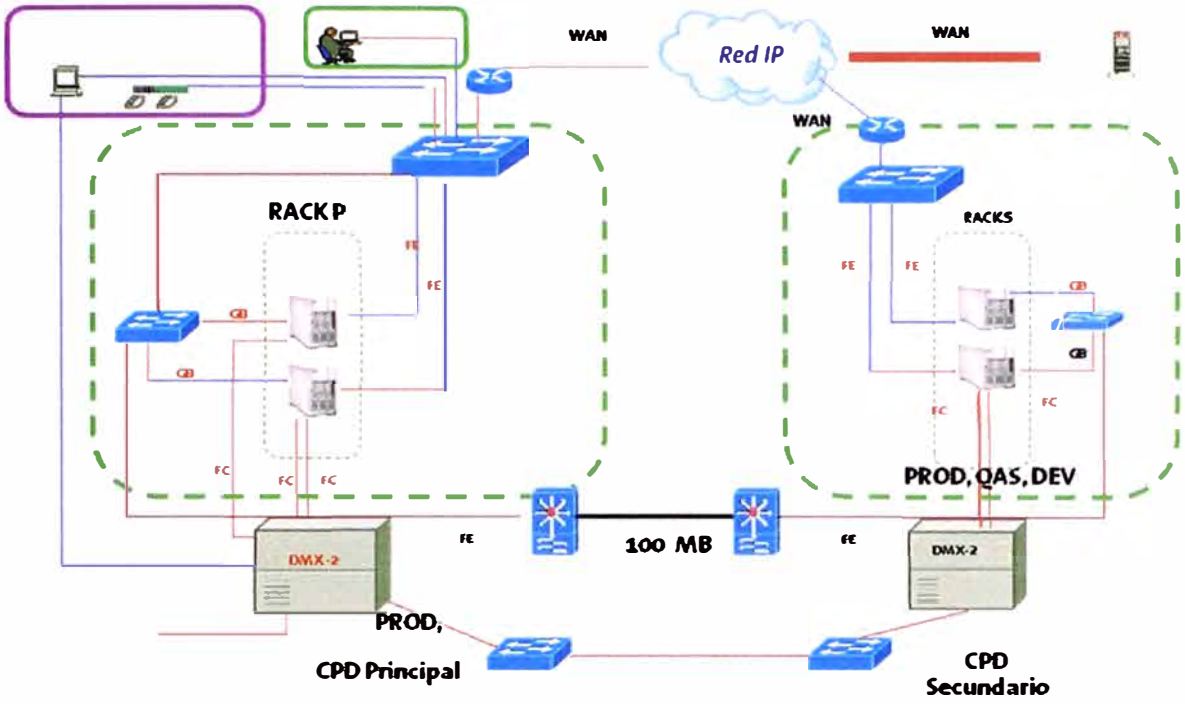


Figura 4.2 Emplazamiento Principal y Secundario

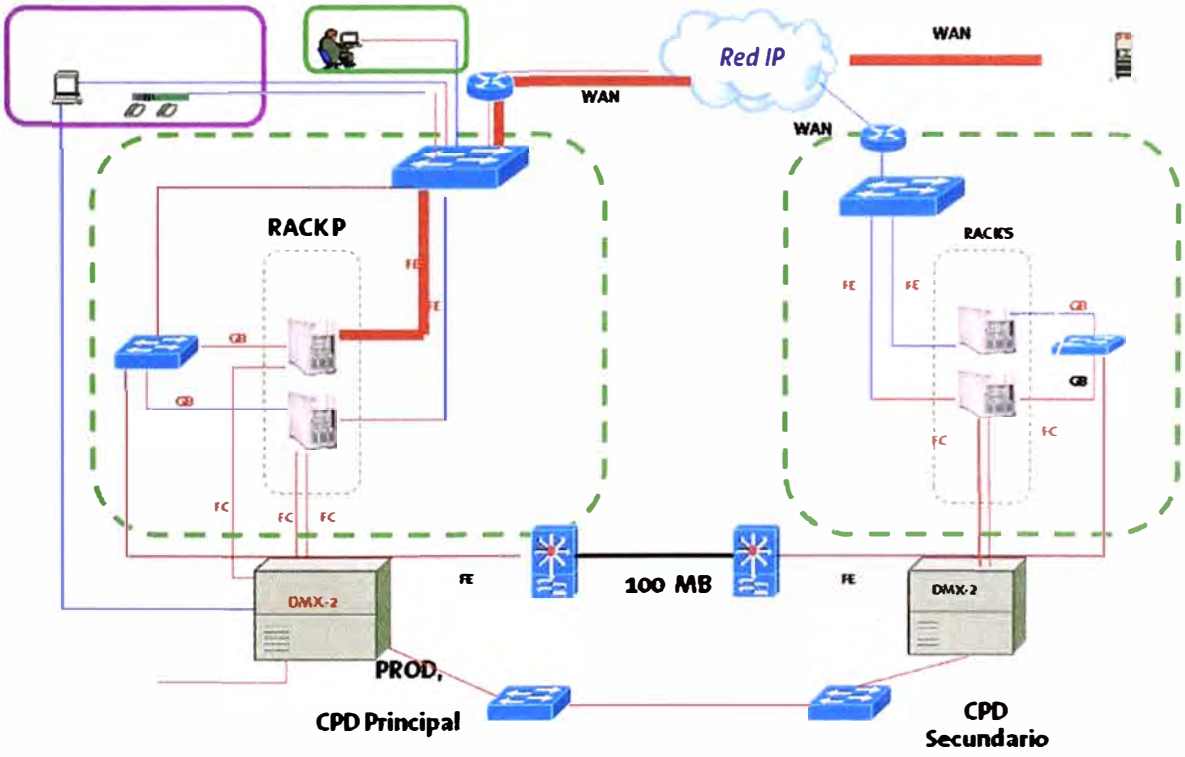


Figura 4.3 Consulta al Servidor de Aplicaciones 1

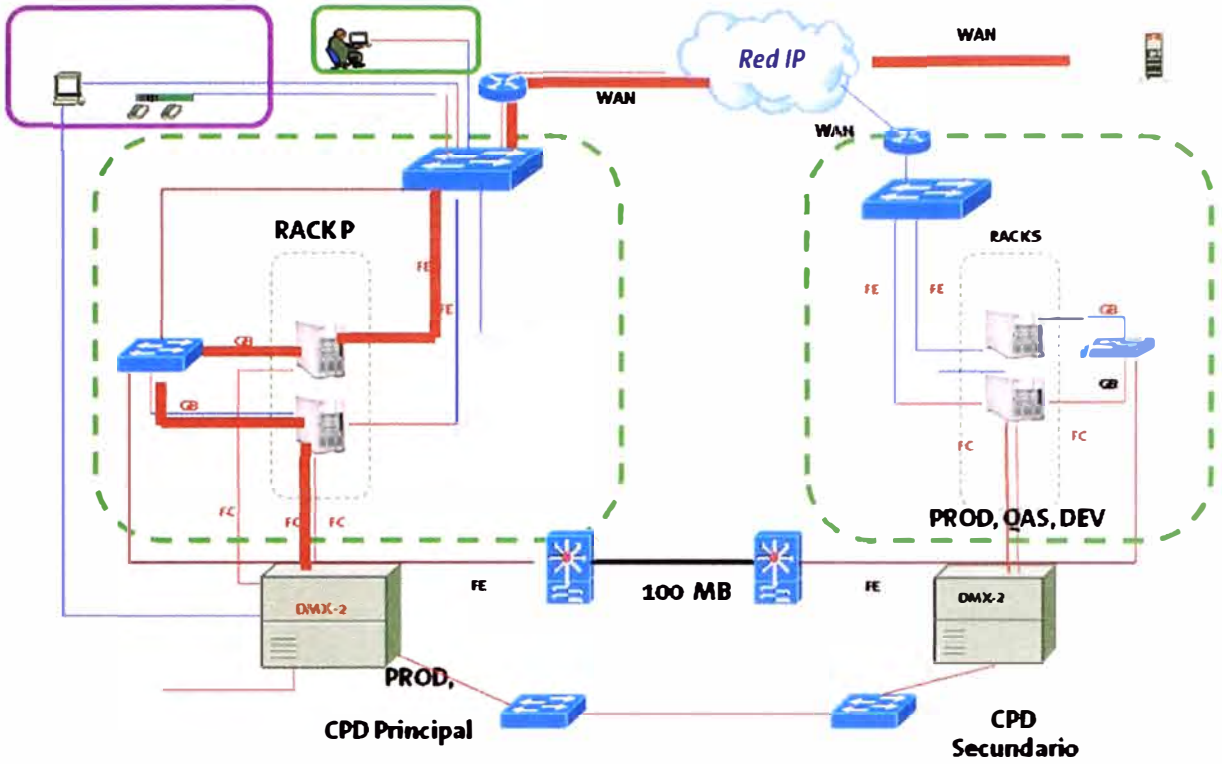


Figura 4.4 Consulta del Servidor de Aplicaciones 1 al Servidor de Base de Datos

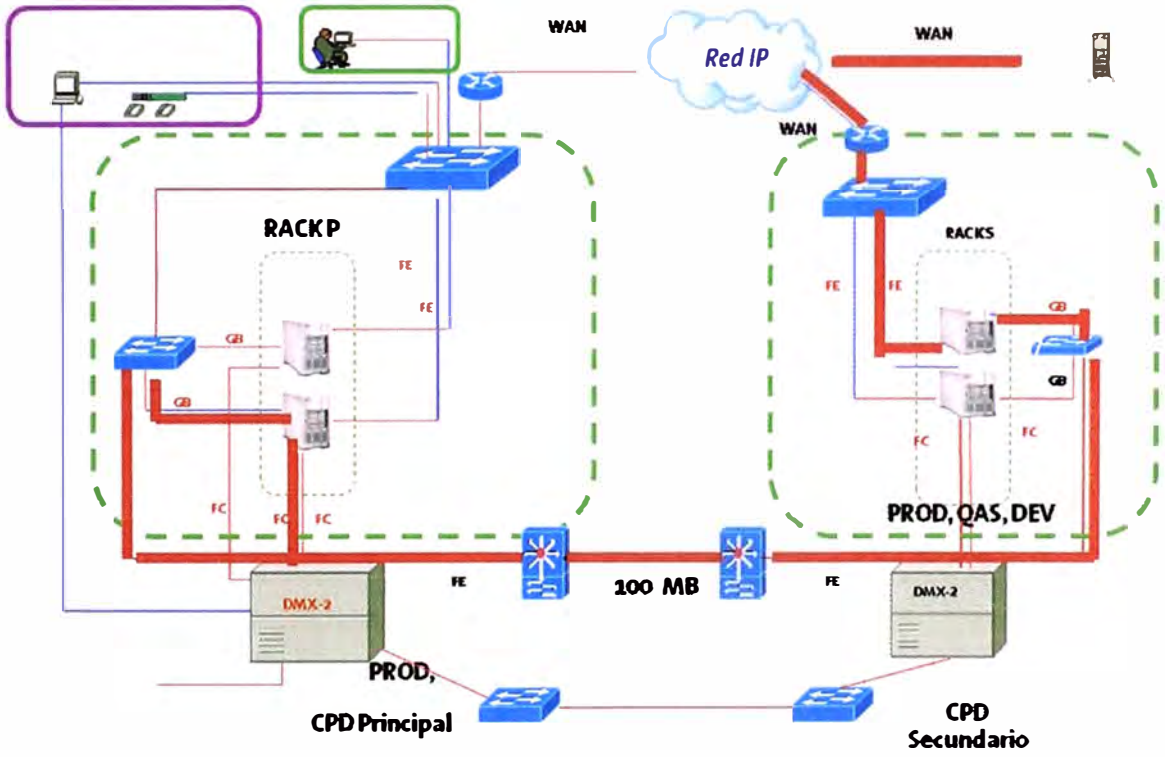


Figura 4.5 Consulta del Servidor de Aplicaciones 2 al Servidor de Base de Datos

e. Consulta de la IP-VPN al Servidor de desarrollo Calidad

La Figura 4.6 muestra como los usuarios consultan al equipo de Desarrollo y Calidad que se encuentra en el emplazamiento Secundario. En la figura F.5 del anexo F se presenta el gráfico en mayor detalle.

f. Replicación síncrona entre el Storage Principal al Secundario

La Figura 4.7 se muestra por que conexión se realiza la replicación de storage del emplazamiento principal al storage ubicado en el emplazamiento secundario. En la figura F.6 del anexo F se presenta el gráfico en mayor detalle.

