UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE CIENCIAS

Tema:

Implementación de un DataCenter para la empresa GesCond247

Nombres: **Moreno Vera, Felipe Adrian (20120354I)**

Pecho Chavez, Augusto Manuel (20124061F)

Curso: **Núcleo y Redes para la Computación Paralela**

Codigo Curso: **CC482**

2016-II

Agradecemos a Wikipedia, Google-Sama, por la cantidad de información brindada y ayudarnos a solucionar nuestras dudas
Ayer, hoy y siempre.

TABLA DE CONTENIDOS

RESUMEN

Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.
Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, computadoras y redes de comunicaciones.

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

Entre los factores más importantes que motivan la creación de un CPD se puede destacar el garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicadas, así como servidores de bases de datos que puedan contener información crítica.

1.- INTRODUCCIÓN

GesCond247 es una empresa dedicada a la solución de gestión y monitoreo de condominios, usando tecnologías que están a la vanguardia del dia a dia.

Cuenta con una linea de investigación dedicada al mejoramiento de la monitorización con adiciones del campo de domótica a su gestión el cual se basa en una red de sensores dispuesto en lugares estratégicos para control de luces, o dispositivos electrónicos conectados a la nube.

Basado por ahora en un servidor local que maneja los dispositivos y la comunicación entre ellos, mediante el protocolo MQTT.

Tecnológicamente, GesCond247 emprende con ahora pocos equipos de cómputo y servidores, para suplir las necesidades principales de administración y seguimiento de los datos sensados.

1.1 Infraestructura de Data-Center

El DataCenter es el sitio donde se agrupan todos los recursos necesarios para el procesamiento de información y comunicaciones de la empresa.

Los recursos consisten en dependencias adecuadamente acondicionadas, computadoras y equipos de redes y comunicaciones.

Como objetivo GesCong247 necesita un Datacenter adecuado para almacenar los datos procesados de sus sensores que cambian de estado debido a las necesidades de cada cliente. Para garantizar la continuidad del servicio a clientes, incluso provedorees de dichos dispositivos y empresas colaboradoras, se necesita un lugar donde la protección física de los equipos informáticos o de comunicaciones es prioridad, así como también de los servidores de las bases de datos que pueden contener información.

1.1.1 Inventario de equipos Servidores

1.1.2 Inventario de equipos de redes y comunicaciones

1.1.3 Servicios Implementados

1.2 Distribución de red LAN

1.2.1 Plano de distribución LAN

1.3 Distribución de red WAN

1.3.1 Diagrama de distribución red WAN

1.4 Levantamiento de Necesidades Técnicas

Los requerimientos técnicos están divididos en varios puntos, teniendo en cuenta que no se iniciará a partir de cero en esta implementación.

1.4.1 Referente a Infraestructura de Data-Center

La infraestructura del DataCenter es una estructura compleja, que permitirá almacenar todos los sistemas de información de la empresa ubicados en los servidores, se debe tomar en cuenta aspectos desde el punto de vista arquitectónico tales como espacio físico, subsistema eléctrico, seguridad de acceso, sistema de detección de incendios.

En la implementación del DataCenter, la característica principal es tratar de eliminar en lo posible los puntos de falla y aumentar la redundancia yconfiabilidad de los servicios y la disponibilidad de la información que maneja la empresa. Como guía de las características de un DataCenter, seguiremos la norma TIA-942, que define claramente en su propósito indicar las mejores prácticas industriales, de construcción y activación del centro de datos en todos sus aspectos, tanto arquitectónicos como tecnológicos, con la finalidad de garantizar seguridad operacional, continuidad del servicio, disponibilidad y solidez.

1.4.2 Referente a Cableado Estructurado y comunicaciones

Adecuación de Áreas Nuevas:

El cableado de “GesCond247” fue realizado en el año 2010 bajo categoría 5E, por presupuestos y decisión administrativa no se considera cambios en el cableado actual del edificio, a excepción de las nuevas oficinas, que serán las áreas de capacitación, auditorio, donde se instalará un cableado estructurado de forma segmentada y se colocaran concentradores por cada área y de estos se conectará hacia el DataCenter.

Cableado estructurado en el DataCenter:

Es necesaria una reubicación del cableado estructurado que llega al DataCenter, conservando criterios de modularidad, basándose en la topología de DataCenter reducido. Por consideraciones de espacio en

el desarrollo del proyecto, se mostrará la adecuación definitiva y organización de los racks.

Telecomunicaciones:

Para telecomunicaciones se depende de proveedores externos, quienes brindan el servicio de enlace dedicado de datos y servicio de Internet, por lo que se plantea el requerimiento de unificar la administración de las comunicaciones con proveedores de servicios externos y enlaces de datos con los puntos de venta, además de colocar enlaces secundarios de respaldo en los principales puntos de distribución, oficinas y supermercados, garantizando una comunicación redundante hacia los puntos remotos, esto implica retirar algunos servicios, mantener otros y contratar nuevos, con la finalidad de tener una infraestructura de comunicaciones robusta, estable y económica, sobre todo con los puntos remotos que tengan mayor nivel de criticidad, en cuanto a necesitad de comunicación en línea.

1.4.3 Referente a Equipamiento, remplazo o reutilización

En referencia a equipamiento, se debe tomar en cuenta los elementos de red tanto activos como pasivos de la infraestructura del DataCenter, los elementos activos son los equipos que consumen energía eléctrica tales como switches, routers, módems, etc., los equipos pasivos son aquellos que no consumen energía o sirven para transportarla tal como cableado, racks, tomas eléctricas, patch panels, canaletas, etc. Como adicional, están los equipos computacionales que se destinarán al DataCenter tales como CPU, servidores, dispositivos de almacenamiento, elementos de central telefónica. El requerimiento que se recoge a este aspecto es ya contando con el inventario de dispositivos recopilado previamente. Según lo recopilado, se detalla los siguientes requerimientos:

a) Conservar los servidores de los sistemas LISA

b) Conservar los servidores de correo electrónico

c) Implementar un storage para almacenamiento de base de datos

d) Desactivar la central telefónica de “GesCond247” incluyendo los teléfonos convencionales.

e) Implementar un servicio de central telefónica IP para que provea el servicio al “GesCond247” incluyendo teléfonos IP para distribuirlos en oficinas y puntos de venta.

f) Adquirir nuevos equipos activos de red para soportar el paso de datos y voz IP y reemplazar los equipos actuales.

g) Reutilizar los equipos activos de red en los sectores que se requiera.

1.4.4 Referente a servicios, actualización o implementación

Es necesario evaluar los sistemas que se encuentran trabajando como:

a) ERP se debe conservar en funcionamiento y la migración de ubicación de servidores debe ser transparente al usuario final.

b) Conservar el servicio de correo electrónico y navegación que posee.

c) Servicios adicionales para áreas específicas de la empresa incluidos los de desarrollo interno.

d) Cubos (Información financiera)

e) PL (Logística y Certificación de despacho)

f) Es necesario incorporar un nuevo servicio de control de dominio y directorio activo bajo el nombre “GesCond247” y asociar a todos los equipos computacionales a este nuevo dominio para mejor control de usuarios y políticas de seguridad.

g) Se implementará el uso del antivirus corporativo para colocarlo en toda la empresa con una administración y distribución de actualizaciones centralizada.

h) Se debe implementar un servicio de actualizaciones automáticas de aplicaciones Windows al que tengan acceso todos los equipos computacionales de la empresa.

i) Se debe activar el servicio de asignación dinámica de direcciones IP DHCP previo un análisis de equipos que requieren una dirección IP estática, equipos que necesitan asignación dinámica con acceso a Internet tanto navegación como servicios web y los que requieren asignación dinámica con acceso únicamente a la red interna para funcionamiento de los sistemas que utilicen.

j) Se implementará el uso del antivirus corporativo para colocarlo en toda la empresa con una administración y distribución de actualizaciones centralizada.

1.5 Levantamiento de Requerimientos Administrativos

Los requerimientos en el aspecto administrativo se detallan en base a como se desea manejar la cultura del área de administración de servicios de redes y telecomunicaciones así como también de los usuarios, se planea mejorar con estas recomendaciones la manera de administrar el personal y el comportamiento de los usuarios con respecto a su trabajo, a la utilización de servicios y aprovechamiento de recursos.

1.5.1 Referente a unificación y administración de Servicios

Los servidores, sistemas y servicios, así como monitoreo de enlaces serán administrados por el área de Redes Servicios y Telecomunicaciones en los que trabajan dos personas. En un comienzo, cada uno tendrá que seguir con el trabajo que ha ido desarrollando en la empresa y sus conocimientos deberán ser compartidos entre ellos para poder alcanzar un nivel homogéneo tal que las funciones puedan ser compartidas y suplidas en caso de que uno de ellos no se encontrase en el momento que se lo requiera.

1.5.2 Referente a procedimientos Implementación Data Center

Los procedimientos que se elaborarán serán guías documentadas de los pasos a seguir para la realización de tareas específicas de la administración de sistemas de redes y telecomunicaciones. Varios de estos procedimientos deben establecerse claramente y servirán como parte de la información y conocimiento. Los procedimientos que debe tener el área de redes y servicios se establecerán según lo requerido por el área administrativa y la gerencia de sistemas, mismos que deberán ser documentados y publicados para conocimiento del personal que los vaya a utilizar como son los siguientes:

a) Configuración de equipos Cliente

b) Creación de Usuarios y asignación de permisosc) Creación de Cuentas de Correo

d) Asignación de permisos para servicios Web

e) Mantenimiento de sistemas y bases de datos

1.5.3 Referente a políticas de uso de servicios y equipos.

Las políticas son guías tanto para el personal administrativo del área de sistemas como para conocimiento del usuario final de cómo debe manejarse frente a la utilización de los accesos otorgados a sistemas o servicios y el manejo de la información, esto permitirá que el personal se acople a reglas claras y de beneficio tanto para sí mismos como para la empresa en el desempeño diario de su trabajo.

Las políticas a establecer son en los siguientes puntos:

a) Política de uso del correo electrónico

b) Política de uso de Internet

c) Política de confidencialidad y manejo de la información empresarial.

2.- FUNDAMENTO TEÓRICO DEL PROYECTO

Debido a la naturaleza del proyecto y a la necesidad de saber lo que está se realizando es indispensable tener conocimiento teórico de todo lo que se va a realizar, por eso es necesario tener claros algunos conceptos y puntos clave que repasaremos a continuación.

2.1 Redes LAN y WAN

La fusión de las computadoras y las comunicaciones ha tenido una profunda influencia en cuanto a la manera en que se organizan los sistemas de cómputo. El concepto una vez dominante del “centro de cómputo” como un salón con una gran computadora a la que los usuarios llevaban su trabajo para procesarlo es ahora totalmente obsoleto (aunque los centros de datos que contienen miles de servidores de Internet se están volviendo comunes). El viejo modelo de una sola computadora para atender todas las necesidades computacionales de la organización se ha reemplazado por uno en el que un gran número de computadoras separadas pero interconectadas realizan el trabajo. A estos sistemas se les conoce como redes de computadoras [2].

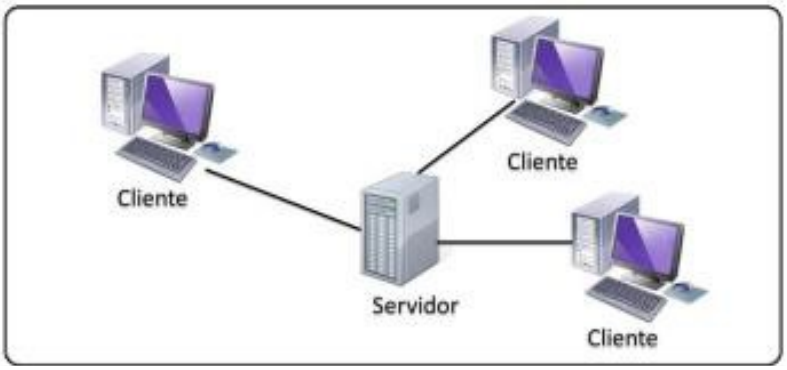
El modelo que se utilizará en esta empresa es conocido como Modelo Cliente-Servidor, donde existen varios clientes (algunos en la oficina y otros en lugares más apartados dentro de la empresa), que requieren acceder a la información que generalmente está contenida en las

principales oficinas de la empresa y que es replicada a los diversos puntos necesarios.

El modelo cliente-servidor se comporta de la siguiente manera:

a) El proceso cliente envía una solicitud a través de la red al proceso servidor y espera una respuesta.

b) Cuando el proceso servidor recibe la solicitud, realiza el trabajo que se le pide o busca los datos solicitados y devuelve una respuesta.



2.1.1 Fundamentos de Redes LAN

Las redes de área local, generalmente llamadas LAN (Local Area Networks), son redes de propiedad privada que operan dentro de un solo edificio, como una casa, oficina o fábrica. Las redes LAN se utilizan ampliamente para conectar computadoras personales y electrodomésticos con el fin de compartir recursos (por ejemplo, impresoras) e intercambiar información. Cuando las empresas utilizan redes LAN se les conoce como redes empresariales.

La topología de muchas redes LAN alámbricas está basada en los enlaces de punto a punto. El estándar IEEE 802.3, comúnmente conocido como Ethernet, es hasta ahora el tipo más común de LAN alámbrica [1].

2.1.2 Fundamentos de Redes WAN

Una Red de Área Amplia, o WAN (Wide Area Network), abarca una extensa área geográfica, por lo general un país o continente. Empezaremos nuestra discusión con las redes WAN alámbricas y usaremos el ejemplo de una empresa con sucursales en distintas ciudades.

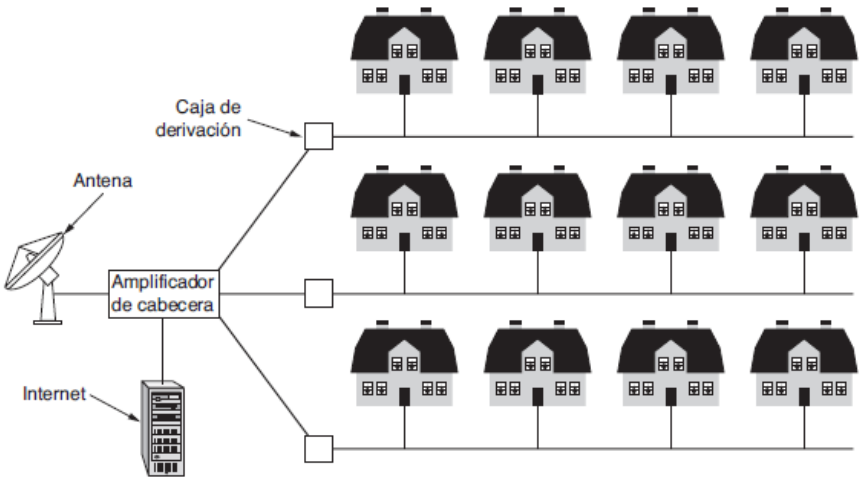
La WAN en la figura de este apartado es una red que conecta las oficinas en Perth, Melbourne y Brisbane. Cada una de estas oficinas

contiene computadoras destinadas a ejecutar programas de usuario (aplicaciones).

Seguiremos el uso tradicional y llamaremos a estas máquinas hosts. Al resto de la red que conecta estos hosts se le denomina subred de comunicación, o para abreviar sólo subred. La tarea de la subred es transportar los mensajes de host a host, al igual que el sistema telefónico transporta las palabras (en realidad sólo los sonidos) de la persona que habla a la persona que escucha.

En la mayoría de las redes WAN, la subred cuenta con dos componentes distintos: líneas de transmisión y elementos de conmutación. Las líneas de transmisión mueven bits entre máquinas. Se pueden fabricar a partir de alambre de cobre, fibra óptica o incluso enlaces de radio. Como la mayoría de las empresas no poseen líneas de transmisión, tienen que rentarlas a una compañía de telecomunicaciones.

Los elementos de conmutación o switches son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea entrante, el elemento de conmutación debe elegir una línea saliente hacia la cual reenviarlos. En el pasado, estas computadoras de conmutación han recibido varios nombres; ahora se conocen como enrutador [3].



2.1.3 Dispositivos de interconexión de redes

(Cisco, 2005) indica que los dispositivos que intervienen en todo el proceso de redes o networking se pueden clasificar en dos grupos: los

dispositivos de usuario final en los que constan computadores, impresoras, scanner, etc., que brindan servicio directamente al usuario y los dispositivos de red que son los que se conectan entre sí a los dispositivos de usuario final.

Los dispositivos de red más conocidos son:

Repetidores: son dispositivos utilizados para regenerar una señal, debido a que en su camino de origen a destino se ve afectada por diversos factores que producen atenuación y es necesario se reconstruya dicha señal con la finalidad de mantener fidelidad en la transmisión de datos. El propósito del repetidor es regenerar y re-temporizar las señales de red a nivel de los bits, para permitir que los bit viajen a mayor distancia a través de los medios.

Puentes: son dispositivos encargados de proporcionar conexiones entre LAN, realizando una administración básica de la transmisión de datos, determinando en los paquetes que se transmiten cuales deben pasar de un sector a otro de la red cruzando el puente; se utilizan para dividir una LAN grande en segmentos más pequeños, más fáciles de manejar y la función del puente es tomar decisiones inteligentes con respecto a pasar las señales al siguiente segmento de la red.

Switches: estos dispositivos concentran múltiples conexiones, además agregan más inteligencia en la administración de la transferencia de los datos, ya que determinan si los datos permanecen en la LAN y también tienen la capacidad de transmitir los datos hacia la conexión especifica que necesita dichos datos. Al igual que los puentes, los switches aprenden y utilizan información sobre los paquetes de datos para generar tablas de envío, y localizar los destinatarios en la red. Un switch tiene muchos puertos con varios segmentos de red conectados a él; tiene la capacidad de elegir el puerto al cual el dispositivo de destino está conectado para enviar los paquetes; este proceso se conoce como conmutación de paquetes.

Routers: además de poseer las características de los dispositivos anteriores, su principal función es conectarse a una WAN, con la finalidad de conectar LAN’s que se encuentran separadas por grandes distancias, estableciendo unaruta de llegada desde la red

origen hacia la red destino; en la mayoría de las WAN’s, la red contiene numerosas líneas de transmisión, cada una de las cuales conecta un par de enrutadores, si dos enrutadores que no comparten una línea de transmisión quieren conectarse, deberán hacerlo de manera indirecta a través de otros enrutadores, estas líneas de comunicación a través de varios dispositivos de conmutación se conocen como rutas. Cuando un paquete es enviado desde un enrutador a otro a través de uno o más enrutadores intermedios, el paquete se recibe en cada enrutador intermedio en su totalidad, se almacena ahí hasta que la línea de salida requerida esté libre y por último se reenvía.

2.1.4 Topología de Redes

La topología de red define la estructura de cómo se encuentra establecida una red, se definen dos partes de la topología de redes:

Topología Física: Corresponde a la disposición real de los cables o medios de interconexión, las topologías físicas más comúnmente usadas son las siguientes:

a) BUS: Una topología de bus usa un solo cable backbone que debe terminarse en ambos extremos, todos los hosts se conectan a este backbone.

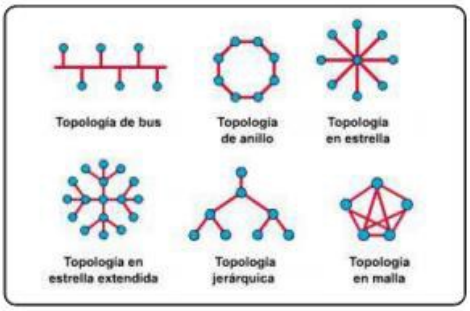
b) ANILLO: Conecta un host con el siguiente y al último host con el primero, esto crea un anillo físico de cable.

c) ESTRELLA: Conecta todos los cables con un punto central de concentración.

d) ESTRELLA EXTENDIDA: Conecta estrellas individuales entre sí mediante la conexión de hubs o switches, esta topología puede extender el alcance y la cobertura de la red.

e) JERARQUICA: Es similar a una estrella extendida, pero en lugar de conectar los switches entre sí, el sistema se conecta con un procesador principal que controla el tráfico de la topología.

f) MALLA: Se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio generando redundancia en las conexiones.