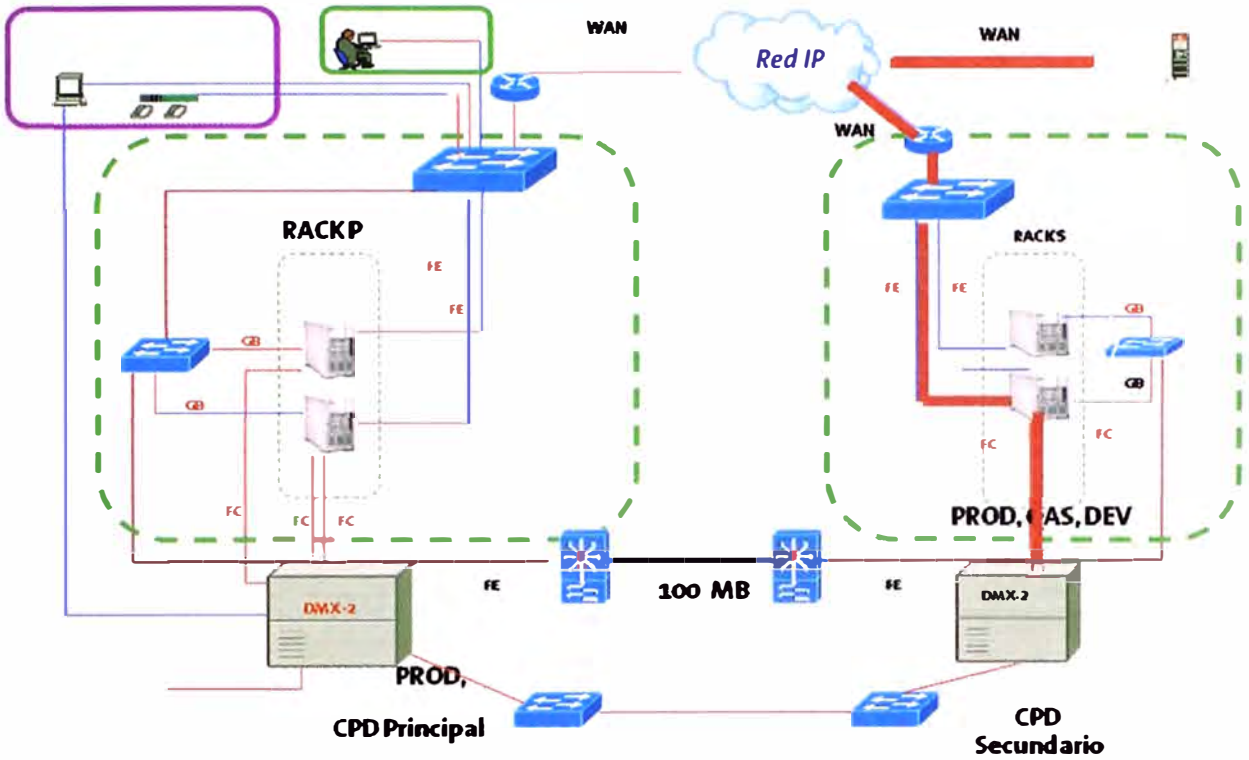


Figura 4.6 Consulta al Servidor de Desarrollo y Calidad

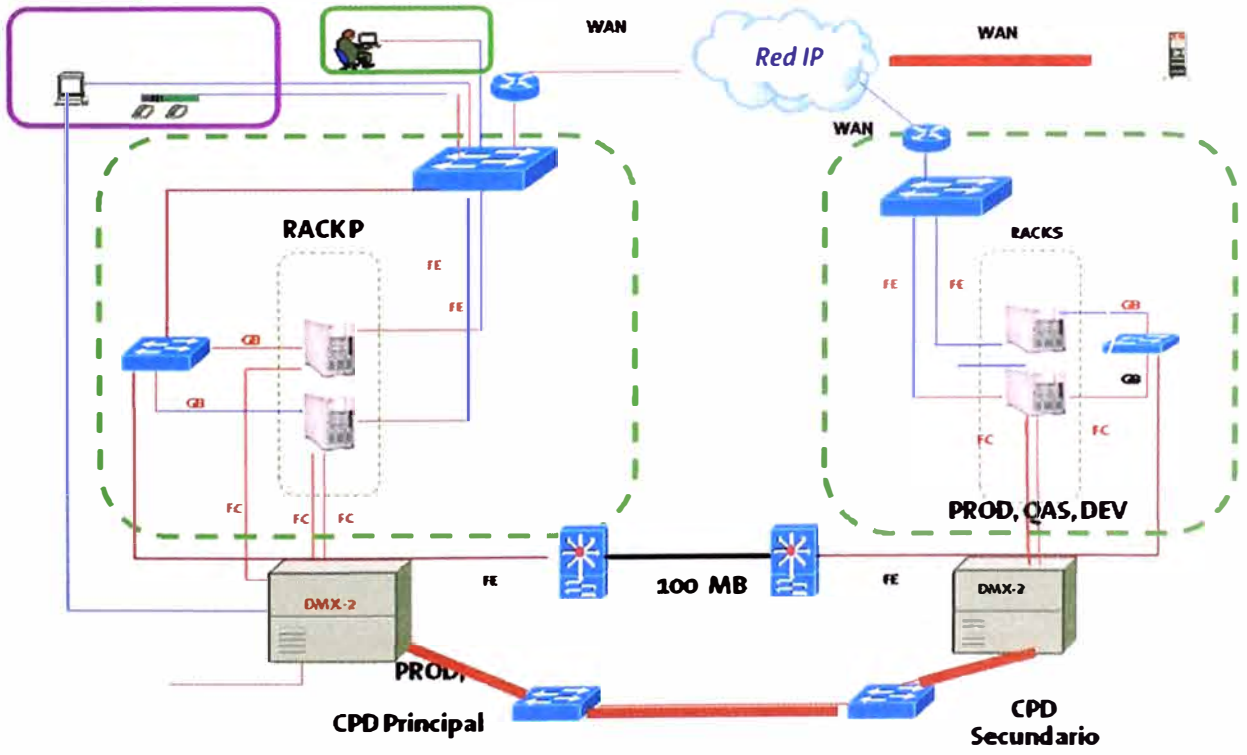


Figura 4.7 Replicación del Emplazamiento Principal al Secundario

g. No hay Servicio en el Emplazamiento Principal

En la Figura 2.8 se observa que no se tiene servicios en el emplazamiento principal y el servidor, que era desarrollo y calidad, ahora se comporta como servidor de base de datos y a través un menú toma los discos replicados del servidor de Base de datos del emplazamiento principal convirtiéndose ahora en el servidor de Base de Datos. En la figura F.7 del anexo F se presenta el gráfico en mayor detalle.

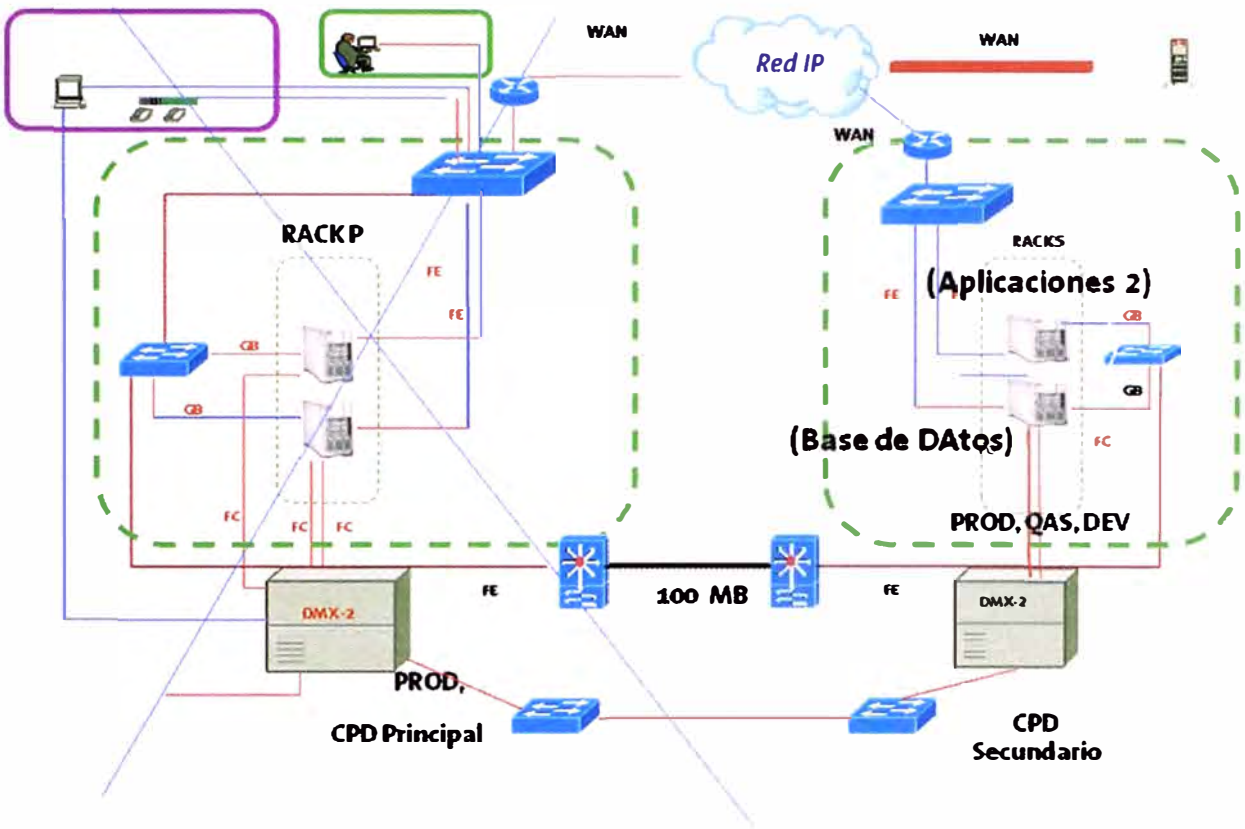


Figura 4.8 Servidor del Emplazamiento Secundario ahora brindaran servicio

A continuación se verá que sucede cuando por algún motivo error humano o desastre natural no se pueden conectar al emplazamiento principal

h. Activado la contingencia

En la Figura 2.9 se puede apreciar cómo todos los usuarios a través de la VPN se conectan al emplazamiento secundario percibiendo una perdida del servicio mínima, que es el tiempo que demora en tomar la decisión de entrar en contingencia. En la figura F.8 del anexo F se presenta el gráfico en mayor detalle.

Luego de estos pasos se procede a desactivar a través de un menú los servidor de Desarrollo y Calidad e indicar el storage secundario que no reciba ninguna replicación si hubiera alguna en el emplazamiento principal.

En la sección siguiente se mostrará a través de un grafico el tema de conectividad de las VPN, ya sea con sedes sólo en Perú y también en el extranjero.

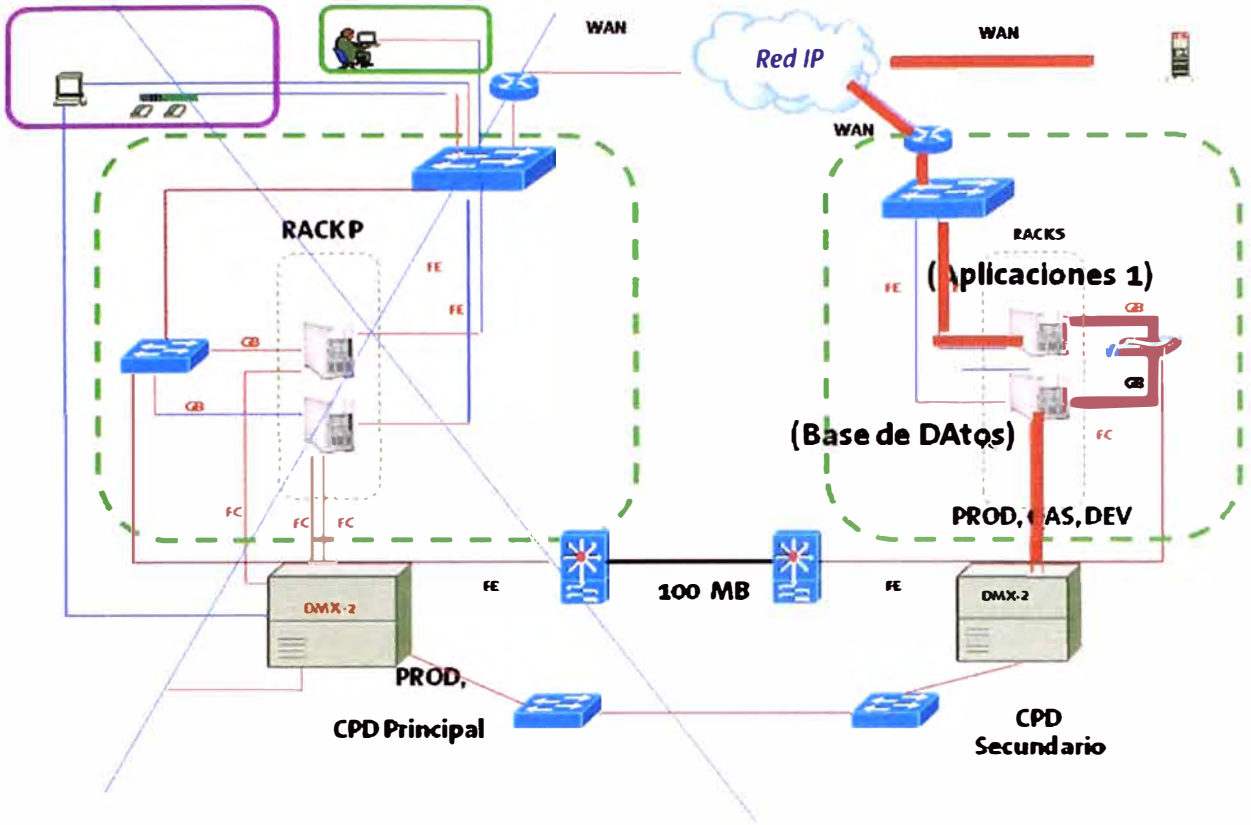


Figura 4.9 Producción en el Emplazamiento Secundario

4.2.3 Conectividad

En el punto anterior 4.2.2 se vio la interacción a través de los emplazamientos cómo funciona la alta disponibilidad de la solución. En la Figura 4.10 se muestra como un VPN tiene varias sedes en lima Perú pero también puede tener sedes en el extranjero que se conectan a través de un VPN al emplazamiento principal y de contingencia. En la Figura F.9 del Anexo F se presenta el diagrama en mayor detalle.

4.2.4 Seguridad

Se implementará un sistema de seguridad basado en el Firewall instalado en el CPD con la finalidad que se mantenga la independencia de las redes LAN internas de proyecto y la red de servidores instalada en el CPD, tanto en emplazamientos principal como contingencia.

4.2.5 Hardware

En la Tabla 4.1 se describen los cuatro servidores que se utilizaron para montar un sistema de alta disponibilidad en dos emplazamientos.

4.2.6 Almacenamiento

A continuación se muestran detalles del Storages utilizado en ambos emplazamientos así cómo sus respectivas ventajas (Los datos fueron provistos por el proveedor del Hardware).

a. Emplazamiento Principal XP24000 6.5TB raw

- HP StorageWorks XP24000 Disk Array
- *Rendimiento 3'500,000 IOPS
- *Alta disponibilidad 99.999%
- *Full redundance - Non Stop Certified
- *4Gbps End-to-End
- (6.5) TB raw utilizando de 146GB de 15,000 rpm
- (20) GB de memoria Caché exclusiva para datos
- (4) GB de memoria Caché compartida para uso del sistema de almacenamiento
- (8) Ports Fibre Channel 4Gbps

b. Emplazamiento Contingencia

- XP24000 6.5TB raw
- HP StorageWorks XP24000 Disk Array
- *Rendimiento 3'500,000 IOPS
- *Alta disponibilidad 99.999%
- *Full redundance - Non Stop Certified
- *4Gbps End-to-End
- (9.5) TB raw utilizando de 146GB de 15,000 rpm
- (20) GB de memoria Caché exclusiva para datos
- (4) GB de memoria Caché compartida para uso del sistema de almacenamiento
- (8) Ports Fibre Channel 4Gbps

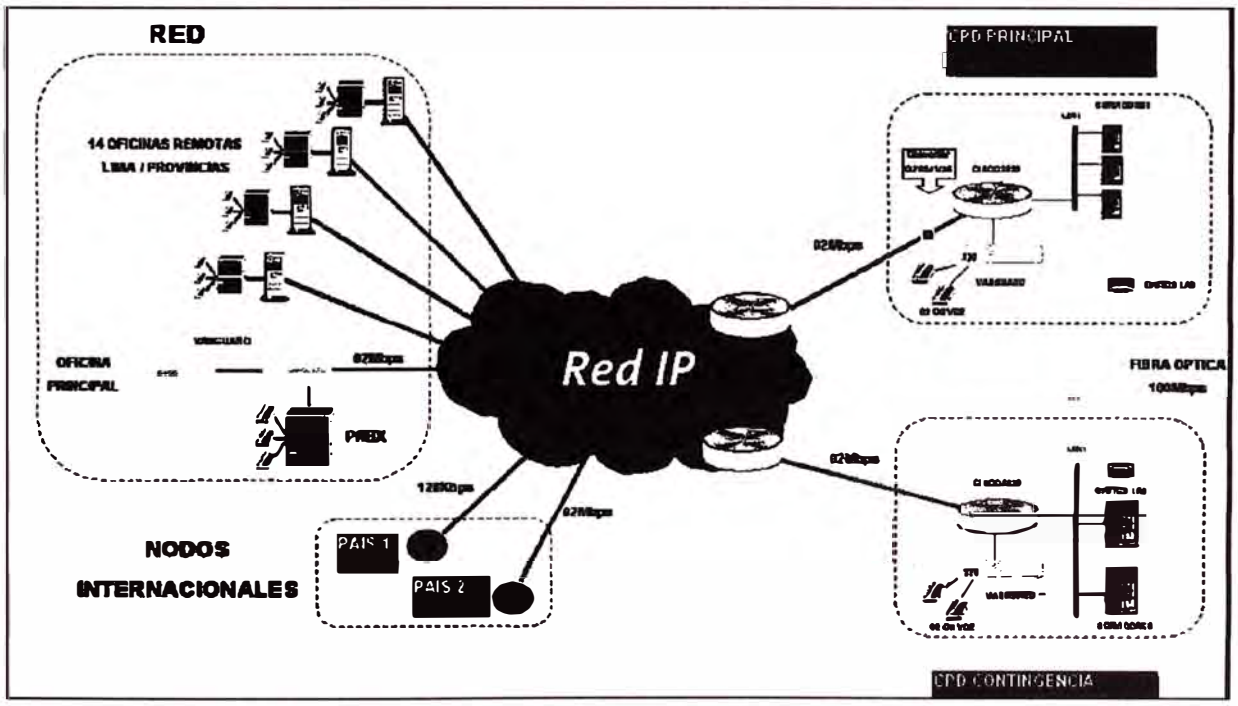


Figura 4.10 IP-VPN de distintas sedes del cliente y los CPD

Tabla 4.1 Servidores usados

Código de Parte	Nombre
	RACK
AF002A	HP Universal Rack 10642 G2 Shock Rack
	RX7640
AB448A	HP Integrity rx7640 8-core FAST Solution
	RX6600 APP 1 y 2
AD134A	HP rx6600 Base System Four Processors
	RX6600 QA/DEV
AD134A	HP rx6600 Base System Four Processors

4.2.7 HP StorageWorks XP Continuous Access

HP StorageWorks XP Continuous Access permite replicar datos de una cabina a otra en tiempo real para HP StorageWorks XP Disk Arrays. Este software forma parte de un grupo global de soluciones HP de disponibilidad y continuidad empresarial que permite el acceso constante a los datos. Los productos HP XP Continuous Access se integran con soluciones de software de clústeres de servidor para ofrecer los niveles más elevados de disponibilidad y tolerancia a desastres. Para proteger su negocio frente a desastres, ya sean locales o de mayor alcance, puede crear soluciones de recuperación de desastres entre Data Center, con un centro de datos ubicado en otro continente. Si usted solo necesita mover datos de una ubicación a otra o de una generación de cabinas HP XP Disk Array a otra, HP XP Continuous Access ofrece una solución de migración de datos segura y de alto rendimiento.

Sus características son:

- Continuidad del negocio.- Mantiene el negocio funcionando en momentos críticos realizando copias en línea de la información importante en centros de datos alternos.
- Fuerte integración con soluciones de software de clústeres.- Coordina las funciones de recuperación/restauración del nodo del clúster de servidores con las funciones de recuperación/restauración del sistema de almacenamiento sin interrupciones en caso de fallo.
- Soluciones entre Data Center.- Proteje la empresa de desastres locales o de mayor alcance utilizando HP StorageWorks XP Continuous Access Journal junto con HP StorageWorks XP Continuous Access Synchronous para obtener dos copias simultáneas de los mismos datos de origen, y cree una solución de recuperación de desastres 3 Data Center.
- Migración de datos.- simplifica los movimientos del centro de datos y las actualizaciones del sistema de almacenamiento con el software HP XP Continuous Access, que permite migrar datos entre ubicaciones y entre familias HP StorageWorks XP Disk Array. Combine HP XP Continuous Access con HP StorageWorks XP

Extemal Storage para migrar datos entre cabinas heterogéneas.

- Replicación remota estable HP StorageWorks XP Continuous Access Journal.- Dado que utiliza un archivo adjunto basado en disco de alta capacidad, HP XP Continuous Access Journal le permite ajustar los enlaces de telecomunicaciones a la frecuencia media de E/S, por lo que usted podrá admitir cortes de enlace más prolongados.

4.3 Pruebas efectuadas

La tercerización de servicios de almacenamiento se realizaba previamente con un CPD, pero esto causaba demoras de reposición del servicio al cliente ante una falla parcial y total, las que se traducían en una pérdida de dinero y clientes insatisfechos.

Tabla 4.2 Tiempo de restauración por componente averiado en un CPD

Componente averiado	Tiempo de restauración del servicios
Servidor	6 horas/ servidor
Switch	4 horas/ switch
Storage	10 horas
Router	3 horas

Tabla 4.3 Tiempo de restauración por aplicación ejecutada en los servidores

Elemento	Tiempo de restauración
Sistema operativo	4 horas/ servidor
Instalación de base de datos	4 horas
Instalación de aplicación	3 horas
Restauración del Backup de la base de datos	14 horas
Restauración del Backup de los archivos de aplicación	4 horas

Tabla 4.4 Tiempo de restauración con un emplazamiento secundario

Elemento	Tiempo de restauración
Declararla la activación de contingencia	5 minutos
Activación de desvío de tráfico al desplazamiento secundario	12 minutos
Desactivación de desarrollo y calidad en emplazamiento secundario	8 minutos
Desactivación de replicación y activación de emplzamiento secundario cómo principal a nivel de storage	20 minutos
Activación de aplicación 2 cómo aplicación 1	5 minutos

La inclusión de un CPD de respaldo optimiza enormemente los tiempos de restauración. Las tablas mostradas (Tabla 4.2, Y 4.3) muestran los tiempos de respuesta con un CPD y con un CPD secundario (Tabla 4.4).

Cómo puede observarse en las tablas 4.2 y 4.3, la falla de un componente demora en su restauración tres horas mínimo, y un tiempo máximo de 48 horas. Siendo de gran impacto en las empresas especialmente si ocurre en días de alta demanda. Con un emplazamiento secundario el tiempo de restauración de alguna falla sería de tan sólo cincuenta minutos.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Las pruebas efectuadas en el campo mostraron claramente que la inclusión de un CPD de respaldo optimizaba ostensiblemente los tiempos de restauración del servicio, el cual representa el 1.7% del tiempo original empleado
2. El servicio de alta disponibilidad del almacenamiento de datos contratado ha representado un ahorro del 95% de los costos en infraestructura y en costos operativos, comprobándose así que la tercerización de servicios de almacenamiento de datos de alta disponibilidad es una inversión altamente rentable.
3. La implementación efectuada ofrece una mayor garantía de la continuidad del acceso a los datos estratégicos.

Recomendaciones

1. Es importante tener en cuenta que las características de los discos en el emplazamiento principal deben ser las mismas que en el emplazamiento secundario para evitar problemas de performance del sistema de contingencia.
2. Es posible mejorar el tiempo de respuesta obtenido hasta en un 40% realizando las actividades en paralelo o mediante la utilización de comandos "batch".
3. El personal técnico de la empresa prestadora del servicio debe ser capacitado y entrenado permanentemente, realizando simulacros continuos en sistemas de desarrollo para mejorar los tiempos de respuesta a contingencias.

ANEXO A
TIPOS DE CONECTIVIDAD

A continuación se explican algunos conceptos importantes relacionados con el tipo de conectividad de redes de datos:

- IP/VPN (red privada virtual).- Es un servicio gestionado de interconexión de redes locales basado en tecnología MPLS (Comunicaciones corporativas seguras) sobre infraestructura IP perteneciente a la empresa proveedora. El servicio permite la creación de redes privadas virtuales sobre dicha infraestructura manteniendo las mismas prestaciones que si fuera una red privada, reduciendo costes y aumentando rendimiento.
- InfoInternet .- Es el servicio de conexión a Internet simétrico y permanente a través de la Red IP MPLS lo cual permite una total gestión del enlace.
- Red Telefónica Básica (RTB) .- Es el conjunto de elementos constituido por todos los medios de transmisión y conmutación necesarios que permite enlazar a voluntad dos equipos terminales mediante un circuito físico que se establece específicamente para la comunicación y que desaparece una vez que se ha completado la misma. Se trata por tanto, de una red de telecomunicaciones conmutada.
- Red Digital de Servicios Integrados (RDSI o ISDN en inglés) .- Es una red que procede por evolución de la Red Digital Integrada (RDI) y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados.