Topología Lógica: Es la forma de comunicarse los hosts a través del medio físico; las más conocidas son:

a) BROADCAST: Cada host envía datos hacia la red llegando a todos los hosts que se encuentran en la red, sin mantener un orden específico de quien debe transmitir y quién no.

b) TRANSMISION DE TOKENS: Se basa en el concepto de controlar el acceso a transmisión en la red, asignando un token electrónico a cada host en la red de forma secuencial, de tal manera que cuando un host recibe el token es quien tiene el turno de enviar los datos a la red, si no lo tiene, pasa el token al siguiente host hasta llegar al último host de la red.

2.1.5 Protocolos De Transmisión

Por lo general, a la capa que está arriba de la capa de interred en el modelo TCP/IP se le conoce como capa de transporte; y está diseñada para permitir que las entidades pares, en los nodos de origen y de destino, lleven a cabo una conversación, al igual que en la capa de transporte de OSI. Aquí se definieron dos protocolos de transporte de extremo a extremo. El primero, TCP (Protocolo de Control de la Transmisión, del inglés Transmission Control Protocol), es un protocolo confiable orientado a la conexión que permite que un flujo de bytes originado en una máquina se entregue sin errores a cualquier otra máquina en la interred. Este protocolo segmenta el flujo de bytes entrante en mensajes discretos y pasa cada uno a la capa de interred. En el destino, el proceso TCP receptor vuelve a ensamblar los mensajes recibidos para formar el flujo de salida. El TCP también maneja el control de flujo para asegurar que un emisor rápido no pueda inundar a un receptor lento con más mensajes de los que pueda manejar.

El segundo protocolo en esta capa, UDP (Protocolo de Datagrama de Usuario, del inglés User Datagram Protocol), es un protocolo sin conexión, no confiable para aplicaciones que no desean la asignación de secuencia o el control de flujo de TCP y prefieren proveerlos por su cuenta. También se utiliza mucho en las consultas de petición-respuesta de una sola ocasión del tipo cliente-servidor, y en las aplicaciones en las que es más importante una entrega oportuna que una entrega precisa, como en la transmisión de voz o video [4].

2.2 Estándar TIA – 942 (Resumen)

2.2.1 Generalidades.

La Asociación de Industrias de Telecomunicaciones (TIA por sus siglas en inglés) tenía la intención de unificar diversos criterios y recomendaciones acerca del diseño de áreas de tecnología y comunicaciones, en Abril del año 2005, se realiza la primera publicación del estándar TIA-942 Telecomunications Infraestructure Standard for Datacenters, en asociación con la Alianza de Industrias Electrónicas (EIA por sus siglas en inglés), que inició como una serie de especificaciones orientadas exclusivamente para comunicaciones y cableado estructurado, posteriormente se incrementa lineamientos para los subsistemas de infraestructura y define como el objetivo o propósito de la publicación de esta norma o estándar, proveer una serie de recomendaciones y guidelines para el diseño e implementación de un DataCenter, con características adecuadas para brindar el respaldo apropiado para todo el equipamiento crítico de hardware y mantener una disponibilidad de sistemas conforme a la demanda de la línea de negocio.

El estándar TIA-942 fue desarrollado por el TIA TR-42.1.1 Network Distribution Nodes subcomitee bajo el proyecto No. 3-0092 con la participación de firmas de arquitectos e ingenieros, consultores, fabricantes y usuarios finales.

La norma o estándar TIA-942 consta de ocho capítulos organizados de la siguiente manera:

a) Alcance

b) Definición de términos, acrónimos, Unidades de Medida

c) Descripción del diseño del DataCenter

d) Infraestructura de Sistema de cableado de DataCenter

e) DataCenter Telecomunicaciones, espacios y topologías relacionadas

f) Sistemas de cableado de DataCenter

g) Vías de Cableados para DataCenter

h) Redundancia de DataCenter

Además cuenta con nueve anexos complementarios e informativos, según la norma que complementan las recomendaciones que los capítulos mencionan.

A. Consideraciones de diseño de Cableado

B. Administración de Infraestructura de telecomunicaciones

C. Información de proveedores de acceso

D. Coordinación de los planes del equipo con otros ingenieros

E. Consideraciones de espacio de DataCenter

F. Selección de Sitio

G. Niveles de infraestructura de DataCenter

2.2.2 Diseño de Data Center

Un DataCenter generalmente incluye los siguientes espacios:

a) Sala de ingreso: espacio usado como interfaz entre el cableado estructurado del DataCenter y el cableado del edificio, por lo general ubicado fuera de la sala de cómputo.

b) Área de distribución principal (MDA): incluye la conexión principal que es el punto central de distribución del cableado estructurado, cada DataCenter debe tener por lo menos una MDA que contenga routers principales, Switches de LAN core, SAN y PBX.

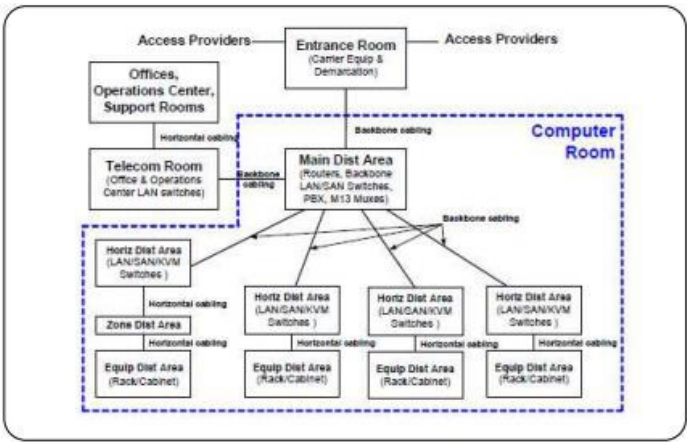
c) Área de distribución Horizontal (HDA): es usado para servir al equipamiento donde el cableado horizontal no está dentro del área de distribución principal, incluye switches de LAN, switches KVM para manejo de equipos ubicados en dicho sitio.

d) Área de distribución de zona (ZDA): es un área opcional como punto de interconexión dentro del cableado horizontal, ubicada entre el HDA y el EDA para permitir fácil reconfiguración y flexibilidad.

e) Área de distribución de equipamiento (EDA): es el espacio destinado para el equipamiento, incluyendo sistemas computacionales y equipamiento de telecomunicaciones.

Algunas áreas podrían no implementarse debido a la disponibilidad del ambiente.

Deben revisarse requerimientos como los siguientes:



a) Carga del piso incluyendo equipamiento, cables, patch cords y medios.

b) Requerimientos de facilidad de movimiento dentro del DataCenter

c) Requerimientos de flujo de aire

d) Requerimientos de montaje

e) Corriente y circuitos

f) Longitud de conectividad de equipamiento

2.2.3 Diseño de Cableado

El sistema de cableado debe ser una infraestructura que pueda soportar un ambiente multi-producto y multi-marca, se debe tomar en cuenta dos aspectos del cableado:

El cableado horizontal que es la porción de cableado que se extiende desde las terminaciones en el área de equipos a cada conexiónen el área de distribución horizontal, incluye cables, terminaciones y patch cords; la distancia del cableado horizontal de una terminación a otra debe tener un máximo de 90 metros para cableado de cobre y 300 metros en cableado de fibra óptica, para cableado de cobre se recomienda cable trenzado de 100-ohm categoría 6 y en fibra óptica multimodo entre 62.5/125 o 50/125 micrones o fibra monomodo.

El cableado de backbone está destinado a proveer conexiones entre las áreas de distribución principal y las demás áreas del DataCenter, consta de cableado de backbone, conexiones principales, conexiones horizontales, terminaciones mecánicas y patch cords; se recomienda

los mismos medios tanto para cableadode cobre como para fibra óptica así como también las distancias entre terminaciones.

2.2.4 Espacio

En el anexo E y F de la norma (TIA-942, 2005) se detalla lo referente a consideraciones de espacio y la selección de un sitio adecuado para el DataCenter, se recomienda que dentro del DataCenter deben ubicarse estrictamente los equipamientos destinados a funcionar dentro de esta zona y que se debe tener una zona específica para el almacenamiento de todo el material de mantenimiento y de repuesto, además de espacio para poder abrir y probar nuevo equipamiento previo a su instalación.

2.2.5 Flujo de Aire

La temperatura y humedad debe ser controlada para proveer una operación continua y debe estar bajo los siguientes rangos:

a) Temperatura 20°C a 25°C

b) Humedad relativa 40% a 55%

c) Máximo flujo 21°C

d) Cambio de temperatura por hora 5°C por hora

e) Equipamiento de humidificación se requiere.

En cuanto al flujo de aire y la ubicación de gabinetes, es necesario definir zonas específicas denominadas pasillos calientes y pasillos fríos, el pasillo frío se ubica en la parte frontal de los equipos y los pasillos calientes se ubican en la parte posterior de los equipos donde expulsan el aire para poder ser absorbido por el sistema de aire acondicionado (TIA-942).

2.2.6 Instalaciones eléctricas (Puesta Tierra)

Se recomienda circuitos dedicados para el uso del equipamiento del DataCenter, en conexiones debidamente distribuidas con voltaje 110V o 220 V según se requiera y además deben ser circuitos separados, deben estar provistos y terminados en su propio panel, debe tener salidas dobles (120 V 20 A) para herramientas y equipo de limpieza o equipos que no se deben conectar en las líneas de equipamiento. Las instalaciones eléctricas del DataCenter deben ser apoyadas por el sistema de generadores del DataCenter, de no

tenerlo debe ser conectado al sistema generador eléctrico del edificio.

2.2.7 Tiers o niveles de infraestructura de Data Center

Existen varios grados de disponibilidad de un DataCenter denominados TIERS, según el nivel más alto de TIER, mayor será el requerimiento de cubrir aspectos para asegurar un correcto funcionamiento del DataCenter y garantizar una mayor disponibilidad.

a) Tier 1 DataCenter Básico

El DataCenter de tipo Tier 1 puede admitir interrupciones sean estas planeadas o no, cuenta con sistema de aire acondicionado, distribución de energía, puede no tener piso falso también llamado piso técnico, UPS o generador eléctrico si los posee, pueden no tener redundancia; la carga máxima de los sistemas es el 100%. El DataCenter deberá estar fuera de servicio al menos una vez al año para mantenimiento, una falla en los componentes de su infraestructura puede causar la interrupción del DataCenter.

Tasa de disponibilidad máxima: 99.671%

b) Tier 2 Componentes Redundantes

En este nivel al tener componentes redundantes, el DataCenter es menos susceptible a interrupciones, sean planeadas o no, el DataCenter de tier 2 debe tener piso falso, UPS y generador eléctrico, pero está conectado a una sola línea de distribución eléctrica. El diseño (N+1) indica que existe al menos un duplicado por cada componente de la infraestructura; la carga máxima de los sistemas es del 100%. Una falla en la línea de distribución eléctrica puede causar una interrupción en el servicio.

Tasa de Disponibilidad máxima: 99.741%

c) Tier 3 Mantenimiento Concurrente

El DataCenter de Tier 3 permite realizar cualquier actividad planeada (mantenimiento, reparación o reemplazo) sobre cualquier componente de la infraestructura sin interrupciones en el servicio. Debe haber doble línea de distribución eléctrica; en este nivel actividades no planeadas aún pueden provocar una falla en el servicio, la carga máxima de los sistemas es del 90%.

Tasa de disponibilidad máxima: 99.982%

d) Tier 4 Tolerante A Fallas

El nivel 4 de Tier permite realizar cualquier actividad planeada sin interrupciones en la disponibilidad del servicio, y además permite seguir trabajando tolerando fallas en un evento crítico o no planeado, se necesita dos líneas de distribución eléctrica simultaneas, dos sistemas de UPS independientes, cada uno con redundancia (N+1); la carga máxima de los sistemas de 90%. Queda un nivel de exposición a fallas por extrema emergencia, ejemplo: un incendio o un apagado de emergencia (EPO), los mismos que existen para cumplir códigos de seguridad contra incendios o fallas eléctricas.

Tasa de disponibilidad máxima: 99.995%

2.3 Administración de Servicios y Sistemas

2.3.1 Active Directory

Según (Holem & Thomas, 2006) es el servicio de controlador de dominio, que provee prestaciones de directorio a clientes de la red.

Active Directory no es solo una base de datos, es una colección de archivos de soporte que incluyen logs de transacción y el volumen de sistema o sysvol, que contiene scripts de acceso e información de políticas de grupo. Cuenta con servicios que soportan y usan la base de datos incluyendo Lightwieght Directory Access Protocol (LDAP), kerberos security protocol, procesos de replicación y el file replication services (FRS). La base de datos y sus servicios se instalan en uno o más controladores de dominio. Un controlador de dominio es un servidor que ha sido promovido por la ejecución del asistente de instalación de Active Directory, una vez que el servidor se ha convertido en un controlador de dominio, almacena una copia del Active Directory; todos los cambios a la base de datos en cualquier controlador del dominio son replicados a todos los demás controladores dentro del dominio.

2.3.2 Unidades organizativas y directivas de seguridad

Los recursos de la empresa en Active Directory se representan como objetos o registros en la base de datos, cada objeto contiene varios atributos o propiedades que lo caracterizan; por ejemplo, un objeto usuario contiene el username y el password; un objeto de grupo

incluye el nombre y la lista de sus miembros. Active Directory es capaz de almacenar millones de objetos incluyendo usuarios, grupos, computadoras, impresoras, carpetas compartidas, sitios, enlaces a sitios, objetos de políticas de grupo (GPO), zonas DNS y registros de host; objetos que sin la debida estructura de acceso y administración serían imposibles de controlar (Holem & Thomas, 2006).

La estructura es función de un tipo de objeto específico llamado unidad organizativa (OU), que son los contenedores dentro de un dominio, que permiten agrupar objetos que comparten similar administración o configuración; aparte de organizar los objetos en Active Directory también suministra importantes características administrativas, porque provee un punto en donde funciones administrativas pueden ser delegadas y políticas de grupo pueden ser enlazadas. Las unidades organizativas son usadas para almacenar objetos como computadores y usuarios, están configurados similarmente y necesitan que cualquier configuración que se pueda hacer al sistema pueda ser manejado centralizadamente a través de una característica de Active Directory llamada política de grupo. Una política de grupo permite especificar configuraciones de seguridad, despliegue de software, y configurar el sistema operativo y aplicaciones sin tocar los equipos cliente; simplemente configurándolas dentro de una GPO.

Las políticas de grupo o GPOs son colecciones de cientos de posibles configuraciones, desde el acceso de los usuarios, hasta los privilegios para la ejecución de programas en el sistema. Una GPO está enlazada a un contenedor dentro de active directory, típicamente una OU; todos los usuarios y computadores incluidos en el contenedor son afectados por las configuraciones realizadas en la GPO.

2.3.3 DHCP

El protocolo de configuración dinámica de host (DHCP) sirve como una función básica de la infraestructura de red Microsoft Windows Server. DHCP provee a los hosts una configuración IP necesitada para comunicarse con otros equipos en la red, esta configuración incluye la dirección IP, la máscara de subred la puerta de enlace predeterminada y los servidores DNS.

DHCP es un estándar diseñado para reducir la complejidad de administración de las configuraciones de direcciones, basándose en una base de datos central de DHCP, automáticamente maneja la asignación de direcciones y configura otras características esenciales para los clientes en la red. Cuando un servidor de DHCP está disponible, los computadores que están configurados para obtener direcciones IP automáticas buscan y reciben dicha configuración del servidor el momento del arranque; cuando el servidor de DHCP no está disponible los clientes automáticamente adoptan una configuración alternativa o una dirección privada automática (APIPA).

La principal ventaja de usar DHCP es que estos servidores reducen grandemente el tiempo de configuración y reconfiguración de los computadores en la red, otra ventaja de DHCP es que la asignación automática de direcciones IP permite evitar errores que resultan de la configuración manual en cada equipo, previniendo conflictos de direcciones al tener dos equipos con la misma dirección.

2.3.4 Políticas de administración de Datos

Dentro de una empresa el activo intangible más importante y vital son los datos; es decir, la información de todo el movimiento de la empresa, su administración y su negocio. Toda la información está contenida en repositorios específicos a los cuales tiene acceso toda la red de usuarios, es necesario definir parámetros y políticas que garanticen una correcta administración, continuidad en la disponibilidad de los datos y acceso a los mismos, así como también respaldo y recuperación en caso de un evento fortuito.

Las políticas son documentos en los que debe constar detalladamente las normas que se deben tomar en cuenta para una correcta administración de la información y el uso de los recursos disponibles, adicionalmente se encuentran los procedimientos que detallan los pasos a seguir en el transcurso de administración de la información y accesos a la misma.

3.- IMPLEMENTACIÓN DEL PROYECTO (Datacenter, Equipos y Redes)

3.1 Adecuación Arquitectónica de Data-Center

Para las adecuaciones de tipo arquitectónico es necesario basarse en los requerimientos que ya han sido levantados, tomando en cuenta cuantos

rack se van a establecer en el DataCenter, calcular el espacio físico garantizando una adecuada ventilación y espacio disponible para el acceso, tanto frontal como posterior a los equipos.

El Data Center es un espacio ambientalmente controlado, que sirve al único propósito de albergar equipamiento y cableado directamente relacionado con los sistemas computacionales y otros sistemas de comunicaciones.

Existen varios requerimientos de los que se detallan los siguientes:

a) Requerimiento de carga de piso incluyendo equipamiento, cableado y medios.

b) Requerimientos de espacio para servicio (se requiere en cada lado el equipamiento un espacio adecuado para la manipulación de los equipos).

c) Requerimientos de flujo de aire

d) Requerimientos de armado

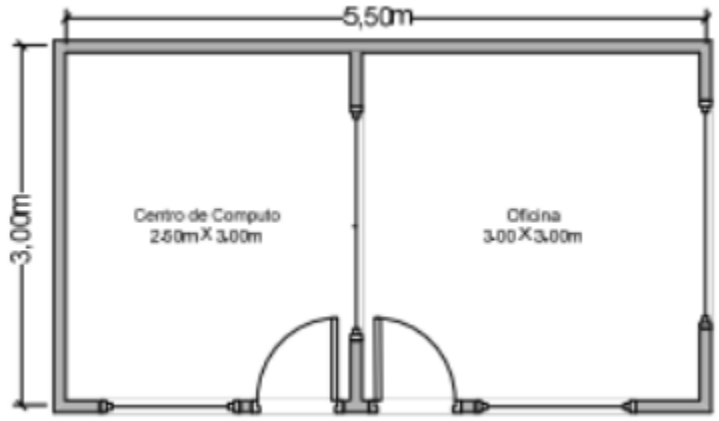
e) Requerimientos de energía eléctrica.