ANEXO B
TOPOLOGÍA DE REDES

La topología hace referencia a una forma de una red. La topología muestra cómo los diferentes nodos que estén conectados entre sí, y la forma de cómo interactúan, está determinada por la topología de la red. Las topologías pueden ser físicas o lógicas.

- **Topología en Malla.-** Los dispositivos están conectado en muchas interconexiones redundantes entre nodos de la red. En una verdadera topología en malla, cada nodo tiene una conexión con cada otro nodo de la red. Ver Figura B.1.
- **Topología en Estrella.-** Todos los dispositivos están conectados a un hub central. Los nodos se comunican en la red a través del hub. Ver Figura B.2.
- **Topología en Bus.-** Todos los dispositivos están conectados a un cable central llamado bus o backbone. Ver Figura B.3.
- **Topología en Anillo.-** Todos los dispositivos están conectados al otro en un bucle cerrado, de esta manera cada dispositivo es conectado directamente con otros dos dispositivos, uno en cada lado de este. Ver Figura B.4.
- **Topología en Árbol.-** Es una topología híbrida. Grupos de redes en estrella son conectados a un bus o backbone lineal. Ver Figura B.5.

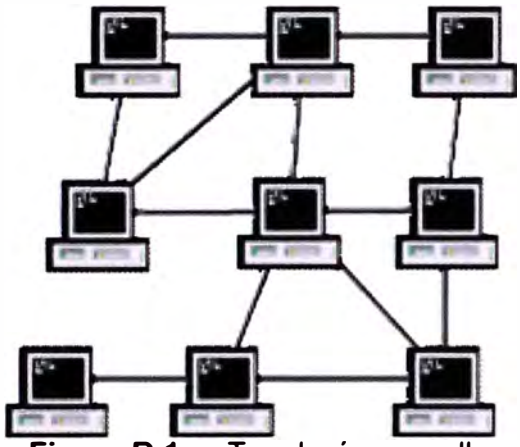


Figura B.1 Topología en malla

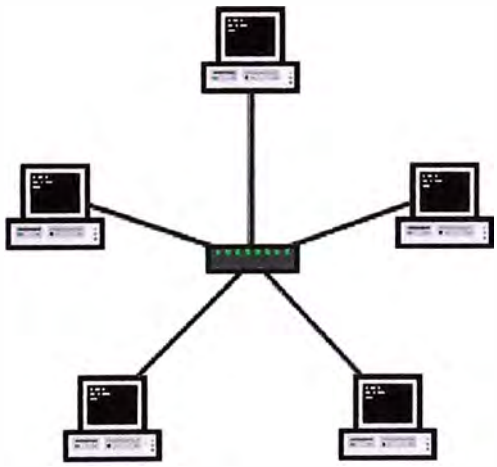


Figura B.2 Topología en estrella

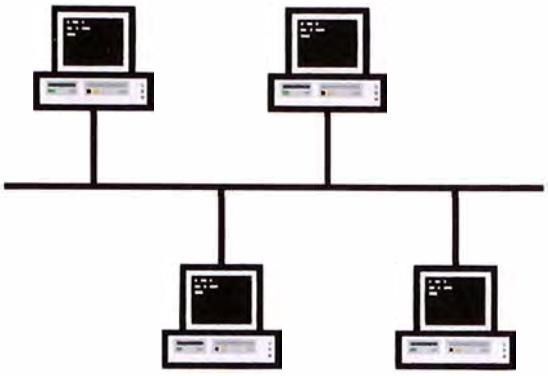


Figura B.3 Topología en bus

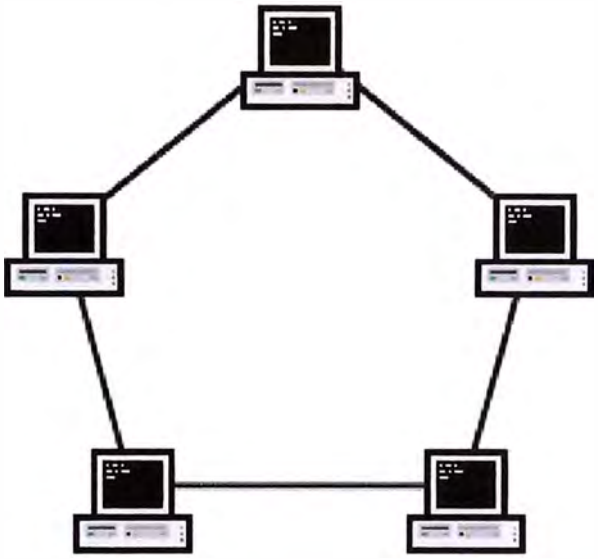


Figura B.4 Topología en anillo

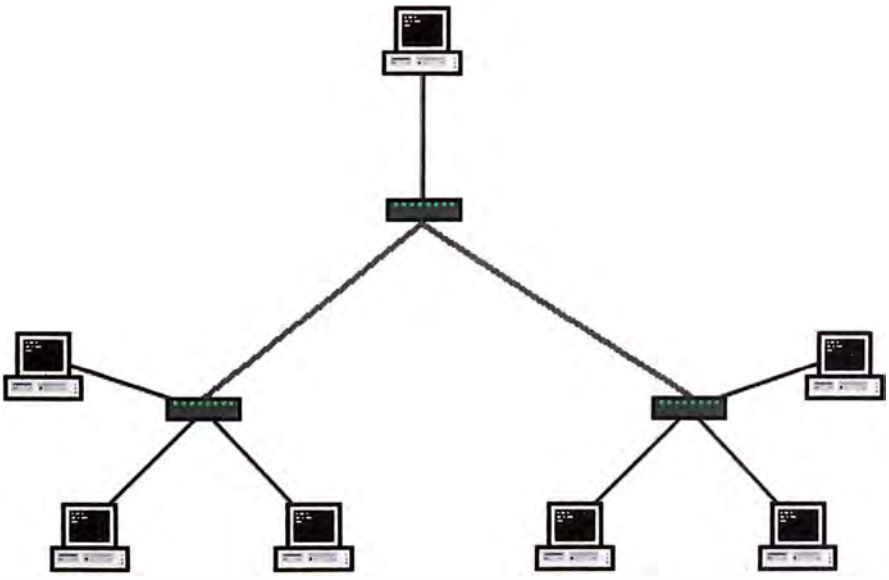
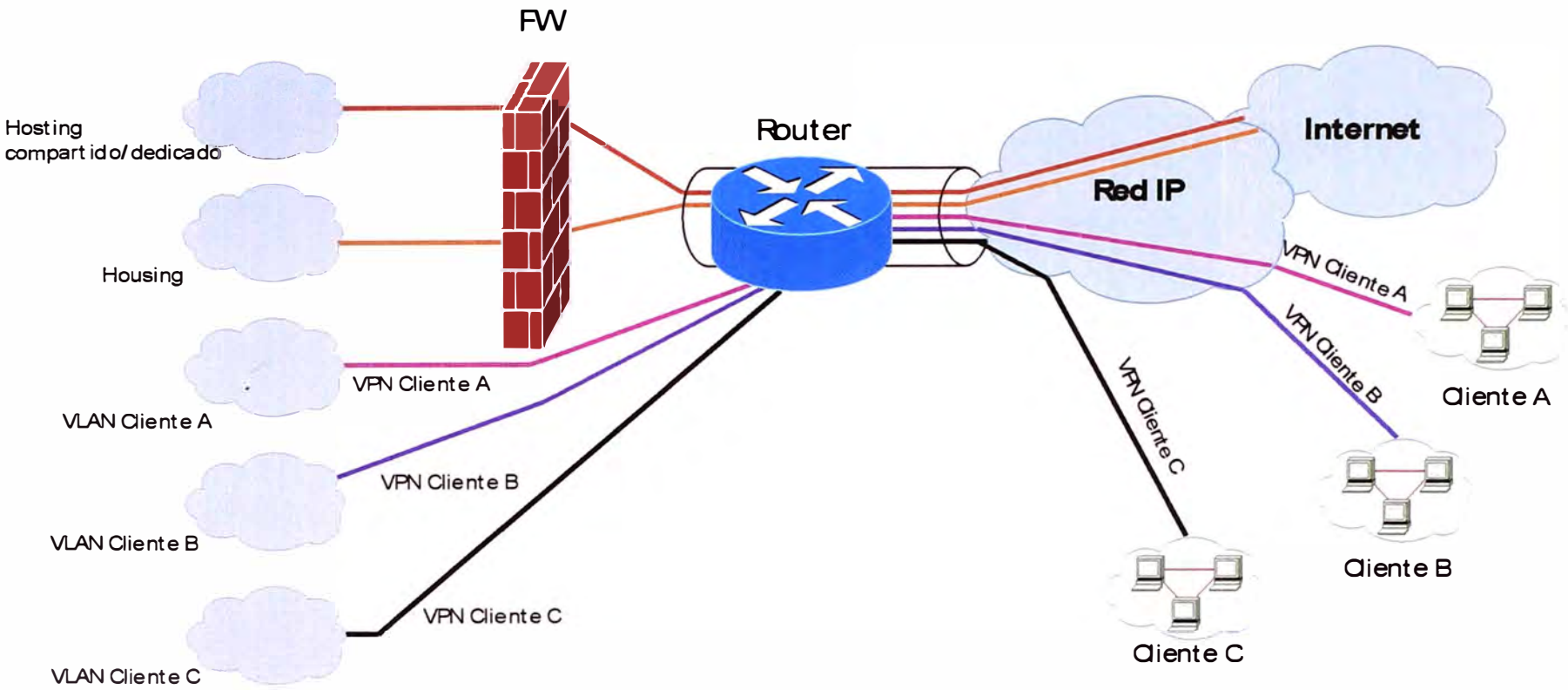


Figura B.5 Topología en árbol

ANEXO C

DIAGRAMA FUNCIONAL DE LOS DISTINTOS SERVICIOS DEL CDP

Diagrama Funcional



Este diagrama muestra la separación funcional de los distintos servicios del TIC. Para evitar la complejidad se han omitido los elementos de redundancia de comunicaciones y seguridad.

FIGURA C.1 Diagrama funcional

ANEXO D
ARQUITECTURA DE LA SOLUCIÓN

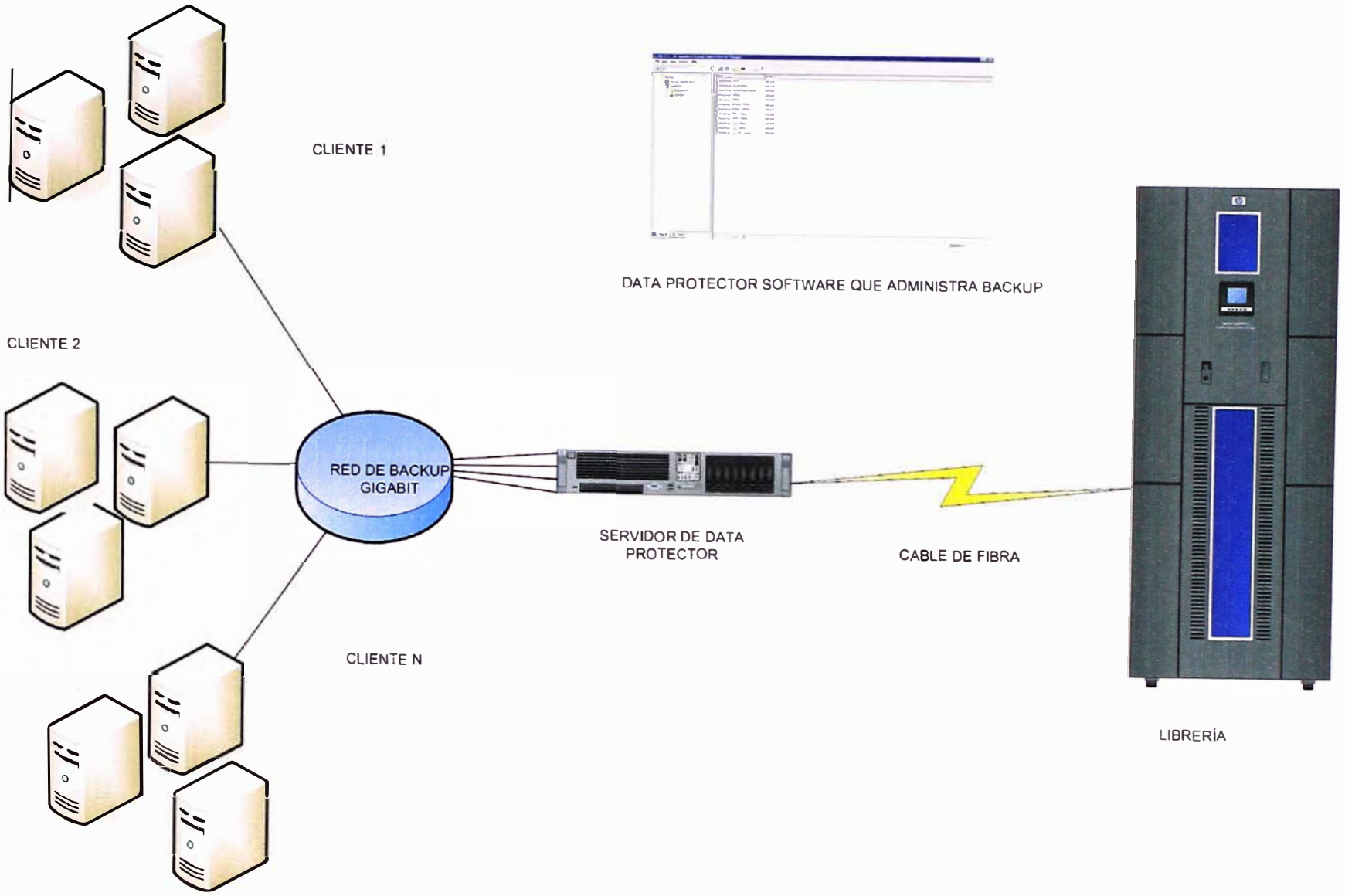


FIGURA D.1 Arquitectura de la solución

ANEXO E
MODELO DE GESTIÓN ITIL

Las buenas prácticas documentadas en IT Infrastructure Library (ITIL) están siendo adoptadas por clientes de todo el mundo y se están convirtiendo rápidamente en el estándar de facto para la gestión de servicios de TI. La adopción de las recomendaciones ITIL permite a las empresas alinear los servicios de TI con las necesidades actuales y futuras del negocio y de sus clientes, mejorar la calidad de los servicios de TI proporcionados y reducir a largo plazo el coste del aprovisionamiento de servicios.

IT Infrastructure Library (ITIL) fue desarrollada a finales de los años ochenta por una rama del gobierno británico como respuesta a la creciente dependencia de las TI. ITIL constituye actualmente un corpus público de conocimientos, que proporciona toda una colección de buenas prácticas de gestión de servicios para ayudar a las organizaciones a mejorar los niveles de servicio y reducir el coste de las operaciones de TI. La biblioteca ITIL se estructura en base las siguientes áreas:

- Soporte a los Servicios.
- Suministro del Servicio.
- Gestión de la Seguridad.
- Gestión de la Infraestructura Tecnológica (ICT)
- Gestión de aplicaciones.

La metodología utilizada por TdP para la gestión de servicios de IT está respaldada por "Information Technology Infrastructure Library" (ITIL) y considera, entre otras, las áreas de atención que se describen a continuación.

Soporte a los servicios (Service Support)

Abarca los siguientes procesos:

- **Mesa de ayuda** (Service Desk).- Mesa de Ayuda (Service Desk) Es el punto donde se reportan las incidencias y se generan los requerimientos. La Mesa de Ayuda tiene la responsabilidad de mantener informados a los usuarios lo que va aconteciendo con la incidencia y/o requerimiento reportado. Service Desk más que un proceso es una función enmarcada dentro de las actividades del Soporte al Servicio.
- **Gestión de Incidencias** (Incident Management).- La meta fundamental del proceso de Gestión de incidencias es restaurar la operación normal del servicio lo más pronto posible y reducir al mínimo el impacto adverso en las operaciones de negocio, asegurando de esta manera los mejores niveles posibles de la calidad y disponibilidad del servicio, manteniendo la operación normal del servicio.

  La operación Normal del servicio, se define aquí como la operación del servicio dentro de los límites del Acuerdo de Niveles de Servicio (SLA). En terminología de ITIL, Incidencia se define como Cualquier acontecimiento que no es parte de la

operación estándar de un servicio y que cause, o puede causar, una interrupción, o una reducción de la calidad de ese servicio.

Se debe tener una interfaz cercana entre el proceso de gestión de incidencias, la gestión de problemas y el proceso de gestión de cambios, así como la función de Mesa de Ayuda. Si no es controlado correctamente, los cambios pueden generar nuevas incidencias. Se requiere una forma de hacerles seguimiento. Por lo tanto, se recomienda que los registros de las incidencias se deben llevar a cabo en la misma Base de Datos de la Gestión de Configuración (CMDB), así como los problemas.

Las prioridades de las incidencias y sus procedimientos de atención necesitan ser acordados como parte del proceso de la administración de niveles de servicio y ser documentados en el SLA.

- **Gestión de Problemas** (Problem Management).- La meta de la gestión del problema es reducir al mínimo el impacto adverso del incidente y los problemas en el negocio que son causados por errores dentro de la infraestructura IT, y prevenir la repetición de los incidentes relacionados con estos errores.

  Para alcanzar esta meta, la gestión del problema buscará conseguir la causa de la raíz de incidentes para luego tomar las acciones de mejorar o corregir la situación. El proceso de la gestión del problema tiene aspectos reactivos y pro-activos.

  El aspecto reactivo se refiere a solucionar problemas en respuesta a uno o más incidentes. Mientras que el aspecto pro-activo, identificará y solucionará los problemas y errores conocidos antes de que los incidentes ocurran.

  El proceso de la gestión del problema requiere la grabación exacta y comprensiva de los incidentes para luego identificar con eficacia y eficiencia su causa. La gestión del problema también necesita una comunicación cercana con el proceso de la gestión de la disponibilidad para identificar las tendencias e instigar a la acción remediadora.

  En términos de una definición formal: un problema es una causa subyacente desconocida de uno o más incidentes, y un error conocido es un problema que se diagnostica con éxito y para el cuál se ha identificado un work-around.

  El control del problema, el control de error y la gestión pro-activa del problema están contenidos dentro del alcance de la gestión del problema.

- **Gestión de Cambios** (Change Management).- Los cambios se presentan como resultado de problemas, pero muchos cambios pueden venir de acciones pro-activas en beneficio del negocio, tales como reducción de costes o mejora de servicios. La meta del proceso de gestión del cambio es asegurarse de que los métodos y los procedimientos estandarizados sean usados para la dirección eficiente de todos los

cambios, para reducir al mínimo el impacto de incidentes relacionados a la calidad del servicio, y por lo tanto mejorar las operaciones cotidianas de la organización.

Efectuar una respuesta apropiada a una petición de cambio (change request) exige una evaluación cercana del riesgo en la continuidad del negocio, del impacto del cambio, de los requerimientos de recurso y de la aprobación del cambio. Es esencial mantener un equilibrio apropiado entre la necesidad de un cambio contra al impacto del cambio.

Es particularmente importante que los procesos de la gestión del cambio tengan alta visibilidad y canales abiertos de comunicación para promover transiciones claras cuando ocurran los cambios.

Los procesos de la gestión del cambio deben de conocer con exactitud los datos de configuración para estar seguros del impacto completo que se producirían al realizar los cambios. Existe por lo tanto una relación muy cercana entre la gestión de configuración, la gestión de versiones y la gestión del cambio.

- **Gestión de Versiones** (Release Management).- Muchos proveedores y distribuidores de servicio pueden estar implicados en el release del hardware y software en un ambiente distribuido.

  Una buena planificación y administración del recurso son esenciales para empaquetar y distribuir con éxito una versión al cliente. La gestión de versiones adopta una visión holística de un cambio de servicio IT y debe asegurarse de que todos los aspectos de una versión, técnico y no técnico, estén considerados juntos. Las metas de la gestión de versiones on:

  - Planear y supervisar la puesta en marcha acertada del software y del hardware relacionado.
  - Diseñar e implementar eficientemente los procedimientos para la distribución e instalación de los cambios en los sistemas IT.
  - Asegurarse de que el hardware y el software que son cambiados sean detectables, seguros y que solamente las versiones correctas, autorizadas y probadas sean instaladas.
  - Comunicar y manejar las expectativas del cliente durante el planeamiento y la puesta en marcha de nuevas versiones.
  - Acordar el exacto contenido y el plan de puesta en marcha para el lanzamiento, con la gestión del cambio.
  - Implementar una nueva versión de hardware o software en un ambiente operacional usando los procesos que controlan la gestión de configuración y la gestión de cambios - una versión debe estar bajo la gestión del cambio y puede

consistir en cualquier combinación de hardware, software, firmware y de documentos CIs.

- Asegurarse de que las copias principales de todo el software estén seguras en la biblioteca definitiva del software (DSL) y que la base de datos de la gestión de configuración (CMDB) sea actualizada.
- Asegurarse de que todo el hardware que esta siendo implementado o cambiado sea seguro y detectable, con los servicios de la gestión de configuración.

El foco de la gestión de versiones es la protección del ambiente en producción y de sus servicios con el uso de procedimientos y revisiones formales.

La gestión de versiones trabaja cerca con los procesos de la gestión del cambio y la gestión de configuración para asegurarse de que la base de datos compartida de la gestión de configuración (CMDB) se mantenga actualizada con los cambios implementados por la nueva versión, y que el contenido de ésas versiones se almacenen en la biblioteca definitiva del software (DSL).

Las especificaciones del hardware, las instrucciones de ensamblaje y la configuración de red también se almacenan en el DSL/CMDB. A menudo, la gestión de versiones se financia de grandes proyectos, en vez de que se incluyan en el costo del servicio normal a los clientes.

Aunque hay costos asociados con la implementación de la gestión del lanzamiento, éstos son lejanos en comparación con los costos potenciales de release del software no planificados adecuadamente, manejando y controlando las versiones de hardware y software.

La gestión de versiones emprende el planeamiento, diseño, construcción, configuración y prueba del hardware y software al crear un set de componentes de lanzamiento para un ambiente en producción. Las actividades también cubren el planeamiento, la preparación y programación de una versión a muchos clientes y localizaciones.

- **Gestión de Configuración** (Configuration Management).- Para ser eficientes y eficaces, todas las organizaciones necesitan controlar su infraestructura y servicios IT. La gestión de configuración proporciona un modelo lógico de la infraestructura o de un servicio, identificando, controlando, manteniendo y verificando las versiones de los Elementos de Configuración (EC) existentes. Las metas de la gestión de configuración son:
  - Contabilizar todos los activos IT y sus configuraciones dentro de la organización y de sus servicios.
  - Proporcionar información exacta de configuraciones y su documentación para

apoyar el resto de procesos de la gestión del servicio.

- Proporcionar una base sólida de información para la gestión de incidencias, gestión del problema, gestión del cambio y gestión de versiones.

Verificar los expedientes de configuración, desde la base de datos de la gestión de configuración (CMDB), contra la infraestructura y corregir cualquier excepción.