3.1.1 Cambios arquitectónicos

La norma TIA-942 sugiere para la selección de ubicación del cuarto de cómputo (computer room) : “se rechace ubicaciones que estén restringidas por componentes de la construcción que puedan limitar la expansión como elevadores, paredes externas, o paredes de construcción fijas. Se debe proveer la accesibilidad para el suministro de equipos de gran tamaño. La habitación debe encontrarse lejos de fuentes de interferencia electromagnética; por ejemplo las fuentes de ruido como son los transformadores de suministro de energía eléctrica, motores y generadores, equipos de rayos X, transmisores de radio o radar, y los dispositivos de sellado por inducción. La sala de informática no debe tener ventanas al exterior, las ventanas exteriores aumentan la carga de calor y reducen la seguridad”. En cuanto al tamaño del DataCenter, la norma TIA-942 indica lo siguiente: “el computer room debe ser dimensionado sabiendo los requerimientos de equipamiento específico incluyendo los debidos espacios libres; esta información puede ser obtenida de los proveedores del equipamiento. El dimensionamiento puede incluir proyección a futuro o requerimientos en el presente”, en el anexo E

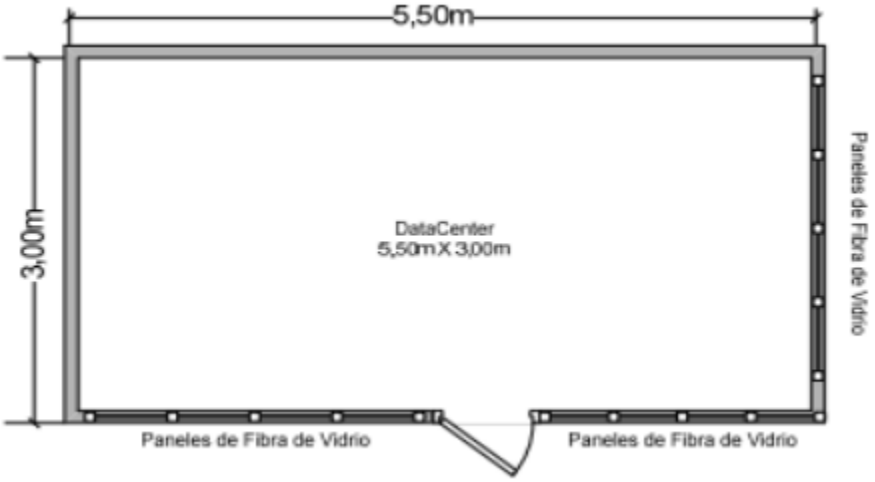
sugiere que: “El centro de datos debe tener una sala de almacenamiento de tamaño adecuado para que equipos en caja, los filtros de aire de repuesto, las baldosas del piso de repuesto, cables de repuesto, equipo de repuesto, medios de repuesto, y papel de repuesto pueden ser almacenados fuera de la sala de cómputo. El centro de datos también debe tener un área de ensayo para desempacar y posiblemente para probar nuevos equipos antes de implementarlos en la sala de cómputo. Es posible reducir drásticamente la cantidad de partículas de polvo suspendidas en el aire en el centro de datos al tener una política de desempaquetado de todo el equipo en la sala de almacenamiento. El metraje cuadrado de espacio requerido está íntimamente relacionada con la distribución del espacio, incluyendo no sólo bastidores de equipos y/o armarios, sino también de gestión de cable y otros sistemas de apoyo, tales como la energía eléctrica, climatización y extinción de incendios. Estos sistemas de apoyo tienen requisitos de espacio que dependen del nivel requerido de redundancia. Si el nuevo centro de datos reemplaza uno o más centros de datos existentes, una forma de estimar el tamaño del centro de datos es hacer un inventario de los equipos que se trasladó al nuevo centro de datos y crear un plano de planta del nuevo centro de datos con este equipo y equipamiento futuro esperado con adyacencias equipos deseados y las distancias deseadas. El diseño debe asumir que los gabinetes y bastidores están eficientemente llenos de equipos. La planta también debería tener en cuenta cualquier cambio de tecnología programados que puedan afectar el tamaño de equipamiento que se encuentra en el centro de datos nuevo. La nueva sala de informática deberá incluir equipos eléctricos y equipos de climatización de apoyo.” el DataCenter debe tener el almacenamiento de todo equipo o cableado que se vaya almacenar fuera de la sala de informática; además debe tener una zona de desempaquetado y prueba de nuevos equipos. Si el nuevo DataCenter remplaza uno o más DataCenter existentes, una forma de estimar el tamaño del DataCenter es realizando un inventario del equipamiento que va a ser movido dentro del nuevo DataCenter y crear un plano del mismo con este equipamiento y las expectativas

del futuro crecimiento. Se debe asumir que los racks o gabinetes están eficientemente llenados con el equipamiento, el plano del nuevo centro de cómputo necesitará incluir el soporte eléctrico y de ventilación para el equipamiento. En base a las recomendaciones escritas en la norma y luego del levantamiento de los requerimientos, se decide mantener en la misma zona el DataCenter; pero ampliar su espacio físico extendiéndose hasta la oficina conjunta que se encuentra separada por una pared de 1 m de alto y una ventana hasta el techo como muestra el diagrama.



Al retirar la ventana de división y derrocar la pared, se obtiene un solo espacio de 5.5m de largo por 3m de ancho; espacio suficiente para ubicar todo lo que se ha establecido como equipamiento del DataCenter. Se retira la puerta del lado izquierdo para dejar un solo acceso al área. Adicional a esto, se procede a retirar las ventanas laterales que colindan con la oficina del personal de administración de sistemas, para completar las paredes de 1m de alto con paneles rellenos de fibra de vidrio, que son utilizados con la finalidad de hermetizar el espacio y mantener la temperatura; similar al funcionamiento de un cuarto de refrigeración, además de reemplazar el techo falso por paneles de refrigeración a base de fibra de vidrio que comúnmente son utilizados en cuartos fríos industriales o frigoríficos de gran tamaño, destinados para mantener temperaturas bajas al igual que el funcionamiento de una refrigeradora, para completar el proceso de hermetización la puerta de acceso al DataCenter también es reemplazada por una puerta de panel de fibra

de vidrio. Se recomienda según la norma TIA-942, las puertas deben tener un mínimo de 1m de ancho y 2.13 de altura, sin umbrales de puertas, bisagras para abrir hacia el exterior o una abertura de lado a lado, o ser desmontables. Con la finalidad de permitir el acceso de equipos de gran tamaño.



Como se puede observar en el diagrama, el área resultante del DataCenter garantiza el espacio adecuado para la ubicación de manera ordenada y óptima de los equipos del DataCenter; además garantiza un fácil acceso del personal al espacio físico para los trabajos de administración y mantenimiento que estos equipos requieran, con una fácil movilidad para su montaje y desmontaje. El área total del nuevo DataCenter tiene 16.50 metros cuadrados. La norma TIA-942 establece que “La altura mínima de la sala de informática será de 2,6 m (8,5 pies) del piso terminado a cualquier obstáculo, como rociadores, accesorios de iluminación o cámaras. Requisitos de refrigeración o racks / gabinetes más altos que 2.13 m (7 pies) puede dictar mayores alturas de techo. Un mínimo de 460 mm (18 in) de espacio libre se mantendrá a partir de los aspersores de agua.” En cuanto al material sugerido por la norma, se debe considerar que deben minimizar la producción de polvo y mantener un color claro en la pintura de las paredes y color del piso para mejorar la iluminación del cuarto, además los pisos deben tener propiedades antiestáticas de acuerdo con la norma IEC 61000-4-2.

Debido al conjunto de equipos electrónicos que se van a instalar en este espacio físico; la cantidad de calor emanada por todos ellos en pleno funcionamiento producirá altas temperaturas sino se controla con un debido sistema de enfriamiento; lo que podría provocar fallas en el funcionamiento de los equipos y por ende fallas en los servicios. El centro de cómputo de GesCond247 aun no posee un sistema de enfriamiento de confort, debido a la carencia se tienel problema de altas temperaturas, las cuales disminuyen el poder de cómputo de nuestros servidores, siendo la primera decisión colocar un aire acondicionado adicional de las mismas características e instalarlo en el DataCenter para que funcione de manera conjunta con su similar. Al inicio esta medida resultó adecuada ya que los aires acondicionados funcionaron sin novedad por un tiempo; luego del cual, uno de ellos colapsó debido a la excesiva carga de trabajo, porque estos equipos no son diseñados para trabajar 24 horas, 365 días por año. Se observa la necesidad de implementar un sistema de enfriamiento de precisión; es decir, un aire acondicionado de tipo industrial, el mismo que es diseñado para soportar altas cargas de trabajo, garantizando una regulación de temperatura adecuada; además de regular la humedad del ambiente en el área en la que está instalada. La norma TIA-942 establece que: “HVAC se debe proveer las 24 horas por día, 365 días por año base. Si el sistema de construcción no puede asegurar la operación continua para aplicaciones de equipos de gran tamaño, una unidad independiente, se debe disponer en el DataCenter ” un sistema de acondicionamiento de aire (HVAC) debe mantener una operación continua; y además debe estar conectado al sistema de generación de energía que alimenta al DataCenter en caso de tener un generador dedicado, caso contrario debería conectarse al generador del edificio. En base a las recomendaciones se evalúa la factibilidad de instalar un sistema de aire acondicionado de precisión, observando el área del DataCenter y al ser relativamente pequeña, se recomienda la instalación de un sistema HVAC compacto; pero que posea las características adecuadas y cumpla con la regulación establecida por la norma. Para la instalación del sistema de

regularización de temperatura de precisión, se evalúa que la ubicación de los racks en el área del DataCenter debe ser de manera horizontal a lo largo del espacio físico, dejando dos pasillos, uno frente a los equipos y otro en la parte posterior, siguiendo la recomendación de que se debe establecer en el área física pasillos calientes y pasillos fríos; el pasillo caliente se encuentra en la parte posterior de los equipos, donde se desfoga todo el aire caliente que producen los mismos, el pasillo frío en la parte frontal de los racks, de donde absorberán los equipos el aire frío para mantener la adecuada temperatura interna. El equipo interno del aire acondicionado está diseñado para absorber el aire caliente por su parte inferior y emitir aire frio por la parte superior, por lo que debe estar ubicado en la parte alta de la pared en la parte posterior de los racks; es decir, en el pasillo caliente, formando así un ciclo de aire de flujo constante en todo el espacio, tomando el aire caliente de la parte inferior del pasillo caliente y emitiendo aire frio por la parte superior paralelo al techo del DataCenter, de tal manera que el flujo de aire frio llegue al pasillo en la parte frontal de los racks; es decir el pasillo frio.

De igual importancia en las adecuaciones arquitectónicas, se encuentran los parámetros relacionados con la seguridad, tanto para acceso físico como para detección de eventos que puedan atentar a la continua operación, como incendios o filtración de agua al interior del DataCenter. Para el acceso físico, se mantiene el control de acceso para el personal que se tenía previamente a las oficinas de sistemas aledañas al DataCenter, que funciona por medio de identificación con tarjetas magnéticas; de tal manera que únicamente el personal que posea la tarjeta de acceso habilitada

para el área de Redes de Servicios y Telecomunicaciones podrá ingresar también al DataCenter.

Se ha realizado un estudio de factibilidad para la instalación de un sistema de extinción de incendios, considerando la recomendación de la norma (TIA-942, 2005, pág. 109) que dice: “Un sistema de extinción de incendios de agente limpio proporciona el más alto nivel de protección para la sala de cómputo y las salas eléctricas y mecánicas. Este sistema debería ser instalado además la pre-acción de supresión y sistemas de detección de humo. El sistema de supresión de fuego está diseñado para que, tras la activación, el gas de agente limpio inunde totalmente la habitación y la zona del piso bajo. Este sistema consta de un gas no tóxico que es superior a la protección de rociadores en varios maneras. En primer lugar, el agente puede penetrar equipo de cómputo para extinguir profundos incendios en equipos electrónicos y otros relacionados. En segundo lugar, a diferencia de los rociadores no hay residuos del gas después de que el sistema se ha activado. Por último,
este agente permite que el fuego se extinguirá sin atentar contra los otros equipos que no participan en el fuego. Por lo tanto, mediante el uso de la supresión gaseosa el DataCenter fácilmente podría volver a funcionamiento después de un evento con un mínimo retraso y la pérdida se limita a los elementos afectados solamente.” Con la utilización de agentes limpios para supresión de incendios; que provee un alto nivel de protección al centro de cómputo y los mecanismos eléctricos que se encuentran asociados a este. Por cuestión de presupuesto no se ha implementado hasta el momento este sistema de supresión de incendios; pero se lo tiene presente

para un futuro cercano. El dimensionamiento del sistema de extinción de incendios se encuentra en el anexo A. Con respecto a la posibilidad de inundación o infiltración de agua al DataCenter, se ha realizado la impermeabilización completa de todo el techo del edificio principal; garantizando que no se producirán infiltraciones de agua debido a las lluvias y en vista que el DataCenter se encuentra ubicado en el segundo piso, no tiene posibilidad de ser víctima de una inundación. Se sugirió en el levantamiento de requerimientos la posibilidad de implementación de piso elevado para el DataCenter, como complemento a este proyecto se ha realizado el diseño de implementación de piso elevado para el DataCenter, lamentablemente por el limitante de altitud en la estructura del edificio no se puede implementar el piso elevado, ya que sobre el DataCenter pasa una de las vigas metálicas del edificio que impide aumentar en altura esta área.

3.1.2 Instalaciones eléctricas

Para determinar una guía de las necesidades técnicas de las instalaciones eléctricas del DataCenter, se aprovecha una herramienta en línea para calcular las dimensiones de consumo eléctrico, supresor de transientes, generador de emergencia y sistema UPS; accediendo a la página www.datacenterconsultores.com/calculadora/, se puede ingresar a estas calculadoras que por medio de una serie de preguntas emiten un resultado de la recomendación, las preguntas y resultados se muestran a continuación:

a. Diseño de una red de supresores de transientes

De acuerdo con ANSI C 62.41, la única forma de lograr una adecuada protección contra transientes de alto voltaje en las instalaciones de misión crítica, es mediante la implementación de una red escalonada de supresores de transientes, desde la acometida de servicio (Clase C), pasando por los subtableros (Clase B), hasta el punto más cercano al equipo a proteger (Clase A).

b. Calculadora de generadores de emergencia

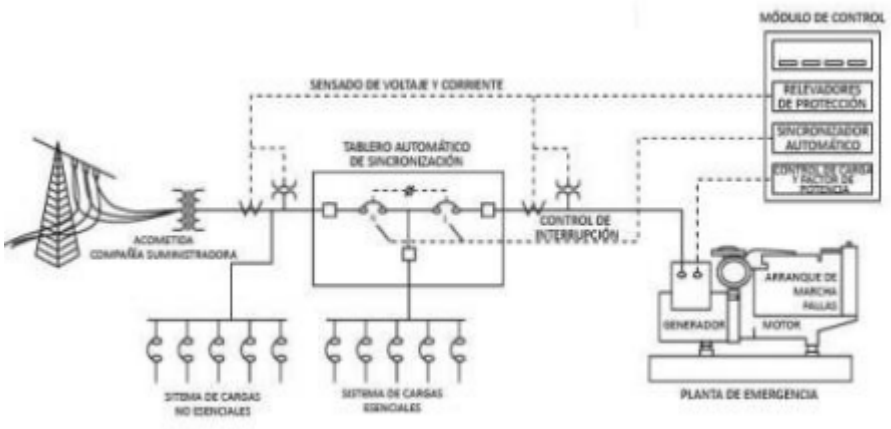
Mediante esta herramienta se puede dimensionar la capacidad mínima requerida para que la planta eléctrica de respaldo pueda soportar las cargas críticas de emergencia, como son sistemas de potencia ininterrumpida (UPS), aire acondicionado, iluminación, y otras cargas críticas a respaldar con el generador.

c. Calculadora de Sistema UPS

Mediante esta herramienta se dimensiona las necesidades de UPS a partir de la información básica disponible de los equipos y sistemas críticos del Centro de Datos.

De acuerdo a las recomendaciones obtenidas en el levantamiento de requerimientos se procede a realizar la instalación eléctrica de la siguiente manera:

Para soportar la carga operativa de todas las oficinas de GesCond247 garantizando un continuo flujo eléctrico; se traslada el UPS que se encuentra en el centro de cómputo hacia el subsuelo del edificio, de igual manera se procede con el UPS que se encontraba instalado en otra área de la empresa, realizando una conexión en serie y repartiendo la carga de todo el edificio incluido el DataCenter, utilizando los dos UPS con balanceo de carga repartido entre dos UPS de 30 KVA. Adicional a los UPS, se realiza el cambio del generador eléctrico por uno de mayor capacidad; la implementación de este generador permite que los UPS soporten la carga operativa en caso de existir un corte de flujo eléctrico convencional, por un tiempo aproximado de veinte minutos como límite máximo. En el momento en que se detecta la falta de energía eléctrica, automáticamente el sistema activa el generador, quien reemplaza la alimentación eléctrica convencional hasta su restablecimiento. El tiempo de encendido del generador es de quince segundos a partir del corte de energía; de igual manera se procede con el apagado del generador una vez que la energía eléctrica se ha restablecido, el esquema de conexión del generador es el siguiente:

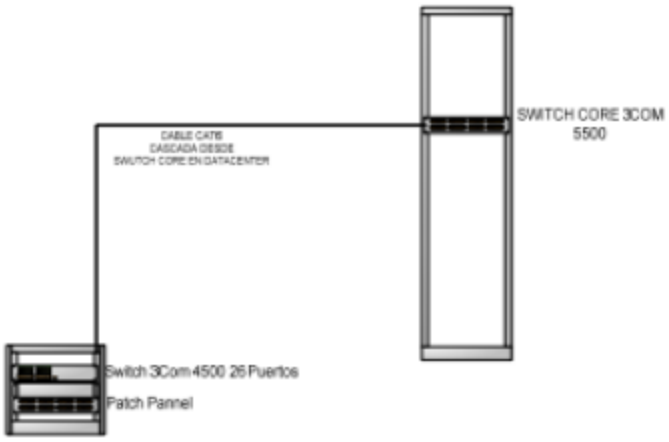


La norma TIA-942 dice: “Separe los circuitos de suministro que abastecen a la sala de computación, se asegurará y termina en su propio panel eléctrico o paneles. La sala de informática tendrá salidas dúplex de conveniencia (120V 20A) para las herramientas eléctricas, equipos de limpieza, y el equipono adecuado para enchufar en líneas de equipos de energía del rack. Los tomacorrientes no deben estar en las mismas unidades de distribución de energía (PDU) o paneles eléctricos como los circuitos eléctricos utilizados en los sectores de telecomunicaciones y equipos de cómputo en la habitación. Los tomacorrientes deben estar espaciados 3,65 m (12 pies) de distancia a lo largo de las paredes de la sala de cómputos, o más cerca si se especifican las ordenanzas locales, y se puede llegar por un 4.5m (15 pies) de cable”. En el DataCenter se procede hacer dos circuitos de acometida de energía eléctrica a 220 voltios para alimentación eléctrica a los equipos servidores, con la finalidad de garantizar el balanceo de carga de alimentación a 220 v. También se realiza una acometida adicional a 110v, manejando el mismo principio de continuidad para alimentar a los equipos que trabajan a este voltaje. La norma TIA-942 indica: “La infraestructura de conexión a tierra de la sala de cómputo crea una referencia de tierra equipotencial para sala de cómputo y reduce perdidas de señales de alta frecuencia. La infraestructura de conexión a tierra del DataCenter consiste en una cuadrícula de conductores de cobre centrales de 0,6 a 3 m (2 a 10 pies) que cubre el espacio en el cuarto entero. El conductor no debe ser menor qué # 6 AWG o equivalente. Una red puede utilizar

cualquiera de los conductores de cobre desnudo o aislado. La solución preferida es el uso de cobre aislado, que es despojado donde las conexiones deben realizarse. El aislamiento evita los puntos de contacto intermitente o no. El color estándar de la industria del aislamiento es verde o marcados con un color verde característico que en ANSI-J-STD-607-A ... Cada armario rack de equipos y gabinetes de equipos requieren su propia conexión a tierra a la infraestructura del DataCenter a tierra. Un mínimo de un conductor de cobre AWG # 6 se debe utilizar para este propósito". Se recomienda para las instalaciones eléctricas también realizar el correspondiente aterrizaje o puesta a tierra, tanto para la infraestructura eléctrica para reducir las señales de alta frecuencia, así como también se recomienda el aterrizaje de los racks instalados dentro del data center. Todas las tomas eléctricas del edificio poseen conexión a tierra, por el mismo sistema de tendido eléctrico que se encuentra instalado en el edificio.

3.1.3 Cableado estructurado de Oficinas

El departamento de contabilidad fue ubicado en la zona que antes era el auditorio de GesCond, se procede a implementar el cableado estructurado con 23 puntos de red. La tecnología utilizada para el cableado estructurado es Categoría 6 para toda el área, se coloca un rack de pared en este departamento, en donde se conectan los puntos de este sector, este rack se interconecta directamente con el Data Center (Cascada).



De igual manera, el Departamento de Sistemas se reubica en el área que anteriormente era destinada para capacitación, ahí se implementan quince puntos de red en cableado de categoría 6.
En esta área se tenía instalado previamente un rack de pared donde llegaba el cableado estructurado, se aprovecha este rack para aterrizar todos los puntos resultantes en la adecuación de esta zona. Este rack tiene conexión directa con el Data Center.

3.2 Adquisición de equipos de redes y comunicaciones

Luego del diseño e implementación del cableado estructurado, todas las modificaciones arquitectónicas y principalmente la implementación del nuevo Data Center; es necesario la adquisición e instalación de dispositivos activos de networking, para soportar la infraestructura que GesCond247 manejará en lo posterior, así como también la adquisición y puesta en marcha de servidores de mejores características para la implementación de nuevos servicios.