ANEXO F
DIAGRAMAS DE FUNCIONAMIENTO DE LA SOLUCIÓN

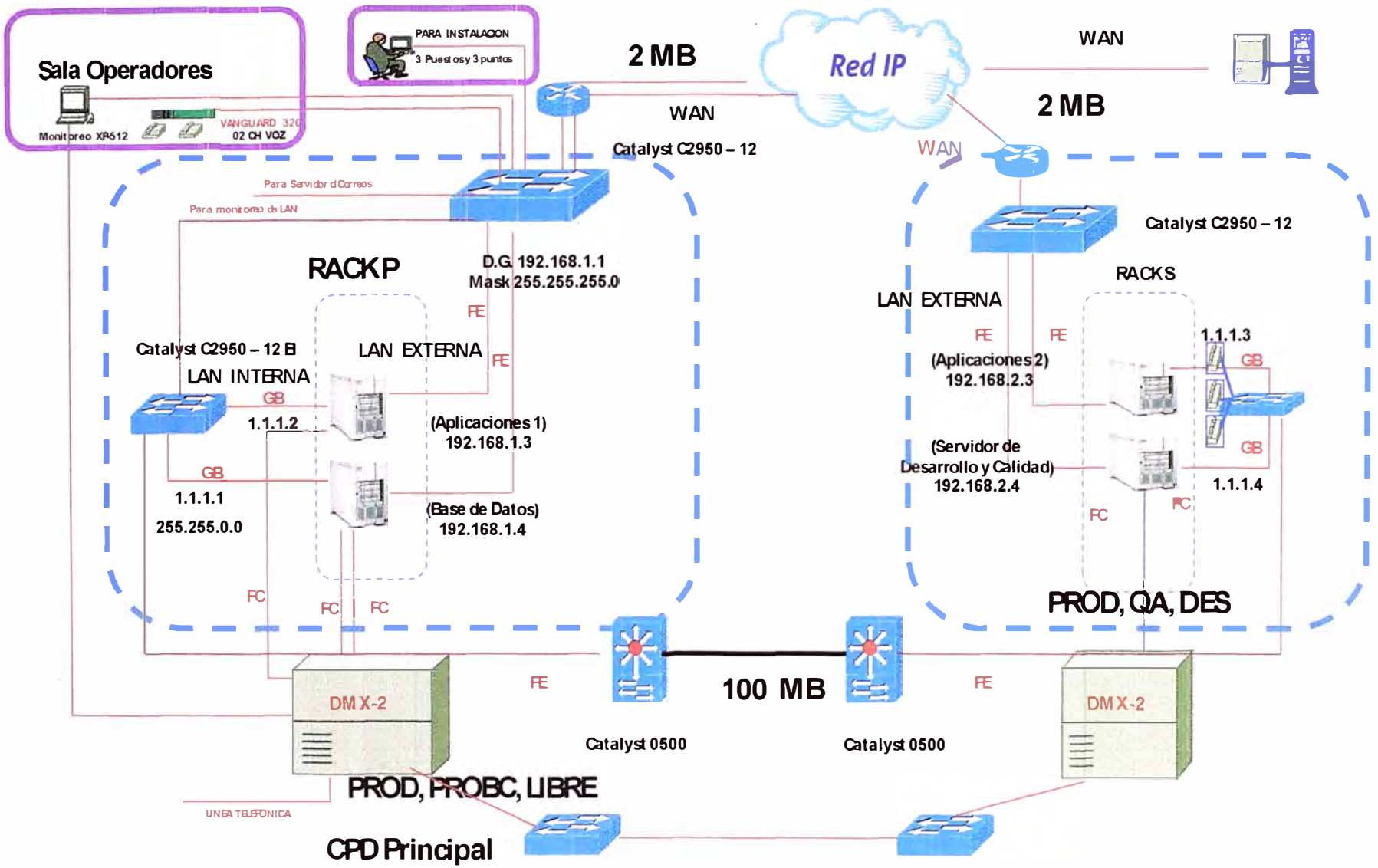


Figura F.1 Emplazamiento Principal y Secundario

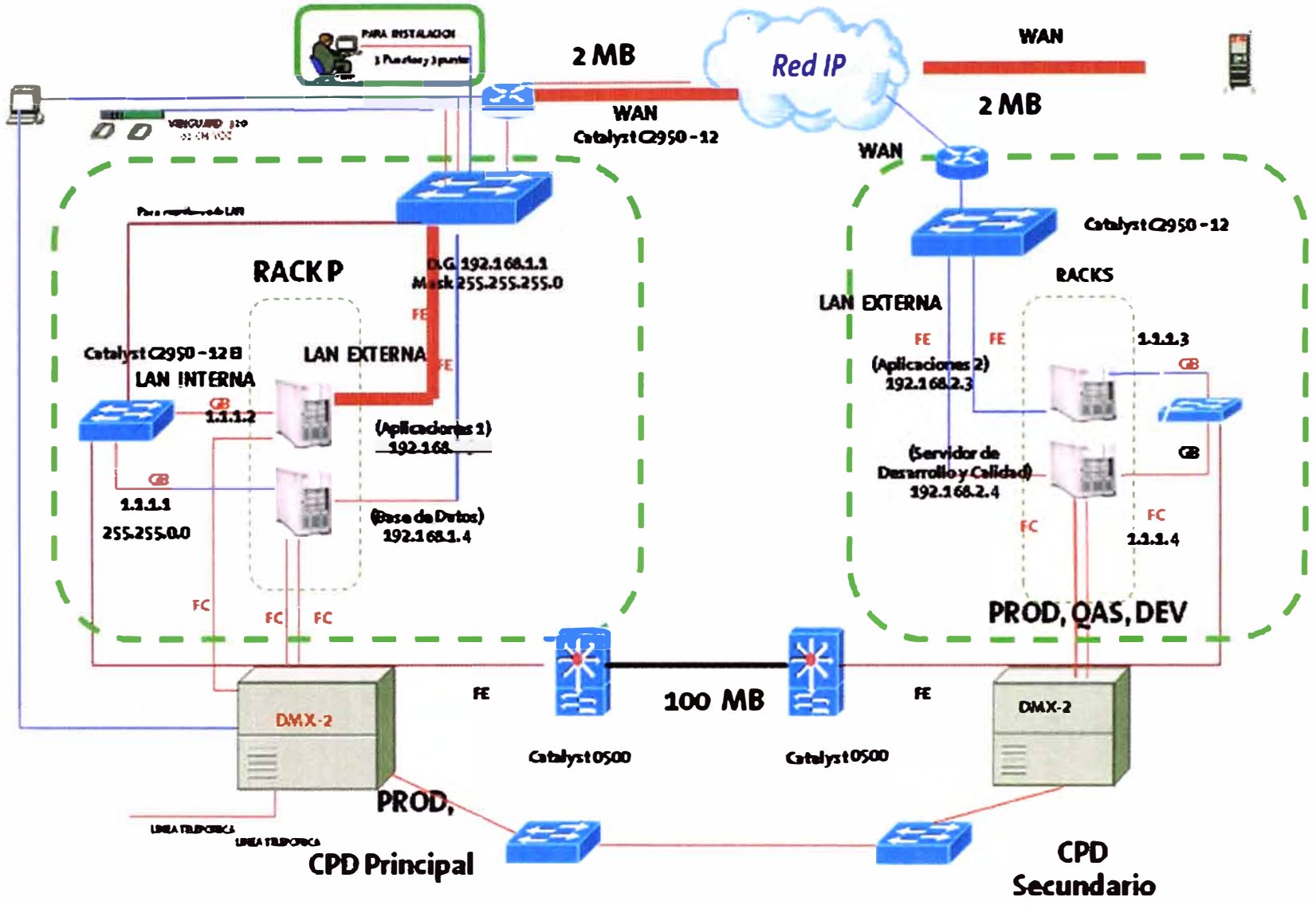


Figura F.2 Consulta al Servidor de Aplicaciones 1

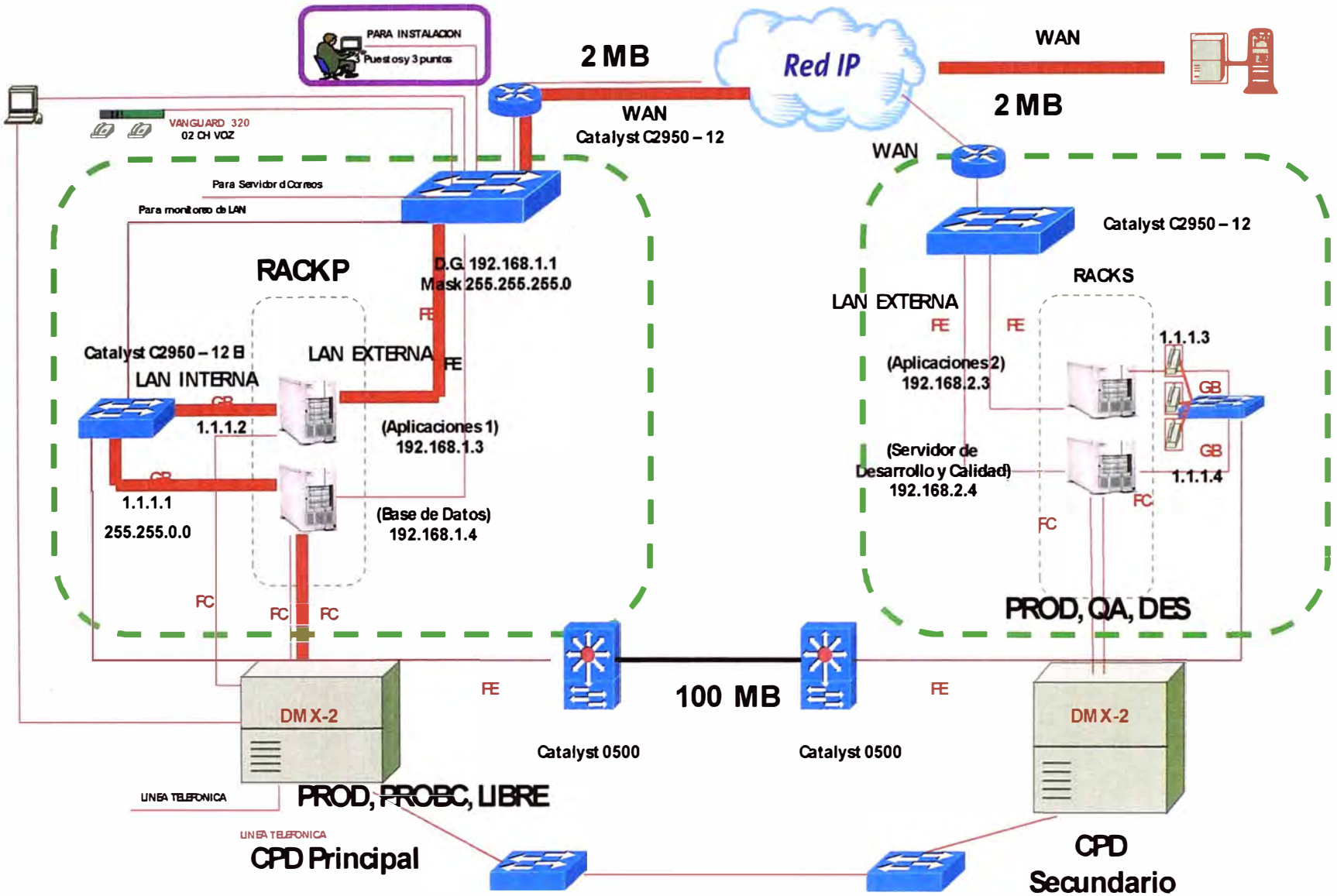


Figura F.3 Consulta del Servidor de Aplicaciones 1 al Servidor de Base de Datos

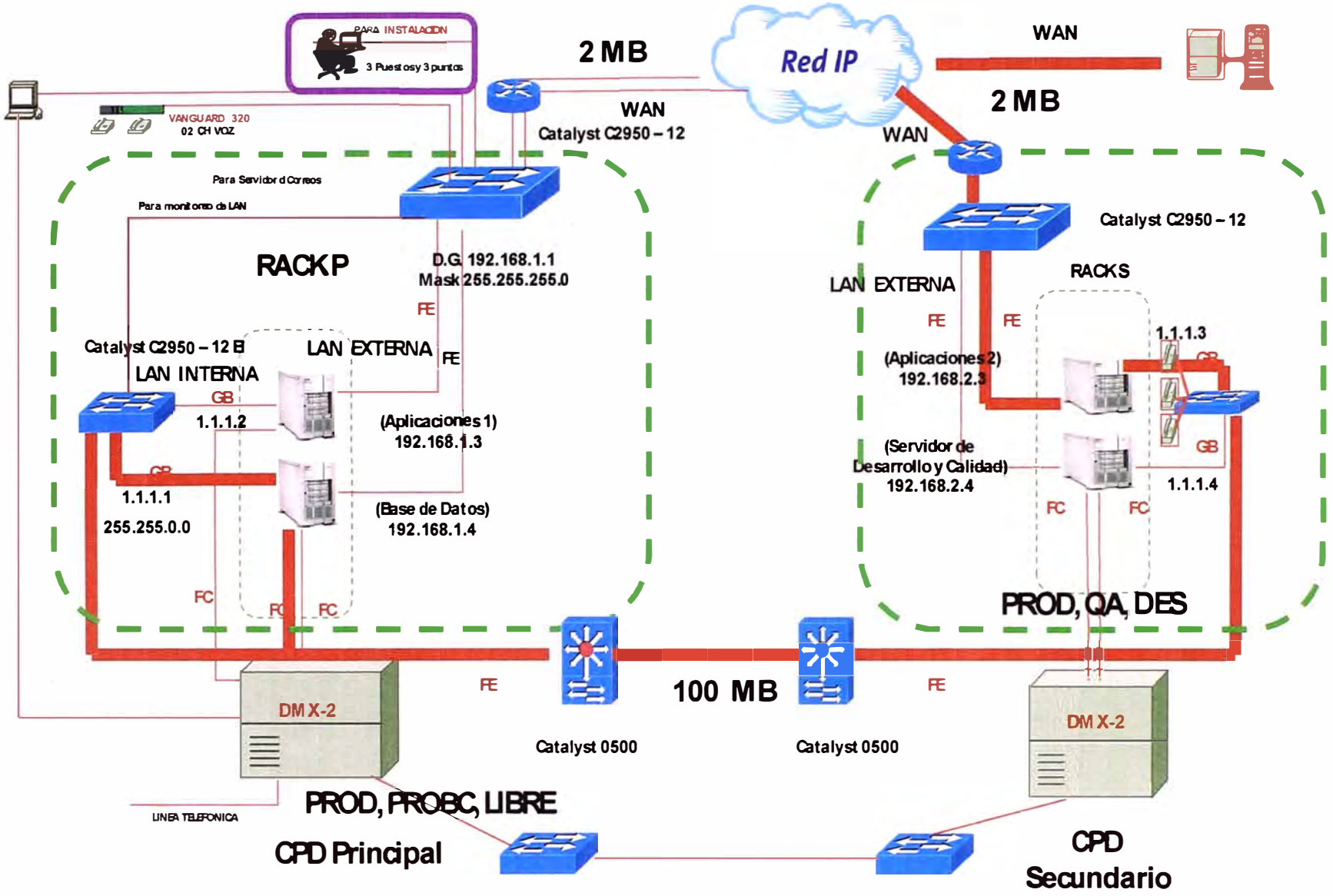


Figura F.4 Consulta del Servidor de Aplicaciones 2 al Servidor de Base de Datos

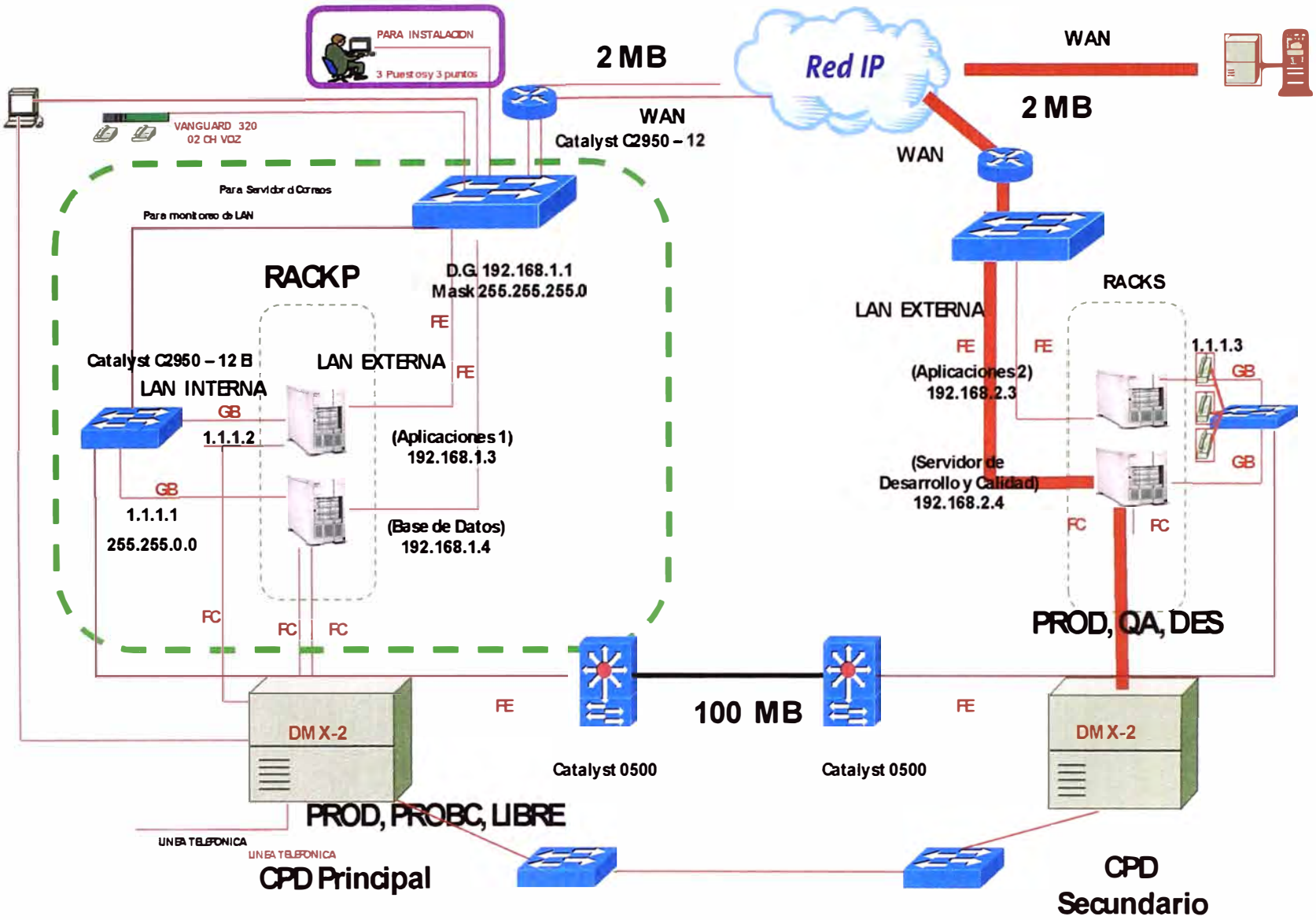


Figura F.5 Consulta al Servidor de Desarrollo y Calidad

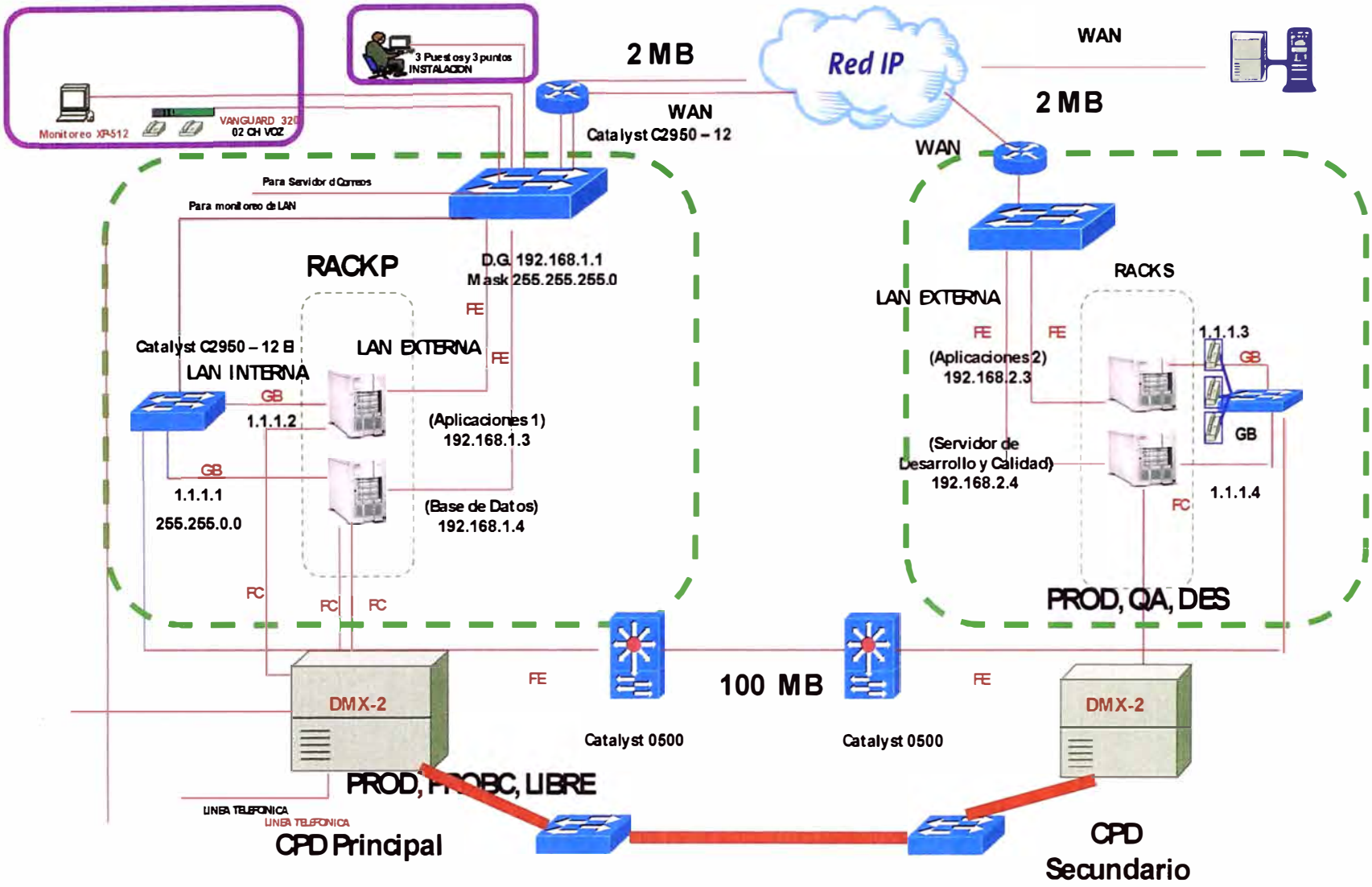


Figura F.6 Replicación del Emplazamiento Principal al Secundario

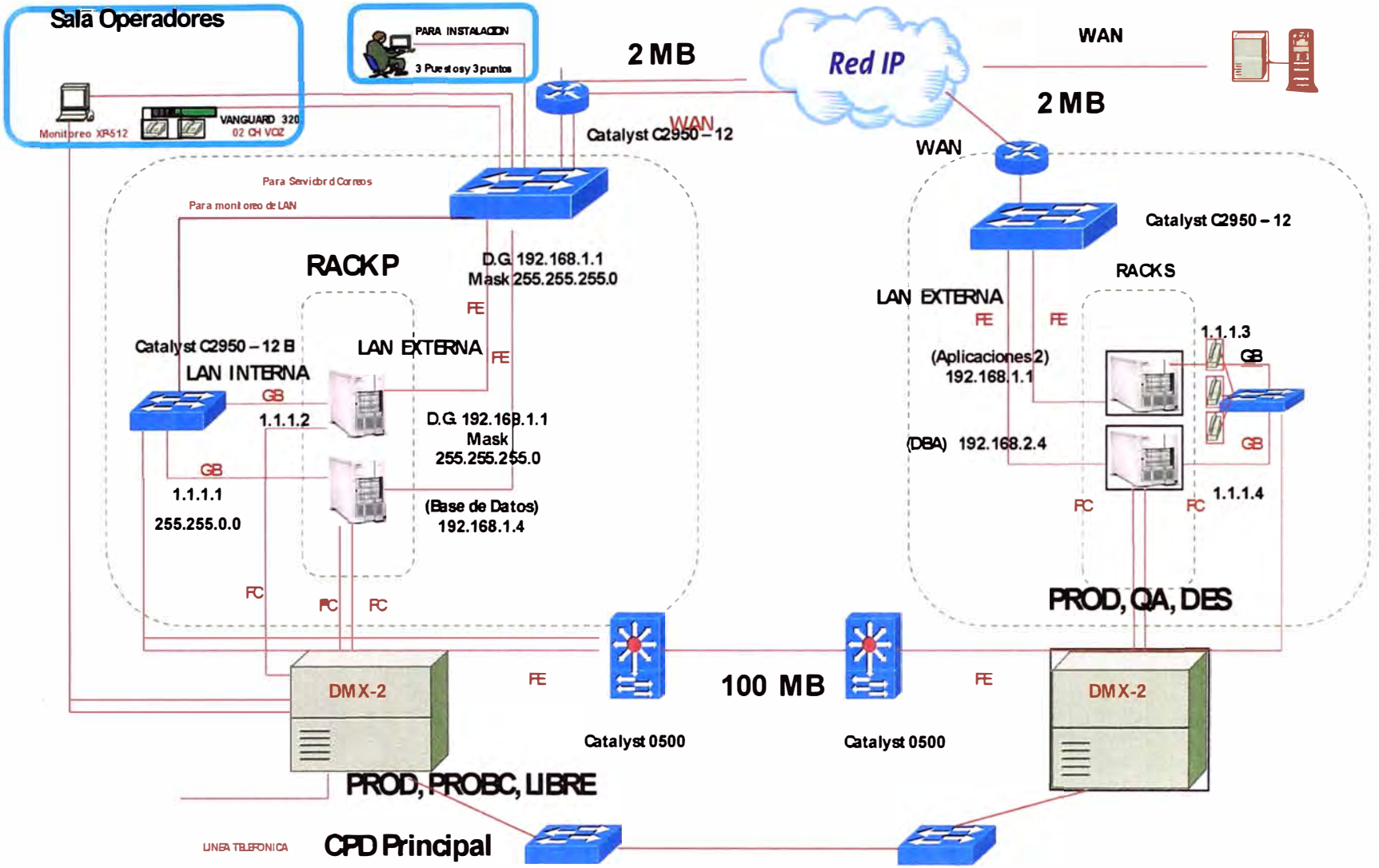


Figura F.7 Servidor del Emplazamiento Secundario ahora brindaran servicio

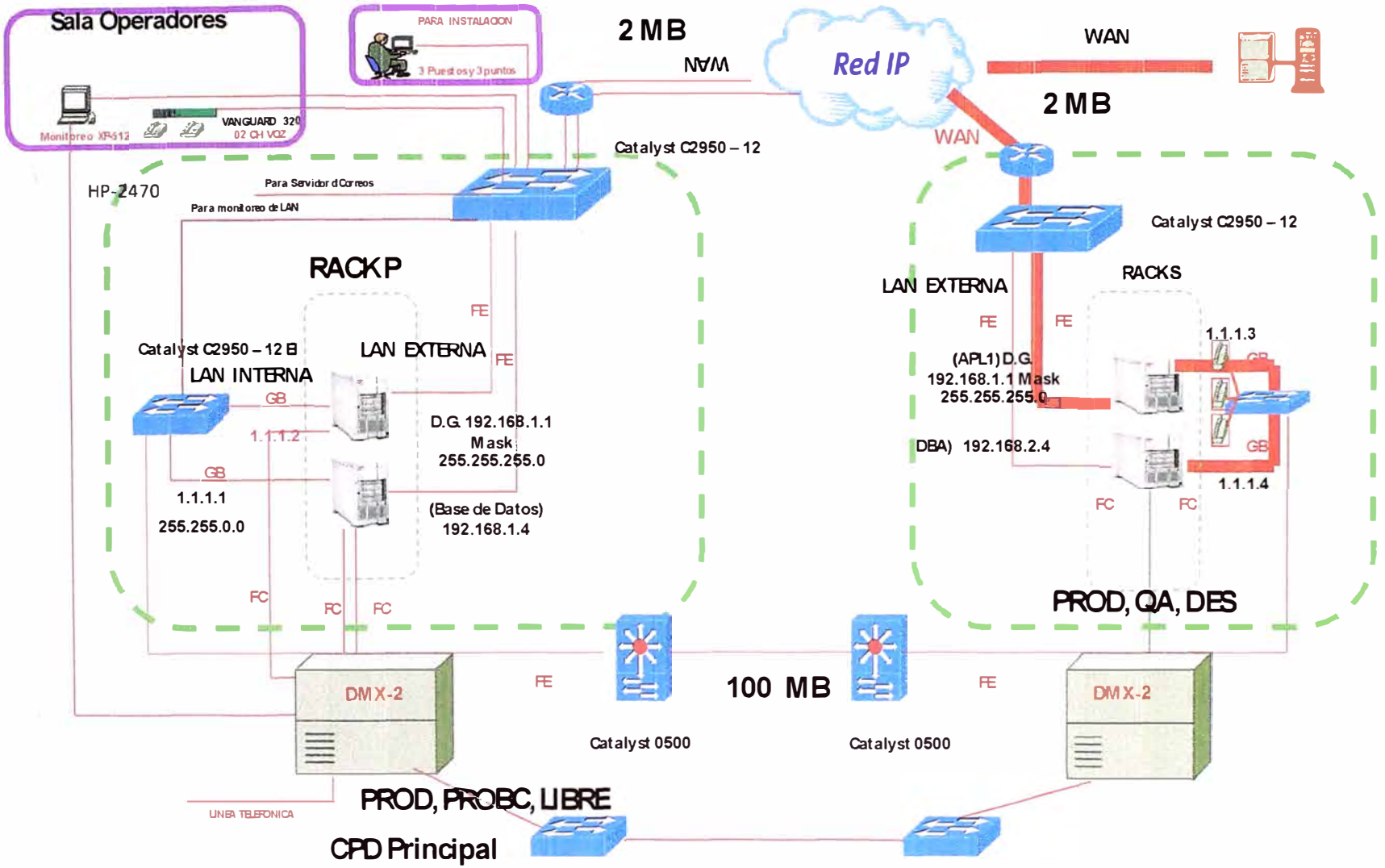


Figura F.8 Producción en el Emplazamiento Secundario

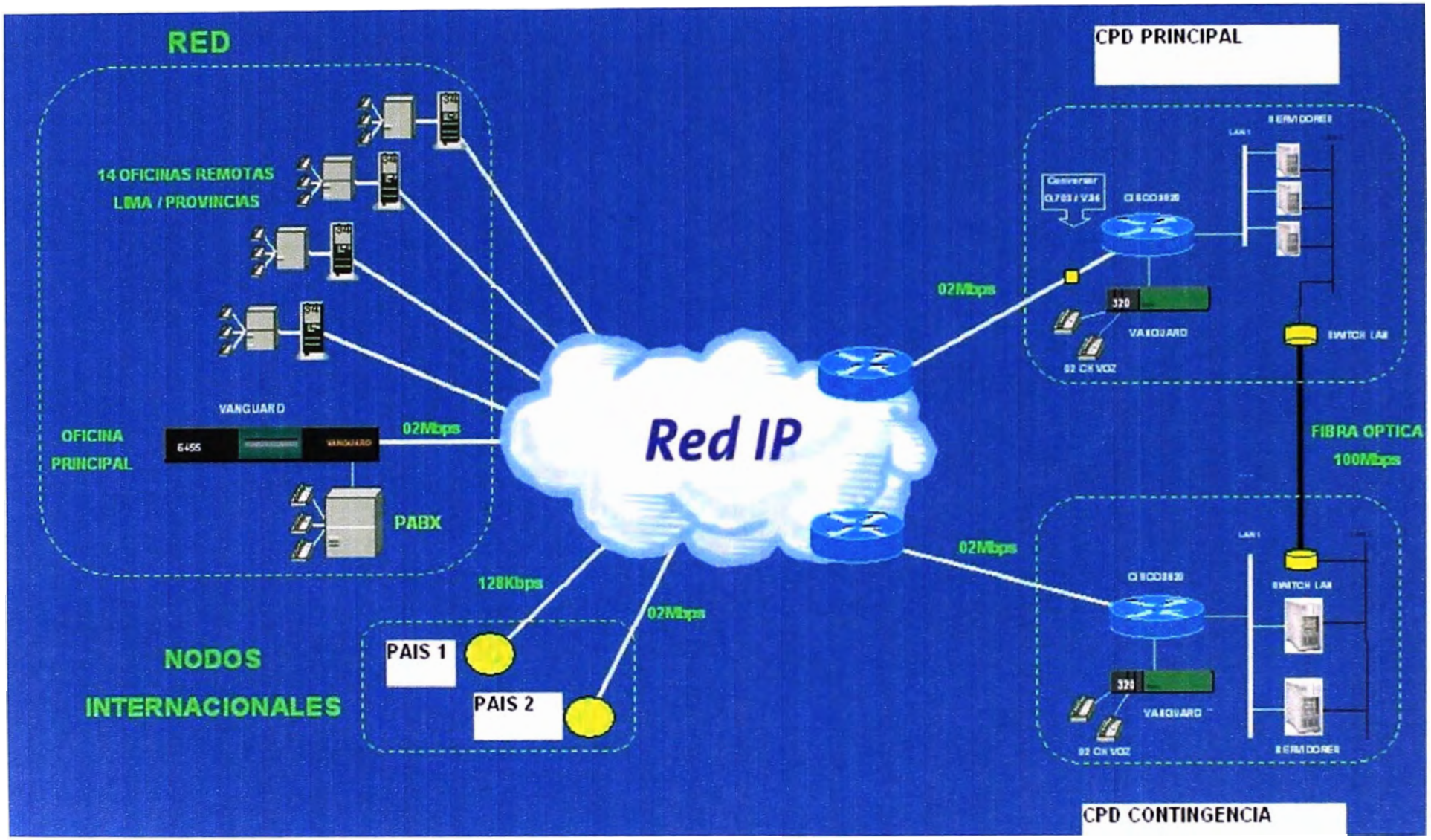


Figura F.9 IP-VPN de distintas sedes del cliente y los CPD

ANEXO I
GLOSARIO DE TÉRMINOS

AA	Aire Acondicionado
ANSI	American National Standards Institute
ATA	Advanced Technology Attachment
Backup	Es la copia total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento
Benchmarks	Técnica utilizada para medir el rendimiento de un sistema o componente de un sistema
BIOS	Sistema básico de entrada/salida de datos
CCTV	Circuito cerrado de televisión
CIFS	Common Internet File System
Cintotecas	Sala donde se almacena las cintas de respaldo
CPD	Ver Data Center.
CPU	Unidad de proceso central
CSMA/CD	Accesos múltiple por sensado de portadora/ Detección de colisiones
DAS	Direct Attached Storage, almacenamiento directamente conectado
Data Center	Centro de procesamiento de datos o CPD. Ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. En Iberoamérica se le conoce como centro de cómputo, y en España cómo centro de cálculo, también se usa la denominación "Centro de Datos" por su equivalente en inglés "Data Center".
DNS	Domain Name System, permiten conectarse con la máquina sin necesidad de usar una dirección IP, por ejemplo 190.81.186.12; basta con ingresar el nombre de dominio, (por ejemplo www.orce.uni.edu.pe), para que el servidor DNS resuelva y establezca una conexión.
Firewall	Es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado
Firmware	Es un bloque de instrucciones de programa para propósitos específicos
ERP	Sistemas de planificación de recursos empresariales
Esclusa	Balance donde separa el ingreso a la Sala de equipos