3.2.1 Características de equipos de Redes

Para la implementación de la red interna se define que debe tener una arquitectura que soporte la red LAN de GesCond247, la red de una farmacia cercana que tiene conexión directa con el edificio y manejar una red para telefonía IP; para poder manejar de una forma adecuada y sin mayor impacto para los usuarios finales se decide manejar dentro de la red LAN tres VLANs o LANs virtuales de la siguiente manera:

* VLAN 1: Red LAN de GesCond (192.168.240.0/24)
* VLAN 2: Red LAN Farmacia “x” (192.168.110.0/24)
* VLAN 3: Red de telefonía IP (192.168.120.252/24)

Se opta por una solución integral con switches 3com, un modelo 5500 de tipo administrable, switch de capa 3 que soporte configuración de VLANs y Ruteo, adicional varios switches 3Com 4500 que se instalarán en puntos estratégicos según el diseño del cableado estructurado, para enlazar todas las dependencias del edificio.

SWITCH 3COM 5500G

Switching Gigabit Ethernet apilable de primera clase El 3Com Switch 5500G-EI 24-Port es un switch 10/100/1000 apilable, con software de imágenes mejoradas (EI) para empresas con las aplicaciones de red más exigentes que requieren la más alta disponibilidad de la red (99,999%). 24 puertos funcionan a 10/100/1000; 4 de estos puertos son de uso dual con cuatro puertos Gigabit basados en SFP. La ranura para módulo de expansión ofrece conectividad adicional Gigabit o 10-Gigabit Ethernet. Dimensiones: Altura: 43,6 mm; anchura: 440 mm, fondo: 450 mm

SWITCH 3COM 4500G

Switch apilable de clase empresarial para aplicaciones de extremo; responde a las necesidades más exigentes de redes convergentes seguras. El switch 10/100 Ethernet apilable 3Com® Switch 4500ofrece switching de Capa 2 y routing dinámico de Capa 3 con variedad de características. Con seguridad robusta, y amplias funcionalidades de administración, priorización de tráfico, y calidad de servicio, el Switch 4500 es capaz de manejar aplicaciones empresariales emergentes. Dimensiones: Altura: 43,6 mm (1U); anchura: 440 mm; fondo: 270 mm Peso: 3,3 kg

3.2.2 Características de Servidores

Con la finalidad de mejorar y robustecer el equipamiento del DataCenter referente a servidores, se evaluó la posibilidad de adquirir una solución de servidores Blade para algunos de los servicios que es necesario implementar y los nuevos sistemas que se pondrán en producción ya con el funcionamiento en pleno de GesCond247.

Servidores Blade

Un servidor Blade o de cuchilla es un tipo de computador robusto, diseñado para alto rendimiento y como principal característica aprovechamiento de espacio, reducción del consumo y simplificación en administración. Esta clase de servidor es una tarjeta que contiene

el microprocesador, memoria, buses de datos y según el modelo también discos duros, no poseen fuente de alimentación ni tarjetas de comunicaciones, estos elementos que más espacio ocupan se colocan en un chasis que se monta en el rack del DataCenter, cada chasis puede albergar según su modelo hasta 16servidores blade, que comparten: fuente de poder redundante y hotplug, ventiladores, tarjetas de conmutación de red, interfaces de almacenamiento, en caso de necesitarse alto nivel de almacenamiento se procede a interconectar con una red SAN (Storage Área Network). Como ventajas principales de un sistema de servidores Blade se destacan:

a) Ocupan menos espacio debido a que son sumamente delgados.
b) Facilidad de instalación, basta montarlo en el chasis ya que el cableado de instalación solo se realiza una vez para todo el Case.
c) Facilidad de administración, permiten una administración centralizada y remota.d) Al no contener elementos mecánicos, tienen menos posibilidad de fallo de hardware.

En el caso de GesCond247 se optó por un sistema de servidores Blade en un Enclosure, este sistema de Blade tiene dos presentaciones tipo torre o tipo Rack, soporta hasta un máximo de 8 servidores.

3.3 Interconexión de redes LAN

Un paso fundamental en el proceso de instalación de este proyecto es establecer una línea de comunicación entre los edificios de oficinas y bodega, estos edificios se encuentran separados a una distancia aproximada de 200 metros, para decidir qué medio se usaría para esto se tiene varias opciones, Cableado UTP, radio enlace y fibra óptica; según la norma de cableado estructurado, la distancia máxima de una instalación con cable UTP es de 90 metros, no es viable utilizarlo a menos que se use un repetidor intermedio, por lo que se descarta esta alternativa, la opción de radio enlace también se descarta porque no existe una línea de vista adecuada, la fibra óptica ofrece la capacidad de mantener la calidad de la señal por mucha mayor distancia y puede ser

instalada de extremo a extremo sin mayores inconvenientes, se decide realizar un tendido de edificio a edificio con este medio.

3.3.1 Tendido de Fibra Óptica

La fibra óptica es un medio de transmisión empleado ampliamente en redes de datos; su estructura es un hilo material transparente, una fibra de vidrio o materiales plásticos ultra delgada protegida por un material aislante por el que se envían pulsos de luz que representan los datos a transmitir de un punto a otro. Además de los cables, debemos tener en cuenta que un sistema de transmisión óptica consta de varios componentes esenciales: la fuente de luz, el medio de transmisión, el detector. El medio de transmisión es la propia fibra de vidrio, la fuente de luz suele ser un láser, y el receptor un elemento fotosensible. La información se codifica de modo que un pulso de luz indique un valor 1 (uno binario) y la ausencia del mismo un 0 (cero binario). El haz de luz se proyecta en el inicio del cable y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, la fuente de luz puede ser láser o un diodo emisor de luz LED. La fibra óptica permite enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio o cable de cobre. Debido a sus materiales la transmisión de datos por este medio es inmune a las interferencias electromagnéticas. La fibra óptica también se utiliza para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión; claro que para distancias cortas es necesario tomaren cuenta el costo beneficio, ya que en instalaciones de red LAN es mucho más económico realizar la instalación con Cableado UTP. Cada filamento de fibra óptica está diseñado de la siguiente manera: consta de un núcleo central de plástico o cristal (óxido de silicio y germanio) con un alto índice de refracción, rodeado de una capa de un material similar con un índice de refracción ligeramente menor. Cuando la luz llega a una superficie que limita con un índice de refracción menor, se refleja en gran parte, cuanto mayor sea la diferencia de índices y mayor el ángulo de incidencia, se habla entonces de reflexión interna total. La parte central de la fibra óptica es el núcleo, su tamaño depende del tipo de

fibra, los estándares son 8.3 µm (monomodo), 50 µm (multimodo) y 62.5 µm (multimodo). El revestimiento tiene un diámetro de 125 µm. como analogía, un cabello humano tiene unos 70 µm de diámetro; los cables están recubiertos por una cubierta protectora, semirrígida, que protege al núcleo y al revestimiento de posibles daños. Tanto el núcleo como el revestimiento están formados por distintos materiales, normalmente cristal de silicio (SiO_2) de distintas composiciones para provocar el fenómeno TIR. En el interior de una fibra óptica, la luz se va reflejando contra las paredes en ángulos muy abiertos, de tal forma que prácticamente avanza por su centro. De este modo, se pueden guiar las señales luminosas sin pérdidas por largas distancias. Una vez que la luz entra en una fibra óptica, se propaga de una forma uniforme llamada modo, es el camino que sigue a través de una fibra (la onda electromagnética), debido a esto y a la cantidad de modos se definen dos tipos de fibra: Monomodo y Multimodo. Una fibra multimodo es aquella en la que los rayos de luz pueden circular por más de un modo o camino. Una fibra multimodo puede tener más de mil modos de propagación de luz. Las fibras multimodo se usan comúnmente en aplicaciones de corta distancia, menores a 1 km; es simple de diseñar y económico. El núcleo de una fibra multimodo tiene un índice de refracción superior, pero del mismo orden de magnitud, que el revestimiento. Debido al gran tamaño del núcleo de una fibra multimodo, es más fácil de conectar y tiene una mayor tolerancia a componentes de menor precisión. Una fibra monomodo es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación. Su transmisión es paralela al eje de la fibra. Las fibras monomodo permiten alcanzar grandes distancias (hasta 400 km máximo, mediante un láser de alta intensidad) y transmitir elevadas tasas de información (decenas de Gb/s). Existen 3 tipos básicos de fibra monomodo: NDSF, DSF yNZ-DSF. Las diferencias entre los 3 tipos se basan principalmente en su adecuación para el funcionamiento con diferente láser que funcione en distintas longitudes de onda. Los conectores son interconexiones fibra a fibra

que alinean el núcleo de ambas fibras y la principal diferencia entre ellos es el tipo de enganchemecánico y su tamaño. Los cables finalizan en diferentes terminaciones que permiten conectarlos a los paneles y bandejas de fibras existentes en el rack de comunicaciones.

3.4 Instalación y Configuración de Equipos de comunicaciones

La instalación de equipos de comunicaciones comprende la de instalación y configuración de switches, cuyas características ya fueron descritas anteriormente, con la instalación en todos los lugares donde se definió deben estar ubicados los dispositivos y su configuración interna.

3.4.1 Switches

Según el diagrama de ubicación de los switches se procede a instalar en el DataCenter el switch 3Com 5500 y dos switches 3Com 4500 de 50 puertos. Para la instalación del switch 3com 5500 y demás dispositivos de comunicaciones como routers y equipos terminales de enlaces se elige un rack de gabinete o armario con bandejas metálicas donde serán ubicados todos estos dispositivos.Para la instalación de los dos switch 3com 4500 de 50 puertos se elige colocarlos en la parte inferior del rack donde se ubican los patch panel de toda la red del primer y segundo piso del edificio. Cada uno de estos switch posee un par de aditamentos metálicos para su instalación en el rack.

Estos aditamentos se atornillan en los costados frontales del switch aprovechando los orificios más pequeños, los orificios más grandes son para colocar los tornillos que sujetan al equipo en el rack.

Una vez realizada la instalación en el rack, se procede a realizar la configuración de cada switch, para configurar el switch se debe conectar por el puerto de consola del dispositivo con el cable de consola hacia el computador.

El extremo RJ45 se conecta al puerto de consola del dispositivo, el extremo con puerto serial RS232 se debe conectar al puerto serial del computador, si no se tiene puerto serial se debe colocar un adaptador USB.

Una vez conectado el dispositivo al computador, se procede a acceder a la información del equipo por medio de HyperTerminal.

3.5 Migración de Equipos

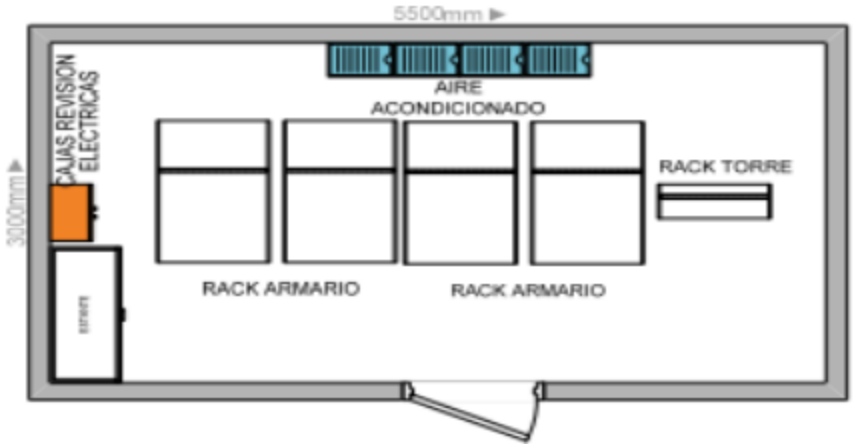
Luego de la adecuación de infraestructura e instalaciones eléctricas, a continuación se describe como se instalan todos los componentes del DataCenter de acuerdo a los requerimientos establecidos anteriormente.

3.5.1 Equipos activos y pasivos

Se consideran equipos activos a todos aquellos dispositivos que generan y/o modifican las señales que se transmiten en la red, es decir switches, routers, etc.; mientras que los elementos pasivos únicamente se encargan de transmitir las señales dentro de la red, como por ejemplo cables, conectores, patch pannels. Para la instalación de estos elementos dentro del DataCenter, es necesario que primero se realice la instalación de los soportes donde irán ubicados todos estos elementos, incluidos también los servidores; dichos soportes son tres racks abiertos tipo torre y dos racks tipo armario, que de acuerdo al área del DataCenter de 5m de largo por 3m de ancho aproximadamente, se decide seguir la recomendación de establecer pasillos calientes y pasillos fríos por lo que se procede a colocar los racks en hilera transversal a lo largo del área como muestra a continuación el diagrama.

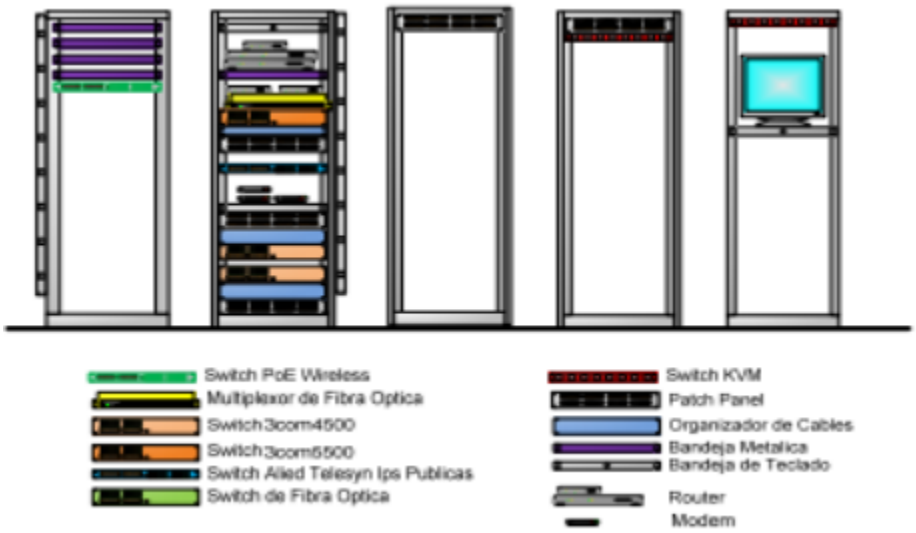
Vista Aérea: En este diagrama se puede observar la distribuciónde los racks en toda el área del DataCenter, se reemplaza dos racks de torreen el costado izquierdo por racks tipo gabinete, mismos que están destinados a albergar todos los dispositivos de la red como son switches, organizadores de cables, patch panel, routers, módems. Además de los equipos que componen la central telefónica; a estos racks se les denominará en adelante Racks de Comunicaciones. Los dos racks de bastidor o armario siguientes se encargan de albergar todos los equipos servidores y tendrán un patch panel para

interconectarse con el rack de comunicaciones. Nótese que el aire acondicionado se encuentra en la parte posterior de los racks, esto con la finalidad de absorber todo el aire caliente que generan los equipos y generar aire frío que es enviado por la parte superior sobre los rack generando un ciclo circular, lo que determina que el pasillo caliente está ubicado en la parte posterior de los racks y el pasillo frío se encuentra en la parte frontal de donde los equipos obtienen el aire frío.



Vista Frontal: en este diagrama se muestra la ubicación de los racks y como están distribuidos en cada uno de ellos los elementos activos y pasivos de la red, en el rack 1 se encuentran los equipos que componen la central telefónica marca Siemens instalada como servicio contratado con la empresa Level3. En el segundo Rack o rack de telecomunicaciones se colocan en la parte inferior los patch panel del cableado estructurado del edificio, cuyos puntos de red llegan directamente al DataCenter, mediante patch cords se conectan a 2 switches 3Com 4500 de 50 puertos, mismos que tienen conexión en cascada con el switch core 3Com 5500; también se colocan en este rack los equipos activos correspondientes a enlacesde datos con sucursales y empresas prestadoras de servicios. En el rack 3 se encuentraun patch panel que interconecta los servidores de dicho rack con el Switch Core. En el Rack 4 se coloca el patch panel que conectan todos los servidores de los rack 4 y 5, además de un switch

KVM que es la interface de interacción con los equipos del rack 3 y 4 para administración. En el rack 5 se encuentra otro switch KVM para la administraciónde los equipos restantes del rack 4 y los equipos del rack 5.



3.5.2 Servidores

La ubicación de servidores se realiza en los racks 3, 4 y 5, en vista de la unificación de servicios y la implementación de nuevos programas y servicios para uso interno de GesCond247, se han retirado algunos equipos por ser muy antiguos y se han reemplazado por nuevos equipos, así como también se reutilizó y asignó nuevas funciones a los servidores existentes, a continuación se muestra la ubicación final de los servidores en el DataCenter y un listado de los mismos junto con sus características.

3.6 Documentación de Red

Es necesario detallar el estado final en que queda la red luego de todas las adecuaciones en el transcurso del proyecto, a continuación se detallan separadas en dos partes, red LAN correspondiente a todo el área destinada a oficinas y red WAN abarcando oficinas remotas.

3.6.1 Red LAN

La red interna se encuentra diseñada para manejar tres redes de área local virtuales (VLAN) sobre su infraestructura física de red.

a) La VLAN No 1 soporta todo el tráfico de la red de datos en su edificio matriz, la dirección IP definida para este segmento de red de clase C es 192.168.238.0/24, lo que indica un tamaño máximo de 254 dispositivos que pueden estar conectados en esta red. Para aumentar el número de equipos soportados por la red se decide migrar a una red de clase B 172.30.0.0/16, lo que nos da un alto número de dispositivos que pueden ser conectados. Considerando la criticidad de las configuraciones de los equipos servidores y también que los enlaces de datos tanto de sucursales como de proveedores, se encuentran diseñados de tal manera que trabajen con la red clase C, se decide mantener esta red únicamente para todo el equipamiento técnico del área de sistemas; es decir servidores, equipos de red como switches, routers, Access point, servidores de impresión y servidores de monitoreo de seguridad.

b) La VLAN No. 2 soporta todo el servicio de telefonía IP tanto el edificio matriz como en sucursales, a esta red se le asigna la dirección IP clase C 192.168.110.0/24.

c) La VLAN No. 3 se encuentra asignada para soportar el tráfico de datos con toda el área correspondiente a farmacias. Se mantiene la dirección de red clase C 192.168.101.0/24. Diagramas de ubicación de puntos de red del cableado estructurado de algunas zonas.

3.6.2 Red WAN

La red WAN es una estrella de enlaces que tiene como punto central a las oficinas de GesCond247, se han colocado enlaces dedicados de datos a todas las farmacias de la empresa con un ancho de banda de

512 Kbps y 256 Kbps utilizando como medio de transmisión ADSL, por fibra óptica y radio enlace. En oficina matriz se encuentran Routers que se comportan como concentradores de los enlaces provistos por cada una de las empresas de telecomunicaciones, aquí se ha definido al router concentrador como router principal, ya que a este llegan el mayor número de enlaces de datos, quien interconectado a los demás Routers determina toda la estructura del núcleo de la topología estrella de la red WAN.

4.- IMPLEMENTACIÓN DEL PROYECTO (Servicios)

4.1 Implementación de Active Directory

La implementación de Active Directory permitirá convertir el servidor seleccionado en un controlador de dominio, provee servicios para organizar, administrar y controlar los recursos disponibles en la red y a su vez obtener la capacidad de administrar de manera centralizada toda la red basada en sistemas operativos Windows.

4.1.1 Configuración

Para la instalación del servicio se debe realizar los siguientes pasos:

a. Hacer click en Inicio, hacer click en Ejecutar, y escribir dcpromo luego dar Enter, esto llamará al asistente para la configuración de active Directory.