Ethernet	Estándar de redes de computadoras de área local con CSMA/CD
GE	Grupo Electrógeno

Host	Cualquier dispositivo terminal en una red de datos, tal cómo un ordenador, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora.
Hot spare	Unidades preinstaladas que pueden usarse inmediatamente
Hot swapping	Referencia a la capacidad de algunos componentes hardware para sufrir su instalación o sustitución sin necesidad de detener
HP-UX	Es la versión de Unix desarrollada y mantenida por Hewlett-Packard desde 1983
HTTP	Hypertext Transfer Protocol
IDC	International Data Corporation
Infointernet	es el servicio de conexión a Internet simétrico y permanente a través de la Red IP MPLS lo cual permite una total gestión del enlace.
IP	Protocolo de Internet.
ISCSI	INTERNET Small Computer System Interface
Isócrono	Realizado en el mismo *tiempo o con el mismo ritmo que otra acción o movimiento
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
JBOD	Just a Bunch Of Drives (concatenación)
LUN	Logical Unit Number. Partición de unidad de almacenamiento.
LSM	Living Stream Media
LVM	Logical volume manager
Main Frame	Es un Servidor grande, potente y costosa usada principalmente por una gran compañía para el procesamiento de una gran cantidad de datos
Memoria Caché	Sistema especial de almacenamiento de alta velocidad.
MPLS	Es una nueva tecnología de conmutación creada para proporcionar circuitos virtuales en las redes IP
MTBF	Mean Time Between Failures. Tiempo medio entre fallas
MTTF	Mean Time to Failure. Tiempo promedio para que falle
NAS	Tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador
NFS	Network File System
Networking	Interconexión de cualquier grupo de computadores, impresoras,

	routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.
ODF	Dispositivo pasivo en el cual se conectan cables, permitiendo que interconexiones arbitrarias puedan ser hechas..
Outsourcing	Tercerización.
OpenVMS	Sistema de Memoria Virtual.
PA-RISC	Nombre por el que se conoce una arquitectura de microprocesadores desarrollada por sistemas Hewlett-Packard.
RAID	Redundant Array of Independent Disk.
RDSI	Red Digital de Servicios Integrados.
ROUTER	Enrutador, encaminador. Dispositivo hardware o software para interconexión de redes de computadoras.
RTB	Red Telefónica Básica.
SAN	Storage Area Network.
SAS	Serial Attached SCSI.
SATA	Serial Advanced Technology Attachment.
SCSI	Small Computer System Interface.
SLA	Service Level Agreement.
SMB	Server Message Block.
Snapshot	Copia de una imagen en algún tiempo para ser restaurado