El asistente verifica:

1. Si el usuario actualmente validado es un miembro del grupo de administradores locales.
2. Si en la computadora está funcionando un sistema operativo que soporte Active Directory.
3. Que una instalación o un retiro anterior de Active Directory no ha ocurrido sin reiniciar el servidor, o que una instalación o un retiro anterior de Active Directory no está en marcha.

b. En la página de bienvenida, hacer click en Siguiente.

c. En la página de Compatibilidad de Sistema Operativo, hacer click en Siguiente.

d. En la página Tipo de Controlador de Dominio, hacer click en Controlador de Dominio para un Dominio Nuevo, y después click en Siguiente.

e. En la página Crear Nuevo Dominio, hacer click en Dominio en un nuevo Bosque, después hacer click en Siguiente.

f. En la página Nuevo Nombre de Dominio, ingrese el Nombre DNS para el nuevo dominio (gescond247.com), y después haga clic en Siguiente.

g. En la página Nombre de Dominio NetBIOS, escribir el nombre NetBIOS (GesCond247) y después haga clic en Siguiente. El nombre NetBIOS identifica el dominio a las computadoras de cliente corriendo versiones anteriores de Windows y Windows NT. El asistente verifica que le nombre NetBIOS sea único; si no lo es, le pide cambiar el nombre.

h. En la página Carpetas de la Base de Datos y Registro, especificar la localización en la cual desea instalar las carpetas de la base de datos y de los logs, se recomienda dejar la información por defecto, y después haga clic en Siguiente.

i. En la página Volumen del Sistema Compartido, especifique la locación en la cual desea instalar la carpeta de SYSVOL, se recomienda mantener la información por defecto, o haga clic en Examinar para elegir una locación diferente, y después haga clic en Siguiente.

j. En la página Diagnóstico de registro de DNS, se verifica si un servidor existente de DNS es autoritario para este bosque; en este caso, haga clic en Instalar y configurar este equipo de manera que utilice este servidor DNS como el preferido, con lo que se configurará automáticamente el servicio DNS asociado a Active Directory para resolución de nombres dentro del nuevo dominio y después haga clic en Siguiente.

k. En la página Permisos, especificar si asigna los permisos por defecto en los objetos usuario y grupo compatible con los servidores que funcionan con versiones anteriores de Windows o Windows NT, o solamente con los servidores Windows Server 2003.

l. En esta página especifique el password para el administrador para el modo de restauración de servicios de Directorio. Los controladores de dominio Windows Server 2003 mantienen una versión pequeña de la base de datos de cuentas de Microsoft

Windows NT 4.0; la única cuenta en esta base de datos es la cuenta del administrador y esta cuenta se requiere para la autentificación al encender el servidor en Directory Services Restore mode, porque Active Directory no se inicia en este modo.

m. Con toda la información recabada por parte del asistente, al final aparece la pantalla de Resumen, se recomienda revisar la información en caso de haber ocurrido un error corregirlo oportunamente.

n. Una vez finalizada la instalación aparece el cuadro de diálogo que solicita reiniciar el servidor.

4.1.2 Configuración de un Controlador de Dominio Adicional

El procedimiento de configuración de controladores de dominio adicionales para el dominio de GesCond247 es similar al procedimiento antes descrito, únicamente en la pantalla del asistente de configuración en lugar de elegir un controlador para un dominio nuevo, se debe elegir “Agregar un Controlador de Dominio Adicional para un Dominio Existente” y seguir con el proceso.

Se configuran dos servidores como controladores de dominios secundarios o adicionales ubicados de la siguiente manera:

1. Controlador de Dominio Principal ubicado en GesCond247 Matriz
2. Controlador secundario en GesCond247 Matriz

4.1.3 Unidades organizativas

Las unidades organizativas son los objetos dentro de Active Directory que se catalogan como contenedores; dentro de las mismas se pueden colocar usuarios, equipos y otras unidades organizativas; con la finalidad de mantener un orden y organización de todos los elementos que conforman el dominio.

Para la elaboración de un esquema de unidades organizativas, se recomienda realizar una evaluación y determinar la manera de organización; esto puede ser catalogar usuarios y equipos, o dividir la organización en oficinas y sucursales o departamentos, todo depende de la forma de organización que defina el administrador para mantener una estructura ordenada.

La creación de unidades organizativas se realiza ingresando en el servidor configurado como Domain Controller, puede ser el

principal o cualquier servidor adicional, la información creada en cualquier servidor que competa a lo que es Unidades Organizativas, y elementos que van dentro de la Unidad Organizativa, como usuarios o equipos.

4.2 Implementación de Directivas de Grupo (GPO)

4.2.1 Instalación de consola de administración de Directivas Grupo

Mediante la creación de una Directiva de Grupo, se puede definir el estado y comportamiento del ambiente de trabajo que van a tener los usuarios al iniciar sesión dentro del dominio, los equipos solicitan al DomainController remita las directivas de grupo para aplicarlas de acuerdo al usuario que está ingresando en dicho computador.

Existen dos configuraciones de GPO, para usuarios y para computadores:

a. Las configuraciones de GPO para usuarios incluyen configuraciones específicas del sistema operativo, escritorio, configuraciones de seguridad, opciones de ejecución de aplicaciones y scripts para logon y logoff. Son aplicados cuando los usuarios inician sesión en el computador y durante un ciclo de actualización periódico.

b. Las configuraciones de GPO para las computadoras incluyen cómo se comporta el sistema operativo, comportamiento de escritorio, configuraciones de seguridad, scripts de startup y shutdown, opciones de aplicaciones, estas GPO se aplican cuando el sistema operativo inicializa y durante un ciclo periódico de actualización.

Para crear directivas de grupo se debe utilizar la Consola de Administración de Directivas de grupo que es una herramienta de manejo de GPO, permite:

a. Administrar las directivas de grupo para múltiples forest, dominios y unidades organizacionales.

b. Exhibe los links, herencia y delegación de GPO.

c. Muestra los contenedores a los cuales se aplican las GPO.

d. Proporciona reportes HTML de las configuraciones.

Esta consola no viene por defecto en la instalación del sistema Operativo Windows, se debe instalar un paquete que puede ser descargado de la página de Microsoft. El proceso de instalación es mediante un asistente que no requiere configuración adicional, únicamente su ejecución y seguir las opciones.

Una vez terminada la instalación se puede ingresar a esta consola haciendo clic en inicio / herramientas administrativas / administración de políticas de grupo.

El forest correspondiente al dominio que se encuentra creado en el servidor debe cargarse automáticamente.

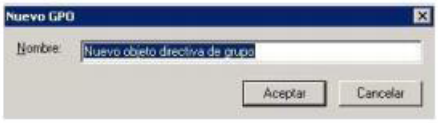
Dentro del forest, se despliegan los dominios en caso de tener varios dominios configurados dentro de un mismo forest. Para el caso de GesCond247 se mostrará un único dominio (gescond247.com), en el panel de navegación ubicado en el costado izquierdo de la consola, se muestra un esquema de árbol basado en el esquema de unidades organizacionales creado en la administración de Active Directory, y dentro de las OU a diferencia de la administración de Active Directory que muestra los equipos o usuarios, esta consola muestra las GPO que se encuentran enlazadas a dicha OU.

4.2.2 Creación de Directivas de Grupo

Para la creación de una nueva directiva de grupo se debe crearla únicamente dentro del contenedor de Objetos de Directivas de Grupo, lo que permite la creación de una GPO sin enlazar a ninguna unidad organizativa, haciendo clic derecho sobre el contenedor de objetos de GPO y seleccionando la opción “Nuevo”.

También se puede crear una nueva GPO que desde su creación ya se encuentre enlazada a un contenedor o una unidad organizativa, haciendo clic derecho sobre la OU que se desee enlazar y seleccionando la opción Crear y Vincular un GPO aquí.

En ambos casos aparece una ventana que solicita el nombre de la nueva GPO, para la creación del nombre de la nueva GPO se recomienda manejar un esquema ordenado y un nombre descriptivo que indique la funcionalidad que se configura en dicha GPO, por ejemplo:



Luego de colocado el nombre, se crea dentro del contenedor la nueva GPO, la configuración de la GPO está vacía y es necesario modificarla para controlar o configurar el comportamiento que deben tener los objetos dentro de la unidad organizativa a la que está vinculada dicha GPO.

Para configurar las características de comportamiento de una GPO se debe hacer clic en el ícono que identifica la GPO a modificar y seleccionar Editar.

Se recomienda crear cada GPO con orientación específica, no aplicar una configuración multipropósito, debido a que puede ocurrir que cierta OU se desee restringir una funcionalidad específica y la GPO que la contiene tiene además de esta configuración otra adicional que no tiene aplicación para el propósito de dicha OU.

4.3 Implementación de DHCP

El servicio DHCP se configura para la asignación dinámica de direcciones de red, DHCP (Protocolo de Configuración Dinámica de Host) es un protocolo de red que permite a los clientes de una red obtener su configuración de servidor de forma dinámica. Se trata de un protocolo de tipo cliente/servidor que posee una lista de direcciones IP dinámicas denominado ámbito y las va asignando a los clientes conforme se van conectando asignándoles una dirección del grupo que se encuentra libre, además se pueden definir direcciones reservadas para equipos específicos que por su configuración de acceso o aplicaciones instaladas necesitan siempre recibir del servidor DHCP la misma dirección IP.

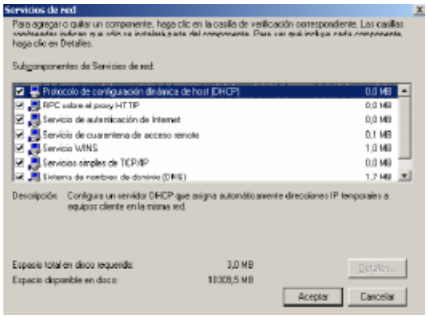
El servicio DHCP debe ser configurado agregándolo dentro de los servicios activos de Windows, para esto se debe realizar lo siguiente:

a. Ingrese por medio de “Panel de Control” a “Agregar o quitar programas”

b. Selecciona la opción “Agregar o quitar componentes de Windows”

c. En la ventana de asistente se debe seleccionar Servicios de Red y luego hacer click en detalles

d. En esta ventana se debe seleccionar Protocolo de configuración dinámica de host (DHCP) con un visto y se da click en Aceptar.



e. Al volver a la ventana anterior se hace click en siguiente hasta que se concluya la instalación y habilitación del servicio.

Una vez que se tiene el servicio activado se debe proceder con la configuración, se debe ingresar a la consola de administración del servicio, haciendo clic en Inicio, Herramientas Administrativas, DHCP.

La configuración del nuevo Ámbito se realiza como se muestra a continuación:

a. Click derecho sobre el nombre del servidor.

b. Seleccionar la opción Ámbito nuevo

c. Aparece la ventana del asistente de configuración, en la primera pantalla que indica una reseña de la funcionalidad del servicio que se configura, hacer click en siguiente.

d. En esa pantalla se debe indicar el nombre del Ámbito y una descripción.

e. En la siguiente pantalla se debe definir el rango de direcciones IP que va a tener el Ámbito.

f. Se pueden agregar exclusiones para direcciones específicas que no estarán disponibles para la asignación dinámica a pesar que se encuentren contempladas dentro del rango definido anteriormente, en esta configuración no se han definido direcciones de exclusión.

g. También se debe configurar la duración mínima de la concesión de la dirección IP que puede ser definida en días, horas y minutos.

Con la configuración ya definida se tiene el servicio activado y los host dentro de la red empezarán a recibir las direcciones dinámicas.

Para la configuración de reservas de direcciones se debe realizar lo siguiente:

a. En la misma consola de administración hacer click derecho en la subcarpeta Reservas y seleccionar la opción Nueva Reserva.

b. En esa ventana que aparecerá se deberán ingresar los siguientes datos para realizar una reserva de dirección IP:

1. Nombre de Reserva: se asignará para distinguir la reserva, este nombre cuando la reserva se efectiviza cambia por el nombre NetBIOS del dispositivo al cual pertenece la reserva.
2. Dirección IP: es la dirección que le será asignada por el servidor DHCP cada vez que el host se conecte a la red.
3. Dirección MAC: es la dirección que valida el servidor DHCP para asignar la dirección IP al host que lo solicita si la dirección MAC coincide con alguna de las reservas el servidor asigna la dirección IP correspondiente.
4. Descripción: campo adicional para indicar un comentario o referencia a la reserva.

c. Se deja por defecto las opciones de Tipos Compatibles y se da clic en Agregar, con esto se irán agregando a la lista de direcciones reservadas en la carpeta Reservas.

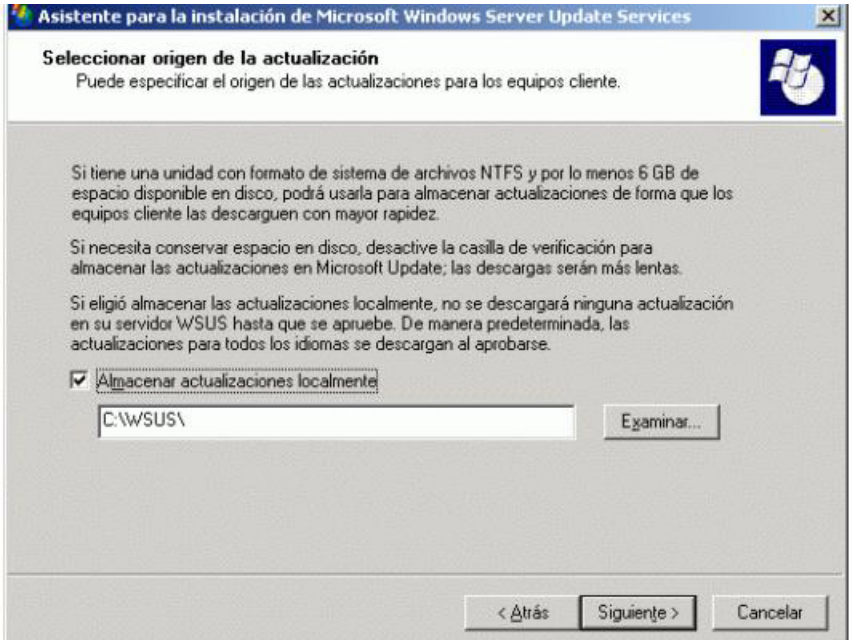
4.4 Implementación de Servicio de Actualizaciones Automáticas WSUS

Microsoft Windows Server Update Services proporciona una solución completa para administrar actualizaciones en la red. Permite centralizar la descarga de actualizaciones de sistema operativo y aplicaciones Microsoft y distribuirlas en todos los equipos cliente mostrando una consola de administración para controlar el estado de los equipos en cuanto a actualizaciones se refiere y también las actualizaciones descargadas que pueden ser aprobadas o negadas para su instalación.

4.4.1 Instalación de WSUS

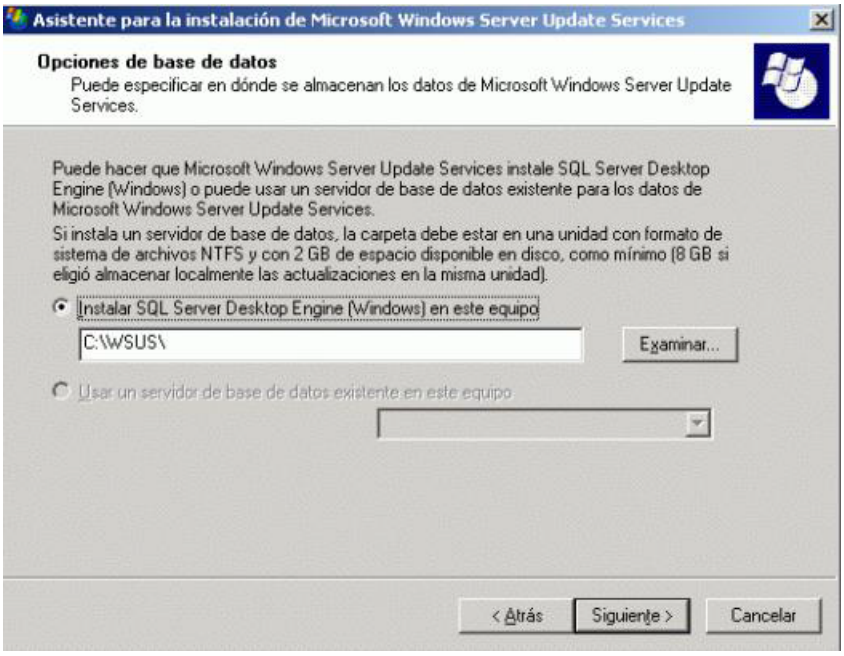
1. Hacer doble click en el instalador WSUSSetup.exe.
2. En la página de bienvenida del Asistente, hacer click en Siguiente.
3. Lea los términos del contrato de licencia detenidamente, haga click en Acepto los términos del Contrato de licencia y, a continuación, haga click en Siguiente.
4. En la página Seleccionar origen de la actualización, puede especificar el lugar de donde los clientes obtendrán las

actualizaciones. Si activa la casilla de verificación Almacenar actualizaciones localmente, las actualizaciones se almacenaran en el servidor WSUS, y deberá seleccionar la ubicación del sistema de archivos en la que se guardarán. Si las actualizaciones no se almacenan localmente, los equipos cliente se conectarán a Microsoft Update para obtener las actualizaciones autorizadas.



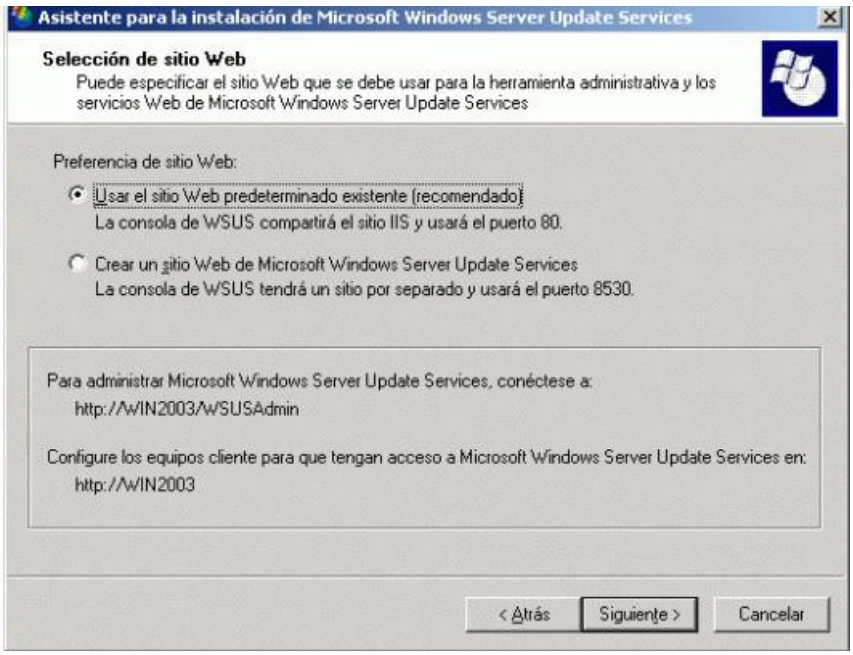
5. En la página Opciones de base de datos, seleccione el software que se utilizará para administrar la base de datos de WSUS. De manera predeterminada, el programa de instalación de WSUS propone instalar WMSDE si el equipo donde va a realizar la instalación ejecuta Windows Server 2003.

Si no se puede utilizar WMSDE, debe especificar la instancia de SQL Server que utilizará WSUS; para ello, haga click en Usar un servidor de base de datos existente en este equipo y escriba el nombre de la instancia en el cuadro Seleccionar instancia SQL. Mantenga las opciones predeterminadas y haga click en Siguiente.



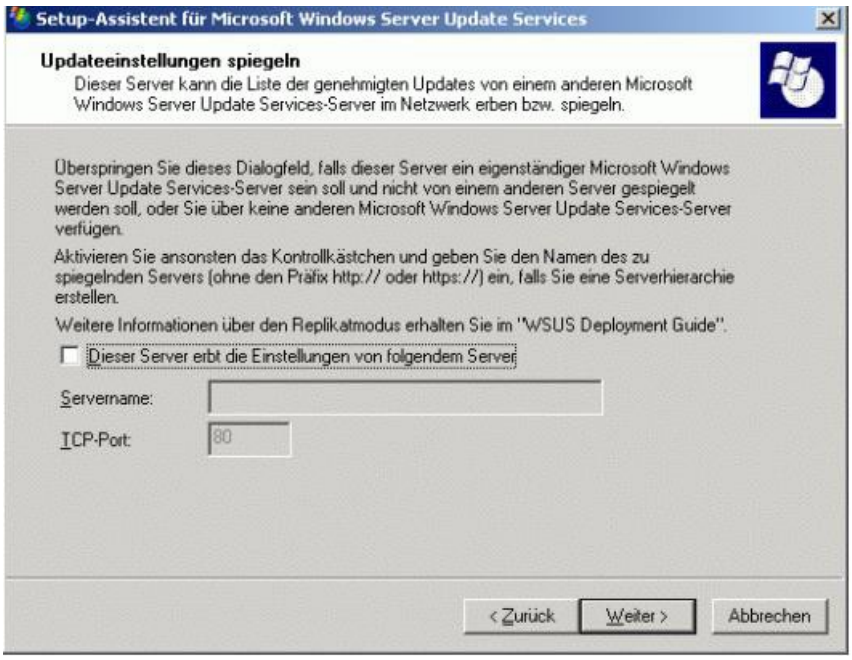
6. En la página Selección de sitio Web, especifique el sitio Web que utilizará WSUS. En esta página también aparecen dos direcciones URL importantes que dependen de lo que seleccione: la dirección URL a la que deben obtener acceso los equipos cliente WSUS para obtener actualizaciones y la dirección URL de la consola de WSUS donde se configurará WSUS.

Si ya tiene un sitio Web en el puerto 80, puede que necesite crear el sitio Web de WSUS en un puerto personalizado. Mantenga la opción predeterminada y haga click en Siguiente.



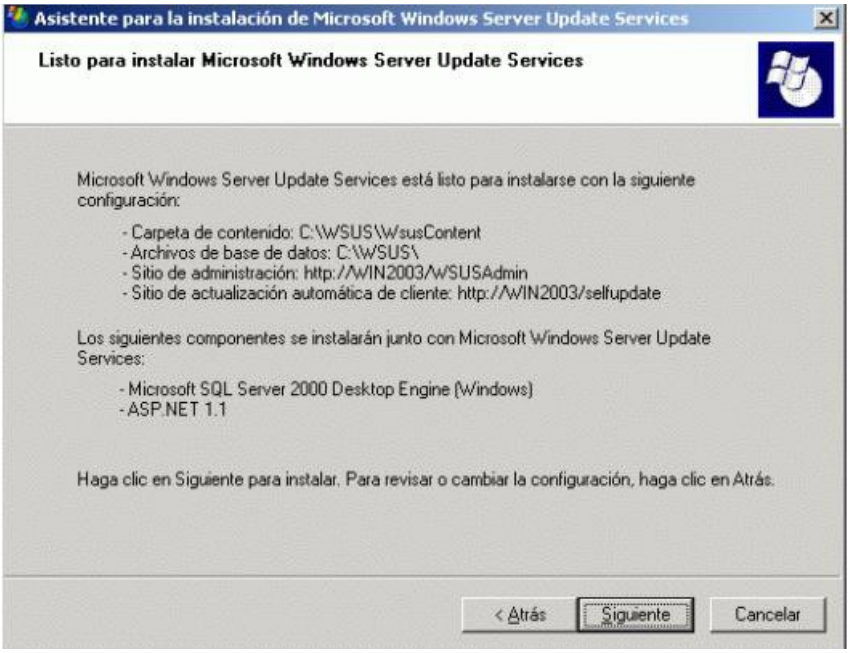
7. En la página Configuración de actualización reflejada, puede especificar la función de administración de este servidor WSUS. Si es el primer servidor WSUS de la red o desea una topología de administración distribuida, omita esta pantalla.

Si desea una topología de administración centralizada y éste no es el primer servidor WSUS de la red, active la casilla de verificación y escriba el nombre de un servidor WSUS adicional en el cuadro Nombre de servidor. Mantenga la opción predeterminada y haga click en Siguiente.



8. En la página Listo para instalar Microsoft Windows Server Update Services, revise las opciones seleccionadas y haga clic en Siguiente.

9. Si la última página del asistente confirma que la instalación de WSUS se ha realizado correctamente, haga clic en Finalizar.



4.4.2 Configuración del servicio de Actualizaciones Automáticas

Luego de instalado el servicio WSUS es necesario configurar varias opciones tanto para que el sistema empiece a descargar actualizaciones,

como para que los clientes se conecten a este servidor para obtener las actualizaciones que necesitan.

Todas las configuraciones se realizan a través de la consola de administración de WSUS. Para iniciar la consola de administración de WSUS, hacer clic en Inicio, seleccionar Todos los programas,

Herramientas administrativas y, a continuación, haga clic en Microsoft Windows Server Update Services 3.0

4.5 Correo electrónico

De acuerdo con las decisiones administrativas de unificación de servicios, conserva el servicio de correo bajo el dominio de la empresa, este servicio que se encuentra configurado en un servidor con sistema operativo Linux Centos, inicialmente se instala y configura el sistema de correo sendmail como el servicio base envío y recepción de correo electrónico, una vez instalado se debe proceder con la instalación del software MailScanner, que es un sistema de e-mail con seguridad con varias funcionalidades añadidas como AntiSpam, protección contra malware y soporte para combinación con sistemas antivirus, que mejora el control en un servicio de alto cuidado como es el correo electrónico.

La configuración de MailScanner puede ser adecuada para filtrar spam y enviarlo a una cuenta en específico, filtrado de archivos adjuntos, por tamaño o extensión para que no se filtren mensajes potencialmente peligrosos o que afecten al rendimiento del servicio, denegación de envío y recepción de correos a una cuenta especifica o a un dominio en general, así como también en caso de correos sospechosos se los almacena en un repositorio denominado de cuarentena.

4.6 Navegación y servicios Web

Para el servicio de navegación y firewall, se mantiene el servidor que utiliza GesCond247 basado en un sistema operativo Linux Centos, configurado como proxy transparente con la utilización del servicio SQUID para permitir la navegación de la red de GesCond247 a internet, basándose en reglas de navegación delimitadas por grupos (ACL); mismas que permiten que un grupo de direcciones IP tengan acceso a un listado definido de sitios web, así como también brindar acceso completo a internet sin restricciones, exceptuando listas de sitios denegados para todos los host que tengan acceso a Internet. Por

ejemplo, el personal de contabilidad necesita acceso únicamente a páginas relacionadas con entidades financieras y bancarias, al definir un ACL de este tipo se puede controlar quien navega y hacia donde lo hace, siempre conservando su línea de desempeño laboral.

Para el control de la navegación en Internet se han definido las siguientes listas de acceso:

a. Entidades Gubernamentales: contiene páginas pertenecientes a entidades del gobierno.

b. Entidades financieras y bancarias: tiene páginas pertenecientes a bancos, cooperativas y agencias afines.

c. Agencias de viajes y aerolíneas: diseñada para permitir el acceso a agencias de viajes, reservas de vuelo y páginas afines.

d. Seguridad y monitoreo: contiene páginas de agencias de seguridad y páginas de monitoreo y rastreo satelital de vehículos.

5.- IMPLEMENTACIÓN DEL PROYECTO (Procedimientos y Políticas)

5.1 Procedimiento de Configuración de equipos Cliente

Se configuró teniendo en cuenta lo siguiente:

a. Asignación de nombre del equipo: el nombre del equipo debe definirse de la siguiente manera:

1. Nombre de agencia (2 caracteres)
2. Nombre del departamento (3 caracteres)
3. Nombre de Equipo (2 digitos)

b. Ingreso del equipo al dominio: un equipo nuevo debe ser agregado como equipo cliente del dominio de la empresa, para esto se debe realizar los siguientes pasos:

1. Click en inicio
2. Click derecho en Equipo
3. Seleccionar propiedades, en la ventana de propiedades se debe hacer click en configuración avanzada del sistema.
4. En la ventana de propiedades seleccionar Nombre del Equipo. Click en el botón cambiar.
5. En la ventana de edición del nombre del equipo se procede a colocar el nombre previamente definido y en el campo Dominio se coloca gescond.com que corresponde al dominio al cual se deberá ingresar el equipo en mención.

6. Clic en Aceptar, en este momento aparecerá la solicitud de ingreso de usuario y contraseña de un usuario con permisos de administrador del dominio para que pueda el equipo ser agregado correctamente, colocarlas credenciales correctas y hacer clic en aceptar.

7. Una vez validado el acceso al dominio y el equipo haya sido agregado correctamente aparecerá un mensaje que indica que se ha unido correctamente al dominio Farmaenlace.com, clic en aceptar.

8. Se solicita reiniciar el equipo para que los cambios realizados surtan efecto es recomendable antes de seguir con cualquier configuración del equipo cliente proceder con el reinicio.

9. Cuando el equipo ya pertenece al dominio se debe ingresar al mismo con las credenciales del usuario previamente creadas en la consola de administración de Active Directory para continuar con la configuración de todos los programas y accesos que vaya a utilizar.

5.2 Creación de Usuarios en el dominio

La información necesaria para crear un nuevo usuario es:

a. Nombres del usuario a crear

b. Área donde pertenece el usuario

El procedimiento para crear un nuevo usuario es:

1. En el controlador de dominio dirigirse a Inicio>Herramientas administrativas>Usuarios y equipos de Active Directory

2. Existe un directorio ya establecido para la creación de usuarios en las áreas de la compañía. Ingresar al directorio al que corresponda el usuario.

3. En la carpeta Usuarios hacer click derecho y luego a Nuevo>Usuario

4. Se procede a llenar los campos que hay. El “Nombre de inicio de sesión de usuario” debe seguir las políticas de creación de usuarios.

5. Ingresar la contraseña por defecto que es el número de cedula del empleado. El usuario deberá cambiarla posteriormente.

6. Una vez creado el usuario hacer click derecho sobre el mismo y en “Propiedades”. En la carpeta de “Miembro de” agregar el grupo de seguridad que le corresponda, generalmente definido con el nombre de su área. Esto servirá para configuraciones automáticas y carpetas compartidas.

5.3 Creación de Cuentas de Correo y Listas de Distribución

La creación de cuentas de correo y listas de distribución de correspondencia electrónica se las debe realizar en el servidor Linux de Correo Electrónico.

Para ingresar al sistema Linux por medio de interfaz de comandos, es necesario utilizar un programa de terminal cliente para Telnet y SSH; en este caso se utiliza el programa PUTTY que utiliza como puerto de conexión SSH el puerto6222. El sistema solicita el usuario y la contraseña que corresponden a una cuenta de usuario previamente creada en el servidor.

Luego del ingreso satisfactorio, ingresar el comando: “su-” para acceder a las funciones administrativas de la consola (Súper Usuario / Root). El sistema solicitará la contraseña para este acceso.

Para acceder a los directorios del sistema ingresar el comando “mc”, lo que activará la interfaz de administración de archivos MidngthCommander y nos mostrará las carpetas y archivos que se encuentran en este servidor de una manera más intuitiva y amigable, diferente a explorar los mismos por interfaz de comandos, para poder gestionar dichos archivos y carpetas se pueden utilizar las siguientes teclas de función:

a. F2: guardar Archivo
b. F3: seleccionar texto
c. F4: abrir archivo
d. F7: buscar
e. F8: borrar un archivo o borrar una línea si se está en edición de archivos
f. F10: salir
g. Enter: ingresar dentro de un directorio.

5.3.1 Creación de cuenta de correo

Para agregar la nueva cuenta se debe digitar el comando “useradd” e ingresar el nombre de la cuenta que irá antes de la información de dominio en la cuenta de correo, es decir antes de @gescond247.com, por ejemplo, si el nuevo usuario tiene el nombre de George Prado el comando deberá ser:

useradd gprado

Una vez ejecutado este comando digitar “passwd” seguido de un espacio y el nombre de la cuenta para asignar una contraseña a la cuenta y posteriormente ingresar la confirmación de la misma, utilizando el ejemplo anterior el comando debería ser:

passwd gprado

Aparecerá un mensaje solicitando la nueva contraseña para la cuenta, digitar la contraseña y presionar Enter, luego se solicitará confirmación de la contraseña; para lo que se debe digitar nuevamente la misma clave. Si el ingreso de la información solicitada es correcto se mostrará un mensaje indicando la actualización correcta de la contraseña.

Acceder a los directorios del servidor mediante el comando “mc” y dirigirse al directorio “/etc/” y abrir el archivo “passwd” utilizando la tecla F4. Localizamos la cuenta creada recientemente y borramos el texto “/bin/bash” y agregamos al final de la línea “/sbin/nologin”. Para que no se permita acceso a la consola mediante este usuario, con lo que se logra que la cuenta creada única y exclusivamente tenga funcionalidad de enviar y recibir correo electrónico.

Como política de seguridad, únicamente las cuentas del personal de administración de sistemas y gerencia de sistemas podrán tener acceso con sus usuarios mediante la interfaz de consola, el resto de cuentas creadas en el servidor deberán tener deshabilitada dicha funcionalidad.

5.3.2 Alias y grupos de correo

Existe la posibilidad de crear alias para un correo, es decir un nombre en particular que redirige los correos hacia una o varias cuentas existentes.

Para crear un alias o un grupo de correo dirigirse al directorio: “/etc/” y abrir el archivo “aliases”.

El formato que se debe utilizar es: el alias o nombre de la lista de correo; debe ser un nombre representativo del grupo o debe ser el nombre de una cuenta de correo ya creada y necesita se reenvíe a mas destinatarios, a continuación se debe colocar dos puntos (:) y luego todas las direcciones de correo a las que se va a dirigir el correo cuando se escriba el alias como destinatario de correo

electrónico, deben ir separadas por una coma; si son direcciones que pertenecen a las cuentas de correo de GesCond247 se deberá digitar el nombre de la cuenta sin el dominio; es decir sin @gescond247.com y si son cuentas de otros dominios se deberá digitar las cuentas de correo completas.

Ejemplo:

Sistemas: ohuarcaya, fmoreno, mpalacios@hotmail.com

Cuando se termina de editar el archivo para guardarlos cambios presionar la tecla F2 y se acepta en la solicitud de confirmación y por último se cierra el archivo presionando la tecla F10.

Cuando se cierre el archivo y se vuelve a la interfaz de comandos se debe ejecutar el comando newaliases para que se procese las nuevas listas de correo.

5.4 Asignación de permisos para servicios de Internet

La asignación de permisos de navegación debe ser realizada en el servidor LINUX de navegación utilizando el servicio de proxy SQUID. El internet se configura en base a las direcciones IP (Internet Protocol) de los equipos, es decir los accesos asignan por dirección de red del equipo.

Existen tres tipos de accesos al internet:

a. Acceso libre: el equipo tiene libertad de navegación, excepto a sitios negados para toda la red que han sido definidos por la gerencia de sistemas.

b. Acceso restringido o filtrado: el equipo puede acceder a páginas específicas solicitadas por el jefe del área a la que pertenece el colaborador.

c. Acceso negado: por defecto que no permite ningún tipo de salida al internet, exceptuando la página institucional de la empresa y aplicaciones web internas (intranet).

5.4.1 Acceso libre

Para otorgar un acceso libre al internet es necesario acceder a editar el archivo que se encuentra en: “ /etc/squid/lista.txt”.

1. Dentro del archivo se debe digitar la dirección IP del equipo al que se va a dar el acceso, la máscara y como comentario luego del símbolo numeral (#) el nombre de la persona responsable del equipo como el siguiente ejemplo lo muestra:

192.168.238.76/255.255.255.255 #Acceso George Prado

2. Guardar el archivo mediante el comando F2 y posteriormente el comando F10 para volver a la consola.

3. En la consola de comandos digitar “service squid reload” para que el servicio cargue las nuevas configuraciones de navegación, en caso de no realizarse correctamente la carga de la configuración de las ACL se deberá reiniciar el servicio SQUID; para lo cual se debe digitar el comando “service squid restart”, que forzará un reinicio del servicio y dejará momentáneamente sin navegación a toda la red de la organización por el rededor de 30 segundos a un minuto.

Se puede monitorear el estado del servicio mediante el comando “service squid status” que indicará si se encuentra corriendo (running) o si presenta alguna anomalía.

5.4.2 Acceso restringido o filtrado

Para otorgar a algún equipo acceso a páginas específicas que ya han sido previamente configuradas y agrupadas por afinidad, es necesario ingresar en el directorio: “/etc/squid/”. En este directorio existen los archivos ACL con nombres como “dominiosweb(num).txt”. Dentro de estos archivos se encuentran los sitios permitidos para los usuarios que tienen este acceso y se encuentran distribuidos con los números como indica la tabla siguiente.

En caso de no existir la página deseada en ninguna de las listas se deberá registrarla en la categoría correspondiente.

NUM	DESCRIPCIÓN
0	ENTIDADES DE GOBIERNO
1	BANCOS Y ENTIDADES FINANCIERAS
2	SEGURIDAD Y MONITOREO
3	SERVICIOS Y TELECOMUNICACIONES
4	TARJETAS Y CELULARES
5	CREDITO Y CONTABILIDAD
6	GESCOND247
7	PERIODICOS Y SEGURO
8	FACEBOOK Y GMAIL
9	EMPLEO Y CAPACITACION
10	ACTUALIZACIONES ANTIVIRUS
11	PAGOS COMPRAS
12	CLIENTES MAYORISTAS

Para otorgar el acceso a dichas páginas para los equipos que deban tener el acceso, en la configuración del servicio SQUID se ha asociado a cada archivo dominiosweb un archivo ipswebque contiene la dirección IP, máscara y usuario del equipo que utiliza ese acceso, el nombre del archivo por lo general es ipsweb(número categoría).txt.

5.5 Procedimiento de Respaldo de información

La información empresarial es el activo intangible más importante de toda compañía, es sumamente importante mantener un respaldo lo más actualizado posible de los datos y aplicaciones que dan servicio a GesCond247.

Se debe tomar en cuenta dos tipos de respaldos:

a. Bases de datos: comprende toda la información contenida dentro de los servidores de Base de datos en el DataCenter, esta información por su alto nivel de actualización constante es necesario respaldarla con la mayor continuidad posible.

b. Aplicaciones: comprenden instaladores, carpetas y archivos de configuración de los sistemas que se encuentran funcionando, mismos que pueden servir para recuperar un servidor en caso de falla, deben ser respaldados una vez y actualizados únicamente cuando haya una nueva versión o se suscite un reemplazo de archivos de aplicaciones.

El Coordinador de Administración de Servicios, Redes y Telecomunicaciones es el responsable de los Backup periódicos de las Bases de Datos, se definirá un proceso automático en el sistema operativo del servidor o en el Administrador de Base de Datos para que se realicen las tareas de backup o mantenimiento de bases de datos en forma automática, no deberán ser ejecutadas manualmente.

El periodo recomendado de obtención de respaldos de bases de datos es el siguiente:

a) Se obtendrá un respaldo o backup completo de la base de datos una vez por semana.

b) Se obtendrá un respaldo diferencial de las bases de datos diariamente a las cero horas que será complementario al último backup completo obtenido en la semana anterior.

c) El periodo de resguardo de la información en respaldos históricos queda bajo decisión expresa de la gerencia de sistemas, pudiendo los

respaldos ser eliminados para recuperación de espacio de almacenamiento siempre y cuando no se elimine el respaldo total más reciente obtenido y los subsiguientes respaldos diferenciales.

La copia de los Backups de aplicaciones y bases de datos deberá ser entregado a custodia del departamento de seguridad y por ende debe ubicarse fuera del área de sistemas.

Los Backups de las aplicaciones deberán ser revisadas y probadas por los menos cada 6 meses, y cada vez que exista una nueva liberación de versiones.

5.6 Solicitud de nuevos enlaces de datos.

Se solicitará la implementación de un nuevo enlace de datos con una sucursal nueva bajo solicitud exclusiva del departamento de proyectos, quienes deberán informar con un mínimo de 45 días al área de Servicios Redes y Telecomunicaciones los datos que son:

a. Dirección exacta de la sucursal

b. Teléfono fijo de la sucursal

c. Nombre de persona de contacto

d. Teléfono fijo y celular de la persona de contacto

e. Número de sucursal correspondiente al número de establecimiento ante el SRL, que será utilizado como parámetro de la dirección IP de la red LAN de la sucursal.

Contando con los datos informativos, se procede a enviar una solicitud de verificación de factibilidad al proveedor de enlaces informando los datos de la nueva sucursal en el formulario que sea indicado para este fin.