SMB	Server Message Block.
Storages	Equipos que sirve para almacenar (Gigas ,Terras de Datos).
Striping	the technique of segmenting logically sequential data.
Switch	dispositivo digital de lógica de interconexión entre redes
TCP	Transmission Control Protocol.
TIC	Tecnologías de la Información y la Comunicación.
Trunk	('troncal') designa una conexión de red que transporta múltiples VLANs identificadas por etiquetas (o *tags*) insertadas en sus paquetes.
TTA	Tablero de transferencia automática.
TTM	Tiempo que toma desde que un producto o servicio es concebido, hasta que está disponible para la venta.
Uptime	Tiempo que tu sistema esta arriba.
UPS	Uninterruptible Power Supply, o Sistema de potencia ininterrumpida. Consiste de un banco de baterías que puede

	proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de las funciones de los UPS es la de mejorar la calidad de la energía eléctrica que llega a los aparatos, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de Corriente Alterna.
VLAN	red de área local virtual es un método de crear redes lógicamente independientes dentro de una misma red física.
VPN	red privada virtual, se construye a base de conexiones realizadas sobre una infraestructura compartida.
Verisign	Proveedor de confianza de servicios de infraestructura de Internet
VSE	Virtual Storage Extended.

BIBLIOGRAFÍA

1. Richard Barker, Paul Massiglia, "Storage Area Networking Essentials" USA 2001 [ISBN: 0471034452]
2. Cisco System "Academia de Networking de Cisco Sytem, Guía del Primer Año CCNA 1 y 2 " Madrid 2004 ISBN: 842054079
3. Hp Corporation "HP StorageWorks SAN design reference guide c00403562.pdf", http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00403562/c00403562.pdf
4. Hp Corporation "HP StorageWorks SAN Designer v1.0 user guide c01079853.pdf", http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01079853/c01079853.pdf
5. Hp Corporation "HP StorageWorks B-Series remote replication solution best practices guide c01081582.pdf ", http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01081582/c01081582.pdf
6. Hp Corporation "HP StorageWorks XP Disk Array Configuration Guide for NonStop guia c01806402.pdf", http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01806402/c01806402.pdf
7. Hp Corporation "HP Integrity rx2660, rx3600, and rx6600 Servers Errata documento guía c01868340.pdf ",http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01868340/c01868340.pdf
8. Telefónica del Perú "Servicios IP-VPN".