El proveedor de enlaces de datos, receptará la solicitud, procesará la verificación de factibilidad y se reserva el derecho de aprobación o negación del servicio en base a la inspección de factibilidad. De haber algún inconveniente solucionable, el proveedor informará inmediatamente al área de Servicios Redes y Telecomunicaciones para realizar las correcciones del caso y se pueda dar una confirmación positiva de la factibilidad. En caso de darse una respuesta negativa como resultado de la inspección de factibilidad, es necesario solicitar el servicio a otro proveedor, siguiendo el mismo procedimiento de pre-factibilidad.

Si el proveedor emite una respuesta positiva a la factibilidad, este informará al área de Servicios Redes y Telecomunicaciones indicando la fecha tentativa de instalación del servicio. Llegada la fecha de instalación, el proveedor deberá informar oportunamente la hora de ingreso del personal técnico con la finalidad de coordinar en el sitio para que se permita el acceso y se brinden las facilidades necesarias para una correcta instalación.

El personal técnico de parte del proveedor asistirá al sitio y realizara la instalación siempre y cuando se cuente con las características necesarias para una correcta implementación.

Una vez realizada la instalación del nuevo enlace, se deben comunicar con el área de Servicios Redes y Telecomunicaciones para realizar las pruebas de conectividad, agregar rutas en los dispositivos de networking que según el proveedor se debe establecer las rutas adecuadas para la correcta comunicación y verificar el funcionamiento del nuevo enlace, si las pruebas resultan exitosas, el proveedor enviará por correo electrónico un acta de aceptación y puesta en marcha del enlace y si el proveedor requiere el documento deberá ser remitido por el mismo medio firmado por el personal autorizado de GesCond247.

5.7 Política de uso del correo Electrónico

Una cuenta de correo electrónico permite el envío y la recepción de mensajes y está asociada a una dirección única, tanto en el ámbito local de la empresa como en Internet.

Para acceder a una cuenta de correo se requiere la dirección única y una contraseña que identificará al usuario en el sistema. GesCond247, administra el servicio de correo electrónico bajo el dominio "gescond247.com".

La forma común de una cuenta de correo electrónico es:

<alias_usuario>@dominio_de_correo

En GesCond247, el <alias_usuario> se construye utilizando los siguientes criterios:

Primera Letra del Nombre y Apellido sin espacios intermedios y todo en minúsculas.

Los caracteres con tilde son sustituidos por el mismo carácter sin tilde, el carácter “ñ” es sustituido por la letra “n”. Si dos o más personas tienen

el mismo identificador de usuario se añadirá a la segunda persona y siguientes el segundo nombre y de coincidir se hará uso del segundo apellido.

En caso de combinaciones que deriven en palabras malsonantes podrá solicitarse el cambio de identificador de usuario.

Algunos pasos a seguir para obtener una cuenta de correo electrónico en GesCond247 son:

a. La solicitud del gerente del departamento o jefe inmediato del colaborador mediante la aplicación de Novedades de Sistemas, especificando los nombres y apellidos completos del colaborador y número de cédula de identidad, área a la que pertenece y si debe pertenecer a alguna lista de correos.

b. Para la creación de la cuenta de correo electrónico se creará con una clave que será el número de cédula la misma que deberá ser cambiada por el usuario antes de su primer acceso.

c. Es responsabilidad del usuario el cambio de clave así como mantener la confidencialidad de la misma.

d. Cada cuenta de correo electrónico tendrá un espacio de almacenamiento ilimitado en el servidor mismo que debe ser vaciado cada vez que el usuario descargue sus correos a su software cliente de correo electrónico principal.

e. Es responsabilidad del usuario depurar su cuenta periódicamente para que exista espacio disponible y administrar su correo en forma responsable.

f. La vigencia de la cuenta comprende el periodo de compromiso de trabajo entre el usuario con la empresa.

g. Es responsabilidad del usuario mantener los respaldos de su cuenta, el Departamento de Sistemas no se hace responsable por pérdidas de información. Dichos respaldos deberán hacerse con la periodicidad que el usuario disponga, para lo cual

5.7.1 Criterios para el envío de Correo Electrónico dentro de la Empresa.

a. Se privilegiará dentro de la empresa la comunicación directa frente al envío de correos electrónicos.

b. En caso de que no sea posible la comunicación directa, se podrá enviar correos electrónicos tomando en cuenta los siguientes factores:

1. El uso del lenguaje para dirigirse a los compañeros de trabajo deberá ser comercial. No se debe utilizar lenguaje coloquial.
2. Los correos electrónicos deberán tener el menor número de destinatarios; esto quiere decir, que únicamente se deberá enviar el correo al interesado, si es necesario al jefe del interesado y si es necesario al jefe inmediato de quien envía el correo. Se deberá utilizar el mejor criterio para el envío de copias, tratando de que éstas se limiten a los estrictamente necesarios.
3. Únicamente en casos excepcionales y de interés puntual los colaboradores copiaran mails a gerentes y/o vicepresidentes.
4. El Departamento de Desarrollo Humano, Departamento de Operaciones y Departamento de Tecnología y Sistemas son los únicos autorizados para enviar correos generales copiados a todos los colaboradores o a una parte de ellos; por lo tanto, si es necesario enviar circulares, se deberá acudir a estos departamentos para hacerlo de acuerdo al tema.

5.8 Política de uso de Internet

La política de uso del internet está definida para normar y delimitar el correcto uso de este servicio en la red interna de GesCond247, estableciendo parámetros y criterios que deben ser debidamente acatados por todo el personal de la empresa, las normas de utilización se describen a continuación:

a. La Red de datos de GesCond247 ha sido concebida para usos laborales, y de administración, estará a cargo del Departamento de Sistemas y administrado por el Área de Redes Servicios y Telecomunicaciones.

b. A través de los equipos de monitoreo y análisis de tráfico instalados en el Departamento de Sistemas, se detectarán a los usuarios que hagan mal uso de los servicios de Internet.

c. El acceso a la Internet es una herramienta valiosa y limitada que deberá ser usada con racionalidad, su mal uso desencadena en la deficiencia de la calidad del servicio.

d. Desde el equipo asignado a cada empleado y que tenga los permisos necesarios será posible hacer uso de Internet, únicamente para fines laborales a los sitios autorizados bajo solicitud expresa y justificada al Departamento de Sistemas, de parte de la gerencia del departamento al que pertenezca el usuario.

e. El uso de comunicación interactiva como chats, Skype, Facebook, Twitter, etc., se permitirá o denegará con previa autorización de la Gerencia de Sistemas.

f. No se permite el uso de sistemas de búsqueda y obtención de archivos de música, videos o archivos comerciales con derechos reservados y la utilización de los recursos para distribución o reproducción, de este tipo de material ya sea vía Web o medios magnéticos.

g. Está totalmente prohibido el ingreso a páginas de contenido pornográfico, descarga de programas que permitan realizar conexiones automáticas o visores de sitios clasificados como pornográficos, la utilización de los recursos para distribución o reproducción, de este tipo de material ya sea vía Web o medios magnéticos.

h. No se permite el participar en juegos de entretenimiento en línea, escuchar música en línea y cualquier servicio interactivo no autorizado.

i. El acceso a Internet y los servicios asociados deberán utilizarse para los propósitos de la propia institución, de forma consistente con las funciones laborales del empleado.

j. El usuario final de Internet, deberá verificar que la información accedida no contenga virus informático o cualquier otro software que ponga en riesgo los bienes o servicios la empresa, antes de ser instalado en algún equipo de cómputo.

k. Emplear el menor número de instancias del explorador de Web en forma simultánea. (No abrir varias ventanas a la vez), si no está navegando por Internet, cierre todas las ventanas abiertas de su explorador.

5.9 Política De Seguridad De Información

Esta política se aplica a todas aquellas personas que utilizan bienes de información, bienes físicos y bienes informáticos de GesCond. Entendiéndose como bienes de información: a los archivos, documentos del sistema, base de datos; como bienes físicos: a computadoras, equipos de comunicación y como bienes informáticos: a aplicaciones y programas informáticos.

Es necesario preservar los siguientes principios de la seguridad informática:

a. Confidencialidad: asegurar que únicamente personal autorizado tenga acceso a la información.

b. Integridad: garantizar que la información no sea alterada, eliminada o destruida por entidades no autorizadas.

c. Disponibilidad: asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

1. Parámetros referentes a usuarios

a. El usuario es único e intransferible, el propietario de la cuenta de usuario será responsable de todas las acciones que sean realizadas en el sistema o en los equipos de GesCond.

b. Todos los accesos deben ser aprobados por el jefe de área.

c. El nombre del usuario estará creado con la primera letra del primer nombre del usuario, seguida sin separaciones del apellido con un máximo de 10 caracteres en total, sin signos de puntuación, símbolos, tildes, eñes o espacios.

d. En caso de coincidir con otro usuario se utilizará la inicial de su segundo nombre y el apellido.

e. En caso de repetirse tanto la inicial del primer como del segundo nombre se utilizará ambas iniciales y el apellido.

f. La creación del usuario se hará con una contraseña por defecto (Numero de Cédula), el usuario tiene la obligación de cambiarla el momento que crea pertinente y será responsable de la misma desde el primer ingreso al sistema.

2. Referente a control de activos

Cada usuario será responsable de los equipos informáticos e información obtenida en la empresa; que haya sido otorgada como herramienta de

trabajoy se encuentren para uso propio o de las personas que tienen a cargo, entiéndase: computadoras, teléfonos, impresoras, equipos de comunicación, POS datafast y medianet, e información en cualquier formato obtenida desde los sistemas de GesCond.

3. Referente a confidencialidad

Con el fin de evitar un acceso no autorizado a los bienes de información que pueda causar una utilización no apropiada de información confidencial o delicada, el usuario tiene la obligación de utilizar contraseñas complejas que guarden las siguientes características mínimas y que han sido adoptadas como políticas de seguridad:

a. La clave no puede ser el mismo nombre de usuario ni la contraseña por defecto.

b. La clave debe tener un mínimo de 9 caracteres.

c. La clave debe poseer números y letras.

d. La clave debe ser cambiada cada 120 días.

e. La clave no puede ser la misma de las últimas dos veces que ingresó una clave nueva.

f. El usuario será bloqueado por 30 minutos luego de 2 intentos fallidos de ingreso a la red.

Queda estrictamente prohibido la utilización de cuentas de usuarios que no corresponden a la persona misma; sea para accesos a las áreas, accesos a los sistemas o códigos para llamadas, así como difundir la información de las contraseñas personales. El propietario de la cuenta de usuario será responsable de cualquier acto que se realice con la misma. De esta manera el Departamento de Sistemas puede asegurar la confidencialidad de la información, donde solo las personas autorizadas puedan acceder a la misma.

4. Referente a uso de recursos

a. Todas las herramientas tales como computadoras, programas y dispositivos externos que GesCond dispone para el normal desenvolvimiento de sus colaboradores, son estrictamente para uso concerniente a la empresa. Queda prohibido la instalación de cualquier tipo de programa que no haya sido aprobado por el Departamento de Sistemas, con el fin de precautelar la información, evitar daños en los

equipos computacionales sea en Software o Hardware y evitar problemas legales.

b. El usuario tiene la obligación de guardar en dispositivos externos propios todo tipo de información de índole personal. El Departamento de Sistemas tiene la potestad de auditar cada una de las máquinas; como procedimiento de rutina sin previo aviso ni necesidad de la presencia del usuario y borrar cualquier tipo de programa no aprobado, así como información que no corresponda a la actividad empresarial de GesCond y que signifique más del 5% del espacio en disco (entiéndase música, videos, fotografías, documentos, etc.).

c. El usuario tiene la obligación de informar al Departamento de Sistemas de cualquier actividad informática ocasionada por terceros que disminuyen su capacidad productiva, tales como virus, correo no deseado, accesos indebidos, daños en los programas, etc. El Departamentode Sistemas está en la obligación de utilizar los medios disponibles para solucionar todo este tipo de inconvenientes.

El Departamento de Sistemas tiene la obligación de mantener estable la operación de los sistemas y telecomunicaciones con el fin de mantener la disponibilidad de la información, para que los usuarios autorizados puedan acceder a la misma en cualquier momento que sea necesario. Además de proteger la infraestructura informática de programas mal intencionados, hackers y hacer respaldos de la información de las bases de datos y la información que los usuarios consideren importante. Con este fin puede tomar las medidas de contingencia que sean convenientes mediante procedimientos debidamente documentados.

5.10 Planes de contingencia

Un plan de contingencia se refiere a un manual que contenga la información de cómo proceder de manera reactiva en el caso de un evento que produzca una falla o que provoque una suspensión de un servicio; dicha falla puede darse por diversos factores tanto lógicos como físicos, el plan de contingencia debe indicar los procedimientos a realizar para la recuperación de la estabilidad de los servicios en el menor tiempo posible y con el menor impacto de operatividad hacia el usuario final.

En GesCond los enlaces de datos se han convertido en las arterias

principales de la empresa puesto que es por donde se mantiene la comunicación tanto de datos como de voz desde las oficinas centrales hacia oficinas remotas y puntos de venta, existen dos principales eventos que pueden producirse y que afectan al normal funcionamiento de un enlace de datos que se detallan a continuación:

a. Caída de enlace de datos: una caída en el enlace se refiere a la pérdida total de conectividad desde la oficina matriz hacia un punto remoto, puede darse debido a los siguientes factores:

1. Falla eléctrica en el punto destino.
2. Falla en el equipo de enlace de datos por inhibición o por dato del equipo.
3. Desconexión de cableado de red.
4. Falla a nivel de proveedor.

El medio de detección del estado del enlace de datos es por medio del sistema de monitoreo de redes instalado en el área de Redes Servicios y Telecomunicaciones.

b. Intermitencia del enlace de datos: en ocasiones puede presentarse el caso de que un enlace de datos tiene tiempos de respuesta sumamente altos, o incluso pérdida de paquetes, generalmente detectados por los usuarios debido a que tienen lentitud en los sistemas o errores de comunicación constantes, estos síntomas son reportados por parte de los usuarios del punto remoto o por el personal de soporte técnico que realiza conexiones de asistencia remota a los usuarios ubicados en puntos distantes, para esto se debe proceder de la siguiente manera:1. Realizar una inspección a los tiempos de respuesta del enlace de datos por medio del comando PING inicialmente hacia el equipo Ruteador ubicado en el sitio remoto y luego a los equipos computacionales de la red LAN en dicho lugar.

2. Si se tiene tiempos de respuesta superiores a los 100ms, el problema puede ser debido a saturación del canal, para lo cual se debe preguntar al personal si se está realizando una transferencia de información demasiado grande o de pronto algún correo electrónico tiene un adjunto de gran tamaño, es necesario identificar el problema ya que es posible que sea debido a motivos de la red interna.

3. Si los tiempos de respuesta son moderados y a pesar de esto se tiene pérdida de paquetes puede ser por motivo de inhibición del equipo del enlace (Router o Módem) o una falla en la conexión del cableado que va al equipo del enlace, para lo cual es necesario comunicarse telefónicamente con el personal en el sitio para que realice una revisión y de ser el caso reinicie el equipo del enlace de datos.
4. Si aun después de estas pruebas el enlace de datos no ha vuelto a su normalidad es necesario reportarlo con el proveedor del enlace para que proceda con una revisión más exhaustiva ya que el problema puede ser a nivel de la red del proveedor y son ellos quienes deben realizar las revisiones respectivas.
Puede presentarse el caso de una pérdida de rutas a nivel de la red LAN de GesCond, para lo cual es necesario revisar la configuración de los equipos de conmutación ubicados en GesCond Matriz, el equipo que debe revisarse es el Switch Core, que es el que mantiene rutas hacia los distintos puntos remotos, puede revisarse por medio de la interfaz web de una manera más fácil e intuitiva y accesible o de ser necesario revisar la configuración del dispositivo por medio de una conexión vía Telnet.

5.10.1 Enlaces de Datos

En GesCond los enlaces de datos se han convertido en las arterias principales de la empresa puesto que es por donde se mantiene la comunicación tanto de datos como de voz desde las oficinas centrales hacia oficinas remotas y puntos de venta, existen dos principales eventos que pueden producirse y que afectan al normal funcionamiento de un enlace de datos que se detallan a continuación:

a. Caída de enlace de datos: una caída en el enlace se refiere a la pérdida total de conectividad desde la oficina matriz hacia un punto remoto, puede darse debido a los siguientes factores:

1. Falla eléctrica en el punto destino.
2. Falla en el equipo de enlace de datos por inhibición o por dato del equipo.
3. Desconexión de cableado de red.

4. Falla a nivel de proveedor.

El medio de detección del estado del enlace de datos es por medio del sistema de monitoreo de redes instalado en el área de Redes Servicios y Telecomunicaciones.

b. Intermitencia del enlace de datos: en ocasiones puede presentarse el caso de que un enlace de datos tiene tiempos de respuesta sumamente altos, o incluso pérdida de paquetes, generalmente detectados por los usuarios debido a que tienen lentitud en los sistemas o errores de comunicación constantes, estos síntomas son reportados por parte de los usuarios del punto remoto o por el personal de soporte técnico que realiza conexiones de asistencia remota a los usuarios ubicados en puntos distantes, para esto se debe proceder de la siguiente manera:1. Realizar una inspección a los tiempos de respuesta del enlace de datos por medio del comando PING inicialmente hacia el equipo Ruteador ubicado en el sitio remoto y luego a los equipos computacionales de la red LAN en dicho lugar.

2. Si se tiene tiempos de respuesta superiores a los 100ms, el problema puede ser debido a saturación del canal, para lo cual se debe preguntar al personal si se está realizando una transferencia de información demasiado grande o de pronto algún correo electrónico tiene un adjunto de gran tamaño, es necesario identificar el problema ya que es posible que sea debido a motivos de la red interna.

3. Si los tiempos de respuesta son moderados y a pesar de esto se tiene pérdida de paquetes puede ser por motivo de inhibición del equipo del enlace (Router o Módem) o una falla en la conexión del cableado que va al equipo del enlace, para lo cual es necesario comunicarse telefónicamente con el personal en el sitio para que realice una revisión y de ser el caso reinicie el equipo del enlace de datos.

4. Si aun después de estas pruebas el enlace de datos no ha vuelto a su normalidad es necesario reportarlo con el proveedor del enlace para que proceda con una revisión más exhaustiva ya que el problema puede ser a nivel de la red del proveedor y son ellos quienes deben realizar las revisiones respectivas.

Puede presentarse el caso de una pérdida de rutas a nivel de la red LAN de GesCond, para lo cual es necesario revisar la configuración de los equipos de conmutación ubicados en GesCond Matriz, el equipo que debe revisarse es el Switch Core, que es el que mantiene rutas hacia los distintos puntos remotos, puede revisarse por medio de la interfaz web de una manera más fácil e intuitiva y accesible o de ser necesario revisar la configuración del dispositivo por medio de una conexión vía Telnet.

5.10.2 Correo Electrónico

El servicio de correo electrónico es de suma importancia dentro de la empresa y es utilizado ampliamente por la mayoría de colaboradores de la misma; en cuanto a este servicio se pueden presentar varios inconvenientes que afecten al correcto funcionamiento como son:

a. Encolamiento excesivo de correos

El servicio de correo maneja una cola que almacena todos los correos que los usuarios envían, generalmente los correos que pertenecen al dominio gescond.com son enviados de inmediato y los correos que tienen destinatarios de otros dominios externos son despachados siempre y cuando el servidor de correo de destino responda a la petición de envío de correo. Para visualizar la cola de correos en el servidor es necesario conectarse vía SSH a la consola de comandos del servidor Linux y digitar el comando mailq, lo que listará todos los correos que se encuentran por despacharse en el servidor y si se desea una descripción más detallada se añade elparámetro (-v), que listará la misma lista pero con características más detalladas de cada correo, como fecha de emisión, estado del envío y tamaño del mismo. Se considera normal ver un encolamiento de hasta 10 correos, cuando se supere ampliamente esta cantidad en la cola puede deberse a factores tales como:

1. Caída del servicio de Internet: al no tener conectividad a Internet no será posible despachar correo electrónico a cuentas externas, es necesario restablecer el servicio de internet para que el servicio vuelva a restablecerse.

2. Dominio en listas negras: puede darse el caso que debido a una alta cantidad de envío de correo, o envío de coreos con adjuntos sospechosos considerados virus o Spam, el dominio sea reportado a nivel internacional como peligroso y las entidades reguladoras en internet coloquen al dominio gescond.com en lo que se denomina listas negras; para solventar este inconveniente es necesario ingresar a las páginas de administración de Listas negras y solicitar se elimine el dominio de dicho listado, ya que cuando un correo se envía, el servidor de correo destinatario revisara si el dominio de origen esta reportado como sospechoso y rechazara el correo que se está tratando de enviar.

3. Rechazo por parte de los servidores de destino: también puede darse el caso que los servidores de destino rechacen el envío de correo por fallas atribuibles a sus servicios, porque están en mantenimiento o están fuera de servicio, en ese momento la cola de correo mantendrá él envió en pendiente por un lapso aproximado de dos horas, si al pasar este tiempo aún no se ha podido realizar un envío exitoso, el servidor enviará una advertencia al remitente indicándole que hay una demora en la entrega de su correo y esperará un lapso adicional de cuatro horas, al finalizar este tiempo dicho correo será eliminado de la cola y se notificará nuevamente al remitente, no es necesaria ninguna acción en este caso salvo averiguar el estado de los dominios de correo destinatarios.

4. Tamaño excesivo en archivos adjuntos: si existen correos cuyo contenido es demasiado grande debido a redacción o archivos adjuntos, el despacho hacia el destino será más lento y ocupará el ancho de banda de mayor manera, provocará que los correos que se agreguen a la cola posteriores al correo de gran tamaño se mantengan a la espera de que el proceso de envió finalice y la cola irá creciendo, para solventar este caso es necesario ingresar a la carpeta donde se encuentran almacenados los correos por despachar ubicada en: /var/spool/MailScanner/mqueue. Localizar el correo que tiene gran tamaño y proceder a eliminarlo de la lista para lograr que los demás correos encolados puedan fluir de

manera normal.

b. Caída del servicio de envío/recepción de correos

Si se presenta una caída en el servicio de correo electrónico, es necesario en primer lugar revisar el estado del servicio, esto se lo realizaconectándose al servidor Linux por medio del terminal Telnet SSH y en la consola de comandos se debe digitar: service MailScanner status.

Debe mostrarse el estado del servicio de correo electrónico, para determinar que el servicio se encuentra operativo la respuesta de este comando debe ser OK. En el caso de que la respuesta del comando sea FAILED o ERROR, se debe reiniciar el servicio como primera medida de contingencia digitando el comando service Mailscanner restart.

El servicio debería restablecerse y la respuesta al comando debe ser OK, si el servicio no se ha restablecido luego de esta acción, el problema con el servicio puede ser debido a corrupción en un archivo del sistema que
corresponde a este servicio.

Para recuperar la configuración correcta de los archivos de correo, es necesario acudir a los archivos de respaldo, que según la política de obtención de respaldos, en los servidores Linux se deben obtener diariamente. Los respaldos están ubicados dentro del servidor Linux de correo en el directorio /etc/home/monitorns/respaldos/ en donde se encuentra un respaldo de todos los archivos de configuración clasificados por fecha y con el mismo esquema de ordenamiento de carpetas y subcarpetas.

c. Daño físico del servidor

Si el servidor presenta un daño físico que implique que el mismo deje de funcionar correctamente, es necesario identificar de forma inmediata cual es el componente que está fallando y si es posible reemplazarlo para recuperarla operatividad estos componentes podrían ser memoria, procesador, MotherBoard, tarjeta de red, fuente de poder.

Los componentes pueden ser reemplazados sin pérdida de

información y puede ser necesario que se configure los controladores de los nuevos dispositivos para que el servidor vuelva a trabajar de manera normal. Este caso no se aplicaría si el daño se presenta en el disco duro del servidor, en este caso es necesario una vez que se ha reemplazado el disco duro se debe realizar los siguientes pasos:

1. Configurar el sistema operativo.
2. Instalar y configurar los dispositivos y periféricos del servidor.
3. Copiar y reemplazar los archivos recientemente instalados por los archivos de configuración que se encuentren en los respaldos del servidor, la primera fuente de recuperación de archivos de respaldo es el disco duro del servidor que guarda sus respaldos en una unidad diferente a los archivos originales; si no se tiene acceso a esta fuente, se debe recurrir a los respaldos de archivos de manera externa que han sido entregados al departamento de seguridad y se encuentran fuera de las instalaciones de GesCond.
4. Probar la configuración y funcionamiento del servidor.

5.10.3 Navegación Web

La pérdida del servicio de navegación web o acceso al Internet, puede presentarse debido a fallas internas o externas, dentro de las fallas externas se tiene como posible una falla en el servicio de internet por parte del proveedor en su infraestructura física de última milla o su salida internacional; compete al proveedor realizar las revisiones correspondientes para el restablecimiento del servicio.

Si la falla es a nivel interno pueden presentarse los siguientes casos:

a. Caída del servicio de proxy Squid

Si se presenta una caída en el servicio de proxy transparente, es necesario en primer lugar revisar el estado del servicio como tal, se realiza conectándose al servidor Linux de navegación y firewall por medio del terminal TelnetSSH y en la consola de comandos se debe digitar: service squid status.

Debe mostrarse el estado del servicio, para determinar que el servicio se encuentra operativo la respuesta de este comando debe ser OK. Si la respuesta del comando sea FAILED o ERROR, se debe

reiniciar el servicio como primera medida de contingencia digitando el comando service squid restart. El servicio debería restablecerse y la respuesta al comando de revisión de estado debe ser OK; si el servicio no se ha restablecido luego de esta acción, el problema con el servicio puede ser debido a corrupción en un archivo del sistema que corresponde a este servicio.

Para recuperar la configuración correcta de los archivos de correo es necesario acudir a los archivos de respaldo, que según la política de obtención de respaldos, en los servidores Linux se deben obtener diariamente. Los respaldos están ubicados dentro del servidor Linux de Correo en el directorio /etc/home/monitorns/respaldos/ en donde se encuentra un respaldo de todos los archivos de configuración clasificados por fecha y con el mismo esquema de ordenamiento de carpetas y subcarpetas.

Con la utilización de un gestor de archivos como por ejemplo MidnigthCommander, proceder a evaluar y detectar el archivo que contenga el error de configuración y localizar su similar en los respaldos y proceder a sustituirlo en el archivo original.

b. Daño físico del servidor

Si el servidor presenta un daño físico que implique que el mismo deje de funcionar correctamente, es necesario identificar de forma inmediata cual es el componente que está fallando y si es posible reemplazarlo para recuperarla operatividad; estos componentes podrían ser memoria, procesador, MotherBoard, tarjeta de red, fuente de poder, todos ellos pueden ser reemplazados sin pérdida de información y puede ser requerido se configure los controladores de los nuevos dispositivos para que el servidor vuelva a trabajar de manera normal. Este caso no se aplicaría si el daño se presenta en el disco duro del servidor, en este caso es necesario una vez que se ha reemplazado el disco duro se debe realizar los siguientes pasos:

1. Configurar el sistema operativo
2. Instalar y configurar los dispositivos y periféricos del servidor3. Copiar y reemplazar los archivos recientemente instalados por los archivos de configuración que se encuentren en los respaldos del servidor, la primera fuente de recuperación de archivos de

respaldo es el disco duro del servidor, que guarda sus respaldos en una unidad diferente a los archivos originales; si no se tiene acceso a esta fuente, se debe recurrir a los respaldos de archivos de manera externa que han sido entregados al departamento de seguridad y se encuentran fuera de las instalaciones de GesCond.

4. Probar la configuración funcionamiento del servidor.

5.10.4 Servidores de aplicaciones

La falla de un servidor de aplicaciones es de alta criticidad, ya que la mayoría de servicios y sistemas en GesCond funcionan bajo el modelo cliente servidor; es decir si un servidor de aplicaciones falla, implica que los sistemas que se encuentran corriendo en dicho servidor se tornen inaccesibles; afectando al normal desenvolvimiento del trabajo diario de la empresa, cabe hacer mencionar que en GesCond no se ha establecido un proyecto aún de virtualización de servidores, por lo que la operatividad de estos equipos se mantiene de manera física; es decir cada servidor tiene su propio sistema operativo y aplicaciones instaladas sobre este.

Los posibles casos de falla de un servidor de aplicaciones son los siguientes:

a. Configuración o actualización de versiones de sistemas

Como política se indica que toda actualización de sistemas, reconfiguración o instalación de nuevas versiones debe realizarse si no es imperativo en horarios fuera de oficina, con la finalidad de minimizar el impacto en operatividad al usuario final. Si la actualización es

imperativa y es necesaria para corregir un error en el funcionamiento del sistema, se lo debe hacer en horarios de labores si no existe otra opción.

Se recomienda que antes de aplicar la actualización o instalación de nuevas versiones, se obtenga un respaldo completo de los archivos que van a ser modificados o reemplazados en un dispositivo externo o una carpeta segura dentro del servidor, de tal manera que se pueda acceder a ellos de forma inmediata en

caso de producirse un error en la actualización. Una vez obtenidos los respaldos y notificados a los usuarios de los sistemas; se debe proceder a realizar la actualización, configuración o instalación de nuevas versiones; en el caso de presentarse un inconveniente que denote que el servicio no está funcionando correctamente, es necesario deshacer dicha actualización; para esto se debe recuperar los archivos respaldados y reemplazarlos en el lugar original, con lo que el sistema recobrará su funcionalidad normal con la versión o configuración anterior.

Una vez recuperado el funcionamiento del sistema, se debe proceder a notificar a los usuarios y se debe mantener un monitoreo y comunicación constante con los mismos; hastaasegurarse de la estabilidad del sistema o el correcto funcionamiento de los servicios.

b. Falla física que no produce suspensión de sistemas y servicios

Un servidor de aplicaciones robusto siempre tiene en su estructura física sistemas de respaldo en caso de fallas de este tipo, por ejemplo poseen dos fuentes de poder redundantes, arreglos de discos duros RAID que pueden estar en nivel 1, 1+0, 5, etc. De tal manera que en el caso de presentarse una falla física en uno de estos componentes, el servidor emite una señal de alarma; sea grafica por medio de un LED encendido, una alarma sonora o mensajes de advertencia al ejecutar herramientas de diagnóstico.

Si se presenta una falla de nivel físico en un componente que tiene respaldo, el rendimiento del servidor se verá afectado pero no implicará una falla o suspensión de los sistemas dejando de funcionar; el procedimiento para restablecer el normal funcionamiento del servidor es el siguiente:

1. Identificar el componente físico que tiene avería.
2. Identificar si el equipo se encuentra en garantía, si es así se debe reportar el caso al centro de soporte técnico de la marca del servidor y abrir un caso indicando la falla del componente y la necesidad de su reemplazo, el servicio técnico dependiendo del

plan de soporte enviará un repuesto o asignará personal técnico en un tiempo prudencial para realizar la reparación del equipo.

3. Si el equipo no tiene plan de garantía o soporte, revisar si se tiene en stock un repuesto de similares características, caso contrario se debe proceder con la adquisición inmediata del componente.

4. Una vez con el componente disponible se debe proceder con su reemplazo; si el componente permite un reemplazo con el equipo encendido se lo puede hacer inmediatamente, como es el caso de discos duros que permiten hacer reemplazo en caliente (Hot Swap).

Si ese no es el caso, se debe programar el mantenimiento correctivo del servidor lo más pronto posible y en horas fuera del horario laboral; donde se procederá a apagar el servidor y reemplazar la pieza dañada, con lo que se recupera funcionalidad total del equipo.

c. Falla física que implica suspensión de sistemas y servicios

Si se produce una falla en un equipo servidor que implique una caída total del servicio debido a una falla en un componente físico, implica una necesidad urgente de recuperar el servicio para esto realizar los pasos siguientes.

1. Si es posible, obtener un respaldo de los archivos más actualizados de las aplicaciones para ser instalados y configurados en un servidor de respaldo.

2. Configurar un servidor de respaldo de manera inmediata con sistema operativo y aplicaciones que posee el equipo averiado, para esto se debe apoyar en los manuales de configuración e instalación entregados por los proveedores de software, se recomienda mantener similares características físicas al servidor de producción, en caso de no poseer un servidor físico se puede configurar un equipo virtual, que inclusive puede ser una imagen exacta del servidor de producción abstraída con anterioridad y reemplazar los archivos de configuracióncon los más actuales obtenidos en los respaldos de información.

3. Colocar en funcionamiento el servidor de reemplazo y notificar a los usuarios para que continúen con sus labores normales.
4. Identificar si el equipo se encuentra en garantía, de ser afirmativo se debe reportar el caso al centro de soporte técnico de la marca del servidor y abrir un caso indicando la falla del componente y la necesidad de su reemplazo, el servicio técnico dependiendo del plan de soporte enviará un repuesto o enviará personal técnico en un tiempo prudencial para realizar la reparación del equipo.
5. Si el equipo no tiene plan de garantía o soporte, revisar si se tiene en stock un repuesto de similares características, caso contrario se debe proceder con la adquisición inmediata del componente.
6. Una vez con el componente de reemplazo disponible se debe proceder a reemplazar en el servidor y recuperar su funcionalidad normal.
7. Con el servidor recuperado y si es necesario, reemplazar inmediatamente el servidor de respaldo por el original de producción, notificar a los usuarios la suspensión temporal del sistema, desactivar el servidor de reemplazo y colocar en su lugar el servidor de producción y ponerlo en funcionamiento. Notificar a los usuarios la restitución del servicio y mantener un constante monitoreo y comunicación con los usuarios hasta determinar la estabilidad del sistema.

5.10.5 Bases de Datos

En GesCond se mantiene un sistema de almacenamiento de información basado en un equipo Storage que tiene una capacidad aproximada de 3 TB y está configurado en varios LUNs o unidades lógicas; mismas que están presentadas a los principales servidores que mantienen los motores de bases de datos, debido a esta configuración los posibles puntos de falla que se pueden presentar son:

a. Falla en el servidor de Base de Datos

Al referirse a una falla en el servidor de base de datos, estamos incurriendo en un caso similar al descrito anteriormente para los

servidores de aplicaciones y por ende, se deben seguir los mismos pasos que ya fueron detallados para fallas físicas que no afectan a los servicios o fallas físicas que provoquen una suspensión del servicio; con la diferencia que en este último caso, donde se necesita configurar un nuevo servidor de respaldo, se debe poder configurar al servidor para que tenga conectividad con el dispositivo de almacenamiento Storage y se le puedan presentar las unidades lógicas LUNs correspondientes, con lo que se lograría una restitución del servicio lo más pronto posible.Si no hay forma de conectar el servidor al Storage, en el momento de preparación del servidor, se debe verificar que tenga espacio suficiente de almacenamiento para soportar el tamaño de las bases de datos que se encuentran fuera de servicio y proceder a restaurar las bases de datos obteniendo del respaldo de información más reciente posible, para garantizar la menor pérdida de información, esto basándose en los procedimientos de obtención de respaldos de la información.

Una vez restablecido el servicio de motor de base de datos y restaurado las bases de datos para su utilización, se debe probar conectividad al servidor y estabilidad de los sistemas que acceden a las bases de datos así como la consistencia de la información, para luego pasar a informar
a los usuarios de la normalización de los sistemas.

b. Falla en el Storage

En el caso de presentarse una falla en el dispositivo de almacenamiento Storage, las fallas pueden ser: de configuración, daño físico que no afecten al funcionamiento del Storage o daño físico que detengan el Storage por avería.

La principal recomendación es siempre mantener los respaldos de la información de bases de datos lo más actualizada y reciente posible.

Al igual que los servidores, un sistema de Storage mantiene componentes redundantes; de tal manera que si uno de ellos falla, no implica una caída total del sistema de almacenamiento con una suspensión de los servicios y sistemas que aprovechan la base de

datos; sino que pueden ser reemplazados sin afectar al funcionamiento o con una incidencia baja sobre el rendimiento de los sistemas. El proceso a seguir para el reemplazo de un componente averiado es el mismo que el descrito para los servidores.

Si se presenta una falla que afecte al funcionamiento completo del sistema de almacenamiento Storage, es necesario restaurar las bases de datos de ser posible en los mismos servidores en una unidad local para no necesitar configuración en servidores de respaldo.

c. Corrupción o pérdida de información de la Base de Datos

De presentarse un evento de corrupción de la información o pérdida de datos en una base, se debe identificar las tablas afectadas y evaluar si dicha información puede ser recuperada sin necesidad de restaurar la base de datos completa; caso contrario se debe informar a todos los usuarios del sistema afectado por la falla de información de la base de datos que se realizará la suspensión temporal del sistema y proceder con la restauración de la base de datos dentro del mismo dispositivo de almacenamiento Storage.

6.- CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Se ha evaluado y diseñado la infraestructura del DataCenter siguiendo las recomendaciones que establece la norma TIA-942, tratando en lo posible de implementarlo; se han tenido restricciones en cuanto a aprobación de presupuesto en algunos de los casos, teniendo que dejar temas pendientes para implementarlos en el futuro como por ejemplo un sistema de extinción de incendios que utilice agentes limpios.

Se tuvo la dificultad para la implementación de piso elevado o piso técnico debido a la altitud de la estructura del edificio de GesCond que no es suficiente para dicha implementación.

No se ha implementado una puerta de seguridad con barra de salida en caso de emergencia, debido a negativa aprobación de presupuesto; en su lugar se ha instalado una puerta insulada de panel de fibra de vidrio

con abertura hacia fuera que brinda características de seguridad, acceso y facilidad de uso suficientes para el actual habitáculo del DataCenter.

En la implementación del proyecto se ha hecho evidente que siempre es necesario recurrir a la guía de estándares y normas ya establecidas, que sirven para implementar de manera correcta y con un fundamento adecuado, la toma de decisiones sin consideración de estas recomendaciones y reglamentos pueden incurrir en errores de implementación, que a corto o mediano plazo provocaran fallas en el correcto desempeño del área o de los sistemas y servicios implementados en la empresa.

Los servicios implementados se encuentran en funcionamiento y demás de ellos se
han venido implementando nuevos servicios y sistemas de acuerdo a las nuevas
necesidades de la empresa, servicios que no forman parte de este proyecto o han
sido solo mencionados en el texto. El TIER del DataCenter de GesCond es considerado de nivel 1, aún queda mucho trabajo por hacer para que el DataCenter aspire a un nivel de Tier que permita tener un rango aceptable, de acuerdo a lo que recomiendan las normas para un correcto diseño de un DataCenter, por lo que el trabajo del presente proyecto solo ha sido una parte inicial.

6.2 Recomendaciones

Se recomienda seguir las normas establecidas para DataCenter para las futuras adecuaciones o mejoras que se planeen hacer al DataCenter de GesCond y continuar con el trabajo de implementar un mejor DataCenter para minimizar los riesgos y sobre todo la afectación a servicios por falla, sean humanas o no.

Se recomienda optimizar y mejorar los sistemas de respaldos y recuperación de información y aplicaciones, ya que al momento se está realizando únicamente para bases de datos y muy poca atención se lo está dando a las aplicaciones más que a instaladores y versionamientos.

Se recomienda dar a conocer al detalle todos los documentos relacionados con políticas y procedimientos inicialmente al área de sistemas completa y luego al personal en general de la empresa y velar

por su aceptación y correcta aplicación, no con el afán de castigar a los usuarios sino de fomentar una cultura de correctoaprovechamiento de los recursos que GesCond brinda para el desempeño de las labores diarias de cada colaborador.

Se recomienda la eliminación de los equipos que no son servidores dentro del DataCenter de GesCond aprovechando las capacidades de los nuevos equipos servidores que han sido adquiridos o implementando nuevos equipos, que tengan características robustas capaces de soportar la demanda de servicios de GesCond, así como también dar de baja aquellos equipos que ya han cumplido su vida útil dentro de los servidores de GesCond.

Bibliografía Anexos

[1] Tanenbaum 5ta Edición. Capítulo 1. Apartado 1.2.2 Redes de área local (páginas 17-20).

[2] Tanenbaum 5ta Edición. Introducción (página 2).

[3] Tanenbaum 5ta Edición. Capítulo 1. Apartado 1.2.4 Redes de área amplia (páginas 20-21).

[4] Tanenbaum 5ta Edición. Capítulo 1. Capa de transporte (página 40).

Simulación usando el Cisco Packet Tracer Student